Anomali ThreatStream - HYAS Insight App User Guide

Release: 1.5.0

February 03, 2022

Support

Support Portal	https://support.hyas.com
Email	support@hyas.com
Phone	+1 (877) 572-6446
Twitter	@hyasinc

Documentation Updates

Date	Version	Description
February 03, 2022	v1.5.0	HYAS Insight C2 (Command and Control) Attribution App for Context-based Enrichments and Pivot-based Enrichments
November 25, 2021	v1.4.0	Python upgradation from v2.7 to v3.7
February 15, 2021	v1.3.0	Pivot-based Enrichments Implementation
August 2, 2020	v1.0.0	A new guide for the Anomali HYAS Insight App for Context-based Enrichments

Contents

About This Release 3
Chapter 1: Introduction 5
Chapter 2: Configuration 6
Chapter 3: Using Anomali HYAS Insight App 9
1. Context-Based Enrichments 9
2. Pivot-Based Enrichments 11

About This Release

What's New in This Release

Version 1.5.0 release includes Context-based Enrichments and Pivot-based Enrichments for Command & Control (C2) Attribution.

Context-based Enrichments:

#	Entity Type
1	IP Address
2	Domain
3	Email
4	SHA-256

Pivot-based Enrichments:

#	Transform From	Transform To	Description
1	Domain	Email	The email connected to the C2 panel
2	Domain	SHA-256	The SHA-256 malware hash
3	Domain	IP	The actor, C2 or referrer IP
4	IP	Domain	The C2 or email domain
5	IP	Email	The email connected to the C2 panel
6	IP	SHA-256	The SHA-256 malware hash
7	SHA-256	IP	The actor, C2 or referrer IP
8	SHA-256	Domain	The C2 or email domain
9	SHA-256	Email	The email connected to the C2 panel
10	Email	IP	The actor, C2 or referrer IP
11	Email	Domain	The C2 or email domain
12	Email	SHA-256	The SHA-256 malware hash

Version 1.4.0 release for upgrading Python version from v2.7 to v3.7. No functional changes were made to Pivot based and Context based enrichments.

Version 1.3.0 release includes Pivot-based Enrichments for the following transformations.

#	Transform From	Transform To
1	Domain	Email
2	Domain	Hash
3	Domain	IP
4	Domain	Nameserver
5	IP	Domain (Passive DNS)
6	IP	Email
7	IP	Hash
8	IP	Domain (Dynamic DNS)
9	Hash	IP
10	Hash	Domain
11	Email	Domain (WHOIS)
12	Email	IP
13	Email	Domain (Dynamic DNS)
14	Email	Nameserver

Version 1.0.0 release includes Context-based Domain and IP Enrichments for the following endpoints.

#	Domain Endpoints	IP Endpoints
1	DYNAMIC DNS	DYNAMIC DNS
2	PASSIVE DNS	PASSIVE DNS
3	PASSIVE HASH	PASSIVE HASH
4	SSL CERTIFICATES	SSL CERTIFICATES
5	MALWARE SAMPLES	MOBILE
6	WHOIS	SINKHOLE

Chapter 1: Introduction

Threat Intelligence provides valuable incident context to help incident responders reduce investigation time and enable a rapid, decisive response. Anomali ThreatStream offers the most comprehensive Threat Intelligence Platform, allowing all threat intelligence feeds to be managed and automatically made available to your security team. By integrating ThreatStream and the HYAS™ Insight API, your security team can gain instant context regarding artifacts associated with an incident.

HYAS has developed a Context-Based Enrichment Integration and Pivot-Based Enrichment Integration for the Anomali ThreatStream platform so that SOC analysts and IR teams can leverage HYAS Insight's On-demand Threat Intelligence within the ThreatStream platform to track down potentially malicious Indicators of Compromise (IoC).

To achieve this integration, Anomali provides an HYAS Insight App for the HYAS Insight API including Command & Control (C2) Attribution. The Anomali HYAS Insight App offers:

- Contextual, enriched threat intelligence received from HYAS Insight including Command & Control (C2) Attribution.
- Pivot-based enriched threat intelligence received from HYAS Insight including Command & Control (C2) Attribution.

This document outlines the process to install the Enrichment Integration provided by HYAS into the Anomali ThreatStream Platform and provides details on how to efficiently use the integration to acquire detailed threat information from HYAS Insight.

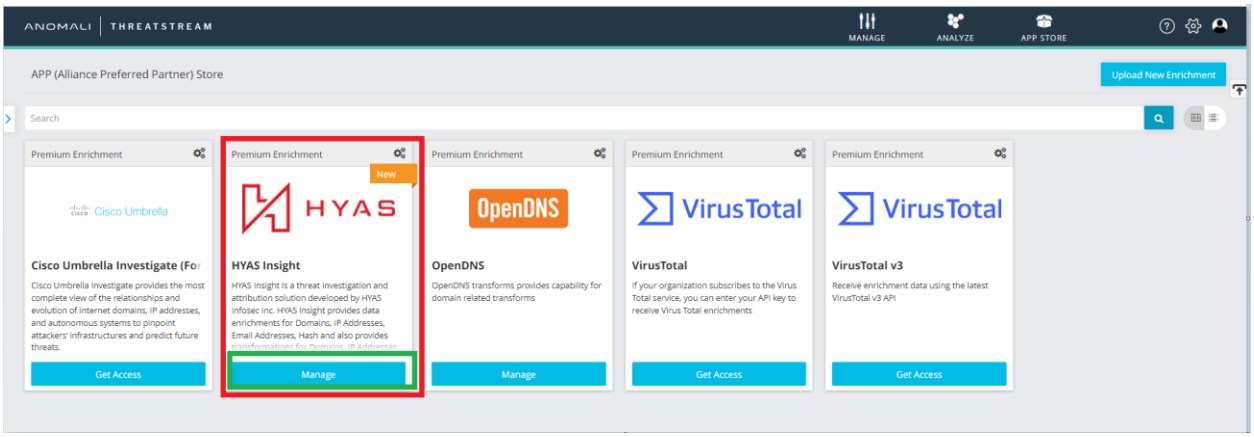
Chapter 2: Configuration

To configure and activate the HYAS Insight App Enrichment bundle for ThreatStream platform, follow the steps mentioned below:

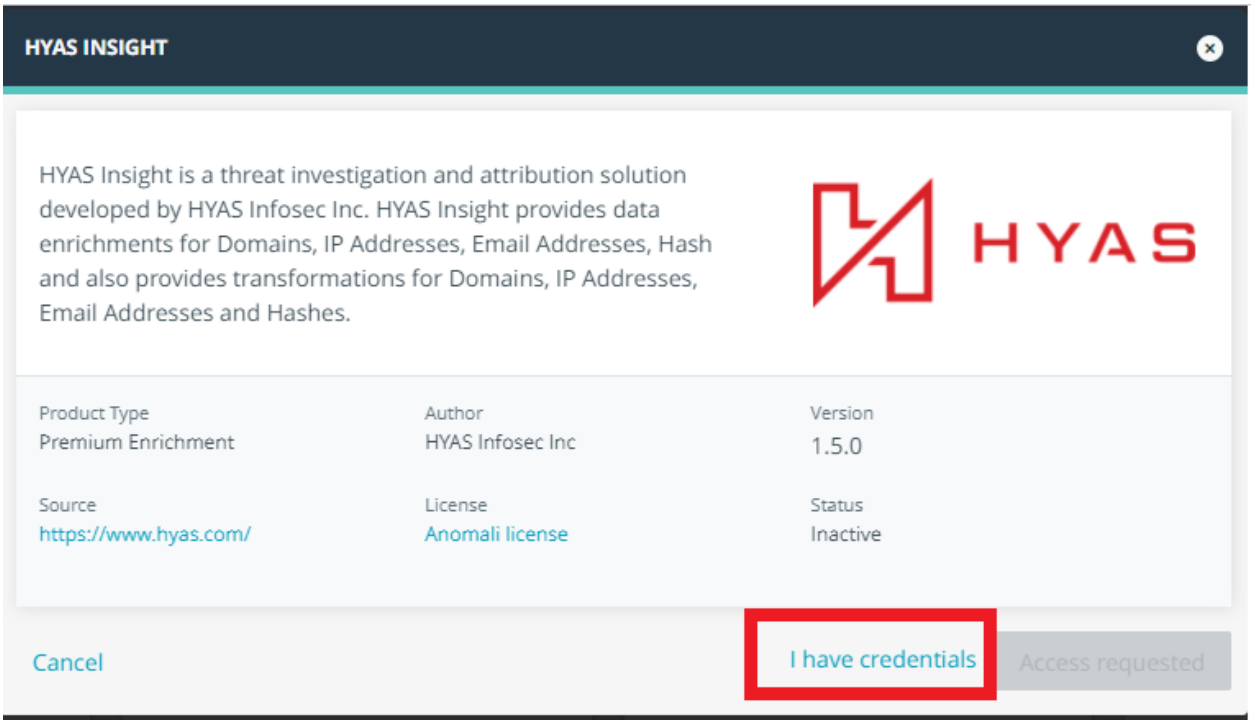
1. Login into Anomali ThreatStream platform

2. Click on “APP STORE” button on the top menu-bar

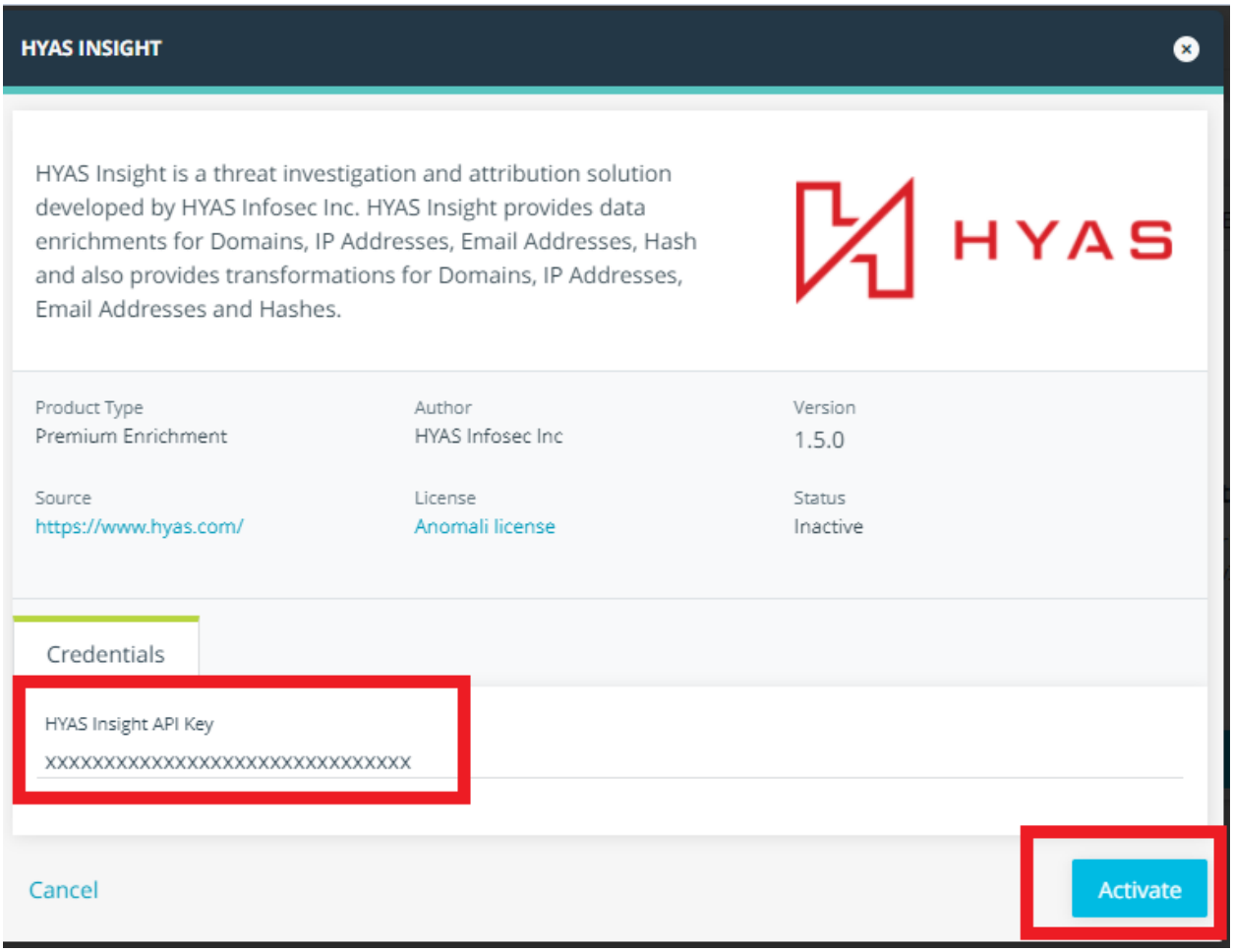
3. All Integrations will be listed here. If you do not see HYAS Insight Integration on the page, contact Anomali Support.
   Within the HYAS integration application, click on the “Manage” button as shown below to configure HYAS Insight App



4. A dialog box will appear as shown below, click on “I have credentials” button if you have obtained an API key from HYAS, otherwise contact support@hyas.com to get your API key.



5. Insert your HYAS Insight API key in the API Key text-field. Finally, click on the Activate button to finish your configuration.



At this point, the configuration for your HYAS Insight Enrichment App is complete and is ready to be used. In case any error occurs, contact Anomali Support for further assistance.

Chapter 3: Using Anomali HYAS Insight App

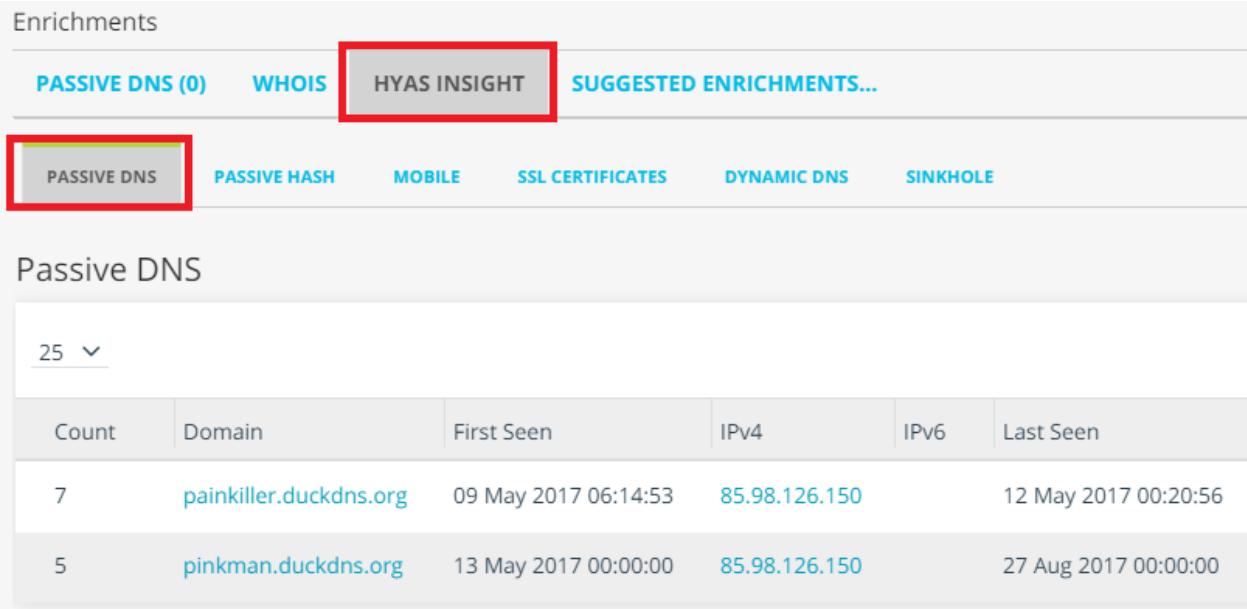
1. Context-Based Enrichments

Context-based enrichments enable analysts to step through entire workflows on observable details pages, thus eliminating the need to jump between product screens. Up to 50 observables from the enrichment source can be displayed using widgets (Table Widget, Chart Widget etc.)

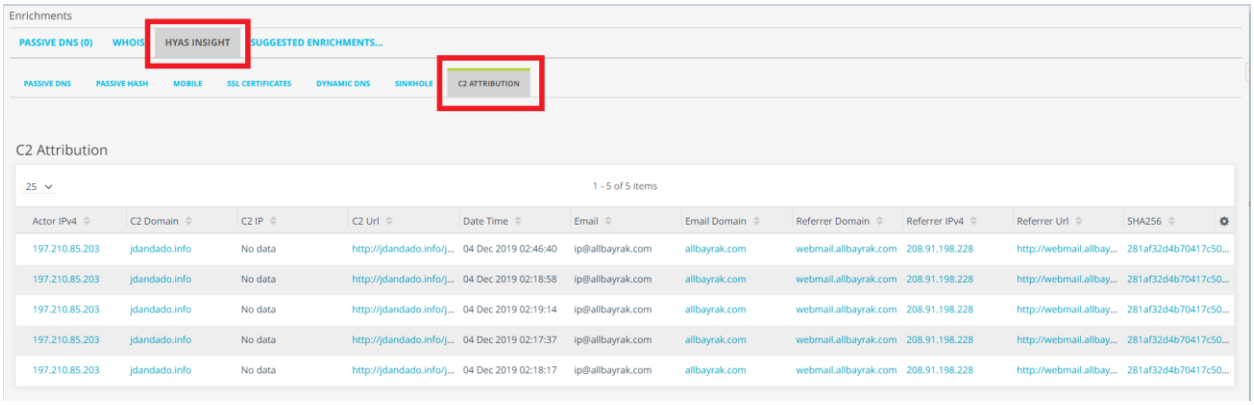
On the details page of an Observable (Domain and IP), click on “HYAS Insight” tab under the Enrichments sections (as shown below) to fetch the enrichment data for that Observable.

Note: Email and SHA-256 Context based enrichments are available for C2 attribution only

For example, the following displays the Context-based Passive DNS information of an IP Address.



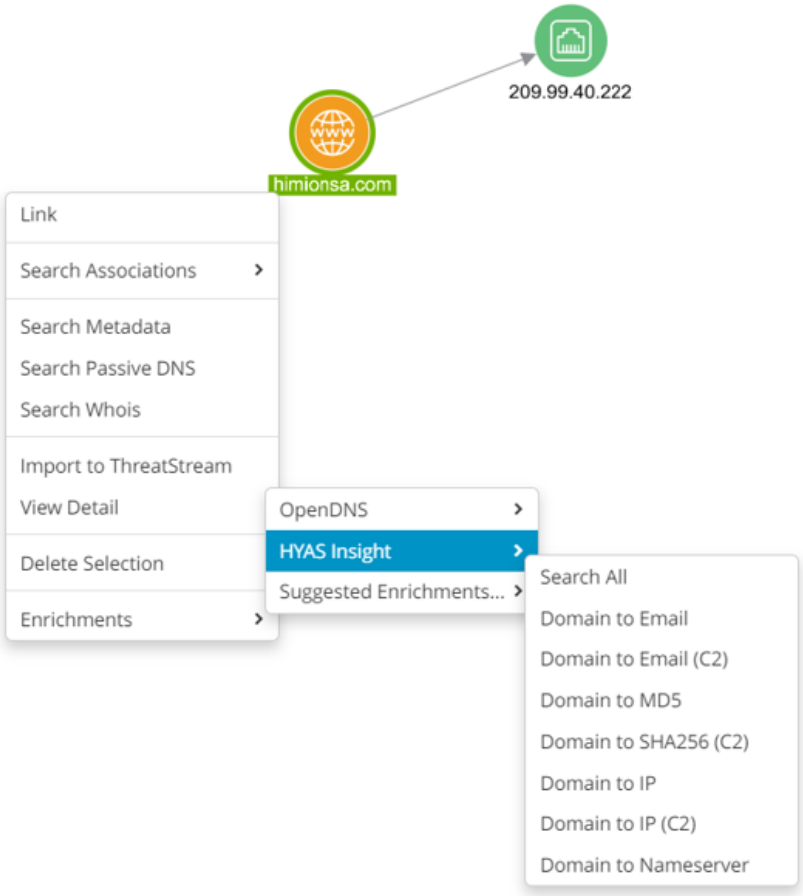
For example, the following displays the Context-based C2 Attribution information of an IP Address.



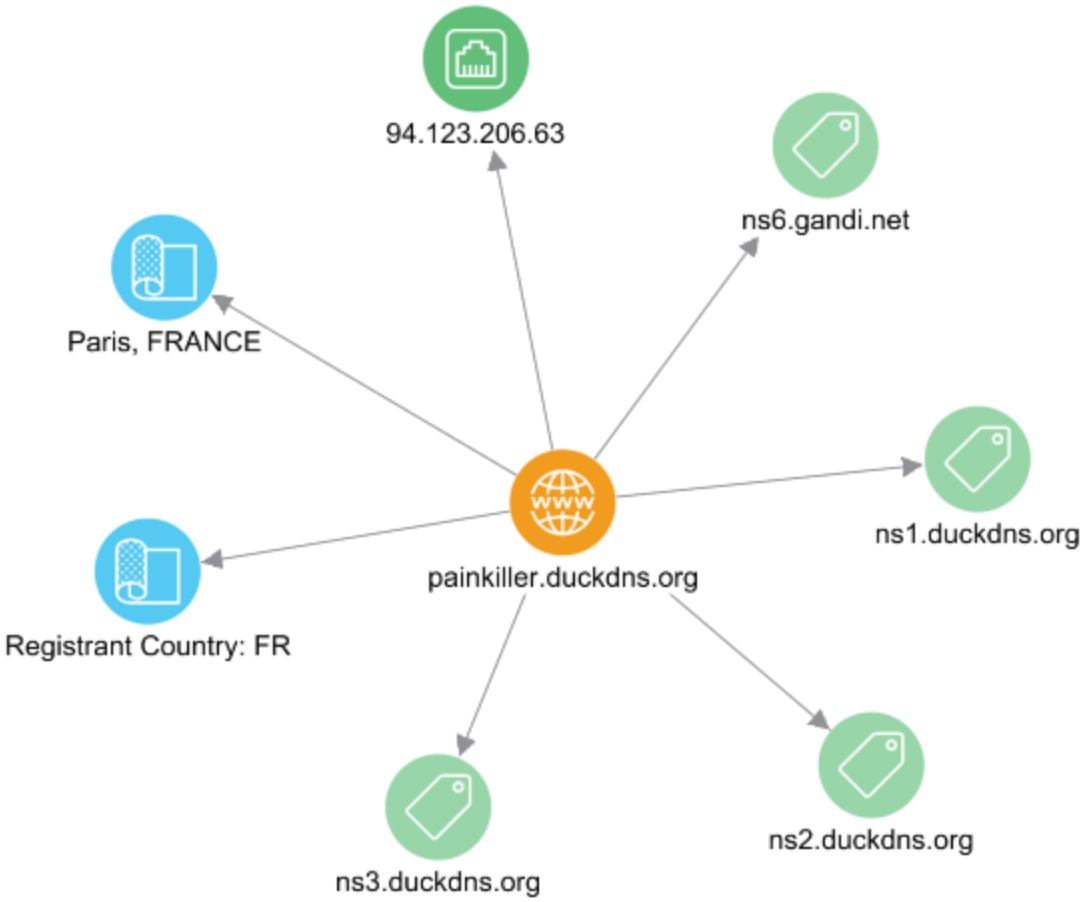
2. Pivot-Based Enrichments

Pivot-based enrichments expand the breadth of data that analysts can use to build out graphical relationships during threat research on the pivoting tool on the Investigations user interface within ThreatStream.

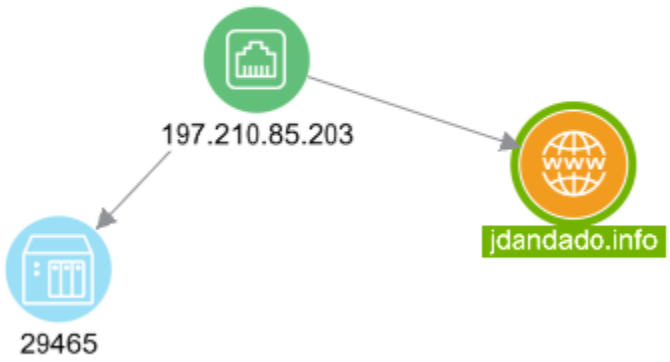
Example: The following displays the list of available Pivot-based transformations for Domain (e.g., Domain to Email, Domain to MD5, Domain to IP (C2) etc.)



Example: The following displays Pivot-based enrichment (Domain to Nameserver transformation)


94.123.206.63
ns6.gandi.net
Paris, FRANCE
ns1.duckdns.org
painkiller.duckdns.org
Registrant Country: FR
ns3.duckdns.org
ns2.duckdns.org

Example: The following displays Pivot-based enrichment (IP to C2 Domain transformation)



About HYAS

HYAS, a First Nations word meaning “great and powerful,” is the world’s leading authority on cyber adversary infrastructure and communication to that infrastructure. HYAS has constructed what is arguably the world’s largest data lake of attacker infrastructure including unrivaled domain-based intelligence. HYAS leverages its infrastructure knowledge to deliver a generational leap forward in cybersecurity. HYAS provides the industry’s first security solution that integrates into an organization’s existing security technology stack to proactively detect and mitigate cyber risks before attacks happen, and to identify the infrastructure behind the attacks. Threat and fraud response teams use HYAS to hunt, find, and identify adversary infrastructure while enterprises can proactively block both known and not-yet-launched phishing and ransomware attacks at the network layer. For more information about HYAS, visit https://www.hyas.com.