



Anomali ThreatStream Next Gen

User Guide

August 31, 2026

ANOMALI®

Copyright Notice

Copyright © 2026 Anomali, Inc. All rights reserved.

Anomali is a registered trademark, ThreatStream is a registered service mark, and Optic, Integrator, STAXX, Anomali Enterprise, Anomali Match, Anomali Security Analytics, Anomali Lens, and Anomali Copilot are trademarks of Anomali, Inc.

All other brands, products, and company names used herein may be trademarks of their respective owners.

Support

Support Portal	https://support.anomali.com
Email	support@anomali.com
Phone	+1 844-4-THREATS

ThreatStream Next Gen Documentation Updates

Date	Description
Aug 30, 2026	Added "Security Operations Overview" on page 16. Added Fleet Overview . Added "Entity Management" on page 160.
Aug 5, 2026	Updated the Threat Model section in PIR: Output Step . Updated the History tab details in "Viewing PIR Details" on page 229. Updated "Dashboard Actions" on page 11. Updated "Using Anomali AI in ThreatStream Next Gen" on page 293.
Jul 30, 2026	Added a note to the PIR: Process Step .
Jul 23, 2026	Added the History Tab to "Viewing PIR Details" on page 229.
Jul 15, 2026	Added the Output Tags option to PIR: Description Step . Added tag creation and tag filtering to "Accessing Organization Reports" on page 273. Added observable association details to PIR: Output Step . Added the Collection Tags option to PIR: Description Step .
Jun 24, 2026	Added "Managing Access to PIRs" on page 241.
Jun 10, 2026	Updated supported browsers in Navigating ThreatStream Next Gen . Added the lookback window option to PIR: Inputs Step .

CONTENTS

ThreatStream Next Gen Documentation Updates	3
Chapter 1: ThreatStream Next Gen Overview	6
Chapter 2: Command Center: Global Threat Landscape	8
Data Generation and Dashboard Architecture	9
Dashboard Actions	11
Chapter 3: Intelligence Search	14
Fields Queried in Intelligence Searches	14
Chapter 4: Security Operations Overview	16
From Logs to Detections	17
From Detections to Alerts	18
From Alerts to Incidents	20
Incident Investigation	20
From Incidents to Cases	21
Approval Queue	22
Human Actions in the SOC Workflow	23
Detection Rules	24
Alert Rules	42
Detections	70
Alerts	78
Incidents	97
Cases	120
Chapter 5: Integrations Marketplace	154
Jira MCP Integration	156
Slack MCP Integration	157
Chapter 6: Entity Management	160

Understanding Entities and Peer Groups	160
Entity Sources	161
Risk Score Modifiers	162
Managing Entities and Groups	162
Identities	163
Assets	178
Peer Groups	191
Entity Risk Scores	199
Entity Summary Widgets	204
Chapter 7: Priority Intelligence Requirements	206
Accessing Priority Intelligence Requirements	207
Creating a PIR	211
Viewing PIR Details	229
Managing PIRs	234
Chapter 8: Case Management	245
Accessing Organization Cases	245
Creating a Case	248
Viewing Case Details	249
Managing Cases	256
Creating and Managing Case Types	265
Chapter 9: Security Reporting	272
Accessing Organization Reports	273
Creating a Report	275
Viewing Report Details	279
Managing Reports	281
Using Report Templates	286
Chapter 10: Using Anomali AI in ThreatStream Next Gen	293
What You Can Do	294
Send Documentation Feedback	296

Chapter 1: ThreatStream Next Gen Overview

ThreatStream Next Gen is an advanced cyber threat intelligence platform designed to help you reduce manual effort, improve visibility, and respond faster to emerging threats. Instead of relying on disconnected tools, repetitive research, and time-consuming workflows, ThreatStream Next Gen brings intelligence operations into one unified environment powered by Anomali AI-assisted automation.

With ThreatStream Next Gen, you can spend less time gathering and organizing data, and more time focusing on the threats and decisions that matter most to your organization.

The platform combines the following integrated capabilities:

- **Command Center** provides a single, personalized dashboard tailored to your organization and industry vertical. It surfaces what matters now — active attacker operations, trending malware, trending vulnerabilities, targeted entities, and curated global news — without requiring you to go looking for it.
- **Intelligence Search** enables you to search across observables, threat models, and feed data from one location. Anomali AI-generated summaries help explain relationships and provide additional context.
- **Integrations Marketplace** serves as your central location for managing ThreatStream Next Gen integrations. From one place, you can configure and manage available integrations.
- **Priority Intelligence Requirements (PIRs)** automate recurring intelligence questions and continuously monitor the data sources you choose. PIRs identify new findings, avoid duplicate reporting, and generate outputs such as threat models, tagged indicators, alerts, tickets, and notifications.
- **Case Management** allows you to investigate, track, and resolve intelligence-driven work directly within the platform. Cases stay linked to related observables, threat models, and PIRs helping preserve context throughout the investigation process.
- **Reporting** helps you create and share professional intelligence reports using reusable templates. You can communicate findings clearly to leadership, stakeholders, and operational teams.

Together, these capabilities create a connected workflow that supports how modern intelligence teams operate. You can monitor priority risks automatically, investigate findings efficiently, and communicate outcomes consistently without switching between multiple systems.

ThreatStream Next Gen is built to help you move from manual processes to scalable intelligence operations, so your team can focus on analysis, decision-making, and protecting the business.

Chapter 2: Command Center: Global Threat Landscape

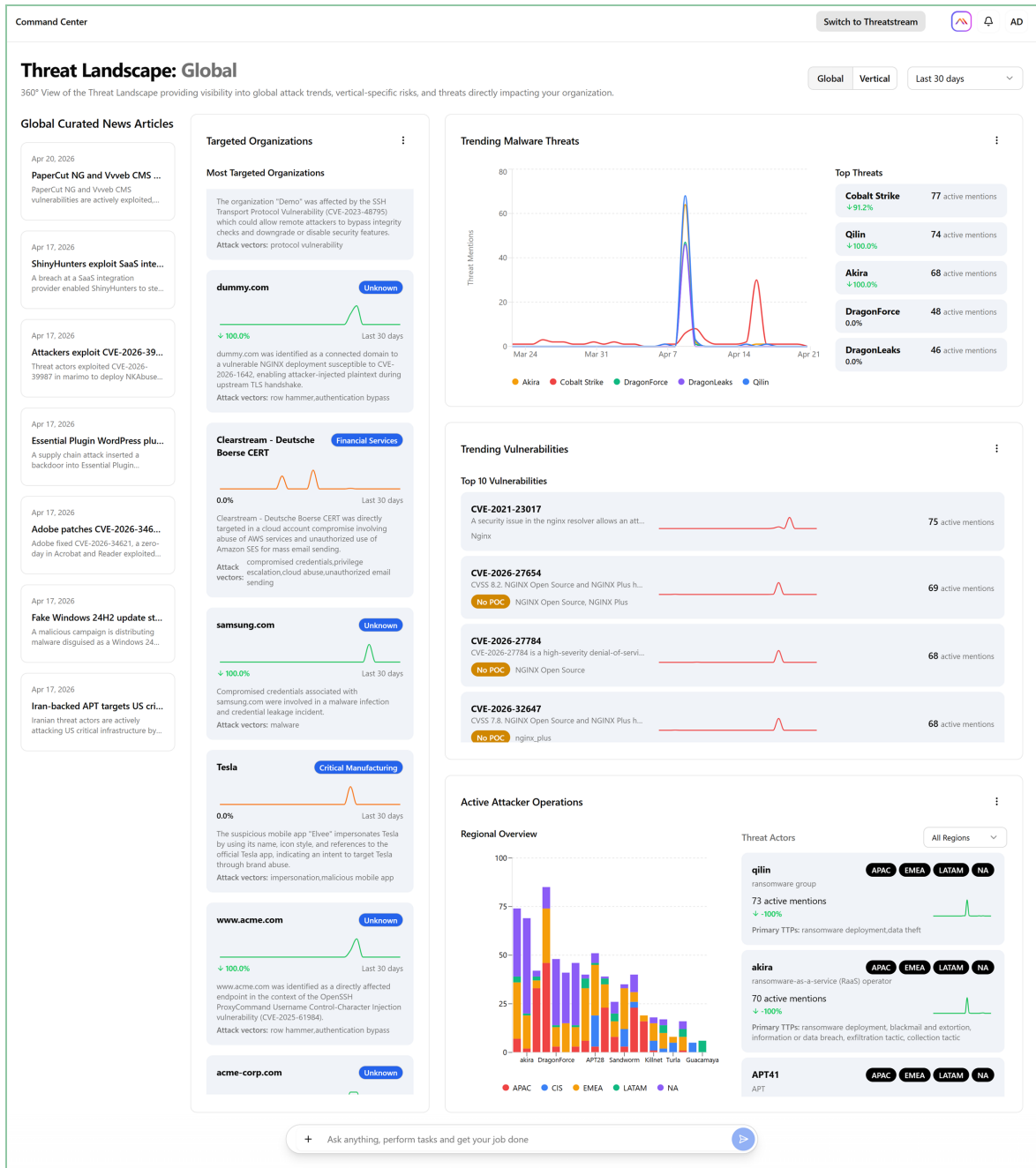
This topic covers the following sections:

Data Generation and Dashboard Architecture	9
Dashboard Actions	11

The **Global Threat Landscape** dashboard (also referred to as Command Center) is designed to replace the traditional data-heavy home view with a more focused, Anomali AI-driven experience that surfaces relevant, timely, and actionable intelligence as soon as you log in. Serving as your starting point for understanding the current threat landscape, Command Center eliminates the need to piece together information across multiple tools by providing a single, centralized dashboard. It brings together the most important intelligence for your organization—such as active attacker operations, trending malware and vulnerabilities, targeted entities, and curated global news—so you can immediately see what matters most.

Once on the dashboard, you can interact with any widget object to quickly orient yourself and take action. Clicking an object opens a concise Anomali AI-generated summary, giving you an at-a-glance understanding of the threat or event. From there, you can dive deeper by opening the object in the threat model advanced search page to explore the underlying source data. When you need to document or share your findings, you can copy a summary to the clipboard or export an object to PDF in just a few clicks.

By consolidating key insights and putting these actions upfront, Command Center helps you prioritize your work and move from awareness to action with greater speed and clarity.



Data Generation and Dashboard Architecture

All dashboard content is generated through curated queries and processed in a nightly batch job, with the results cached to ensure fast page loading. The data presented is based on open-source intelligence and does not include any customer-private information.

The Global Threat Landscape dashboard offers two views:

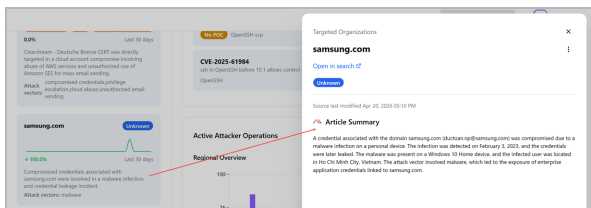
- **Global:** displays global widget data based on open-source intelligence available for Anomali.
- **Vertical:** displays details specific to the industry selected from the drop-down list. The Vertical list includes the following industries, which are aligned with the STIX 2.1 and CISA critical infrastructure sector vocabularies.
 - Aerospace
 - Automotive
 - Chemical
 - Commercial
 - Construction
 - Dams
 - Defense
 - Education
 - Emergency Services
 - Energy
 - Entertainment
 - Finance
 - Food
 - Government
 - Healthcare
 - Hospitality-Leisure
 - Insurance
 - Legal
 - Manufacturing

- Nuclear
- Retail
- Technology
- Telecommunications
- Transportation
- Utilities
- Water

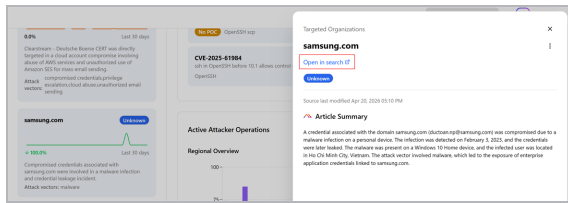
Dashboard Actions

On the Global Threat Landscape dashboard, you can quickly understand what's happening by viewing concise summaries of widget objects. If you need to share or document your findings, you can export widget data as a PDF or copy the widget summary for use elsewhere. When a summary isn't enough, you can dive deeper by navigating to dashboard object sources on the threat model advanced search page and exploring the data deeper.

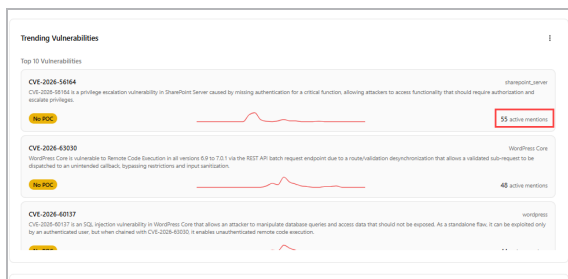
- **To view a dashboard object summary**, click the object of your interest. The summary window opens.



- **To view sources of a dashboard object**, click the object of your interest and then click **Open in search**. You are redirected to the threat model advanced search query page where you can view all threat models that served as a source for creating the dashboard object.

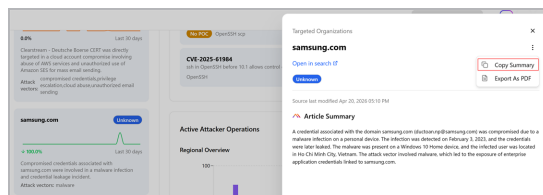


The **Trending Vulnerabilities** widget also includes the number of active mentions, which represents the total number of threat intelligence entities—such as Threat Bulletins, Malware entities, Vulnerabilities, and Actor records—that reference the vulnerability by name, alias, tag, or within their content during the selected 7-, 30-, or 90-day period. The total number of mentions is the sum of the daily trend counts.



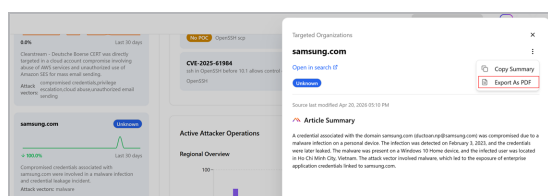
- **To copy a summary of a dashboard object:**
 - a. Click the object of your interest.
 - b. In the summary window, click the more options menu (...).
 - c. Select **Copy Summary**.

The summary is copied to the clipboard. You can paste it anywhere you need.



- **To export a dashboard object to PDF:**

- a. Click the object of your interest.
 - b. In the summary window, click the more options menu (...).
 - c. Click **Export As PDF**.
- The download process starts immediately.



Chapter 3: Intelligence Search

This topic covers the following sections:

- Fields Queried in Intelligence Searches 14

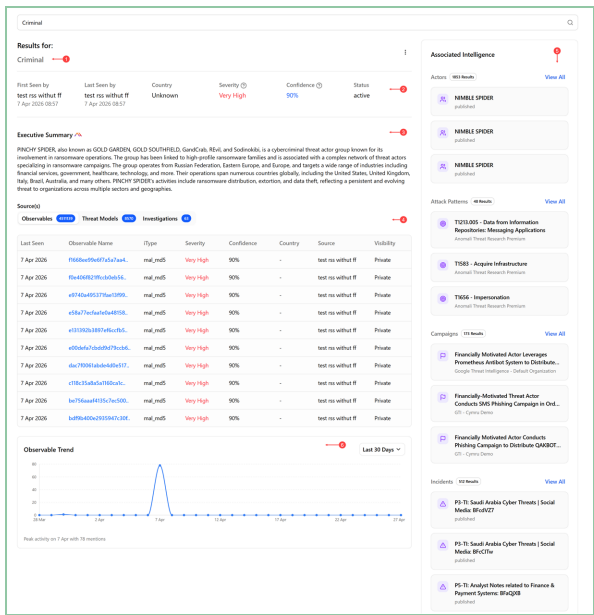
The **Intelligence Search** page provides a unified search experience across all historical observables, threat models, and feed data. You can receive AI-generated natural language explanations of how observables relate to threat motivations and threat models — turning raw search results into actionable context.

The search box on the Intelligence Search page queries all available observables and threat model entities in a single search. Search queries are not case sensitive and results are returned regardless of case.

Fields Queried in Intelligence Searches

Universal search queries observable values for observables and Aliases, Descriptions, Names, and Tags for threat model entities.

Below is an example of search results for the query Criminal.



- 1 Entered keyword that returned the results below.
- 2 Metadata that includes earliest created and last modified date, source, country of origin, severity, confidence, and status.

- 3 Anomali AI-generated executive summary for the query search results.
- 4 Intelligence associated with the results returned: observables, threat models, and investigations. You can click any of the listed items to drill down into their details.



Note: Only observables with the status Active are queried.

- 5 **Associated intelligence:** Threat models associated with the intelligence returned in search results.
- 6 **Observable Trend:** Select the time range for the observable trend. Available options include: 7 days, 30 days, and 90 days.

Chapter 4: Security Operations Overview

- From Logs to Detections 17
- From Detections to Alerts 18
- From Alerts to Incidents 20
- Incident Investigation 20
- From Incidents to Cases 21
- Approval Queue 22
- Human Actions in the SOC Workflow 23
- Detection Rules 24
- Alert Rules 42
- Detections 70
- Alerts 78
- Incidents 97
- Cases 120

Anomali Agentic SOC Operations provides a structured workflow that helps you move from raw security telemetry to investigation and case management within the platform. The workflow progressively turns security activity into events that require more focused attention:

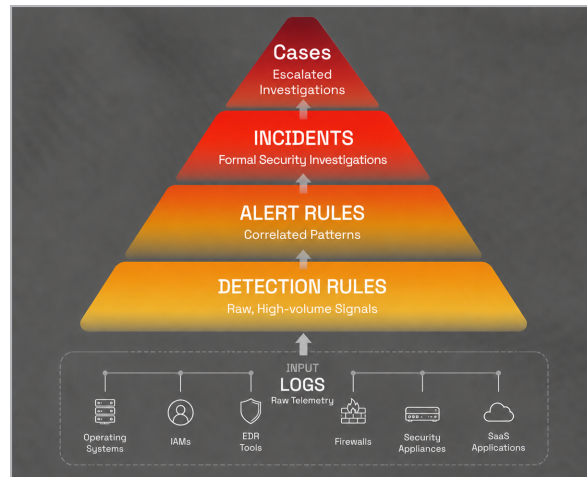
Logs → Detections → Alerts → Incidents → Cases

The workflow is designed to reduce the time required to move from a raw signal to a resolved case.

The Agentic Fleet performs triage, correlation, investigation, and case analysis work that would otherwise require significant analyst effort, and presents the resulting decisions and recommendations for human review where required.

Detection and alert rules define which activity is important in your environment. Anomali Agentic Fleet then analyzes the resulting alerts, investigates incidents, and organizes the resulting investigations into cases. Throughout the workflow, the Anomali Unified Response Agent (AURA) coordinates the appropriate agents and platform capabilities, while platform governance controls determine which recommendations require human approval.

For more information about AURA, see [Understanding AURA](#).



SOC Operations workflow: Logs provide input to Detection Rules, and activity becomes progressively more actionable through Alerts, Incidents, and Cases.



Note: The agents analyze, investigate, and document security activity and recommend what should happen next. They do not carry out response actions in your environment. Remediation steps such as isolating a host or blocking a domain are performed by you after you review the recommendation.

From Logs to Detections

Logs provide the foundation for the SOC operations workflow. They contain raw telemetry collected from sources across your environment, such as operating systems, identity and access management systems, EDR tools, firewalls, security appliances, and SaaS applications.

Detection rules evaluate this data using scheduled Anomali Query Language (AQL) searches with configured search schedules and look-back windows. You can use pre-built detection rules or create custom rules with AQL queries or natural-language prompts.

When activity in the logs matches a detection rule, the Anomali platform generates a detection. You can review generated detections in the Detections dashboard, where related activity is organized by severity and associated MITRE ATT&CK tactics.

Detection rules establish the first layer of logic in the workflow and are fully controlled by you. The agentic workflow does not define or replace these rules, or independently create alerts from raw logs.

For details on configuring detection rules, refer to ["Detection Rules" on page 24](#).

From Detections to Alerts

Alert rules evaluate the generated detections to identify activity that requires further attention. An alert can be based on a single detection or a pattern involving multiple detections. Alert rules can identify significant individual events, repeated activity, or related activity that forms a larger pattern.

When the conditions of an alert rule are met, Anomali platform generates an alert. By default, alerts generated by an alert rule are automatically evaluated by AURA's specialized agent—the Alert Triage Agent—using relevant context, such as enrichment data, entity risk, historical activity, threat intelligence, and relationships with other alerts. It can also identify situations where multiple alerts become significant when considered together. The agent also takes the alert severity and its own confidence into account.

Based on its analysis, the Alert Triage Agent then **recommends** one of the following actions:

- **Promote:** AURA has enough evidence to recommend moving the alert to an incident for formal investigation. Promote does not mean that AURA has definitively determined that the activity is malicious. When AURA recommends Promote, the recommendation is presented for human approval. After approval, Anomali creates the incident and preserves the relevant source-alert linkage automatically.
- **Investigate:** The available evidence is not sufficient to recommend promotion or monitoring, therefore, the Alert Triage Agent will continue to investigate further. An alert with an Investigate recommendation remains an alert and stays In Progress. No incident is created at this point. If the deeper investigation produces enough evidence to warrant promotion, the resulting Promote recommendation follows the normal approval path, as described in ["From Alerts to Incidents" on page 20](#).
- **Monitor:** The available evidence does not justify creating an incident, but it also does not provide enough positive evidence to classify the activity as benign.
- **False Positive:** The available evidence clearly shows why the activity is benign.



Note: A lack of evidence that the activity is malicious is not, by itself, enough to classify an alert as a false positive.

While Investigate, Monitor, and False Positive recommendations do not require any action from you, the Promote recommendation is sent to the Approval Queue for your approval. See ["Approval Queue" on page 22](#).

Investigate and Monitor are working states rather than final outcomes:

- An alert with an **Investigate** recommendation remains with the Alert Triage Agent, which continues to gather evidence. You cannot change the recommendation while the agent is still working on the alert. When sufficient evidence is available, the agent revises its recommendation.
- An alert with a **Monitor** recommendation is re-evaluated on a schedule. Each re-evaluation looks for additional evidence that would support promoting the alert or classifying it as a false positive.

Alerts with an Investigate or Monitor recommendation do not appear in the Approval Queue. You can view them on the Alerts page. See ["Alerts" on page 78](#).

Alerts classified as False Positive are automatically resolved and removed from the active work queue. The decision, rationale, and supporting evidence remain part of the auditable history of the alert for later review. You can view the alerts marked as False Positive on the Alerts page. See ["Alerts" on page 78](#).

If you do not want alerts automatically evaluated by the Alert Triage Agent, that is, if you want to review alerts yourself, you can disable the Auto Triage with AURA setting when setting up an alert rule. Alert rules with Auto Triage with AURA disabled are not automatically evaluated by the Alert Triage Agent and must be triaged manually. See ["Creating Alert Rules" on page 45](#) for details.

Triaging an Alert Manually

You can run the Alert Triage Agent on an individual alert at any time. Open the alert and select **Triage with AURA**. Use this to triage alerts generated by alert rules that have Auto Triage with AURA disabled. See ["Viewing Alert Details" on page 81](#) for details.

When you invoke an agent manually, it operates within your assigned role and permissions. See [Governance, Permissions, and Human Control](#).

Alert Status and Agent Activity

When the Alert Triage Agent picks up an alert, the alert status changes to In Progress. An alert with a status of Open has not been picked up by an agent because its alert rule has Auto Triage with AURA disabled, or because it existed before Agentic SOC was enabled in your environment (applicable to customers migrating from an existing environment).

Alerts and incidents that an agent has handled and that are waiting on your decision display a Decision required badge. This badge does not appear on records that are not handled by an agent.



Note: Agents evaluate alerts generated after agents are enabled in your environment. Alerts that already existed at that time are not evaluated retroactively. You can triage them with **Triage with AURA**.

From Alerts to Incidents

When the Alert Triage Agent recommends promotion of an alert to an incident, the recommendation appears in the Approval Queue. After you approve the recommendation, the agent creates the incident and associates the source alert or alerts with it. A group of related alerts can be promoted together so that you do not need to create the incident and link the alerts manually.

The incident is then automatically handed off to the Incident & Investigation Agent for further investigation. You do not need to perform a manual hand-off before the incident investigation begins.

Incident Investigation

The Incident & Investigation Agent performs a hypothesis-driven investigation of the incident and its associated alerts.

During the investigation, the agent:

- Identifies the entities involved
- Reviews relevant context and previous activity
- Develops an investigation hypothesis
- Runs targeted searches against the security data available in your environment
- Uses the results to confirm, deny, or refine the hypothesis

The agent evaluates the available evidence and records its investigation findings and supporting evidence.

You do not need to follow each investigation step. All of these happen autonomously, orchestrated by AURA. At the end of the investigation, the Incident & Investigation Agent recommends one of two incident outcomes, which you see in the Approval Queue:

- **Escalate**—when broader investigation, response, or coordination is required.
- **Close**—when no further case-level handling is required. A closure reason is required, such as resolved, benign, suspicious, duplicate, superseded, or inconclusive. If the available evidence remains inconclusive, the incident remains under investigation according to the re-investigation workflow rather than being closed automatically.



Note: When the evidence is incomplete, conflicting, or requires stronger validation, the Incident & Investigation Agent can perform structured multi-perspective hypothesis testing. This analysis deliberately looks for both supporting and contradictory evidence, including evidence that could disprove the current hypothesis. As the evidence changes, confidence in the resulting recommendation can increase or decrease. A lower confidence score means the available evidence is weaker or more conflicting; it does not mean that the agent run failed.

From Incidents to Cases

After you approve an escalation recommendation, the Anomali platform creates the case and the Case Management Agent enriches and manages the case from that point on. It assembles the complete picture of the activity, including alerts, incidents, investigation evidence, threat intelligence, organizational context, and relevant history.

What a Case Contains

The agent organizes the case into a narrative describing what happened, the findings that support it, and recommended next steps. The case record can include any or all of the following that are available:

- The incidents linked to the case and their investigation results



Note: When another incident is linked to an existing case, the Case Management Agent re-runs its review so the case summary, evidence, correlations, and recommendations reflect the newly added information.

- The source alerts associated with those incidents

- The entities involved in the activity
- Linked threat intelligence, including indicators from ThreatStream
- Related cases that involve the same entities or activity

Recommended Response Steps

The agent recommends these steps. It does not perform them. You review the recommended steps and carry them out in your environment.

See ["Using the Response Workbook" on page 139](#) for details.

Assigning and Closing a Case

The Case Management Agent does not assign cases to users. After you review a case, assign it to the appropriate analyst or team. Close the case when the response is complete. See ["Managing Access to Cases" on page 142](#) for details.

Evidence and Audit History

The evidence collected during triage, investigation, and case compilation is retained with the case and can be reviewed at any time. The case audit history records the actions taken on the case and distinguishes activity performed by an agent, a system component, or a human user. See [Viewing Case Details](#) for details.

Exporting a Case Report

You can export a case as a formatted report targeted to different audiences, such as an executive summary for management or a technical report for analysts. Report content is generated from the evidence and information already associated with the case rather than requiring you to recreate the investigation manually. See ["Exporting Cases" on page 145](#) for details.

Approval Queue

The Approval Queue is the primary workspace for decisions that require your attention.

Approval Queue
Review agent-proposed actions, monitor autonomous activity, and manage auto-approval rules.

Approval Queue

Q Search requested actions... Criticality Risk Type Status: decision_required Reset

Items per page: 10 1-10 of 2,093 Results < Previous 1 2 3 ... Next > @

Requested action	Criticality	Type	Risk	Policy	Age	Status
C2 Multi-Host Beaconing — PROMOTE	Critical	human	Critical	soc:alert_triage-f628	just now	Decision Required
C2 Multi-Host Beaconing — PROMOTE	Critical	human	Critical	soc:alert_triage-4cd3	13m ago	Decision Required
C2 Multi-Host Beaconing — PROMOTE	Critical	human	Critical	soc:alert_triage-42ff	29m ago	Decision Required
C2 Multi-Host Beaconing — PROMOTE	Critical	human	Critical	soc:alert_triage-7a35	43m ago	Decision Required
C2 Multi-Host Beaconing — PROMOTE	Critical	human	Critical	soc:alert_triage-a1fe	56m ago	Decision Required
Test	High	human	High	soc:alert_triage-3edc	1h ago	Decision Required
Test	High	human	High	soc:alert_triage-836f	1h ago	Decision Required
C2 Multi-Host Beaconing — PROMOTE	Critical	human	Critical	soc:alert_triage-c5a6	1h ago	Decision Required
C2 Multi-Host Beaconing — PROMOTE	Critical	human	Critical	soc:alert_triage-411f	1h ago	Decision Required

Instead of showing you every alert generated in your environment, the queue focuses on agent recommendations and workflow decisions that require human approval. For alert triage, this typically means reviewing a recommendation to promote an alert or group of related alerts to an incident. You can also see incident-level recommendations, such as escalating an incident to a case or closing an incident.

Not every agent decision requires your review. Depending on the applicable governance controls, AURA can handle some supported dispositions without waiting for your approval. For example, an alert with positive evidence that it is benign can be automatically classified as a false positive. An alert that requires continued observation can remain in the monitoring workflow. Automatically handled decisions remain traceable. When the workflow supports it, you can review or override an automatically applied disposition.

When you review a decision in the Approval Queue, you can see the recommendation, confidence, evidence, reasoning, and history. Use this information to make your decision. When you override an agent disposition, the override is recorded in the audit history.

For details on using the Approval Queue, see [Using Approval Queue](#).

Human Actions in the SOC Workflow

In the overall agentic SOC workflow, the following remain your responsibility:

- Configure detection rules. See ["Creating Detection Rules" on page 27](#).
- Configure alert rules. See ["Creating Alert Rules" on page 45](#).
- Examine the Approval Queue for tasks that require your input: an alert that needs to be triaged to the Promote verdict or an incident that should be Escalated to a

case or Closed. See [Using Approval Queue](#).

- Review cases on the Cases page. See ["Cases" on page 120](#).
- Perform the recommended response actions. See ["Using the Response Workbook" on page 139](#).

Detection Rules

The **Detection Rules** page is where you view, filter, create, and manage detection rules created within your organization. Detection rules form the foundation of your threat detection pipeline, generating detections that ultimately feed into alerts for analysts to investigate. Each rule defines a specific pattern of suspicious activity, expressed as an AQL query or generated from a natural-language AI prompt, and runs continuously against incoming log data on a configurable schedule. A detection is automatically generated whenever the pattern matches.

Every rule includes a risk score, one or more MITRE ATT&CK technique mappings, and an OCSF category, helping you prioritize and triage detections consistently across your environment. You can use Anomali pre-built detection rules (coming soon) or create your own. The output of a rule feeds directly into alert rules, which group and escalate detections into alerts for analysts to investigate. For more information on alerts, see ["Alerts" on page 78](#).

To access your detection rules, navigate to **ThreatStream Next Gen > Security Operations > Detection Rules**.

Name	Risk Score	MITRE Techniques	OCSF Category	Frequency	Last Triggered	Source	Status
qa-api-run-history-86cc898a	3	—	Authentication	Just now	Just now	Custom	Enabled
qa-api-match-row-comment-364ab607	3	—	Authentication	Just now	Just now	Custom	Enabled
qa-api-run-comment-9bd0badd	3	—	Authentication	Just now	Just now	Custom	Enabled
qa-api-nomatch-56c42770	2	—	Authentication	4h ago	4h ago	Custom	Disabled
qa-api-e2e-ab22cb02	3	—	Authentication	Just now	Just now	Custom	Enabled
qa-api-cross-19-history-c2629f12	3	—	Authentication	Just now	Just now	Custom	Enabled
qa-api-cross-17-rule-B-74d78e47	4	—	Authentication	4h ago	4h ago	Custom	Disabled
qa-api-cross-17-rule-A-12224d18	4	—	Authentication	4h ago	4h ago	Custom	Disabled
qa-api-cross-15-disable-5cd77683	3	—	Authentication	Just now	Just now	Custom	Enabled
qa-api-threshold-prereq-bda1dd39	3	—	Authentication	Just now	Just now	Custom	Enabled

- 1 Search:** Search detection rules by their names. The search is case insensitive and updates incrementally.
- 2 Status:** Filter detection rules by their status—Enabled, Disabled, or All.
- 3 OCSF Category:** Filter rules by their assigned Open Cybersecurity Schema Framework (OCSF) category.
- 4 MITRE Technique:** Filter rules by MITRE ATT&CK technique ID or name. For example, T1021 or Remote Services.
- 5 Source:** Filter rules by their origin.
- 6 Name:** Name of the rule. Click the name to open the rule configuration view.
- 7 Risk Score:** A circular badge showing the risk score of the rule, on a scale of 1 (lowest) to 5 (highest). See ["Entity Risk Scores" on page 199](#) for details.
- 8 MITRE Techniques:** The MITRE ATT&CK technique(s) associated with the rule, shown as badges. When more techniques are mapped than can be displayed, an overflow badge (+N) indicates additional techniques.
- 9 OCSF Category:** The OCSF category assigned to the rule. For example, System Activity, Network Activity, or Discovery.

- 10 Frequency:** A 7-day sparkline showing how often the rule has been triggered recently.
- 11 Last Triggered:** Timestamp of when the rule most recently fired.
- 12 Source:** Indicates where the rule came from.
- 13 Status:** Toggle to enable or disable the rule directly from the list. Toggling a status of the rule takes effect immediately and is recorded in the audit trail. For other ways of enabling/disabling rules, see ["Enabling Detection Rules" on page 38](#) and ["Disabling Detection Rules" on page 37](#).



Note: Only Organization Administrators, rule owners, or users who have both the Manage Detection Rules permission and write ACL on the specific rule can enable/disable it. See ["Detection Rule Actions and Their Required Permissions" on page 41](#) for details.

- 14 More options menu:**
- **Edit:** Edit the detection rule. See ["Editing Detection Rules" on page 32](#) for details.
 - **Duplicate:** Create a copy of the rule that can be customized independently. See ["Duplicating Detection Rules" on page 35](#) for details.
 - **Test Rule:** Test the detection rule. See ["Testing Detection Rules" on page 36](#) for details.
 - **Manage Access:** Define who can access the detection rule. See ["Managing Access to Detection Rules" on page 40](#) for details.
 - **Disable/Enable:** Turned the detection rule off/on. See ["Disabling Detection Rules" on page 37](#) and ["Enabling Detection Rules" on page 38](#) for details.
 - **Delete:** Delete the detection rule. See ["Deleting Detection Rules" on page 39](#) for details.
- 15 View Settings:** Select the columns and table density (default or compact) to be displayed. By clicking the drag handle icon (⋮), drag and drop columns to change their position in the table. To return the view back to its default settings, click **Reset View**.
- 16 New Rule:** Create a new detection rule. For details, see ["Creating Detection Rules" on the next page](#).

Creating Detection Rules



Note: Only Organization Administrators and users with the Manage Detection Rules permission can create detection rules. See [Managing Roles](#) for details.

The detection rule creation process includes defining the rule and its detection logic, configuring the OCSF category, look-back window, run schedule, risk score, and optional MITRE ATT&CK techniques, and then validating and testing the rule before publishing it. Query validation enables you to identify issues that could result in noisy, duplicate, or unusable detections before the rule runs in production.

Validation happens in two tiers, run in sequence:

Validation	Description
Tier 1	<i>Checks if the rule is correctly constructed.</i> Runs automatically on every field or query edit. Hard blocks disable further rule testing.
Tier 2	<i>Checks if the rule works well with data in your environment.</i> When Tier 1 validation passes successfully, simulates runs using the lookback and run interval of the rule to check volume, entity resolution, and duplicates.

To create a new detection rule:

1. Navigate to **ThreatStream Next Gen > Security Operations > Detection Rules**.
2. Click **New Rule**.
3. On the New Detection Rule page, configure the following fields:

Field	Description
Name	Enter a unique name for the detection rule. For example, <i>Failed API activity</i> .

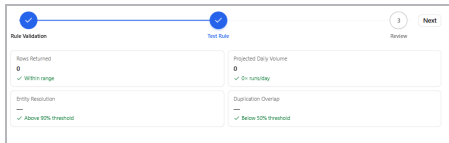
Field	Description
Description	(Optional) Enter a description for the detection rule. For example, <i>Detects failed API activity attempts by human user accounts, excluding machine-generated noise.</i>
AQL/NL Prompt	Define the rule detection logic in one of the following ways: ▪ AQL: write an AQL query. For example, <pre>ocsf where class_name = 'API Activity' AND activity_id = 2 AND status = 'Failure' AND actor.user.name IS NOT NULL AND actor.user.name NOT LIKE '%\$' fields actor.user.name, actor.user.uid, src_endpoint.ip, message, severity, activity_ name</pre> ▪ AI Prompt: describe what this rule should detect. For example, <i>Alert when a user logs in from two different countries within 30 minutes.</i> Click Generate AQL to generate an AQL query for this request.
OCSF Category	Select an OCSF category associated with this detection rule. See Supported OCSF Categories for details.

Field	Description
Look Back	Select how far back into the data lake a detection rule must reach every time it runs: 15 minutes, 1 hour, 4 hours, 24 hours, or 7 days. Note that Lookback Window should always be equal to or greater than the Run Schedule interval, to ensure no log data falls outside the query window between runs. For example, if a rule runs every 30 minutes, but only looks back 15 minutes, there is a 15 minute gap of logs that never gets evaluated by any run.
Run Schedule	Select how often you want to run this detection rule: every 5 minutes, every 15 minutes, every 30 minutes, hourly, every 6 hours, every 12 hours, or daily.
Risk Score	Set the risk score for the detection rule. For more information on risk scores, see "Entity Risk Scores" on page 199 .
MITRE ATT&CK Techniques	(Optional) Select MITRE ATT&CK techniques associated with this detection rule.

The validation agent performs a static analysis of AQL structure and rule configuration, including detection configuration, AQL query, and alert-rule checks (Tier 1). The analysis is performed automatically when a rule field or AQL query is created or modified. If a hard block is found, the Test Rule action and activation are disabled until the issue is resolved. Warnings do not prevent testing. See ["Troubleshooting Rule Validation and Test Issues" on the next page](#) for troubleshooting recommendations.

4. When no issues are detected, click **Next**.

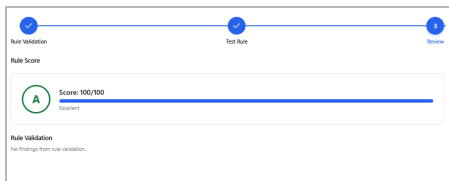
5. Click **Test Rule** to run the specified query against recent data from your environment and confirm it is valid (Tier 2). If the test is unsuccessful returns no results, see "[Troubleshooting Rule Validation and Test Issues](#)" below for troubleshooting recommendations.



6. Review the rule score. The rule readiness score ranges from 0 to 100 and reflects the results of validation. The score includes warning deductions from Tier 1 and Tier 2 runtime calibration results. It is broken down in the UI into AQL Query, Detection Config, Alert Rules, and Runtime.

A score below 50 is classified as poor and indicates high risk. Review the category breakdown and address the warnings or runtime findings that have the greatest effect on the score. A low score does not by itself indicate that the rule is blocked, but it is a strong indication that improvements are recommended before activation.

7. Click **Publish Rule**.



The detection rule is added to the list of rules on the Detection Rules page.

Troubleshooting Rule Validation and Test Issues

During detection rule creation, validation checks the rule configuration and AQL query before you activate the rule. Tier 1 performs static validation automatically when you create or modify the rule. After Tier 1 completes without blocks, use Test Rule to run Tier 2 validation against recent data from your environment. Use the validation results to identify issues that could prevent the rule from running correctly or reduce the quality of the detections it produces. The validation agent provides recommendations for addressing detected issues, but it does not modify the rule automatically. You must make the required changes and run validation again.

If validation reports a block

A block indicates an issue that must be resolved before you can continue with testing or activation. Tier 1 blocks disable **Test Rule** and **Activate**. Review the block details and follow the recommendation to correct the rule configuration or AQL query.

For example, a block can occur when the query does not return a recognized entity field. Entity context is required for downstream functions such as alert rule binding, suppression, UEBA risk accumulation, and investigation of the Incident and Investigation Agent. Another entity-related block can occur when an aliased output field cannot be traced back to a recognized entity source field.

After you correct the rule, Tier 1 validation runs automatically again. You can proceed to **Test Rule** when no Tier 1 blocks remain.

If validation reports a warning

Warnings identify issues that may affect rule quality but do not prevent testing. When Tier 1 has no blocks, **Test Rule** remains available even if warnings are present.

Review each warning and determine whether you should correct the issue or acknowledge the warning. For example, a warning can indicate that the look-back window is long enough that Tier 2 results may be partial. Address warnings where possible to improve the rule readiness score and detection quality.

Warnings can contribute to the rule readiness score. If you acknowledge a warning rather than correcting it, the acknowledgement is recorded.

If the rule test is unsuccessful

Test Rule runs Tier 2 validation against recent data from your environment. Tier 2 checks runtime behavior such as result volume, entity resolution, duplication, log source availability, and threshold calibration.

If Tier 2 reports a block, review the result details and make the recommended changes to the rule. For example, an excessive result volume can indicate that the query scope is too broad. A duplication result can indicate that the rule is producing overlapping detections across its simulated runs.

Tier 2 uses two offset simulation windows to identify duplicate detections. An overlap of 50% or more between the runs, based on entity and event timestamp, is identified as a duplication issue. If excessive overlap is reported, review the query logic, look-back window, and run schedule to determine whether the rule is evaluating overlapping data unnecessarily.

After changing the rule, run **Test Rule** again to rerun Tier 2 validation.

If the test returns no results

A test that returns zero results does not necessarily mean that the query is invalid. The relevant OCSF class may simply have no data available for your tenant.

For example, the `ZERO_RESULTS_MISSING_SOURCE` check is triggered when the test returns zero results and the OCSF class has no data for the tenant in the last seven days. The validation engine cross-references the OCSF parser catalog and surfaces the active parsers for the class and tenant.

In this situation, activation can remain enabled. Review the available data sources and parsers before changing a query that may otherwise be valid.

Managing Detection Rules

You can take several actions on detection rules to which you have access. You can edit the configuration of a rule, view its detection history to see firing trends and outcomes over time, or duplicate a rule to create an independent, editable copy. This is especially useful if you want to build a variant of an Anomali authored rule, since those cannot be edited directly. You can also test a rule against recent data to confirm its logic works as expected, without triggering real alerts or creating detection records. Additionally, you can manage access to your rules, disable them temporarily, and enable them again when you are ready to resume normal operation, either one at a time or in bulk. Finally, you can delete rules you no longer need.

Editing Detection Rules

Detection rules can be edited on the Detection Rules page or directly from a detection rule match on the Detections page.



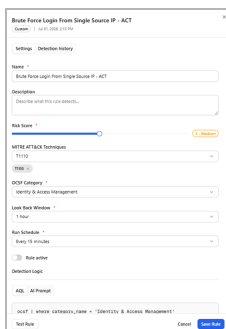
Notes:

- Only Organization Administrators, and users who have both the Manage Detection Rules permission and write ACL on the specific rule, can edit it. Rule owners inherently have owner-level access, so as long as they also hold the Manage Detection Rules permission, they can edit rules they own. See ["Detection Rule Actions and Their Required Permissions "](#) on [page 41](#) for details.
- Anomali authored detection rules cannot be edited.

Editing Detection Rules from the Detections Rules Page

To edit a detection rule:

1. Navigate to **ThreatStream Next Gen > Security Operations > Detection Rules**.
2. On the Detection Rules page, click the rule of your interest. Alternatively, open the more options menu (...) for the detection rule and then click **Edit**. The rule opens in the edit mode.
3. On the Settings tab, configure the fields you need.

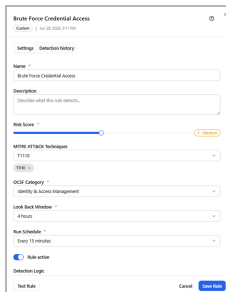


4. Click **Test Rule** to confirm that your changes are valid.
5. Click **Save Rule**.

Editing Detection Rules from Detection Rule Matches

To edit a detection rule from a detection rule match:

1. Navigate to **ThreatStream Next Gen > Security Operations > Detections**.
2. On the Detections page, locate a detection rule match whose rule you want to update and click the corresponding more options menu (...).
3. Click **Edit Rule**.
4. On the Settings tab, configure the fields you need.



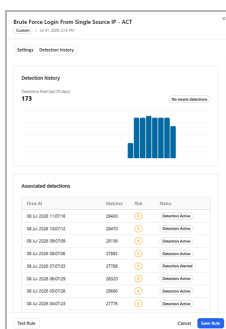
5. Click **Test Rule** to confirm that your changes are valid.
6. Click **Save Rule**.

Viewing Detection History

Detection History is the activity log of a detection rule, showing both the trend (how often it has been firing over the last month) and the detail (each individual firing event and what happened to the detections it produced).

To view detection history of a rule:

1. Navigate to **ThreatStream Next Gen > Security Operations > Detection Rules**.
2. On the Detection Rules page, click the rule whose detection history you want to view. Alternatively, open the more options menu (...) for the detection rule and then click **Edit**.
3. Click **Detection History**.



The Detection history chart displays a day-by-day chart of firing volume alongside a status indicator.

The Associated detections table shows a row for every time the rule has fired, listing the timestamp of when it was fired, the number of records matched in that run, the risk score assigned to that firing, and the resulting outcome, shown as either Detection Active or Detection Alerted.

4. Click **Save Rule** or **Cancel** when done.

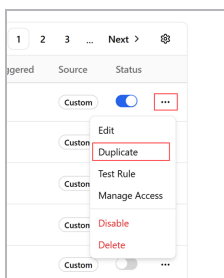
Duplicating Detection Rules

Duplicating a detection rule gives you an independent, editable copy of the full configuration for an existing rule, so you can build on logic that already works instead of starting from scratch. You will find this especially useful when working with Anomali Authored rules, since you cannot edit those directly. See [Detection Packs](#) for details.

Duplicate an Anomali Authored rule, and you will get a custom variant you are free to tune however you like, while the original rule stays untouched. You might also reach for duplication when you want to create a variant of a rule with a different threshold or Look Back Window, test a change to the detection logic without risking the version already running in production, adapt the same logic to a different OCSF category or MITRE technique, or quickly build out a set of related rules that share most of the setup but differ in just one or two conditions.

To duplicate a detection rule:

1. Navigate to **ThreatStream Next Gen > Security Operations > Detection Rules**.
2. On the Detection Rules page, locate the detection rule of your interest.
3. Open the corresponding more options menu (...) and click **Duplicate**.



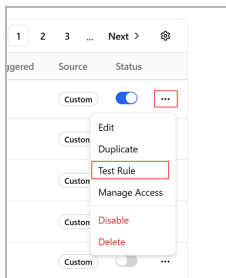
The rule duplicate is added to the list of detection rules with the word (Copy) appended to its original name.

Testing Detection Rules

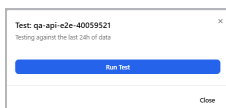
Testing an already-created detection rule lets you confirm its logic still behaves as expected before making it active or after adjusting it, using real historical data with no risk of side effects. Since a test run does not create detection records or trigger any alerts, you can run it as many times as needed to check whether the rule finds what you intend.

To test a detection rule:

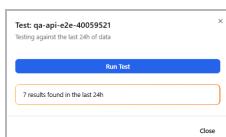
1. Navigate to **ThreatStream Next Gen > Security Operations > Detection Rules**.
2. On the Detection Rules page, locate the detection rule you want to test.
3. Open the corresponding more options menu (...) and click **Test Rule**.



4. In the pop-up message that appears, click **Run Test**. The test is performed against the last 24 hours of data.



5. View test results.



Managing Access to Detection Rules

For details on managing access to detection rules, see ["Managing Access to Detection Rules" on page 40](#).

Disabling Detection Rules

You can disable a Detection Rule to temporarily stop it from running without deleting it. Common reasons include tuning a rule that's generating too many false positives, working through a maintenance window where expected activity would otherwise trigger it, or keeping a superseded rule as a backup after replacing it with a newer one.

You can disable an individual detection rule or in bulk.

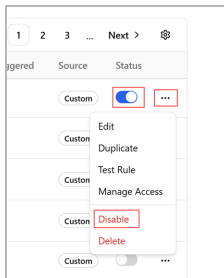


Note: Only Organization Administrators, rule owners, or users who have both the Manage Detection Rules permission and Write ACL on the specific rule can disable it. See ["Detection Rule Actions and Their Required Permissions "](#) on page 41 for details.

To disable a detection rule:

1. Navigate to **ThreatStream Next Gen > Security Operations > Detection Rules**.
2. On the Detection Rules page, locate the detection rule you want to disable.
3. Click the corresponding toggle in the Status column.

Alternatively, open the corresponding more options menu (...) and click **Disable**.



4. In the pop-up message that appears, click **Disable**.

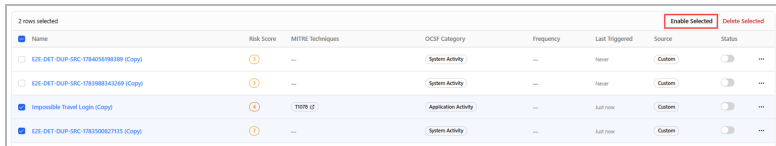


The detection rule is disabled.

To disable detection rules in bulk:

To enable detection rules in bulk:

1. Navigate to **ThreatStream Next Gen > Security Operations > Detection Rules**.
2. On the Detection Rules page, select the detection rules you want to enable and click **Enable Selected**.



Name	Risk Score	MITRE Techniques	OCSF Category	Frequency	Last Triggered	Source	Status
IDS DET-DUP-SEC-17840598189 (Copy)	0	---	System Activity	---	Never	Custom	Off
IDS DET-DUP-SEC-1783088143269 (Copy)	0	---	System Activity	---	Never	Custom	Off
Impossible Travel Login (Copy)	0	T109.02	Application Activity	---	Last now	Custom	Off
IDS DET-DUP-SEC-178350827118 (Copy)	0	---	System Activity	---	Last now	Custom	Off

The selected detection rules are enabled.

Deleting Detection Rules

You can delete a detection rule when it's no longer needed. For example, if it has been permanently replaced by another rule or the detection logic is no longer relevant to your environment. Deleting a rule is permanent and cannot be undone, so consider disabling it first if you may want to reuse it later.

You can delete an individual detection rule or in bulk.

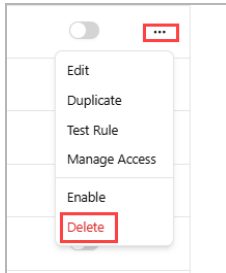


Notes:

- Only Organization Administrators and the current detection rule owner can delete detection rules.
- Anomali authored detection rules cannot be deleted.

To delete a detection rule:

1. Navigate to **ThreatStream Next Gen > Security Operations > Detection Rules**.
2. On the Detection Rules page, locate the detection rule you want to delete.
3. Open the corresponding more options menu (...) and click **Delete**.



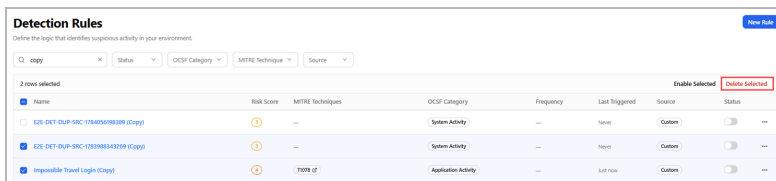
4. In the pop-up message, confirm the deletion by clicking **Delete**.



The detection rule is deleted.

To delete detection rules in bulk:

1. Navigate to **ThreatStream Next Gen > Security Operations > Detection Rules**.
2. On the Detection Rules page, select the detection rules you want to delete and click **Delete Selected**.



3. In the pop-up message, confirm the rule deletion by clicking **Delete**.



The selected detection rules are deleted.

Managing Access to Detection Rules

Detection rule access is governed by two independent permission layers that both must pass:

- **Permissions** determine what actions a user can perform on detection rules as a class. For example, viewing rules or managing (creating, editing, deleting, enabling/disabling) them.
- **Per-object access control (ACL)** determines which users can access a specific detection rule, and at what level.

Detection Rule Actions and Their Required Permissions

The following table lists the available detection rule actions and the required combination of permissions and ACL access levels for each action. Both requirements must be met. If either check fails, the action is denied. Users who do not have an ACL access level assigned to them cannot view detection rules.



Notes:

- Organization Administrators can view, edit, enable, disable, and delete any detection rule regardless of their ACL.
- The creator is the owner of the detection rule by default. The owner can restrict a rule to Private or share it to specific roles.
- New detection rules default to Read ACL. All users with the View Detection Rules permission can see them.

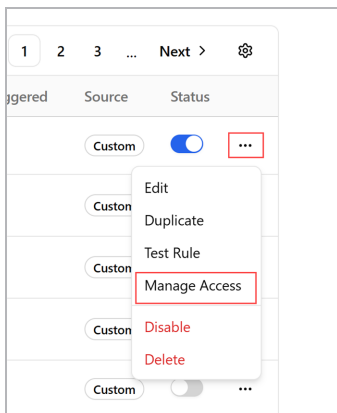
Action	Permission Required	Access Level Required
View a detection rule	View Detection Rules	Read or higher
Create a detection rule	Manage Detection Rules	n/a
Edit a detection rule	Manage Detection Rules	Write or Owner
Delete a detection rule	Manage Detection Rules	Owner
Enable or disable a detection rule	Manage Detection Rules	Write or Owner
Transfer ownership	n/a	Owner

Action	Permission Required	Access Level Required
Configure sharing	n/a	Owner

Managing Access to an Individual Detection Rule

To manage access to a detection rule:

1. Navigate to **ThreatStream Next Gen > Security Operations > Detection Rules**.
2. Click the more options menu and select **Manage Access**.



3. If necessary, change the owner.
4. Select roles to which you want grant Write ACL.
5. Click **Save Changes**.

Access permissions to the rule have been updated.

Alert Rules

The **Alert Rules** page is where you view, create, enable, disable, suppress, and manage all alert to which you have access.

An alert rule defines how one or more detections are grouped and escalated into an alert. An alert rule is a distinct, configurable record, separate from the alerts it produces. Whereas detection rule evaluates raw log data, an alert rule evaluates

already-produced detection records, watching for a pattern such as a single high-severity detection, a repeated detection, a multi-stage sequence, or a correlated pair of detections that together represent a meaningful security event.

To access your alert rules, navigate to **ThreatStream Next Gen > Security Operations > Alert Rules**.

Alert Rules
Define how detections are grouped and escalated into alerts.

Search alert rules... Type Severity Status

Items per page: 10 11-20 of 22 Results < Previous 1 2 3 Next >

Name	Type	Severity	Alerts (7d)	Last Fired	Suppression	Actions	Auto Triage	Status
☐ Authentication Brute Force Attack Followed By Succ...	Correlation	Critical	168	33d ago	—	—	On	On
☐ Vulnerability Burst By Asset - ACT	Threshold	High	0	Never	—	—	On	On
☐ High Volume AD Object Attribute Replication - ACT	Threshold	High	165	33d ago	—	—	On	On
☐ Mass File Deletion By Single User - ACT	Threshold	High	149	43m ago	—	—	On	On
☐ DNS Exfiltration Via High Unique Subdomain Count...	Threshold	Critical	149	43m ago	—	—	On	On
☐ Brute Force Login From Single Source IP - ACT	Threshold	High	158	33d ago	—	—	On	On
☐ WDigest Credential Caching Registry Modification ...	Simple	High	671	Just now	—	—	On	On
☐ Outbound Connection To Tor Exit Node - ACT	Simple	Critical	168	Just now	—	—	On	On
☐ DCSync Attack Via Directory Replication - ACT	Simple	Critical	80	33d ago	—	—	On	On
☐ Security Event Log Cleared - ACT	Simple	Critical	671	Just now	—	—	On	On

Items per page: 10 + Ask anything, perform tasks and get your job done < Previous 1 2 3 Next >

1 Search: Search alert rules by their names. The search is case insensitive and updates incrementally.

2 Type: Filter alert rules by their type:

- **Simple**—triggers an alert when a single detection meets the configured risk threshold.
- **Threshold**—triggers an alert when the same detection recurs for the same entity and observable values within a defined time window.
- **Compound**—triggers an alert when an ordered sequence of stages is satisfied and all stages share the same Group By value.
- **Correlation**—triggers an alert when an ordered sequence of detection conditions is satisfied, including conditions based on the presence or absence of an expected detection.

3 Severity: Filter alert rules by the severity assigned to the alerts they produce—Critical, High, Medium, or Low.

- 4 Status:** Filter alert rules by their status—Active, Inactive, or Suppressed.
- 5 Name:** Name of the rule, shown as a clickable link that opens the rule for editing. If the rule has a description, it appears as a subtitle beneath the name.
- 6 Type:** A badge showing the rule type: Simple, Threshold, Compound, or Correlation.
- 7 Severity:** A color-coded severity badge: Critical (red), High (orange), Medium (yellow), Low (green).
- 8 Alerts (7d):** The count of alerts the rule has produced in the past seven days.
- 9 Last Fired:** A relative timestamp showing when the rule most recently produced an alert; blank if the rule has never fired.
- 10 Suppression:** Displays a dash if the rule is not suppressed, or "Suppressed until [date]" with a clock icon if a suppression is active. Click to open the suppression management dialog.
- 11 Actions:** Icons for any notification channels configured on the rule. For example, webhook (🔗) or email (✉️). If no channels are configured, a dash (-) is displayed.
- 12 Auto Triage:** Displays whether Auto Triage with Aura is enabled for the rule.
- 13 Status:** An enable and disable toggle for the rule; changing it prompts for confirmation.
- 14 More options menu:**
 - **Edit:** Edit the alert rule. See ["Editing Alert Rules" on page 60](#) for details.
 - **Duplicate:** Create a copy of the rule that can be customized independently. See ["Duplicating Alert Rules" on page 61](#) for details.
 - **Add Suppression:** Temporarily suppress the rule from producing new alerts. See ["Adding Suppression to Alert Rules" on page 62](#) for details.
 - **Test Rule:** Test the alert rule. See ["Testing Alert Rules" on page 63](#) for details.
 - **Manage Access:** Define who can access the alert rule. See ["Managing Access to Alert Rules" on page 63](#) for details.
 - **Disable/Enable:** Turn the alert rule off/on. See ["Disabling Alert Rules" on page 64](#) and ["Enabling Alert Rules" on page 65](#) for details.
 - **Delete:** Delete the alert rule. See ["Deleting Alert Rules" on page 66](#) for details.

15 View Settings: Select the columns and table density (default or compact) to be displayed. By clicking the drag handle icon (⋮), drag and drop columns to change their position in the table. To return the view back to its default settings, click **Reset View**.

16 New Alert Rule: Create a new alert rule. For details, see ["Creating Alert Rules" below](#).

Creating Alert Rules



Note: To create alert rules, you must have the required permissions. For details, see ["Alert Rule Actions and Their Required Permissions" on page 68](#).

To create a new alert rule:

1. Navigate to **ThreatStream Next Gen > Security Operations > Alert Rules**.
2. Click **New Alert Rule**.
3. Configure the following universal fields, which apply to every rule regardless of type:

Field	Description
Name	Enter a unique, descriptive name for the rule.
Description	(Optional) Provide a note describing what the rule detects and why it matters.

Field	Description
Type	Select the type of the alert rule. The selected option displays the corresponding fields in the Rule Configuration section. Possible values: ▪ Simple ▪ Threshold ▪ Compound ▪ Correlation See "Configuring the Alert Rule Type" on page 49 for more information on the fields specific to each type.
Severity	Select the severity assigned to alerts this rule produces: Critical, High, Medium, or Low.
Detection Rule	Select one or more detection rules for this rule to watch. Applies to Simple, Threshold, and Compound rule types; see "Configuring the Alert Rule Type" on page 49 for each type's specific behavior. Not applicable to Correlation rules, which select a detection rule per step instead.
Minimum Risk Score	Select the minimum detection risk score, Low to Critical, required to count toward this rule. Applies to Simple and Threshold rule types only; see "Configuring the Alert Rule Type" on page 49 for details.
Rule Active	(Optional) Toggle to determine whether the rule begins evaluating immediately on save. Enabled by default.

Field	Description
Auto Triage with AURA	(Optional) When enabled, alerts generated by this rule are automatically picked up and evaluated by the Alert Triage Agent. The Agent analyzes and annotates each alert and routes it (for example, promote, investigate, monitor, or close as false positive) without requiring manual assignment. All alerts evaluated by the Alert Triage Agent can then be reviewed on the Approval Queue page. See Approval Queue. When disabled, alerts from this rule are created without an Agent verdict and left unassigned. They are not included in automatic threshold checks or scheduled bulk reviews. They wait in the queue until an analyst reviews them. The setting is enabled by default.
Actions	(Optional) Configure one or more notification actions (coming soon). See "Configuring Alert Rule Actions" on page 58.

New Alert Rule

?

×

Name *

e.g. Brute Force + Credential Dump

Description

Describe what this alert rule does...

Type *

Simple

Triggers when a single detection rule fires.

Threshold

Triggers when a detection fires N times within a time window.

Compound

Triggers when multiple detections fire together within a time window.

Correlation

Triggers when detections fire in a specific sequence.

Severity *

Select severity...

Rule Configuration

Detection Rule *

Select detection rule...

Minimum Risk Score *

4 — High

Rule active

Auto Triage with AURA

Actions

Configure what happens when this rule fires.

No actions configured. Alerts will appear in the alerts list only.

+ Add Action

Cancel

Save Rule

Anomali ThreatStream Next Gen

Page 48 of 297

4. Click **Save Rule**.

The alert rule is added to the list of rules on the Alert Rules page.

Configuring the Alert Rule Type

Simple Rule

A Simple rule watches for a specific detection and produces one alert per matching detection. Use Simple rules for detections significant enough on their own to always warrant analyst attention.

Type *

Simple
Triggers when a single detection rule fires.

Threshold
Triggers when a detection fires N times within a time window.

Compound
Triggers when multiple detections fire together within a time window.

Correlation
Triggers when detections fire in a specific sequence.

Severity *

Medium

Rule Configuration

Detection Rule *

E2E-DET-SEARCH-ALPHA-1782152946819

Minimum Risk Score *

4 — High

☒ Rule active

☒ Auto Triage with AURA

Actions

Configure what happens when this rule fires.

Email to soc-team@anomali.com

Edit

☒

×

+ Add Action

Test Rule

Cancel

Save Rule

- **Detection Rule** — required; a searchable multi-select for one or more detection rules to watch. Selected rules appear as removable chips.
- **Minimum Risk Score** — required; a slider from one to five (Low to Critical). Detections below this score are observed but do not trigger the alert.

Threshold Rule

A Threshold rule watches for the same detection occurring repeatedly within a time window, and fires once the count reaches the configured minimum.

Type *

Simple

Triggers when a single detection rule fires.

Threshold

Triggers when a detection fires N times within a time window.

Compound

Triggers when multiple detections fire together within a time window.

Correlation

Triggers when detections fire in a specific sequence.

Severity *

Medium

Rule Configuration

Detection Rule *

E2E-DET-SEARCH-ALPHA-1782152946819

Minimum Risk Score *

4 — High

Count Threshold *

Alert when this rule fires at least 5 times

Time Window *

Within 15 min

☒ Detections must all involve the same entity

☒ Rule active

☒  Auto Triage with AURA

Actions

Configure what happens when this rule fires.

Email to soc-team@anomali.com

Edit

☒

×

+ Add Action

Test Rule

Cancel

Save Rule

- **Detection Rule** — required; a searchable multi-select for one or more detection rules to watch.
- **Minimum Risk Score** — required; same one-to-five slider as the Simple type.
- **Count Threshold** — required; the minimum number of matching detections needed to fire the alert.
- **Time Window** — required; the window within which the count must be reached, for example within 15 min or within 1 hour.
- **Detections must all involve the same entity** — a toggle restricting matches to detections sharing the same entity.

Compound Rule

A Compound rule detects multi-stage activity by evaluating an ordered set of stages, where each stage is its own configurable condition.

Type *

Simple

Triggers when a single detection rule fires.

Threshold

Triggers when a detection fires N times within a time window.

Compound

Triggers when multiple detections fire together within a time window.

Correlation

Triggers when detections fire in a specific sequence.

Severity *

Medium

Rule Configuration

Detection Rules *

E2E-DET-SEARCH-ALPHA-1782152946819

E2E-DET-SEARCH-ALPHA-1782152... x

Stages

Detection Rule

E2E-DET-SEARCH-ALPHA-1782152946819

Sub-type

SINGLE

Invert

Time Window *

Within 1 hour

☒ All detections must involve the same entity

☒ Rule active

☒ Auto Triage with AURA

Actions

Configure what happens when this rule fires.

Email to soc-team@anomali.com

Edit

x

+ Add Action

Cancel

Save Rule

- **Detection Rules** — required; a multi-select pool of detection rules available to reference across the stages of the rule. Selected rules appear as removable chips.

Under **Stages**, each stage references one of the selected detection rules and a sub-type that determines its condition:

- **SINGLE** — the stage is satisfied when the selected detection rule fires at least once. No additional fields are shown.
- **THRESHOLD** — the stage is satisfied when the selected detection rule fires at least **Count** times within the stage's **Time Window**.
- **UNIQUE_VALUES** — the stage is satisfied when at least **Count** distinct values of the specified **Field**, for example `destination_ip`, are observed within the stage's **Time Window**.

Additionally, each stage also has an **Invert** toggle. Turning it on requires that the stage's condition does **not** occur, rather than requiring that it does.

- **Time Window** — required; the overall window governing the timing between stages.
- **All detections must involve the same entity** — a toggle requiring every stage to resolve against the same entity.

Correlation Rule

A Correlation rule detects an ordered sequence of detections, including cases where an expected detection is absent.

Type *

Simple
Triggers when a single detection rule fires.

Threshold
Triggers when a detection fires N times within a time window.

Compound
Triggers when multiple detections fire together within a time window.

Correlation
Triggers when detections fire in a specific sequence.

Severity *

Medium

Rule Configuration

Step 1

E2E-DET-SEARCH-ALPHA-1782152946819

Followed by

↑

↓

Step 2

E2E-RANGE-005-1783551673498

Followed by

↑

↓

+ Add Step

Time Window *

Within 1 hour

☒ Rule active

☒ Auto Triage with AURA

Actions

Configure what happens when this rule fires.

Email to soc-team@anomali.com

Edit

☒

×

+ Add Action

Cancel

Save Rule

Each step in the sequence has a **Select rule** search field for choosing the detection rule that step watches and a condition drop-down setting the relationship to the previous step:

Rule Configuration

Step 1

E2E-DET-SEARCH-ALPHA-1782152946819

Followed by

↑

↓

×

Step 2

E2E-DET-EDIT-BEFORE-1782155749644

Not followed by

↑

↓

×

Step 3

E2E-RANGE-005-1783551673498

Followed by

↑

↓

×

+ Add Step

Time Window *

Within 1 hour

☒ Rule active

☒ Auto Triage with AURA

Actions

Configure what happens when this rule fires.

Email to soc-team@anomali.com

Edit

☒

×

+ Add Action

Cancel

Save Rule

- **Followed by** — the step's detection must occur after the previous step, within the time window.
- **Not followed by** — the step's detection must not occur after the previous step, within the time window. The absence itself is the signal.

Use the up and down arrows next to each step to reorder the sequence, and **+ Add Step** to extend it. A single **Time Window** field below the steps sets the window for the sequence. Available Time Window options across rule types include **within 5 min**, **within 15 min**, **within 1 hour**, **within 6 hours**, and **within 24 hours**.

Configuring Alert Rule Actions

By default, a new rule has no actions configured, and its alerts appear in the alerts list only.

To configure a new action:

Click **+ Add Action** to open the action picker, which lists two categories:

- **Email (SMTP)** — Sends an email through a configured SMTP integration each time the rule fires.
- **Webhook** — Sends the alert payload as a POST request to a configured webhook endpoint, for example a SIEM or ticketing system.

Each action you add appears as a row in the Actions section with an icon, display name, an **Edit** button, an enabled and disabled toggle, and a remove control. Toggling an action off pauses it without removing it from the rule.

Selecting **Email (SMTP)** opens the **Configure Email Notification** dialog, where you set **To**, **CC**, and **BCC** recipients (suggested addresses appear below each field), a **Subject Template**, and a **Message Body**. Both the subject and body accept variable placeholders, for example `{alert_number}`, `{rule_name}`, `{severity}`, and `{alert_link}`, which are filled in automatically when the notification is sent.

Configure Email Notification ✕

To *

john.doe@acme.corp ✕

Type email and press Enter...

scott@anomali.com soc-team@anomali.com ir-leads@anomali.com

CC

Type email and press Enter...

scott@anomali.com soc-team@anomali.com ir-leads@anomali.com

BCC

Type email and press Enter...

scott@anomali.com soc-team@anomali.com ir-leads@anomali.com

Subject Template *

Alert {alert_number}: {rule_name}

Available variables: {alert_number}, {rule_name}

Message Body

An alert has been triggered.

Alert: {alert_name}
Severity: {severity}
Entities: {entity_names}
Detection Count: {detection_count}

View alert: {alert_link}

Available variables: {alert_name}, {severity}, {entity_names}, {detection_count}, {alert_link}

Cancel Save Action

Click **Save Rule** to save the rule, or **Cancel** to discard changes.

Managing Alert Rules

You can take several actions on alert rules to which you have access. You can edit a rule configuration, duplicate it to create an independent variant, or add a temporary suppression window to pause the alerts it produces. You can also test the logic of a rule against existing data without creating an alert record, manage who besides the rule owner can access it, disable it temporarily, enable it again when you are ready to resume normal operation, and delete it when you no longer need it, either one at a time or in bulk.

Editing Alert Rules



Note: To edit alert rules, you must have the required permissions. For details, see ["Alert Rule Actions and Their Required Permissions"](#) on page 68.

To edit an alert rule:

1. Navigate to **ThreatStream Next Gen > Security Operations > Alert Rules**.
2. Click the rule name, or open the more options menu (...) for the rule and click **Edit**.

The screenshot shows the 'Alert Rules' management interface. At the top, there's a header 'Alert Rules' with a subtitle 'Define how detections are grouped and escalated into alerts.' and a 'New Alert Rule' button. Below the header is a search bar and filters for 'Type', 'Severity', and 'Status'. A table lists several alert rules with columns: Name, Type, Severity, Alerts (7d), Last Fired, Suppression, Actions, Auto Triage, and Status. The 'Actions' column for the second rule, 'E2E-THRESHOLD-178288656872', is expanded, showing options: Edit, Duplicate, Add Suppression, Test Rule, Manage Access, Disable, and Delete. The 'Edit' option is highlighted with a red box.

Name	Type	Severity	Alerts (7d)	Last Fired	Suppression	Actions	Auto Triage	Status
E2E-THRESHOLD-5E-1783014493387	Threshold	Medium	0	Never	—	—	On	On
E2E-THRESHOLD-178288656872	Threshold	High	0	Never	—	⊕	On	On
qa_device_host_findings	Simple	High	186	14d ago	—	—	On	On
i3-both-fields-alert	Simple	Medium	7	11d ago	—	⊕	On	On
i2-tactic-only-alert	Simple	Medium	7	11d ago	—	—	On	On

The rule opens in the same dialog that was used to create it, with all fields pre-populated, as shown below:

Edit: qa-wf01-alert-bc26c402

Name: qa-wf01-alert-bc26c402

Description: Describe what this alert rule does...

Type: Simple (selected), Threshold, Compound, Correlation

Severity: High

Rule Configuration: Detection Rule: qa-wf01-det-64e88437

Buttons: Cancel, Save Changes

3. Configure the fields you need. See ["Creating Alert Rules" on page 45](#) for field descriptions.
4. Click **Save Rule**.

Duplicating Alert Rules

Duplicating a rule gives you an independent, editable copy of its full configuration, so you can build a variant without disturbing the original rule already running in production. This is especially useful when you want to test a different Minimum Risk Score, Count Threshold, or Time Window without risking the live rule, adapt an existing rule's detection rules and severity to a related scenario, or quickly build out a set of similar rules that share most of their configuration but differ in just one or two conditions.

To duplicate an alert rule:

1. Navigate to **ThreatStream Next Gen > Security Operations > Alert Rules**.
2. Locate the alert rule of your interest.
3. Open the corresponding more options menu (...) and click **Duplicate**.

Alert Rules

Define how detections are grouped and escalated into alerts.

Search alert rules... Type Severity Status

Items per page: 10 71-75 of 75 Results

Name	Type	Severity	Alerts (7d)	Last Fired	Suppression	Actions	Auto Triage	Status
E2E-THRESHOLD-5E-1783014493387	Threshold	Medium	0	Never	—	—	On	On
E2E-THRESHOLD-178286856872	Threshold	High	0	Never	—	—	On	On
qa_device_host_findings	Simple	High	186	14d ago	—	—	On	On
i3-both-fields-alert	Simple	Medium	7	11d ago	—	—	On	On
i2-tactic-only-alert	Simple	Medium	7	11d ago	—	—	On	On

Items per page: 10 71-75 of 75 Results

More options menu for E2E-THRESHOLD-178286856872: Edit, Duplicate, Add Suppression, Test Rule, Manage Access, Disable, Delete

The duplicate opens in the editing mode, pre-populated with the same configuration as the original. Rename it and adjust any fields you need, then click **Save Rule**.

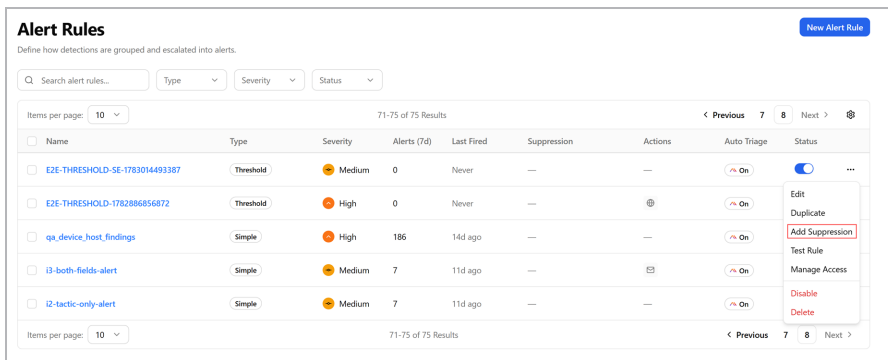
Adding Suppression to Alert Rules

While suppressed, the rule continues to evaluate detections but does not produce new alerts until the suppression expires.

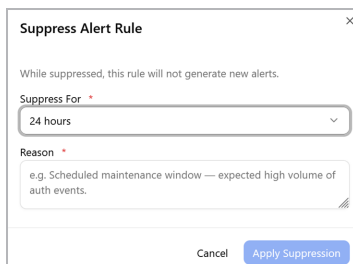
To add suppression to an alert rule, you must have the required permissions. For details, see ["Alert Rule Actions and Their Required Permissions" on page 68](#).

To suppress an alert rule:

1. Navigate to **ThreatStream Next Gen > Security Operations > Alert Rules**.
2. Locate the alert rule you want to suppress.
3. Open the corresponding more options menu (...) and click **Add Suppression**.



4. In the Suppress Alert Rule dialog box, select a duration from the **Suppress For** drop-down list.
5. Enter a mandatory reason in the **Reason** field.
6. Click **Apply Suppression**.



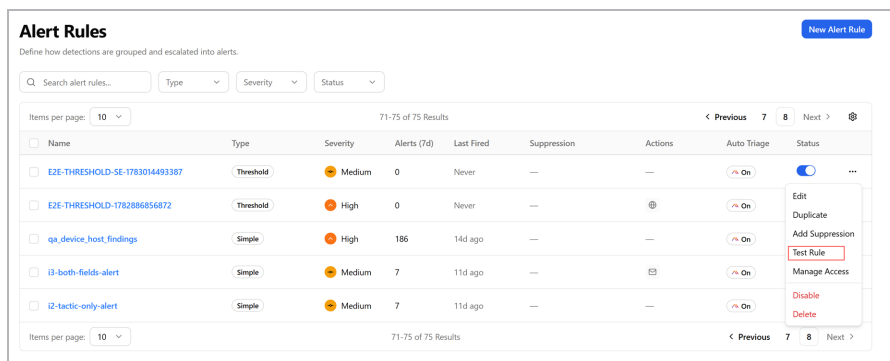
The suppression expires automatically at the selected date and time. No manual action is required to resume normal evaluation. A suppressed rule shows its expiry date in the Suppression column and remains distinct from a rule that is fully disabled.

Testing Alert Rules

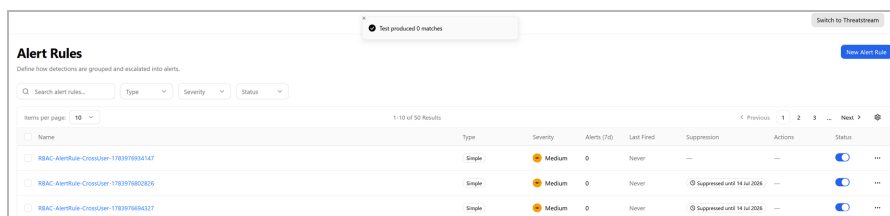
Testing an alert rule lets you confirm its logic behaves as expected before relying on it, using existing data with no risk of side effects. A test run does not create an alert record, so you can run it as many times as needed.

To test an alert rule:

1. Navigate to **ThreatStream Next Gen > Security Operations > Alert Rules**.
2. Locate the alert rule you want to test.
3. Open the corresponding more options menu (...) and click **Test Rule**.



4. View the match count returned in the confirmation message.



Managing Access to Alert Rules

See "[Managing Access to Alert Rules](#)" on page 67 for more details on managing access to alert rules.

Disabling Alert Rules

You can disable an alert rule to temporarily stop it from producing new alerts without deleting it. Common reasons include tuning a rule that is generating too many false positives, working through a maintenance window where expected activity would otherwise trigger it, or keeping a superseded rule as a backup after replacing it with a newer one.

You can disable an individual alert rule or in bulk.



Notes: To disable alert rules, you must have the required permissions. For details, see ["Alert Rule Actions and Their Required Permissions" on page 68](#).

To disable an alert rule:

1. Navigate to **ThreatStream Next Gen > Security Operations > Alert Rules**.
2. Locate the alert rule you want to disable.
3. Open the corresponding more options menu (...) and click **Disable**. Alternatively, you can also toggle the **Status** switch off in the rules list.

The screenshot shows the 'Alert Rules' management interface. At the top, there's a 'New Alert Rule' button and a description: 'Define how detections are grouped and escalated into alerts.' Below this are filters for 'Search alert rules...', 'Type', 'Severity', and 'Status'. A table lists several alert rules. The first two are 'E2E-THRESHOLD-SE-1783014493387' and 'E2E-THRESHOLD-178288656872', both of type 'Threshold'. The next two are 'qa_device_host_findings' and 'i3-both-fields-alert', both of type 'Simple'. The last one is 'i2-tactic-only-alert', also of type 'Simple'. Each rule row has columns for Name, Type, Severity, Alerts (7d), Last Fired, Suppression, Actions, Auto Triage, and Status. The 'Status' column shows a toggle switch. For the 'i2-tactic-only-alert' rule, the 'Actions' column has a menu icon (three dots) that is open, showing options: Edit, Duplicate, Add Suppression, Test Rule, Manage Access, **Disable** (highlighted in red), and Delete. The interface also includes pagination controls at the bottom, showing '71-75 of 75 Results'.

Name	Type	Severity	Alerts (7d)	Last Fired	Suppression	Actions	Auto Triage	Status
E2E-THRESHOLD-SE-1783014493387	Threshold	Medium	0	Never	—	—	On	On
E2E-THRESHOLD-178288656872	Threshold	High	0	Never	—	—	On	On
qa_device_host_findings	Simple	High	186	14d ago	—	—	On	On
i3-both-fields-alert	Simple	Medium	7	11d ago	—	—	On	On
i2-tactic-only-alert	Simple	Medium	7	11d ago	—	—	On	On

4. Confirm the action when prompted.

The alert rule is disabled.

To disable alert rules in bulk:

1. Navigate to **ThreatStream Next Gen > Security Operations > Alert Rules**.
2. Select two or more rules and click **Disable Selected**.

Alert Rules

Define how detections are grouped and escalated into alerts.

Search alert rules...

Type

Severity

Status

2 rows selected

Disable Selected

Delete Selected

☒	Name	Type	Severity	Alerts (7d)	Last Fired	Suppression	Actions	Auto Triage	Status
☐	slam_t_c	Simple	Critical	8	Just now	—	—	—	☒
☐	qa-test-severity-criticala (maj)	Simple	Critical	213	Just now	—	—	On	☐
☒	decision-required-alert	Simple	Critical	59	10h ago	—	—	On	☒
☒	qa-promote-group-single-alert-copy	Simple	High	322	Just now	—	—	On	☒

3. Confirm the action when prompted.

The selected alert rules are disabled.

Enabling Alert Rules

You can enable an individual alert rule or in bulk to resume evaluation after it has been disabled.



Note: To enable alert rules, you must have the required permissions. For details, see ["Alert Rule Actions and Their Required Permissions" on page 68.](#)

To enable a disabled alert rule:

- 1. Navigate to **ThreatStream Next Gen > Security Operations > Alert Rules**.
- 2. Locate the alert rule you want to enable.
- 3. Open the corresponding more options menu (...) and click **Enable**, or toggle the **Status** switch in the list on.

2 rows selected

Enable Selected

Delete Selected

☒	Name	Type	Severity	Alerts (7d)	Last Fired	Suppression	Actions	Auto Triage	Status
☐	slam_t_c	Simple	Critical	8	Just now	—	—	—	☒
☒	qa-test-severity-criticala (maj)	Simple	Critical	213	Just now	—	—	On	☐
☒	decision-required-alert	Simple	Critical	59	10h ago	—	—	On	☒
☐	qa-promote-group-single-alert-copy	Simple	High	322	Just now	—	—	On	☒
☐	aura_disabled_oklahoma-promote-alert-copy	Simple	High	284	16h ago	—	—	—	☒
☐	aura_disable_dangerous_host_alert_copy	Simple	High	891	Just now	—	—	On	☒
☐	test verdict alert (maj)	Simple	Critical	1272	Just now	—	—	On	☒

Edit

Duplicate

Add Suppression

Test Rule

Manage Access

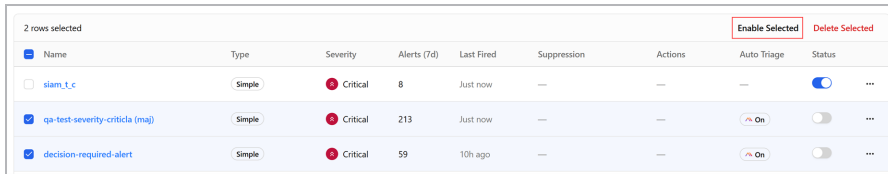
Enable

Delete

The rule is enabled.

To enable alert rules in bulk:

1. Navigate to **ThreatStream Next Gen > Security Operations > Alert Rules**.
2. Select two or more disabled rules and click **Enable Selected**.



2 rows selected								Enable Selected	Delete Selected
☐	Name	Type	Severity	Alerts (7d)	Last Fired	Suppression	Actions	Auto Triage	Status
☐	slam_t_c	Simple	Critical	8	Just now	---	---	---	On
☒	qa-test-severity-critical (maj)	Simple	Critical	213	Just now	---	---	On	On
☒	decision-required-alert	Simple	Critical	59	10h ago	---	---	On	On

3. Confirm the action when prompted.

The selected alert rules are enabled.

Deleting Alert Rules

You can delete an alert rule when it is no longer needed, for example if it has been permanently replaced by another rule. Deleting a rule is permanent and cannot be undone, so consider disabling it first if you may want to reuse it later.

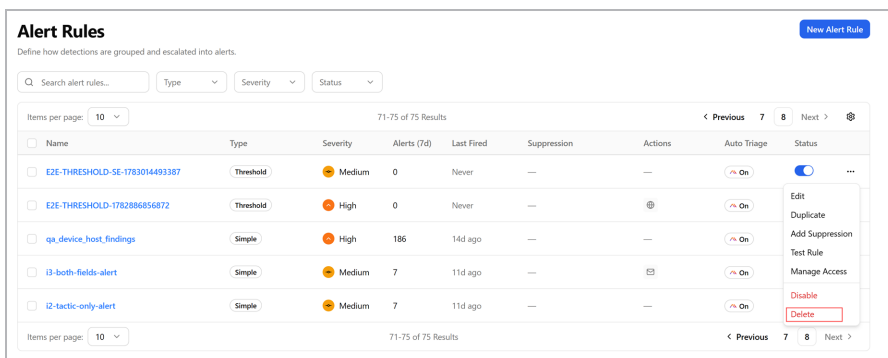
You can delete an individual alert rule or in bulk.



Note: To delete alert rules, you must have the required permissions. For details, see ["Alert Rule Actions and Their Required Permissions" on page 68](#).

To delete an alert rule:

1. Navigate to **ThreatStream Next Gen > Security Operations > Alert Rules**.
2. Locate the alert rule you want to delete.
3. Open the corresponding more options menu (...) and click **Delete**.



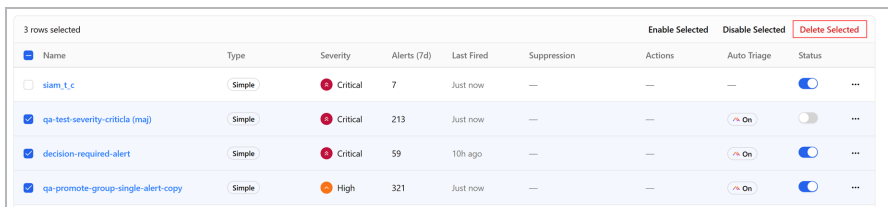
Alert Rules										New Alert Rule
Define how detections are grouped and escalated into alerts.										
Q Search alert rules... Type Severity Status										
Items per page: 10 71-75 of 75 Results < Previous 7 8 Next >										
☐	Name	Type	Severity	Alerts (7d)	Last Fired	Suppression	Actions	Auto Triage	Status	
☐	E2E-THRESHOLD-5E-1783014493387	Threshold	Medium	0	Never	---	---	On	On	...
☐	E2E-THRESHOLD-178286856872	Threshold	High	0	Never	---	---	On	On	...
☐	qa_device_host_findings	Simple	High	186	14d ago	---	---	On	On	...
☐	i3-both-fields-alert	Simple	Medium	7	11d ago	---	---	On	On	...
☐	I2-tactic-only-alert	Simple	Medium	7	11d ago	---	---	On	On	...
Items per page: 10 71-75 of 75 Results < Previous 7 8 Next >										

4. Confirm the deletion when prompted.

The alert rule is deleted.

To delete alert rules in bulk:

1. Navigate to **ThreatStream Next Gen > Security Operations > Alert Rules**.
2. Select two or more rules and click **Delete Selected**.



3 rows selected							Enable Selected	Disable Selected	Delete Selected
☐	Name	Type	Severity	Alerts (7d)	Last Fired	Suppression	Actions	Auto Triage	Status
☐	slam_1_c	Simple	Critical	7	Just now	—	—	—	On
☒	qs-test-severity-critical (maj)	Simple	Critical	213	Just now	—	—	On	On
☒	decision-required-alert	Simple	Critical	59	10h ago	—	—	On	On
☒	qs-promote-group-single-alert-copy	Simple	High	321	Just now	—	—	On	On

3. Confirm the deletion when prompted.

The selected alert rules are deleted.

Managing Access to Alert Rules

Alert rule access is governed by two independent permission layers that both must pass:

- **Permissions** determine what actions a user can perform on alert rules as a class. For example, viewing rules or managing (creating, editing, deleting, enabling/disabling, suppressing) them. See [Managing Roles](#) for details on permissions that can be assigned to roles.
- **Per-object access control (ACL)** determines which users can access a specific alert rule, and at what level.

Alert Rule Actions and Their Required Permissions

The following table lists the available alert rule actions and the required combination of permissions and ACL access levels for each action. Both requirements must be met. If either check fails, the action is denied. Users who do not have an ACL access level assigned to them cannot view alert rules.



Notes:

- Organization Administrators can view, edit, and delete any alert rule, regardless of their ACL.



- The creator is the owner of the alert rule by default. The owner can restrict a rule to Private or share it to specific roles.
- New alert rules default to Read. All users with the View Alert Rules permission can see them.
- Suppressing an alert rule requires the Suppress Alert Rules permission specifically. This permission does not by itself grant the ability to edit or delete the rule.

Action	Permission Required	Access Level Required
View an alert rule	View Alert Rules	Read or higher
Create an alert rule	Manage Alert Rules	n/a
Edit an alert rule	Manage Alert Rules	Write or Owner
Delete an alert rule	Manage Alert Rules	Owner
Enable or disable an alert rule	Manage Alert Rules	Write or Owner
Suppress an alert rule	Suppress Alert Rules	Write or Owner
Transfer ownership	n/a	Owner
Configure sharing	n/a	Owner

Managing Access to an Individual Alert Rule

The Sharing & Permissions dialog box controls who besides the rule owner and organizational administrators can access the rule. It shows the current Owner and a Write Access table listing roles, with the option to grant that role write access to the rule. Organization Administrators always have full access regardless of these settings.

To manage access to an alert rule:

1. Navigate to **ThreatStream Next Gen > Security Operations > Alert Rules**.
2. Open the more options menu (...) for the rule and click **Manage Access**.

Sharing & Permissions

Control who can access this alert rule

Owner

tech-mcp

Write Access

Role	Write
Everyone in My Organization	☐
it_users_azure	☐
SOC - Incident Responder	☐
AnomaliRole_SOC - Incident Delete	☐
dy_test_role	☐
rhac case mgmt manager	☐

Organizational Administrators always have full access regardless of these settings.

CancelSave Changes

3. If necessary, change the owner.
4. Select the **Write** permission to grant that role write access.
5. Click **Save Changes**.

Access permissions to the rule have been updated.

Detections

The **Detections** page displays the entire catalog of signals produced in your environment when the platform identifies a specific behavioral pattern, policy violation, or threat indicator within log data. These signals are organized by detection rules created on the platform and are grouped for quick review, enabling you to monitor detection volume across severity levels, investigate matched entities, and act on individual detection instances.

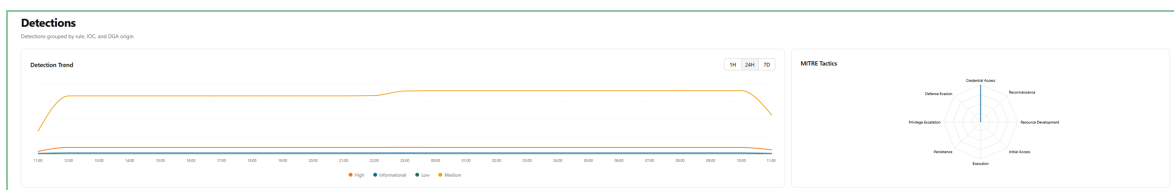


Note: Viewing detections and adding annotations require the View Detections permission. See [Managing Roles](#) for details.

Each detection is enriched automatically with entity context and MITRE ATT&CK technique mappings before it is surfaced to analysts.

To access detections, on the left navigation menu, click **Security Operations > Detections**.

Understanding Detections

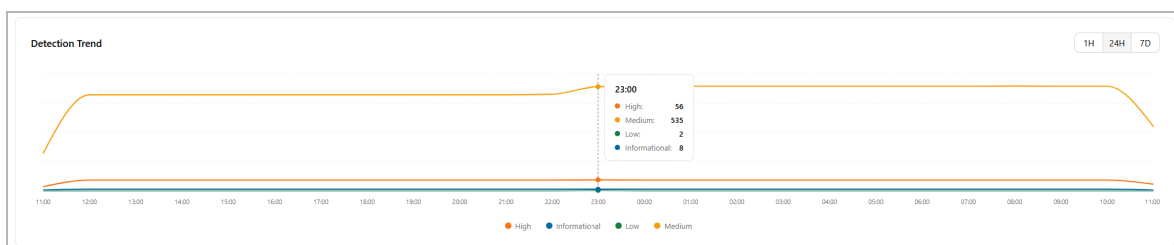


Detections provide two important visualizations:

Detection Trend Chart

The **Detection Trend** chart displays detection volume over the selected time range, with a separate line series per severity level: Critical (Red), High (orange), Medium (yellow), Low (green), and Informational (blue). Use the **1H**, **24H**, and **7D** radio buttons in the top-right corner of the chart to change the time range. This time range also applies to the ["Understanding Detection Rule Matches" on page 72](#).

Hover over any point on the chart to see a tooltip showing the per-severity counts at that timestamp.



MITRE Tactics Chart

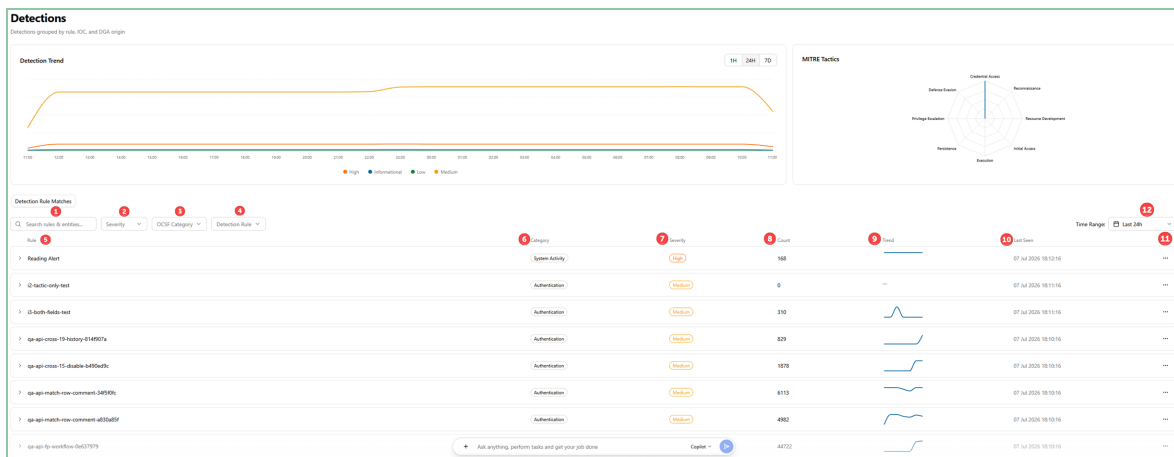
The **MITRE Tactics** chart uses a radar diagram to show the distribution of active detections across MITRE ATT&CK tactics. Each axis represents one tactic. The example image below represents detections in a polygon area displaying multiple MITRE tactics such as Credential Access, Initial Access, Reconnaissance,

Resource Development, and more. This area grows as more detections map to a particular tactic.

Hover over any tactic axis to see a tooltip showing the tactic name and the total detection count for that tactic.



Understanding Detection Rule Matches



Detection Rule Matches represent detections produced by AQL rules, grouped by rule name. Each group row represents one detection rule and the set of entities that triggered it within the active time range.

- 1 Search rule & entities:** free-text search across rule names and entity values
- 2 Severity:** multi-select filter by severity level
- 3 OCSF Category:** multi-select filter by OCSF category assigned to the rule

- 4 **Detection Rule:** search by rule name
- 5 **Rule:** Denotes the detection rule name and the matched entities.
- 6 **Category:** Signifies the OCSF category assigned to the rule, such as Authentication or Network Activity.
- 7 **Severity:** Captures the color-coded severity badge for the rule, containing levels such as Critical (Red), High (orange), Medium (yellow), Low (green), and Informational (blue).
- 8 **Count:** Counts the total number of detection instances in the active time range.
- 9 **Trend:** Shows detection frequency over the time range using a sparkline trend.
- 10 **Last Seen:** Denotes the timestamp of the most recent detection instance.
- 11 **More Options:** Click the ellipsis icon (...) on each row to select one of two options:
 - **Detail:** This option displays the configuration for the detection rule that produced this set of involved entities. The panel displays the rule name, severity, and OCSF category in the header, and a **Rule** tab with the following fields: Description, OCSF Category, Severity, Base Risk Score, Detection Count (30 days), Look-back Window, Run Schedule, MITRE ATT&CK, and the AQL Query used by the rule.

The screenshot shows a configuration panel for a detection rule. At the top, the rule name 'qa-api-fp-workflow-0a04321e' is displayed with a close button. Below it, a 'High' severity badge and 'Network Activity' category are shown. A 'Rule' tab is active, displaying the following details:

Rule	
Description	False positive workflow E2E test
OCSF Category	Network Activity
Severity	High
Base Risk Score	4
Detection Count (30d)	0
Look-back Window	24 hours
Run Schedule	Every 5 minutes
MITRE ATT&CK	None

Below the rule details, the 'AQL Query' section shows the query: `ocsf | where category_name = 'Network Activity'`.

- **Edit Rule:** This option opens the detection rule editor. See [Detection Rules](#) for more information.

12 Time Range: time range selector on the top-right that sets the active time window for both the charts and the detection list. Options include **Last 1h**, **Last 24h**, **Last 7d**, **Last 30d**, and **Custom**.

Viewing Per-Detection Details

Expanding each row reveals the individual entities matched by that rule within the active time range.

See "[Viewing Matched Detections](#) " below for more information.

Viewing Matched Detections

You can view details about all detections for an entity under a matched rule, along with related observables, audit history, and comments.



Note: Viewing detection details requires the View Detections permission. For details, see [Managing Roles](#).

Accessing Detection Rule Matches

Rule	Category	Severity	Count	Trend	Last Seen	
Field renaming	Network Activity	Medium	264		25 Aug 2026 10:57:24	...
Converge-QA-system-activity	Authentication	Info	221		25 Aug 2026 10:57:24	...

Entity	Count	First Seen	Last Seen	Alert
027970a11c4bc48805958869e69c	220	24 Aug 2026 11:12:25	25 Aug 2026 10:57:24	—
0376414128b4008260240d912ae55	220	24 Aug 2026 11:12:25	25 Aug 2026 10:57:24	—
04883803b43430c8ca63bdeed1daabf2	220	24 Aug 2026 11:12:25	25 Aug 2026 10:57:24	—
04cc25e402284296a4054ffbc29dd10	220	24 Aug 2026 11:12:25	25 Aug 2026 10:57:24	—
04db3aa5699848d3a4f34e549a55151	220	24 Aug 2026 11:12:25	25 Aug 2026 10:57:24	—
06ae7d416dc74005b77efea2a60cab2	220	24 Aug 2026 11:12:25	25 Aug 2026 10:57:24	—
07180d31e79e534bdfb0564d1cde0	220	24 Aug 2026 11:12:25	25 Aug 2026 10:57:24	—
077902b16642fabac1176b86fa34	220	24 Aug 2026 11:12:25	25 Aug 2026 10:57:24	—
07762b010804415930a5d39dc95d4ce	220	24 Aug 2026 11:12:25	25 Aug 2026 10:57:24	—
0008888a554642b42d161855c69986	220	24 Aug 2026 11:12:25	25 Aug 2026 10:57:24	—

Click an arrow next to a rule to view the list of entities impacted.

Each entity row includes the following:

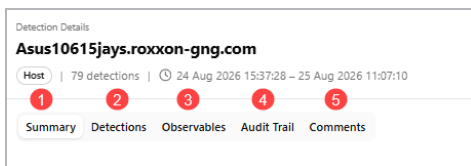
- 1 Entity:** Entity type icon and entity value, such as an IP address or hostname
- 2 Count:** Number of times this entity triggered the rule
- 3 First Seen:** Timestamp of the first detection for this entity under this rule
- 4 Last Seen:** Timestamp of the most recent detection for this entity
- 5 Alert:** Linked alert badge if this detection has been elevated to an alert

6 View: Opens the Detection Details view for this entity

Entity rows paginate independently within the expanded group. The default is 10 results per page.

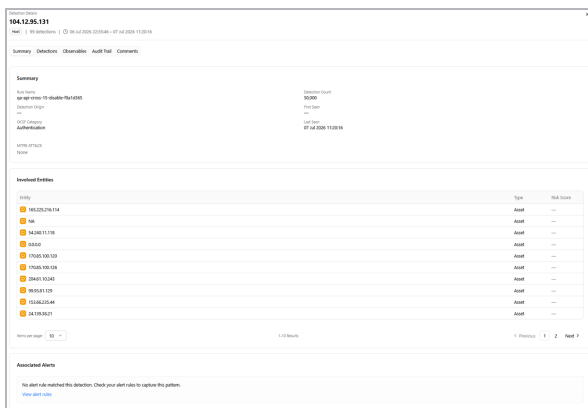
Viewing Detection Details

The **Detection Details** panel gives you a complete view of how a specific entity has been matched by a detection rule — covering detection history, extracted observables, a system audit trail, and a space for analyst collaboration. This panel lets you understand the full scope of a match and further investigate the detection before any subsequent action.



1 Summary Tab

The **Summary** tab gives you an at-a-glance overview of the detection rule, the entities involved, and whether any alert rules have been triggered by this detection.



It contains three sections;

Summary — a metadata card that shows the following fields:

- **Rule Name:** the name of the detection rule that matched this entity
- **Detection Origin:** the origin type of the detection, being either AQL rule, IOC match, or DGA match

- **OCSF Category:** the OCSF category assigned to the rule, such as Authentication or Network Activity
- **MITRE ATT&CK:** MITRE technique mapped to the rule
- **Detection Count:** total number of detection instances for this entity under this rule
- **First Seen:** timestamp of the first detection
- **Last Seen:** timestamp of the most recent detection

Involved Entities — a paginated table that lists all entities associated with this detection.

- **Entity:** entity type icon and identifier value
- **Type:** such as Asset
- **Risk Score:** current risk score; shown as a dash when not yet calculated

Associated Alerts — lists any alerts that were generated from this detection. Click the **View alert rules** link to view the associated alert rules that trigger these alerts.

2 Detections Tab

The **Detections** tab lists the individual detection instances for this entity under the matched rule.

The tab displays the exact timestamp when the detection ran, the current lifecycle status of the detection instance, and the number of log events matched by the rule in that detection run.



Timestamp	Lifecycle	Count
17 Jul 2024 11:07:19	Detection Active	50/50
17 Jul 2024 11:07:19	Detection Active	50/50
17 Jul 2024 11:07:19	Detection Active	50/50
17 Jul 2024 11:07:19	Detection Active	50/50
17 Jul 2024 11:07:19	Detection Active	50/50

3 Observables Tab

The **Observables** tab lists observables extracted from the detection events for this entity, with specific details such as:

- **Type:** observable type such as IP address
- **Value:** the observable value such as an IP address
- **Source Field:** the log field from which this observable was extracted
- **TI Match:** indicates whether this observable matches a ThreatStream observable.

APP-GIS01-345.agency.OK.local

new | 10 detections | @ 30 Jul 2024 17:02:11 - 07 Jul 2025 17:07:17

Summary Detections Observations Audit Trail Comments

Observations

Type	Value	Source Field	To Match
#	48.126.23.182	"	--
#	48.126.23.26	"	--
#	2080:1836:38F7::adbc:5	"	--
#	48.126.24.24	"	--
#	105.225.36.188	"	--
#	48.126.24.96	"	--
#	208.190.135.44	"	--
#	208.190.135.42	"	--
#	208.190.153.32	"	--
#	48.126.23.98	"	--

Nets per page: 10 > 10 Results <

< Previous 1 2 Next >

4 Audit Trail Tab

The **Audit Trail** tab is a chronological system log of all lifecycle events for this detection record.

[illegible]

Entries are written by the system and are immutable.

Each entry shows a timestamp, an event name, supporting detail on the line below, and the author.

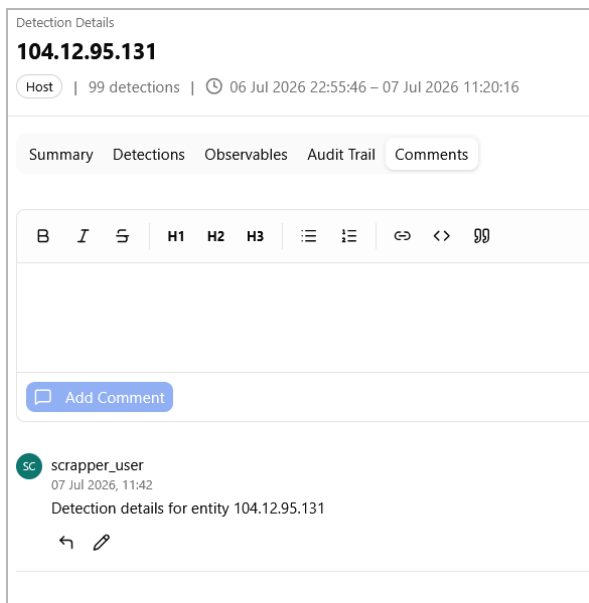
Audited event types include:

- **Detection Active** — records the timestamp the detection was produced, severity level, and enrichment manifest details when a detection becomes active
- **Detection Created** — records the match count when the detection record is first created

- **Detection Run Status Changed** — records status transitions in the detection pipeline, such as `DETECTION_STARTED` → `SEARCH_STARTED` → `SEARCH_PROCESSING` → `SEARCH_FINISHED`.

5 Comments Tab

The **Comments** tab allows analysts to add notes and context to the detection record. A rich-text composer appears at the top of the tab and includes a toolbar with standard text-formatting options.



Click **Add Comment** to add a comment.

Each comment entry shows:

- Author's name and timestamp
- The actual comment
- Per-comment action icons: **Reply** (↩) available on all comments and **Edit** (✎) available only on your own comments.

Alerts

The **Alerts** page is your primary place for managing alerts related to your security operations environment. Alerts are generated when one or more detections meet the conditions defined in an alert rule, such as a threshold, sequence, entity

correlation, or compound logic pattern. Each alert gives you a meaningful, actionable signal, helping you decide whether it warrants deeper investigation or should be escalated urgently to an incident.

From this page, you can:

- Filter and search the alert list by status, severity, triage verdict, MITRE ATT&CK tactic or technique, or assignee, or search by alert rule name, to quickly narrow down the queue
- View alert details
- Assign alerts to yourself, another analyst, or agent for investigation
- Record a triage verdict to capture your assessment of an alert
- Suppress alert rules temporarily if they generate alerts you do not currently need to act on
- Escalate alerts to incidents

To access your alerts, navigate to **ThreatStream Next Gen > Security Operations > Alerts**.

Alert Name / ID	Severity	Top Entity	Entity Risk	Detection Count	MITRE	Assignee	Last Updated	Triage Verdict	Status
12 Aug 2026 22:42 alerts_hostname_test AL-30114	High	api_gateway	1	1	T1003 (C) T1059 (C) +1	AURA	12 Aug 2026 22:44	Monitor	Triaged
12 Aug 2026 22:37 Security Event Log Cleared - ACT AL-30113	Critical	---	---	1	T1005 (C) T1070 (C)	AURA	12 Aug 2026 22:41	Decision Required	In Progress
12 Aug 2026 22:37 WDigest Credential Caching Registry Modification - ACT AL-30112	High	---	---	1	T1006 (C) T1003 (C)	AURA	12 Aug 2026 22:41	Investigate	Triaged
12 Aug 2026 22:37 qa_alert_rule_test AL-30111	High	idoe@corp.exercice.local	1	1	T1003 (C) T1059 (C) +2	AURA	12 Aug 2026 22:40	Decision Required	In Progress
12 Aug 2026 22:37 Hisashi Hands-on Testing AL-30109	Low	AsusT4648@omniurawson-grp.com	1	1	T1003 (C) T1056 (C)	AURA	12 Aug 2026 22:42	False Positive	False Positive
12 Aug 2026 22:37 alerts_hostname_test AL-30107	High	api_gateway	1	1	T1003 (C) T1059 (C) +1	AURA	12 Aug 2026 22:45	Pending	In Progress
12 Aug 2026 22:32 alerts_hostname_test AL-30106	High	api_gateway	1	1	T1003 (C) T1059 (C) +1	AURA	12 Aug 2026 22:34	Monitor	Triaged
12 Aug 2026 22:27 alerts_hostname_test AL-30105	High	api_gateway	1	1	T1003 (C) T1059 (C) +1	AURA	12 Aug 2026 22:29	Monitor	Triaged
12 Aug 2026 22:22 WDigest Credential Caching Registry Modification - ACT AL-30104	High	---	---	1	T1006 (C) T1003 (C)	AURA	12 Aug 2026 22:25	Monitor	Triaged
12 Aug 2026 22:22 Security Event Log Cleared - ACT AL-30103	Critical	---	---	1	T1005 (C) T1070 (C)	AURA	12 Aug 2026 22:25	Decision Required	In Progress

1 Status Tabs: A tab bar scoping the list to a specific lifecycle state: All, Open, In Progress, Triaged, Incident Linked, False Positive, or Closed. Selecting a tab immediately filters the list to that group.

2 Search: Search alerts by their associated alert rule name.

3 Severity: Filter alerts by severity: Critical, High, Medium, or Low.

- 4 Triage:** Filter alerts by a triage verdict: Pending, Promote, Investigate, or Monitor. See ["Triaging Alerts" on page 90](#) for verdict descriptions.
- 5 MITRE Tactic / Technique:** Multi-select filtering by MITRE ATT&CK tactic or technique. The search field lets you find a specific entry by name or TA code.
- 6 Assigned To:** Filter by self, unassigned, a specific analyst, or agent-assigned alerts.
- 7 First Seen:** The timestamp of the first constituent detection.
- 8 Alert ID:** The unique alert reference in AL - {NNNN} format; click to open the Alert Detail View.
- 9 Severity:** A color-coded severity badge: Critical (red), High (orange), Medium (yellow), Low (green).
- 10 Top Entity:** The highest-risk entity involved in the alert.
- 11 Entity Risk:** The risk score of the top entity, shown as a color-coded badge.
- 12 Detection Count:** The count of constituent detections grouped under this alert.
- 13 MITRE:** The MITRE ATT&CK tactic or technique associated with the constituent detections.
- 14 Assignee:** The assigned analyst; agent-assigned alerts show an AI attribution icon alongside the agent name; unassigned alerts show "Unassigned."
- 15 Last Updated:** The timestamp of the most recent change to the alert record, such as a status transition, triage update, assignment change, or new comment. The list is sorted by this column, most recent first, by default.
- 16 Triage Verdict:** A verdict badge showing the current analyst decision: Pending (grey), Promote (green), Investigate (blue), or Monitor (orange).
- 17 Status:** The current status of the alert lifecycle.
- 18 More options menu:**
 - **View Details:** Open the Alert Detail panel for the selected alert. See ["Viewing Alert Details" on the next page](#) for details.
 - **Escalate to Incident:** Promote the alert into a new incident for formal investigation. See ["Escalating Alerts to Incidents" on page 93](#) for details.
 - **Suppress:** Temporarily suppress the alert rule that produced this alert. See ["Adding Suppression to Alerts" on page 95](#) for details.

19 View Settings: Select the columns and table density (default or compact) to be displayed. By clicking the drag handle icon (⋮), drag and drop columns to change their position in the table. To return the view back to its default settings, click **Reset View**.

20 Date Range: The time span from the first to the most recent constituent detection, showing the full activity window of the alert.

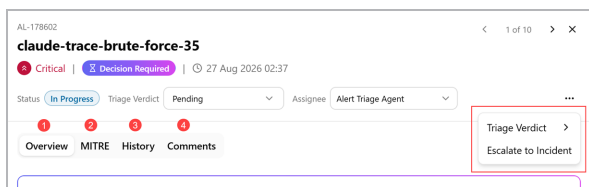
Viewing Alert Details

The alert details panel provides full context of an alert, including its constituent detections, involved entities, MITRE technique mappings, lifecycle history, and analyst comments.



Note: Viewing an alert and adding comments require the View Alerts permission. Which specific alerts you can see also depends on the eventlog or OCSF data filters configured for your role, since alert visibility follows the detections and events that produced the alert. For details, see [Managing Roles](#).

To access an alert details panel, on the Alerts page, click the name of the alert whose details you want to view, or click the more options menu (...) and select **View Details** to open the alert details panel.



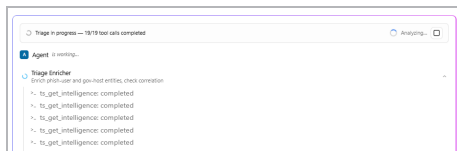
The page header displays the alert ID, alert rule name, severity badge, triage verdict badge, and the timestamp of the first detection. The header also contains the following three inline drop-downs that can be updated from any tab without switching context:

- **Status**—current lifecycle status of the alert.
- **Triage Verdict**— triage verdict on this alert. Setting a verdict transitions the alert to Triaged status automatically. Triage verdict cannot be configured for open alerts.
- **Assignee**— user or agent assigned to the alert. Setting an assignee on an Open alert transitions its status to In Progress automatically.

If you want the Alert Triage Agent to analyze the alert, click **Triage with Aura**. The Overview tab is populated with the Agent's analysis. See "[Overview Tab](#)" on the next page for details.



If you need to stop the analysis before it is fully completed, select **Analyzing**.



The more options menu (...) in the top-right of the header includes two additional actions:

- **Escalate to Incident:** Promote this alert to an incident. Clicking this option opens the Create Incident dialog-box pre-populated with the alert rule name, severity, and priority. Fill out the details using the instruction from "[Creating Incidents](#)" on [page 99](#). You must have the required permissions to perform this action. See Incident Actions and Their Required Permissions.
- **Triage Verdict:** Select a triage verdict (Promote, Investigate, Monitor, or False Positive). In the Set triage verdict dialog box that opens, select High, Medium, or Low confidence, provide a rationale, and then click **Save verdict**.



Note: The Triage Alerts permission is required to assign alerts, record a triage verdict, and mark an alert as a false positive. See [Managing Roles](#) for details.

1 Overview Tab

The **Overview** tab provides an at-a-glance summary of the alert rule, involved entities, constituent detections, and any linked incidents, supplying all the information an analyst needs to assess a match before deciding on a triage verdict.

The tab contains the following sections:

Section Name	Description
Alert Summary	Anomali AI-generated alert summary.

Section Name	Description
Agent	Alerts analyzed by Alert Triage Agent include the following fields: • Applied verdict: Final verdict applied by the Agent. Proposed verdicts require your decision to either accept the recommendation or submit one of the override actions: ▪ Promote: recommends creating an incident. Choose this when the alert represents a real security event that needs formal investigation and tracking. You can promote a single alert or select multiple related alerts to promote together into one incident. Note that this verdict does not automatically create an incident. ▪ Investigate: sends the alert for further investigation before a final call is made. Use this when you suspect something is wrong but don't yet have enough evidence to promote or dismiss it. If the investigation confirms a real threat, you'll still need to approve creating an incident . ▪ Monitor: keeps the alert open for ongoing observation instead of resolving it right away. Use this for alerts that aren't clearly malicious but are worth watching, For example, low-confidence signals that may escalate over time. The alert will be periodically re-evaluated and will eventually be promoted or closed, depending on what happens next.

Section Name	Description
	▪ False Positive: marks the alert as not a genuine security concern. Alerts classified as false positive are automatically resolved and removed from the active work queue. The decision, rationale, and supporting evidence remain part of the auditable history for later review of these alerts.  • Confidence: Percentage or qualitative score (for example, 90%) representing the Agent's certainty in its proposed verdict. • Analyst Note: (optional) add a note to the incident. An analyst note is required when submitting an override action. • Evidence: Structured list of verified signals and data points (for example, intelligence hits, metadata matches) that support the investigation. This section is distinct from the reasoning, as it focuses on factual, cited data. • How I reached this decision: Agent's reasoning. • Agent trace: Sub agents that evaluated data. Click the expand arrow of a sub agent to view its responsibility and finding.
Enrichment	Summary of all involved threat model entities with their risk context.

Section Name	Description
Alert Details	Metadata that includes the following: • Alert Rule: Name of the alert rule that generated this alert • Rule Type: Alert rule type, such as SIMPLE • Severity: Severity level assigned to the rule • OCSF Category: OCSF category associated with the rule. For example, Network Activity. • MITRE Techniques: Chip badges for each MITRE technique mapped to the constituent detections; each chip links out to the MITRE ATT&CK knowledge base • First Detection: Relative timestamp of the earliest constituent detection • Detection Count: Total number of detections grouped under this alert
Associated Detections	A paginated table of the constituent detections that triggered this alert: • Rule: Detection rule name that produced the detection • Time: Relative timestamp of when the detection ran • Entity: Entity type icon and identifier value • Risk: Risk score of the entity at the time of detection

Section Name	Description
Linked Incidents	Any incidents that arise as an escalation of this alert. The Linked Incidents table lists each incident this alert has been escalated into or associated with. Each row shows the incident Name as a clickable link to open the incident record, along with its Severity, Status, Priority, and the total number of Alerts linked to that incident.

AL-178353

< 2 of 10 > X

claude-trace-brute-force-35

⬆️ Critical

Promote

🕒 26 Aug 2026 19:07

Status

Incident Linked

Triage Verdict

Promote

Assignee

Alert Triage Agent

...

Overview

MITRE

History

Comments

 Alert Summary

A critical standalone brute-force credential alert involves an active malware and command-and-control IP with ThreatStream confidence 95.

Picked up from alert rule claude-trace-brute-force-35 (3668). Contribution from detection rule 35.

Generated by Anomali AI

Alert Details

Alert Rule

claude-trace-brute-force-35

Severity

Critical

MITRE Techniques

T1110

First Detection

7h ago

Rule Type

SIMPLE

OCSF Category

Identity & Access Management

Detection Count

1

Involved Entities

Entity	Type	Risk Score
 orichardson@apex.com	user	0
 akraus@apex.com	user	0
 jrodriguez@apex.com	user	0
 ggreen@apex.com	user	0
 sharvey@apex.com	user	0
 schang@apex.com	user	0
 arandhawa@apex.com	user	0
 alopez@apex.com	user	0
 emoulin@apex.com	user	0
 gestrada@apex.com	user	0

Items per page:

10

1-10 of 83 Results

< Previous

1

2

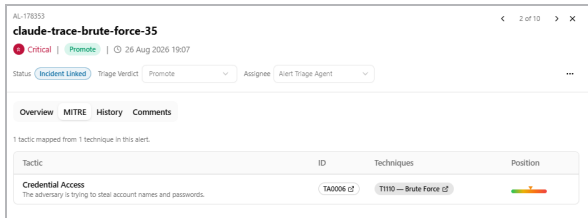
3

...

Next >

2 MITRE Tab

The **MITRE** tab shows the full ATT&CK mapping for this alert.



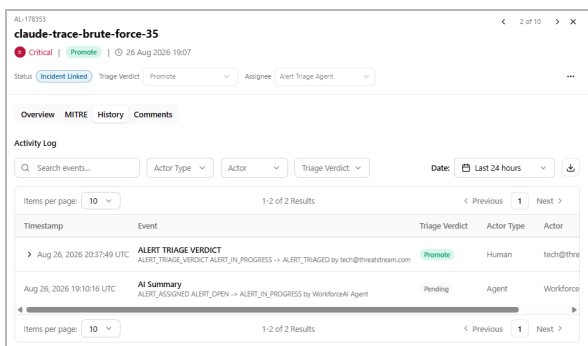
A summary line at the top states the number of tactics and techniques mapped. For example: "1 tactic mapped from 3 techniques in this alert."

The tab displays a table with the following four columns:

- **Tactic**—ATT&CK tactic name and description
- **ID** —tactic code with a link to the MITRE knowledge base
- **Techniques**—chip badges for each technique mapped under the tactic; each chip shows the technique ID and name, with a link to the MITRE knowledge base
- **Position**—color-coded bar showing the relative position of this tactic within the ATT&CK kill chain

3 History Tab

The **History** tab provides a chronological record of all triage verdicts recorded on this alert. Each entry shows the analyst name, the verdict applied, and the timestamp of the action. Use this tab to review how the alert has been assessed over time and to understand any changes in verdict.



4 Comments Tab

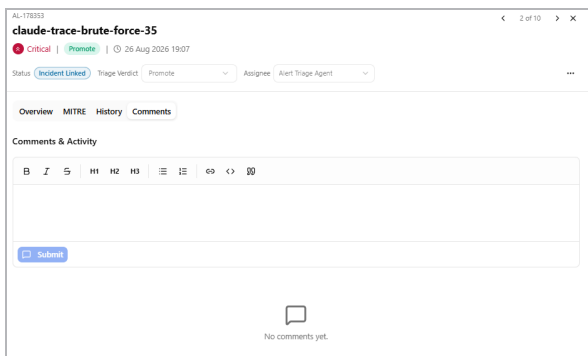
The **Comments** tab enables you to add notes and context to the alert record.

A rich-text composer at the top of the tab includes all the standard text formatting tools.

Click **Submit** to post a comment.

Each comment entry shows:

- Author name and timestamp
- The actual comment
- Per-comment action icons: **Reply** (↩) available on all comments and **Edit** (✎) available only on your own comments.



Managing Alerts

You can take the following actions for alerts generated by alert rules: assign alerts to analysts for investigation, record triage verdicts to capture your assessment, escalate confirmed threats to incidents, suppress alert rules that are generating unwanted alerts, and dismiss alerts as false positive that don't require further action.

Assigning Alerts

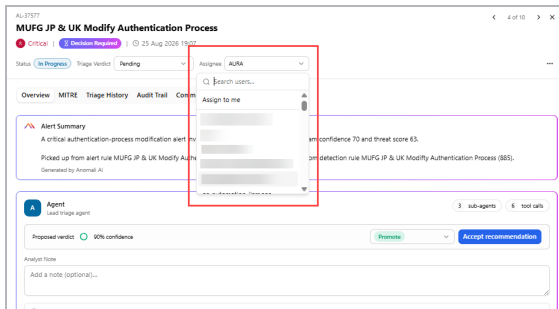


Note: You must have the Triage Alerts permission to assign alerts. See [Managing Roles](#) for details.

Open and In Progress alerts can be manually assigned to analysts for investigation. You can assign an individual alert from the alert details panel or multiple alerts from the Alerts page.

To assign an individual alert from the alert details panel:

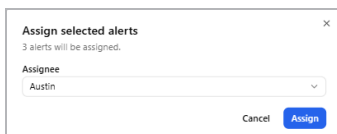
1. Navigate to **ThreatStream Next Gen > Security Operations > Alerts**.
2. Click the alert you want to assign to open the alert details panel.
3. Select an analyst from the Assignee drop-down list.



The alert is assigned to the selected analyst.

To assign alerts in bulk:

1. Navigate to **ThreatStream Next Gen > Security Operations > Alerts**.
2. Using the checkbox column, select one or more alerts you want to assign.
3. Click **Assign To**.
4. Select a user from the Assignee drop-down list.



5. Click **Assign**.

The alert is assigned.

Triaging Alerts



Notes:

- You must have the Triage Alerts permission to triage alerts. See [Managing Roles](#) for details.



- Unassigned alerts cannot be triaged.

You can set one of the following triage verdicts for alerts from the alert details panel or from the Alerts page:

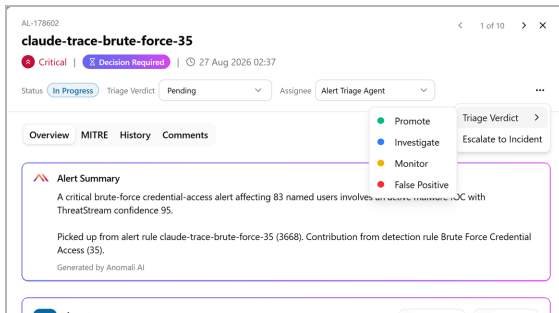
- **Promote:** recommends creating an incident. Choose this when the alert represents a real security event that needs formal investigation and tracking. You can promote a single alert or select multiple related alerts to promote together into one incident. Note that this verdict does not automatically create an incident.
- **Investigate:** sends the alert for further investigation before a final call is made. Use this when you suspect something is wrong but don't yet have enough evidence to promote or dismiss it. If the investigation confirms a real threat, you'll still need to approve creating an incident .
- **Monitor:** keeps the alert open for ongoing observation instead of resolving it right away. Use this for alerts that aren't clearly malicious but are worth watching, For example, low-confidence signals that may escalate over time. The alert will be periodically re-evaluated and will eventually be promoted or closed, depending on what happens next.
- **False Positive:** marks the alert as not a genuine security concern. Alerts classified as false positive are automatically resolved and removed from the active work queue. The decision, rationale, and supporting evidence remain part of the auditable history for later review of these alerts.

To set a triage verdict from the alert details panel:

1. Navigate to **ThreatStream Next Gen > Security Operations > Alerts**.
2. Open an alert details panel for the alert.
3. Review the associated detections, involved entities, and MITRE techniques in the Overview and MITRE tabs.
4. When ready, select one of the following verdicts from the Triage Verdict drop-down list: **Promote**, **Investigate**, **Monitor**, or **False Positive**. Alternatively, click the more options menu (...) and select a triage verdict.



Note: Pending means that no verdict has been recorded yet. This is the default state for any alert awaiting triage and it cannot be selected.

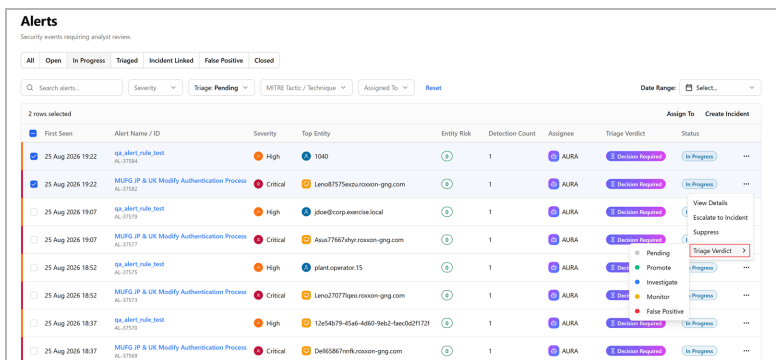


The verdict is recorded in the Triage History tab. See "[History Tab](#)" on page 88 for details.

The triaged alerts with Promote, Investigate, and Monitor verdicts appears under the Triaged tab on the Alerts page. See "[Alerts](#)" on page 78 for details.

To set a triage verdict from the alert details panel:

1. Navigate to **ThreatStream Next Gen > Security Operations > Alerts**.
2. Locate the alert of your interest and click the corresponding more options menu (...).
3. Click **Triage Verdict** and select one of the following verdicts: **Promote**, **Investigate**, **Monitor**, or **False Positive**.



The verdict is recorded in the Triage History tab. See "[History Tab](#)" on page 88 for details.

The triaged alerts with Promote, Investigate, and Monitor verdicts appears under the Triaged tab on the Alerts page. See "[Alerts](#)" on page 78 for details.

Escalating Alerts to Incidents

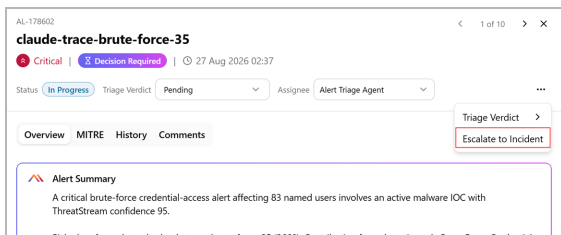


Note: This action requires the Create Incidents permission. For details on incident permissions and access, see [Managing Access to Incidents](#).

When an alert is confirmed as a true positive, escalate it to an incident for formal investigation. Alerts can be escalated to incidents from the alert details panels and the Alerts page.

To escalate an alert from the alert details panel:

1. Navigate to **ThreatStream Next Gen > Security Operations > Alerts**.
2. Open the details panel of the alert which you want to escalate to an incident.
3. In the top right corner, click the more options menu (...) and select **Escalate to Incident**. The Create Incident dialog box opens.



4. In the Create Incident dialog box, review the pre-populated title and severity (drawn from the alert), adjust as needed, and optionally assign an analyst. For details on the fields in the Create Incident dialog box, see ["Creating Incidents" on page 99](#).

Create Incident

Title *

prompte-generate-rule

Description

Describe the incident...

Priority *

P2 High

Severity *

High

Assign To

Unassigned

Associated Alerts

1 alert selected

prompte-generate-rule (AL-177568)

Tags

Search or add tag...

Cancel

Create Incident

5. Click **Create Incident**.

The alert transitions to the Incident Linked status on the Incident page.

To escalate alerts to an incident from the Alerts page:

1. Navigate to **ThreatStream Next Gen > Security Operations > Alerts**.
2. Select one or more related alerts using the checkbox column.

Alerts

Security events requiring analyst review.

AllOpenIn ProgressTriagedIncident LinkedFalse PositiveClosed

Search alerts...

Severity

Triage

MITRE Tactic / Technique

Assigned To

Reset

Date Range: Select...

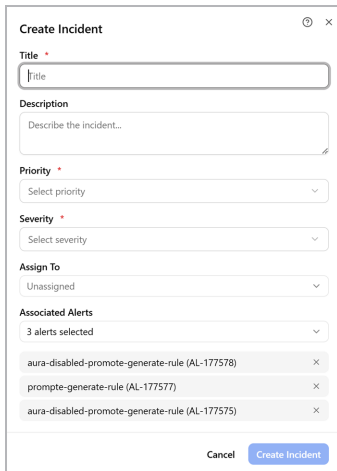
3 rows selected

Assign To>Create Incident

First Seen	Alert Name / ID	Severity	Top Entity	Entity Risk	Detection Count	Assignee	Triage Verdict	Status
☒	25 Aug 2026 1942 aura-disabled-prompte-generate-rule AL-177518	High	—	—	1	Alert Triage Agent	Monitor	Triaged
☒	25 Aug 2026 1942 prompte-generate-rule AL-177517	High	—	—	1	Alert Triage Agent	Monitor	Triaged
☒	25 Aug 2026 1937 aura-disabled-prompte-generate-rule AL-177515	High	—	—	1	Alert Triage Agent	Monitor	Triaged
☐	25 Aug 2026 1937 prompte-generate-rule AL-177514	High	—	—	1	Alert Triage Agent	Monitor	Triaged

3. Click **Create Incident**.

4. Fill out the fields in the Create Incident dialog box. For details on the fields in the Create Incident dialog box, see ["Creating Incidents" on page 99](#).

A screenshot of the 'Create Incident' dialog box. It has a title bar with a close button. The form includes: a 'Title' field with a red asterisk; a 'Description' field with placeholder text 'Describe the incident...'; a 'Priority' dropdown menu with 'Select priority' text; a 'Severity' dropdown menu with 'Select severity' text; an 'Assign To' dropdown menu with 'Unassigned' text; an 'Associated Alerts' dropdown menu with '3 alerts selected' text; and a list of three selected alerts: 'aura-disabled-promote-generate-rule (AL-177578)', 'prompte-generate-rule (AL-177577)', and 'aura-disabled-promote-generate-rule (AL-177575)'. At the bottom are 'Cancel' and 'Create Incident' buttons.

5. Click **Create Incident**.

All selected alerts transition to the Incident Linked status and are linked to the same incident record. Use this method when related alerts represent a single coordinated event that should be investigated together.

Adding Suppression to Alerts



Note: This action requires the Suppress Alert Rule permission on the alert rule that produced the alert, and at least Write access level to that rule. For details, see ["Managing Access to Alert Rules" on page 67](#).

Suppressing an alert temporarily pauses the alert rule that produced it, so it stops generating new alerts for a defined window.

To add suppression to an alert:

1. Navigate to **ThreatStream Next Gen > Security Operations > Alerts**.
2. Open the more options menu (...) of the alert you want to suppress and click **Suppress**.

Alerts
Security events requiring analyst review.

Filters: All | Open | In Progress | **Triaged** | Incident Linked | False Positive | Closed

Search: Search alerts... | Severity: [v] | Triage: [v] | MITRE Tactic / Technique: [v] | Assigned To: [v] | Date Range: [v] | Reset

Items per page: 10 | 11-20 of 46,951 Results | < Previous | 1 | 2 | 3 | ... | Next > | ⚙

☐ First Seen	Alert Name / ID	Severity	Top Entity	Entity Risk	Detection Count	Assignee	Triage Verdict	Status
☐ 25 Aug 2026 19:37	prompt-generate-rule AL-177514	High	—	—	1	Alert Triage Agent	Monitor	Triaged
☐ 25 Aug 2026 19:32	azure-disabled-prompt-generate-rule AL-177511	High	—	—	1	Alert Triage Agent	Monitor	View Details Escalate to Incident Suppress
☐ 25 Aug 2026 19:32	prompt-generate-rule AL-177510	High	—	—	1	Alert Triage Agent	Monitor	Triaged
☐ 25 Aug 2026 19:27	azure-disabled-prompt-generate-rule AL-177509	High	—	—	1	Alert Triage Agent	Monitor	Triaged
☐ 25 Aug 2026 19:27	prompt-generate-rule AL-177508	High	—	—	1	Alert Triage Agent	Monitor	Triaged

3. Select a suppression duration from the **Suppress For** drop-down and enter a mandatory reason.
4. Click **Apply Suppression** to activate the suppression window.

Suppress Alert Rule

While suppressed, this rule will not generate new alerts.

Suppress For *

24 hours

Reason *

Schedule Maintenance Window

Cancel **Apply Suppression**

While suppressed, the alert rule does not generate new alerts.

Alternatively, alert rules can be suppressed on the Alert Rules page. See ["Adding Suppression to Alert Rules" on page 62](#) for details.

Viewing Alert Details

See ["Viewing Alert Details" on page 81](#) for details on the Alert Detail panel and its five tabs.

Incidents

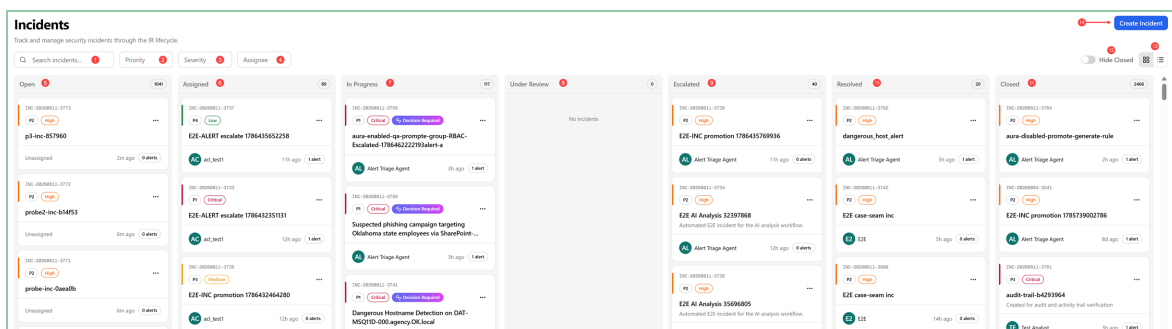
The **Incidents** page is where you track and manage security incidents throughout their lifecycle, from initial assignment and investigation through review, escalation, resolution, and closure. Incidents can be created manually by users or promoted from alerts by the Alert Triage Agent as part of the agentic workflow.

From this page, you can:

- View and organize incidents in either the tile view (grouped by lifecycle status) or a list view
- Search and filter incidents
- Create new incidents manually when an issue needs to be tracked outside the automated agentic workflow
- Track progress and update status of incidents
- Take action on incidents

To access incidents created in your organization, navigate to **ThreatStream Next Gen > Security Operations > Incidents**.

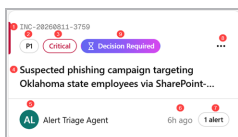
The Incidents page defaults to the tile view. Use the tile and list view icons ( ) in the top right corner to toggle between views.



The columns on the tile view correspond to incident lifecycle states:

- 1 **Search:** Search across incident titles and descriptions.
- 2 **Priority:** Filter incidents by their priorities—P1, P2, P3, or P4.

- 3 Severity:** Filter incidents by their severity—Critical, High, Medium, or Low.
 - 4 Assignee:** Filter incidents by their assignee.
 - 5 Open:** Unassigned incidents with no active owner. These are manually created incidents that are ready to be picked up by an assignee for investigation.
 - 6 Assigned:** Incidents with an analyst assigned but the investigation has not started. At this stage, assignees can either start an investigation and move the incident to In Progress, or close it.
 - 7 In Progress:** Incidents which are actively being investigated. Incidents created by the Alert Triage Agent land in this column and require your decision to either escalate them to a case, move them to the Under Review column, or close.
 - 8 Under Review:** Incidents under review. Incidents in this status remain open while a human evaluates the findings, recommendations, or proposed disposition.
 - 9 Escalated:** Incidents that have been escalated to a case by a human or agent for broader case management and response. You can either add them to cases or move them back to the In Progress status for further investigation.
 - 10 Resolved:** Incidents that have been fully investigated and resolved. You can either add them to cases or close.
 - 11 Closed:** Resolved and closed incidents. This column is hidden by default when **Hide Closed** is on.
 - 12 Hide Closed:** Use this toggle to show or hide the **Closed** column without changing underlying data.
 - 13** Tile view or list view of the incidents. Click the view you prefer.
 - 14 Create Incident:** Click **Create Incident** to manually create a new incident. See ["Creating Incidents" on the next page](#) for details.
- Additionally, each incident tile displays the following:



- 1** Priority left-border color (P1-red, P2-orange, P3-yellow, P4-green)
- 2** Priority badge
- 3** Severity badge

- 4 Incident title that you can click to open the **Incident Detail** panel
- 5 Assignee avatar and name
- 6 Relative timestamp
- 7 Alert count badge
- 8 More options menu (...) to access the following actions:
 - **View Details:** Opens the Incident Details slide-over panel. See ["Viewing Incident Details" on page 111](#) for details.
 - **Open Incident Page:** Opens the incident in a dedicated full-page view. See ["Opening the Full Incident Page" on page 119](#) for details.
 - **Add to Case:** Links the incident to an existing case or creates a new one. See ["Managing Incidents" on page 102](#) for details.



Note: An incident can only be linked to one case. Incidents that are already linked to a case do not show the **Add to Case** option.

- **Assign To:** Assigns the incident to an analyst. See ["Assigning Incidents" on page 102](#) for details.
- **Move to:** Changes the incident lifecycle status. See ["Changing Incident Status" on page 104](#) for details.
- **Close:** Closes the incident directly from the tile. See ["Managing Incidents" on page 102](#) for details.

- 9 **Decision Required:** Incidents created by the agent that require your decision.

Additionally, you can change the lifecycle status of an incident by directly dragging a card to a different column.

Creating Incidents



Note: Creating an incident, whether manually or by escalating an alert, requires the Create Incidents permission. For details on incident permissions and access, see [Managing Access to Incidents](#).

Incidents can be created manually from the Incidents page, or by escalating an existing alert. See ["Escalating Alerts to Incidents" on page 93](#) for details on creating an incident from an alert.

To create a new incident:

1. Navigate to **ThreatStream Next Gen > Security Operations > Incidents**.
2. Click **Create Incident** in the top right corner of the Incidents page.
3. In the **Create Incident** dialog, provide the following:

Create Incident

Title *

Title

Description

Describe the incident...

Priority *

Select priority

Severity *

Select severity

Assign To

Unassigned

Associated Alerts

Select alerts...

Tags

Search or add tag...

Cancel

Create Incident

- **Title** (required) — a descriptive name for the incident
- **Description** (optional) — a summary of the incident context
- **Priority** (required) — P1, P2, P3, or P4
- **Severity** (required) — Critical, High, Medium, or Low
- **Assign To** (optional) — defaults to Unassigned
- **Associated Alerts** (optional) — search and select existing alerts to link to this incident
- **Tags** (optional) — analyst-applied tags for categorization and filtering

4. Click **Create Incident**.

The incident is created and added to the Incidents board.

Managing Incidents



Note: To manage incidents, the Manage Incidents permission is required. For details, see [Managing Roles](#).

You can take several actions on the incidents in your environment. You can assign an incident to an analyst, move it through its lifecycle as work progresses, link it to a case, or close it when the investigation is complete.

Incidents handled by the Incident & Investigation Agent only require you to approve escalation or closing of incidents in the Approval Queue. See [Using Approval Queue](#) for details.

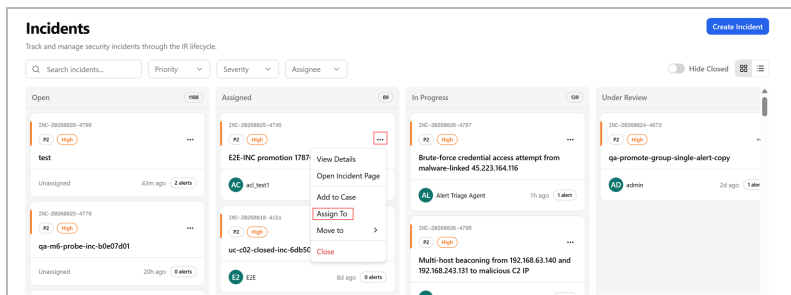
Assigning Incidents

You can assign an incident to an analyst for investigation in one of the following ways:

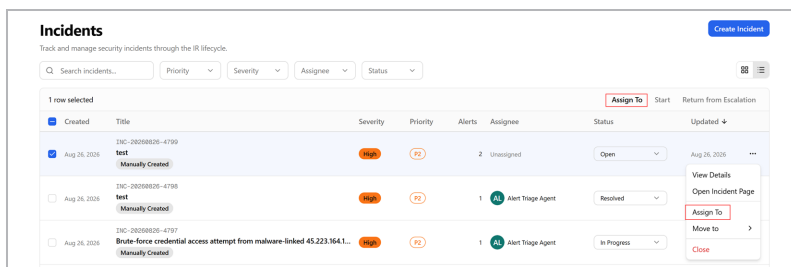
User Guide

Chapter 4: Security Operations Overview

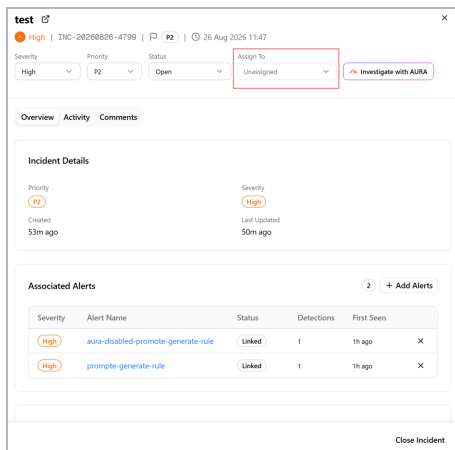
- From the incident tile on the Incidents page (tile view):



- From the Incidents page (list view)

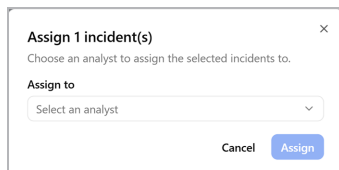


- From the Incident Details panel/page



To assign an incident from the Incidents page:

1. Navigate to **ThreatStream Next Gen > Security Operations > Incidents**.
2. Locate the incident of your interest and click the corresponding more options menu (...).
3. Click **Assign To** and choose an analyst from the Assign to drop-down list.



4. Click **Assign**.

The incident analyst is assigned.

To assign an incident from the Incident Details page:

1. Navigate to **ThreatStream Next Gen > Security Operations > Incidents**.
2. Locate the incident of your interest, click the corresponding more options menu (...), and then click **View Details**.
3. Select an analyst from the Assign To drop-down list.

The incident analyst is assigned.

Changing Incident Status

An incident moves through the following lifecycle as work progresses:

- **Open**—incident has been created but investigation has not yet started.
- **Assigned**—incident has been created and assigned to an analyst or the Incident & Investigation Agent for investigation.
- **In Progress**—incident is actively being investigated or worked on by an analyst or agent.
- **Under Review**—investigation is complete or awaiting a decision, and the findings or recommended next action are being reviewed.
- **Escalated**—incident requires further response or coordination and has been escalated to a case.

- **Resolved**—incident has been investigated and handled. No further investigation or escalation to a case is required.
- **Closed**—incident is in a terminal state and no further action is required.

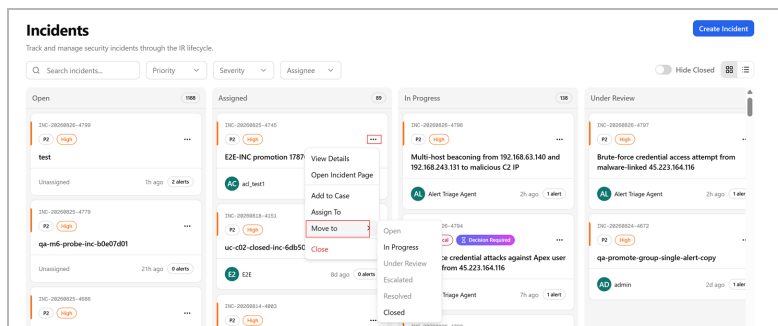
You can change an incident status from the Incidents page or from the Incident Details panel.

To change an incident status from the Incidents page:

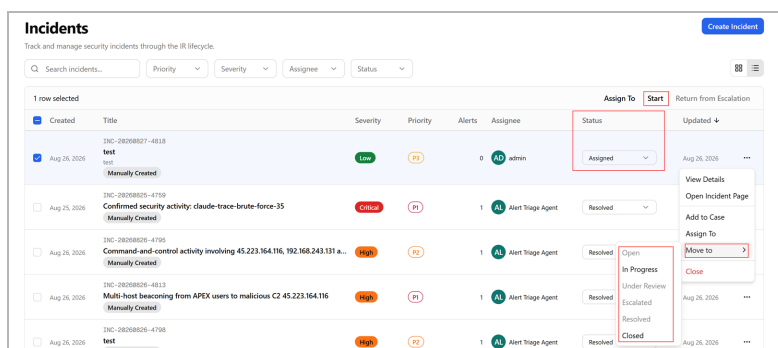
1. Navigate to **ThreatStream Next Gen > Security Operations > Incidents**.
2. On the Incidents board, drag the incident card to a different column, or open its more options menu (...) and select **Move to**, then select the next available lifecycle state—in **Progress**, **Under Review**, **Escalated**, **Resolved**, or **Closed**.



Note: Resolving or closing an incident requires the Resolve Incidents permission. See [Managing Roles](#) for details.



Alternatively, in the Incidents list view, use the inline Status drop-down on the incident row or the more options menu to change an incident status.



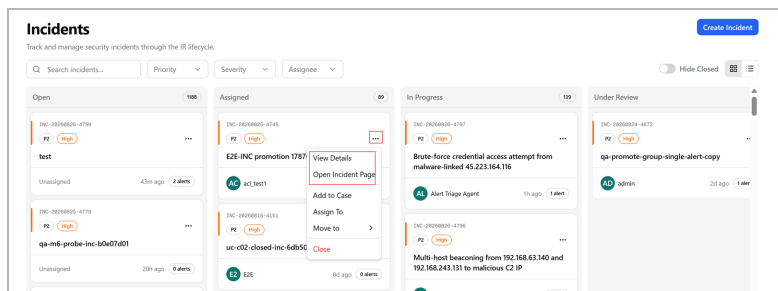


Note: You can also move an assigned incident to the In Progress status by starting incident investigation. To start an investigation, on the Incidents list view page, select the incident of your interest and click **Start**. The incident changes status to In Progress.

The incident status is updated.

To change an incident status from the Incident Details panel:

1. Navigate to **ThreatStream Next Gen > Security Operations > Incidents**.
2. On the Incidents board, locate the incident of your interest and click **View Details** or **Open Incident Page** to view incident details.



3. Select a required status.

test

High | INC-20260826-4799 | P2 | 26 Aug 2026 11:47

Severity: High | Priority: P2 | Status: Open | Assign To: Unassigned | Investigate with AURA

Overview | Activity | Comments

Incident Details

Priority: P2 | Severity: High

Created: 1h ago | Last Updated: 1h ago

Associated Alerts (2) + Add Alerts

Severity	Alert Name	Status	Detections	First Seen	
High	aura-disabled-promote-generate-rule	Linked	1	2h ago	X
High	prompte-generate-rule	Linked	1	2h ago	X

Close Incident

The incident status is updated.

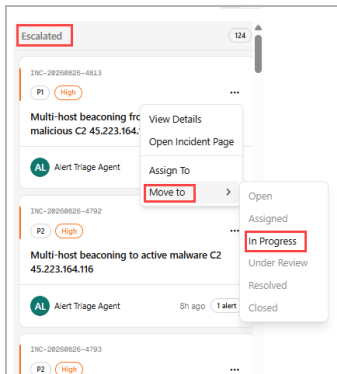
Returning Incidents From Escalation

If an incident no longer needs to sit with the escalated tier, you can return it to active work. This transitions the incident from Escalated back to In Progress, so it continues moving toward resolution instead of remaining flagged for higher-tier attention.

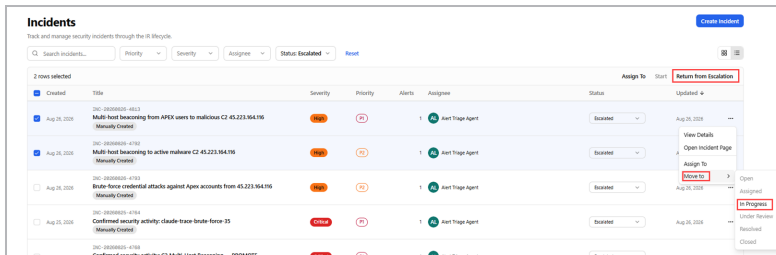
This is useful in cases when, for example, a senior analyst has completed the portion of the investigation that required their involvement and the incident can go back to the original analyst or team, when an incident was escalated in error, or when the reason for escalation no longer applies.

To return an incident from escalation:

1. Navigate to **ThreatStream Next Gen > Security Operations > Incidents**.
2. Locate the incident which you want to return from escalation, click the corresponding more options menu (...), and then click **In Progress**.



Alternatively, select one or more incidents on the Incidents list view page and click **Return from Escalation**. You can also use the more options menu (...) to move an individual escalated incident to the in Progress status.



The incident is returned to the in Progress status.

Adding an Incident to a Case

You can add an incident to a case from the Incidents page or from the Incident Details page.

- "Creating a New Case" below
- "Linking to an Existing Case" on page 111

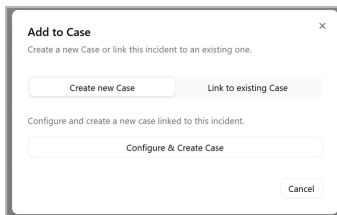
Creating a New Case

1. Navigate to **ThreatStream Next Gen > Security Operations > Incidents**.
2. Locate the incident for which you want to create a case, click the corresponding more options menu (...), and then click **Add to Case**.



Note: An incident can only be linked to one case. Incidents that are already linked to a case do not display the **Add to Case** option.

3. In the Add to Case dialog box, click **Create new Case**.



4. Click **Configure & Create Case** to open the New Case dialog box.

Complete the following fields:

- **Case Title** (required) — a descriptive name for the case
- **Case Type** (optional) — select from the available case type categories
- **Severity** — pre-populated from the incident severity; adjustable
- **TLP** — Traffic Light Protocol designation for the case (for example, GREEN)
- **Visibility** — **My Org** (visible to your organization) or **Private**
- **Tags** (optional) — analyst-applied tags for the case

- **Description** (optional) — a summary of the case context

New Case

Create a new security operations case.

Case Title *

Enter case title

Case Type

Select case type...

Severity

Medium

TLP

GREEN

Visibility

☒ My Org ☐ Private

Tags

Add tag and press Enter...

Description

Optional case description...

Cancel Create Case

5. Click **Create Case**.

The incident is linked to the new case immediately.

Linking to an Existing Case

1. Navigate to **ThreatStream Next Gen > Security Operations > Incidents**.
2. Locate the incident which you want to add to an existing case, click the corresponding more options menu (...), and then click **Add to Case**.



Note: An incident can only be linked to one case. Incidents that are already linked to a case do not display the **Add to Case** option.

3. In the Add to Case dialog box, select **Link to existing Case**.
4. Select an existing case from the Select a Case drop-down list. Each result shows the case name and the number of incidents already linked to it.

When another incident is linked to an existing case, the Case Management Agent re-runs its review so the case summary, evidence, correlations, and recommendations reflect the newly added information.

5. Click **Add to Case**.

The incident is linked to the existing case.

Viewing Incident Details

See "[Viewing Incident Details](#)" below for details on the Incident Details panel and its tabs.

Viewing Incident Details



Note: Viewing an incident requires the View Incidents permission and at least Read access to that specific incident. For details, see Managing Access to Incidents.

You can view the full context of an incident, including its source alerts, related entities, activity history, and analyst comments, in the incident details panel or the dedicated full-page view.

To open the incident details panel, click the more options menu (...) for an incident in the list view and select **View Details**. You can also click the incident title directly.

The Incident Details panel provides a focused view of a single incident across three tabs: Overview, Activity, and Comments. Use these tabs to review source alerts and incident details, track lifecycle activity, and collaborate with your team without leaving the Incidents page.

Windows Security Event Log Cleared – Possible Defense Evasion (T1070)

Critical

INC-20260810-0015

P1

10 Aug 2026 15:29

Severity

Critical

Priority

P1

Status

Resolved

Assign To

agent.soc+org_id_2956...

4

...

1

2

3

Overview

Activity

Comments

Incident Summary

A Windows Security event log was reportedly cleared, but the absence of host, user, process, and correlated activity prevents determining whether the action was malicious or authorized.

Picked up from alert Security Event Log Cleared - ACT (68466) (alert rule Security Event Log Cleared - ACT (7), detection rule Security Event Log Cleared - ACT (50)).

Generated by Anomali AI

A

Agent

Lead incident investigation agent

6

sub-agents

10

tool calls

Applied verdict

90% confidence

Analyst Note

Add a note (optional)...

Closure reason: Inconclusive

Evidence

How I reached this decision

Agent trace

Incident Details

Priority

P1

Severity

Critical

Created

21h ago

Last Updated

2h ago

Associated Alerts

0

+ Add Alerts

No associated alerts.

Relationships

No linked case.

1 Overview Tab

The **Overview** tab is the default landing tab. It gives you a summary of the incident metadata, its source alerts, and any case relationships that you may need to assess the incident before taking action.

The tab includes the following sections:

Section Name	Description
Incident Summary	Anomali AI-generated incident summary.

Section Name	Description
Agent	Incidents created by the Alert Triage Agent include the following fields: Proposed verdict: Final action recommended by the Incident Response Agent after evaluating the alerts associated with the incident. Incidents with the In Progress status require you to either accept the recommendation of the Agent, or submit an override action along with the note describing the reason for escalation. • Confidence: Percentage or qualitative score (for example, 90%) representing the Agent's certainty in its proposed verdict. • Analyst Note: (optional) add a note to the incident. • Evidence: Structured list of verified signals and data points (for example, intelligence hits, metadata matches) that support the investigation. This section is distinct from the reasoning, as it focuses on factual, cited data. • How I reached this decision: Agent reasoning. • Agent trace: Sub agents that evaluated data. Click the expand arrow of a sub agent to view its responsibility and finding.

Section Name	Description
Incident Details	Metadata displaying the following incident details: • Priority: Current incident priority badge (P1–P4) • Severity: Current incident severity badge (Critical, High, Medium, or Low) • Created: Relative timestamp of when the incident record was created • Last Updated: Relative timestamp of the most recent change to the incident record
Associated Alerts	Source alerts linked to this incident, with a count badge and an + Add Alerts button to link additional alerts. The source alerts table includes the following columns: • Severity: color-coded severity badge for the alert • Alert Name: alert name as a clickable link to the Alert Details panel. • Status: current alert status. • Detections: count of constituent detections in the alert • First Seen: relative timestamp of the earliest constituent detection
Relationships	Displays any case to which this incident has been linked. An incident can only be linked to one case. Click Open to open the linked case in a new tab and view the details of the case. See "Viewing Case Details" on page 125 for more information.

2 Activity Tab

The screenshot displays the 'E2E UI audit escalate test' incident page. At the top, the incident title is followed by a link icon. Below the title, the severity is 'Medium' (orange dot), priority is 'P3' (blue dot), and the timestamp is '08 Jul 2026 05:57'. A filter bar shows 'Severity: Medium', 'Priority: P3', 'Status: Assigned', and 'Assign To: admin'. Below this is a tab bar with 'Overview', 'Activity', and 'Comments'. The 'Activity' tab is selected, showing an 'Activity Log' with four entries: 1. 'Incident INC-20260708-1396 created by scrapper_user' (Created badge, 8h ago). 2. 'Alert run 1780 linked by scrapper_user' (Alert badge, 8h ago). 3. 'Assigned to admin by scrapper_user' (Assignment badge, 1m ago). 4. 'Status changed OPEN → ASSIGNED' (Status badge, 1m ago).

The **Activity** tab displays the **Activity Log** — a chronological, immutable record of all system and analyst events on this incident. Each entry shows a color-coded dot, an event description, an event type badge, the author, and a relative timestamp.

Logged event types include:

- **Created**—records when the incident record was first created and by whom
- **Alert**—records when an alert is linked to the incident
- **Assignment**—records when the incident is assigned to an analyst
- **Status**—records a status transition, for example OPEN → ASSIGNED

3 Comments Tab

E2E UI audit escalate test

Medium

P3

08 Jul 2026 05:57

Severity

Priority

Status

Assign To

Medium

P3

Assigned

admin

Overview

Activity

Comments

Comments & Activity

SR

B

I

S

H1

H2

H3

Comment

SC

scrapper_user

08 Jul 2026, 14:07

Comment for E2E UI incident.

The **Comments** tab allows you to add notes and context to the alert record. A rich-text composer appears at the top of the tab that includes all the standard text formatting tools.

Click **Submit** to post a comment.

Each comment entry shows:

Anomali ThreatStream Next Gen

Page 118 of 297

- Author name and timestamp
- The actual comment
- Per-comment action icons: **Reply** (↩) available on all comments and **Edit** (✎) available only on your own comments.

3 Actions Menu

Click the action menu and select **Add to Case** to add the incident to a case. For details, see "[Managing Incidents](#)" on page 102.

Opening the Full Incident Page

To open an incident in a dedicated full-page view, click the external link icon next to the incident title.

The full-page view expands the same **Overview**, **Activity**, and **Comments** tabs into a two-column layout: the Summary sidebar on the left and the tab content on the right.

The screenshot displays the full incident page for an incident titled "E2E UI audit escalate test". The interface is divided into a left sidebar and a main content area.

Left Sidebar (Summary):

- Incident ID: INC-2020087005-1396
- Priority: P3
- Severity: Medium
- Status: Assigned
- Assign To: admin
- Created: 8h ago
- Last Updated: 2m ago
- Tags: Search or add tag...

Main Content Area:

- Incident Details:** Shows Priority (P3), Severity (Medium), Created (8h ago), and Last Updated (2m ago).
- Associated Alerts:** A table with 5 columns: Severity, Alert Name, Status, Detections, and First Seen. It contains one entry: Severity: High, Alert Name: qa_detections_tests_arc, Status: Linked, Detections: 1, First Seen: 8h ago. There is an "Add Alerts" button.
- Relationships:** Shows "No linked case".

At the top right of the main content area, there are tabs for "Overview", "Activity", and "Comments", and an "Add to Case" button.

Cases

The **Cases** page is your top-level investigation place in Anomali Agentic SOC Operations Security Operations. Cases compile incidents, alerts, detections, evidence, threat intelligence, analyst decisions, recommendations, and audit history into governed records.

A case also provides the capabilities beyond what an incident offers:

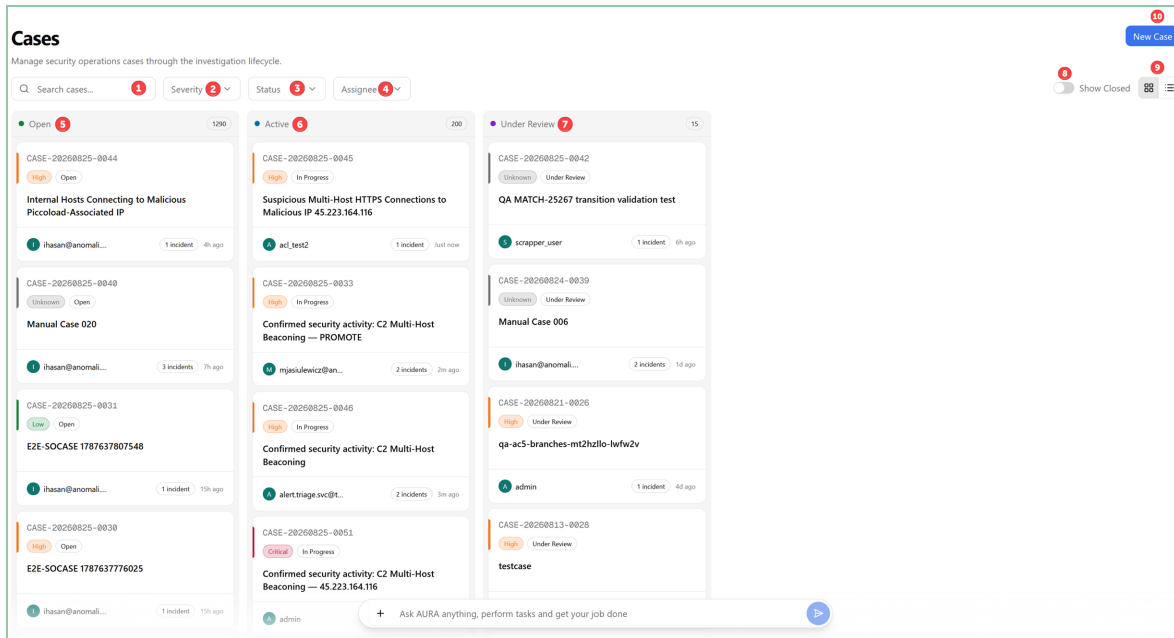
- **Evidence Locker** that serves as an immutable evidence store wherein files, SIEM search results, and system-generated artifacts are stored with SHA-256 integrity hashing. See ["Using the Evidence Locker" on page 134](#) for details.
- **Response Workbook** that comprises a structured four-phase incident response plan with task tracking and an Anomali AI-generated case summary. See ["Using the Response Workbook" on page 139](#) for details.

To access cases created within your organization, navigate to **ThreatStream Next Gen > Security Operations > Cases**.

You can use the tile or list view of the Cases page to manage cases in your organization.

Related topics:

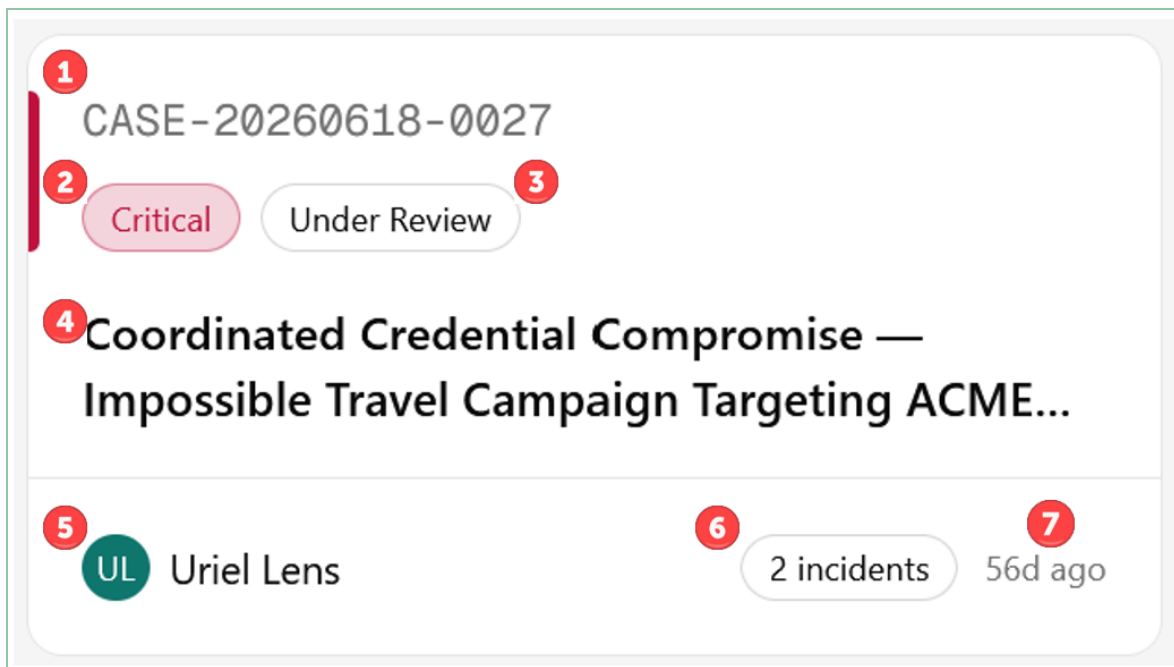
- ["Creating a Case" on page 123](#)
- ["Managing Access to Cases" on page 142](#)
- [Managing Access to Cases](#)
- ["Viewing Case Details" on page 125](#)
- ["Using the Evidence Locker" on page 134](#)
- ["Using the Response Workbook" on page 139](#)
- ["Closing Cases" on page 149](#)



The Cases page defaults to the Kanban board view. The board has four columns representing the case lifecycle: **Open**, **Active**, **Under Review**, and **Closed**.

- 1 Search:** Free-text search across existing cases.
- 2 Severity:** Filter cases by severity. Possible values include Critical, High, Medium, Low, or Unknown.
- 3 Status:** Filter cases by lifecycle status.
- 4 Assignee:** Filter by the assigned lead analyst.
- 5 Open:** Denotes that the case has been created and is ready for investigation but has not yet been started.
- 6 Active:** Implies the case is actively in progress. Active cases display a sub-state badge:
 - **In Progress**— investigation is ongoing
 - **On Hold**— investigation has been temporarily paused
 - **Escalated**—investigation has been raised to a higher tier of criticality
- 7 Under Review:** Signifies that the investigation work is complete and the case has been submitted for sign-off by the assigned approver.

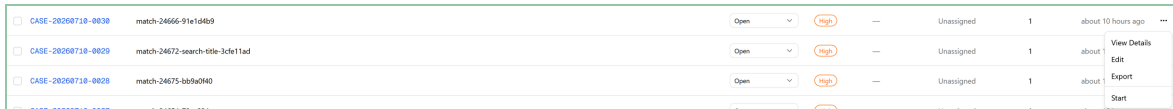
- 8 Show Closed:** Toggle the **Show Closed** switch to display closed cases. Closed cases are read-only and are a hidden column by default. See ["Closing Cases" on page 149](#) for more details on the case closure and reopening workflow.
- 9** Click the grid icons to switch between a Kanban board view or a list view of all the cases.
- 10** Click **New Case** in the top-right corner of the page to manually create a new case. See ["Creating a Case" on the next page](#) for more information.



Each case card on the board displays:

- 3 Case number:** Auto-generated identifier in CASE - {YYYYMMDD} - {NNNN} format
- 1 Severity:** Severity level of the case, shown as a color-coded left border and badge (Critical=red, High=orange, Medium=yellow, Low=green, Unknown=gray)
- 2 Case Status:** Status of the case.
- 4 Case Title:** Name of the case.
- 5 Lead Analyst:** Avatar and name of the assigned analyst. A case is automatically assigned to the analyst that created it.
- 6 Incidents:** Number of incidents linked to the case.
- 7 Last Updated:** Relative timestamp of when the case was last updated

Click a card to open the case in a slide-over panel. See ["Viewing Case Details" on page 125](#) for more information.



Case ID	Match	Status	Priority	Count	Timestamp	Actions
CASE-26258718-0829	match-24666-91e1d4b9	Unassigned	High	1	about 10 hours ago	Open, View Details, Edit, Export, Start
CASE-26258718-0829	match-24672-search-title-3c111ad	Unassigned	High	1	about	Open, View Details, Edit, Export, Start
CASE-26258718-0829	match-24675-bb9d0f40	Unassigned	High	1	about	Open, View Details, Edit, Export, Start

Switch to the list view and click the more options menu icon (...) to access more actions you can take on cases:

- **View Details:** Opens the case slide-over panel. See ["Viewing Case Details" on page 125](#) for more information.
- **Edit:** Opens an edit modal to update case metadata. See ["Editing Cases" on page 144](#) for more information.
- **Export:** Generates a TLP-filtered evidence package export. See ["Exporting Evidence" on page 137](#) for more information.
- **Start:** Opens the Start Case modal. See ["Starting Cases" on page 146](#) for more information.
- **Additional Actions:** Select one or more cases and click **Assign To** to assign the case to an analyst, or click **Add Tags** to add one or more tags to the case. See ["Assigning Cases" on page 142](#) and ["Adding Tags to Cases" on page 143](#) for details.

You can also change the lifecycle status of a case directly by dragging its card to a different column on the board. See ["Changing a Status of Cases" on page 147](#) for more information.

Creating a Case

If you do not use the agentic SOC Operations workflow for your security operations, you can create cases manually.



Note: Creating a case requires the Create Cases permission. See [Managing Roles](#) for details.

To manually create a new case:

1. Navigate to **ThreatStream Next Gen > Security Operations > Cases**.
2. Click **New Case** in the top-right corner of the Cases page to open the New Case dialog box.
3. Define values for the following fields:

Field	Description
Case Title	Provide a short unique name for the case.
Description	(Optional) Enter a summary of the case.
Associated Incidents	Select one or more incidents linked to this case.
Severity	Select a severity level of the case— Critical , High , Medium , Low , or Unknown . Default: Unknown.
Assign To	(Optional) Select an analyst to lead the case.
Approver	(Optional) Select a case approver.
Visibility	Set a case visibility: ▪ My Org—makes the case visible to your organization. ▪ Private—restricts access to the user managing the case. Default: <i>My Org</i> .
Tags	Select tags to be associated with the case. The available tags are derived from the ThreatStream Preferred Tags list. See Adding Preferred Tags to Intelligence for more information. To create a custom tag, enter the desired tag value in the search field and click +.

New Case

Create a new security operations case.

Case Title *
Enter case title

Description
Optional case description...

Associated Incidents *
Select incidents...

Severity
Unknown

Assign To
Select analyst...

Approver
Select approver...

Visibility
☒ My Org ☐ Private

Tags
Add tag and press Enter...

Cancel Create Case

4. Click **Create Case**.

The case is assigned an auto-generated case number and placed in the Open column on the Cases page.

Viewing Case Details

On this page:

- ["Using the Case Details Panel" on the next page](#)
- ["Accessing the Case Full-Page View" on page 133](#)

Related topics:

- ["Cases" on page 120](#)
- ["Managing Access to Cases" on page 142](#)
- ["Using the Evidence Locker" on page 134](#)
- ["Using the Response Workbook" on page 139](#)
- ["Closing Cases" on page 149](#)



Note: The View Cases permission is required to view case details. See [Managing Roles](#) for details.

On the **Case Details** panel, you can view the full context of a case, including its metadata, associated incidents, evidence, audit log, and comments.

To open the Case Details panel, click a case tile on the Cases page or select **View Details** from the Cases list view page.

For a more comprehensive investigation experience, you can open the case in the full-page version. The full-page view provides additional capabilities such as linked cases, response workbook, and case closure details.

See "[Accessing the Case Full-Page View](#)" on page 133 for details.

Using the Case Details Panel

A Case Details slide-over panel displays a case header followed by the Overview, Incidents, Evidence Locker, Audit Log, and Comments tabs.

Case Details

Multi-host C2 beaconing to Piccoload infrastructure 45.223.164.116

High

CASE-20260828-0008

1 incident

Created 4h ago · Updated 4h ago

Status

Severity

Assignee

Open

High

Overview

Incidents

Evidence Locker

Audit Log

Comments

Case Description

Three endpoints made corroborated outbound connections to 45.223.164.116:443 in one escalated incident; retain the case at HIGH while validating endpoint activity, preserving missing evidence, and tuning existing C2 detection coverage.

Generated by Copilot

AURA

Case ready

Case preparation complete — 28/28 tool calls completed

Case Details

AURA

✓ Main Agent

✓ Entity Correlation Agent

✓ Timeline Agent

✓ Intel Aggregation Agent

✓ Evidence Auditor

✓ Attack Chain Agent

✓ Severity & Scope Agent

✓ Response Planning Agent

✓ Report Writer Agent

Case preparation complete.

Linked Incidents

Multi-host C2 beaconing to malware infrastructure 45.223.164.116

Critical

Regulatory & Compliance

Compliance Frameworks

NIST_CSF

NIST_800_53

ISO_27001

SOC2

PCI_DSS

HIPAA

GDPR

CIS_CONTROLS

MITRE_ATTACK

FEDRAMP

Note

Add compliance notes...

Anomali ThreatStream Next Gen

Page 127 of 297

1 Case header: displays the case title, a case severity badge, a unique case ID, the number of linked incidents, and creation/update timestamps. Below that, there are dropdown fields for Status, Severity, and Assignee, allowing you to quickly view and update these key case attributes.

2 Overview Tab

The **Overview** tab is the default landing tab of the case details panel. It contains the following sections:

Section Name	Description
Case Description	Anomali AI-generated case summary, synthesized from all linked incidents, evidence, and threat intelligence.

Section Name	Description
AURA	AURA (Anomali Unified Response Agent) is the orchestrator behind the Agentic Fleet. At the case level, AURA runs the Case Management Agent, which consolidates all linked incidents, alerts, detections, evidence, and threat intelligence into a complete case enrichment. The section displays the agent status, the number of tool calls completed, and a checklist of the following sub-agents: • Main Agent • Entity Correlation Agent • Timeline Agent • Intel Aggregation Agent • Evidence Auditor • Attack Chain Agent • Severity & Scope Agent • Response Planning Agent • Report Writer Agent Additionally, this section includes the Case Details button allowing you to open a full-page view of the case. See "Accessing the Case Full-Page View" on page 133 for details.
Linked Incidents	Incidents linked to the case. You can click each incident to view incident details. See "Viewing Incident Details" on page 111 for more information on incident details.

Section Name	Description
Regulatory & Compliance	Compliance tags applicable to the case (such as PCI-DSS, HIPAA, or GDPR). Click a tag you consider relevant to the case. Use the Note field to leave compliance notes.

OverviewIncidentsEvidence LockerAudit LogComments

Case Description

Two independent security clusters require continued investigation; an inconclusive repeated-failed-MFA cluster and a suspected-C2 cluster derived from a disabled QA fixture. No compromised user, system, or cross-incident attack chain is confirmed.
Generated by Copilot

AURA

Case ready

Case preparation complete — 34/34 tool calls completed

Case Details

AURA

✓ Main Agent

✓ Entity Correlation Agent

✓ Timeline Agent

✓ Intel Aggregation Agent

✓ Evidence Auditor

✓ Attack Chain Agent

✓ Severity & Scope Agent

✓ Response Planning Agent

✓ Report Writer Agent

Case preparation complete.

Linked Incidents

Suspected C2 Communication with 45,225,135.18 Tagged for Backdoor and Malware Activity

High

Confirmed security activity: claude-trace-brute-force-35

Critical

Regulatory & Compliance

Compliance Frameworks

NIST_CSF NIST_800_53 ISO_27001 SOC2 PCI_DSS HIPAA GDPR CIS_CONTROLS MITRE_ATTACK FEDRAMP

Note

Add compliance notes...

3 Incidents Tab

The **Incidents** tab is the primary place for managing incidents linked to the case.

Case Details

E2E-SOCASE 1787637776025

High

CASE-20208825-0028

2 incidents

Created 17h ago · Updated 1h ago

Status

Severity

Assignee

In Progress

High

ac1.test1

OverviewIncidentsEvidence LockerAudit LogComments

Linked Incidents (2)

Add Incidents()

Q Search incidents...

Priority

Severity

Assigned To

Status

Reporter

Items per page: 10

1-2 of 2 Results

< Previous

1

Next >

\$

Time

Incident ID

Title

Priority

Status

Assignee

Reporter

1h ago

[INC-20208825-4584](#)

Multi-host C2 beaconing to PicoLoad infrastructure at 45.223.164.116

P1

In Progress

Alert Triage Agent

393

...

17h ago

[INC-20208825-4735](#)

rbac-v0 patch-inc-1a2d4d95 RBAC test incident

P2

Closed

E2E cleanup

1894

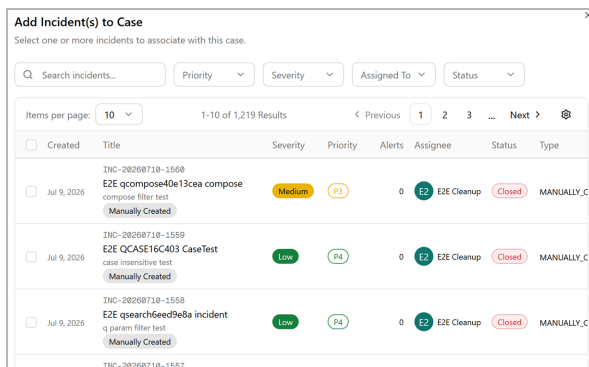
...

The tab header shows **Linked Incidents (N)**. Filter incidents by priority, severity, analyst assigned to, and status. Select one or more incidents and confirm to link them.

If you need to add more incidents to the case, click **Add Incident(s)** to open a search modal for linking existing incidents to the case.

All linked incidents are provided in a table with the following columns:

Column	Description
Created	Date the incident was created.
Title	Incident (INC) number, incident title, short description, and incident type.
Severity	Severity level of the incident.
Priority	Priority level of the incident (P1–P4).
Alerts	Count of alerts linked to the incident.
Assignee	Avatar and name of the analyst assigned to the incident.
Status	Current lifecycle state of the incident
Type	Incident type (for example, Manually Created).
Updated	Relative timestamp of when the incident was last updated.



4 Evidence Locker Tab

The **Evidence Locker** tab provides access to the case evidence page. See ["Using the Evidence Locker" on page 134](#) for full documentation of evidence ingestion, TLP classification, exports, and the Audit Log.

5 Audit Log Tab

The case-level **Audit Log** tab is the single record of all activity on the case. Each entry displays a UTC timestamp, an event type, a description of the action taken, the actor type (Human or System), the actor name, and the source.

Use the Search events field and the Actor Type, Actor, and Source filters to narrow results. Use the Date preset to adjust the time range. Click the download icon to export the log as a CSV, PDF, or DOCX file. Audit log entries are immutable.

Timestamp	Event	Actor Type	Actor	Source
Aug 26, 2024 17:48:53 UTC	Locker Page Opened Locker page opened by viewsearch@anomaly.com	Human	viewsearch@anomaly.com	Case
Aug 26, 2024 00:01:11 UTC	Case Closed Case closed by scraper_user	Human	scraper_user	Case
Aug 26, 2024 00:01:11 UTC	Comment Case resolved (FALSI_POSITIVE) by scraper_user	Human	scraper_user	Case
Aug 26, 2024 00:01:09 UTC	Comment Workbook template loaded: R_STANDARD	Human	scraper_user	Case
Aug 26, 2024 00:01:10 UTC	Status Case status changed (OPEN -> R_RESOLVED) by scraper_user	System	scraper_user	Case
Aug 26, 2024 00:01:09 UTC	Case Created Case CASE-20240826-0000 created by scraper_user	Human	scraper_user	Case

6 Comments Tab

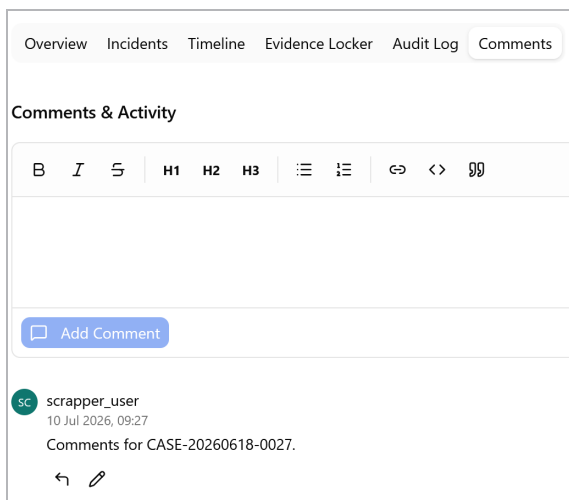
The **Comments** tab allows analysts to add notes and context to the case record. A rich-text composer appears at the top of the tab that includes all the standard text formatting tools.

Click **Submit** to post a comment.

Each comment entry shows:

- Author name and timestamp
- The actual comment
- Per-comment action icons: **Reply** (↩) available on all comments and **Edit** (✎)

available only on your own comments.



7 More options menu:

- **Share:** Click **Share** to copy the case link to clipboard.
- **Export:** Click **Export** > **Download** to download a .zip folder with all files associated with the case.

Accessing the Case Full-Page View

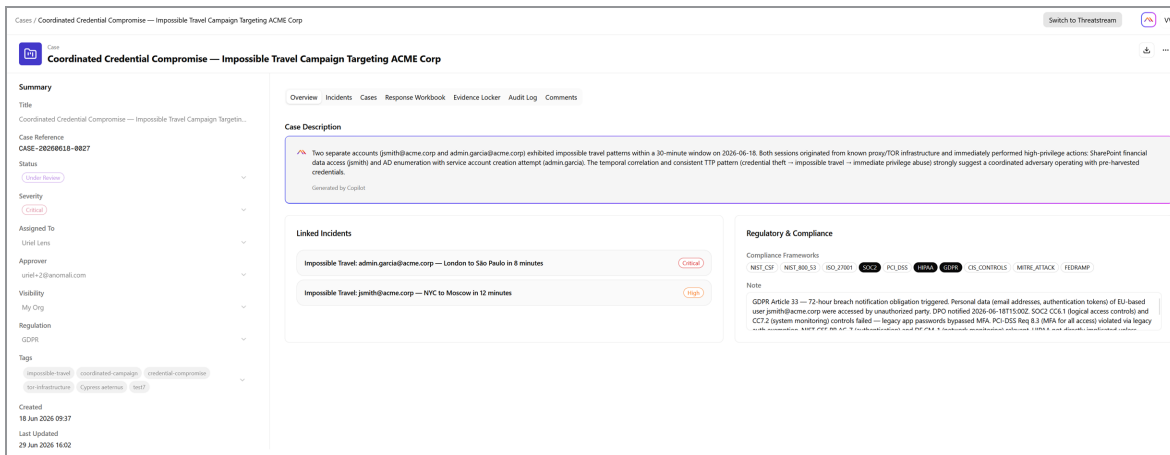
To open the dedicated case full-page view, click the external link icon (🔗) next to the case title in the Case Details slide-over panel header, or select **Open Case Page** from the more options menu (...) on the Cases list view page.

Use the full-page view as the primary workspace for in-depth case investigation. Unlike the slide-over panel, it keeps key case metadata visible in the left sidebar as you move between tabs.

The full-page view also provides the following additional capabilities:

- AI-generated case description.
- Cases tab: Lets you link related cases.
- Response Workbook tab: Lets you track incident response phases, generate a lessons learned record, and coordinate approver sign-off before closing the case. See ["Using the Response Workbook" on page 139](#) for details.
- Closure Record tab: Appears after the case is closed and displays closure details, including the case resolution, the user who closed the case, and the

closure date. See ["Closing Cases" on page 149](#) for more information on the full closure workflow.



Using the Evidence Locker

The **Evidence Locker** is an immutable evidence store attached to every case. It preserves files, investigation artifacts, and system-generated

evidence with SHA-256 integrity hashing for chain-of-custody tracking. Evidence items added to the Evidence Locker cannot be deleted or modified after addition.

On this page:

- ["Adding Evidence" below](#)
- ["Understanding Evidence Locker Components" on page 137](#)

Related topics:

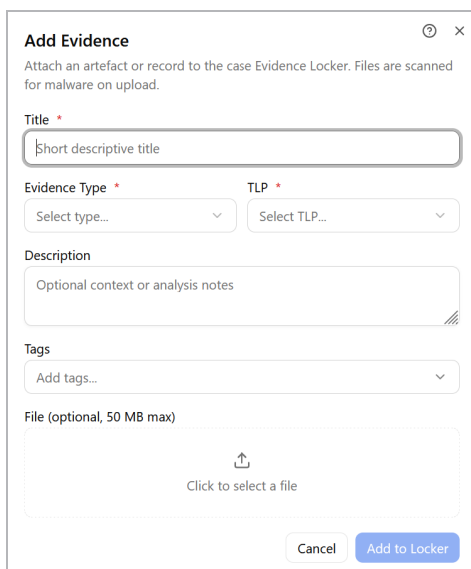
- ["Cases" on page 120](#)
- ["Viewing Case Details" on page 125](#)

Adding Evidence

You can attach one or more artifacts or records to the evidence locker associated with a case.

1. Navigate to **ThreatStream Next Gen > Security Operations > Cases**.
2. Click on a case tile.
3. Click the **Evidence Locker** tab.
4. Click **Add Evidence**.

5. In the upload modal, complete the required fields:
 - **Title:** Enter a title for the evidence.
 - **Evidence Type:** Select the type of the evidence artifact. See "[Evidence Types](#)" below for a list of supported formats.
 - **TLP Classification:** select one of the classification options: WHITE, GREEN, AMBER, RED
6. (Optional) Add a description and tags.
7. Select the file to upload. Maximum file size is 50 MB per file.
8. Click **Upload**.



The screenshot shows the 'Add Evidence' modal window. It has a title bar with a close button. The main content area includes a 'Title' field with a placeholder 'short descriptive title'. Below it are two dropdown menus: 'Evidence Type' and 'TLP', both with 'Select type...' and 'Select TLP...' options. There is a 'Description' text area with a placeholder 'Optional context or analysis notes'. Below that is a 'Tags' dropdown with 'Add tags...'. At the bottom is a 'File' section with a placeholder 'File (optional, 50 MB max)' and a large dashed box containing an upload icon and the text 'Click to select a file'. At the very bottom are 'Cancel' and 'Add to Locker' buttons.

Uploaded files are scanned for malware on ingest. A file with a detected threat is rejected immediately and the rejection is recorded in the Audit Log with the reason. If the scan fails, contact Anomali Support for assistance .

Evidence Types

The **Evidence Type** field categorizes each item added to the Evidence Locker.



Note: Maximum file size: 50 MB. Maximum total Case Locker storage: 5 GB per case.

Available types include:

Evidence Type	Description
Log Extract	Raw or processed log file extract. Supported formats: .log and .txt.
Screenshot	Screenshot or image file. Supported formats: PNG, JPG, JPEG, GIF, BMP, TIFF, and WEBP
File	Any other document, spreadsheet, or text file. Supported formats: PDF, DOCX, DOC, TXT, MD, RTF, XLSX, XLS, CSV, and HTML.
IOC Set	Collection of IOCS, such as IP addresses, domains, URLs, or file hashes, associated with the investigation.
Memory Dump	Captured copy of system memory that can be analyzed for evidence of malicious activity, processes, or artifacts.
Packet Capture	Capture of network traffic that provides detailed information about communications observed during the investigation. Supported formats: PCAP, PCAPNG.
Report	Structured document that summarizes investigation findings, supporting evidence, and relevant conclusions or recommendations. Supported formats: PDF and DOCX.
Other	Any binary or file not covered by the other types.

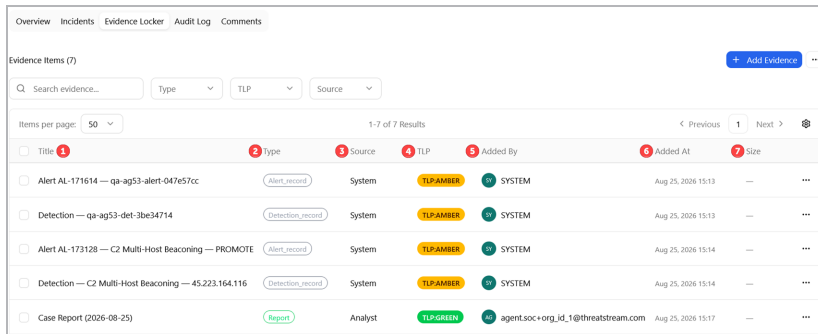
Using System-Generated Evidence

Evidence items can arrive in the Evidence Locker automatically from external investigation systems. This is the primary mechanism for capturing SIEM log search results, investigation reports, and detection artifacts without requiring analysts to manually export and re-upload files.

System-generated items appear in the Evidence Locker with the originating system identity as the source and labeled as `SYSTEM`, rather than an analyst name.

Understanding Evidence Locker Components

Evidence Items



The screenshot shows the 'Evidence Locker' tab in a software interface. It displays a table of evidence items with the following columns: Title, Type, Source, TLP, Added By, Added At, and Size. The table contains five rows of data, each representing a different evidence item. The first row is 'Alert AL-171614 — qa-ag53-alert-047e57cc' with Type 'Alert_record', Source 'System', TLP 'TLP:AMBER', Added By 'SYSTEM', Added At 'Aug 25, 2026 15:13', and Size '—'. The second row is 'Detection — qa-ag53-det-3be34714' with Type 'Detection_record', Source 'System', TLP 'TLP:AMBER', Added By 'SYSTEM', Added At 'Aug 25, 2026 15:13', and Size '—'. The third row is 'Alert AL-173128 — C2 Multi-Host Beacons — PROMOTE' with Type 'Alert_record', Source 'System', TLP 'TLP:AMBER', Added By 'SYSTEM', Added At 'Aug 25, 2026 15:14', and Size '—'. The fourth row is 'Detection — C2 Multi-Host Beacons — 45.223.164.116' with Type 'Detection_record', Source 'System', TLP 'TLP:AMBER', Added By 'SYSTEM', Added At 'Aug 25, 2026 15:14', and Size '—'. The fifth row is 'Case Report (2026-08-25)' with Type 'Report', Source 'Analyst', TLP 'TLP:GREEN', Added By 'agent.soc+org_id_1@threatstream.com', Added At 'Aug 25, 2026 15:17', and Size '—'. The interface also includes a search bar, filters for Type and TLP, and a 'Add Evidence' button.

1 Title	2 Type	3 Source	4 TLP	5 Added By	6 Added At	7 Size
Alert AL-171614 — qa-ag53-alert-047e57cc	Alert_record	System	TLP:AMBER	SYSTEM	Aug 25, 2026 15:13	—
Detection — qa-ag53-det-3be34714	Detection_record	System	TLP:AMBER	SYSTEM	Aug 25, 2026 15:13	—
Alert AL-173128 — C2 Multi-Host Beacons — PROMOTE	Alert_record	System	TLP:AMBER	SYSTEM	Aug 25, 2026 15:14	—
Detection — C2 Multi-Host Beacons — 45.223.164.116	Detection_record	System	TLP:AMBER	SYSTEM	Aug 25, 2026 15:14	—
Case Report (2026-08-25)	Report	Analyst	TLP:GREEN	agent.soc+org_id_1@threatstream.com	Aug 25, 2026 15:17	—

The **Evidence Items** sub-tab lists all evidence files in the case. Each evidence item row contains the following information:

- 1 Title:** Filename shown below the title.
- 2 Type:** Colored badge such as Screenshot or Other.
- 3 Source:** Analyst for manual uploads, or the originating system name for system-generated items.
- 4 TLP:** Colored badges such as TLP:WHITE, TLP:GREEN, TLP:AMBER, or TLP:RED
- 5 Added By:** Email address of the user adding the evidence.
- 6 Added At:** Absolute timestamp of when the evidence was added
- 7 Size:** Total case storage capacity is 5 GB.

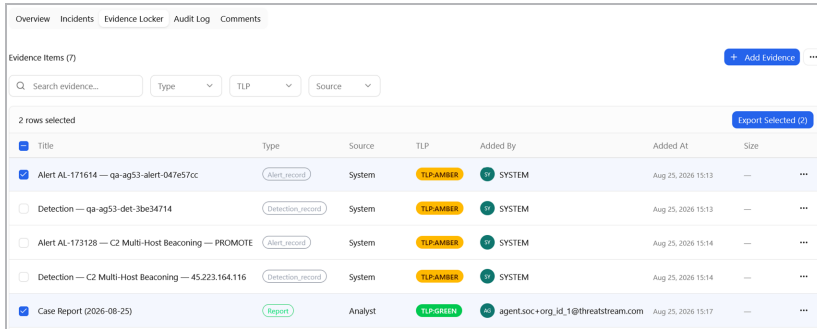
Click the more options menu (...) of the evidence item you are interested in and then click Download to download the evidence file if available.

Exporting Evidence

An evidence package export produces a TLP-filtered ZIP archive containing the selected files in their original format and a JSON manifest with item metadata and SHA-256 integrity hashes.

To generate a new export:

1. Select one or more evidence items.
2. Click **Export Selected (N)**, where N is the number of evidence items you are about to export.
3. Select the maximum TLP level for the export from the **Max TLP** drop-down list.
4. Click **Export** to finish the export.

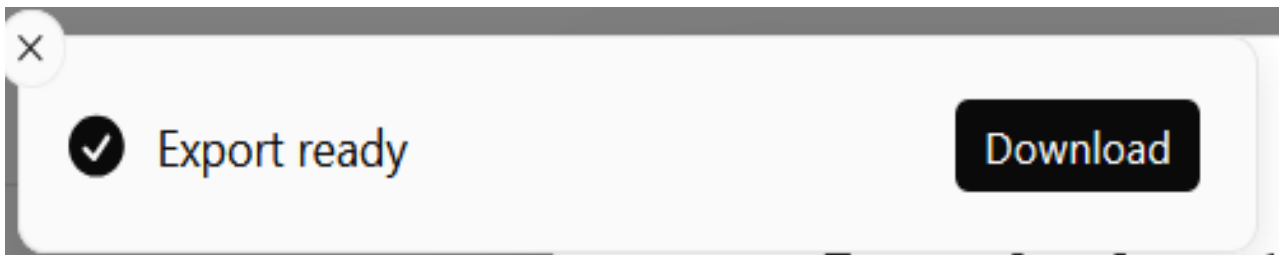


Evidence Items (7)						
Q Search evidence...						
Type TLP Source						
2 rows selected						
Title	Type	Source	TLP	Added By	Added At	Size
☒ Alert AL-171614 — qa-ag53-alert-047e57cc	Alert_record	System	TLP:AMBER	SYSTEM	Aug 25, 2026 15:13	—
☐ Detection — qa-ag53-det-3be34714	Detection_record	System	TLP:AMBER	SYSTEM	Aug 25, 2026 15:13	—
☐ Alert AL-173128 — C2 Multi-Host Beaconing — PROMOTE	Alert_record	System	TLP:AMBER	SYSTEM	Aug 25, 2026 15:14	—
☐ Detection — C2 Multi-Host Beaconing — 45.223.164.116	Detection_record	System	TLP:AMBER	SYSTEM	Aug 25, 2026 15:14	—
☒ Case Report (2026-08-25)	Report	Analyst	TLP:GREEN	agent.soc+org_id_1@threatstream.com	Aug 25, 2026 15:17	—



Note: Generating an evidence package export requires the Export Case Evidence permission. See [Managing Roles](#) for details.

Once the export is complete, click **Download** to start the download.



The following is an example screenshot of a JSON manifest from an export.

```
{
  "applied_tlp_filter": {
    "include_item_ids": [
      "258a32ae-fc01-4b8c-9795-165051218170",
      "e3f63771-e19e-4869-9baf-ebedf343d22e",
      "4ecd54da-db99-41c1-8afe-956992b353bb"
    ],
    "max_tlp": "AMBER"
  },
  "item_count": 2,
  "items": [
    {
      "added_at": "2026-08-25T22:15:01.783765+00:00",
      "added_by": "SYSTEM",
      "evidence_type": "ALERT_RECORD",
      "file_name": null,
      "file_size_bytes": null,
      "integrity_hash": "0604558e28cf15df2f3efc67ea4c8600bf253b6502c07ab13e48b8570872f457",
      "integrity_hash_algorithm": "SHA-256",
      "item_id": "258a32ae-fc01-4b8c-9795-165051218170",
      "source_layer": "ALERT",
      "source_record_id": "180641",
      "title": "Alert AL-173549 \u2014 C2 Multi-Host Beacons \u2014 PROMOTE",
      "tlp": "AMBER"
    },
    {
      "added_at": "2026-08-25T22:15:01.844343+00:00",
      "added_by": "SYSTEM",
      "evidence_type": "DETECTION_RECORD",
      "file_name": null,
      "file_size_bytes": null,
      "integrity_hash": "be87d20c97c0ac08afee397f5df6038b6ae6aee97b8cbd1db6cac3fcab74f686",
      "integrity_hash_algorithm": "SHA-256",
      "item_id": "e3f63771-e19e-4869-9baf-ebedf343d22e",
      "source_layer": "DETECTION",
      "source_record_id": "917031",
      "title": "Detection \u2014 C2 Multi-Host Beacons \u2014 45.223.164.116",
      "tlp": "GREEN"
    }
  ]
}
```

An export record itself is permanently logged in the Audit Log tab. See ["Audit Log Tab" on page 132](#) for details.

Using the Response Workbook

The **Response Workbook** is a structured incident response plan attached to every case. It organizes response tasks into four sequential incident response phases, tracks task completion, generates a Lessons Learned record,

On this page:

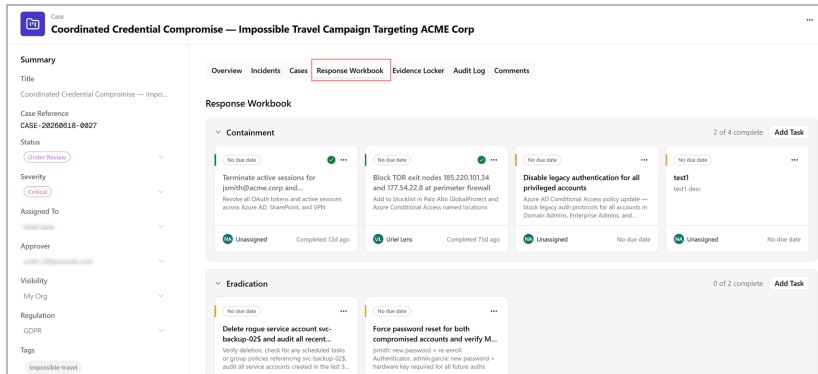
- ["Understanding Response Phases" on the next page](#)
- ["Adding Tasks" on the next page](#)
- ["Editing Tasks" on page 141](#)
- ["Tracking Task Progress" on page 142](#)

Related topics:

- ["Accessing the Case Full-Page View" on page 133](#)

and captures approver sign-off before the case is closed.

To access the Response Workbook, open the case of your interest in full-page view. See ["Accessing the Case Full-Page View" on page 133](#) for details.



Understanding Response Phases

The Response Workbook organizes tasks into four incident response phases:

1. **Containment** — actions taken to limit the spread or impact of the incident, for example, isolating affected systems or revoking compromised credentials.
2. **Eradication** — actions taken to remove the threat from the environment, for example, removing malware, patching vulnerabilities, or deleting unauthorized accounts.
3. **Recovery** — actions taken to restore normal operations, for example, restoring systems from backups or re-enabling services.
4. **Review & Close** — post-incident activities including lessons learned, stakeholder reporting, and case closure sign-off.

Each phase panel displays a header row with the phase name, a phase status label (such as Not Started, In Progress, or Complete), and a task counter in the N / N tasks format denoting completed / total tasks.

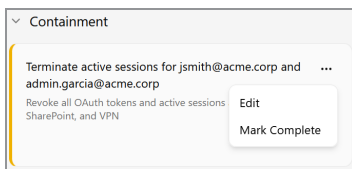
Adding Tasks

To add a task to a phase:

1. Click **Add Task** within the phase body.
2. In the **Add Task** dialog, complete the following fields:
 - **Title** (required) — a short description of the task.
 - **Description** (optional) — additional context for the task.
 - **Assignee** — the analyst responsible for completing the task.
 - **Target Asset** — the asset the task applies to. Search and select from available assets.
 - **Target Identity** — the identity the task applies to. Search and select from available identities.
 - **Due Date** — the date by which the task should be completed.
3. Click **Add Task**.

Tasks added by analysts appear in the phase with the Pending status.

Editing Tasks



To edit a task:

1. Click the more options menu (...) on the task card and select **Edit**.
2. In the **Edit Task** dialog box, update any of the following fields:
 - **Title** — the task name.
 - **Description** (optional) — additional context for the task.
 - **Status** — the current state of the task: Pending, In Progress, or Complete.
 - **Assignee** — the analyst responsible for completing the task.
 - **Target Asset** — the asset the task applies to.

- **Target Identity** — the identity the task applies to.
- **Due Date** — the date by which the task should be completed.

3. Click **Save**.

To mark a task complete without opening the edit dialog, click the more options menu (...) on the task card and select **Mark Complete**.

Tracking Task Progress

Task status is indicated by the border color of the task card: an orange card border implies the task is Pending, while a green card border implies the task is **Complete**.

Each phase header shows a task counter in the N / N tasks format (completed tasks / total tasks), so you can see phase-level progress at a glance without expanding individual tasks. Phase statuses are updated automatically as tasks are completed.

Managing Cases

You can take several actions to manage cases in your queue. You can assign cases to lead analysts, add tags for categorization, edit case metadata, export case packages, start cases when they are ready for investigation and move cases through their lifecycle.

Assigning Cases



Note: The Manage Cases permission is required to assign cases. See [Managing Roles](#) for details.

Assigning a case establishes the lead analyst responsible for investigating the case. You can change the assignee only for Open and Active cases.

You can assign cases for investigation in one of the following ways:

On this page:

- ["Assigning Cases" below](#)
- ["Adding Tags to Cases" on the next page](#)
- ["Editing Cases" on page 144](#)
- ["Exporting Cases" on page 145](#)
- ["Starting Cases" on page 146](#)
- ["Changing a Status of Cases" on page 147](#)

[Cases" on page 148](#)

[Case Details" on page 148](#)

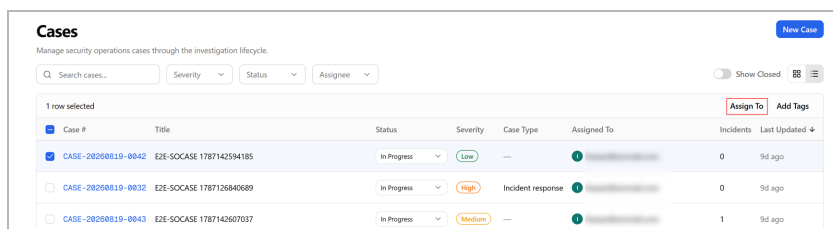
Related topics:

- ["Cases" on page 120](#)
- ["Creating a Case" on page 123](#)
- [Managing Access to Cases](#)
- ["Viewing Case Details" on page 125](#)

- From the Cases page (list view)
- From the Case Details panel/page

To assign a case from the Cases page (list view):

1. Navigate to **ThreatStream Next Gen > Security Operations > Cases**.
2. Switch to the Cases list view.
3. Select a case or more and click **Assign To**.



Case #	Title	Status	Severity	Case Type	Assigned To	Incidents	Last Updated
☒ CASE-20200819-0042	EZE-SOCASE 1787142594185	In Progress	Low	—	1	0	9d ago
☐ CASE-20200819-0032	EZE-SOCASE 1787126840689	In Progress	High	Incident response	1	0	9d ago
☐ CASE-20200819-0043	EZE-SOCASE 1787142607037	In Progress	Medium	—	1	1	9d ago

4. Select a user and click **Assign**.

The user is assigned to the selected cases.

To assign a case from the Case Details panel/page:

1. Navigate to **ThreatStream Next Gen > Security Operations > Cases**.
2. Locate the case of your interest and open its details panel of full-page view. See ["Viewing Case Details" on page 125](#) for details.
3. Select a user from the Assignee drop-down list.

The user is assigned to the case.

Adding Tags to Cases

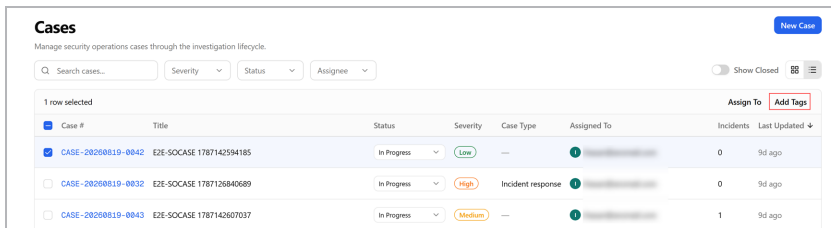


Note: The Manage Cases permission is required to add tags to cases. See [Managing Roles](#) for details.

You can add tags to cases to help you categorize and filter cases.

To add tags to cases:

1. Navigate to **ThreatStream Next Gen > Security Operations > Cases**.
2. Switch to the Cases list view.
3. Select one or more cases
4. Click **Add Tags**.



5. Select tags to be associated with the case.
6. The available tags are derived from the ThreatStream Preferred Tags list. See [Adding Preferred Tags to Intelligence](#) for more information. To create a custom tag, enter the desired tag value in the search field and click **+**. Repeat these steps to add additional tags.
7. Click **Add Tags**.

The tags are added to the selected cases.

Editing Cases



Note: The Manage Cases permission is required to edit cases. See [Managing Roles](#) for details.

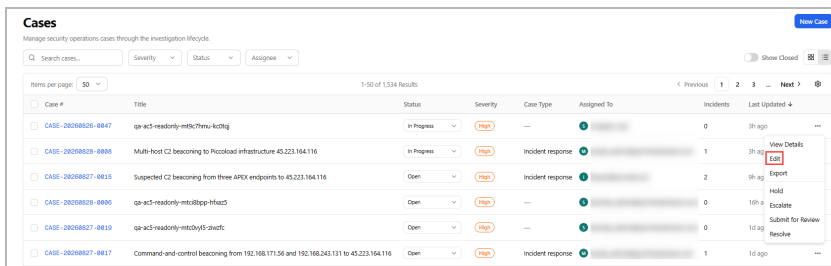
You can edit cases that are either in Open or Active status, in one of the following ways:

- From the Cases page (list view)
- From the Case Details panel/page

To edit a case from the Cases page:

1. Navigate to **ThreatStream Next Gen > Security Operations > Cases**.
2. Switch to the list view.

3. Click more options menu (...) of the case you want to edit and click **Edit**.



Case #	Title	Status	Severity	Case Type	Assigned To	Incidents	Last Updated
CASE-20090820-0847	qa-ac5-readonly-mitc/Phru-Achly	In Progress	High	---	---	0	3h ago
CASE-20090820-0808	Multi-host C2 beaconing to Piccolad infrastructure 45.223.164.116	In Progress	High	Incident response	---	1	3h ago
CASE-20090827-0815	Suspected C2 beaconing from three APEX endpoints to 45.223.164.116	Open	High	Incident response	---	2	5h ago
CASE-20090820-0805	qa-ac5-readonly-mitc/Phru-Achly	Open	High	---	---	0	10h ago
CASE-20090827-0810	qa-ac5-readonly-mitc/Phru-Achly	Open	High	---	---	0	1d ago
CASE-20090827-0817	Command and control beaconing from 192.168.171.56 and 192.168.243.131 to 45.223.164.116	Open	High	Incident response	---	1	1d ago

4. Update the case fields as needed. The changes are saved automatically.

To update a case from the Case Details panel/page:

1. Navigate to **ThreatStream Next Gen > Security Operations > Cases**.
2. Click the case you want to edit.
3. Update the case fields as needed.

The changes are saved automatically.

Exporting Cases



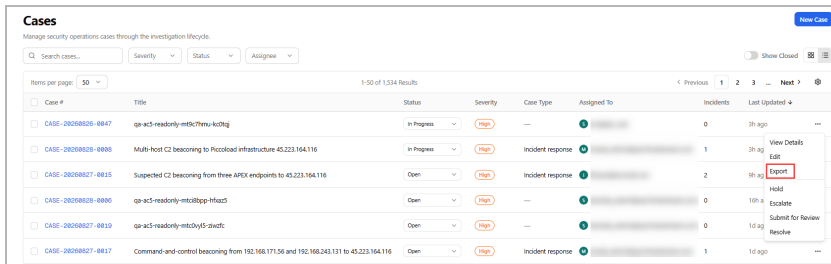
Note: The Export Cases permission is required to export cases. See [Managing Roles](#) for details.

You can export case details in a .zip file in one of the following ways:

- From the Cases page (list view)
- From the Case Details panel/page

To export a case from the Cases page (list view)

1. Navigate to **ThreatStream Next Gen > Security Operations > Cases**.
2. Switch to the list view.
3. Click the case more options menu (...) and then click **Export** to initiate the export.



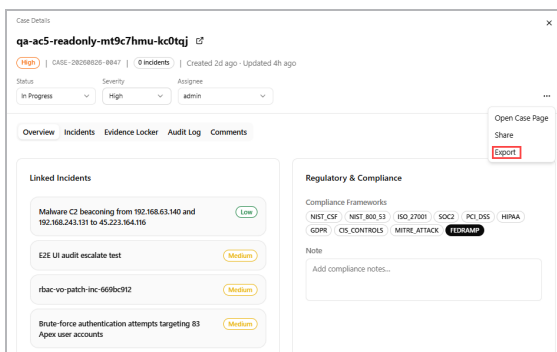
Case #	Title	Status	Severity	Case Type	Assigned To	Incidents	Last Updated
CASE-28098528-8847	qa-ac5-readonly-mt9c7hmu-kc0tqj	In Progress	High	---	[User]	0	3h ago
CASE-28098528-8888	MULTI-host C2 beaconing to PicoCloud infrastructure 45.223.164.116	In Progress	High	Incident response	[User]	1	3h ago
CASE-28098527-8815	Suspected C2 beaconing from three APEX endpoints to 45.223.164.116	Open	High	Incident response	[User]	2	5h ago
CASE-28098528-8885	qa-ac5-readonly-mt9c7hmu-kc0tqj	Open	High	---	[User]	0	10h ago
CASE-28098527-8819	qa-ac5-readonly-mt9c7hmu-kc0tqj	Open	High	---	[User]	0	1d ago
CASE-28098527-8817	Command-and-control beaconing from 192.168.171.56 and 192.168.243.131 to 45.223.164.116	Open	High	Incident response	[User]	1	1d ago

4. When the export is ready, click **Download** to download the exported files.

The download process starts immediately.

To export a case from the Case Details panel/page:

1. Navigate to **ThreatStream Next Gen > Security Operations > Cases**.
2. Click the case you want to edit.
3. On the Case Details panel/page, click the more options menu (...) and then click **Export** to initiate the export.



4. When the export is ready, click **Download** to download the exported files.

The download process starts immediately.

Starting Cases

A newly created case begins in the Open state, with the assignee being the user who created it.

To start a case:

1. Navigate to **ThreatStream Next Gen > Security Operations > Cases**.
2. Switch to the list view.
3. Click the more options menu (...) of the case you want to start.
4. Select **Start**.

The case status transitions to In Progress.

Changing a Status of Cases

A case moves through its lifecycle as work progresses: from **Open** to **Active** (sub-statuses: **In Progress**, **On Hold**, or **Escalated**), then to **Under Review** once submitted for approver sign-off, and finally to **Closed** once the approver approves.

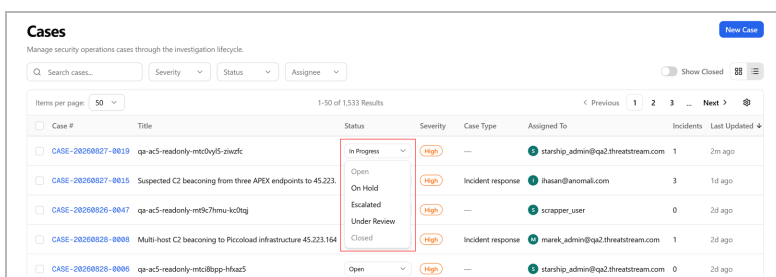
You can change the status of open and active cases from the Cases list view page or from the Case Details panel/page. For details on closing cases, see "[Closing Cases](#)" on page 149.

To change a case status from the Cases list view page:

1. Navigate to **ThreatStream Next Gen > Security Operations > Cases**.
2. Switch to the Cases list view and locate the case whose status you want to change.
3. Select the desired status from the case Status drop-down list.

If you select **On Hold** or **Escalate**, provide a reason for putting the case on hold and click **Confirm**.

If you select **Under Review**, verify that the case has an approver assigned to it and all incidents linked to the case are closed. See "[Submitting Cases for Review](#)" on page 149 for details.



Case #	Title	Status	Severity	Case Type	Assigned To	Incidents	Last Updated
CASE-20200827-0019	qa-ac5-readonly-mtc0y5-ziwdf	In Progress	High	—	starship_admin@qa2.threatstream.com	1	2m ago
CASE-20200827-0015	Suspected C2 beaconing from three APEX endpoints to 45.223.164	Open	High	Incident response	hasan@anomali.com	3	1d ago
CASE-20200826-0047	qa-ac5-readonly-mtc0y5-ziwdf	On Hold	High	—	scrapper_user	0	2d ago
CASE-20200828-0000	Multi-host C2 beaconing to Piccoload infrastructure 45.223.164	Escalated	High	—	—	0	2d ago
CASE-20200828-0000	Multi-host C2 beaconing to Piccoload infrastructure 45.223.164	Under Review	High	Incident response	marek_admin@qa2.threatstream.com	1	2d ago
CASE-20200828-0000	qa-ac5-readonly-mtc0y5-ziwdf	Closed	High	—	—	0	2d ago
CASE-20200828-0000	qa-ac5-readonly-mtc0y5-ziwdf	Open	High	—	starship_admin@qa2.threatstream.com	0	2d ago

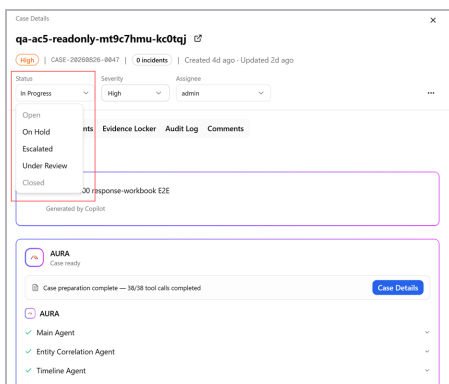
The case status is updated.

To change a case status from the Case Details panel/page:

1. Navigate to **ThreatStream Next Gen > Security Operations > Cases**.
2. Open the Case Details panel or full-page view. See [Viewing Agent Details](#) for details.

If you select **On Hold** or **Escalate**, provide a reason for putting the case on hold and click **Confirm**.

If you select **Under Review**, verify that the case has an approver assigned to it and all incidents linked to the case are closed. See ["Submitting Cases for Review" on the next page](#) for details.



3. Select the available status from the Status drop-down list.

The case status is updated.

Closing Cases

Closing a case marks the investigation complete and makes the case read-only. Closure requires an assigned approver to review and sign off on the investigation before the case can transition to Closed.

See ["Closing Cases" on the next page](#) for more information on the full closure workflow, including approver assignment, the review process, and reopening a closed case.

Viewing Case Details

See ["Viewing Case Details" on page 125](#) for details on the case slide-over panel and full-page view.

Closing Cases

Closing a case in Anomali Agentic SOC Operations is a two-step workflow:

- Case owner submits the case for review
- Assigned approver then approves or returns it

Once approved, the case transitions to the Closed status and becomes read-only. A closure record is created automatically and is accessible from the Closure Record tab on the full-page Case view.

On this page:

- ["Submitting Cases for Review" below](#)
- ["Approving or Returning Cases" on the next page](#)
- ["Reopening Closed Cases" on page 151](#)

Related topics:

- ["Cases" on page 120](#)
- ["Managing Access to Cases" on page 142](#)
- ["Viewing Case Details" on page 125](#)

Submitting Cases for Review



Note: You must have the Resolve Case permission to submit cases for a review. See [Managing Roles](#) for details on permissions.

When an investigation is complete, the case owner assigns an approver and submits the case for review. The case transitions to **Under Review** and the approver is notified.

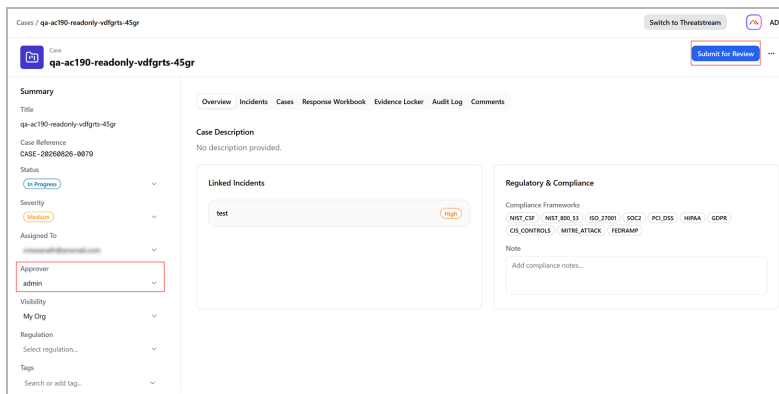
To submit a case for review:

1. Navigate to **ThreatStream Next Gen > Security Operations > Cases**.
2. From the tile view, click the case and click the Open in New Tab () icon to open the case in full page in a new tab. Alternatively, switch to the Cases list view and then click the case name to open the case in full page.
3. Select an approver from the Approver drop-down list on the left pane.



Note: The approver must have the Approve Case Closure permission. See [Managing Roles](#) for details on permissions.

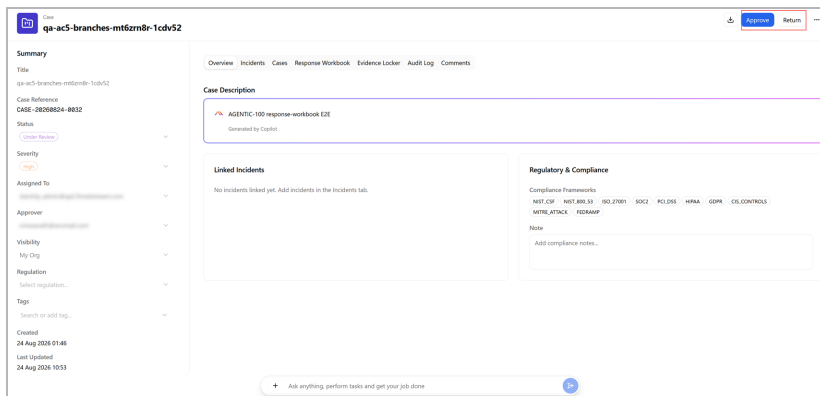
4. Click **Submit for Review** in the top-right corner of the page.



The case status changes to Under Review. The assigned approver can now approve or return the case.

Approving or Returning Cases

When a case is submitted for review, the assigned approver can see the **Approve** and **Return** buttons in the top-right corner of the case full-page view.



To approve and close a case:

1. Navigate to **ThreatStream Next Gen > Security Operations > Cases**.
2. Open the full-page view of the case you want to approve and close.
3. Click **Approve**.
4. In the confirmation dialog, click **Approve & Close**.

The case transitions to the Closed status and becomes read-only. A Closure Record is created under the Closure Record case tab.

To return a case to the Active status:

1. Navigate to **ThreatStream Next Gen > Security Operations > Cases**.
2. Open the full-page view of the case you want to return to the Active status.
3. Click **Return**.
4. In the Return this case? dialog, enter a note explaining what needs to be addressed. This field is required.
5. Click **Return to Active**.

The case returns to its previous Active sub-state (In Progress, On Hold, or Escalated) and the case assignee is notified.

Reopening Closed Cases

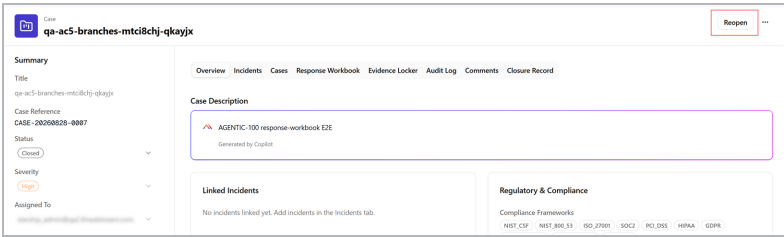


Note: The Manage Cases permission is required to reopen cases. See [Managing Roles](#) for details.

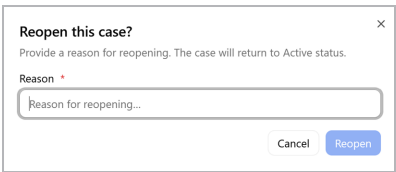
Reopening a case returns it to the Active status and preserves the existing closure record.

To reopen a closed case:

1. Navigate to **ThreatStream Next Gen > Security Operations > Cases**.
2. Enable the **Show Closed** toggle in the top-right corner to display closed cases.
3. Locate the closed case you want to re-open and open it in the full-page view. See ["Accessing the Case Full-Page View" on page 133](#) for details.
4. Click **Reopen** in the top-right corner of the page.



5. In the Reopen this case? dialog, enter a reason for reopening. This field is required.



6. Click **Reopen**.

The case returns to Active status. The closure record from the previous closure is preserved in the Closure Record tab.

Chapter 5: Integrations Marketplace

This topic covers the following sections:

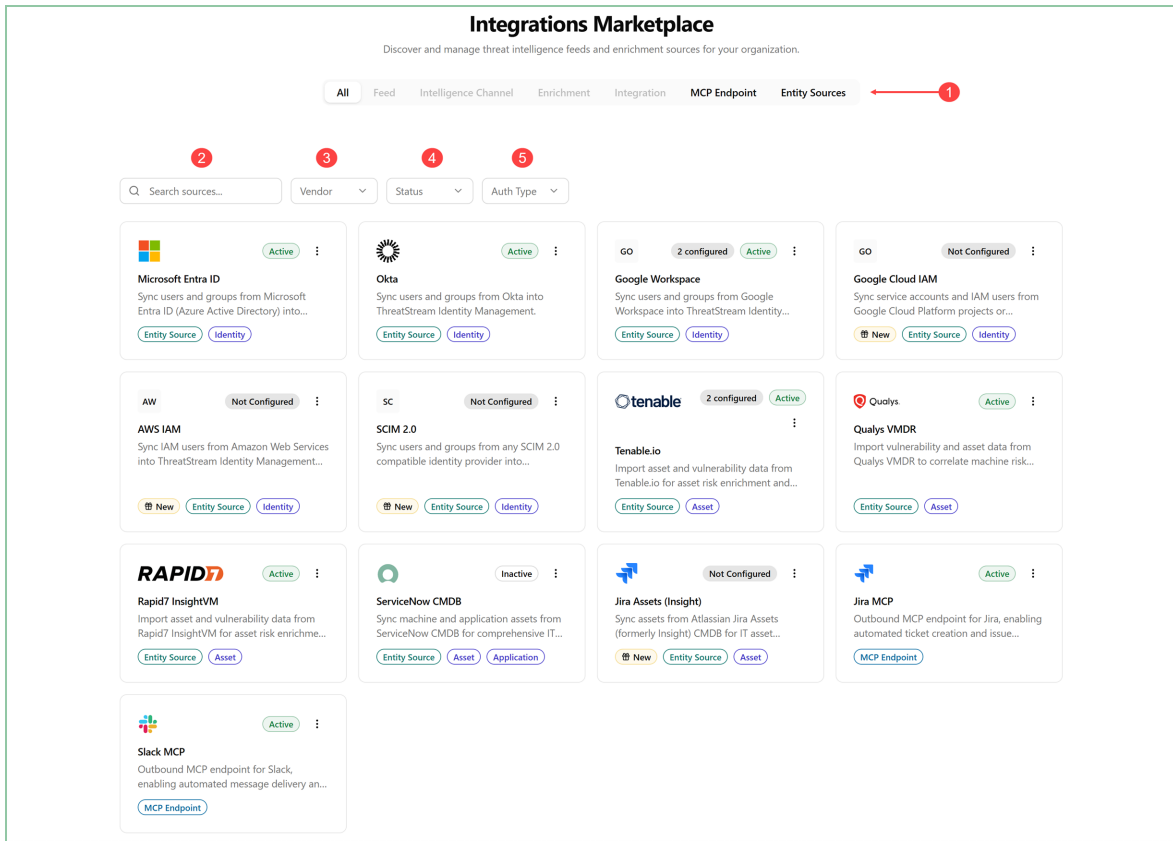
Jira MCP Integration	156
Slack MCP Integration	157

Integrations Marketplace is your one-stop place for managing all types of ThreatStream Next Gen integrations.

They include:

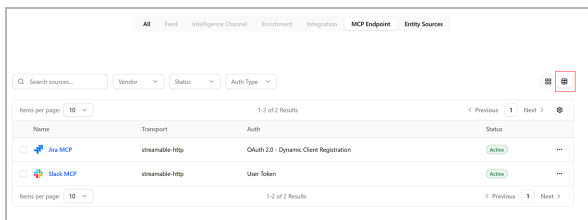
- [MCP Endpoint](#)
- [Entity Sources](#)
- Feeds (coming soon)
- Intelligence channels (coming soon)
- Enrichments (coming soon)
- Direct integrations (coming soon)

To access Integration Marketplace, navigate to **ThreatStream NextGen > Integrations Marketplace**.



1 Integration Types. Click any available tab to filter integrations by their integration type.

On every integration type page, you can switch to the list view. The list view also gives you access to the integration actions menu. See [Managing Entity Source Integrations](#) for details.



2 Search sources: Search integrations by their name.

3 Vendor: Filter integrations by a vendor's name.

4 Status: Filter integrations by their status—Not Configured, Active, or Inactive.

5 Auth Type: Filter integrations by their authentication type—Bearer Token or OAuth.

Jira MCP Integration

You can integrate **Jira MCP** with ThreatStream Next Gen to automatically create Jira tickets based on PIR findings and notify specified Jira users about them.

Configuring Jira MCP Integration

To start using Jira MCP in ThreatStream Next Gen, you need to configure the Jira MCP integration on the Integrations Marketplace.

Before You Begin

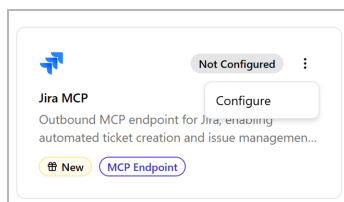
Before configuring the Jira MCP integration, you must add the following domain to the list of Atlassian supported domains to allow ThreatStream Next Gen to access Jira.

- https://api.threatstream.com/** (for US Cloud)
- https://api-eu.threatstream.com/** (for EU Cloud)

See [Control Atlassian Rovo MCP Server Settings/Add domains](#) for details.

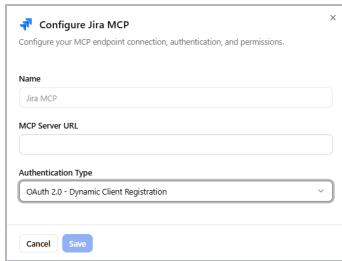
To configure Jira MCP integration:

1. Navigate to **ThreatStream Next Gen > Integrations Marketplace**.
2. Locate the **Jira MCP** tile.
3. Click the three-dot vertical menu and then click **Configure**. The Configure Jira MCP dialog box opens.



4. Provide a **Name** for the Jira MCP integration.
5. Enter the **MCP Server URL**:
`https://mcp.atlassian.com/v1/mcp`
6. Select **OAuth 2.0 - Dynamic Client Registration** as the **Authentication Type**.
7. Enter your **Client ID** and **Client Secret** from the Atlassian developer console.

8. Click **Save**.



The Jira MCP integration is now configured and ready for use.

You can now configure your PIRs to create Jira tickets. For details on enabling Jira integration in PIRs, see ["Configuring Jira Output" on page 225](#).

Slack MCP Integration

You can integrate **Slack MCP** with ThreatStream Next Gen to send PIR updates and results directly to Slack channels and direct messages. This allows you to share intelligence, notify stakeholders, and keep teams aligned without leaving ThreatStream Next Gen.

Activating Slack MCP Integration

To start using Slack integration in ThreatStream Next Gen, you need to activate the Slack MCP Endpoint integration on the **Integrations Marketplace** page.

Before You Begin

Before configuring Slack MCP integration, you must:

1. Navigate to <https://api.slack.com/apps> and create an OAuth app from scratch to authenticate to the remote MCP server from Threatstream Next Gen. For details, see [Creating an app](#).
2. After creating an app, add the following permission scopes to your app:
 - `search:read.public`
 - `search:read.private`
 - `users:read`
 - `chat:write`

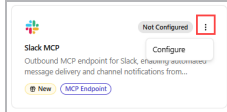
3. Add the following MCP server URL to your app configuration:
 - https://api.threatstream.com/api/v1/mcp_integration/oauth_callback/ (US Cloud)
 - https://api-eu.threatstream.com/api/v1/mcp_integration/oauth_callback/ (EU Cloud)
4. Generate a User OAuth Token.
Note that a Bot User OAuth Token will not work. If a User OAuth Token is not available, you must reinstall the app to generate a User OAuth Token.



Note: If you plan to use the OAuth 2.0 method of authentication, copy and save Client ID and Client Secret for the app you created.

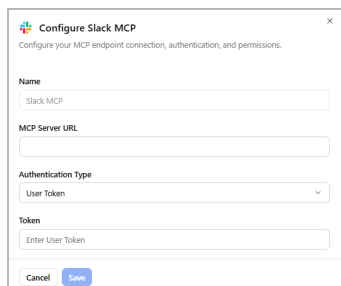
To configure Slack MCP integration:

1. Navigate to **ThreatStream Next Gen > Integrations Marketplace**.
2. Locate the **Slack MCP** tile.
3. Click the three-dot vertical menu and then click **Configure**.



4. Provide a Slack MCP **Name**.
5. Enter the **MCP Server URL**:
<https://mcp.slack.com/v1>
6. Select an **Authentication Type**— **User Token** or **OAuth 2.0 - Manual Client Registration**.
7. Enter one of the following:
 - If you selected User Token as your authentication type, enter your user OAuth token.
 - If you selected OAuth 2.0 - Manual Client Registration as your authentication type, enter your **Client ID** and **Client Secret**.

8. Click **Save**.



The screenshot shows a dialog box titled "Configure Slack MCP" with a close button (X) in the top right corner. Below the title is a subtitle: "Configure your MCP endpoint connection, authentication, and permissions." The dialog contains four input fields: "Name" (with "Slack MCP" entered), "MCP Server URL" (empty), "Authentication Type" (a dropdown menu with "User Token" selected), and "Token" (with "Enter User Token" as a placeholder). At the bottom left are "Cancel" and "Save" buttons.

The Slack MCP Integration is configured and is now ready for use. You can now configure your PIRs to send their results to public Slack channels or direct messages. For details on enabling Slack integration in PIRs, see ["Configuring Slack Output" on page 227](#).

Chapter 6: Entity Management

- Understanding Entities and Peer Groups 160
- Entity Sources 161
- Risk Score Modifiers 162
- Managing Entities and Groups 162
- Identities 163
- Assets 178
- Peer Groups 191
- Entity Risk Scores 199
- Entity Summary Widgets 204

Entities and Peer Groups are the foundation for understanding who and what is in your environment. It provides a centralized view of every identity and asset the platform monitors—the people, accounts, and systems that make up your organization’s security operations workflow. The platform pulls entity data from connected external systems, monitors entities for suspicious activity, and calculates a risk score for each one. Peer groups and risk score modifiers provide the organizational context that makes those scores meaningful.

Understanding Entities and Peer Groups

An entity is any identity or asset that the Anomali platform monitors and scores. There are two entity types:

- **Identities** include human and non-human accounts in your organization: users, contractors, and service accounts. Each identity is displayed with attributes such as username, email address, the groups it belongs to, and its current risk score.
- **Assets** include the devices across your environment: computers, mobile devices, routers, servers, and other infrastructure. Each asset is displayed with attributes such as host name and MAC address.

Each entity has a risk score that reflects the detections triggered against it. The risk score is adjusted by any risk score modifiers applied to the entity or its peer groups. Each entity also has a detail view that shows the current score and its contributing factors, associated detections, related entities, and a history of attribute changes.

A **peer group** is a collection of entities that share a common role, function, or access level. Peer groups provide critical context for risk scoring by allowing a Risk Score Multiplier to be applied to a set of entities as a group. Groups can be imported from a connected identity provider such as Active Directory or Okta among several others, or created manually within the platform. A risk modifier between 0.1 and 2.0 is associated with each group, where 1.0 is neutral. Groups are hierarchical: a parent group can contain child groups, allowing a multiplier to be set at a broad level with more specific overrides applied below. An entity can belong to more than one group; when it does, its effective multiplier is the average across all groups it belongs to.



Note: Peer group membership for identity-provider-sourced groups is managed in the source system and reflected in the platform on the next sync cycle.

Entity Sources

Entity data is brought into the platform through Entity Sources, accessible from the Integrations Marketplace, or imported manually via CSV. See [Entity Sources](#) for details.

These sources perform an initial full sync of records from the source system and keep that data current through scheduled incremental syncs. The sources fall into two categories:

- **Identity sources** import user accounts and group memberships from identity providers. Supported sources include Microsoft Entra ID, Okta, AWS IAM, Google Cloud IAM, Google Workspace, SCIM 2.0.
- **Asset sources** import device and infrastructure records from vulnerability management and IT service management systems. Supported sources include ServiceNow CMDB, Qualys VMDR, Tenable, and Rapid7 InsightVM. Jira Assets is also supported as a combined source.

Configuring a Source

Sources are configured from the **Entity Sources** tab of the Integrations Marketplace. Each configuration requires:

- Credentials for the source system
- Field mappings from source attributes to Anomali fields

- A sync frequency (15 minutes to daily)

A **Test Connection** check validates the credentials before saving. Multiple independent configurations of the same connector type are supported—for example, two separate Okta tenants can each be configured independently.

Sync Behavior

On first activation, a source performs a full sync. Subsequent runs are incremental. Organization Administrators can trigger a sync on demand. If an entity is removed or disabled in the source system, its status is set to **Disabled** rather than deleted, preserving its detection history for investigation.



Note: Configuring or triggering a source sync requires the Manage Entities permission. Users with only the View Entities permission can see source status and record counts but cannot configure or trigger syncs. For details, see [Managing Roles](#).

Risk Score Modifiers

Entities and Groups provides two configurable modifiers that allow users with the Manage Entities permission to adjust risk scoring to reflect their organizational context. Both modifiers accept values from 0.1 to 2.0 and default to 1.0, which applies no adjustment to the underlying score.

- **Peer Group Risk Score Multiplier** is configured at the group level. For entities that belong to more than one group, the multiplier is applied as a weighted average across all groups. Use this modifier to increase scoring sensitivity for groups such as privileged accounts, or to reduce it for groups where expected routine activity would otherwise produce frequent detections.
- **Entity Risk Override** is configured at the individual entity level and applied after all group multipliers have been calculated. Use this modifier when a specific entity requires a different sensitivity setting than the rest of its peer group—for example, a user account that has been temporarily granted elevated access.

Managing Entities and Groups

Entities and Groups is accessible from the main navigation bar of the Anomali Agentic SOC Operations. It provides two primary management areas:

- **Entities** displays a summary of entities by type and risk level, followed by a searchable and filterable list of all entity records. Users with the Manage Entities permission can create manual entity records, import entities from a CSV file, and open individual entity detail views. For details, see [Managing Roles](#).
- **Peer Groups** displays all configured peer groups, including groups sourced from a connected identity provider and groups created manually in the platform. Users with the Manage Entities permission can create and manage groups, set the Risk Score Multiplier for each group, and view group membership and hierarchy. For details, see [Managing Roles](#).

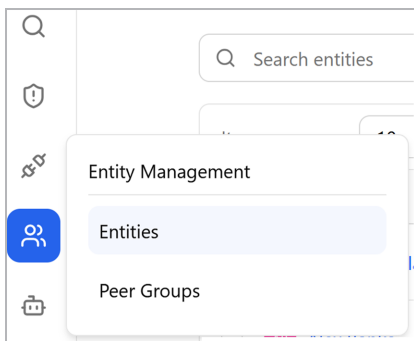
Identities

The **Identities** page lists all identity entities that Anomali Agentic SOC Operations has consolidated from your connected identity providers. Each entry displays the identity risk score, source, group memberships, and status, giving your team a complete view of every monitored identity in your organization.

Accessing Identities

To access Identities:

1. On the left navigation bar, click **Entity Management > Entities**.
2. On the **Entities** page, click the **Identities** tab.



Understanding the Identities List

The Identities list displays all identity entities in your organization. Use the search field and filters to narrow results. Click an identity name to open its details.

The screenshot shows the 'Identities' tab in the Anomali ThreatStream Next Gen interface. At the top, there are filters for Search entities (1), Source (2), Risk Score (3), Group (4), and Status (5). A 'Add Identity' button (14) is in the top right. Below the filters, a table lists identities with columns: Username (6), Email (7), Department (8), Groups (9), Risk Score (10), Source (11), Status (12), and Last Seen (13). The table shows 1-10 of 304 results. The first six rows of data are visible, each with a checkbox, a profile icon, a username, an email address, a department, groups, a risk score, source, status, and last seen date.

	Username	Email	Department	Groups	Risk Score	Source	Status	Last Seen
☐	Ashraf Abdelazim	[redacted]	—	EMEA Sales Enablement Field Sal...	+2	google_workspace	Active	1 year ago
☐	Alex Banks	[redacted]	—	-		google_workspace	Active	4 months ago
☐	Andres Bermudez	[redacted]	—	Anomali Match Team Company	+1	google_workspace	Active	7 days ago
☐	Adam Caldwell	[redacted]	—	Communications (Mark... ISAC Info	+4	google_workspace	Active	12 days ago
☐	Adrian Carlos	[redacted]	—	-		google_workspace	Active	6 days ago
☐	Al Curitana	[redacted]	—	-		google_workspace	Active	5 days ago

- 1 **Search Entities:** Filter the identities list by name. Results update as you type.
- 2 **Source:** Filter the list by the identity provider the identity was ingested from.
- 3 **Risk Score:** Filter the list by risk score range.
- 4 **Group:** Filter the list by peer group membership.
- 5 **Status:** Filter the list by identity status. Possible values are **Active** and **Inactive**.
- 6 **Username:** The display name of the identity. Click a username to open the Identity Details panel. See "[Viewing Identity Details](#)" on page 166.
- 7 **Email:** The primary email address associated with the identity.
- 8 **Department:** The organizational department the identity belongs to, as synced from the identity provider.
- 9 **Groups:** The peer groups this identity belongs to. If the identity belongs to more than one group, additional groups are indicated with a count.
- 10 **Risk Score:** The current risk score for the identity, calculated from detections in a rolling 24-hour window. See "[Entity Risk Scores](#)" on page 199.
- 11 **Source:** The identity provider the record was ingested from, such as Google Workspace or Azure AD.
- 12 **Status:** The current status of the identity record. Possible values are **Active** and **Inactive**.
- 13 **Last Seen:** The time elapsed since the identity was last observed in a detection or activity event, and not considered for risk scoring. last_seen reflects when the

connector last observed the entity (when the IDP or scanner reports the entity), and not when a detection fired against it.

14 Add Identity: Opens the form to manually add a new identity. See ["Adding an Identity" on page 170](#).

Click the **View Settings** gear icon () in the pagination bar to customize the table. The View Settings panel lets you toggle column visibility, drag columns to reorder them, and reset the layout to defaults with **Reset View**. Use the **Density** toggle to switch between **Default** and **Compact** row height.

Understanding Identity Permissions

Users with the Manage Entities permission can change individual risk overrides, change group multipliers, add, edit, or remove entities, and add or remove entities from peer groups.

Action	Permission Required
View the identities list and identity details	View Entities
Export identity data	
Add an identity manually or through CSV import	Manage Entities
Edit an identity record	
Merge identity records	
Set or change an entity risk override	
Add or remove identities from peer groups	

See [Managing Roles](#) for more information on how roles and permissions work.

Understanding Identity Details

The Identity Details panel gives you a complete view of a single monitored identity, including its current risk score on a 0–100 scale, active detections within the current 24-hour window, profile fields, aliases, and peer group memberships. Reviewing the Risk Score tab shows how peer group multipliers and any configured overrides contribute to the final score. See ["Viewing Identity Details" on the next page](#).

Adding an Identity

Each identity record represents a single user or account monitored by Anomali Agent SOC Operations. You can create identities either manually, one at a time, or

import them in bulk at once through a CSV file. See ["Adding an Identity" on page 170](#).

Managing Existing Identities

Use bulk actions to apply risk overrides, assign identities to peer groups, or export records for multiple selected identities at once. Each row also has an options menu that lets you view details, edit, or remove a single identity without a bulk selection. See ["Managing Identities" on page 176](#).

Viewing Identity Details

The Identity Details panel provides a complete profile of a single identity entity, including its current risk score, active detections, field-level details, aliases, group memberships, and activity history. To open it, click any identity name in the ["Identities" on page 163](#) list.

All the identity data is organized across the following tabs:

- ["Overview Tab" below](#)
- ["Risk Score Tab" on page 168](#)
- ["Detections Tab" on page 169](#)
- ["History Tab" on page 170](#)

Overview Tab

The Overview tab summarizes the risk posture of an identity and displays its profile fields.

The screenshot displays the 'Identity Details' interface for a user named Ashraf Abdelazim. At the top, the user's name is shown with a link icon, and the 'Current Risk Score' is 0. Below this, there are tabs for 'Overview', 'Risk Score', 'Detections', and 'History'. The 'Overview' tab is active, showing two summary cards: 'Risk Score' (0) and 'Detections' (0). The 'Details' section follows, listing various identity fields in a two-column layout. The 'Aliases' section lists alternate identifiers like email addresses, usernames, and UPNs. At the bottom, there is a 'Group Memberships' section.

Details	
Display Name	Job Title
Ashraf Abdelazim	-
Primary Identifier Type	Primary Identifier
Email	[Redacted]
Department	Manager
-	-
Employee ID	Status
-	Active
Last Login	Source
5 Mar 2025 20:22	google_workspace

Aliases

Field	Value
Email(s)	[Redacted]
Usernames	[Redacted]
UPN(s)	[Redacted]

Group Memberships

The top of the tab shows two summary cards: **Risk Score**, the current score of the identity on a 0–100 scale, and **Detections**, the number of active detections within the rolling 24-hour window.

The **Details** section lists the identity profile fields as synced from the source identity provider:

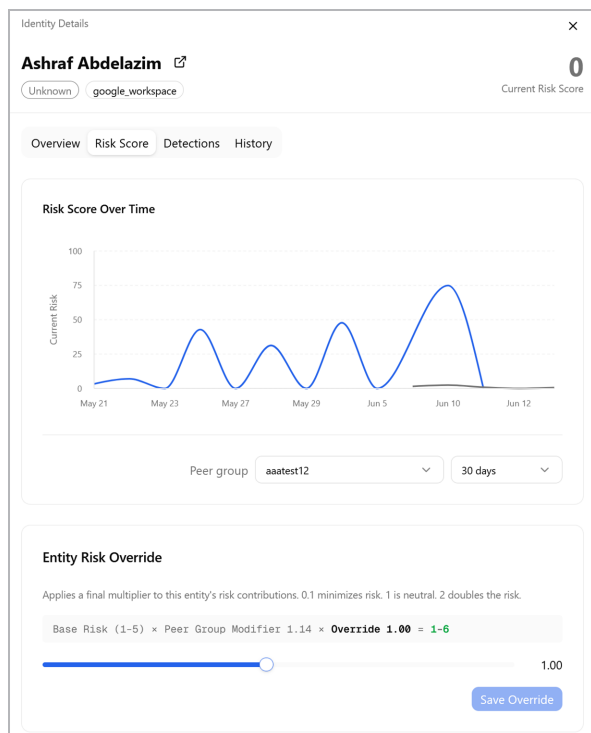
- **Display Name** and **Job Title**
- **Primary Identifier Type** (for example, Email) and **Primary Identifier**
- **Department** and **Manager**
- **Employee ID** and **Status**
- **Last Login** and **Source**

The **Aliases** section lists all known alternate identifiers for this identity, including email addresses, usernames, and User Principal Names (UPNs) across connected sources.

The **Group Memberships** section lists the peer groups this identity belongs to. Each entry displays the group name, the source system the group was synchronized from (for example, `google_workspace`), and the current risk score multiplier of the group (for example, $\times 1.0$). Group memberships determine which peer group risk multipliers apply to the score for this identity. See ["Peer Groups" on page 191](#) for more information.

Risk Score Tab

The **Risk Score** tab shows the score history of the identity and provides controls to configure its entity risk override.



Risk Score Over Time

The Risk Score Over Time chart plots the current risk score of the identity across a selected time period. Use the **Peer group** drop-down to view how scoring varies by group context, and the time period drop-down to adjust the chart window, ranging anywhere between 7–180 days.

Entity Risk Override

The Entity Risk Override section applies a final multiplier to the risk contributions of the identity. The override range is 0.1 to 2.0, where 0.1 minimizes risk, 1.0 is the

default and represents neutral risk, and 2.0 doubles the risk.



Note: Changing the override requires the **Manage Entities** permission (`can_entities_manage`). Viewing the identity detail page, including its risk score and override value, requires **View Entities** (`can_entities_view`) or higher.

The following formula shows how the override compounds with the base risk and peer group modifier:

Base Risk (1–5) × Peer Group Modifier × Override = Result.

Adjust the slider to the desired value and click **Save Override** to apply.

See ["Entity Risk Score Override" on page 202](#) for more information.

Detections Tab

The Detections tab lists all active detections associated with this identity within the current 24-hour window.

Asset Details

rafael.mccoy

73.53
Current Risk Score

High

Overview Risk Score **Detections** History

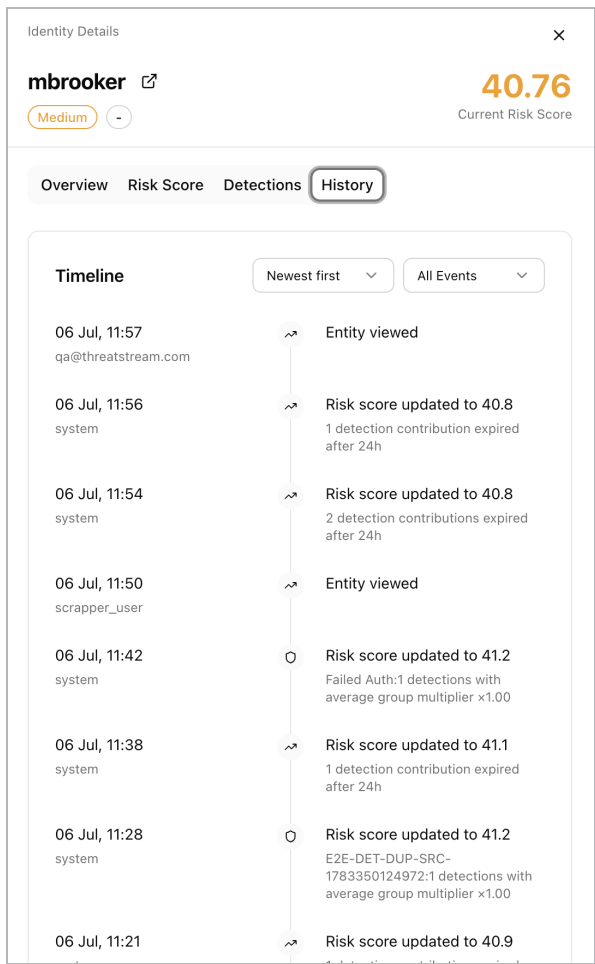
Recent Detections

Rule Name	Category	Date	Severity
qa_detection_rule_test	detection	6 Jul 2026	Medium
iocmatch_ocsf_batch_2606b570f9986d0e	iocmatch_ocsf	6 Jul 2026	Low
iocmatch_ocsf_batch_ed333e050056fafa	iocmatch_ocsf	6 Jul 2026	Low

Each detection card in the **Recent Detections** list displays the **Rule Name** that produced the detection, the detection **severity** (for example, Low, Medium, High), its **Category** (for example, iocmatch), and the **Date** the detection was recorded. Detections expire from this list 24 hours after they are produced. See ["Entity Risk Scores" on page 199](#).

History Tab

The History tab provides a chronological record of all events and changes associated with this identity.



The **Timeline** lists events in reverse chronological order by default. Use the sort dropdown to switch between **Newest first** and **Oldest first**.

Use the event type filter to narrow results: **All Events**, **Actions**, or **Detections**. Each entry shows the timestamp, the user or system that generated the event, and the event description.

Adding an Identity

You can add identities to Anomali Agentic SOC Operations either manually or in bulk by importing a CSV file. Identities synced automatically from connected identity providers do not require manual entry.



Note: Adding an identity, whether manually or through CSV import, requires the Manage Entities permission. For details, see [Managing Roles](#).

To add a new identity:

1. On the left navigation bar, click **Entity Management > Entities > Identities**.
2. On the "[Identities](#)" on page 163 page, click **Add Identity**.
3. Click either the **Manual** or **CSV Import** tabs.

Adding an Identity Manually

The **Manual** tab lets you register a single identity by entering its details directly.

Add New Identity

×

Register identities individually or import via CSV.

Manual

CSV Import

Display Name *

e.g. Jane Doe

Primary Identifier Type *

Select identifier type

▼

Primary Identifier *

Please select an Identifier Type first

Employee ID

e.g. EMP-1201

Department

e.g. Engineering

Job Title

e.g. Senior Engineer

Account Type

Select account type

▼

Account Status

Select account status

▼

Tags

Add tag...

▼

Cancel

Add Identity

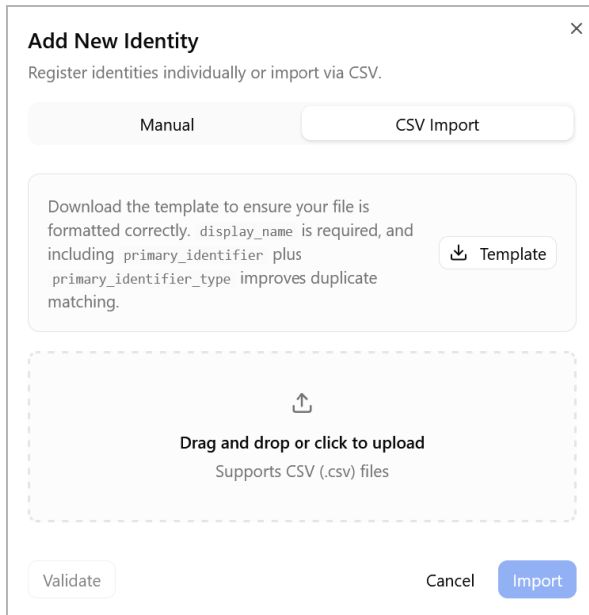
Field	Description
Display Name *	The full name used to identify this identity in Anomali Agentic SOC Operations.
Primary Identifier Type *	The type of the primary identifier for this identity, such as email or username.
Primary Identifier *	The unique identifier value matching the selected type, for example, an email address. This field becomes active after a Primary Identifier Type is selected.
Employee ID	(Optional) The internal employee identifier assigned by the organization.
Department	(Optional) The organizational department to which this identity belongs.
Job Title	(Optional) The job title for this identity within the organization.
Account Type	(Optional) The type of account, such as employee or service account.
Account Status	(Optional) The current status of the account.
Tags	(Optional) Labels to categorize or organize this identity.
Aliases - Email(s)	(Optional) Additional email addresses associated with this identity, comma-separated.
Aliases - Usernames	(Optional) Additional usernames associated with this identity, comma-separated.
Aliases - UPNs	(Optional) User Principal Names associated with this identity, comma-separated.

Click **Add Identity** to save, or **Cancel** to discard.

Before creating the record, the system checks for potential duplicates. If a match is found, it is flagged by the **Potential Identity Conflict** dialog. See "[Resolving Identity Conflicts](#)" on page 175 for more information.

Adding Identities through CSV

The **CSV Import** tab lets you register multiple identities at once by uploading a formatted CSV file.



The screenshot shows a dialog box titled "Add New Identity" with a close button (X) in the top right corner. Below the title, it says "Register identities individually or import via CSV." There are two tabs: "Manual" and "CSV Import", with "CSV Import" being the active tab. Below the tabs, there is a text box that says: "Download the template to ensure your file is formatted correctly. `display_name` is required, and including `primary_identifier` plus `primary_identifier_type` improves duplicate matching." To the right of this text is a button labeled "Template" with a download icon. Below this is a large dashed box representing the upload area. Inside the dashed box is an upward arrow icon and the text: "Drag and drop or click to upload" and "Supports CSV (.csv) files". At the bottom of the dialog, there are three buttons: "Validate", "Cancel", and "Import".

To import identities through CSV:

1. Click **Template** to download the CSV template. The template includes all supported column headers.
 - a. **display_name** is required in every row.
 - b. Including **primary_identifier** and **primary_identifier_type** improves duplicate detection during import.
2. Populate the template with your identity data. Supported columns are:
`display_name`, `primary_identifier`, `primary_identifier_type`, `department`, `job_title`, `employment_type`, `identity_category`, `cost_center`, `risk_sensitivity`, `is_privileged`, `privilege_level`, `status`, `given_name`, `surname`, `employee_id`
3. Drag and drop your completed CSV file onto the upload area, or click to browse and upload the file.
4. Click **Validate** to check the file for formatting errors before importing. The **Validation Results** dialog reviews every row without committing any records.

See ["Validating Identities" below](#) for more information.

- 5. Click **Import** to complete the import, or **Cancel** to discard.

Validating Identities

When you click **Validate**, the platform validates the uploaded files and presents its evaluation in the **Validation Results** dialog, without committing any records to the system.

Add New Identity

Register identities individually or import via CSV.

Manual

CSV Import

Download the template to ensure your file is formatted correctly. `display_name` is required, and including `primary_identifier` plus `primary_identifier_type` improves duplicate matching.

Template

Drag and drop or click to upload

Supports CSV (.csv) files

identity-new-updated-one.csv 283 B

1 data rows detected.

1 Ready

0 Warnings

0 Errors

View Details

Validate

Cancel

Import

A summary bar shows the total count for each outcome: **Ready**, **Warnings**, and **Errors**. Clicking **View Details** displays a table with one row per CSV row.

Validation Results

1 row validated. Review issues and resolve conflicts before importing.

1 Ready

0 Warnings

0 Errors

Status	Display Name	Primary Identifier	Identifier Type	Issue
Ready	Ashraf	ashraf@ashraf.com	email	---

Items per page: 100

1-1 of 1 Results

< Previous 1 Next >

Close

Here, the **Status** column shows one of three values:

- **Ready**—the row passed validation and will import without issues.
- **Warning**—the row has a non-blocking issue. The record will still import, but review the **Issue** column for details.
- **Error**—the row has a blocking issue and will not be imported. Correct the source file and re-upload to resolve.

Click **Close** to return to the CSV Import tab.

Resolving Identity Conflicts

When you submit a new identity, whether manually or through CSV, the system checks whether any existing identity matches on the **Display Name**, **Primary Identifier**, or any alias fields such as **Email**, **Username**, or **UPN**.

Matching is cross-field: for example, if an incoming primary identifier matches an existing email alias, a conflict is still detected. If a match is found, the **Potential Identity Conflict** dialog appears before the record is created.

Potential Identity Conflict [X]

A matching identity already exists. Merge or create new?

Matched on: primary_identifier, email

Field	Existing	Incoming	Merge
Primary Identifier	[redacted]	[redacted]	☐
Email(s)	[redacted]	[redacted]	☐

Cancel Create New Merge

Potential Identity Conflict [X]

A matching identity already exists. Merge or create new?

Matched on: primary_identifier, display_name, email

Incoming	Merged
[redacted]	[redacted]
Arav Soni	Arav Soni
[redacted]	[redacted]

Cancel Create New Merge

The dialog displays the **Matched on:** field that identifies the fields that triggered the conflict, for example, `primary_identifier` or `email`. It also includes a comparison table with three columns:

- **Existing:** Values on the record already in the system.
- **Incoming:** Values from the record you are adding.

- **Merged:** Auto-resolved result of combining both records. For single-value fields such as **Primary Identifier**, the value of the existing record takes precedence. For multi-value fields such as **Email(s)**, all unique values from both records are combined into a single list.

Choose one of the following actions:

- **Merge:** Combines the two records into a single canonical identity. All unique identifier values from both records are preserved as aliases. The merge is logged in the history of the identity.
- **Create New:** Creates the incoming record as a separate identity without merging, even though a potential duplicate exists.
- **Cancel:** Closes the dialog and returns you to the form without creating any record.

Managing Identities

The **Identities** list provides bulk actions for managing one or more identities at once. Select one or more rows using the checkboxes to reveal the available actions in the toolbar.



Note: Setting overrides, adding identities to peer groups, editing, and removing identities require the Manage Entities permission. Exporting identities requires either View Entities or Manage Entities. For details, see [Managing Roles](#).

Q Search entities					Source	Risk Score	Group	Status	Add Identity			
1 row selected										Set Override	Add to Group	Export
☒	Username	Email	Department	Groups	Risk Score	Source	Status	Last Seen				
☐	 Anar Sani	[REDACTED]	---	qa_test_group, fx		google_workspace	Active	Just now		...		
☐	 Anja Lynch	[REDACTED]	---	-		google_workspace	Active	18 hours ago		...		
☐	 Satyaji Roy	[REDACTED]	---	-		google_workspace	Active	Just now		...		
☐	 TestUser	[REDACTED]	---	TestCustomSubgroup		---	Active	---		...		
☐	 Saeid Ahmad	[REDACTED]	---	-		google_workspace	Active	9 hours ago		...		
☒	 Ashraf Abdelazim	[REDACTED]	---	EMEA Sales Enablement Field Sal... +2		google_workspace	Active	1 year ago		...		

Setting a Risk Override

Use **Set Override** to apply a risk override multiplier to the selected identities. The override range is 0.1 to 2.0, where 1.0 is neutral. This action applies the same override value to all selected identities in a single operation.

To set a risk override:

1. On the left navigation bar, click **Entity Management > Entities > Identities**.
2. Select one or more identities.
3. Click **Set Override** in the toolbar.
4. Set the override value and confirm.

See ["Entity Risk Score Override" on page 202](#) for more information on how risk scoring and overrides work.

Adding Identities to a Peer Group

Use **Add to Group** to assign the selected identities to one or more peer groups. Group membership determines which risk multipliers apply to the score for an identity.

To add identities to a peer group:

1. On the left navigation bar, click **Entity Management > Entities > Identities**.
2. Select one or more identities.
3. Click **Add to Group** in the toolbar.
4. Search for and select the peer group, then confirm.

See ["Peer Groups" on page 191](#) for more information.

Exporting Identities

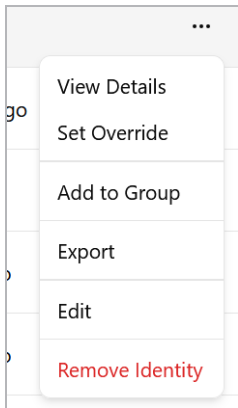
Use **Export** to download the selected identity records.

To export identities:

1. On the left navigation bar, click **Entity Management > Entities > Identities**.
2. Select one or more identities.
3. Click **Export** in the toolbar.

Taking Individual Identity Actions

Each identity row has an options menu (...) that provides actions for that specific identity without requiring a selection.



The options menu includes the following actions:

- **View Details**—opens the **Identity Detail** side panel. See ["Viewing Identity Details" on page 166](#) for more information.
- **Set Override**—applies a risk override multiplier to this identity. See ["Entity Risk Score Override" on page 202](#) for more information.
- **Add to Group**—assigns this identity to a peer group. See ["Peer Groups" on page 191](#) for more information.
- **Export**—downloads the identity record.
- **Edit**—opens the identity form to modify its details.
- **Remove Identity**—permanently removes the identity from the platform.

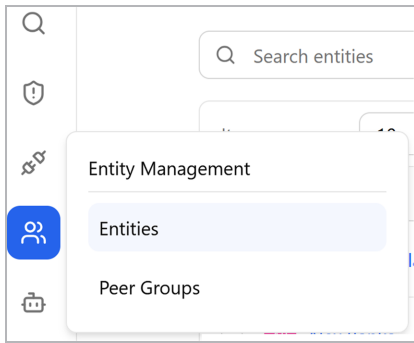
Assets

The **Assets** page lists all asset entities that Anomali Agentic SOC Operations has consolidated from your connected asset management systems and data sources. Each entry displays the asset risk score, source, group memberships, and status, giving your team a complete view of every monitored asset in your organization.

Accessing Assets

To access Assets:

1. On the left navigation bar, click **Entity Management > Entities**.
2. On the **Entities** page, click the **Assets** tab.



Understanding the Assets List

The Assets list displays all asset entities in your organization. Use the search field and filters to narrow results. Click an asset hostname to open its details.

A screenshot of the 'Assets' list interface. At the top, there's a search bar and several filter buttons: Source, Risk Score, Group, Status, Owner, and OS. Below these are pagination controls and a table of assets. The table has columns for Hostname, MAC Address, Platform, Owner, Tags, Risk Score, Source, and Last Seen. The first row shows an asset named 'manual-test' with a MAC address '01:02:03:00'. The second row shows 'Linux Kernel 2.6'. The third and fourth rows also show 'Linux Kernel 2.6'. The table is paginated, showing 1-10 of 256,103 results. Numbered callouts (1-15) point to various UI elements: 1. Search assets, 2. Source filter, 3. Risk Score filter, 4. Group filter, 5. Status filter, 6. Owner filter, 7. OS filter, 8. Hostname column, 9. MAC Address column, 10. Platform column, 11. Owner column, 12. Tags column, 13. Risk Score column, 14. Source column, 15. Last Seen column.

1 Search Assets: Filter the assets list by hostname, IP address, or MAC address. Results update as you type.

2 Source: Filter the list by the data source the asset was ingested from, for example, EDR, CMDB, or Tenable.

3 Risk Score: Filter the list by risk level. Possible values are **Critical** (75–100), **High** (50–74), **Medium** (25–49), and **Low** (0–24).

4 Group: Filter the list by peer group membership.

5 Status: Filter the list by asset status. Possible values are **Active** and **Inactive**.

6 Owner / OS: Filter the list by assigned owner or by operating system platform.

7 Hostname: The primary identifier for the asset. Click a hostname to open the Asset Details panel. See ["Viewing Asset Details" on page 181](#) for more information.

8 Hostname: The primary identifier for the asset. Click a hostname to open the Asset Details panel. See ["Viewing Asset Details" on page 181](#) for more information.

- 9 MAC Address:** The hardware MAC address of the asset.
- 10 Platform:** The operating system or platform of the asset, for example, Windows 11 Pro or Ubuntu 22.04 LTS.
- 11 Owner:** The individual or team assigned as responsible for this asset.
- 12 Tags:** Labels assigned to the asset for categorization or search.
- 13 Risk Score:** The current risk score for the asset, calculated from detections in a rolling 24-hour window. See ["Entity Risk Scores" on page 199](#) for more information.
- 14 Source:** The data source the asset record was ingested from.
- 15 Last Seen:** The time elapsed since the asset was last observed in a detection or activity event.

To export all assets matching the current filters, click the more options menu () to the right of the **Add Asset** button, then select **Export Assets**. The export downloads the full current result set based on applied filters.

Click the **View Settings** gear icon () in the pagination bar to customize the table. The View Settings panel lets you toggle column visibility, drag columns to reorder them, and reset the layout to defaults with **Reset View**. Use the **Density** toggle to switch between **Default** and **Compact** row height.

Understanding Asset Details

The Asset Details panel gives you a complete view of a single monitored asset, including its current risk score on a 0–100 scale, active detections within the current 24-hour window, profile fields, and peer group memberships.

Reviewing the Risk Score tab shows how peer group multipliers and any configured overrides contribute to the final score.

See ["Viewing Asset Details" on the next page](#) for more information.

Understanding Asset Permissions

Users with the Manage Entities permission can add, edit, or remove assets, set or change risk overrides, and add or remove assets from peer groups. Users with only the View Entities permission can view the assets list, asset details, and export asset data.

Action	Permission Required
View the assets list and asset details	View Entities
Export asset data	
Add an asset manually	Manage Entities
Edit an asset record	
Merge asset records	
Set or change an asset risk override	
Add or remove assets from peer groups	

For details on assigning these permissions to a role, see [Managing Roles](#).

Adding an Asset

Each asset record represents a single endpoint, device, or other resource monitored by Anomali Agentic SOC Operations. You can create assets manually one at a time. See ["Adding an Asset" on page 185](#) for more information.

Managing Existing Assets

Use bulk actions to apply risk overrides, assign assets to peer groups, or export records for multiple selected assets at once. Each row also has an options menu that lets you view details, edit, or remove a single asset without a bulk selection. See ["Managing Assets" on page 189](#) for more information.

Viewing Asset Details

The Asset Details panel provides a complete profile of a single asset entity, including its current risk score, active detections, field-level details, group memberships, and activity history. To open it, click any asset hostname in the ["Assets" on page 178](#) list.

The panel header displays the asset hostname, status, source, and current risk score.

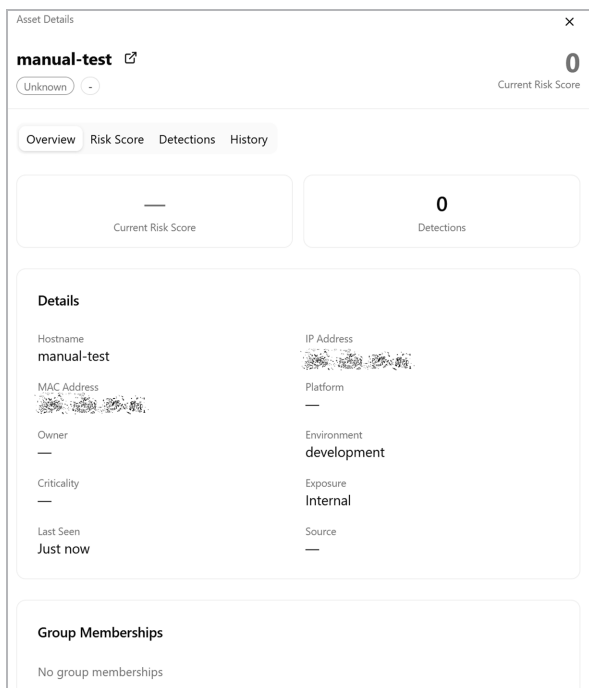
When opened in full-page mode, a summary panel on the left displays key fields: **Hostname**, **Asset Type**, **OS**, **Environment**, **Risk Level**, **Source**, **Status**, and **Last Seen**.

All the asset data is organize across the following tabs:

- "Overview Tab" below
- "Risk Score Tab" on the next page
- "Detections Tab" on page 184
- "History Tab" on page 185

Overview Tab

The Overview tab summarizes the risk posture of an asset and displays its profile fields.



The top of the tab shows two summary cards: **Risk Score**, the current score of the asset on a 0–100 scale, and **Detections**, the number of active detections within the rolling 24-hour window.

The **Details** section lists the asset profile fields:

- **Hostname** and **IP Address**
- **MAC Address** and **Platform**
- **Owner** and **Environment**

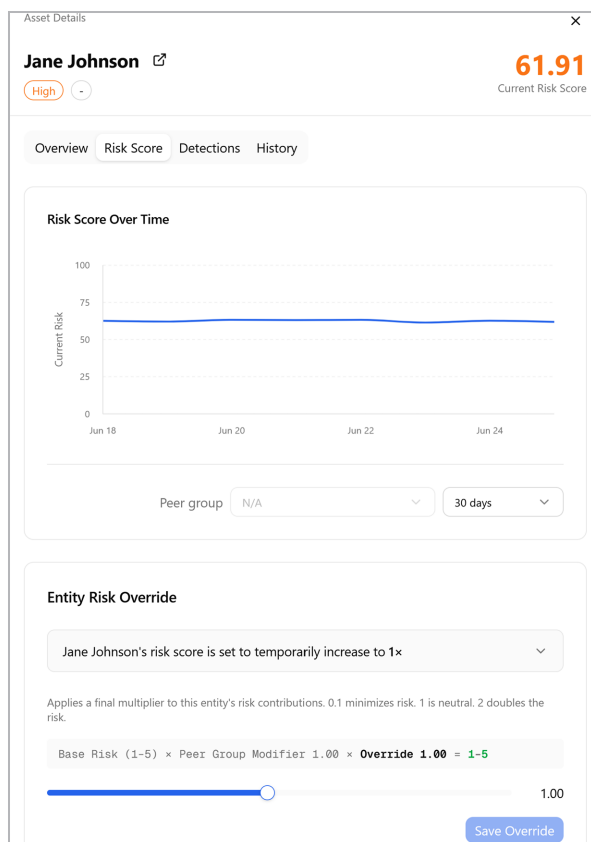
- **Criticality** and **Exposure**
- **Last Seen** and **Source**

The **Group Memberships** section lists the peer groups to which this asset belongs. Each entry displays the group name, the source system from which the group was synchronized, and the current risk score multiplier of the group (for example, $\times 1.0$). Group memberships determine which peer group risk multipliers apply to the score for this asset.

See ["Peer Groups" on page 191](#) for more information.

Risk Score Tab

The **Risk Score** tab shows the score history of the asset and provides controls to configure its entity risk override.



Risk Score Over Time

The Risk Score Over Time chart plots the current risk score of the asset across a selected time period. Use the **Peer group** drop-down to view how scoring varies in a group context, and the time period drop-down to adjust the chart window, for example, **30 days**.

Entity Risk Override

The Entity Risk Override section applies a final multiplier to the risk contributions of the asset. The override range is 0.1 to 2.0, where 0.1 minimizes risk, 1.0 is the default and indicates neutral risk, and 2.0 doubles the risk.



Note: Changing the override requires the **Manage Entities** permission. Viewing the asset detail page, including its risk score and override value, requires **View Entities** or higher.

The following formula displayed shows how the override compounds with the base risk and peer group modifier:

Base Risk (1–5) × Peer Group Modifier × Override = Result.

Adjust the slider to the desired value and click **Save Override** to apply.

See ["Entity Risk Score Override" on page 202](#) for more information.

Detections Tab

The Detections tab lists all active detections associated with this asset within the current 24-hour window.

The screenshot shows the 'Asset Details' page for 'Jane Johnson'. At the top right, the 'Current Risk Score' is 61.91. Below the name, there's a 'High' risk indicator. The 'Detections' tab is selected, showing a list of 'Recent Detections'. Each detection card includes the 'Rule Name', 'Category', 'Date', and 'Severity' (Low).

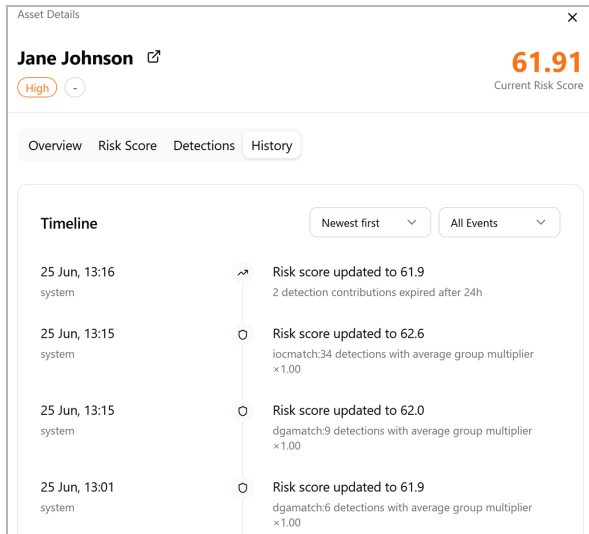
Rule Name	Category	Date	Severity
iocmatch_batch_2b1c0de8a6fe844d	iocmatch	25 Jun 2026	Low
dgamatch_batch_080b0ed2869dbada	dgamatch	25 Jun 2026	Low
dgamatch_batch_744d442cca0d27a6	dgamatch	25 Jun 2026	Low

Each detection card in the **Recent Detections** list displays the **Rule Name** that fired the detection, the detection **severity** (for example, Low, Medium, High), its **Category**, and the **Date** the detection was recorded. Detections expire from this list 24 hours after they fire.

See ["Entity Risk Scores" on page 199](#) for more information.

History Tab

The History tab provides a chronological record of all events and changes associated with this asset.



The **Timeline** lists events in reverse chronological order by default. Use the sort drop-down to switch between **Newest first** and **Oldest first**.

Use the event type filter to narrow results: **All Events**, **Actions**, or **Detections**. Each entry shows the timestamp, the user or system that generated the event, and the event description.

Adding an Asset



Note: Adding an asset, whether manually or through CSV import, requires the Manage Entities permission. For details, see [Managing Roles](#).

You can add assets to the platform either manually or in bulk by importing a CSV file. Assets synced automatically from connected asset management systems and data sources do not require manual entry.

To open add a new asset:

1. On the ["Assets" on page 178](#) page, click **Add Asset**.
2. Click either the **Manual** or **CSV Import** tabs.

Adding an Asset Manually

The **Manual** tab lets you register a single asset by entering its details directly.

Add Asset

Register assets individually or import via CSV.

Manual

CSV Import

Hostname *

e.g. WKSTN-ENG-099

IP Address

e.g. 10.0.0.5

MAC Address

XXXXXXXXXXXX

Asset Type

Select type

Environment

Select environment

Cancel

Add Asset

Field	Description
Hostname *	The primary identifier for this asset, for example, WKS-NYC-001.
IP Address	(Optional) The IPv4 or IPv6 address of the asset.
MAC Address	(Optional) The hardware MAC address of the asset.
Platform	(Optional) The operating system or platform of the asset, for example, Windows 11 Pro or Ubuntu 22.04 LTS.
Asset Type	(Optional) The classification of the asset, for example, Workstation, Laptop, Server, or OT Device.
Owner	(Optional) The individual or team assigned as responsible for this asset.
Environment	(Optional) The deployment environment of the asset, for example, Production or Development.
Criticality	(Optional) The business criticality rating of the asset, for example, Critical, High, Medium, or Low.
Exposure	(Optional) The network exposure classification of the asset, for example, Air-gapped, Internal, or Internet-facing.

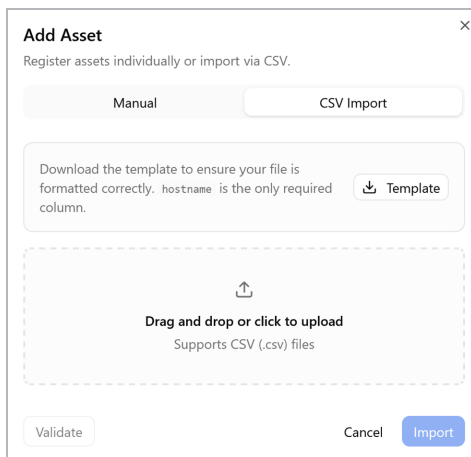
Field	Description
Business Unit	(Optional) The name of the business organizational unit, for example, Engineering, HR, or Marketing.
Tags	(Optional) Labels to categorize or organize this asset.

Click **Add Asset** to save, or **Cancel** to discard.

Before creating the record, the system checks for potential duplicates. If a match is found on Hostname, IP Address, or MAC Address, the system displays the **Potential Asset Conflict** dialog. See ["Resolving Asset Conflicts" on page 189](#) for more information.

Adding Assets through CSV

The **CSV Import** tab lets you register multiple assets at once by uploading a formatted CSV file.



The screenshot shows a modal window titled "Add Asset" with a close button (X) in the top right corner. Below the title is the instruction "Register assets individually or import via CSV." There are two tabs: "Manual" and "CSV Import", with "CSV Import" being the active tab. Below the tabs, there is a text box that says "Download the template to ensure your file is formatted correctly. hostname is the only required column." and a button labeled "Template" with a download icon. Below this is a large dashed box containing an upload icon and the text "Drag and drop or click to upload" and "Supports CSV (.csv) files". At the bottom of the dialog are three buttons: "Validate", "Cancel", and "Import".

To import assets through CSV:

1. Click **Template** to download the CSV template. The template includes all supported column headers.
 - a. **hostname** is required in every row.
 - b. Including **ip_address** and **mac_address** improves duplicate detection during import.
2. Populate the template with your asset data. Supported columns are:

```
hostname, ip_address, mac_address, platform, asset_type, owner,
environment, criticality, exposure, tags
```

3. Drag and drop your completed CSV file onto the upload area, or click to browse and upload the file.
4. Click **Validate** to check the file for formatting errors before importing. The **Validation Results** dialog reviews every row without committing any records. See ["Validating Assets" below](#) for more information.
5. Click **Import** to complete the import, or **Cancel** to discard.

Validating Assets

When you click **Validate**, the platform validates the uploaded file and presents its evaluation in the **Validation Results** dialog, without committing any records to the system.

Add Asset ×

Register assets individually or import via CSV.

Manual **CSV Import**

Download the template to ensure your file is formatted correctly. hostname is the only required column. [Template](#)

Drag and drop or click to upload
Supports CSV (.csv) files

my-new-asset.csv 704 B

1 data rows detected.

0 Ready 1 Warnings 0 Errors [View Details](#)

Validate **Cancel** **Import**

A summary bar shows the total count for each outcome: **Ready**, **Warnings**, and **Errors**. Clicking **View Details** displays a table with one row per CSV row.

Validation Results ×

1 row validated. Review issues and resolve conflicts before importing.

0 Ready 1 Warnings 0 Errors

Status	Hostname	IP	MAC Address	Type	Issue
Warning	webserver01	192.168.1.1	08:00:27:00:00:00	server	Matched on scanner key

Items per page: 100 1-1 of 1 Results < Previous 1 Next >

Close

The **Status** column shows one of three values:

- **Ready**—the row passed validation and will import without issues.
- **Warning**—the row has a non-blocking issue. The record will still import, but review the **Issue** column for details.
- **Error**—the row has a blocking issue and will not be imported. Correct the source file and re-upload to resolve.

Click **Close** to return to the CSV Import tab.

Resolving Asset Conflicts

When you submit a new asset, the system checks whether any existing asset matches on the Hostname, IP Address, or MAC Address fields. If a match is found, the **Potential Asset Conflict** dialog appears before the record is created.

The dialog includes a comparison table with three columns:

- **Existing:** Values on the record already in the system.
- **Incoming:** Values from the record you are adding.
- **Merged:** Auto-resolved result of combining both records. For single-value fields, the value from the existing record takes precedence.

Choose one of the following actions:

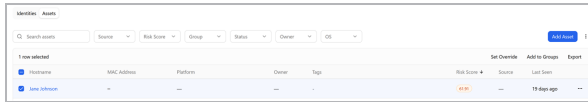
- **Merge:** Combine the two records into a single canonical asset. All unique identifier values from both records are preserved. The merge is logged in the history of the asset.
- **Create New:** Creates the incoming record as a separate asset without merging, even though a potential duplicate exists.
- **Cancel:** Closes the dialog and returns you to the form without creating any record.

Managing Assets



Note: Setting overrides, adding assets to peer groups, editing, and removing assets all require the Manage Entities permission. Exporting assets requires either View Entities or Manage Entities. For details, see [Managing Roles](#).

The Assets list provides bulk actions for managing one or more assets at once. Select one or more rows using the checkboxes to reveal the available actions in the toolbar.



Setting a Risk Override

Use **Set Override** to apply a risk override multiplier to the selected assets. The override range is 0.1 to 2.0, where 1.0 is neutral. This action applies the same override value to all selected assets in a single operation.

To set a risk override:

1. On the left navigation bar, click **Entity Management > Entities > Assets**.
2. Select one or more assets.
3. Click **Set Override** in the toolbar.
4. Set the override value and confirm.

See ["Entity Risk Score Override" on page 202](#) for more information on how risk scoring and overrides work.

Adding Assets to a Peer Group

Use **Add to Group** to assign the selected assets to one or more peer groups. Group membership determines which risk multipliers apply to the score for an asset.

To add assets to a peer group:

1. On the left navigation bar, click **Entity Management > Entities > Assets**.
2. Select one or more assets.
3. Click **Add to Group** in the toolbar.
4. Search for and select the peer group, then confirm.

See ["Peer Groups" on the next page](#) for more information.

Exporting Assets

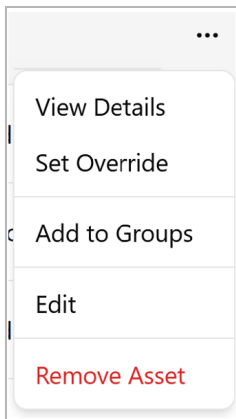
Use **Export** to download the selected asset records.

To export assets:

1. On the left navigation bar, click **Entity Management > Entities > Assets**.
2. Select one or more assets.
3. Click **Export** in the toolbar.

Taking Individual Asset Actions

Each asset row has an options menu (...) that provides actions for that specific asset without requiring a selection.



The options menu includes the following actions:

- **View Details**—opens the **Asset Detail** side panel. See "[Viewing Asset Details](#)" on page 181 for more information.
- **Set Override**—applies a risk override multiplier to this asset. See "[Entity Risk Score Override](#)" on page 202 for more information.
- **Add to Group**—assigns this asset to a peer group. See "[Peer Groups](#)" below for more information.
- **Export**—downloads the asset record.
- **Edit**—opens the asset form to modify its details.
- **Remove Asset**—permanently removes the asset from the platform.

Peer Groups

Peer groups are logical collections of entities, identities and assets, that share common characteristics, permissions, or organizational attributes.

In Anomali Agentic SOC Operations, peer groups serve two purposes:

- **Organizational Context:** Each group carries a Risk Score Multiplier that contributes to the weighted average peer group modifier applied during risk calculation for all member entities. Assigning appropriate multipliers allows your team to encode organizational context directly into the scoring engine: a detection for a privileged administrator carries materially different risk weight than the same detection for a read-only service account. See ["Entity Risk Scores" on page 199](#) for details on how multipliers factor into the formula.
- **Risk Comparison:** Peer groups provide a basis for comparison in the Risk Score tab of each entity detail page, allowing administrators to plot an entity risk score against its peers in the group and, therefore, better understand whether an elevated entity score reflects a genuine outlier or a pattern shared across the group.

Group Types

Anomali Agentic SOC Operations supports two group types:

- **IDP-sourced groups:** Synchronized from an external identity or asset management system, for example, Active Directory, Okta, or a CMDB. Membership is managed at the source and is read-only within the platform. Administrators can configure the Risk Score Multiplier for any IDP-sourced group.
- **Custom groups:** Created and managed directly within Anomali Agentic SOC Operations. Both the membership and the Risk Score Multiplier are fully configurable. Custom groups are visually distinguished with a **Custom** badge in all list and detail views. See ["Creating Custom Peer Groups" on page 196](#) for more information.

Group Hierarchy

Peer groups support parent-child relationships. Hierarchies are visible in the **Peer Group** list panel, where child groups are indented beneath their parent and can be expanded or collapsed. Additionally, custom groups can be configured as subgroups of both custom and IDP-sourced groups.

Risk Score Multiplier

Every group has a Risk Score Multiplier with a range of 0.1 to 2.0 and a default value of 1.0 (neutral). Values above 1.0 increase the risk contribution of detections for all member entities, whereas values below 1.0 reduce it. When an entity belongs to multiple groups, the system calculates the weighted arithmetic mean of all applicable group multipliers as the peer group modifier for that entity.

Multiplier changes take effect on the next risk calculation cycle for all member entities, so all member entities will have their scores recomputed using the updated multiplier on the next cycle based on the updated risk calculation. All changes are recorded in the audit log with the previous value, new value, timestamp, and administrator identity.

Accessing Peer Groups

To access **Peer Groups**, on the left navigation bar, click **Peer Groups**. See ["Understanding Peer Groups" below](#) for a detailed description of the interface.

Permissions

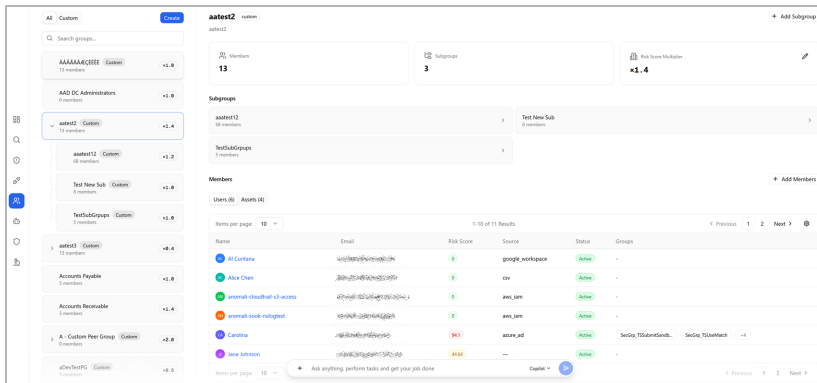
Access to peer groups is governed by the same two permissions that apply to all entity management. There is no per-group sharing, that is, a permission grants access to all peer groups in the organization, or none of them.

Action	Permission Required
View peer groups and group membership	View Entities
Set or change a Risk Score Multiplier	Manage Entities
Create a custom peer group	
Edit or delete a custom peer group	
Add or remove entities from a custom group	

For details on assigning these permissions to a role, see [Managing Roles](#).

Understanding Peer Groups

The **Peer Groups** page lists all groups in your organization in a scrollable panel on the left. Selecting a group displays its details on the right, including member counts, subgroups, and the current Risk Score Multiplier. You can browse and configure any group without leaving the page.



Using the Group List Panel

The left panel lists all peer groups available in your organization. It includes the following controls:

- **All / Custom toggle**—switches the list between all groups and custom-only groups.
- **Search groups**—filters the list by group name as you type.
- **Create**—opens the Create Custom Peer Group modal. See ["Creating Custom Peer Groups" on page 196](#) for more information.

Each entry in the list shows the group name, a **Custom** badge if the group was created in the platform, the member count, and the current Risk Score Multiplier value. The currently selected group is highlighted in the list.

Using the Group Detail Panel

The right panel displays the full detail for the selected group, including three stat cards and sections for subgroups and members.

The header of the detail panel shows the group name, the source badge (for example, Active Directory), and the group description.

The three stat cards are:

- **Members**—the total count of entities in the group.
- **Subgroups**—the count of direct child groups.
- **Risk Score Multiplier**—the current multiplier value with a pencil (edit) icon. See ["Configuring the Risk Score Multiplier" on the next page](#).

For custom groups, a **+ Add Subgroup** button is visible at the top right of the detail panel. See ["Creating Custom Peer Groups" on page 196](#) for more information.

Understanding Subgroups

When a group has child groups, a **Subgroups** section appears below the stat cards. Subgroups are displayed as a two-column grid of clickable cards. Each card shows the subgroup name and member count. Clicking a subgroup card navigates to that subgroup detail in the panel.

Understanding Members

The **Members** section displays the entities in the group, organized into two tabs. Each tab label includes the current member count, for example, **Users (3)** and **Assets (12)**.

The **Users** tab lists identity members along with information about **Name**, **Email**, **Risk Score**, **Source**, **Status**, and **Groups**.

The **Assets** tab lists asset members along with information about : **Hostname**, **IP Address**, **Risk Score**, **Source**, **Status**, and **Groups**.

Entity names in both tables are clickable links that open the entity detail flyout or full page.

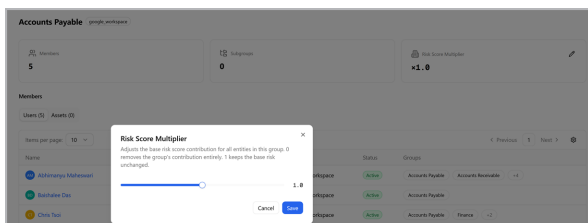
Configuring the Risk Score Multiplier

Both IDP-sourced and custom groups support Risk Score Multiplier configuration.

To configure the multiplier for a group, click the edit icon () on the **Risk Score Multiplier** stat card.



Note: Configuring the multiplier requires the **Manage Entities** permission. Viewing peer groups and their current multiplier requires **View Entities** permission or higher. See [Managing Roles](#) for more information.



The modal includes a description of the multiplier effect on risk scoring and a slider for setting the value. The slider range is 0.1 to 2.0. Click **Save** to apply the change, or **Cancel** to discard it.

Multiplier changes take effect on the next risk calculation cycle for all member entities. All changes are recorded in the audit log.

See ["Entity Risk Scores" on page 199](#) for more information on how the multiplier factors into risk calculations.

Creating Custom Peer Groups

Custom peer groups let you define and manage logical collections of entities directly within Anomali Agentive SOC Operations, without requiring an external identity or asset management system. You can assign a Risk Score Multiplier to a custom group and add identities or assets as members.

Creating a Custom Group

To create a custom peer group:

1. On the left navigation bar, click **Entity Management > Peer Groups**.
2. On the "[Understanding Peer Groups](#)" on page 193 page, click **Create** in the left panel. The **Create Custom Peer Group** modal opens.



Note: Creating and configuring custom peer groups requires the **Manage Entities** permission. See [Managing Roles](#) for more details.

3. Enter a **Group Name**. This field is required.
4. (Optional) Enter a **Description** to explain the purpose of the group.
5. Set the **Risk Score Multiplier** using the slider. The default value is 1.0 (neutral). Use values above 1.0 to increase the risk weight for group members and values below 1.0 to reduce it. The range is 0.1 to 2.0.
6. Click **Create Group** to save, or **Cancel** to discard.

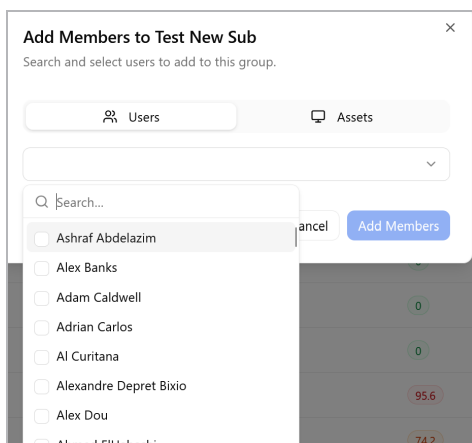
The group is created with an empty member list. Custom groups appear in the group list with a **Custom** badge and are immediately available for member assignment and multiplier configuration.

Adding Members to a Custom Group

After creating a custom group, you can add identity or asset members to it.

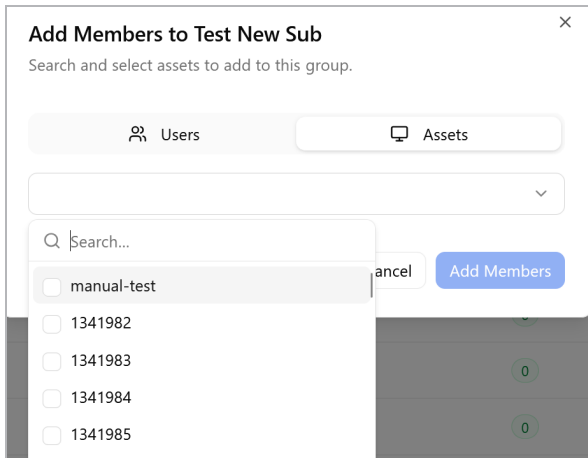
To add identity members:

1. On the left navigation bar, click **Entity Management > Peer Groups**.
2. Select the intended parent group in the group list panel.
3. Switch to the **Custom** tab on the left pane.
4. Click **Add Members**.
5. Click the **Users** tab, then Search for and select the identities to add.
6. Click **Add Members** to confirm the selection.



To add asset members:

1. On the left navigation bar, click **Entity Management > Peer Groups**.
2. Select the intended parent group in the group list panel.
3. Switch to the **Custom** tab on the left pane.
4. Click the **Assets** tab, then search for and select the assets to add.
5. Click **Add Members** to confirm the selection.



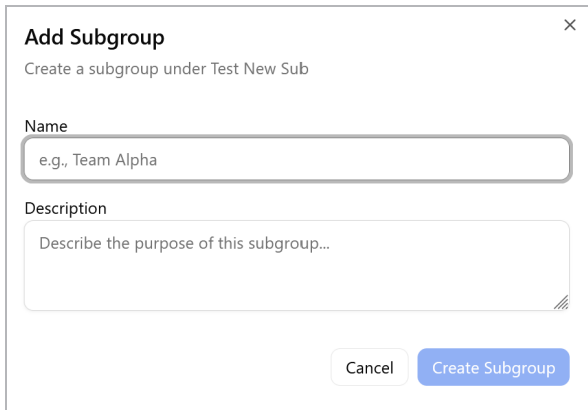
You can also add individual entities to a custom group from the Identities or Assets list. Click the row actions menu (...) for the entity, then select **Add to Group** and select the custom group. See ["Managing Identities" on page 176](#) and ["Managing Assets" on page 189](#) for more information.

Adding a Subgroup

Custom groups can be organized as subgroups of other groups, both custom and IDP-sourced, to reflect your organizational hierarchy. When a group is configured as a child of another group, the effective Risk Score Multiplier for the child group is the product of the parent multiplier and the child multiplier.

To add a subgroup:

1. On the left navigation bar, click **Entity Management > Peer Groups**.
2. Select the intended parent group in the group list panel.
3. In the group detail panel, click **+ Add Subgroup** at the top right.
4. Enter a **Name** for the subgroup. This field is required.
5. (Optional) Enter a **Description**.
6. Click **Create Subgroup** to save, or **Cancel** to discard.



The 'Add Subgroup' dialog box is titled 'Add Subgroup' with a close button (X) in the top right corner. Below the title is the subtitle 'Create a subgroup under Test New Sub'. There are two input fields: 'Name' with a placeholder 'e.g., Team Alpha' and 'Description' with a placeholder 'Describe the purpose of this subgroup...'. At the bottom, there are two buttons: 'Cancel' and 'Create Subgroup'.

The new subgroup appears indented beneath the parent group in the group list panel and is immediately available for member assignment and multiplier configuration.

Entity Risk Scores

Anomali Agentic SOC Operations calculates a dynamic risk score for each identity and asset based on detection events, peer group membership, and per-entity administrative overrides. This score gives your team a prioritized, context-aware view of which entities need immediate attention.

Understanding the Risk Formula

Each time a detection fires for an entity, the system calculates the raw risk contribution of that detection using the following formula:

Raw Detection Risk = Base Risk (1–5) × Peer Group Weighted Average Modifier × Entity Override.



Note: For correlations, the base risk is always 1. Additionally, each detection has a configurable risk score.

The three factors in this formula are described in the following sections.

Understanding Base Risk

Each detection rule has a base risk value assigned as an integer from one to five. This value reflects the severity of the signal the rule identifies.

Score	Severity	Description
1	Informational	Low-signal event providing context only, for example, a DNS lookup to a known benign domain.
2	Low	Minor indicator requiring additional context, for example, a failed authentication attempt.
3	Medium	Moderate concern warranting review, for example, Windows admin activity or a UEBA deviation.
4	High	Likely malicious activity, for example, suspected firewall misuse or a privilege escalation attempt.
5	Critical	Confirmed or near-certain attack indicator, for example, confirmed lateral movement or a critical process crash in production.

Using the Peer Group Weighted Average Modifier

Each peer group has a configurable Risk Score Multiplier with a range of 0.1 to 2.0 and a default of 1.0 (neutral). See ["Peer Groups" on page 191](#) for information on configuring group multipliers.

When an entity belongs to one or more groups, the system calculates the weighted arithmetic mean of all applicable group multipliers:

Peer Group Weighted Average Modifier = SUM of all group multipliers ÷ number of groups

For example, an entity in four groups with multipliers 1.0, 0.5, 1.3, and 1.1 has a peer group modifier of $(1.0 + 0.5 + 1.3 + 1.1) \div 4 = 0.975$.

When an entity belongs to no groups, the system applies a default modifier of 1.0, leaving the base risk unaffected.

Using Entity Override

The Entity Override is a per-entity multiplier applied as a final adjustment after the peer group modifier. The range is 0.1 to 2.0 and the default is 1.0 (neutral). Administrators use overrides to elevate the risk weight for sensitive entities such as privileged administrators, or to reduce it for known-safe automation accounts. See ["Entity Risk Score Override" on page 202](#) for more information.

Understanding Current Risk Score

The Current Risk Score is the value displayed on entity detail pages and in the entity list. It represents the compressed sum of all raw detection risk values from detections that fired within the past 24 hours.

The score is bounded between 0–100. Raw risk values are compressed using a tier model that preserves headroom as detection volume grows — a large number of moderate-severity detections will not saturate the scale and prevent meaningful high-severity signals from registering.

The score is color-coded by risk level:

Risk Level	Score Range	Color
Critical	75–100	Red
High	50–74	Orange-Red
Medium	25–49	Orange/Yellow
Low	0–24	Green

Understanding Score Decay

Each detection contribution expires exactly 24 hours after the detection fires. When a detection expires, its raw risk value is removed from the accumulator and the Current Risk Score is automatically recalculated. This means the score reflects current threat posture rather than an accumulation of historical activity.

If all detections for an entity expire, the Current Risk Score returns to zero. The system processes expiry in a background task that runs approximately every five minutes.

Example

A detection with base risk 3 fires for an identity in four peer groups with multipliers 1.0, 1.1, 1.5, and 0.9. The identity has an entity override of 1.2.

Peer Group Weighted Average Modifier = $(1.0 + 1.1 + 1.5 + 0.9) \div 4 = 4.5 \div 4 = 1.125$

Raw Detection Risk = $3 \times 1.125 \times 1.2 = 4.05$

This value of 4.05 is added to the raw risk accumulator for the entity and the Current Risk Score is recomputed from the updated total.

Permissions

Action	Permission Required
View entity risk scores and contributing factors	View Entities
Set or change an entity risk override	Manage Entities
Set or change a peer group Risk Score Multiplier	

For details on assigning these permissions to a role, see [Managing Roles](#).

Entity Risk Score Override

The Entity Risk Override is a per-entity multiplier that applies a final adjustment to the risk contribution of all detections associated with that entity. It allows administrators to express organizational context that cannot be captured by peer group membership alone — for example, elevating the risk weight for a specific privileged administrator or reducing it for a known-safe automation account.



Note: Setting or changing an override, individually or in bulk, requires the Manage Entities permission. This permission is not limited to Organization Administrators — any role granted it can set overrides. For details, see [Managing Roles](#).

Using Override Range and Defaults

The override range is 0.1 to 2.0 with a precision of two decimal places. The default value for all new entities is 1.0 (neutral). At 1.0, the override has no effect on the calculated risk. Values above 1.0 increase the risk contribution; values below 1.0 reduce it.

The override is applied after the peer group weighted average modifier in the risk formula:

Raw Detection Risk = Base Risk (1–5) × Peer Group Weighted Average Modifier × Entity Override

See ["Entity Risk Scores" on page 199](#) for the full formula and worked examples.

Understanding When to Override

Override values above 1.0 are appropriate for entities where the same detection carries higher risk than it would for a typical member of the group. Examples include:

- Executives and privileged administrators whose accounts are high-value targets.
- Entities under active investigation where temporary risk elevation is warranted.

Override values below 1.0 are appropriate for entities where expected detection volume or known-safe behavior would otherwise produce misleading scores.

Examples include:

- Approved automation accounts or service accounts with predictable, high-volume activity.
- Test systems or sandbox environments generating expected detection patterns.

Setting an Override from the Entity Detail Page

Overrides can be set for individual entities from the entity detail page.

To set an override from the entity detail page:

1. On the left navigation bar, click **Entity Management > Entities**.
2. Open the entity detail page for the identity or asset. See ["Viewing Identity Details" on page 166](#) or ["Viewing Asset Details" on page 181](#).
3. Click the **Risk Score** tab.
4. In the **Entity Risk Override** section, adjust the slider to the desired value.
5. Click **Save Override** to apply.

The override takes effect on the next risk calculation cycle.

Setting an Override

Overrides can be applied to an entity from the Identities or Assets list, as follows:

1. On the left navigation bar, click **Entity Management > Entities**.
2. Open the entity detail page for the identity or asset.
3. Click the **Risk Score** tab.
4. In the **Entity Risk Override** section, adjust the slider to the desired value.
5. Click **Save Override** to apply.

See ["Managing Identities" on page 176](#) and ["Managing Assets" on page 189](#) for more information on bulk actions.

Leveraging Audit and History

All override changes are recorded in the History tab of the entity with the previous value, new value, timestamp, and the administrator who made the change. Override changes are immutable audit records and cannot be deleted.

To review the override history for an entity, open the entity detail page and click the **History** tab. Filter by **Actions** to show override changes only.

To ensure efficient performance, this tab shows the last seven days of data and the most recent 100 records.

Entity Summary Widgets

The top of the Entities page displays four summary widgets side by side. The widgets give analysts an immediate, prioritized view of where risk is concentrated and where it is growing — without sorting or filtering the full entity list. Each entry in every widget is a clickable link to the corresponding entity detail page.

Top 5 Risky Identities ¹	Top 5 Risky Assets ²	Top 5 Rising Risk ³	Top 5 Stale Entities ⁴
Highest risk score identities right now	Highest risk score assets right now	Entities with biggest score increase in last 7 days	Active entities not seen in 30+ days
APEX\akraus 68.88	eze-grpfit-1787119421171 90.00	scanner-1787544617-a7... +37.1	audit-a6453c23 93d
APEX\csoto 62.72	eze-dd-pairmiss-1787164... 90.00	scanner-1787631055-56... +37.1	resurrected-6f316331 93d
APEX\orichardson 62.69	eze-dd-pairmiss-1787473... 90.00	host-v2 +31.6	eze-bulk-031252 66d
Alice Johnson 40.62	LT-453744 86.17	host-v2 +31.6	eze-bulk-031252 66d
Chris Miller 40.62	192.168.243.131 76.87	host-v2 +14.9	eze-bulk-031252 66d

1 Top 5 Risky Identities

Displays the five identity entities with the highest current risk scores, updated in real time. Each row shows the entity name and a color-coded risk score badge.

In the example above, the top three identities — APEX\akraus (68.88), APEX\csoto (62.72), and APEX\orichardson (62.69) — cluster in the High risk range, while Alice Johnson and Chris Miller both sit at 40.62 in the Medium range. This tiered distribution shows that risk is spread across multiple identities rather than concentrated in a single outlier, which can indicate a broader pattern of suspicious activity worth investigating across the identity population. Because risk scores are calibrated to organizational context through peer group multipliers, the highest scoring identity reflects meaningful relative risk.

2 Top 5 Risky Assets

Displays the five asset entities with the highest current risk scores, updated in real time. Each row shows the entity name and a color-coded risk score badge.

In the example above, the top three assets score 90.00, followed by LT-453744 at 86.17 and 192.168.243.131 at 76.87 — all five fall in the Critical risk range (75–100). A full widget of critically scored assets suggests a shared detection pattern firing across multiple systems, which may point to a broader issue such as a compromised network segment rather than a single isolated endpoint.

3 Top 5 Rising Risk

Displays the five entities with the largest risk score increase over the last seven days. Each row shows the entity name and the score delta, for example, +78.5.

In the example above, two scanner assets are tied at +37.1, and three host-v2 instances show increases of +31.6, +31.6, and +14.9. Multiple assets from similar naming conventions rising together can indicate a shared detection rule firing across a group of related systems — entities that may not yet appear in the Risky Assets widget but are trending toward criticality. Because scores are recalculated continuously from a rolling 24-hour window, this widget surfaces entities whose activity is trending upwards.

4 Top 5 Stale Entities

Displays the five active entities that have had no observed activity, no log events, detections, or sync updates for 30 or more days. Each row shows the entity name and the number of days since last seen, for example, 41 days.

In the example above, audit-a6453c23 and resurrected-6f316331 have been unseen for 93 days, and three e2e-bulk-031252 entries for 86 days. Entities stale for 90 or more days may represent decommissioned or forgotten assets that remain active in the system, expanding the attack surface without generating detections.

Chapter 7: Priority Intelligence Requirements

Accessing Priority Intelligence Requirements207

Creating a PIR211

Viewing PIR Details229

Managing PIRs234

A **Priority Intelligence Requirement** (PIR) is a high-level intelligence question or topic that an organization formally considers critical for supporting business decision-making and risk management. PIRs define what your intelligence team should be tracking to protect and support your organization. They represent a consensus between executive leadership and the threat intelligence team about what the organization cares about most, which risks require ongoing monitoring, and what type of reporting leadership expects. PIRs help ensure that intelligence efforts are aligned with business priorities—not just collecting data, but answering the right questions.

ThreatStream Next Gen enables you to create PIRs based on the requirements of your organization, run them on your schedule, analyze the results with Anomali AI, deduplicate findings against existing intelligence in ThreatStream, and deliver structured outputs via new threat models, reports, email notifications, or investigations. By managing PIRs within the ThreatStream Next Gen platform, you can turn them into actionable, trackable intelligence drivers. When properly operationalized, PIRs elevate threat intelligence from time-consuming, passive monitoring to an automated, strategic business function.

Characteristics of an Effective PIR

Effective PIRs are precise, measurable, and decision-oriented.

An effective PIR should:

- Ask a single, focused question
- Address a fact, event, or activity that can be answered with intelligence
- Support a specific decision
- Be time-sensitive
- Be tied directly to decisions key stakeholders must make

Examples of Priority Intelligence Requirements

Organizations typically define a small set of core PIRs (often 5–10) that guide daily intelligence activities and threat monitoring efforts. They vary by industry, geography, and business model.

Below are PIR examples based on common organizational needs.

Industry-Focused PIRs

- What threat actors are actively targeting the financial services industry?
- What emerging ransomware groups are attacking regional banks?
- What cyber campaigns are targeting healthcare providers?

Organization-Specific PIRs

- Are any threat actors actively targeting our organization?
- Has our company been mentioned on dark web forums?
- Are there leaked credentials associated with our employees or domains?

Geographic PIRs

- What cyber threats are active in our city or region?
- Are there politically motivated cyber activities affecting businesses in our country?

Technology- or Asset-Focused PIRs

- Are there active exploits targeting our critical software stack?
- What vulnerabilities are being weaponized against our cloud provider?

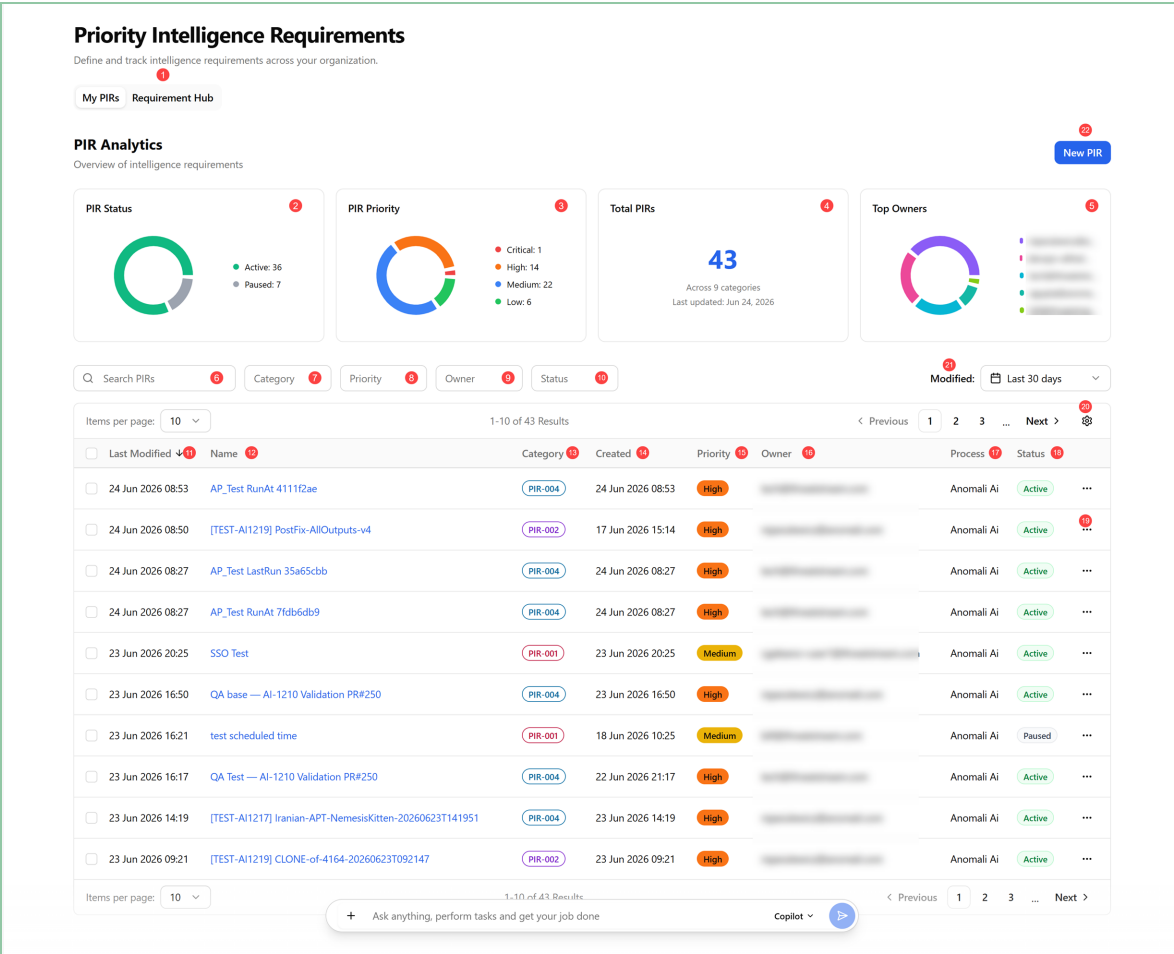
Accessing Priority Intelligence Requirements

All Priority Intelligence Requirements (PIRs) created within your organization are listed on the **Priority Intelligence Requirements** page. On this page, you get a centralized view of all PIRs to which you have access, making it easy to track their status, priority, ownership, and category. From this page, you can also create new PIRs. You can quickly get started by selecting AI-recommended PIR presets in the Requirement Hub, tailored to your environment and workflows, or you can create

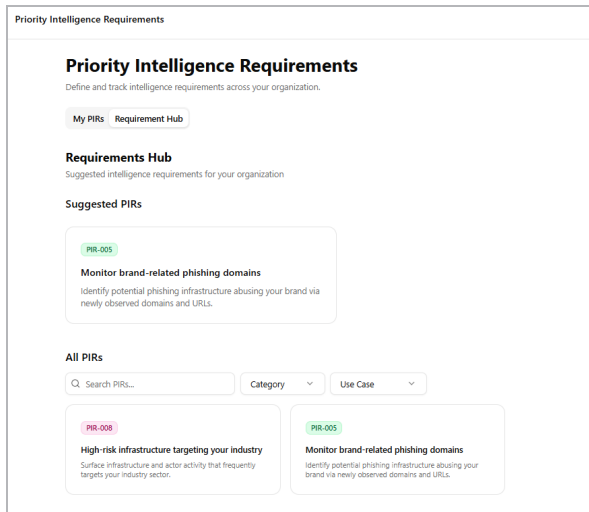
your own through a simple guided process—defining what you want to track, setting a schedule, and assigning owners and stakeholders.

To access PIRs created within your organization, navigate to **ThreatStream Next Gen > Priority Intelligence Requirements.**

Below is an example of the Priority Intelligence Requirements page.



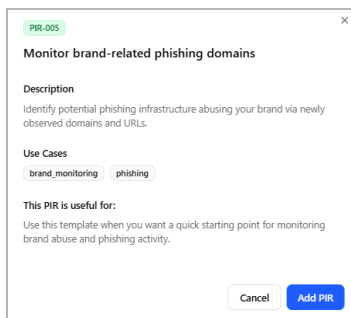
1 Requirement Hub. Explore suggested intelligence requirements (examples) for your organization. Use keywords or Category and Use Case filters to search for PIR templates that may interest you.



Click a suggested PIR to view its description, use cases, and what it can be useful for.

If you want to add it to your organization, click **Add PIR**. You are redirected to the Create New PIR workflow with the pre-populated fields.

Follow the steps described in ["Creating a PIR " on page 211](#) and make the necessary changes to finish creating the PIR.



- 2 PIR Status:** Displays the distribution of PIRs by status, such as Active or Paused.
- 3 PIR Priority:** Displays the breakdown of PIRs by their priority level (Critical, High, Medium, or Low).
- 4 Total PIRs:** Displays the total number of PIRs across all categories and the timestamp of when the PIR data was last updated.
- 5 Top Owners:** Displays the users with the highest number of assigned PIRs.

6 Search PIRs: Search PIRs by their names. The search is case-insensitive and updates incrementally.

7 Category: Filter PIRs by one of the following categories: PIR-001 Domain Risk, PIR-002 Infrastructure Risk, PIR-003 Tech Stack Risk, PIR-004 Emerging Threats, PIR-005 Phishing, PIR-006 Supply Chain, PIR-007 Brand Monitoring, PIR-008 Target Industry, PIR-009 Target Location, and PIR-010 Source Location.

8 Priority: Filter PIRs by their priority level—Critical, High, Medium, or Low.

9 Owner: Filter PIRs by their owner.

10 Status: Filter PIRs by their status.

11 Last Modified: Timestamp of when the PIR was last modified.

12 Name: Name of the PIR.

13 Category: Category of the PIR.

14 Created: Timestamp of when the PIR was created.

15 Priority: Priority status of the PIR.

Possible values include Critical, High, Medium, and Low.

16 Owner: User who owns the PIR.

17 Process: The process type used for creating the PIR—Anomali AI or Manual. See ["AI-Generated vs. Manual PIR Process" on page 222](#) for more information.

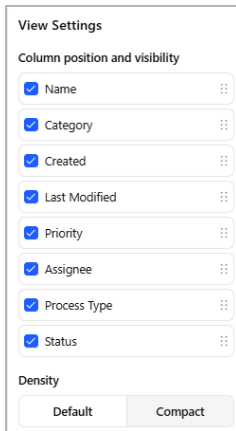
18 Status: Status of the PIR:

- Active—active PIR that runs on a specified schedule.
- Paused—disabled PIR that cannot be executed.

19 More options menu (...):

- **Status:** Change the PIR status to Active or Paused.
- **Delete:** Delete the PIR. See ["Deleting PIRs From the Priority Intelligence Requirements Page" on page 240](#) for details.

20 View Settings: Select the columns and table density (default or compact) to be displayed. By clicking the drag handle icon () , drag and drop columns to change their position in the table. To return the view back to its default settings, click **Reset View**.



- 21 Modified:** Select a time range to filter PIRs based on when they were last updated.
Possible values include: All time, last 24 hours, last 7 days, last 30 days, last 90 days, and this year.
By default, last 30 days is selected.

- 22 New PIR.** Create a new PIR. See ["Creating a PIR " below](#) for details.

Creating a PIR



Note: Only Organization Administrators or users with Create PIR Configuration permission can create PIRs. See [Managing Roles](#) for details.

To create a PIR, you must define a PIR question, configure its execution schedule, select input types, define the analytical process and configure the outputs.

You can create PIRs in two ways:

- Use a suggested PIR from the Requirement Hub and then configure all PIR workflow steps. For details, see [Requirement Hub](#).
- Create a PIR from scratch, as described below.

To create a PIR:

1. Navigate to **ThreatStream Next Gen > Priority Intelligence Requirements**.
2. Click **New PIR**. The Create New PIR workflow opens.

3. On the *Description* step, configure the following fields:

Field	Description
Name (Intelligence Question)	Enter a concise title that identifies the intelligence requirement or a question that this PIR should address. For example, <i>Credential Phishing Campaigns Targeting Executive Accounts</i> <i>Ransomware Campaigns Targeting Healthcare Sector</i> <i>What phishing campaigns are targeting our organization?</i> <i>What threat actors are targeting the financial sector in the US?</i> For more PIR examples, see "Examples of Priority Intelligence Requirements" on page 207.
Description	Enter a description for the PIR. When creating a description, Anomali AI reads a PIR name and description to understand the focus of your PIR and uses that context to suggest relevant process steps on the Process step. This means: ■ Naming specific threat actors or malware families helps the AI recommend targeted correlation steps ■ Naming specific techniques helps the AI recommend technique-specific analysis ■ Vague language (for example, "monitor for threats") gives the AI nothing specific to work with, resulting in generic recommendations

Field	Description
Category	Select one of the following PIR categories: PIR-001 Domain Risk, PIR-002 Infrastructure Risk, PIR-003 Tech Stack Risk, PIR-004 Emerging Threats, PIR-005 Phishing, PIR-006 Supply Chain, PIR-007 Brand Monitoring, PIR-008 Target Industry, PIR-009 Target Location, and PIR-010 Source Location.
Output Tags	(Optional) Configure tags to be automatically applied to the outputs generated by the PIR. When you select a PIR category, the corresponding category tag is automatically assigned to the PIR. To apply additional tags to the outputs generated by this PIR, select one or more tags from the available list or create custom tags. The available tags are derived from the ThreatStream Preferred Tags list. See Adding Preferred Tags to Intelligence for more information. To create a custom tag, enter the desired tag value into the search field and click +.

Field	Description
Collection Tags	(Optional) Configure tags to be automatically applied to observables, threat models, and investigations matched during PIR execution. These tags make it easier to find, filter, and operationalize the intelligence identified by the PIR. A tag with the PIR name is automatically assigned. To apply additional tags, select Tag all collected intelligence, and then select one or more tags from the available list or create custom tags. The available tags are derived from the ThreatStream Preferred Tags list. See Adding Preferred Tags to Intelligence for more information. To create a custom tag, enter the desired tag value in the search field and click +.  Note: This is a limited-availability feature. Contact Anomali Customer Support for more information.
PIR Run Schedule	(Optional) Define how often you want to run this PIR. Select frequency (daily, weekly, or monthly) and time. By default, your current local hour is displayed. Anomali recommends selecting a time right before you begin your work, so it would be ready before you start working. On each run, PIR checks what it has previously added to output and filters out already-reported findings.
Expiry Date	(Optional) Set an expiry date for the PIR. When the expiry date is reached the PIR automatically changes its status to Paused and stops running on its schedule.
Stakeholders	(Optional) Select ThreatStream users who you think is interested in this PIR.
Owner	Select an owner of the PIR.

Field	Description
Priority	Define priority of the PIR—Critical, High, Medium, or Low.

Create New PIR

1

Description

2

Inputs

3

Process

4

Output

5

Review

PIR Description

Name (Intelligence Question) *

What threat actors are targeting the financial sector in the US

Description *

This PIR will track actors targeting the financial sector in the US.

Category *

PIR-008 Target Industry

Tagging

Output Tag

pir-008 Target Industry

PIR-008 Target Industry

Collection Tags

log all collected intelligence

threat_actor_report

threat_actor_report

PIR Run Schedule

Daily

At

1400

Expiry Date

No expiry date set

Stakeholders

gcp@stakeholder.com

gcp@stakeholder.com

Owner *

gcp@stakeholder.com

Priority

Medium

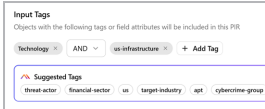
Cancel

Previous

Next

- Click **Next**.
- On the *Inputs* step, define what data needs to be analyzed:

Field	Description
Inputs	Select the type of intelligence for the PIR to track—Observables/IOCs, Threat Models, or Investigations. Anomali leverages AI to assist with recommended inputs. The AI icon () in the platform indicates the areas where AI is at work for your PIR. ■ <i>Use Observables</i> when your PIR is focused on detecting or tracking specific technical threat data. When selecting Observables as an input type, you can further refine your PIR by selecting specific observable types such as IP Addresses, Domains, URLs, File Hashes, and Email Addresses. ■ <i>Use Threat Models</i> when your PIR is focused on understanding adversary context, behavior patterns, or campaign activity. When selecting Threat Models as an input type, you can choose from the threat model types available in your organization. You can get granular in the type of threat model that will be searched. ■ <i>Use Observables and Threat Models</i> when you think that your PIR can benefit from combining both input types. ■ <i>Use Investigations</i> when your PIR should incorporate findings from ongoing analytical work that is contained in an ongoing or past investigation.
Lookback Window	Limit input data to records created or modified within a time window. Default value is 24 hours and the setting is enabled by default for newly created PIRs.

Field	Description
Input Tags	(Optional) Select tags that are available in your ThreatStream instance by which you want to filter intelligence that will be included in the PIR. You can add tags from the Suggested Tags section, or add your own tags by using the + Add Tag button. When you select tags, only observables, threat models and investigations that carry those tags will be included in the PIR results. Additionally, within the Selected Tags section, you can choose which tags must be included (AND operator) and which tags are optional (OR operator). These tags will be used to match observables and threat models with the specified tags. For example, when all observables and threat model types are selected as inputs and two tags are combined using the AND operator, the PIR includes only observables and threat models that contain both tags. If the OR operator is used, the PIR includes observables and threat models that contain either tag. If neither tag is found in the observables or threat models, the PIR returns no results.  The screenshot shows a UI for selecting input tags. At the top, it says 'Input Tags' and 'Objects with the following tags or field attributes will be included in this PIR'. Below this, there's a row with 'Technology' and 'us infrastructure' separated by an 'AND' operator, followed by an '+ Add Tag' button. Below that, there's a 'Suggested Tags' section with a list of tags: 'threat-actor', 'financial sector', 'uk', 'target industry', 'apt', and 'cybercrime-group'.
Included Keywords	(Optional) Enter comma-separated keywords by which you want to filter intelligence that will be included in the PIR. Note that keywords are only applied to selected threat models and investigations. Keywords are disregarded for observables. When you enter keywords, the PIR uses them to search threat model content and to identify which investigations are included in results.

Create New PIR

Start by describing your intelligence questions, the scope, and what you want the PIR to produce. [Learn more](#)

1 Description 2 **Inputs** 3 Process 4 Output 5 Review

Inputs

Select which data sources to include in this PIR

Based on your PIR category and title, we've suggested relevant data source types for your intelligence requirements.

Observable / IOC
Include indicators of compromise and observable data

Observable Types Deconstruct All

- Domain
- IP
- Hash
- Email
- IPv6
- URL

Threat Models
Include threat actor profiles and models

Threat Model Types Deconstruct All

- Actions
- Campaigns
- Capabilities
- Incidents
- Intelligence Sets
- Signatures
- Tools
- Vulnerabilities
- Attack Patterns
- Course of Action
- Exercises
- Infrastructure
- Malware
- Threat Bulletin
- TTPs

Investigations
Include ongoing and past investigations

Lookback Window

Limit input data to records created or modified within a time window

☒ Only include records created or modified in the last 24 hours

When enabled, each PIR can only pull observables, threat models, and investigations that have been created or modified within the configured time window. Items unpublished to past all matching records, regardless of age.

Input Tags

Objects with the following tags or field attributes will be included in this PIR

Tags + Add Tag

Suggested Tags

Threat actor Financial sector CA Target Industry API Cybercrime group Banking North America Malware Reconnaissance Phishing Credential Theft Mitre attack Sector targeting Geographic focus

Included Keywords

Objects containing these keywords will be included in this PIR

Enter comma-separated keywords (e.g., APT28, Cozy Bear, Ransomware)

Suggested Keywords

APT28 Cybercat Capital Group Lazarus Group North Korea Evilware WOTW Dridex NotBot Eveeet Magnet Malware Banking Trojan Credential Theft SANSI Attacks Spear Phishing Initial Access Tactics Techniques and Procedures

MITRE ATT&CK Financial Services United States

Cancel Previous **Next**

When a threat model is selected as an input along with a tag and a keyword, the system applies an OR operator between the tags and keywords. For example, a threat model is selected as an input. A single tag labeled financial-sector is selected on the Inputs page. The following keywords are also included: initial access broker, BlackCat, ALPHV, LockBit, double extortion, RaaS, credential harvesting, financial services.

6. Click **Next**.

7. On the *Process* step, define the process to be used to analyze the intelligence collected for this PIR.

Select one of the following options:

- **Anomali Ai Execution:** (Recommended) Analytical process generated with Anomali AI based on the input provided on the previous steps.
To generate the proposed process, click **Generate Analytical Process**.

If necessary, customize the steps of the generated prompt using the following action buttons:

- Move one step up (^)
- Move one step down (v)

- Edit (✎)
- Delete (🗑)

Create New PIR

Start by describing your intelligence questions, the scope, and what you want the PIR to produce. [Learn more if](#)

```
graph LR; 1((1)) --- 2((2)) --- 3((3)); 4((4)); 5((5));
```

Analytical Process

Define the process that will be used to analyze the intelligence collected for this PIR.

Animal AI Execution

Let Animal AI perform these process steps. Turn this off if analysts will run the process manually.

Process Steps

- 1. Identify and Categorize Threat Actors Targeting US Financial Sector
- 2. Map Tactics, Techniques, and Procedures (TTPs) to MITRE ATT&CK

Previous **Next**

- **Manual Process:** Manually defined steps of an analytical process. A manual process step is a text-based instruction that an analyst will follow when the PIR executes and surfaces results.

To learn more about the usage of AI-generated and manual processes, refer to ["AI-Generated vs. Manual PIR Process"](#) on page 222.

To define a manual process:

- i. Click **Add Step**.
- ii. Enter a step title, description, and links to external resources.
- iii. Click **Add Step**.
- iv. Repeat steps A-D as many times as you need.

```

graph LR
    Discover[Discover] --> Ingest[Ingest]
    Ingest --> Process[Process]
    Process --> Output[Output]
    Output --> Review[Review]
  
```

The diagram illustrates the Analytical Process flow, which consists of five sequential steps: Discover, Ingest, Process, Output, and Review. The first three steps (Discover, Ingest, and Process) are currently active, indicated by blue checkmarks above each label. The last two steps (Output and Review) are inactive, indicated by grey circles above each label. The flow is represented by a horizontal line connecting the steps, with arrows pointing from left to right.



Note: If you add any time references to your analytical step descriptions (for example, "analyze last 7 days"), they will be ignored during data fetching because time range filtering is determined by the PIR Run Schedule and Lookback Window settings only. To match your intended time range, configure the Lookback Window setting either on the Inputs step or on the PIR details page after completing the PIR creation. For details, see [Step 2: Inputs](#) and ["Editing PIRs" on page 234](#).

8. Click **Next**.
9. On the *Output* step, configure how you want to receive and share the results of the PIR. The right combination depends on who needs the results and what they need to do with them.

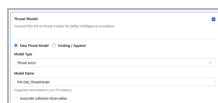
You can select the following options:

- **Generate Report:** Creates a shareable, Anomali AI-generated summary that can be used for briefings or shared with stakeholders.

When you select a report as an output, the embedded AI suggests a report template based on your PIR category and inputs. You can use the drop-down menu to select a different report template or use the template that Anomali AI recommends. Report templates are managed in the Reporting section of ThreatStream Next Gen. See ["Using Report Templates" on page 286](#) for details.



- **Threat Model:** Select one of the following actions:
 - **Add Threat Model**—if you want to add a new threat model to your ThreatStream environment after each PIR run. Then select the threat model type, enter a name, and specify whether to associate collected observables with the threat model generated by this PIR.



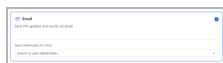
- **Existing/Append**—if you want to update an existing threat model in your ThreatStream environment with PIR findings after each PIR run. Then

select the threat model type, choose the threat model to update, and specify whether to associate collected observables with it. Each PIR run updates the selected threat model with the latest analysis and adds new associations while preserving existing ones.



Note: Associate collected observables is a limited-availability feature. Contact Anomali Customer Support for more information.

- **Email:** Sends automatic PIR updates to the specified users outside the platform, who need visibility into PIR findings.



- **Investigate:** Creates a new investigation or links this PIR to an existing investigation in ThreatStream. Additionally, you can define whether you want to associate collected observables with the investigations triggered by this PIR.



- **Slack:** Sends PIR updates and results to Slack users and public channels of your organization. See ["Configuring Slack Output" on page 227](#) for details.

- **Jira:** Creates Jira tickets for PIR findings and actions. See "[Configuring Jira Output](#)" on page 225 for details.

Create New PIR
Start by describing your intelligence question, the scope, and what you want the PIR to produce. [Learn more](#)

Progress: 1 Description, 2 Inputs, 3 Process, 4 Output, 5 Review

Expected Output
Configure how you want to receive and share the results of this PIR

- ☐ **Generate Report**
Create comprehensive intelligence reports with findings from this PIR
- ☐ **Investigate**
Create or link investigations for this PIR
- ☐ **Slack**
Send PIR updates and results to Slack channels
- ☐ **Threat Model**
Connect this PIR to threat models for better intelligence correlation
- ☐ **Email**
Send PIR updates and results via email
- ☒ **Jira**
Create Jira tickets for PIR findings and actions

[Configure integration](#)

Buttons: Cancel, Previous, Next

10. Click **Next**.

11. On the *Review* step, review all PIR details.
If you need to edit a section, click **Edit** and make the necessary changes.

Create New PIR

Progress: 1 Description, 2 Inputs, 3 Process, 4 Output, 5 Review

Review
Review your PIR details before creating

PIR Description [Edit](#)

PIR Name: Which Nation-State APT are targeting critical US infrastructure?

Category: PIR-005 Phishing

Priority: medium

Assignee: John Doe

Description: This PIR tracks APT groups pre-positioning in US critical infrastructure using living off the land techniques with focus on related clusters targeting energy, water, and communications OT environments.

Stakeholders: John Doe

Schedule: Daily at 09:00 UTC

Intelligence Inputs [Edit](#)

Output Type: [Empty]

Buttons: Cancel, Previous, Create PIR

12. Click **Create PIR**.

The PIR is created and added to the list of PIRs of your organization on the Priority Intelligence Requirements page.

AI-Generated vs. Manual PIR Process

In ThreatStream Next Gen, the *Process* step of a Priority Intelligence Requirement (PIR) defines the actions performed when the PIR returns matching results. These actions guide analysts through evaluation, correlation, escalation, and response.

You can build the process using:

- **Anomali AI-generated process steps**, recommended by Anomali.
- **Manual process steps**, defined by an analyst.

To learn more about the *Process* step of the PIR creation, refer to [Process Step](#).

Anomali AI-Generated Process Steps

When you reach the *Process* step during PIR creation, Anomali AI analyzes the inputs provided in earlier PIR creation steps and generates recommended process steps.

Behavior

- Process steps are generated at PIR creation time
- The AI uses only the context provided on the *Description* and *Inputs* steps
- Recommendations do not update automatically if description and inputs are modified after a PIR creation
- Output quality depends on the specificity and completeness of the inputs

Usage

Anomali AI-generated process steps provide a baseline workflow based on common CTI practices. Use these steps as a draft that must be reviewed and refined.

For each recommended step, you can:

- Accept and leave the step as is if it is relevant and actionable
- Edit the step to align with your environment
- Remove the step if it is not applicable

When to Use AI-generated Process

- To quickly create an initial PIR workflow
- When working with standard or well-defined intelligence requirements
- To ensure common analysis steps are included
- When building or standardizing processes across teams

Manual Process Steps

Manual process steps are analyst-defined instructions that specify what actions to take when the PIR surfaces results.

Behavior

- Manual steps are text-based instructions
- They are executed by analysts, not automated by the system
- They can include references to internal procedures, tools, and teams

When to Use

- To incorporate organization-specific procedures or policies
- To define actions in external systems (for example, SIEM, SOAR, or ticketing platform).
- To document escalation, notification, or reporting workflows
- When the process requires analyst interpretation or decision-making

Writing Manual Process Steps

Manual process steps must be clear, specific, and actionable.

Guidelines for Creating Manual Process Steps

- Start with an action verb (for example, Review, Correlate, Escalate, Notify, Document)
- Describe what to do and what to look for
- Reference specific tools, systems, or teams, where applicable
- Limit each step to one action
- Ensure the step is self-contained and can be followed without additional context

Examples

Weak Step	Improved Step
Check the results	Review surfaced indicators against the internal blocklist and escalate any matches
Look for threats	Correlate identified threat actor TTPs with SIEM detections to identify matching activity
Tell the team	Notify the incident response team via the designated escalation channel when critical indicators are identified

Best Practice

1. Generate initial steps using Anomali AI
2. Review and refine all recommended steps
3. Add manual steps to address gaps and align with internal workflows

This approach ensures that the PIR process is both comprehensive and operationally relevant.

PIR MCP Integrations

On the *Output* step of the Priority Intelligence Requirement (PIR) creation process, you can choose integrations like Jira and Slack to automatically route PIR results and alerts to the right teams. See [PIR Output](#) for details.

These integrations help you create and update Jira issues for tracking work, as well as send real-time Slack notifications to coordinate response and keep stakeholders informed.

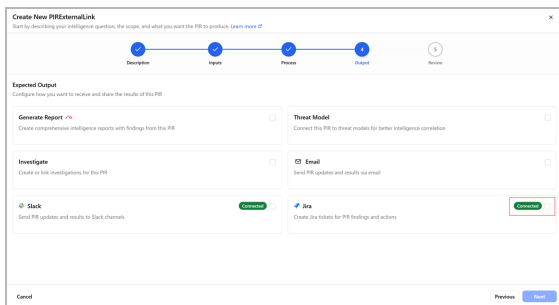
Configuring Jira Output

Choosing Jira as one of your PIR output options, enables you to automatically create Jira issues, assign them to the appropriate team members, and update ticket status as investigations progress based on the PIR findings.

Before configuring the Jira output of a PIR, verify that the JIRA MCP integration is configured on the Integrations Marketplace. See ["Jira MCP Integration" on page 156](#) for details.

To configure the Jira output:

1. Navigate to **ThreatStream Next Gen > Priority Intelligence Requirements**.
2. Click **New PIR**. The Create New PIR workflow opens.
3. Complete the *Description*, *Input*, and *Process* steps. See "[Creating a PIR](#)" on [page 211](#) for details.
4. On the *Output* step, select **Connected** in the Jira section. The Jira dialog box opens.



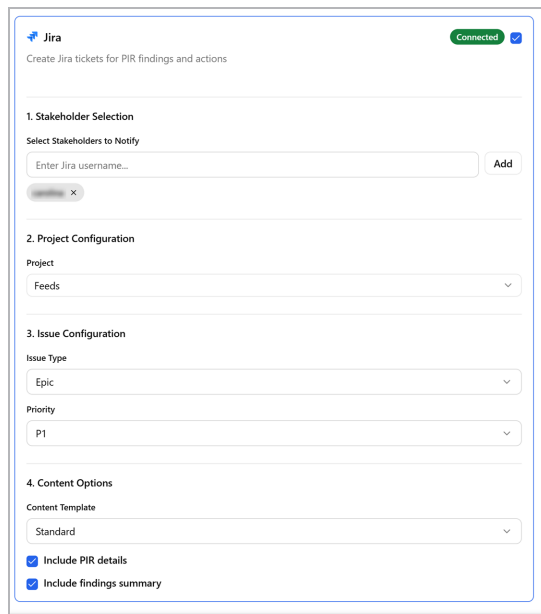
5. Configure the following parameters:
 - **Stakeholder Selection:** Use the **Add** button to add Jira users that will be notified.
 - **Project Configuration:** Select a Jira project associated with this PIR topic.
 - **Issue Configuration:** Select an issue type and its priority.

For example:

Issue Type—Epic, Bug, Task, Sub-task, and so on.

Priority—P1, P2, P3, Blocked, and so on.
 - **Content Options:** Select a content type. Possible options include: Standard, Brief, and Detailed.
 - **Include PIR details:** Select this option if you want to include PIR details in the Jira tickets.
 - **Include findings summary:** Select this option if you want to include a

findings summary in the Jira tickets.



The screenshot shows a 'Jira' configuration dialog box with a 'Connected' status indicator. The dialog is titled 'Create Jira tickets for PIR findings and actions'. It contains four sections: 1. Stakeholder Selection, which includes a text input for 'Enter Jira username...' and an 'Add' button; 2. Project Configuration, with a 'Project' dropdown menu set to 'Feeds'; 3. Issue Configuration, with 'Issue Type' set to 'Epic' and 'Priority' set to 'P1'; and 4. Content Options, which includes a 'Content Template' dropdown set to 'Standard' and two checked checkboxes: 'Include PIR details' and 'Include findings summary'.

6. When you are done configuring all output options, click **Next**.

Configuring Slack Output

When threats are detected by a PIR or investigations require coordination, ThreatStream Next Gen can automatically notify the right people and let them take action directly in Slack.

Before configuring the Slack output of a PIR, verify that the Slack MCP integration is configured on the Integrations Marketplace. See ["Slack MCP Integration" on page 157](#) for details.

To configure the Slack output:

1. Navigate to **ThreatStream Next Gen > Priority Intelligence Requirements**.
2. Click **New PIR**. The Create New PIR workflow opens.
3. Complete the *Description*, *Input*, and *Process* steps. See ["Creating a PIR " on page 211](#) for details.
4. On the *Output* step, select **Connected** in the Slack section. The Slack dialog box opens.

Create New PIR External Link

Step 4 of 5: Output

Expected Output

Configure how you want to receive and share the results of this PIR

☒ Generate Report
Create comprehensive intelligence reports with findings from this PIR

☒ Threat Model
Connect this PIR to threat models for better intelligence correlation

☒ Investigate
Create or link investigations for this PIR

☒ Email
Send PIR updates and results via email

☒ Slack
Send PIR updates and results to Slack channels

☒ Azure
Create links to PIR findings and actions

Cancel Previous Next

5. Configure the following parameters:

- **Channel Selection:** Select public channels and/or users that will be notified of the PIR findings.
- **Message Formatting:**
 - Select a **Message Template**—Brief Summary, Detailed Report, or Custom.
 - Select a **Notification Frequency**—Immediate, Hourly Digest, or Daily Digest.
 - Select a **Severity Threshold**—All Severities, High Only, Medium and Above.

Slack

Send PIR updates and results to Slack channels

Connected

1. Channel Selection

Public Channels

#general

Direct Messages

+2

2. Message Formatting

Message Template

Detailed Report

☒ Include attachments (reports, charts, etc.)

Notification Frequency

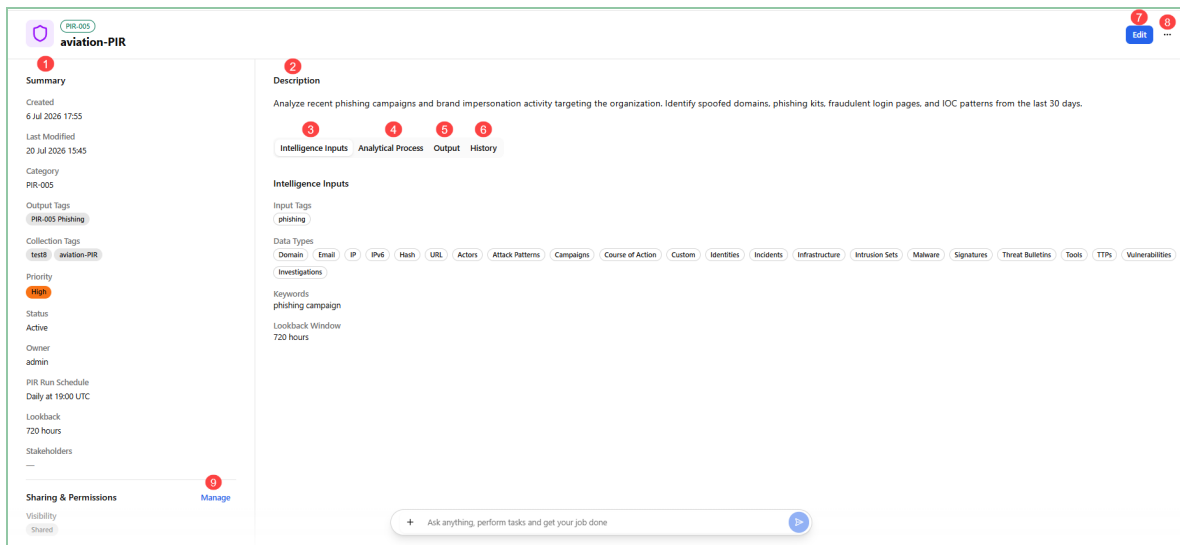
Immediate

Severity Threshold

Medium and Above

Viewing PIR Details

On the Priority Intelligence Requirements page, you can click any of the listed PIRs to view its details. The PIR details page provides a full picture of the PIR, including its summary, description, priority, category, and metadata such as status, owner, schedule, and stakeholders. It also shows the configured intelligence inputs (tags, data types, and keywords), the analytical process used to generate results, and the outputs produced, including reports, threat models, and investigations. In addition, you can review a run history log, edit any section of the PIR, access more actions such as running the PIR on demand or sharing it, and manage sharing and permissions.



1 Summary: Every PIR summary includes the following details:

Attribute	Description
Name	Name of the PIR.
Created	Timestamp of when the PIR was created.
Last Modified	Timestamp of when the PIR was last modified.

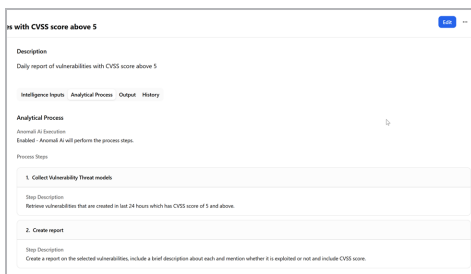
Attribute	Description
Category	Category of the PIR. Possible values include: PIR-001 Domain Risk, PIR-002 Infrastructure Risk, PIR-003 Tech Stack Risk, PIR-004 Emerging Threats, PIR-005 Phishing, PIR-006 Supply Chain, PIR-007 Brand Monitoring, PIR-008 Target Industry, PIR-009 Target Location, and PIR-010 Source Location.
Output Tags	Tags applied to the selected outputs generated by the PIR.
Priority	Priority of the PIR: Critical, High, Medium, or Low.
Status	Status of the PIR: Active or Paused. Active PIRs run on a configured schedule. Paused PIRs are inactive and won't run until made active again.
Owner	User who owns the PIR.
PIR Run Schedule	Frequency of PIR runs.
Lookback	PIR lookback window.
Stakeholders	Users who receive PIR updates.

2 Description: Description of the PIR.

3 Intelligence Inputs: View the type of data analyzed in the PIR.

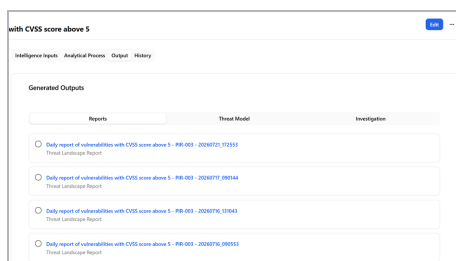
- **Input Tags:** Displays all input tags used for filtering intelligence for this PIR.
- **Data Types:** Displays all intelligence types used for analysis in the PIR.
- **Keywords:** Displays all keywords used for filtering intelligence for the PIR.
- **Lookback Window:** Displays how far back in the time the PIR looks before its run.

4 Analytical Process: View the steps of the analytical process used for the PIR.

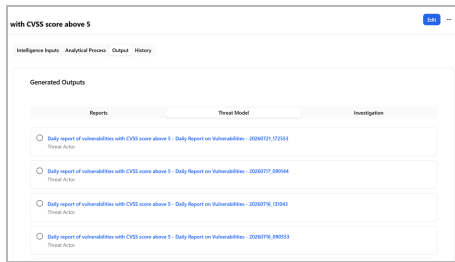


5 Output: View the list of generated outputs and output settings for the PIR:

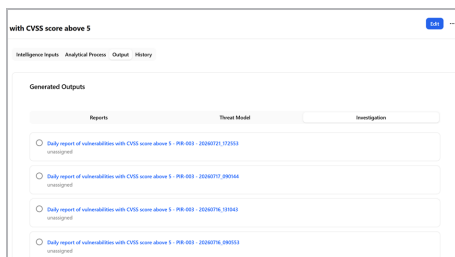
- **Reports:** View the list of all reports generated for the PIR. Click a report to view report details. All generated reports can also be accessed on the Security Reporting page. See ["Accessing Organization Reports" on page 273](#) for details.



- **Threat Models:** View the list of threat models created for the PIR. Click a threat model to view its details in ThreatStream.



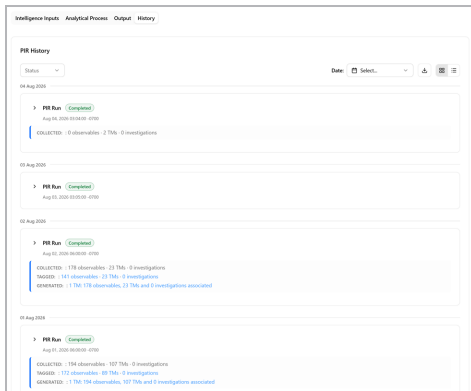
- **Investigations:** View the list of investigations started for the PIR. Click an investigation to view its details in ThreatStream.



- 6 History:** View a diagnostic log for every PIR run or export PIR logs in a CSV file. The PIR logs can be filtered by their status:

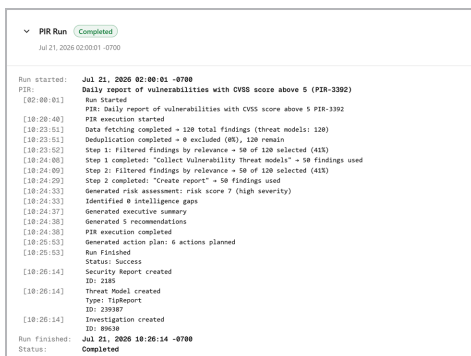
- **Completed**—the run executed from start to finish without errors and reached its expected end state. All steps in the process finished successfully, and all expected outputs were produced.
- **Failed**—the run started but stopped before finishing because of an error.
- **Timed Out**—the run started but didn't finish within the allotted time window, so the system killed it or gave up waiting.
- **In Progress**—the run has started and is actively executing but hasn't reached a terminal state yet.

Each PIR run entry displays a summary banner with clickable counts of what that run collected, tagged, and generated. Each count links to the items from that run in ThreatStream.



A PIR log provides visibility into what the PIR agent did, how long each step took, and whether outputs were delivered successfully. Retention for PIR trace logs is 6 months.

To view PIR log details, click the PIR log of your interest:



To export PIR logs in CSV format, click the export icon (📄). The file downloading process starts immediately.

7 Edit: Click **Edit** to modify any section of the PIR. To update the analytical process step and output options, switch to the corresponding tabs. Click **Update** when done.

8 More actions menu (...):

- **Run Now:** Run a PIR on demand. See ["Running PIRs on Demand" on page 235](#) for details.
- **Manage Access:** Configure access to the PIR. See ["Managing Access to PIRs" on page 241](#) for details.

- **Share:** Copy the link to the PIR to clipboard. See ["Sharing a PIR From the PIR Details Page" on page 237](#) for details.
- **Delete:** Remove the PIR from the list of PIRs in your organization. See ["Deleting PIRs From PIR Details Pages" on page 241](#) for details.

9 Sharing & Permissions: See ["Managing Access to PIRs" on page 241](#) for details on managing PIR permissions.

Managing PIRs

You can apply the following actions to PIRs created within your organization:

[Edit PIRs](#)

[Run PIRs on demand](#)

[Share links to PIRs](#)

[Summarize PIRs](#)

[Update status of PIRs](#)

[Delete PIRs](#)

Editing PIRs

To edit PIRs, you must have the required permissions. For details, refer to ["PIR Actions and Their Required Permissions" on page 242](#).

To edit a PIR:

1. Navigate to **ThreatStream Next Gen > Priority Intelligence Requirements**.
2. On the Priority Intelligence Requirements page, click the PIR you want to edit.
3. On the PIR details page, click **Edit**. The PIR opens in the editing mode.

Critical Vulnerability Exposure (PIR-002) [Update] [Cancel] [More]

Summary

Created: 21 Apr 2026 10:15
Last Modified: 27 May 2026 12:05

Category: PIR-002 Infrastructure Risk

Output Tags: CypressPreferredTagtestimonium

Priority: Critical

Status: Active

Owner: [User]

PIR Run Schedule: Daily, 09:00 UTC

Description

Track newly disclosed and actively exploited critical vulnerabilities affecting technologies in our environment. Provide early warning of exploitation in the wild, proof-of-concept availability, and estimated time-to-exploit so the Vulnerability Management team can prioritise emergency patching and the SOC can deploy detections before exploitation reaches our organisation.

Intelligence Inputs

Based on your PIR category and title, I've suggested relevant data source types for your intelligence requirements.

Observables / IOCs [x] Include indicators of compromise and observable data

Threat Models [x] Include threat actor profiles and models

Investigations [] Include related investigations and cases

Observable Times [Select All]

Threat Model Times [Select All]

Ask anything, perform tasks and get your job done

Course of Action

4. Make the necessary changes. You can edit all summary fields, PIR Description, PIR tags and keywords, Lookback Window, Intelligence Inputs, Analytical Process, and Output options.

5. Click **Update** when done.

The PIR is updated.

Running PIRs on Demand

When there's an immediate or emerging threat that can't wait for the next scheduled run, such as an active incident or newly discovered indicators, you can run a PIR on demand. To manually run a PIR, you must have the required permissions. For details, refer to ["PIR Actions and Their Required Permissions" on page 242](#).



Note:

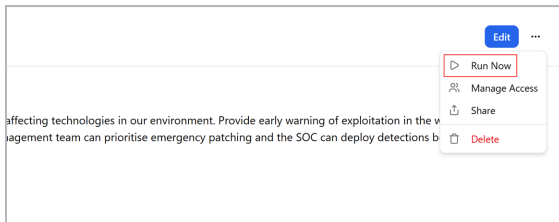
You cannot run on demand:

- Manual PIRs
- Paused Anomali AI PIRs
- Already scheduled AI PIRs

To run a PIR on demand:

1. Navigate to **ThreatStream Next Gen > Priority Intelligence Requirements**.
2. On the Priority Intelligence Requirements page, click the PIR you want to run on demand.
3. On the PIR details page, click the more options menu (...) and click **Run now**.

The following message appears: The execution is scheduled. Please check back in a few minutes for the results.



Sharing PIRs

You can share a link to a PIR with other users of your organization using one of the following ways:

- [From the Priority Intelligence Requirements page](#)
- [From the PIR details page](#)



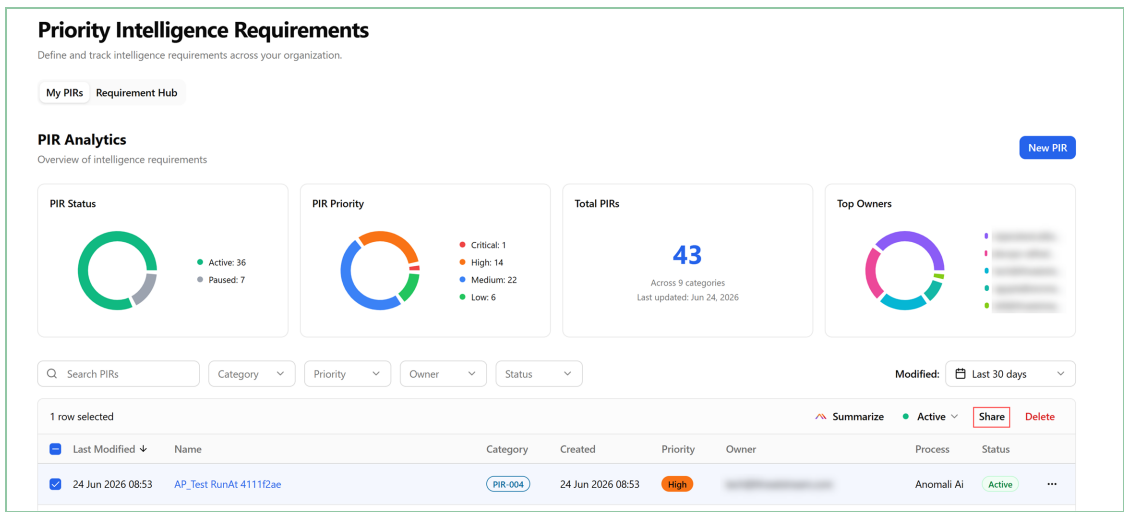
Note: Private PIRs cannot be shared.

Sharing a PIR From the Priority Intelligence Requirements Page

To share a PIR from the Priority Intelligence Requirements page:

1. Navigate to **ThreatStream Next Gen > Priority Intelligence Requirements**.
2. Select the PIR you want to share.
3. Click **Share**.

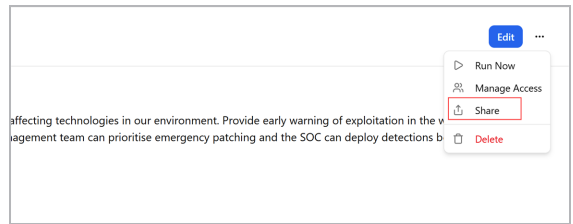
The link to the PIR is copied to the clipboard.



Sharing a PIR From the PIR Details Page

To share a PIR from the PIR details page:

1. Navigate to **ThreatStream Next Gen > Priority Intelligence Requirements**.
2. Click the PIR you want to share.
3. On the PIR details page, click the more options menu (...) and click **Share**. The link to the PIR is copied to the clipboard.



Summarizing PIRs

Use the Anomali AI-based Summarize feature to get a quick summary of any PIR in your organization. A PIR summary usually includes a clear definition of the intelligence focus and objective, explaining what is being monitored and why it matters (for example, tracking vulnerabilities above a certain severity to inform stakeholders). It also outlines how data is collected and analyzed, including sources, filters, and reporting methods.

In addition, it highlights any coverage gaps or limitations in the current setup, along with potential overlaps if multiple PIRs exist. Finally, it provides actionable insights by identifying priority areas for improvement. For example, expanding coverage, refining data sources, or increasing analytical depth.

To summarize a PIR:

1. Navigate to **ThreatStream Next Gen > Priority Intelligence Requirements**.
2. On the Priority Intelligence Requirements page, select the PIR you want to summarize.
3. Click **Summarize**.

Anomali AI starts generating a PIR summary on the left side of the screen.

Updating a PIR Status

You can update a PIR status in one of the following ways:

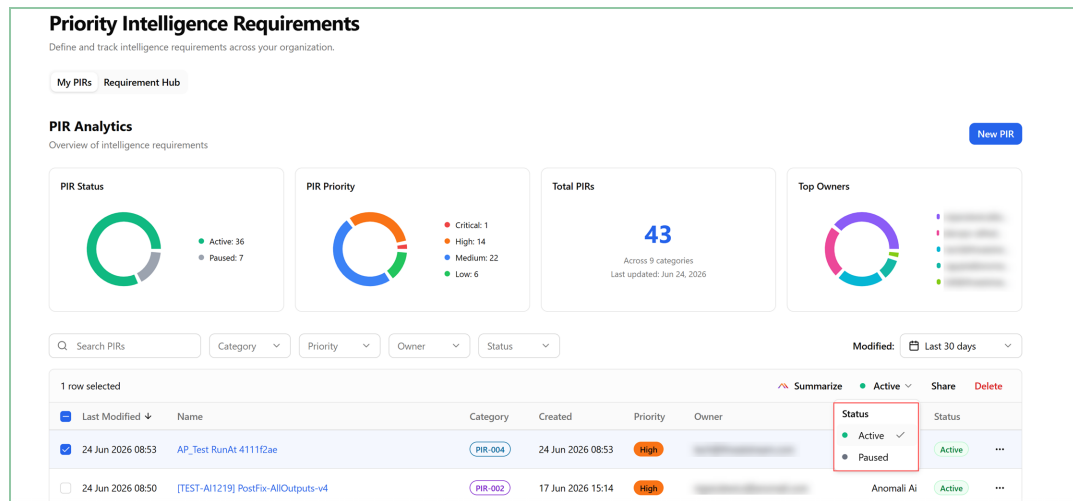
- [From the Priority Intelligence Requirements page](#)
- [From the PIR details page in the editing mode](#)

To update a PIR status, you must have the required permissions. For details, refer to ["PIR Actions and Their Required Permissions"](#) on page 242.

Updating a PIR Status From the Priority Intelligence Requirements page

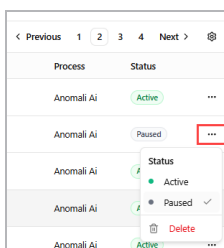
To update a PIR status from the Priority Intelligence Requirements page:

1. Navigate to **ThreatStream Next Gen > Priority Intelligence Requirements**.
2. On the Priority Intelligence Requirements page, select the PIR whose status you want to update.
3. Click **Status** and select **Active** or **Paused**.



a.

Alternatively, click the more options menu (...) and change the PIR status by clicking **Active** or **Paused** there.



Updating a PIR Status From the PIR Details Page

A PIR status can also be updated on the PIR details page in the editing mode.

To update a PIR status from the PIR details page:

1. Navigate to **ThreatStream Next Gen > Priority Intelligence Requirements**.
2. Click the PIR whose status you want to update.
3. On the PIR details page, click **Edit**.

4. In the Summary section, change the PIR status.



5. Click **Update**.

The PIR status has changed.

Deleting PIRs

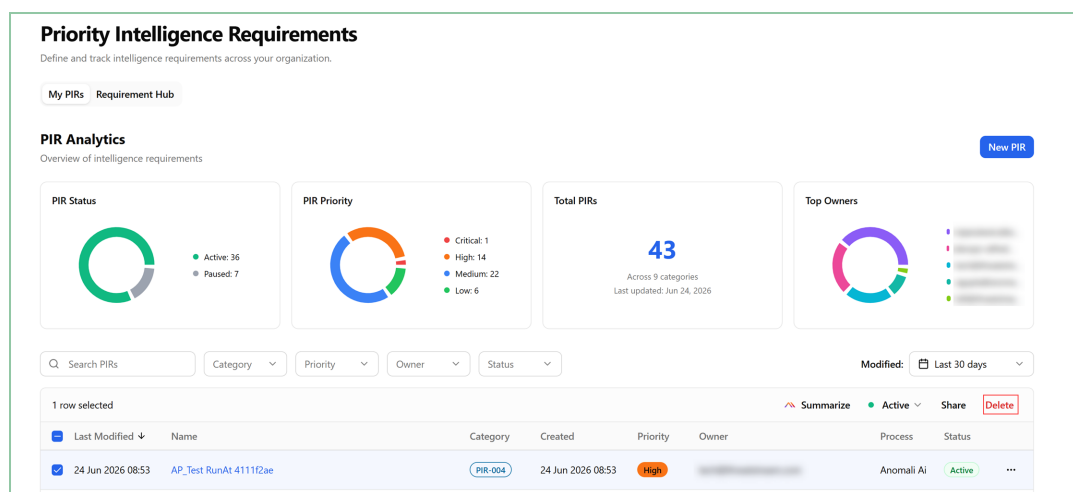
Organization Administrators and PIR owners can delete PIRs in one of the following ways:

- From the [Priority Intelligence Requirements](#) page
- From a [PIR details](#) page

Deleting PIRs From the Priority Intelligence Requirements Page

1. Navigate to **ThreatStream Next Gen > Priority Intelligence Requirements**.
2. Select one or multiple PIRs that you want to delete.
3. Click **Delete**.

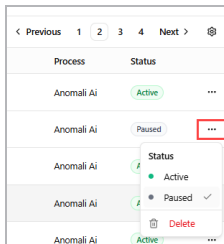
The selected PIRs are removed from the list of PIRs of your organization.



a.

Alternatively, to delete a single PIR, click the more options menu (...) of the PIR you want to delete and click **Delete**.

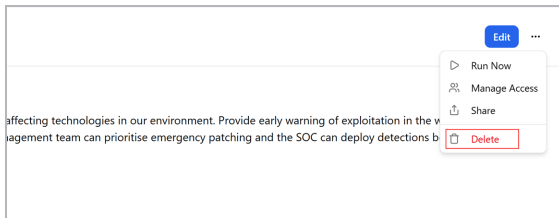
The PIR is removed from the list of PIRs of your organization.



Deleting PIRs From PIR Details Pages

To delete a PIR from the PIR details page:

1. Navigate to **ThreatStream Next Gen > Priority Intelligence Requirements**.
2. Click the PIR you want to delete.
3. On the PIR details page, click the more options menu (...) and click **Delete**.



Managing Access to PIRs



Note: PIRs that users could access before the introduction of role-based access control (RBAC) for PIRs remain accessible after the feature is enabled. During migration, the existing *Assignee* value is mapped to the *Owner* field.

PIR access is governed by two independent permission layers that both must pass:

- **PIR Permissions** determine what actions a user can perform on PIRs. For example, view, create, edit, delete, run, or pause/resume PIRs. PIR Permissions

are assigned to user roles by an Organization Administrator. A user inherits the permissions of all roles assigned to them. For details on PIR permissions that can be assigned to roles, see [Managing Roles](#).

When ThreatStream Next Gen is enabled for an organization, the following system roles are automatically assigned to users:

- **PIR Manager:** Assigned to all non-Read-Only and Read-Only users in organization that have access to ThreatStream Next Gen.
- **PIR Viewer:** Assigned to all Read-Only users in organizations that have access to ThreatStream Next Gen.

For details on the PIR Manager and PIR Manager roles, refer to [Using System Roles](#).

Organization Administrators can modify roles and permissions at any time through Role Management. See [Managing Roles](#) for details.

Roles of SSO users must be modified through the identity provider of their organization. See [Enabling User Management with Third-Party Identity Providers](#) for details.

- **Per-PIR access control level (ACL)** determines which users can access a PIR and at what level. For details, see "[PIR Actions and Their Required Permissions](#)" below and "[Managing Access to an Individual PIR](#)" on the next page.

PIR Actions and Their Required Permissions

The following table lists the available PIR actions and the required combination of permissions and ACL access levels for each action. Both requirements must be met; if either check fails, the action is denied. Users who do not have an ACL access level assigned to them cannot view the PIR.

Action	Permission Required	ACL Access Level Required
Configure sharing	N/A	PIR Owner/Organization Administrator
Create a new PIR	Create PIR Configurations	N/A
Delete a PIR	Delete PIR Configurations	PIR Owner/Organization Administrator

Action	Permission Required	ACL Access Level Required
Edit a PIR	Update PIR Configurations	PIR Owner/Write/Organization Administrator
Manually run a PIR	Run PIR Configurations	Read or Higher
Pause/resume a PIR	Pause/Resume PIR Configurations	PIR Owner/Write/Organization Administrator
Transfer ownership	N/A	PIR Owner/Organization Administrator
View a PIR and its outputs	View PIR Configurations	Read or Higher

Managing Access to an Individual PIR

To manage access to a PIR:

1. Navigate to **ThreatStream Next Gen > Priority Intelligence Requirements**.
2. Click the PIR for which you want to configure access.
3. Click the more options menu (...) and select **Manage Access**. Alternatively, click **Manage** in the Sharing & Permissions section.

The screenshot displays the ThreatStream Next Gen interface for a specific Priority Intelligence Requirement (PIR). The page is titled "What are the top threat actors affecting the Energy Industry vertical". On the left, a sidebar provides metadata for PIR-008, such as its creation and modification dates, category, output tags, priority (Medium), status (Active), owner (Jwoodward), and run schedule. The main content area shows the description, intelligence inputs, and data types. At the bottom left, a "Sharing & Permissions" section includes a "Manage" link. In the top right corner, a dropdown menu is open, showing options: "Run Now", "Manage Access" (highlighted with a red box), "Share", and "Delete".

4. In the Sharing and Permissions dialog box, change the owner if required. Note that only the PIR owner or an Organization Administrator can transfer PIR ownership.



Note: When ownership of a PIR is transferred, the new owner can perform only the actions permitted by their assigned role. For example, a user with only the View PIR Configurations permission can view the PIR but cannot edit, run, pause, or perform other actions that require additional permissions, even as the PIR owner. Although PIR owners typically have at least the Create PIR Configurations permission, verify the recipient's permissions before transferring ownership.

5. In the Visibility section, click:
 - **Private**, if you want the PIR to be visible only to the owner.
 - **Shared**, if you want to share the PIR with other users of your organization. Select which roles can access the PIR and the level of access granted to each role.

For details on permissions and ACL levels, refer to ["PIR Actions and Their Required Permissions" on page 242](#).

For details of user roles, refer to [Managing Roles](#).

Role	Read	Write
Everyone in My Organization	☒	☐
it_user_azure	☐	☐
stinltest-awsipc	☐	☐
SOC - Triage	☐	☐
SOC - Incident Responder	☐	☐
AnomaliRole_SOC - Incident Delete	☐	☐
stinltest-adminrole1	☐	☐

6. Click **Save Changes**.

Access to the PIR is updated.

Chapter 8: Case Management

This chapter covers the following topics:

Accessing Organization Cases	245
Creating a Case	248
Viewing Case Details	249
Managing Cases	256
Creating and Managing Case Types	265

Case Management in ThreatStream Next Gen gives you a built-in way to manage intelligence-driven work without ever leaving the platform. Instead of jumping between ThreatStream and external ticketing systems, you can create, assign, track, and close cases right where your intelligence already lives. This keeps your workflow streamlined and ensures that all relevant context stays in one place.

When you create a case, you can choose from configurable case types that reflect how your team operates. You can assign the case to yourself or a teammate, update its status as work progresses, and collaborate through comments. At the same time, you can link the case directly to PIRs, observables and threat models, so all supporting intelligence is preserved alongside the work you’re doing—no copying, pasting, or losing context.

Anomali AI is embedded throughout the experience to help you move faster and make better decisions. As you work on a case, Anomali AI can generate summaries on demand and recommend next steps based on the case context. For asset- or host-based cases, it can even pre-enrich the case with related data before you open it, giving you immediate context and reducing manual investigation time. In addition, Organization Administrators can define case types with built-in Anomali AI prompts that reflect standard operating procedures of your organization, so every case starts with guided, consistent actions.

Access to cases is governed by permissions and a per-case access control list, and is not the same for every case. For details on which actions require which permission and access level, see Managing Access to Cases.

Accessing Organization Cases

The **Case Management** page acts as a central workspace where you can view, filter, create, and manage cases, while also tracking key attributes such as case status, priority, case type, and ownership.

To access your organization cases, navigate to **ThreatStream Next Gen > Investigation & Analysis > Case Management**.

Case Management
Track and manage cases across your organization.

Cases Case Intelligence

Latest Cases
Recently created cases listed below

30 Apr 2026
E2E CM-2 NoPriority 1777582547299
Open Low

30 Apr 2026
E2E Test Case 1777582493185
Open High

30 Apr 2026
test tags creation
Open Medium

30 Apr 2026
E2E CM-2 NoPriority 1777531264770
Open Low

Q Search Cases Assignee Type Priority Status Modified: All time

Items per page: 10 1-10 of 733 Results

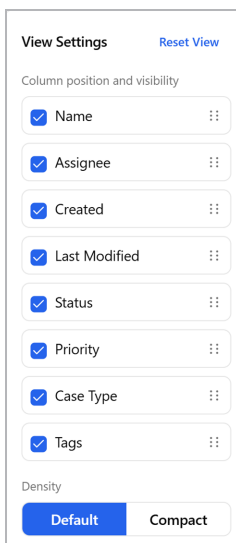
Name	Assignee	Created	Last Modified	Status	Priority	Case Type	Tags
Suspicious Phishing Email Campaign	Investigator	20 Apr 2026	01 May 2026	Open	High	Phishing Investigation	CypressPreferredTagadstringo Cypress pecto +1
E2E CM-2 NoPriority 1777582547299	Investigator	30 Apr 2026	01 May 2026	Open	Low	Compromised Credentials_Test	Cypress aeternus Cypress deleo +3
test tags creation	Investigator	30 Apr 2026	30 Apr 2026	Open	Medium	Compromised Credentials	Cypress curto Cypress pecto +3
E2E Test Case 1777582493185	Investigator	30 Apr 2026	30 Apr 2026	Open	High	Compromised Credentials_Test	—
E2E CM-2 NoPriority 1777531264770	Investigator	30 Apr 2026	30 Apr 2026	Open	Low	Compromised Credentials_Test	Cypress aeternus Cypress deleo +4
E2E Test Case 1777531222589	Investigator	30 Apr 2026	30 Apr 2026	Open	High	Compromised Credentials_Test	—
E2E CM-2 NoPriority 1777444888728	Investigator	29 Apr 2026	29 Apr 2026	Open	Low	Compromised Credentials_Test	—
E2E Test Case 1777444843021	Investigator	29 Apr 2026	29 Apr 2026	Open	High	Compromised Credentials_Test	—
E2E CM-2 NoPriority 1777417228136	Investigator	28 Apr 2026	28 Apr 2026	Open	Low	Compromised Credentials_Test	—
E2E Test Case 1777417177988	Investigator	28 Apr 2026	28 Apr 2026	Open	High	Compromised Credentials_Test	—

Items per page: 10 1-10 of 733 Results

+ Ask anything, perform tasks and get your job done

- 1 Case Intelligence:** Create and manage case types. For details, see "[Creating and Managing Case Types](#)" on page 265.
- 2 Latest Cases:** View the last cases created by your organization members, their status, priority, and date created.
- 3 Search & Filter Cases:**
 - Search:** Search cases by their names. The search is case insensitive and updates incrementally.
 - Assignee:** Filter cases by the user to whom they are assigned.

- **Type:** Filter cases by their type. To learn more about case types, see "[Creating and Managing Case Types](#)" on page 265.
 - **Priority:** Filter cases by their priority—Critical, High, Medium, and Low.
 - **Status:** Filter cases by their status—Open, In Progress, and Closed.
- 4 Name:** Name of the case.
 - 5 Assignee:** User assigned to this case.
 - 6 Created:** Timestamp of when the case was created.
 - 7 Last Modified:** Timestamp of when the case was last modified.
 - 8 Status:** Status of the case. Possible values include Open, In Progress, and Closed.
 - 9 Priority:** Priority of the case. Possible values include Critical, High, Medium, and Low.
 - 10 Case Type:** Type assigned to the case.
 - 11 Tags:** Tags assigned to the case during the case creation.
 - 12 View Settings:** Select the columns and table density (default or compact) to be displayed. By clicking the drag handle icon (⋮), drag and drop columns to change their position in the table. To return the view back to its default settings, click **Reset View**.



The screenshot shows a 'View Settings' dialog box with a 'Reset View' link. It contains two sections: 'Column position and visibility' and 'Density'. The first section lists columns with checkboxes and drag handles: Name, Assignee, Created, Last Modified, Status, Priority, Case Type, and Tags. The second section has two buttons: 'Default' (selected) and 'Compact'.

- 13 More options menu (...):**

- **View:** View case details. See "[Viewing Case Details](#)" on the next page for details.
- **Edit:** Edit the case. See "[Editing Cases](#)" on page 257 for details.
- **Delete:** Delete the case. See "[Deleting Cases](#)" on page 263 for details.

14 Modified: Select a time range for cases to be displayed. By default, all cases ever created within your organization are displayed.

Possible values include: Last 24 hours, Last 7 days, Last 30 days, Last 90 days, This year, and Custom.

15 New Case: Create a new case. See "[Creating a Case](#)" below for details.

Creating a Case

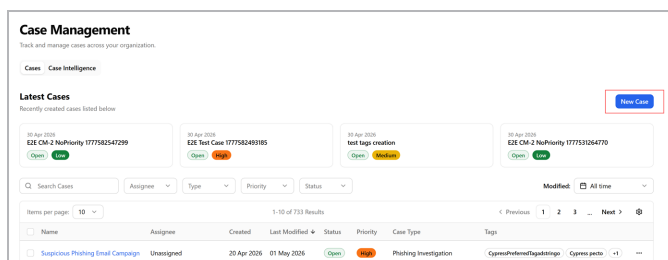
All organization users can create cases.



Note: Case types must be created by your Organization Administrator prior to creating cases. See "[Creating and Managing Case Types](#)" on page 265 for details.

To create a new case:

1. Navigate to **ThreatStream Next Gen > Investigations & Analysis > Case Management**.
2. On the Case Management page, click **New Case**.



3. In the Create New Case dialog box that opens, enter a unique case name.
4. (Optional) Provide a description for the case.
5. Select a case type.

6. (Optional) Select a user to whom you want to assign the case investigation.
7. Select a case priority—Critical, High, Medium, or Low. By default, Low priority is assigned.
8. (Optional) Select the tags you want to assign from the preferred list of tags, or add custom tags by entering a tag name and clicking +.

The screenshot shows a 'Create New Case' modal window. At the top, it says 'Create a new case with the details below. [Learn more](#)'. The form contains several fields: 'Case Name' with the value 'Suspicious Phishing Email Campaign_May'; 'Description' with a detailed text about a phishing campaign; 'Case Type' set to 'Phishing Investigation'; 'Assign To' set to 'Select assignee'; 'Priority' set to 'High'; and 'Tags' with 'phishing' selected and added as a tag. At the bottom right are 'Cancel' and 'Create Case' buttons.

9. Click **Create Case**.

The new case is created and added to the list of organization cases visible to all users.

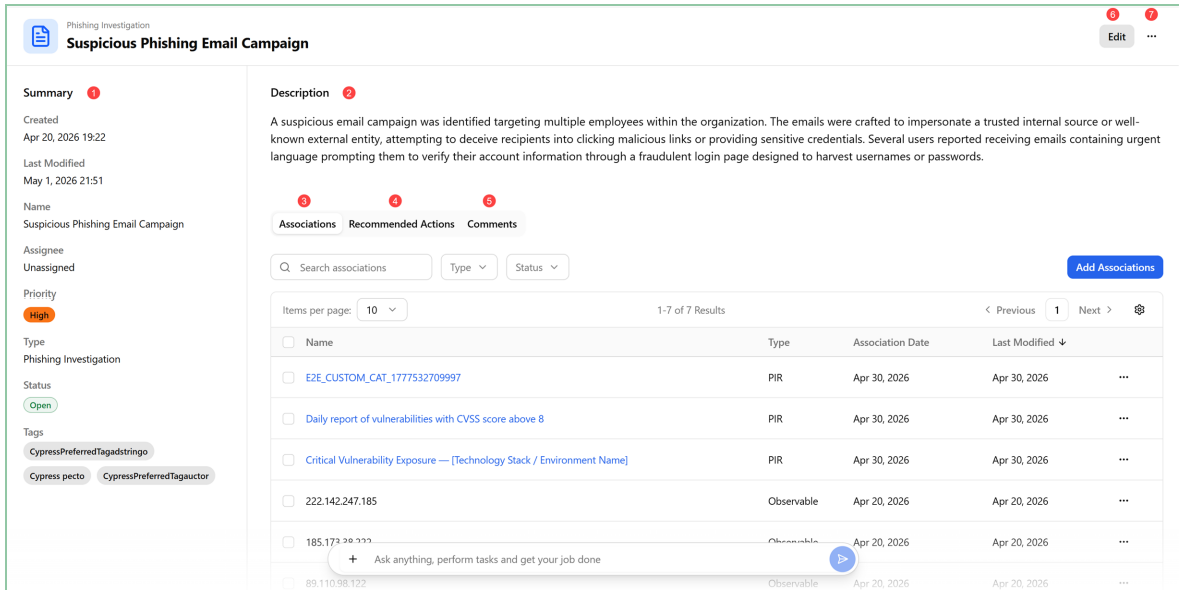
Viewing Case Details

On the Case Management page, you can click any of the listed cases to view its details.

On **case details** pages, you can view a case summary, description, priority, type, status, assignee, assigned tags, associated PIRs, observables, threat models, recommended actions, and comments from users in your organization. On a case details page, you can also add and manage case associations, generate or

manually add recommended actions, edit case information, and take key actions such as summarizing, sharing, exporting, or deleting a case.

Below is an example of the Suspicious Phishing Email Campaign case.



1 Summary: Every case summary includes the following details:

Attribute	Description
Created	Timestamp of when the case was created.
Last Modified	Timestamp of when the case was last modified.
Name	Name of the case.
Assignee	User to whom the case is assigned for analysis.
Priority	Priority of the case. Possible values include Critical, High, Medium, or Low.
Type	Type associated with the case.

Attribute	Description
Status	Case status. Possible values include: Open—The case has been created but work hasn't started yet. It's waiting to be picked up or assigned. In Progress—The case is actively being investigated or worked on by an analyst. Closed—The case has been completed. All required actions or investigations are finished, and no further work is expected.
Tags	Displays the tags assigned to this case.

2 Description: Description of the case.

3 Associations: View all intelligence and records associated with this case and add more associations. This may include PIRs, cases, observables, threat models, and investigations that are present in your ThreatStream environment. Use the search functionality and filtering options to locate the associations you need.

To learn how to add associations to a case, see ["Adding Associations to Cases" on page 253](#).

To learn how to summarize, share, and delete associations, see ["Managing Case Associations" on page 254](#).

AssociationsRecommended ActionsComments

Q Search associations

Type▼Status▼

Add Associations

Items per page: 10▼

1-7 of 7 Results

< Previous1Next >

☐ Name	Type	Association Date	Last Modified ↓	
☐ E2E_CUSTOM_CAT_1777532709997	PIR	Apr 30, 2026	Apr 30, 2026	---
☐ Daily report of vulnerabilities with CVSS score above 8	PIR	Apr 30, 2026	Apr 30, 2026	---
☐ Critical Vulnerability Exposure — [Technology Stack / Environment Name]	PIR	Apr 30, 2026	Apr 30, 2026	---
☐ 222.142.247.185	Observable	Apr 20, 2026	Apr 20, 2026	---
☐ 185.173.38.222	Observable	Apr 20, 2026	Apr 20, 2026	---
☐ 89.110.96.122	Observable	Apr 20, 2026	Apr 20, 2026	---
☐ Test	PIR	Apr 20, 2026	Apr 20, 2026	---

Items per page: 10▼

1-7 of 7 Results

< Previous1Next >

+

Ask anything, perform tasks and get your job done

🔍

4 Recommended Actions: View actions recommended by Anomali-AI based on the case type and add new actions. To learn how to add an action, see ["Adding Actions to Cases"](#) on page 254.

AssociationsRecommended ActionsComments

Recommended Actions

Actions derived from case findings and analysis

GenerateAdd Action

Phishing Investigation

Pending▼---

Analyze phishing indicators, identify affected users, check email headers, quarantine malicious emails, and recommend user awareness training.

If necessary to edit, copy or delete an action, click the more options menu (...) and select the corresponding menu item.

Pending▼...

Edit

Copy

Delete

5 Comments: View and add comments related to the case. Note that you can edit or delete only the comments you have added.

AssociationsRecommended ActionsComments

Comments & Activity

TE

B / 5 H1 H2

≡ / E

🔗

Comment

Cancel

6 Edit: Click **Edit** to modify the case. You can modify case name, assignee, case priority, type, status, and description. Furthermore, you can add or delete case

associations, add, modify, or delete recommended actions, and add comments to the case.

Click **Update** when done.

7 Case actions. You can take the following actions from the case details pages.

- **Summarize:** Click **Summarize** to generate a summary of the case.
- **Share:** Click **Share** to copy the link to the case to clipboard. For details, see ["Sharing Cases \(Coming Soon\)" on page 260](#).
- **Export:** Click **Export** to save the case details in the PDF format. For details, see ["Exporting Cases" on page 262](#).
- **Delete:** Click **Delete** if you want to delete the case. For details, see ["Deleting Cases" on page 263](#).

Adding Associations to Cases

On the Associations tab of a case details page, you can link existing PIRs, cases, observables, threat models, and investigations from your ThreatStream environment to the case.

To add an association:

1. On the Associations tab of a case, click **Add Associations**.
2. In the add Associations dialog box that opens, select an object type—PIR, Case, Observable, Threat Model, or Investigation. Use the Search functionality and the Status filter to locate the objects you need.

Add Associations
Select objects to associate with this case

Object Type
Observable

Search... Status

Items per page: 10 1-10 of 63421519 Results < Previous 1 Next > ⚙

☐	Name	Status	Last Modified
☐	89.110.98.122	Active	Apr 20, 2026
☐	185.173.38.222	Active	Apr 20, 2026
☐	222.142.247.185	Active	Apr 20, 2026
☐	43.248.173.97	Active	Apr 20, 2026
☐	59.177.100.107	Active	Apr 20, 2026
☐	119.400.176.130	Active	Apr 20, 2026

Cancel Add

3. Select the objects you want to associate with the case.

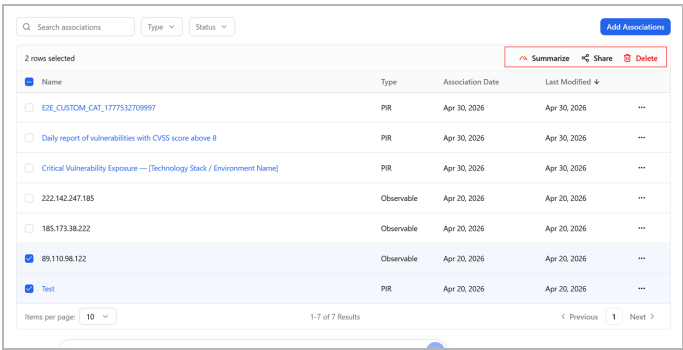
4. Click **Add**.

The associations are added to the case.

Managing Case Associations

By selecting associations of your interest, you can apply the following actions to them by clicking the corresponding action button:

- **Summarize** (applicable to PIRs only)
- **Share** the link to the association
- **Delete** associations



The screenshot shows a table titled 'Case Associations' with columns: Name, Type, Association Date, and Last Modified. There are 7 rows of data. The first three rows are PIRs, and the last four are Observables. The 'Test' row is selected. Above the table, there are filters for 'Search associations', 'Type', and 'Status'. To the right of the table, there are three buttons: 'Summarize' (with a funnel icon), 'Share' (with a link icon), and 'Delete' (with a trash icon). The 'Summarize' button is highlighted with a red box.

Name	Type	Association Date	Last Modified
☐ E2E_CUSTOM_CAT_1777532709997	PIR	Apr 30, 2026	Apr 30, 2026
☐ Daily report of vulnerabilities with CVSS score above 8	PIR	Apr 30, 2026	Apr 30, 2026
☐ Critical Vulnerability Exposure — [Technology Stack / Environment Name]	PIR	Apr 30, 2026	Apr 30, 2026
☐ 222.142.247.185	Observable	Apr 20, 2026	Apr 20, 2026
☐ 185.173.38.222	Observable	Apr 20, 2026	Apr 20, 2026
☒ 85.110.98.122	Observable	Apr 20, 2026	Apr 20, 2026
☒ Test	PIR	Apr 20, 2026	Apr 20, 2026

Alternatively, you can use the more actions menu (...) to view details of associations or remove them from the list of case associations.



The screenshot shows a row from the 'Case Associations' table. The 'More Actions' menu (three dots) is open, showing two options: 'Open' and 'Remove'.

☐ Daily report of vulnerabilities with CVSS score above 8	PIR	Apr 30, 2026	Apr 30, 2026	...
☐ Critical Vulnerability Exposure — [Technology Stack / Environment Name]	PIR	Apr 30, 2026	Apr 30, 2026	...

Adding Actions to Cases

If Anomali AI-generated actions are not sufficient for a case remediation, you can manually add more actions. You can click **Generate** to add Anomali AI-recommended action or add them manually.

To add Anomali AI-recommended actions:

1. On the Recommended Actions tab of a case, click **Generate**. Anomali AI generates the list of recommended actions which include an action name,

description, and rationale (optionally).

The screenshot displays the 'Recommended Actions' tab in the Anomali ThreatStream interface. At the top, there are three tabs: 'Associations', 'Recommended Actions', and 'Comments'. Below the tabs, the 'Recommended Actions' section is titled 'Recommended Actions' with a subtitle 'Actions derived from case findings and analysis'. There are two buttons: 'Generate' and 'Add Action'. The main content area lists three actions, each with a title, a description, a rationale, and a status dropdown menu set to 'Pending'.

Action Title	Description	Rationale	Status
Phishing Investigation	Analyze phishing indicators, identify affected users, check email headers, quarantine malicious emails, and recommend user awareness training.		Pending
Block Malicious URLs and IPs in Security Controls	Immediately add the identified phishing URLs and associated IPs (222.142.247.185, 185.173.38.222, 89.110.98.122) to email, web proxy, and firewall blocklists. Confirm blocks are active and monitor for related traffic.	Blocking known malicious infrastructure prevents further user exposure and lateral movement, reducing the risk of credential compromise.	Pending
Reset Credentials for Impacted Users	Identify users who interacted with the phishing emails or entered credentials. Force password resets and review for unauthorized access. Notify users of the reset and provide guidance on secure password practices.	Compromised credentials are a primary risk; resetting them quickly limits attacker access and potential escalation.	Pending

2. (Optional) Select an action status:

Pending—If the action has been created but not yet been started.

In Progress—If the action is currently being actively worked on by an assigned analyst.

Completed—If the action has been fully carried out. The expected outcome has been achieved and no further work is needed for this specific action.

Dismissed—If the action has been reviewed and determined to be unnecessary or irrelevant to the case.

3. (Optional) Using the more actions menu (...), take the following actions:

Edit—If you need to modify name, description, or rationale of an action.

Copy—If you need to copy an action to a clipboard.

Delete—If you need to delete an action.

To add an action manually:

1. On the Recommended Actions tab of a case, click **Add Action**.
2. In the dialog box that opens, enter a name and description for the action.

Recommended Actions
Actions derived from case findings and analysis

Generate Add Action

Isolate affected accounts Pending

Suspend or lock any user accounts that clicked the malicious link or submitted credentials to prevent further unauthorized access.

Rationale (optional)

Update Cancel

3. (Optional) Provide a rationale for adding this action.

4. Select one of the following action statuses:

Pending—If the action has been created but not yet been started.

In Progress—If the action is currently being actively worked on by an assigned analyst.

Completed—If the action has been fully carried out. The expected outcome has been achieved and no further work is needed for this specific action.

Dismissed—If the action has been reviewed and determined to be unnecessary or irrelevant to the case.

5. Click **Update**.

The action is added to the list of actions recommended for the case.

Managing Cases

You can apply the following actions to cases created within your organization:

- [Edit cases](#)
- [Share cases](#)
- [Summarize cases](#)
- [Export cases](#)
- [Delete cases](#)



Note: Only case creators, assignees, and Organization Administrators can edit and delete cases.

Editing Cases

You can edit cases in one of the following ways:

- [From the Case Management page](#)
- [From the case details page](#)



Note: Only case creators, assignees, and Organization Administrators can edit cases.

Editing Cases From the Case Management Page

To edit a case from the Case Management page:

1. Navigate to **ThreatStream Next Gen > Investigations & Analysis > Case Management**.
2. Locate the case you want to edit.
3. Click the more options menu (...) and click **Edit**. The case opens in the editing mode.

The screenshot displays the 'Case Management' interface. At the top, there's a 'Switch to Threatstream' button and user information 'AD'. Below, the 'Latest Cases' section shows four case cards: 'hkhjkh' (High), 'New Case' (Low), 'Suspicious Phishing Email Campaign' (High), and 'APT29 Campaign Analysis' (High). Each card has an 'Open' button. Below the cards are filters for 'Search Cases', 'Assignee', 'Type', 'Priority', 'Status', and 'Modified'. A table lists the cases, with 'New Case' selected. A context menu is open for the 'New Case' row, showing 'View', 'Edit', and 'Delete' options. The 'Edit' option is highlighted.

Name	Assignee	Created Date	Last Modified Date	Status	Priority	Case Type
hkhjkh	readonly600@threatstream.com	20 Apr 2026	20 Apr 2026	Open	High	Ransomware Response
New Case	Unassigned	20 Apr 2026	20 Apr 2026	Open	Low	Incident Response
Suspicious Phishing Email Campaign	Unassigned	20 Apr 2026	20 Apr 2026	Open	High	Phishing Investig
APT29 Campaign Analysis	qa_ds@threatstream.com	20 Apr 2026	20 Apr 2026	Open	High	Ransomware Res

4. Make the required changes. You can modify case name, assignee, case priority, type, status, and description. Furthermore, you can add or delete case

associations, add, modify, or delete recommended actions, and add comments to the case.

For details on how to add associations, see ["Adding Associations to Cases"](#) on page 253.

For details on how to add actions, see ["Adding Actions to Cases"](#) on page 254.

For details on how to edit, copy or delete actions, see [Managing Actions](#).

The screenshot shows the 'Case Management / Suspicious Phishing Email Campaign' interface. On the left is a 'Summary' sidebar with fields for Name, Assignee, Priority, Type, Status, Tags, Created, and Last Modified. The main area is titled 'Phishing Investigation' and 'Suspicious Phishing Email Campaign'. It includes a 'Description' field with a rich text editor and a description of a phishing campaign. Below the description are tabs for 'Associations', 'Recommended Actions', and 'Comments'. The 'Associations' tab is active, showing a table of associations with columns for Name, Type, Status, Association Date, and Last Modified. The table lists two associations: a 'Threat Model' and an 'Observable'.

Name	Type	Status	Association Date	Last Modified
☐ Black Basta-linked attacks target executives via Teams phishing (report--b73767829b636b78d48b246f0cc8f86c77719c8176bd1045babd20c1955b4964)	Threat Model		Apr 20, 2026	Apr 20, 2026
☐ 222.142.247.185	Observable		Apr 20, 2026	Apr 20, 2026

5. When done editing, click **Update**.

The case is updated successfully.

Editing Cases From the Case Details Pages

To edit a case from the case details page:

1. Navigate to **ThreatStream Next Gen > Investigations & Analysis > Case Management**.
2. Locate and click the case you want to edit. The case details page opens.
3. Click **Edit**. The case opens in the editing mode.

Case Management / Suspicious Phishing Email Campaign Switch to Threatstream AD

Summary

Name
Suspicious Phishing Email Campaign

Assignee
Unassigned

Priority
High

Type
Phishing Investigation

Status
Open

Tags
None

Created
Apr 20, 2026 19:22

Last Modified
Apr 21, 2026 01:54

Suspicious Phishing Email Campaign Edit ...

Description

A suspicious email campaign was identified targeting multiple employees within the organization. The emails were crafted to impersonate a trusted internal source or well-known external entity, attempting to deceive recipients into clicking malicious links or providing sensitive credentials. Several users reported receiving emails containing urgent language prompting them to verify their account information through a fraudulent login page designed to harvest usernames or passwords.

Associations **Recommended Actions** **Comments**

Search associations Type Status Add Associations

Items per page: 10 1-5 of 5 Results < Previous 1 Next > ⚙

☐	Name	Type	Status	Association Date	Last Modified	
☐	Black Basta-linked attacks target executives via Teams phishing (report--b73767829b636b78d48b246f0cc8f86c77719c8176bd1045bad20c1955b4964)	Threat Model		Apr 20, 2026	Apr 20, 2026	...
☐	222.142.247.185	Observable		Apr 20, 2026	Apr 20, 2026	...
☐	185.173.38.222	Observable		Apr 20, 2026	Apr 20, 2026	...
☐	89.110.98.122	Observable		Apr 20, 2026	Apr 20, 2026	...

4. Make the required changes. You can modify case name, assignee, case priority, type, status, and description. Furthermore, you can add or delete case associations, add, modify, or delete recommended actions, and add comments to the case.

For details on how to add associations, see ["Adding Associations to Cases" on page 253](#).

For details on how to add actions, see ["Adding Actions to Cases" on page 254](#).

For details on how to edit, copy or delete actions, see [Managing Actions](#).

Case Management / Suspicious Phishing Email Campaign

Switch to Threatstream

Summary

Name: Suspicious Phishing Email Campaign

Assignee: Unassigned

Priority:

Type: Phishing Investigation

Status: Open

Tags: None

Created: Apr 20, 2026 19:22

Last Modified: Apr 20, 2026 19:22

Phishing Investigation

Suspicious Phishing Email Campaign

Description

A suspicious email campaign was identified targeting multiple employees within the organization. The emails were crafted to impersonate a trusted internal source or well-known external entity, attempting to deceive recipients into clicking malicious links or providing sensitive credentials. Several users reported receiving emails containing urgent language prompting them to verify their account information through a fraudulent login page designed to harvest usernames and passwords.

Associations Recommended Actions Comments

Search associations Type Status Add Associations

Items per page: 10 1-5 of 5 Results < Previous 1 Next >

Name	Type	Status	Association Date	Last Modified
Black Basta-linked attacks target executives via Teams phishing (report--b73767829b636b78d48b246f0cc886c77719c8176bd1045babd20c1955b4964)	Threat Model		Apr 20, 2026	Apr 20, 2026
222.142.247.185	Observable		Apr 20, 2026	Apr 20, 2026

5. When done editing, click **Update**.

The case is updated successfully.

Sharing Cases (Coming Soon)

You can share a link to a case with other users of your organization.

To share a case:

1. Navigate to **ThreatStream Next Gen > Investigations & Analysis > Case Management**.
2. Locate and click the case you want to edit. The case details page opens.
3. Click the more options menu (...) and select **Share**. The shareable link to the case is copied to clipboard.



Summarizing Cases

You can generate a short summary of every case created within your organization. A generated summary includes a high-level overview of the case, such as its status, priority, and assignee, along with a concise analysis of the threat or incident. It highlights key observations, recommended actions, and relevant associations. It

also calls out any gaps or unclear information and concludes with an overall assessment of risk and next steps.

You can generate a case summary in one of the following ways:

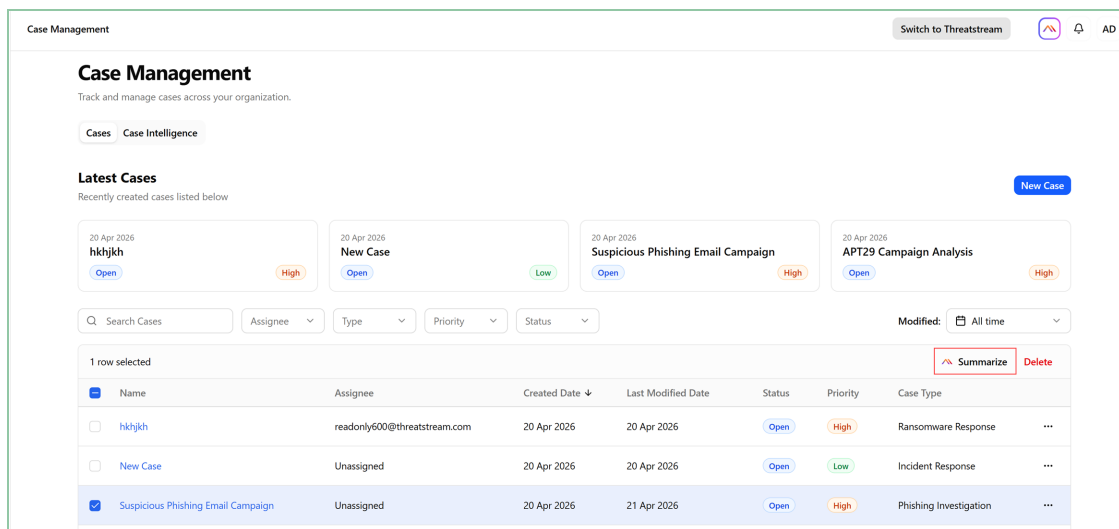
- [From the Case Management page](#)
- [From the case details pages](#)

Summarizing Cases From the Case Management Page

To summarize a case from the Case Management page:

1. Navigate to **ThreatStream Next Gen > Investigations & Analysis > Case Management**.
2. Locate and select the case you want to summarize.
3. Click **Summarize**.

The Security Case Analysis Summary is created.



Summarizing Cases From the Case Details Pages

To summarize a case from a case details page:

- a. Navigate to **ThreatStream Next Gen > Investigations & Analysis > Case Management**.
- b. Locate and click the case you want to summarize.

c. Click **Summarize**.

The Security Case Analysis Summary is created.

Below is an example of the case summary generated by Anomali AI.

Security Case Analysis Summary

Case 1: Suspicious Phishing Email Campaign

Overview

A high-priority, open case involves a sophisticated phishing campaign targeting multiple employees. The attackers impersonate trusted internal or external entities, using urgent language to pressure recipients into clicking malicious links or submitting credentials on fraudulent login pages. The campaign aims to harvest usernames and passwords, posing a significant risk of unauthorized access.

Threat Analysis

- **Attack Vector:** Email phishing, leveraging social engineering and impersonation tactics.
- **Targets:** Multiple employees across the organization.
- **Malicious Infrastructure:** Three specific IP addresses (222.142.247.185, 185.173.38.222, 89.110.98.122) are associated with the campaign, indicating a coordinated effort.
- **Tactics:** Use of urgency and authority in messaging to increase the likelihood of user interaction.
- **Potential Impact:** Credential compromise, unauthorized access, lateral movement, and possible data exfiltration.

Current Status

- **All recommended actions are pending.** No mitigation steps have been completed yet.
- **No assignee is currently handling the case.**
- **Associations:** The campaign is linked to tactics observed in Black Basta-related attacks, specifically targeting executives via phishing (as per the referenced tip report).

Gaps / Unclear Information

- **Scope of Impact:** The exact number of affected users and whether any credentials have already been compromised is not specified.
- **User Interaction:** It is unclear how many users, if any, have clicked the links or entered credentials.
- **Forensic Evidence:** No details on collected evidence or analysis results are provided.
- **Pirconfiguration:** The relevance of the "Test" configuration is not explained.

Recommendations (Pending)

1. **Phishing Investigation:** Analyze indicators, identify affected users, and enhance user awareness.
2. **Block Malicious Infrastructure:** Add identified URLs and IPs to blocklists and monitor for related activity.
3. **Credential Reset:** Force password changes for impacted users and review for unauthorized access.
4. **Evidence Preservation:** Collect and preserve all relevant emails, headers, and network logs for further analysis and potential legal action.

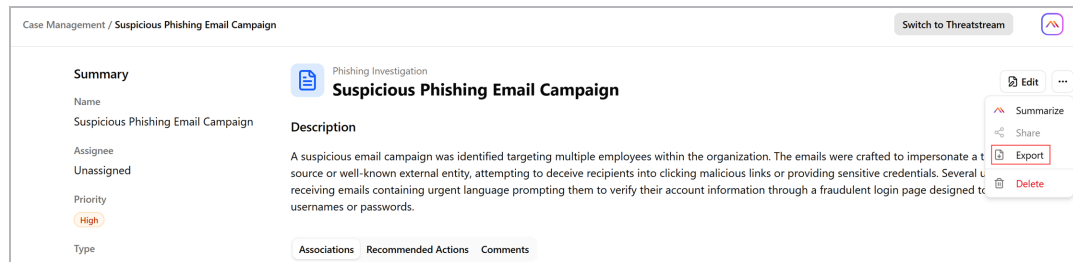
Conclusion:

This case represents an active and credible phishing threat with potential links to known threat actor tactics. Immediate action is required to contain the threat, assess the scope of compromise, and prevent further credential harvesting. The lack of an assigned responder and pending status of all actions increases organizational risk. Further information is needed to clarify the extent of user impact and evidence collected.

Exporting Cases

You can export cases in PDF format.

1. **To export a case:**
 - a. Navigate to **ThreatStream Next Gen > Investigations & Analysis > Case Management**.
 - b. Locate and click the case you want to export.
 - c. On the case details page, click the more options menu (...) and select **Export**. The downloading process starts immediately.



Deleting Cases

Organization Administrators, case creators and case assignees can delete cases. Cases can be deleted in the following ways:

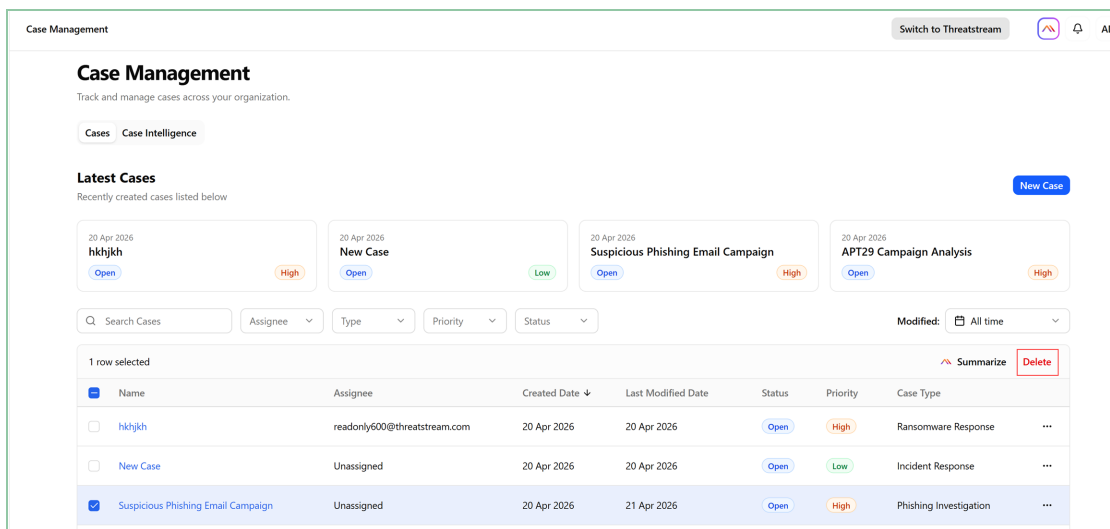
- [From the Case Management page](#)
- [From the case details pages](#)

Deleting Cases From the Case Management Page

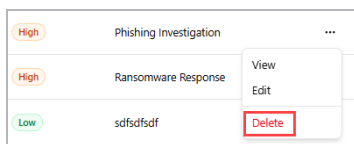
To delete a case from the Case Management page:

1. Navigate to **ThreatStream Next Gen > Investigations & Analysis > Case Management**.
2. Locate and select the case you want to delete.

3. Click **Delete**.



Alternatively, click the more options menu (...) of the case you want to delete and click **Delete**.



The case is successfully deleted.

Deleting Cases From Case Details Pages

To delete a case from the case details page:

1. Navigate to **ThreatStream Next Gen > Investigations & Analysis > Case Management**.
2. Locate the case you want to delete.
3. On the case details page, click the more options menu (...) and click **Delete**.



The case is successfully deleted.

Creating and Managing Case Types



Note: The Case Intelligence tab is visible only to Organization Administrators.

On the **Case Intelligence tab** of the Case Management page, you can create case types for your organization. Case types in your environment are fully customizable, which means you define the categories that best match your workflows and security operations of your organization. As an Organization Administrator, you can create and manage these case types from scratch. There are no predefined (out-of-the-box) options, therefore everything is tailored to your needs.

Each case type includes a built-in Anomali AI prompt field where you can embed your standard operating procedures (SOPs) or recommended actions. When a case is created under a specific type, Anomali AI uses this prompt to generate context-aware guidance, helping you respond consistently and efficiently based on your internal processes.

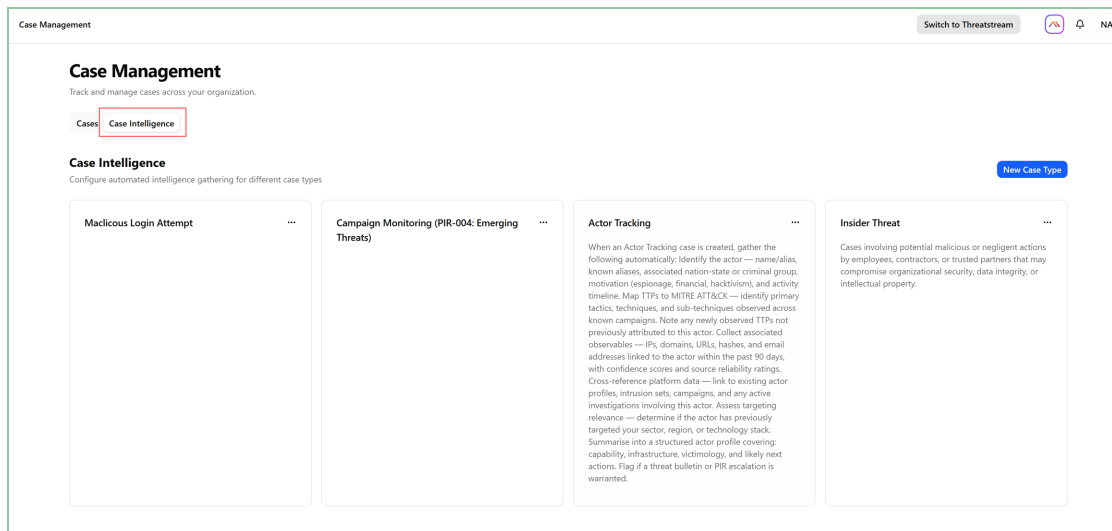
These case types are private to your organization, allowing you to safely align them with your internal terminology and workflows.

Creating Case Types

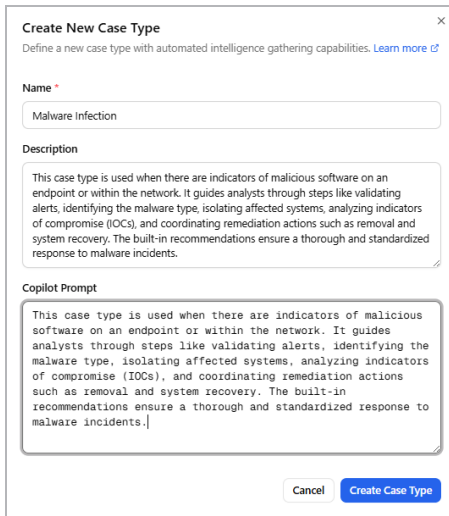
Case types act as predefined response framework for various categories of threats (for example, phishing, malware, or insider threats). By assigning a case type, you immediately define what the case is about, what kind of investigation it requires, and how it needs to be handled. This ensures that similar incidents are treated in a consistent, repeatable way across the team.

To create a case type:

1. Navigate to **ThreatStream Next Gen > Investigations & Analysis > Case Management**.
2. On the Case Management page, click **Case Intelligence**.



3. On the Case Intelligence tab, click **New Case Type**.
4. In the Create New Case Type dialog box, enter a unique name for the case type.
5. (Optional) Enter a case type description.
A good case type description helps users of your organization to quickly understand when to use this case type and what it's meant to cover. It should tell what kinds of alerts or situations fall into it, so they don't have to guess. It also provides the key things they should focus on during investigation and the standard steps they are expected to follow to respond and remediate.
6. Enter an AI-prompt for the case.
AI prompts in case types define how Anomali AI behaves when helping users work on a case of this type. They act as embedded playbooks that tell Anomali AI what your standard operating procedures are for that specific type of incident. For examples of case types descriptions and prompts, refer to ["Examples of Case Types" on page 268](#).



Create New Case Type

Define a new case type with automated intelligence gathering capabilities. [Learn more](#)

Name *

Malware Infection

Description

This case type is used when there are indicators of malicious software on an endpoint or within the network. It guides analysts through steps like validating alerts, identifying the malware type, isolating affected systems, analyzing indicators of compromise (IOCs), and coordinating remediation actions such as removal and system recovery. The built-in recommendations ensure a thorough and standardized response to malware incidents.

Copilot Prompt

This case type is used when there are indicators of malicious software on an endpoint or within the network. It guides analysts through steps like validating alerts, identifying the malware type, isolating affected systems, analyzing indicators of compromise (IOCs), and coordinating remediation actions such as removal and system recovery. The built-in recommendations ensure a thorough and standardized response to malware incidents.

Cancel Create Case Type

7. Click **Create Case Type**.

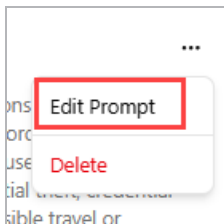
The case type is added to the case type collection of your organization.

Editing AI Prompts

If necessary, you can adjust AI prompts of case types to better guide users in creating cases.

To edit an AI prompt of a case type:

1. Navigate to **ThreatStream Next Gen > Investigations & Analysis > Case Management**.
2. On the Case Management page, click **Case Intelligence**.
3. Click the more options menu (...) of a case type you want to modify.



4. Click **Edit Prompt**.
5. In the Edit Prompt dialog box, modify the prompt.

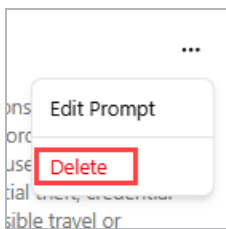
6. Click **Save Changes**.

The prompt of the case type is edited.

Deleting Case Types

To delete a case type:

1. Navigate to **ThreatStream Next Gen > Investigations & Analysis > Case Management**.
2. On the Case Management page, click **Case Intelligence**.
3. Click the more options menu (...) of a case type you want to delete.



4. Click **Delete**.
5. In the confirmation message that appears, click **Delete**.

The case type is deleted.

Examples of Case Types

The following case type examples are designed to support Cyber Threat Intelligence (CTI) operations. Each case type example includes a description and predefined AI. When added to the Case Intelligence tab, these case types can further be used for creating cases.

For details on creating case types, refer to ["Creating and Managing Case Types" on page 265](#).

For details on creating cases, refer to ["Creating a Case" on page 248](#).

Threat Actor Investigation

Description

Use this case type to investigate and monitor known or suspected actors by analyzing their infrastructure, malware, tactics, techniques, procedures (TTPs),

campaigns, and targeting behavior over time. Suitable for ongoing adversary tracking and sector-specific threat analysis.

AI Prompt

This is a Threat Actor Investigation case. Using ThreatStream, identify all associated observables, campaigns, malware families, and TTPs linked to the actor. Map identified tactics and techniques to the MITRE ATT&CK framework. Assess the targeting patterns of the actor, including industries, geographic regions, and known victims. Review intelligence confidence levels and source reliability. Identify any newly discovered or recently updated infrastructure such as IP addresses, domains, or certificates. Determine whether this actor has previously targeted our organization, industry, or partners. Generate a structured threat actor profile that includes key findings, risk assessment, recommended defensive actions, and detection opportunities.

Threat Campaign Analysis

Description

Use this case type to investigate active or historical cyber campaigns involving coordinated malicious activity, shared infrastructure, malware, or TTPs across multiple targets or organizations.

AI Prompt

This is a Threat Campaign Analysis case. Search ThreatStream for all indicators, malware families, infrastructure, and TTPs associated with this campaign. Establish the campaign timeline, initial access methods, delivery mechanisms, and operational objectives. Identify targeted sectors and geographic regions. Correlate findings with known threat actors or previously observed campaigns. Monitor for newly associated indicators or intelligence updates. Determine whether any campaign-related observables have been detected within our environment. Produce a concise campaign assessment suitable for operational security teams and intelligence stakeholders.

Emerging Threat Intelligence

Description

Use this case type when evaluating newly identified threats such as zero-day vulnerabilities, emerging malware, active exploit activity, or high-profile cyber incidents that require rapid intelligence analysis and response.

AI Prompt

This is an Emerging Threat Intelligence case. Search ThreatStream for all available intelligence related to the reported threat, including associated CVEs, malware samples, observables, affected vendors, exploit activity, and threat reports. Assess the quality, credibility, and completeness of available intelligence and identify any information gaps. Determine whether the threat is relevant to our technology stack, geographic footprint, or industry sector. Prepare a concise threat advisory summarizing current findings, affected entities, indicators to monitor, and recommended mitigation actions. Indicate whether escalation, customer notification, or a formal intelligence response is required.

Observable Enrichment and Validation

Description

Use this case type to enrich, validate, and quality-check observables before operational use, customer distribution, or integration into detection and response systems.

AI Prompt

This is an Observable Enrichment and Validation case type. For each observable associated with this case, review ThreatStream intelligence including confidence scores, severity ratings, source feeds, historical sightings, related Campaigns, and associated threat Actors. Identify false positives, low-confidence observables, or observables requiring additional verification. Flag shared or potentially benign infrastructure such as CDNs, hosting providers, or commonly used services that may require careful handling. Assess observable freshness and determine whether observables remain active or relevant. Generate a validated observable report with confidence assessments and recommended actions such as block, monitor, investigate, or discard.

Industry Threat Landscape Review

Description

Use this case type to conduct periodic intelligence assessments focused on threats affecting a specific industry sector, including adversary activity, malware trends, targeting patterns, and emerging risks.

AI Prompt

This is an Industry Threat Landscape Review case. Search ThreatStream for threat actors, campaigns, malware families, vulnerabilities, and intelligence reports targeting the specified industry sector during the selected timeframe. Identify the most active and impactful threat actors affecting the sector. Analyze common TTPs, attack vectors, and operational trends. Highlight any notable changes in targeting behavior, tooling, or campaign activity. Summarize the most significant threats relevant to the sector and provide prioritized recommendations for detection, mitigation, and monitoring. Output should be appropriate for both operational teams and executive-level intelligence reporting.

Geopolitical Cyber Threat Monitoring

Description

Use this case type to monitor cyber threats associated with geopolitical developments, nation-state operations, hacktivist activity, regional conflicts, or politically motivated cyber campaigns that may impact the organization.

AI Prompt

This is a Geopolitical Cyber Threat Monitoring case. Search ThreatStream for nation-state actors, hacktivist groups, campaigns, and threat activity associated with the specified region, country, or geopolitical event. Identify related infrastructure, malware, TTPs, and recent intelligence updates. Assess whether cyber activity has escalated or changed in response to real-world developments. Determine potential impact and relevance to the operations, partners, or regional exposure of the organization. Monitor for new threat reports, advisories, or intelligence bulletins related to this geopolitical context. Produce a situational intelligence summary that includes risk indicators, emerging concerns, and recommended monitoring priorities.

Chapter 9: Security Reporting

This chapter covers the following topics:

Accessing Organization Reports	273
Creating a Report	275
Viewing Report Details	279
Managing Reports	281
Using Report Templates	286

Reporting in ThreatStream Next Gen is where your threat intelligence work comes together into something you can share, communicate, and act on. It allows you to turn raw intelligence into clear, structured, and executive-ready reports that stakeholders across your organization can easily understand and use.

A report is a structured summary of a security issue, investigation, or intelligence topic. Depending on how it is created, a report may include an executive summary, an overview of the threat, affected assets, attribution details, targeted infrastructure, observables, a risk assessment, and recommended actions. Some reports are designed for leadership and focus on high-level insights, while others provide more detailed technical analysis for security teams.

You can create reports in several ways. Reports may be generated automatically from Priority Intelligence Requirements (PIRs), created manually to document specific investigations, or assisted by Anomali AI to streamline the process. Regardless of how they are created, all reports along with any shared with you by other organizations are centralized on the Security Reporting page. From there, you can view and manage reports based on attributes such as name, author, creation date, visibility, TLP classification, and status, making it easier to organize and track your reporting over time.

Templates play a key role in making reporting efficient and consistent. A template defines the structure of a report by organizing it into predefined sections, so you do not need to build reports from scratch. This allows you to focus on analysis rather than formatting, while ensuring that important information is consistently included. Templates also help standardize reporting across your team, making reports easier to read and compare.

ThreatStream Next Gen includes a set of ready-to-use templates, and also allows you to create custom templates tailored to the needs of your organization.

Overall, reports help security analysts transform complex and distributed threat data into clear and standardized communication. Reports support consistent reporting practices, improve efficiency, and ensure that the right level of information is

delivered to the right audience—whether technical analysts or executive stakeholders.

Accessing Organization Reports

All reports created manually or generated by PIRs within your organization are listed on the Security Reporting page. Additionally, you can also see reports shared with you by other organizations.

To learn how reports are generated from PIRs, see [Configuring PIR Outputs](#).

To access reports, navigate to **ThreatStream Next Gen > Investigation & Analysis > Reporting**.

Security Reporting
Create, manage, and share comprehensive security reports with customizable templates and collaborative workflows.

My Reports **Template Management**

Latest Reports
Recently created reports listed below

New Report

6 Jul 2026
QA Test — AI-1215 All Outputs - PIR-004 - 20260706_160143
Weekly Cyber Threat Intelligence Report - Test (Copy)

6 Jul 2026
QA Test — AI-1215 Output Validation - PIR-004 - 20260706_150420
Weekly Cyber Threat Intelligence Report - Test (Copy)

6 Jul 2026
QA Test — AI-1215 Output Validation - PIR-004 - 20260706_145452
Weekly Cyber Threat Intelligence Report - Test (Copy)

6 Jul 2026
QA Test — AI-1215 All Outputs - PIR-004 - 20260706_145417
Weekly Cyber Threat Intelligence Report - Test (Copy)

Search Reports Template Author Visibility TLP Status Tags Modified: Last 30 days

Items per page: 10 1-10 of 112 Results < Previous 1 2 3 ... Next >

☐	Last modified	Name	Template	Tags	Author	Created	Visibility	TLP	Status
☐	6 Jul 2026	QA Test — AI-1215 All Outputs - PIR-004 ...	Weekly Cyber ...	PIR-004 Emerging Threats	admin	6 Jul 2026	My Organization	TLP:AMBER	Published
☐	6 Jul 2026	QA Test — AI-1215 Output Validation - PI...	Weekly Cyber ...	PIR-004 Emerging Threats	admin	6 Jul 2026	My Organization	TLP:AMBER	Published
☐	6 Jul 2026	QA Test — AI-1215 Output Validation - PI...	Weekly Cyber ...	PIR-004 Emerging Threats	admin	6 Jul 2026	My Organization	TLP:AMBER	Published
☐	6 Jul 2026	QA Test — AI-1215 All Outputs - PIR-004 ...	Weekly Cyber ...	PIR-004 Emerging Threats	admin	6 Jul 2026	My Organization	TLP:AMBER	Published
☐	6 Jul 2026	QA Test — AI-1215 Capacity Load 01 - PI...	Weekly Cyber ...	—	admin	6 Jul 2026	My Organization	TLP:AMBER	Published
☐	6 Jul 2026	E2E Table Render Test 1783331267173	Weekly Cyber ...	—	starship_us...	6 Jul 2026	My Organization	TLP:AMBER	Draft
☐	6 Jul 2026	E2E Author Test 1783331266662	Weekly Cyber ...	—	starship_us...	6 Jul 2026	My Organization	TLP:AMBER	Draft
☐	6 Jul 2026	E2E Test Report 1783331217757	Weekly Cyber ...	—	starship_us...	6 Jul 2026	My Organization	TLP:AMBER	Draft
☐	6 Jul 2026	Critical Vulnerability Exposure — report I...	Threat Landsc...	testPIR002	mjasulewic...	6 Jul 2026	My Organization	TLP:AMBER	Published
☐	6 Jul 2026	Daily report of vulnerabilities with CVSS s...	Threat Landsc...	PIR-003 Tech Stack Risk	admin	6 Jul 2026	My Organization	TLP:AMBER	Published

Items per page: 10 1-10 of 112 Results < Previous 1 2 3 ... Next >

1 Template Management: View report templates offered by Anomali out of the box and create new templates that suit your organization needs. For details, see ["Using Report Templates" on page 286](#).

2 Latest Reports: View the most recently added reports in your organization, the templates used to create them, and their creation dates.

3 Search Reports: Search reports by their names, template, and author. The search is case insensitive and updates incrementally.

4 Template: Filter reports by the template used for their creation.

5 Author: Filter reports by their author.

6 Visibility: Filter reports by their visibility.

Possible values include:

- **Private**—report is visible only to the author.
- **My Organization**—report is visible to all organization users.
- **Anomali Community**—report is visible to all organizations that use ThreatStream Next Gen.

7 TLP: Filter reports by their TLP color. Possible values include: red, amber, green, and clear.

The TLP color provides a mechanism to communicate to report readers whether further dissemination of information in the report is allowed; if yes, how freely can this information be distributed. To learn more about TLP, search for "Traffic Light Protocol" in your favorite search engine.

8 Status: Filter reports by their status. Possible values include

- **Draft**—report is still being created or edited, and its content may be incomplete or unverified.
- **In Review**—report has been completed by the author and is undergoing validation.
- **Published**—report is finalized and approved.

9 Tags: Filter reports by the tags assigned to them. Note that if you want to filter reports by a tag that is not part of the Preferred Tags list (this includes PIR tags), you must enter the full tag value in the search field and press **Enter**.

10 Last Modified: Timestamp of when the report was last modified.

11 Name: Name of the report

12 Template: Template that was used to create the report.

- 13 Tags:** Tags associated with the report.
- 14 Author:** User who created the report.
- 15 Created:** Timestamp of when the report was created.
- 16 Visibility:** Report visibility—Private, My Organization, or Anomali Community.
- 17 TLP:** Traffic Light Protocol (TLP) associated with the report. To learn more about TLP, search for "Traffic Light Protocol" in your favorite search engine.
- 18 Status:** Status of the report.
- 19** Horizontal more options menu (...):
 - **Publish:** Publish a report. See ["Publishing a Report From the Security Reporting Page" on page 284](#) for details.
 - **View:** Click this option to view report details. For more information on report details pages, see ["Viewing Report Details" on page 279](#).
 - **Edit:** Edit a report. See ["Editing a Report From the Security Reporting Page" on page 282](#) for details.
 - **Delete:** Delete a report. See ["Deleting Reports" on page 285](#) for details.
- 20 View Settings:** Select the columns and table density (default or compact) to be displayed. By clicking the drag handle icon (⋮), drag and drop columns to change their position in the table. To return the view back to its default settings, click **Reset View**.
- 21 Modified:** Select a time range to filter reports based on when they were last updated. By default, last 30 days is selected.
Possible values include: Last 7 days, last 30 days, and last 90 days.
- 22 New Report:** Create a new report. See ["Creating a Report" below](#) for details.

Creating a Report

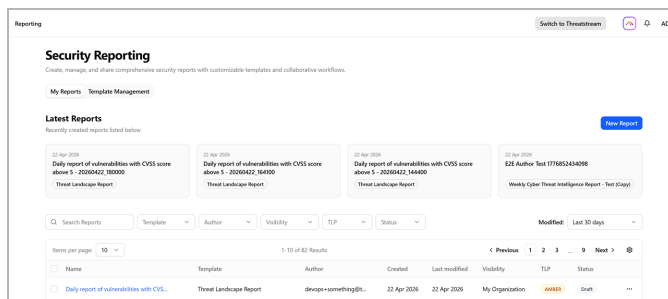
Besides the automatic generation of reports from PIRs, you can also create reports manually or with the help of Anomali AI.

To learn how to create a report with Anomali AI, see ["Creating Reports with Anomali AI" on page 277](#).

To learn how PIRs can be configured to generate automatic reports, see [Configuring PIR Outputs](#).

To manually create a new report:

1. Navigate to **ThreatStream Next Gen > Investigations & Analysis > Reporting**.



2. On the Security Reporting page, click **New Report**.
3. In the Create New Report dialog box that opens, select a template. For more information on report templates, see ["Using Report Templates" on page 286](#).
4. Enter a report name. For example, *Recent Threat Types Relevant to My Organization* or *NIMBLE SPIDER Threat Actor Updates*.
5. Select a report visibility:
 - **Private**—to make the report visible only to the author.
 - **My Organization**—to make the report visible to all organization users.
 - **Anomali Community**—to make the report visible to all users who use ThreatStream Next Gen.

By default, visibility is set to My Organization.

6. Select a Traffic Light Protocol (TLP) that should be associated with the report.

Possible values include: red, amber, green, and clear. The default value of the report is amber.

The TLP color provides a mechanism to communicate to report readers whether further dissemination of information in the report is allowed; if yes, how freely can this information be distributed.

To learn more about TLP, search for "Traffic Light Protocol" in your favorite search engine.

Learn more'. The form contains several fields: 'Template' (dropdown menu showing 'Threat Actor Report'), 'Name' (text input field with 'Daily Report of Threat Actors'), 'Visibility' (dropdown menu showing 'My Organization'), 'TLP' (dropdown menu showing 'AMBER' with a yellow circle icon), and 'Tags' (text input field with 'threat_actor_report' and a tag chip below it labeled 'threat_actor_report' with a close button). At the bottom right are 'Cancel' and 'Create Report' buttons."/>

Create New Report ×

Create a new report based on a template. Fill in the details below to get started. [Learn more](#)

Template *

Threat Actor Report

Name *

Daily Report of Threat Actors

Visibility

My Organization

TLP

AMBER

Tags

threat_actor_report

threat_actor_report ×

Cancel Create Report

7. Select or create tags to associate with the report. Tags available for selection are derived from the ThreatStream Preferred Tags list. See [Adding Preferred Tags to Intelligence](#) for more information. To add a new tag to the report, enter a tag value in the search field and click **+**. The newly created tag is displayed under the Tags field. Note that tags created within the report are not added to the list of Preferred Tags.

8. Click **Create Report**.

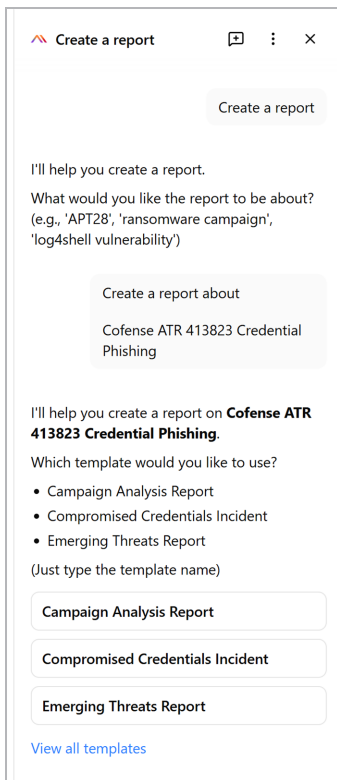
The new report is created and added to the list of organization reports visible to all users.

Creating Reports with Anomali AI

To speed up the process of report creation, you can use the Anomali AI assistant to create a report for you.

To create a report with Anomali AI:

1. Navigate to **ThreatStream Next Gen > Investigations & Analysis > Reporting**.
2. Click the Anomali AI icon () at the top right corner of your screen.
3. On the slide-out panel, click **Create Report**.
4. Tell Anomali AI what the report is about.
5. Select a report template.



The screenshot shows a slide-out panel titled "Create a report" with a close button (X) in the top right corner. Inside the panel, there is a "Create a report" button. Below it, a message says "I'll help you create a report. What would you like the report to be about? (e.g., 'APT28', 'ransomware campaign', 'log4shell vulnerability')". A text input field contains "Cofense ATR 413823 Credential Phishing". Below the input field, a message says "I'll help you create a report on **Cofense ATR 413823 Credential Phishing**. Which template would you like to use?". A list of three templates is shown: "Campaign Analysis Report", "Compromised Credentials Incident", and "Emerging Threats Report". Below the list, a note says "(Just type the template name)". Three buttons are provided for each template: "Campaign Analysis Report", "Compromised Credentials Incident", and "Emerging Threats Report". At the bottom, there is a link "View all templates".

6. Confirm a suggested report name or modify it.

The new report is created. Click the report to view its details.

Great! I'll create a **Compromised Credentials Incident** report on **Cofense ATR 413823 Credential Phishing**.

Suggested name: **Cofense Atr 413823 Credential Phishing Compromised Credentials Incident Report - 2026-04-22**

Would you like to use this name? (Type 'yes' or provide a different name)

Yes, use 'Cofense Atr 413823 Credential Phishing Compromised Credentials Incident Report - 2026-04-22'

No, use a different name

Yes, use 'Cofense Atr 413823 Credential Phishing Compromised Credentials Incident Report - 2026-04-22'

I've created your report. You can view it now.

 Cofense Atr 413823 Credential ...

Viewing Report Details

On the Security Reporting page, you can click any report to view its details. Each report includes common report attributes such as the report name, visibility, status, creation date, and last modified date, along with report content defined by the threat type and the report template or PIR used to generate it.

To learn how reports are generated from PIRs, see [Configuring PIR Outputs](#).

Below is a report example generated by a PIR.

Report name

20260715_090533

Report Author

admin

Visibility

My Organization

Report Status

AMBER

Last Modified

15 Jul 2026

Tags

PIR-003 Tech Stack Risk

Executive Summary

Between January and July 2026, a series of vulnerabilities with CVSS scores above 5 were identified across a diverse set of software products and platforms. These vulnerabilities affected widely used applications and infrastructure components, including Oracle Java SE, GIMP, ImageMagick, Glances, NGINX, the Linux kernel, Redis, Samba, JupyterLab, Palo Alto Networks, Rsyslog, and several others. The vulnerabilities ranged from remote code execution and privilege escalation to denial of service and information disclosure. Notably, several vulnerabilities had public exploits available, increasing the risk of active exploitation. The findings underscore the critical need for timely vulnerability management, asset inventory, and coordinated remediation efforts to mitigate the risk posed by these emerging threats.

Key Findings

- Multiple high-severity vulnerabilities (CVSS > 5) were identified in widely deployed software, including Oracle Java SE, GIMP, NGINX, and the Linux kernel.
- Vulnerabilities included remote code execution, privilege escalation, denial of service, information disclosure, path traversal, and cross-site scripting.
- Public exploits were available for several vulnerabilities, notably in react-native, NoofResearch hermes-agent, mastergo-design, mastergo-design, Docker, Samba, JupyterLab, Palo Alto Networks, Rsyslog, and several others.
- Vulnerabilities were found in both open-source and commercial products, affecting a broad range of industries and environments.
- Several vulnerabilities were remotely exploitable and could be leveraged by unauthenticated attackers.
- The presence of vulnerabilities in third-party and supply chain components (e.g., libraries, drivers) increases the complexity of remediation.

Threat Overview

The vulnerabilities reported between January and July 2026 present significant risks to organizations relying on affected software. Attackers could exploit these vulnerabilities to execute arbitrary code, escalate privileges, disrupt services, or exfiltrate sensitive information. The availability of public exploits for several vulnerabilities further elevates the threat level, as it lowers the barrier to entry for opportunistic and targeted attacks. The affected products are commonly used in enterprise, cloud, and development environments, amplifying the potential impact.

1 Report name.

2 Report Status.

Possible values include:

- **Draft**—report is still being created or edited, and its content may be incomplete or unverified.
- **In Review**—report has been completed by the author and is undergoing validation.
- **Published**—report is finalized and approved.

3 Report Author: User who created the report

4 Visibility: Report visibility indicating who can access this report.

Possible values include:

- **Private**—report is visible only to the author.
- **My Organization**—report is visible to all organization users.
- **Anomali Community**—report is visible to all ThreatStream Next Gen users, inside and outside of your organization.

5 TLP: Traffic Light Protocol (TLP) associated with the report. The TLP color provides a mechanism to communicate to report readers whether further dissemination of information in the report is allowed; if yes, how freely can this information be distributed.

To learn more about TLP, search for "Traffic Light Protocol" in your favorite search engine.

6 Report Date: Timestamp of when the report was created.

7 Last Modified: Timestamp of when the report was last modified.

8 Tags: Tags associated with this security report.

9 Report Text: The content of reports can vary depending on how they are created. Manually created reports typically include the sections defined by the template used at the time of creation (unless those headers have been modified or removed).

Reports generated by a PIR usually follow a more structured format. They always include an executive summary that highlights key findings such as identified threats, affected assets and the overall significance of the activity. They also contain technical details, including identified vulnerabilities, associated infrastructure, ISP information, and scan results. In addition, PIR-generated reports include a risk

assessment and recommendations, as well as PIR-specific metadata such as the PIR name, category, description, priority, tags, and the data sources used during execution.

10 Edit: Edit the report. See ["Editing a Report From the Report Details Page" on the next page](#) for details.

11 Horizontal more options menu (...):

- **Publish/Unpublish:** Publish or unpublish the report. See ["Publishing a Report From the Report Details Page" on page 284](#) for details.
- **Threat Bulletin (coming soon)**
- **Export As PDF:** Export the report to PDF. See ["Exporting Reports to PDF" on page 283](#) for details.
- **Schedule (coming soon)**
- **Share (coming soon)**

Managing Reports

You can apply the following actions to reports created within your organization:

[Edit report](#)

[Publish report](#)

Create Threat Bulletins from reports (coming soon)

[Export reports to PDF](#)

[Delete report](#)

Editing Reports



Note: Only Organization Administrators and report authors can edit reports.

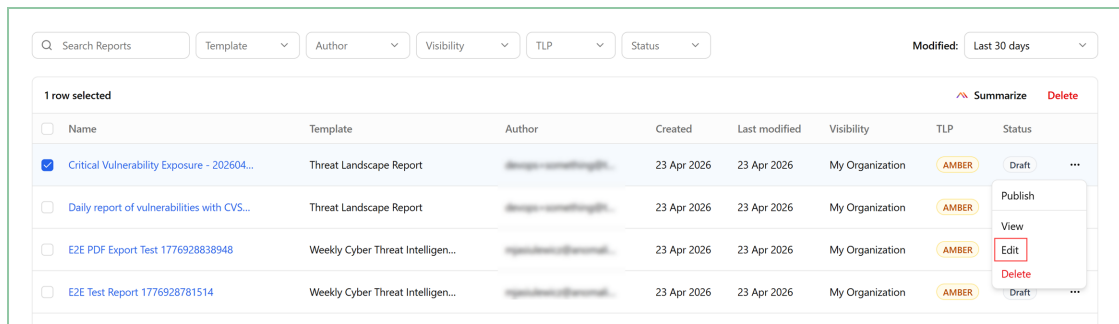
You can edit reports in one of the following ways:

- [From the Security Reporting page](#)
- [From a report details page](#)

Editing a Report From the Security Reporting Page

To edit a report from the Security Reporting page:

1. Navigate to **ThreatStream Next Gen > Investigations & Analysis > Reporting**.
2. Locate the report you want to edit and click the more options menu (...)
3. Click **Edit**. The report opens in the editing mode.



☐	Name	Template	Author	Created	Last modified	Visibility	TLP	Status
☒	Critical Vulnerability Exposure - 202604...	Threat Landscape Report	...	23 Apr 2026	23 Apr 2026	My Organization	AMBER	Draft
☐	Daily report of vulnerabilities with CVS...	Threat Landscape Report	...	23 Apr 2026	23 Apr 2026	My Organization	AMBER	
☐	E2E PDF Export Test 1776928838948	Weekly Cyber Threat Intelligen...	...	23 Apr 2026	23 Apr 2026	My Organization	AMBER	
☐	E2E Test Report 1776928781514	Weekly Cyber Threat Intelligen...	...	23 Apr 2026	23 Apr 2026	My Organization	AMBER	

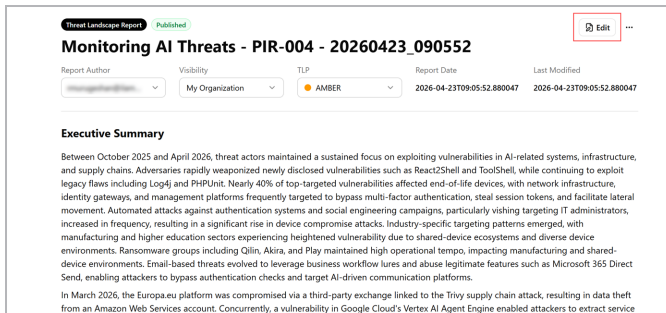
4. Make the necessary changes in the report.
5. Click **Update**.

The report is updated.

Editing a Report From the Report Details Page

To edit a report from the report details page:

1. Navigate to **ThreatStream Next Gen > Investigations & Analysis > Reporting**.
2. Click the report you want to edit.
3. On the report details page, click **Edit**.



4. Make the required changes.
5. Click **Update**.

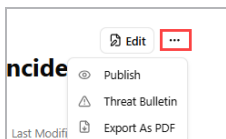
The report is updated.

Exporting Reports to PDF

All reports that are available to you can be exported to PDF.

To export a report to PDF:

1. Navigate to **ThreatStream Next Gen > Investigations & Analysis > Reporting**.
2. Click the report you want to export. The report details page opens.
3. Click the more options menu (...).



4. Click **Export As PDF**.

The downloading process starts immediately.

Publishing Reports

Report drafts that have been reviewed by required stakeholders and approved can be published.

You can publish a report in one of the following ways:

- [From the Security Reporting page](#)
- [From a report details page](#)

Publishing a Report From the Security Reporting Page

To publish a report from the Security Reporting page:

1. Navigate to **ThreatStream Next Gen > Investigations & Analysis > Reporting**.
2. Locate the report you want to publish and click the more options menu (...).



Note: You can only publish reports that are in Draft or In Progress status.

3. Click **Publish**.

Q

Search Reports

Template

▼

Author

▼

Visibility

▼

TLP

▼

Status

▼

Modified:

Last 30 days

▼

1 row selected

Summarize

Delete

☐	Name	Template	Author	Created	Last modified	Visibility	TLP	Status
☒	Critical Vulnerability Exposure - 202604...	Threat Landscape Report	...	23 Apr 2026	23 Apr 2026	My Organization	AMBER	Draft
☐	Daily report of vulnerabilities with CVS...	Threat Landscape Report	...	23 Apr 2026	23 Apr 2026	My Organization	AMBER	Publish
☐	E2E PDF Export Test 1776928838948	Weekly Cyber Threat Intelligen...	...	23 Apr 2026	23 Apr 2026	My Organization	AMBER	View
☐	E2E Test Report 1776928781514	Weekly Cyber Threat Intelligen...	...	23 Apr 2026	23 Apr 2026	My Organization	AMBER	Edit
								Delete
								Draft

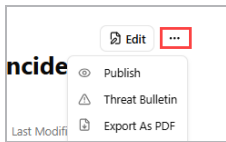
4. Click **Publish**.

The report status is changed to **Published**.

Publishing a Report From the Report Details Page

To publish a report from the report details page:

1. Navigate to **ThreatStream Next Gen > Investigations & Analysis > Reporting**.
2. Click the report you want to publish.
3. On the report details page, click the more options menu (...).



4. Click **Publish**.

The report status is changed to **Published**.

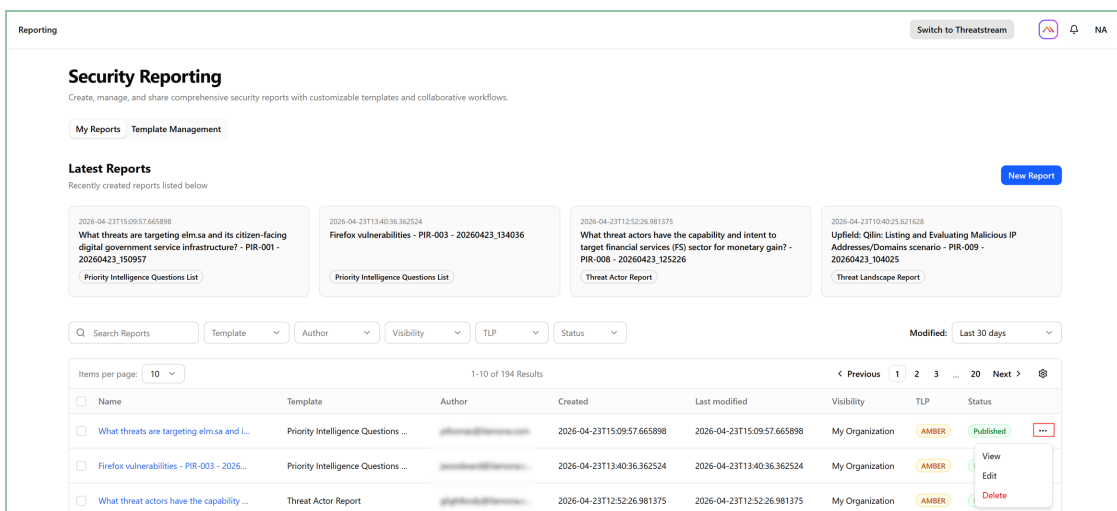
Deleting Reports

Organization Administrators and report authors can delete reports. You can delete an individual report or in bulk.

Deleting an Individual Report

To delete an individual report:

1. Navigate to **ThreatStream Next Gen > Investigations & Analysis > Reporting**.
2. Locate a report you want to delete.
3. Click the more options menu (...) and click **Delete**.



The report is deleted.

Deleting Reports in Bulks

To delete reports in bulk:

1. Navigate to **ThreatStream Next Gen > Investigations & Analysis > Reporting**.
2. Select the reports you want to delete.
3. Click **Delete**.

The reports are deleted.

Security Reporting
Create, manage, and share comprehensive security reports with customizable templates and collaborative workflows.

My Reports | Template Management

Latest Reports
Recently created reports listed below

New Report

23 Apr 2026
Critical Vulnerability Exposure - 20260423_090004
Threat Landscape Report

23 Apr 2026
Daily report of vulnerabilities with CVSS score above 5 - 20260423_090004
Threat Landscape Report

23 Apr 2026
E2E PDF Export Test 1776928838948
Weekly Cyber Threat Intelligence Report - Test (Copy)

23 Apr 2026
E2E Test Report 1776928781514
Weekly Cyber Threat Intelligence Report - Test (Copy)

Search Reports | Template | Author | Visibility | TLP | Status

E2E Test Report 1776928781514
Modified: Last 30 days

3 rows selected | Summarize | Delete

☐	Name	Template	Author	Created	Last modified	Visibility	TLP	Status
☒	Critical Vulnerability Exposure - 202604...	Threat Landscape Report	[Redacted]	23 Apr 2026	23 Apr 2026	My Organization	AMBER	Draft
☒	Daily report of vulnerabilities with CVS...	Threat Landscape Report	[Redacted]	23 Apr 2026	23 Apr 2026	My Organization	AMBER	Draft
☒	E2E PDF Export Test 1776928838948	Weekly Cyber Threat Intelligen...	[Redacted]	23 Apr 2026	23 Apr 2026	My Organization	AMBER	Draft

Using Report Templates

Report templates in security reporting are your guide for creating clear and consistent reports. They give you a predefined structure—so instead of figuring out what to include every time, you already have sections laid out for things like a threat summary, overview, attribution, motivations and objectives, targeting profile, tools, infrastructure, and recommendations.

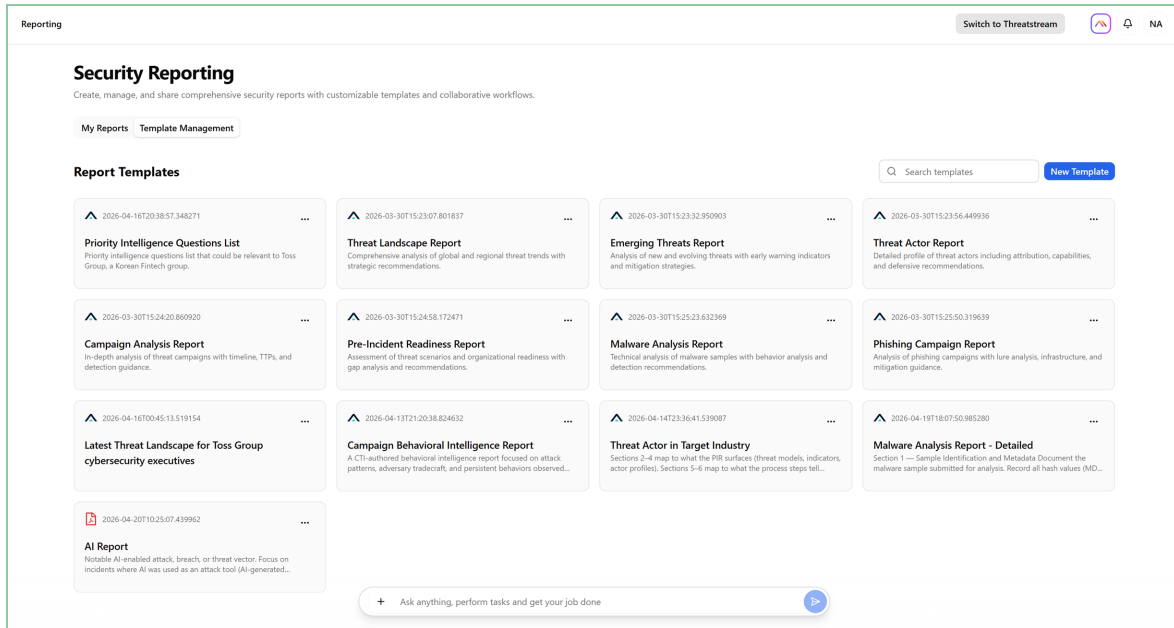
When you use a template, it helps you stay organized and makes sure you don't miss any important details. You can focus more on analyzing the problem and less on formatting the report. It also keeps your reports consistent with others across your team, which makes them easier for anyone to read and understand.

Templates also save you time. You can quickly create reports by filling in the required sections, and with the help of Anomali AI reports can even be generated automatically using predefined templates.

Overall, they make your reporting process faster, more structured, and more effective—both for you and for anyone reviewing your reports.

ThreatStream Next Gen offers you out-of-the-box templates that can be used right away for creating reports. However, you can also create custom templates to suit the needs of your organization.

To access available report templates, navigate to **ThreatStream Next Gen > Investigations & Analysis > Reporting**. Click **Template Management**.



The following report templates are available to all users out of the box:

Report Template	Description
Threat Landscape Report	Comprehensive analysis of global and regional threat trends with strategic recommendations.
Emerging Threats Report	Analysis of new and evolving threats with early warning indicators and mitigation strategies.
Threat Actor Report	Detailed profile of threat actors including attribution, capabilities, and defensive recommendations.
Campaign Analysis Report	In-depth analysis of threat campaigns with timeline, TTPs, and detection guidance.
Pre-Incident Readiness Report	Assessment of threat scenarios and organizational readiness with gap analysis and recommendations.

Report Template	Description
Malware Analysis Report	Technical analysis of malware samples with behavior analysis and detection recommendations.
Phishing Campaign Report	Analysis of phishing campaigns with lure analysis, infrastructure, and mitigation guidance.

To learn how to create a custom report template, see ["Creating a Report Template" below](#).

Creating a Report Template

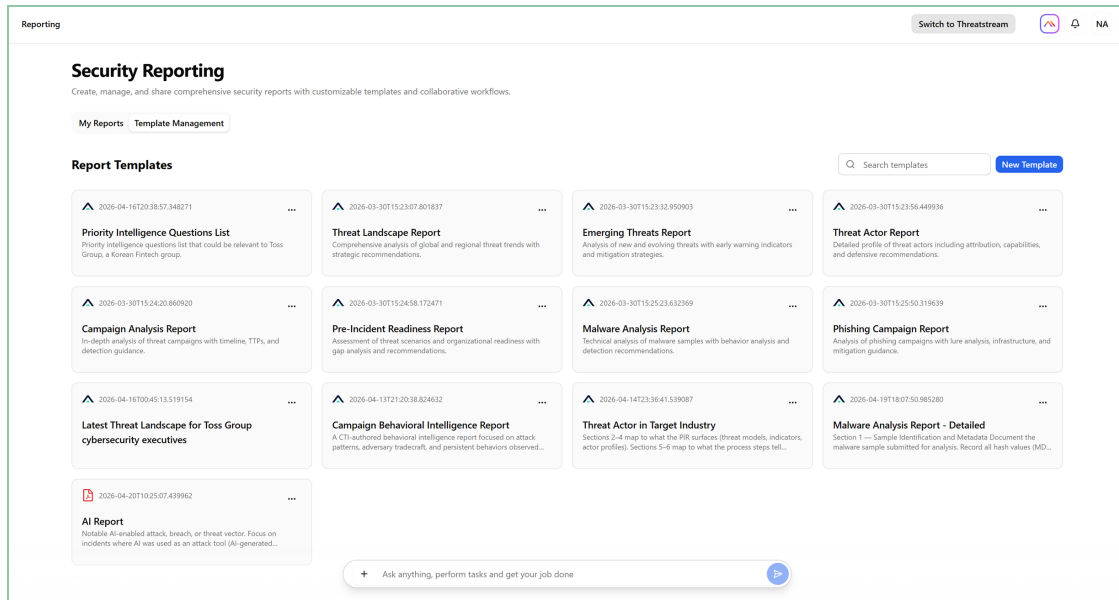
On the Template Management tab of the Security Reporting page you can create custom report templates that all users within your organization can use for creating reports. The process involves defining basic details like the template name and description, optionally adding branding such as a logo, and choosing how to build the content—either by creating sections manually or by uploading a file for automatic extraction. Once created, the template is saved and made available for using in the report creation process. To learn how templates are used for report creation, see ["Creating a Report" on page 275](#).



Note: An organization can create up to 10 report templates.

To create a report template:

1. Navigate to **ThreatStream Next Gen > Investigations & Analysis > Reporting**.
2. Click the **Template Management** tab.



3. Click **New Template**. The Create Template dialog box opens.
4. Enter a unique template name and description.
5. (Optional) Upload a logo. The supported file types are SVG, PNG, and JPG. The logo file size should not exceed 1 MB.
6. Provide template section names, which will define report headings aimed at helping report authors understand what information needs to be included in the report.
Use one of the following options to add headings to the template.

- **Manual**—if you want to enter sections (headings) manually.

Create Template
Create a new template with custom sections [Learn more](#)

Template Name
Campaign Behavioral Intelligence Report

Description
A CTI-authored behavioral intelligence report focused on attack patterns, adversary tradecraft, and persistent behaviors observed across active or recent campaigns. Designed for SOC, threat hunting, and vulnerability management audiences across Financial Services, Government, Oil & Gas, Energy, and Retail / Entertainment sectors. Prioritizes behavioral indicators and TTP patterns over static IOCs to support durable detection and proactive defense.

Logo (Optional)
Drag and drop or click to upload
Supports PNG, JPG, GIF

☒ Manual ☐ Upload File

Sections

- Campaign Overview
- Behavioral Summary & Adversary Fingerprint
- Attack Lifecycle & Phase Mapping
- Observed Attack Patterns & Tradecrafts
- File System & Directory Behavior
- Process & Execution Behavior
- Persistence & Registry Behavior
- Network & C2 Communication Patterns
- Credential Access & Lateral Movement Patterns
- Defense Evasion Techniques
- Vulnerability & Exploitation Behavior
- Campaign TTP Breakdown & Execution Context
- Behavioral Detection Opportunities
- Threat Hunting Hypotheses
- Durable Indicators & Signatures
- Static IOCs (Reference Only)
- Intelligence Confidence & Source Assessment
- Appendix

Cancel Create Template

- **Upload File**—if you want to add sections (headings) by uploading a PDF or DOCX file. Anomali will extract the required information for you.

Create Template
Create a new template with custom sections

Template Name
Campaign Behavioral Intelligence Report

Description
A CTI-authored behavioral intelligence report focused on attack patterns, adversary tradecraft, and persistent behaviors observed across active or recent campaigns. Designed for SOC, threat hunting, and vulnerability management audiences across Financial Services, Government, Oil & Gas, Energy, and Retail / Entertainment sectors. Prioritizes behavioral indicators and TTP patterns over static IOCs to support durable detection and proactive defense.

Logo (Optional)
Drag and drop or click to upload
Supports PNG, JPG, GIF

☐ Manual ☒ Upload File

Upload Template
Drag and drop or click to upload
Supports pdf, docx files, but not templates with sections
[report template.pdf](#)

Extracted Templates (3 Items)
Backend-generated template structure

1. # [Section Title]
2. ## [Subsection Title]
3. ### [Sub-subsection Title]

Cancel Create Template

7. Click **Create Template**.

The template is created and added to the list of report templates on the Template Management tab.

Users of your organization can now use it for creating reports.

Managing Report Templates

You can apply the following actions to report templates:

[Edit templates](#)

Clone templates

Delete templates



Note:

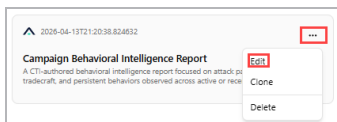
- Anomali out-of-the-box report templates cannot be modified or deleted.
- Only Organization Administrators and template owners can edit and delete report templates.

Editing Report Templates

Organization Administrators and template owners (creators) can edit report templates.

To edit a report template:

1. Navigate to **ThreatStream Next Gen > Investigations & Analysis > Reporting**.
2. Click the **Template Management** tab.
3. On the template you want to edit, click the more options menu (...) and then click **Edit**.



4. In the Edit Template dialog box that opens, make the required changes such as a template name, description, logo, and sections.
5. When done, click **Update**.

The template is updated. The template changes impact only new reports that will be created with it.

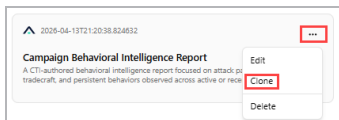
Reports created with this template before the update are not affected.

Cloning Report Templates

If you want to create a report template similar to an existing one (including Anomali-created templates), you can clone the existing template and modify it as needed.

To clone a report template:

1. Navigate to **ThreatStream Next Gen > Investigations & Analysis > Reporting**.
2. Click the **Template Management** tab.
3. On the template you want to clone, click the more options menu (...) and then click **Clone**.



4. In the Clone Template dialog box that opens, make the required changes, if necessary.
5. When done, click **Clone Template**.

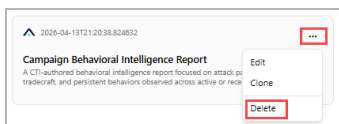
The clone template is added to the list of available templates.

Deleting Templates

Organization Administrators and template owners (creators) can delete report templates.

To delete a report template:

1. Navigate to **ThreatStream Next Gen > Investigations & Analysis > Reporting**.
2. Click the **Template Management** tab.
3. On the template you want to delete, click the more options menu (...) and then click **Delete**.



4. In the confirmation pop-up message, click **Delete**.

The report template is deleted.

Chapter 10: Using Anomali AI in ThreatStream Next Gen

This chapter covers the following topics:

What You Can Do 294

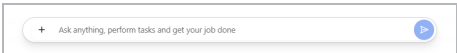
Anomali AI transforms threat intelligence and telemetry into actionable decisions for modern security teams. By delivering AI-driven insights, it helps analysts investigate threats faster, respond more effectively, and operationalize threat intelligence and analytics with confidence.

Within the ThreatStream Next Gen platform, Anomali AI serves as an intelligent assistant that understands natural language. You can use it to ask questions about threat intelligence, search for observables in your environment, and generate reports—all without leaving the platform.

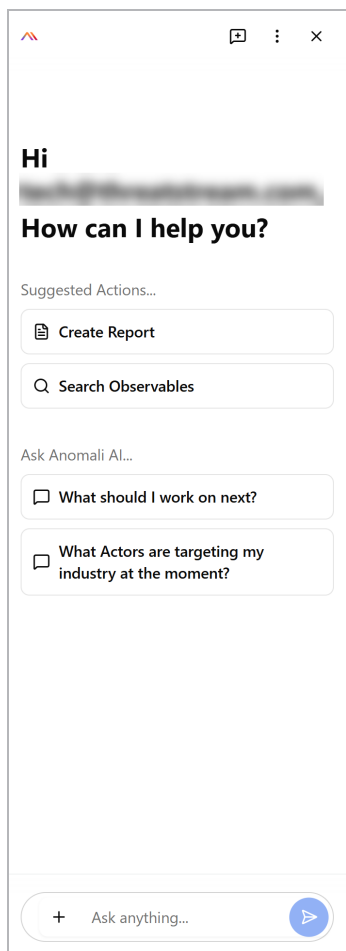
Anomali AI searches the threat intelligence and data accessible to the signed-in user, including premium and open-source intelligence feeds configured for the organization, threat models, investigations, and PIRs.

You can open Anomali AI from anywhere in ThreatStream Next Gen using either of these options:

- **Chat bar** — A persistent input bar appears at the bottom of every page. Click it and start typing to begin a conversation.



- **Anomali AI icon** — Click the Anomali AI icon (🗨️) in the interface to open the full chat panel.



What You Can Do

Once the chat panel is open, Anomali AI offers the following capabilities:

- **Ask a Question**

Type any question in natural language and click the Send button.

For example:

"What are trending actors in the IT industry now?"

"What should be my next steps after detecting this suspicious login?"

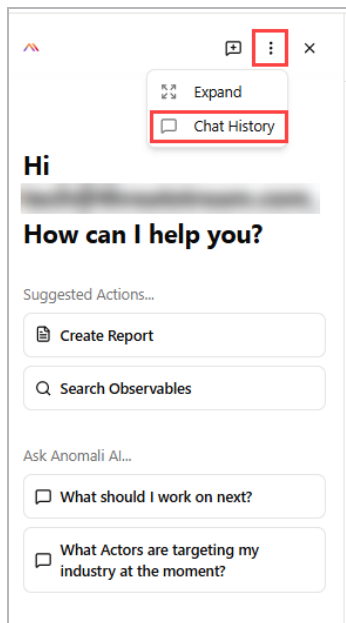
- **Create a Report**

Click **Create Report** to generate an intelligence report. For step-by-step instructions, see ["Creating Reports with Anomali AI" on page 277](#)

■ **Search Observables**

Click **Search Observables** to find observables available in your environment.

All conversations with Anomali AI are automatically saved and accessible at any time through Chat History.



Send Documentation Feedback

If you have comments about this document, you can contact the documentation in these ways:

- Click [contact the documentation team](#) to send an email. If you have an email client configured on this system, an email window will open with the following information in the subject line:

Feedback on User Guide (AQL Search)

- Send your feedback to docs@anomali.com.

Thank you for your feedback!

