LiveAction®

ThreatEye

User Guide

LiveAction, Inc.
960 San Antonio Road, Ste. 200
Palo Alto, CA 94303, USA
+1 (888) 881-1116
https://www.liveaction.com

20221017-TEU_10a

Contents

CHAPTER 1

Introduction

In this chapter:

About ThreatEye

ThreatEye by LiveAction is an AI-powered Network Detection and Response (NDR) platform that combines machine learning with connection fingerprinting, behavioral asset characterization, and simplified threat investigation life cycle management, using high-fidelity and enriched findings to track and resolve incidents.

System Requirements

The system requirements for ThreatEye are:

- LiveWire with a valid ThreatEye Probe license for sending telemetry to ThreatEye
- A web browser

ThreatEye Workflow

ThreatEye is simple and easy to use! Here are the steps to get you started:

1. If not already done by LiveAction, set up the ThreatEye probe (LiveWire appliance). You will need to make sure the ThreatEye license is installed and that a ThreatEye capture is created and sending telemetry to ThreatEye. See *Sending Telemetry to ThreatEye* on page 3.
2. Log into ThreatEye using the URL provided by LiveAction. See *Logging into ThreatEye* on page 14.
3. View the **Executive Dashboard** to get a birds-eye overview of what is going on in your environment. See *Executive Dashboard* on page 17.
4. View the **Analyst Dashboard** to see more in-depth information on the types of threats and attacks monitored in your environment. See *Analyst Dashboard* on page 19.
5. View the **Policy Investigation Dashboard** to see the high-level policy information about what is going on in your environment. Policy information is driven by Flow data. See *Policy Investigation Dashboard* on page 21.
6. View the **Findings Explorer** to see more in-depth information on the types of threats and attacks monitored in your environment. Findings are a crucial component to ThreatEye and can be filtered and searched to display more targeted results. See *Findings Explorer* on page 22.
7. View the **Casebooks Dashboard** to see and manage the casebooks assigned to individuals within your organization. See *Casebooks* on page 24.
8. View the **Settings** to see and manage *Filters*, *Tags*, and *Omnipeek Integration*. The **Settings** are only available to users that have been assigned an Administrator role with ThreatEye. See *Settings* on page 26.

Contacting LiveAction Support

Please contact LiveAction support at *https://www.liveaction.com/contact-us* if you have any questions about using ThreatEye.

An RMA (Return Material Authorization) number must be obtained from LiveAction before returning any hardware. Please contact LiveAction technical support at *https://www.liveaction.com/support/technical-support/* for instructions.

CHAPTER 2

Sending Telemetry to ThreatEye

In this chapter:

About Sending Telemetry to ThreatEye

The LiveAction LiveWire is designed to work as a ThreatEye Probe, extracting rich metadata, including more than 150 packet dynamic features, to support threat and anomaly detection, response, hunting, forensics, and compliance validation reporting in ThreatEye. Additionally, because packet dynamic-based metadata focuses on packet traits and behaviors—not contents—this data collection technique works equally well with encrypted and unencrypted traffic.

To use LiveWire with ThreatEye, you must first license and configure ThreatEye. Once configured, you must then configure LiveWire to send telemetry to ThreatEye. This chapter describes the tasks you need to perform in order to properly send telemetry from LiveWire to ThreatEye.

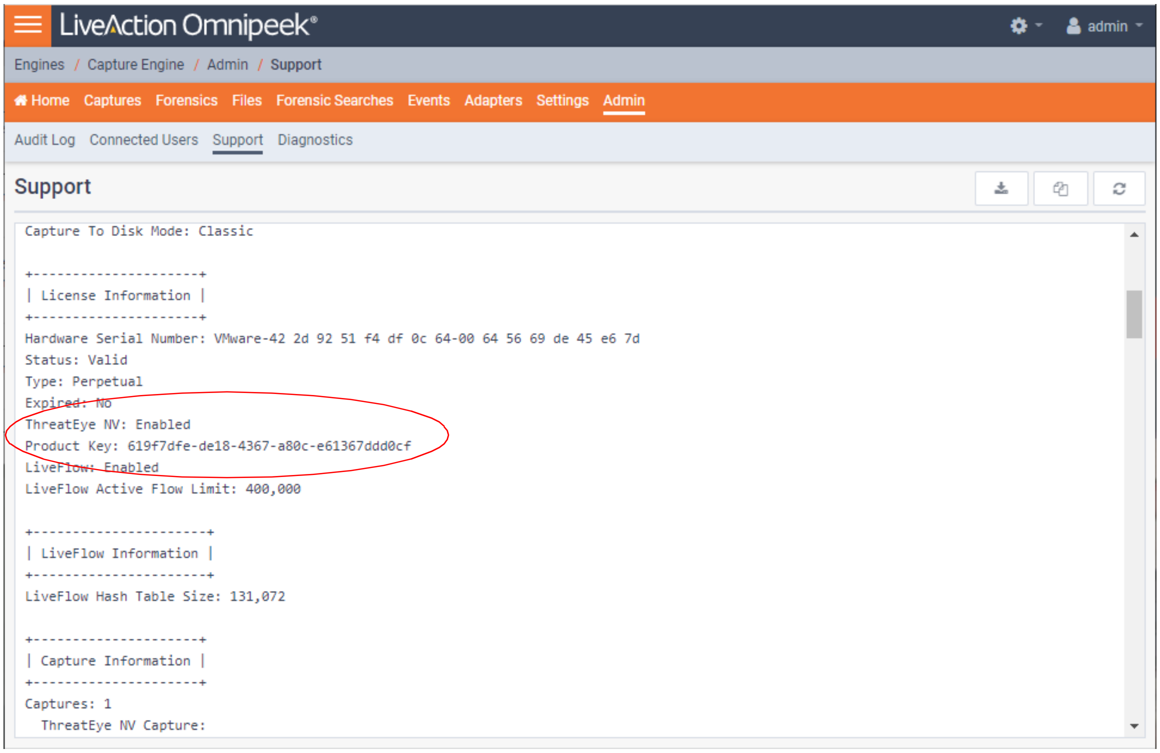
Viewing and Updating the ThreatEye License

In order to use the ThreatEye Probe on LiveWire, you must have a ThreatEye license installed and enabled on LiveWire.

Viewing Your ThreatEye License

To view your license information on LiveWire:

1. Use Omnipeek to view the *Admin* > *Support* page:
2. Scroll down to the *License Information* section of the Support page.


LiveAction Omnipeek®
admin
Engines / Capture Engine / Admin / Support
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin
Audit Log Connected Users Support Diagnostics
Support

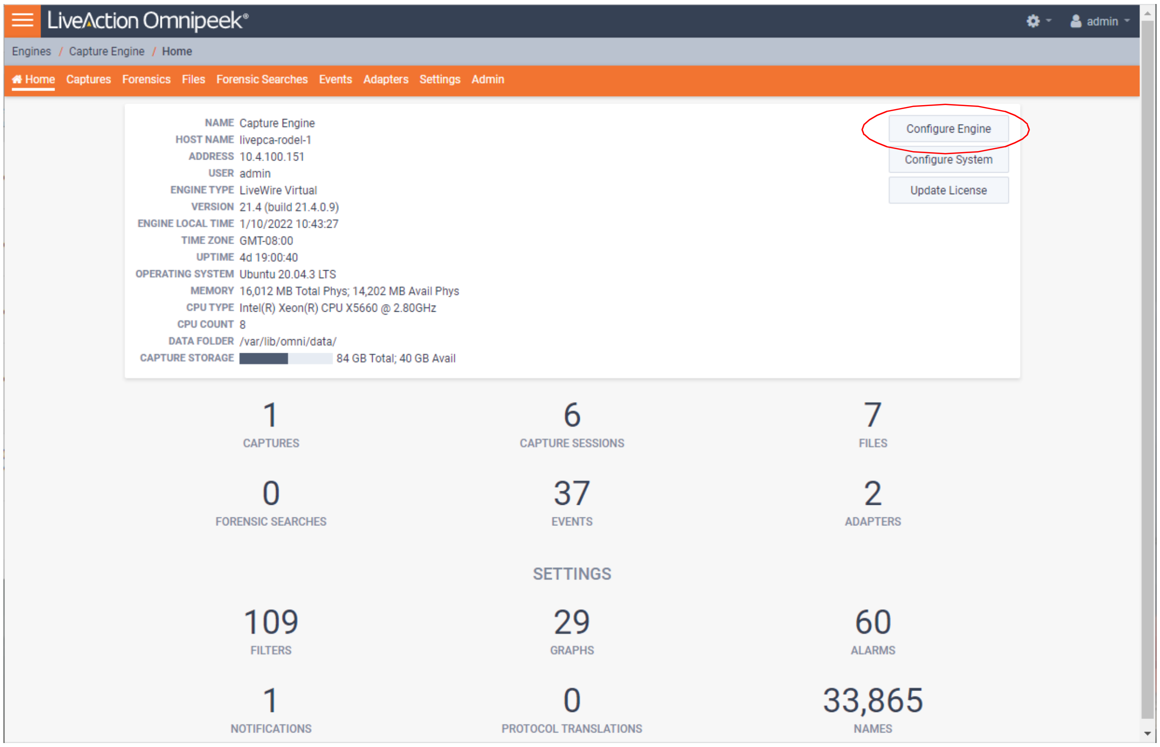
```
Capture To Disk Mode: Classic

+---------------------+
| License Information |
+---------------------+
Hardware Serial Number: VMware-42 2d 92 51 f4 df 0c 64-00 64 56 69 de 45 e6 7d
Status: Valid
Type: Perpetual
Expired: No
ThreatEye NV: Enabled
Product Key: 619f7dfe-de18-4367-a80c-e61367ddd0cf
LiveFlow: Enabled
LiveFlow Active Flow Limit: 400,000

+----------------------+
| LiveFlow Information |
+----------------------+
LiveFlow Hash Table Size: 131,072

+---------------------+
| Capture Information |
+---------------------+
Captures: 1
  ThreatEye NV Capture:
```

3. If the line *ThreatEye NV* is *Enabled* and also displays a corresponding *Product Key*, then ThreatEye is already installed on LiveWire and is ready to begin capturing data by creating a ThreatEye capture. See *Configuring LiveWire to Send Telemetry to ThreatEye* on page 7.

   If the line *ThreatEye NV* is *Disabled*, you will need to first install and update your ThreatEye license on LiveWire. See *Updating Your ThreatEye License* on page 5.

Updating Your ThreatEye License

1. Use Omnipeek to view the *Home* page.


LiveAction Omnipeek®
admin
Engines / Capture Engine / Home
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin
Configure Engine
Configure System
Update License

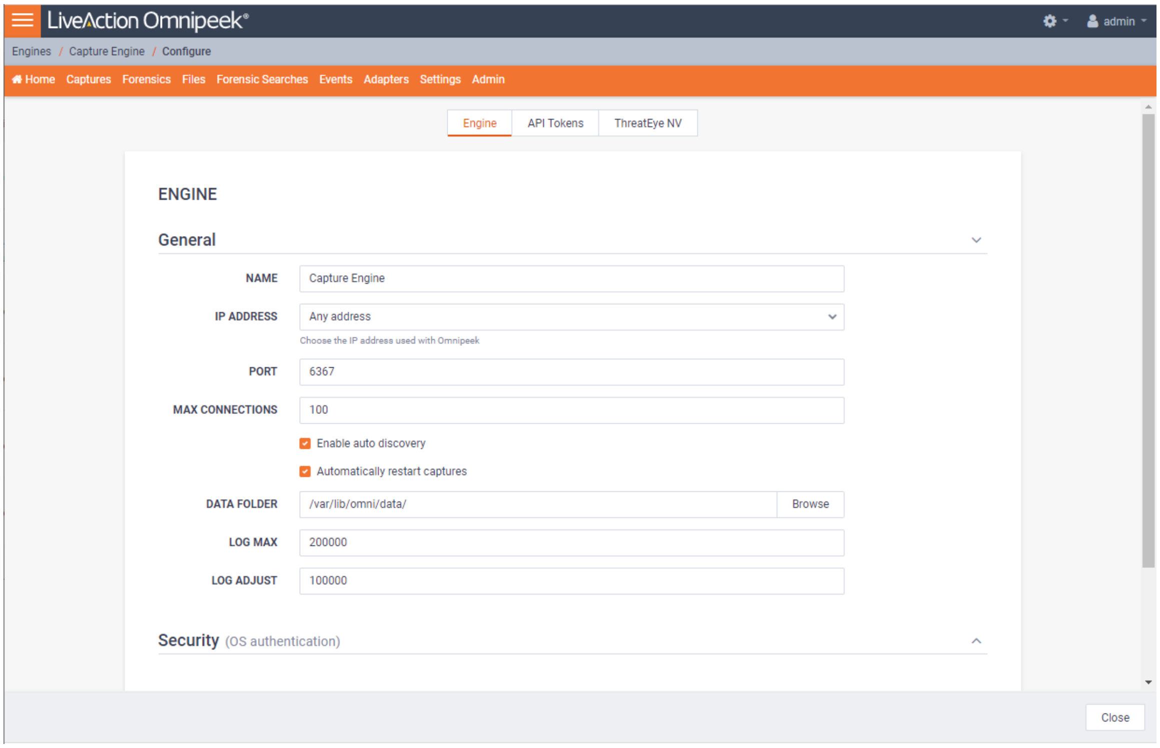
NAME Capture Engine
HOST NAME livepca-rodel-1
ADDRESS 10.4.100.151
USER admin
ENGINE TYPE LiveWire Virtual
VERSION 21.4 (build 21.4.0.9)
ENGINE LOCAL TIME 1/10/2022 10:43:27
TIME ZONE GMT-08:00
UPTIME 4d 19:00:40
OPERATING SYSTEM Ubuntu 20.04.3 LTS
MEMORY 16,012 MB Total Phys; 14,202 MB Avail Phys
CPU TYPE Intel(R) Xeon(R) CPU X5660 @ 2.80GHz
CPU COUNT 8
DATA FOLDER /var/lib/omni/data/
CAPTURE STORAGE 84 GB Total; 40 GB Avail

1 CAPTURES
6 CAPTURE SESSIONS
7 FILES
0 FORENSIC SEARCHES
37 EVENTS
2 ADAPTERS

SETTINGS

109 FILTERS
29 GRAPHS
60 ALARMS
1 NOTIFICATIONS
0 PROTOCOL TRANSLATIONS
33,865 NAMES

2. Click **Configure Engine**. The *Engine* page appears.


LiveAction Omnipeek®
admin
Engines / Capture Engine / Configure
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin
Engine
API Tokens
ThreatEye NV
Browse
Close

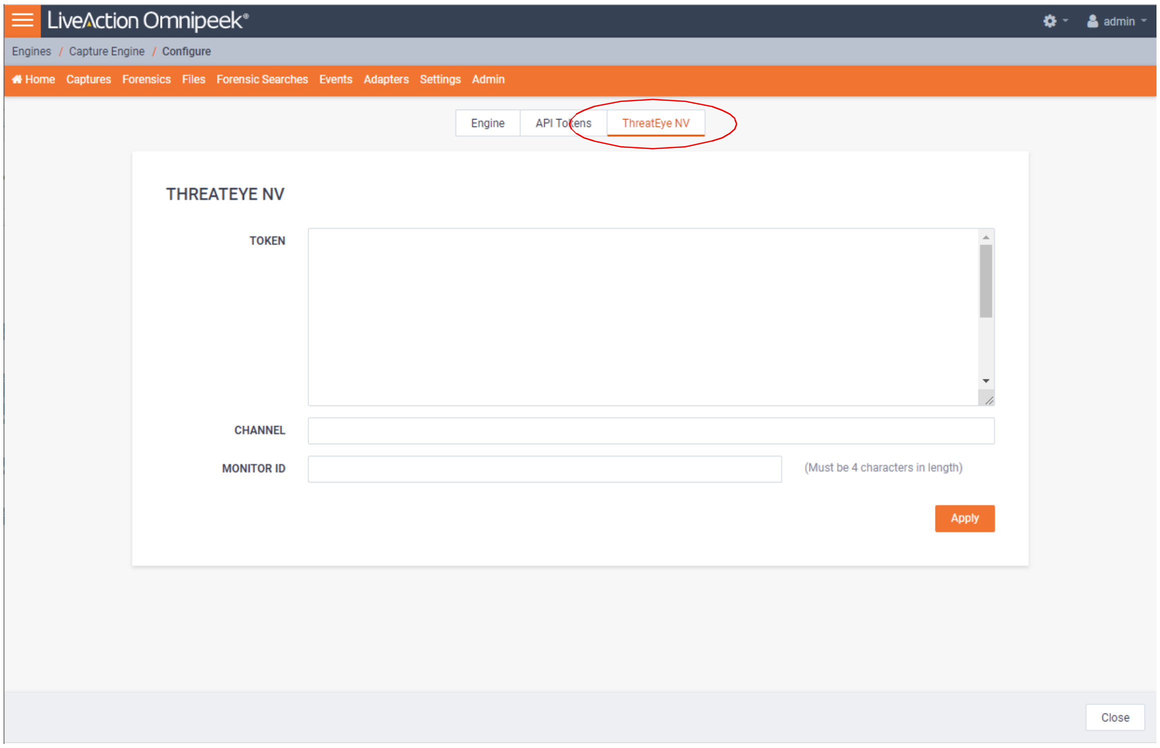
ENGINE

General

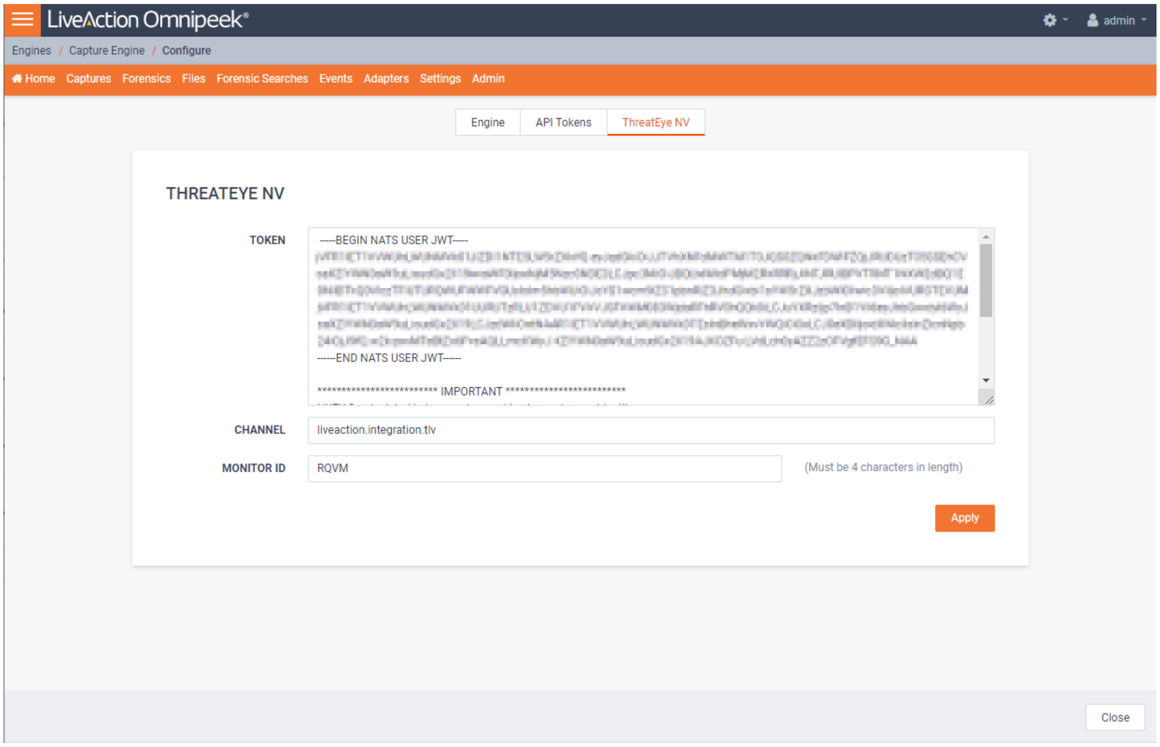
NAME Capture Engine
IP ADDRESS Any address
Choose the IP address used with Omnipeek
PORT 6367
MAX CONNECTIONS 100
☑ Enable auto discovery
☑ Automatically restart captures
DATA FOLDER /var/lib/omni/data/
LOG MAX 200000
LOG ADJUST 100000

Security (OS authentication)

3. Click **ThreatEye NV**. The *ThreatEye NV* page appears.


LiveAction Omnipeek®
admin
Engines / Capture Engine / Configure
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin
Engine API Tokens ThreatEye NV
THREATEYE NV
TOKEN
CHANNEL
MONITOR ID
(Must be 4 characters in length)
Apply
Close

4. Configure the *ThreatEye NV* page. You will need to enter both the *Token* and *Channel* settings that you must obtain from LiveAction as part of the licensing process.


LiveAction Omnipeek®
admin
Engines / Capture Engine / Configure
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin
Engine API Tokens ThreatEye NV
THREATEYE NV
(Must be 4 characters in length)
Apply
Close

TOKEN

```
-----BEGIN NATS USER JWT-----
[redacted]
------END NATS USER JWT------

************************ IMPORTANT ************************
```

CHANNEL: liveaction.integration.tlv

MONITOR ID: RQVM

- *Token*: The *Token* is the authentication method used to connect to our SaaS platform. The *Token* is a highly sensitive token and should be treated with the same precautions as a critical password. The *Token* is provided by LiveAction and is made available as part of the licensing process.

  A valid *Token* starts with a block:

-----BEGIN NATS USER JWT-----

and ends with a string of "*" characters:

****

- *Channel*: The *Channel* is used for routing messages to each specific customer's data processing stack. The *Channel* is provided by LiveAction and is made available as part of the licensing process.

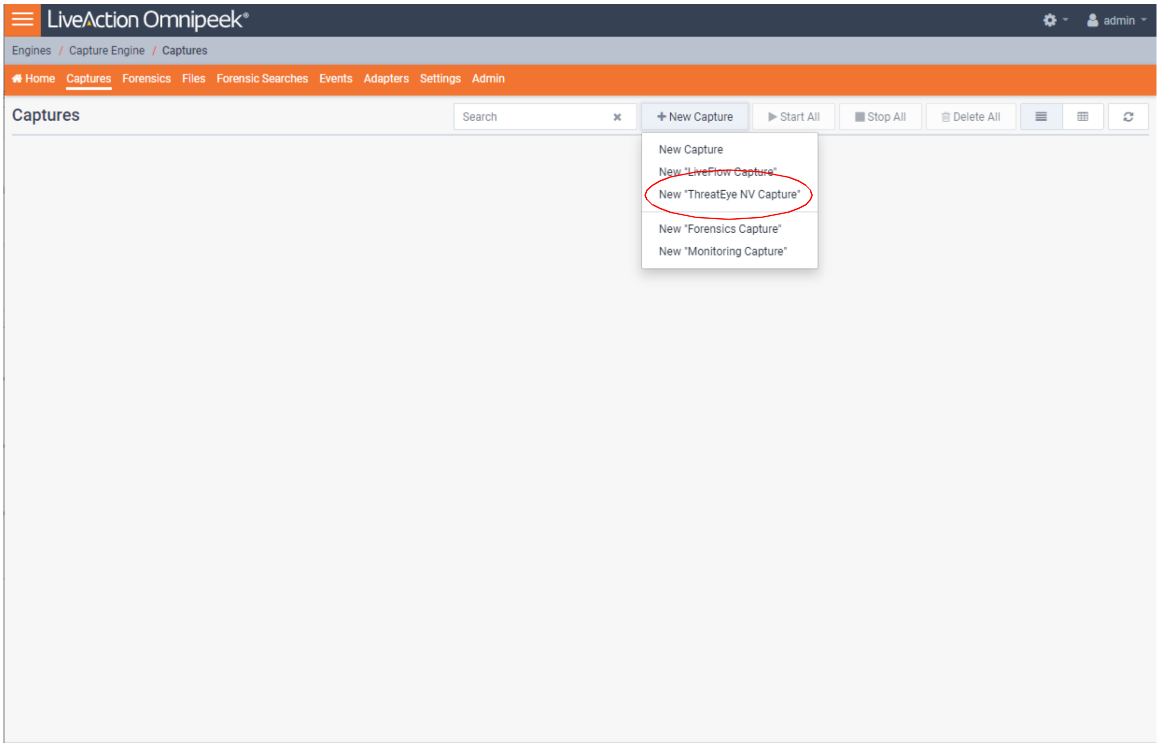
Important! When a new customer comes on board, LiveAction will send them a secure link (via *1password*) that will provide them with both the *Token* and the *Channel* name. Each customer must securely store their own *Token* and *Channel* name as they will only be able to see the contents of the secure *1password* link one time.

- *Monitor ID*: Enter an ID (must be four characters in length, an IPv4 address, or a 32-bit unsigned integer) that helps to identify the ThreatEye capture.

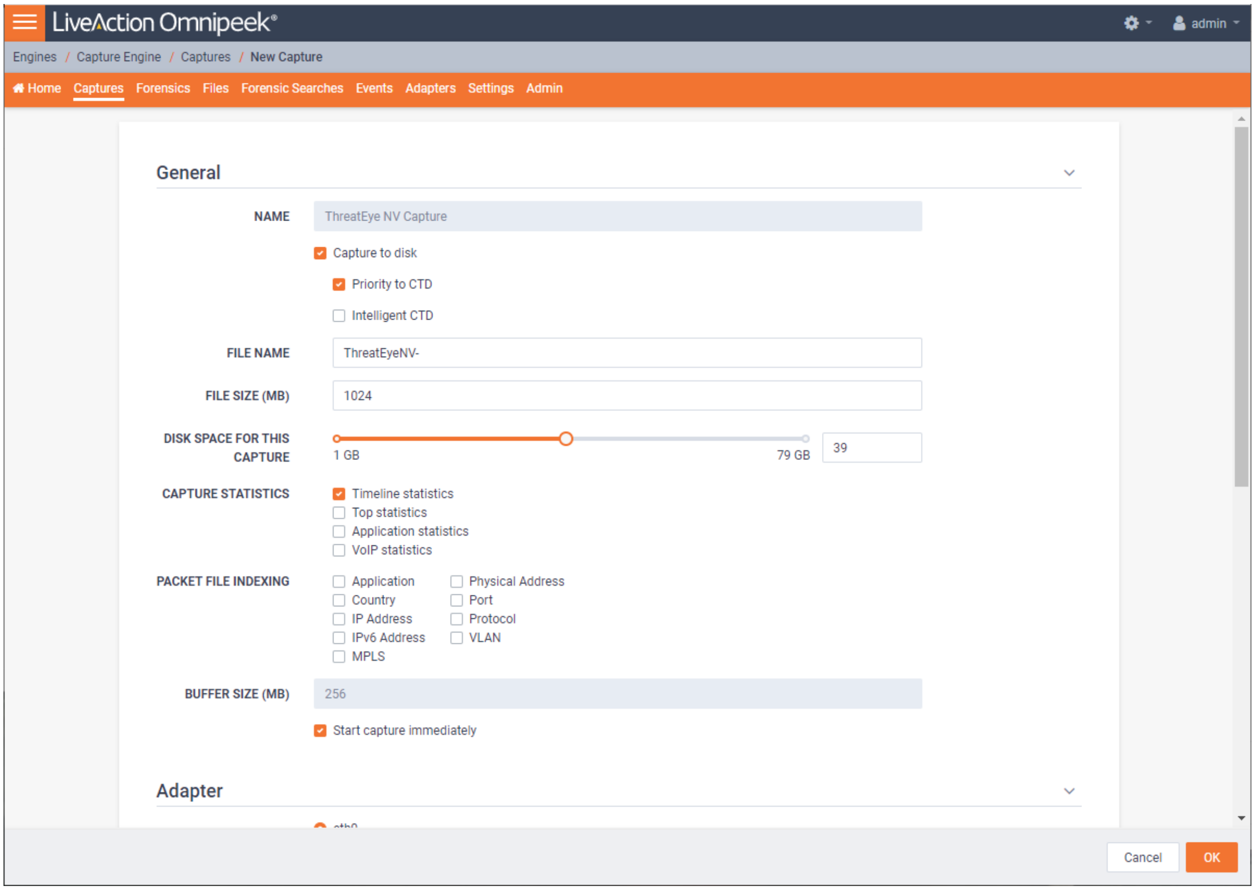
5. Click **Apply**.

Configuring LiveWire to Send Telemetry to ThreatEye

1. Use Omnipeek to view the *Captures* page.
2. Click **+New Capture** and select *New "ThreatEye NV Capture"*.



3. Configure the ThreatEye NV Capture.



General

NAME: ThreatEye NV Capture

☑ Capture to disk

☑ Priority to CTD

☐ Intelligent CTD

FILE NAME: ThreatEyeNV-

FILE SIZE (MB): 1024

DISK SPACE FOR THIS CAPTURE: 1 GB – 79 GB: 39

CAPTURE STATISTICS:
☑ Timeline statistics
☐ Top statistics
☐ Application statistics
☐ VoIP statistics

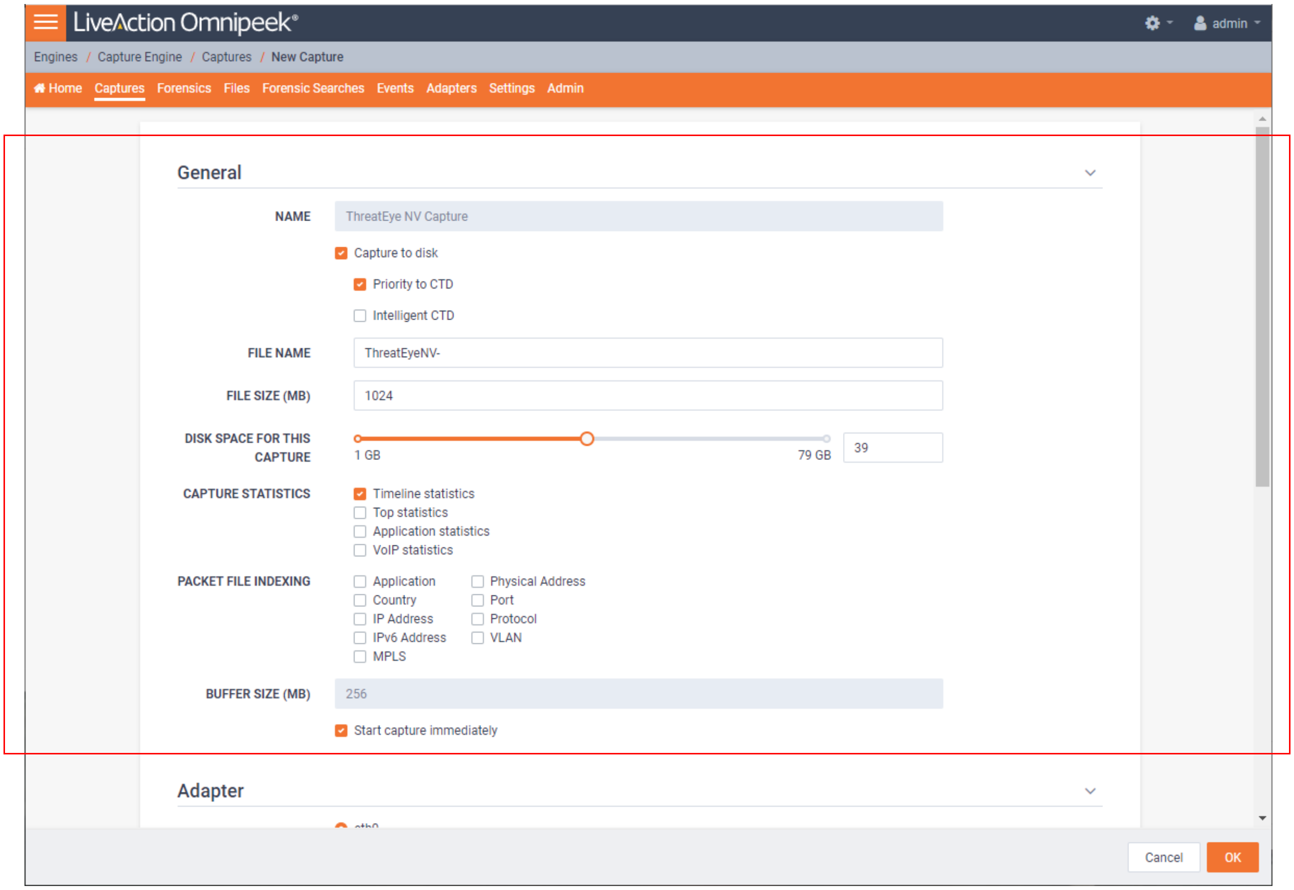
PACKET FILE INDEXING:
☐ Application
☐ Country
☐ IP Address
☐ IPv6 Address
☐ MPLS
☐ Physical Address
☐ Port
☐ Protocol
☐ VLAN

BUFFER SIZE (MB): 256

☑ Start capture immediately

General

The *General* settings let you set up and configure the ThreatEye NV capture.


LiveAction Omnipeek®
admin
Engines / Capture Engine / Captures / New Capture
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin
Adapter
eth0
Cancel
OK

General

NAME: ThreatEye NV Capture

☑ Capture to disk

☑ Priority to CTD

☐ Intelligent CTD

FILE NAME: ThreatEyeNV-

FILE SIZE (MB): 1024

DISK SPACE FOR THIS CAPTURE: 1 GB — 79 GB: 39

CAPTURE STATISTICS:
☑ Timeline statistics
☐ Top statistics
☐ Application statistics
☐ VoIP statistics

PACKET FILE INDEXING:
☐ Application
☐ Country
☐ IP Address
☐ IPv6 Address
☐ MPLS
☐ Physical Address
☐ Port
☐ Protocol
☐ VLAN

BUFFER SIZE (MB): 256

☑ Start capture immediately

- *Name:* Displays the name for the ThreatEye NV capture.
- *Capture to disk:* Select this option to save packet files on your disk. Packet files saved to your hard disk (and the individual packets/packet decodes in each of the files) can be opened and analyzed at a later time with Omnipeek. If you are more interested in speeding up analysis of the data and conserving hard disk space, you may want to disable *Capture to disk*.
- *Priority to CTD:* Select this option so that real-time analysis doesn't impact the capture-to-disk (CTD) performance. When this option is enabled, it is less likely that packets are dropped when they are captured to disk. If capturing all the packets to disk is desirable, enable *Priority to CTD*. If analysis is more important, disable *Priority to CTD*.
- *Intelligent CTD:* Select this option to reduce the amount of data stored to disk and increase your retention time by intelligently slicing off encrypted payloads. It does this by tracking flows—if a flow is encrypted, the full data for the first 20 packets is kept and the payload from the rest of the packets is sliced. It keeps the first 20 without slicing so the certificate exchange is always included.
- *File Name:* Type the name used as a base file name prefix for each capture file that is created using the *Capture to disk* option. Additionally, each capture file is appended with a timestamp indicating the date and time the file was saved. The format of the timestamp is *YYYY-MM-DD-HH.MM.SS.mmm*.
- *File Size (MB):* Enter or select the maximum file size before a new file is created.
- *Disk Space For This Capture:* Move the slider control to set the amount of hard disk space allocated for the capture. The minimum value of the slider is the minimum size of disk space a capture can occupy.
- *Capture Statistics:* Select the type of statistics desired for the capture:
  - *Timeline Statistics:* Select this option to populate the capture engine database with capture data and basic network statistics such as utilization, size, distribution, etc. These statistics are then made available through the *Capture Engine Forensics* tab.

  - *Top Statistics:* Select this option to populate the capture engine database with top nodes and top protocols statistics. These statistics are then made available through the *Capture Engine Forensics* tab.
  - *Application Statistics:* Select this option to populate the capture engine database with applications statistics which are made available through the various 'application' displays.
  - *VoIP Statistics:* Select this option to populate the capture engine database with VoIP call quality and call volume statistics. These statistics are then made available through the *Capture Engine Forensics* tab.

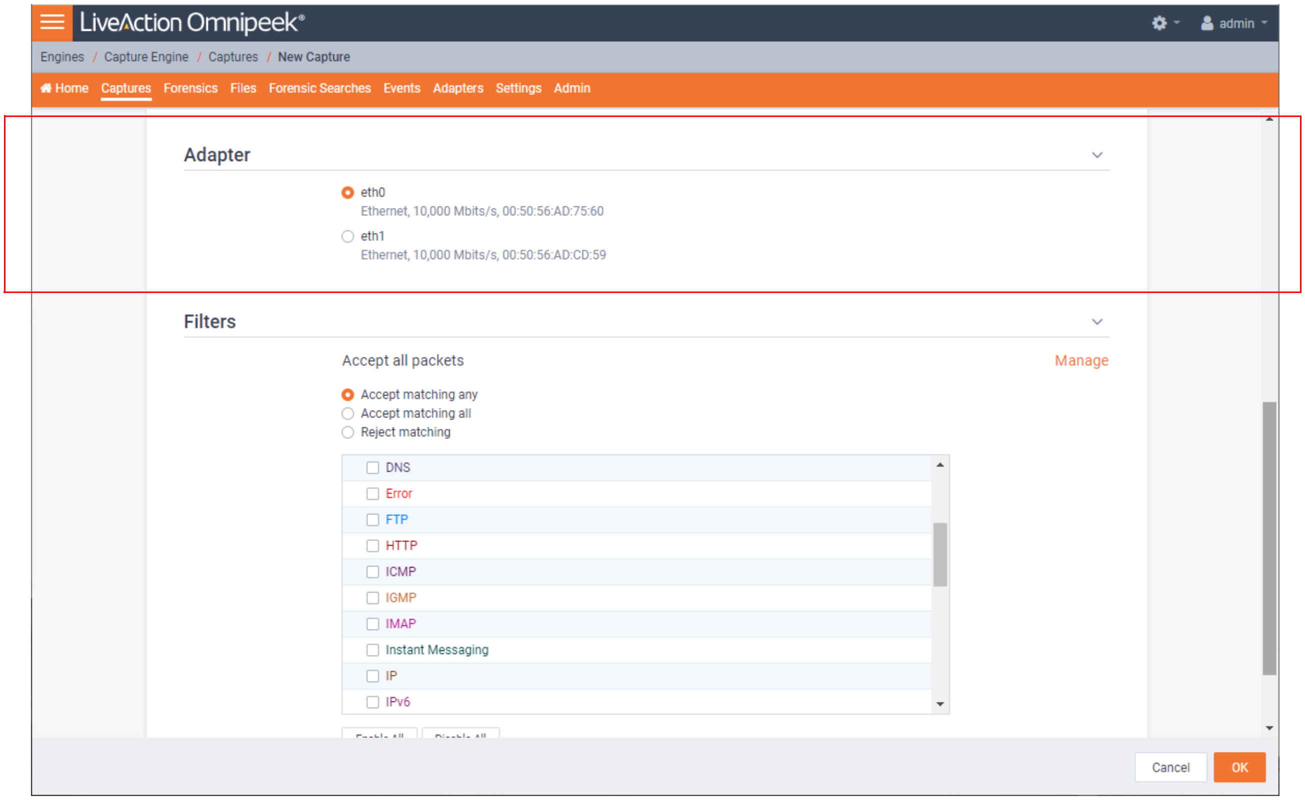
Note Selecting the *VoIP Statistics* option may affect capture performance, especially when there are more than 2000 simultaneous calls on the network. Selecting the *Top Statistics* option may affect capture performance, especially when there are more than 10,000 active nodes captured on the network.

- *Packet File Indexing:* Under certain conditions, *Packet File Indexing* increases performance for forensic searches that use software filters. Overall capture-to-disk performance can degrade slightly, but forensic search results may be returned significantly faster if the packet elements being filtered are contained in the index and the packet characteristic is sparsely located within the packet files being searched. Enable the packet characteristics below you are most likely to use in a forensic search software filter.
  - *Application*
  - *Country*
  - *IP Address*
  - *IPv6 Address*
  - *MPLS*
  - *Physical Address*
  - *Port*
  - *Protocol*
  - *VLAN*
- *Buffer Size (MB):* Enter a buffer size, in megabytes, for the amount of memory dedicated for the capture buffer. The capture buffer is where packets are placed for analysis. The default is 256 megabytes. A larger buffer can reduce or eliminate packet loss due to spikes in traffic. When *Capture to disk* is enabled, the *Buffer Size* option is unavailable.
  - *Start Capture Immediately:* Select this option to immediately begin capturing packets once you click **OK**.

Adapter

The *Adapter* settings display the capture adapters available on LiveWire. All locally installed capture adapters are listed; however, only a supported capture adapter can be selected as the ThreatEye NV capture adapter.

- Select the desired adapter as the ThreatEye NV capture adapter.


LiveAction Omnipeek®
admin
Engines / Capture Engine / Captures / New Capture
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin
Cancel
OK

Adapter

● eth0
Ethernet, 10,000 Mbits/s, 00:50:56:AD:75:60

○ eth1
Ethernet, 10,000 Mbits/s, 00:50:56:AD:CD:59

Filters

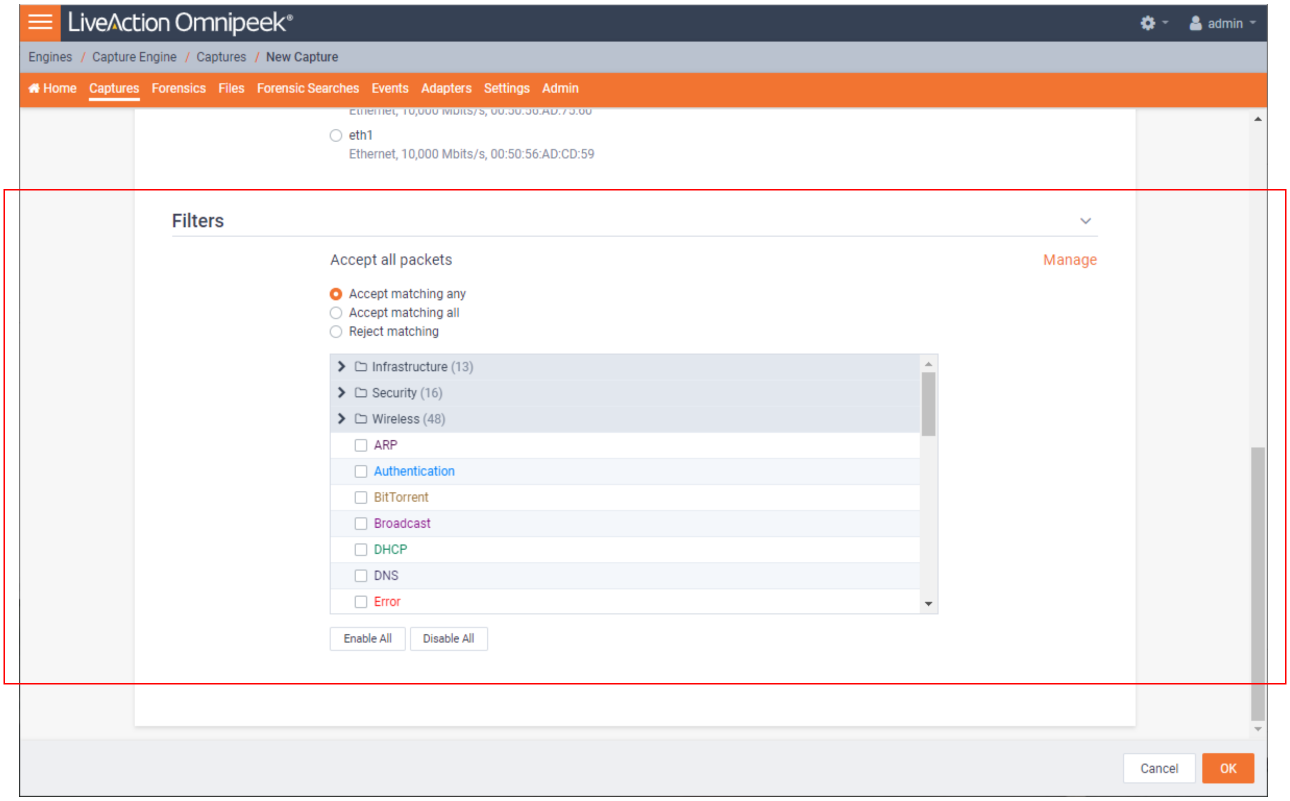
Accept all packets — Manage

● Accept matching any
○ Accept matching all
○ Reject matching

□ DNS
□ Error
□ FTP
□ HTTP
□ ICMP
□ IGMP
□ IMAP
□ Instant Messaging
□ IP
□ IPv6

Filters

The *Filters* settings let you enable or disable filters used when capturing packets or opening packet files. Select the filters you want to enable and then click *Accept Matching Any*, *Accept Matching All*, or *Reject Matching*.


LiveAction Omnipeek®
admin
Engines / Capture Engine / Captures / New Capture
Home Captures Forensics Files Forensic Searches Events Adapters Settings Admin
Enable All
Disable All
Cancel
OK

Ethernet, 10,000 Mbits/s, 00:50:56:AD:75:60

○ eth1
Ethernet, 10,000 Mbits/s, 00:50:56:AD:CD:59

Filters

Accept all packets — Manage

● Accept matching any
○ Accept matching all
○ Reject matching

> Infrastructure (13)
> Security (16)
> Wireless (48)
□ ARP
□ Authentication
□ BitTorrent
□ Broadcast
□ DHCP
□ DNS
□ Error

- *(Accept all packets)*: Click to configure filter settings. You can select which filters to enable, and whether or not to accept or reject the packets matching the filters into the buffer.
  - *Accept Matching Any:* When you choose *Accept Matching Any*, only those packets which match the parameters of at least one of the enabled filters are placed into the capture buffer.
  - *Accept Matching All:* When you choose *Accept Matching All*, only those packets which match the parameters of all the enabled filters are placed into the capture buffer.
  - *Reject Matching:* When you choose *Reject Matching*, only those packets which do not match any of the enabled filters are placed into the capture buffer.
  - *Enable All:* Click to enable all filters.
  - *Disable All:* Click to disable all filters.

4. Click **OK**.

CHAPTER 3

Using ThreatEye

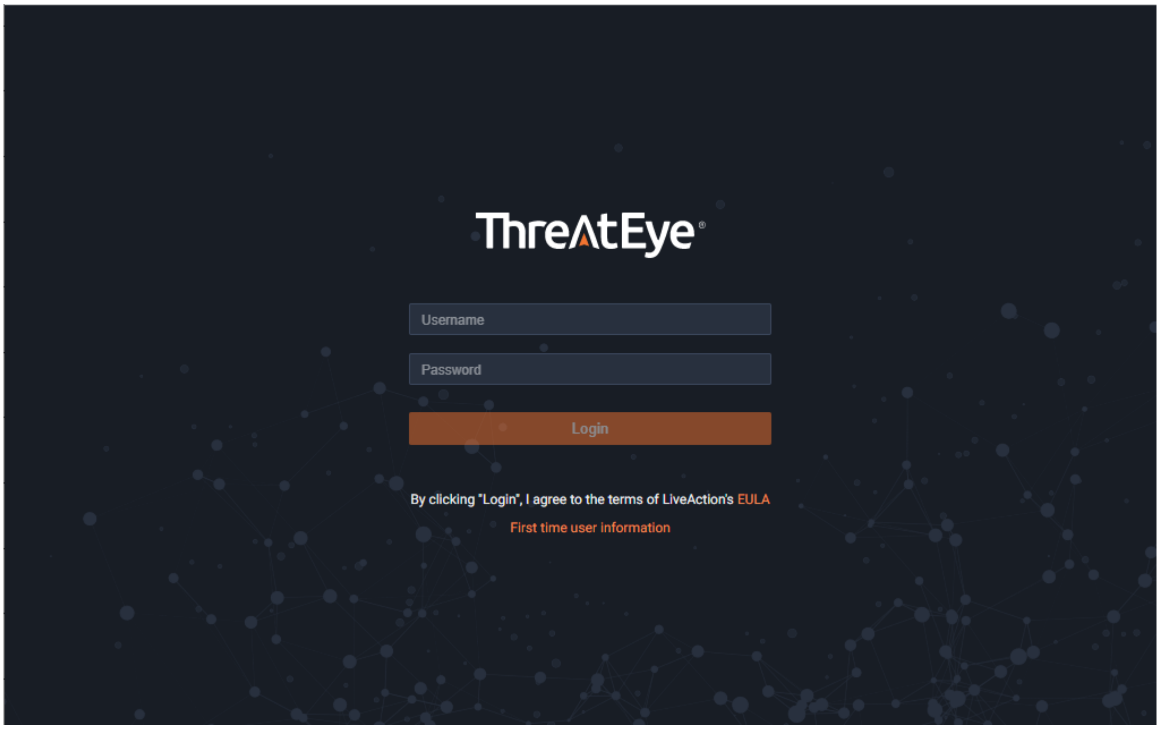
In this chapter:

Logging into ThreatEye

ThreatEye uses Role Based Access Control (RBAC) to restrict access to various components of ThreatEye. Your ThreatEye admin assigns the roles for various users. If you are assigned an Administrator role, you have full access to all ThreatEye components, including the *Settings* options. If you are not assigned an Administrator role, the *Settings* options are not displayed and available when you log into ThreatEye.

To log into ThreatEye:

1. Enter the URL provided by LiveAction into your browser to access the ThreatEye login screen.



By clicking "Login", I agree to the terms of LiveAction's EULA

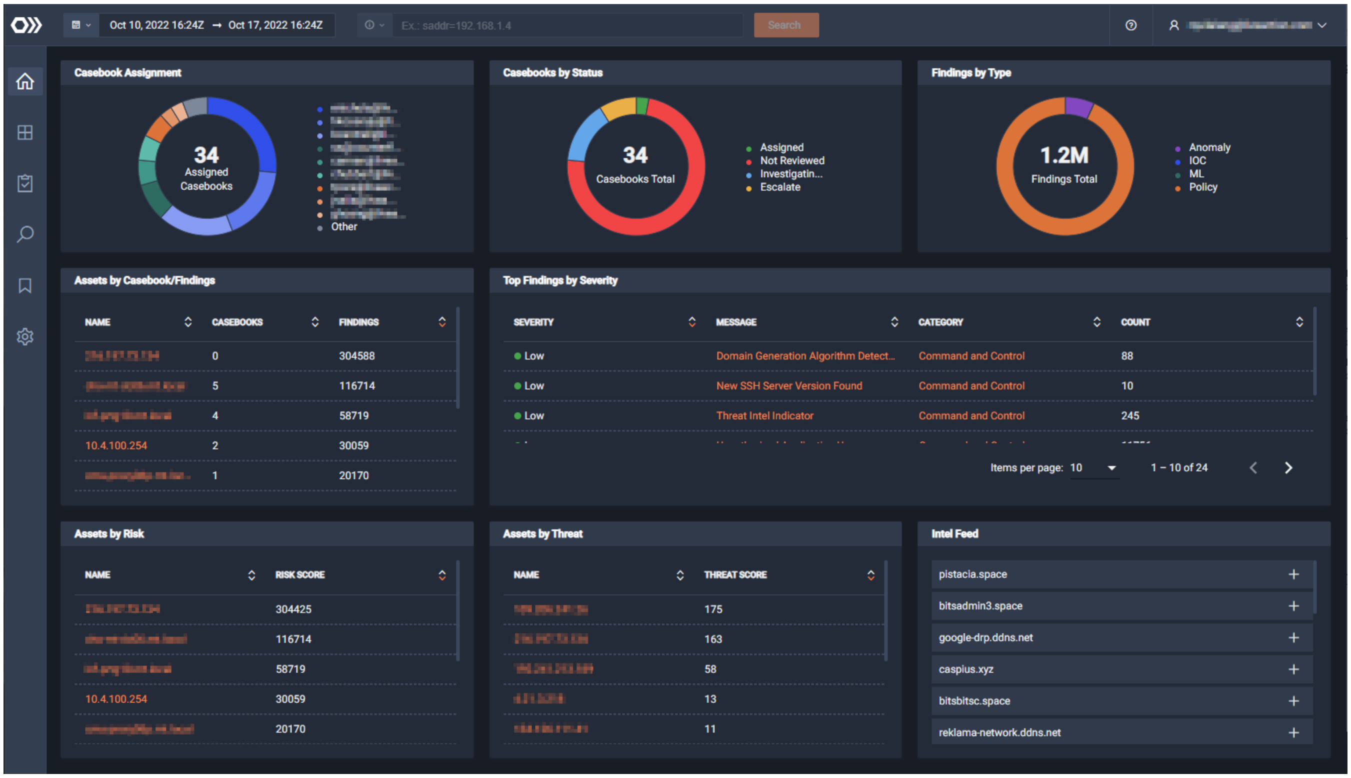
First time user information

2. Enter your *Username* and *Password* and click **Login**.

Note Your access to ThreatEye is available for one hour. After one hour, you will automatically be logged out of ThreatEye and you will need to log in again if you want to continue using ThreatEye.

The ThreatEye Interface

The ThreatEye interface is where managers and analysts can see their network environment's health using ThreatEye's comprehensive dashboards and widgets. The dashboards and widgets give a quick overview, and if needed, the ability to drill down in more detail. The remainder of this guide describes the various parts of the ThreatEye interface.



Assets by Casebook/Findings

NAME	CASEBOOKS	FINDINGS
[redacted]	0	304588
[redacted]	5	116714
[redacted]	4	58719
10.4.100.254	2	30059
[redacted]	1	20170

Top Findings by Severity

SEVERITY	MESSAGE	CATEGORY	COUNT
● Low	Domain Generation Algorithm Detect...	Command and Control	88
● Low	New SSH Server Version Found	Command and Control	10
● Low	Threat Intel Indicator	Command and Control	245

Items per page: 10 1 – 10 of 24

Assets by Risk

NAME	RISK SCORE
[redacted]	304425
[redacted]	116714
[redacted]	58719
10.4.100.254	30059
[redacted]	20170

Assets by Threat

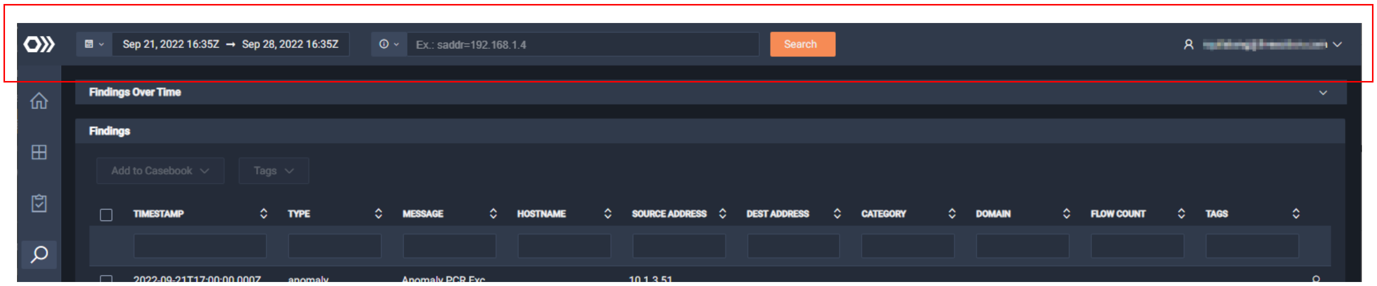
NAME	THREAT SCORE
[redacted]	175
[redacted]	163
[redacted]	58
[redacted]	13
[redacted]	11

Intel Feed

- pistacia.space +
- bitsadmin3.space +
- google-drp.ddns.net +
- caspius.xyz +
- bitsbitsc.space +
- reklama-network.ddns.net +

ThreatEye Header

The ThreatEye header at the top of the ThreatEye interface contains a *Date/Time Picker*, *Search* bar, and a *User-Preferences* drop-down menu.

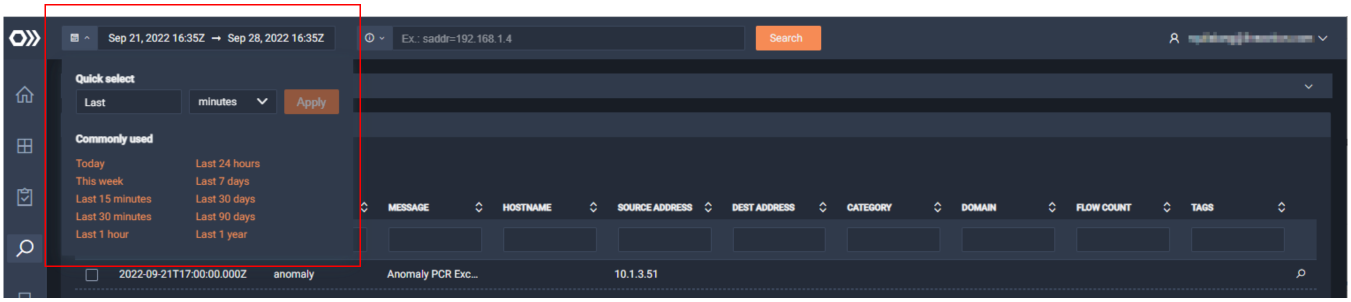


□	TIMESTAMP	TYPE	MESSAGE	HOSTNAME	SOURCE ADDRESS	DEST ADDRESS	CATEGORY	DOMAIN	FLOW COUNT	TAGS
□	2022-09-21T17:00:00.000Z	anomaly	Anomaly PCR Exc		10.1.3.51					

Date/Time Picker

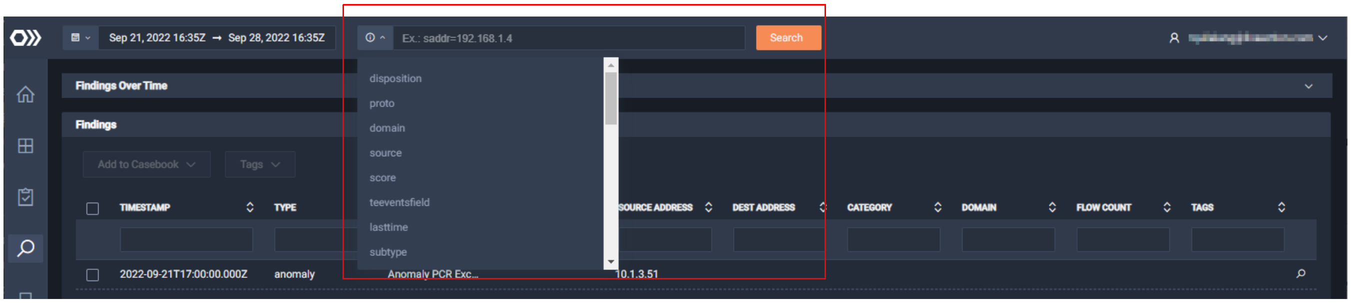
The *Date/Time Picker* lets you specify a time range for the data displayed in the dashboards and widgets below. The *Date/Time Picker* is always in UTC. All time displayed in ThreatEye is in UTC. You have three options for specifying a time range:

- *Quick select*: Click the drop-down to select a time period that occurred in the past. Click **Apply**.
- *Commonly used*: Select a pre-defined time period.
- *Manually*: Click inside the box and manually select a time period. Click **Apply**.



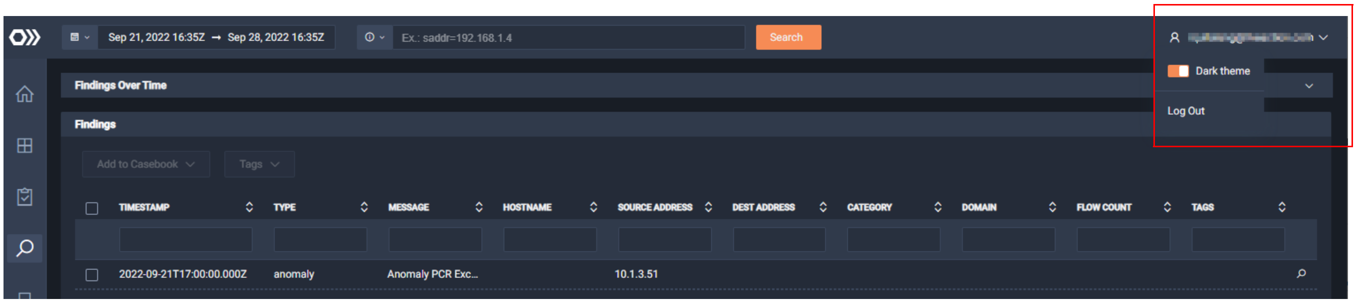
Search

The *Search* bar is used exclusively in the *Findings Explorer* dashboard and allows you to further filter the findings displayed in the *Findings Explorer* dashboard. See *Findings Explorer* on page 22 for additional information on using the Search bar in the *Findings Explorer* dashboard.



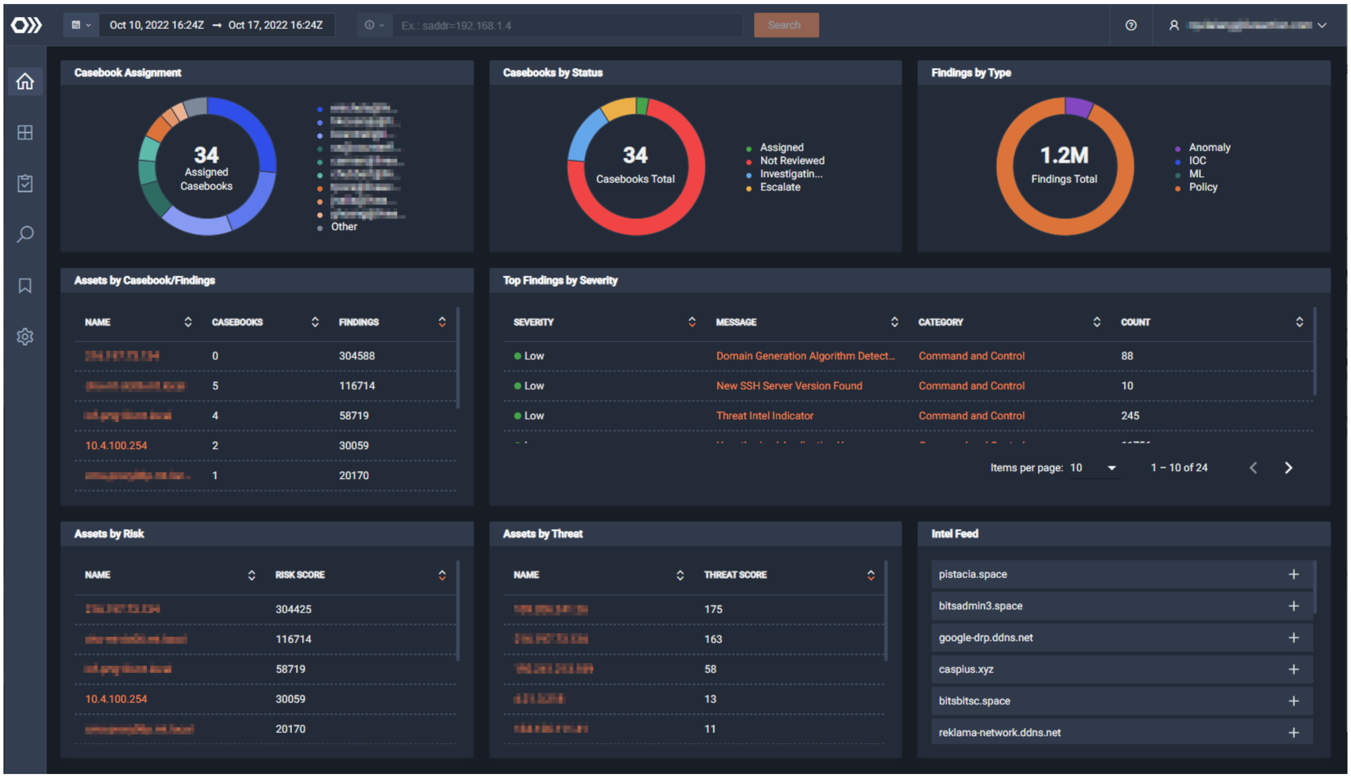
User Preferences

The *User Preferences* drop-down menu lets you toggle the interface between a dark or light theme, and also lets you *Log Out* of ThreatEye.



Executive Dashboard

The Executive Dashboard displays a high level detail of all the casebooks, findings, risks, and threats. This gives managers and analysts a birds-eye overview of what is going on in your environment. The *Casebook by Assignment* and *Casebook by Status* widgets display data for all time. The remaining widgets display data for the time-frame configured in the *Date/Time Picker*.



Assets by Casebook/Findings

NAME	CASEBOOKS	FINDINGS
[redacted]	0	304588
[redacted]	5	116714
[redacted]	4	58719
10.4.100.254	2	30059
[redacted]	1	20170

Top Findings by Severity

SEVERITY	MESSAGE	CATEGORY	COUNT
● Low	Domain Generation Algorithm Detect...	Command and Control	88
● Low	New SSH Server Version Found	Command and Control	10
● Low	Threat Intel Indicator	Command and Control	245

Items per page: 10 1 – 10 of 24

Assets by Risk

NAME	RISK SCORE
[redacted]	304425
[redacted]	116714
[redacted]	58719
10.4.100.254	30059
[redacted]	20170

Assets by Threat

NAME	THREAT SCORE
[redacted]	175
[redacted]	163
[redacted]	58
[redacted]	13
[redacted]	11

Intel Feed

- pistacia.space +
- bitsadmin3.space +
- google-drp.ddns.net +
- caspius.xyz +
- bitsbitsc.space +
- reklama-network.ddns.net +

Casebook Assignment

The *Casebook Assignment* widget displays the number of casebooks assigned to each analyst/manager. This allows you to view how workloads are currently distributed across the organization. Assigned casebooks exclude closed cases.

Casebooks by Status

The *Casebook by Status* widget displays the total number of casebooks and their reviewed status (*Assigned*, *Not Reviewed*, *Investigating*, and *Escalate*). This allows you to view if there are a backlod of casebooks that are not being worked on, or if casebooks are being escalated and not being closed. *Casebook by Status* exclude closed cases.

Findings by Type

The *Findings by Type* widget displays a breakdown of different types of findings:

- *Anomaly*: These are behaviorial anomalies, which are deviations from an average over time.
- *IOC*: These are matches against the Silent Push threat feed, which are basically the sessions that match an IP or domain in that particular threat feed.
- *ML*: These are threats to the network discovered by Machine Learning. These threats are not obvious and are a collection of bad actors' behaviors over time.

- *Policy*: These are policy violations specific to your company's policies. For example, a session that uses a DNS server that is not an approved DNS server, or a session that uses an unsupported TLS version, like an old TLS version.

Assets by Casebook/Findings

The *Assets by Casebook/Findings* widget displays the number of casebooks that reference a particular asset, and the number of findings that are associated with the asset. This allows you to view what assets in your environment have been targeted.

- *Name*: The name of the asset within your environment. Click the *Name* of an asset to open a new tab that displays details of the findings associated with the asset.
- *Casebooks*: The number of casebooks that reference the asset.
- *Findings*: The number of findings associated with asset.

Top Findings by Severity

The *Top Findings by Severity* widget displays details about the findings within your environment.

- *Severity*: The severity level of the finding (*Low*, *Medium*, *High*, *Critical*)
- *Message*: The name of the threat. Click the *Message* to open a new tab that displays details of the findings associated with the message.
- *Category*: The category of the threat. Click the *Category* to open a new tab that displays details of the findings associated with the category.
- *Count*: The number of times a finding was reported.

Assets by Risk

The *Assets by Risk* widget displays the assets within your environment and their associated risk score.

- *Name*: The name of the asset.
- *Risk Score*: The number of policy violations associated with the asset.

Assets by Threat

The *Assets by Threat* widget displays the top ten assets within your environment and their respective threat score. This widget allows managers/analysts to see what assets are being targeted by threats.

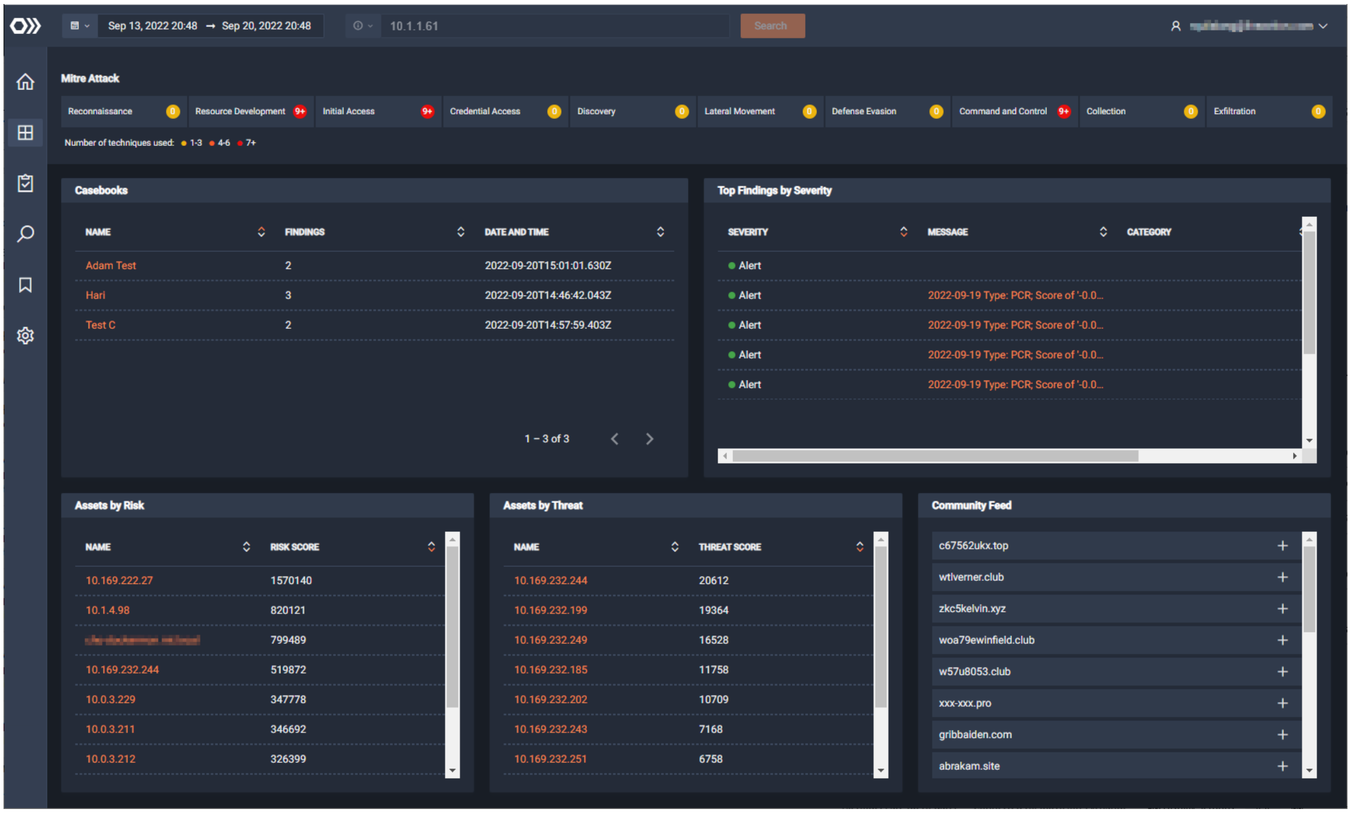
- *Name*: The name of the asset.
- *Threat Score*: The calculated score that shows how much of a threat an asset is to your environment. The *Threat Score* is directly related to the number of findings.

Intel Feed

A feed in Silent Push that aggregates indicators from various threat feeds and displays the top 20 threats that you should be aware of. Click on a feed to show you the context. The *Intel Feed* is constantly updated every 12 hours.

Analyst Dashboard

The *Analyst Dashboard* displays more in-depth information on the types of threats and attacks monitored in your environment. This dashboard allows the analyst to see specific casebooks, findings, and assets. The *Casebooks* widget displays data for all time. The remaining widgets display data for the time-frame configured in the *Date/Time Picker*.



Casebooks

NAME	FINDINGS	DATE AND TIME
Adam Test	2	2022-09-20T15:01:01.630Z
Hari	3	2022-09-20T14:46:42.043Z
Test C	2	2022-09-20T14:57:59.403Z

1 – 3 of 3

Top Findings by Severity

SEVERITY	MESSAGE	CATEGORY
● Alert		
● Alert	2022-09-19 Type: PCR; Score of '-0.0...	
● Alert	2022-09-19 Type: PCR; Score of '-0.0...	
● Alert	2022-09-19 Type: PCR; Score of '-0.0...	
● Alert	2022-09-19 Type: PCR; Score of '-0.0...	

Assets by Risk

NAME	RISK SCORE
10.169.222.27	1570140
10.1.4.98	820121
[redacted]	799489
10.169.232.244	519872
10.0.3.229	347778
10.0.3.211	346692
10.0.3.212	326399

Assets by Threat

NAME	THREAT SCORE
10.169.232.244	20612
10.169.232.199	19364
10.169.232.249	16528
10.169.232.185	11758
10.169.232.202	10709
10.169.232.243	7168
10.169.232.251	6758

Community Feed

c67562ukx.top +
wtlverner.club +
zkc5kelvin.xyz +
woa79ewinfield.club +
w57u8053.club +
xxx-xxx.pro +
gribbaiden.com +
abrakam.site +

Mitre Attack

The *Mitre Attack* widget shows you the number of findings in the various categories used to attack/infiltrate your environment. Click a *Mitre Attack* category and the *Top Findings by Severity* widget is updated to show the findings associated with the category. The descriptions for various attacks can be found here: *https://attack.mitre.org/tactics/enterprise/*.

- *Reconnaissance*: Displays how many times your environment has been tested or checked for potential vulnerabilities.
- *Resource Development*: Displays how many times your environment has been under threat by external entities to gain resources for supporting their operations within your environment.
- *Initial Access*: Displays how many times your environment has been breached to give initial access to an external resource.
- *Credential Access*: Displays how many times usernames/passwords have been compromised within your environment.
- *Discovery*: Displays how many times your environment has been mapped to gain knowledge about your system and environment.
- *Lateral Movement*: Displays how many times an external entity has moved within resources in your environment.
- *Defense Evasion*: Displays how many times an external entity has used an evasive technique to avoid detection.

- *Command and Control*: Displays how many times an external entity has attempted to communicate and control potential compromised systems.
- *Collection*: Displays how many times different collection techniques have been implemented to gather data and information within your environment.
- *Exfiltration*: Displays how many times data has been extracted from in your environment.

Casebooks

The *Casebooks* widget displays the number of casebooks.

- *Name*: The name of the casebook. Click the *Name* to view the casebook in the *Casebooks* dashboard.
- *Findings*: The number of findings within the casebook.
- *Date and Time*: The date and time each casebook is opened/updated.

Top Findings by Severity

The *Top Findings by Severity* widget displays details about the findings within your environment.

- *Severity*: The severity level of the finding (Low, Medium, High, Alert)
- *Message*: Name of the Threat. Click the *Message* to open a new tab that displays details of the findings associated with the message.
- *Category*: Category of the Threat. Click the *Category* to open a new tab that displays details of the findings associated with the category.
- *Count*: Number of times finding was reported.

Assets by Risk

The *Assets by Risk* widget displays the assets in your environment and their associated risk score.

- *Name*: The name of the asset.
- *Risk Score*: The number of policy violations associated with the asset.

Assets by Threat

The *Assets by Threat* widget displays the assets in your environment and their respective threat score. This widget allows managers/analysts to see what assets are being targeted by threats.

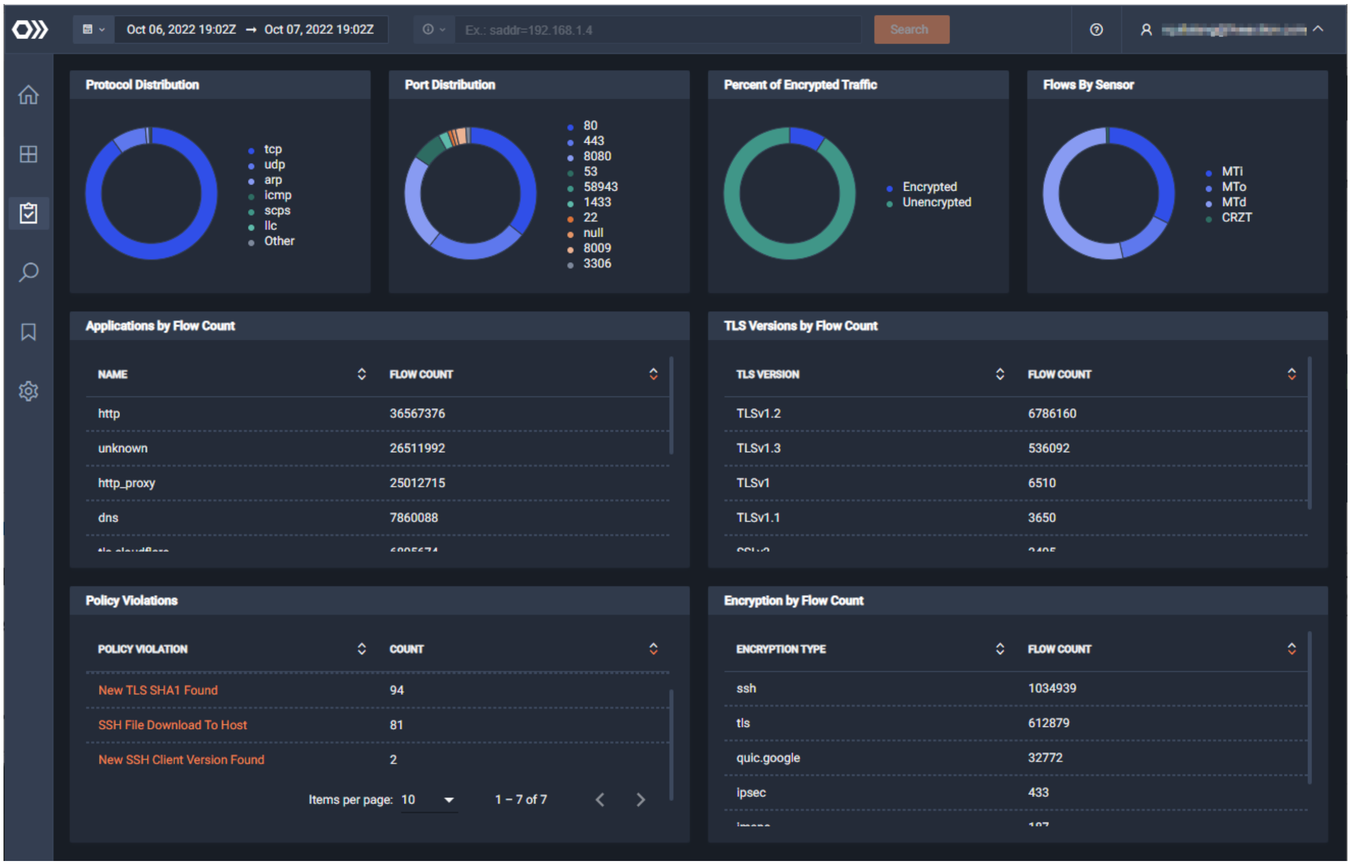
- *Name*: The name of the asset.
- *Threat Score*: The calculated score that shows how much of a threat an asset is to your environment. The *Threat Score* is directly related to the number of findings.

Intel Feed

A feed in Silent Push that aggregates indicators from various threat feeds and displays the top 20 threats that you should be aware of. Click on a feed to show you the context. The *Intel Feed* is constantly updated every 12 hours.

Policy Investigation Dashboard

The *Policy Investigation* dashboard contains widgets that display high-level policy information about what is going on in your environment in the time-frame configured in the *Date/Time Picker*.



Applications by Flow Count

NAME	FLOW COUNT
http	36567376
unknown	26511992
http_proxy	25012715
dns	7860088

TLS Versions by Flow Count

TLS VERSION	FLOW COUNT
TLSv1.2	6786160
TLSv1.3	536092
TLSv1	6510
TLSv1.1	3650

Policy Violations

POLICY VIOLATION	COUNT
New TLS SHA1 Found	94
SSH File Download To Host	81
New SSH Client Version Found	2

Items per page: 10 1 – 7 of 7

Encryption by Flow Count

ENCRYPTION TYPE	FLOW COUNT
ssh	1034939
tls	612879
quic.google	32772
ipsec	433

Protocol Distribution

The *Protocol Distribution* widget displays the type of protocols and their frequency that are being used to communicate in your environment. For example, TCP, UDP, etc.

Port Distribution

The *Port Distribution* widget displays the ports and their frequency that are being used for various connections in your environment.

Percent of Encrypted Traffic

The *Percent of Encrypted Traffic* widget displays the percent of traffic that is encrypted vs. unencrypted in your environment.

Flows By Sensor

The *Flows By Sensor* widget displays the number of flows by the LiveWire connected to ThreatEye.

Applications by Flow Count

The *Applications by Flow Count* widget displays the applications and their number of flows used in your environment.

- *Name*: The name of the type of communication protocol used in your environment.

- *Flow Count*: The number of flows the communication protocol has initiated in your environment.

TLS Versions by Flow Count

The *TLS Versions by Flow Count* widget displays the TLS versions and their number of flows in your environment.

- *TLS Version*: The version of TLS in your environment.
- *Flow Count*: The number of flows within each TLS Version.

Policy Violations

The *Policy Violations* widget displays the policy violations and their counts that were detected in your environment.

- *Policy Violation*: The type of policy violation occurring within your environment.
- *Count*: The number of times the policy has been violated.

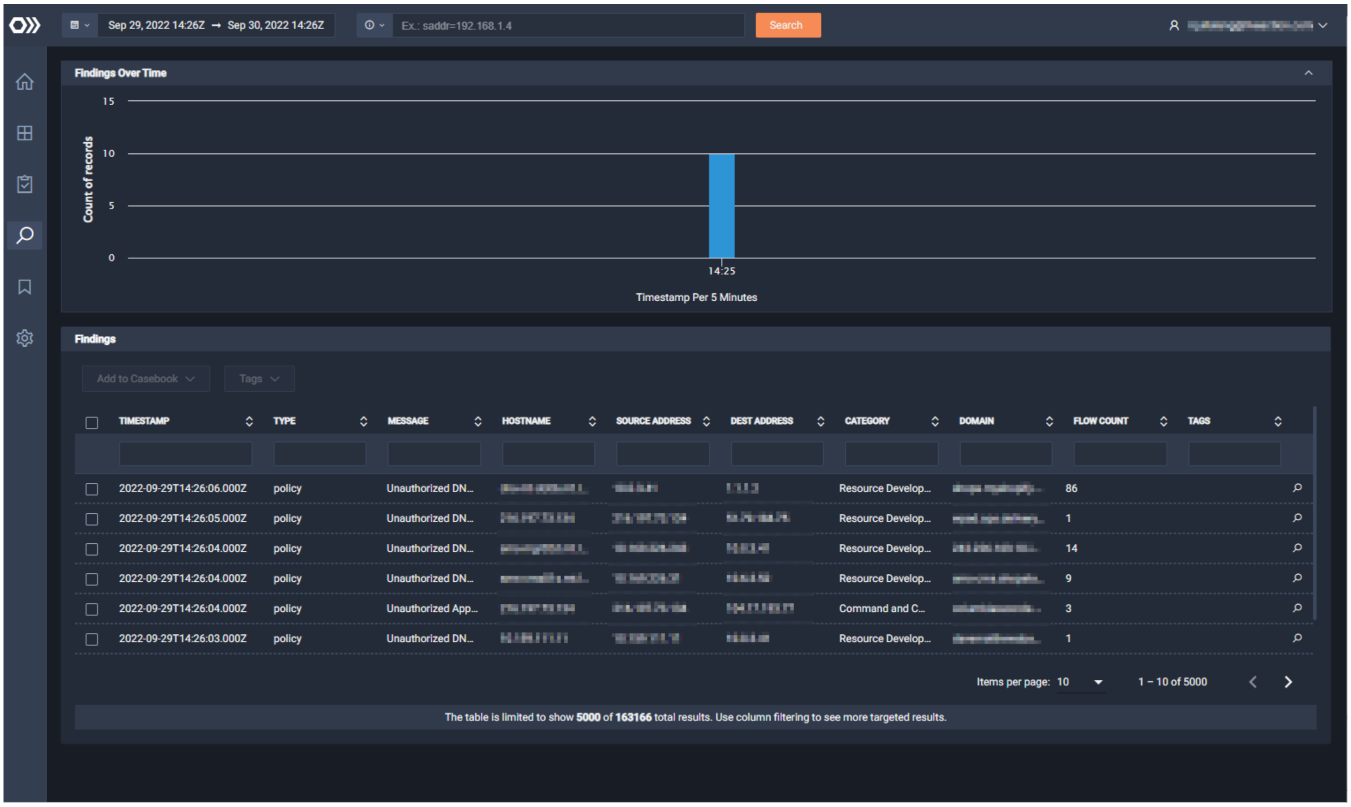
Encryption by Flow Count

The *Encryption by Flow Count* widget displays the encryption type and the number of flows that were detected in your environment.

- *Encryption Type*: The type of encryption protocol.
- *Flow Count*: The number of flows within each encryption type.

Findings Explorer

The *Findings Explorer* dashboard displays more details of the findings in your environment in the timeframe configured in the *Date/Time Picker*. These can be viewed as the number of *Findings Over Time* as well as individual *Findings*.



□	TIMESTAMP	TYPE	MESSAGE	HOSTNAME	SOURCE ADDRESS	DEST ADDRESS	CATEGORY	DOMAIN	FLOW COUNT	TAGS
□	2022-09-29T14:26:06.000Z	policy	Unauthorized DN...	[redacted]	[redacted]	[redacted]	Resource Develop...	[redacted]	86	
□	2022-09-29T14:26:05.000Z	policy	Unauthorized DN...	[redacted]	[redacted]	[redacted]	Resource Develop...	[redacted]	1	
□	2022-09-29T14:26:04.000Z	policy	Unauthorized DN...	[redacted]	[redacted]	[redacted]	Resource Develop...	[redacted]	14	
□	2022-09-29T14:26:04.000Z	policy	Unauthorized DN...	[redacted]	[redacted]	[redacted]	Resource Develop...	[redacted]	9	
□	2022-09-29T14:26:04.000Z	policy	Unauthorized App...	[redacted]	[redacted]	[redacted]	Command and C...	[redacted]	3	
□	2022-09-29T14:26:03.000Z	policy	Unauthorized DN...	[redacted]	[redacted]	[redacted]	Resource Develop...	[redacted]	1	

Items per page: 10 1 – 10 of 5000

The table is limited to show **5000** of **163166** total results. Use column filtering to see more targeted results.

Findings Over Time

The *Findings Over Time* widget displays a bar graph of the distribution of findings for the Findings listed below. This graph helps to show how often your environment is targeted and when it has been targeted. Click the up and down arrow to show or hide the bar graph.

Findings

The *Findings* widget is a table that displays each finding with information that can help you see more detailed information. Only 5000 of the total results can be displayed in the table. You can use the column filtering and the *Search* bar to see more targeted results.

- *Add to Casebook*: Click to add the selected findings to a new or existing casebook.
- *Tags*: Click to assign or unassign tags to the selected findings.
- *Timestamp*: The date and time of the finding.
- *Type*: The type of threat.
- *Message*: The name of the threat.
- *Hostname*: The hostname from where the finding originated.
- *Source Address*: The source IP address of the finding.
- *Dest Address*: The destination IP address of the finding.
- *Category*: The category of the finding which tells the analyst the type of attack.
- *Disposition*: The outcome of the research set by analyst.
- *Domain*: The domain of the finding.
- *Flow Count*: The number of flows that include the finding.
- *Tags*: The tags that help the analyst search on the type of finding.
- *Magnifying Glass (icon)*: Click the magnifying glass icon to view the details of the finding. (*Details*, *Flows*, *Finding JSON*, *PassiveDNS*, *Intelligence*, *Comments*).
    - **Findings workflow**: All findings start in the 'Not Reviewed' state. When an analyst changes the state to 'Investigating,' 'Escalate,' or 'Closed,' the assigned user is changed to the person who made the change in status. To mark a finding as 'Closed,' you must set a disposition (either *True Positive* or *False Positive*), as well as set the *Context* before you are allowed to apply the change.
    - *PassiveDNS* information is available for a finding. You can search by IP or domain.
    - *Threat Intelligence* lookup is available for the destination IP or Domain in a finding.

Note You can use the column filtering box below each of the column headings to filter for more targeted results. Simply enter a text string in the desired text box to display values matching the text string. Observe the 'total results' count at the bottom of the widget change as you filter for more targeted results.

Using the Search Bar

You can use the *Search* bar to also filter for more targeted results in your findings.

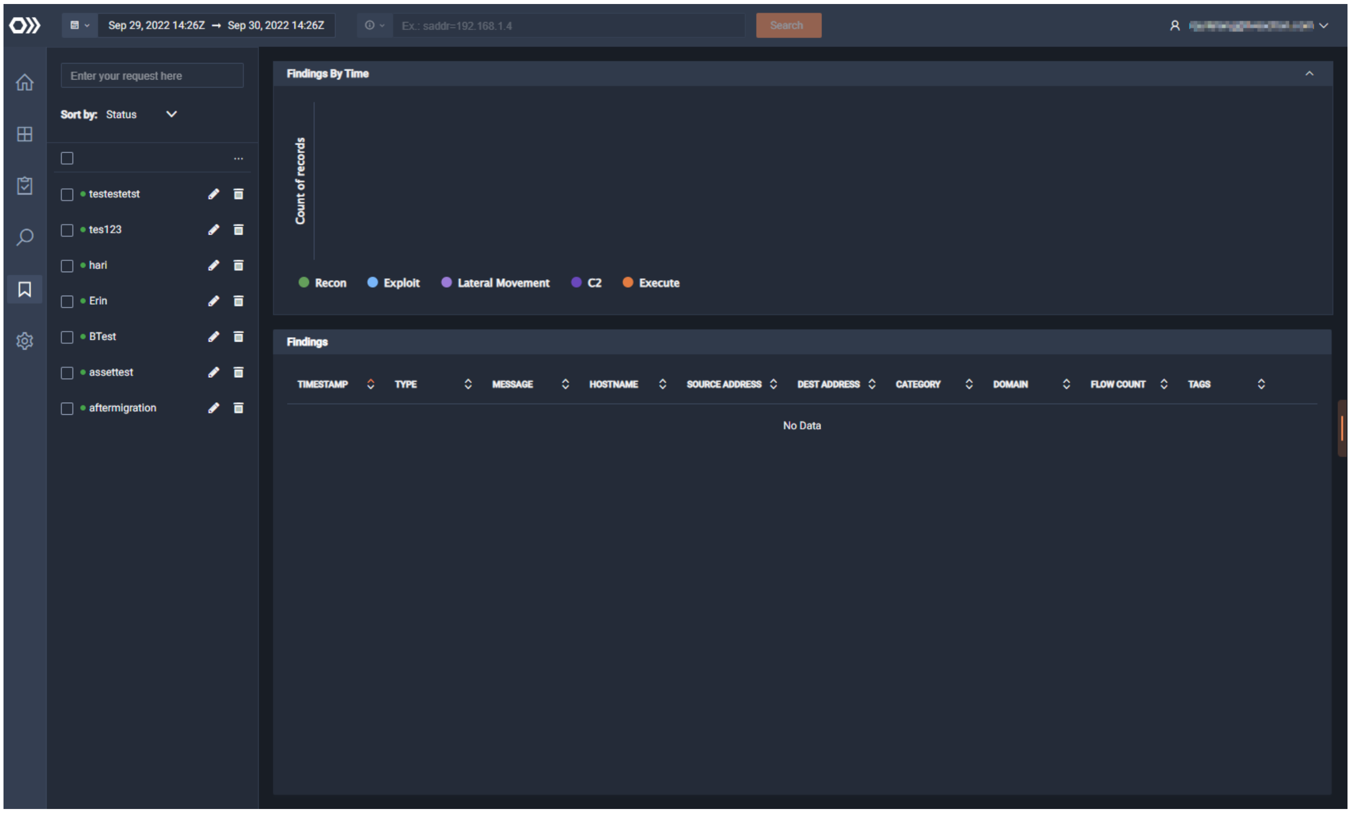
To use the search bar, you will need to:

1. Select or enter a type of key (click the *Search* drop-down to see and/or select valid keys)
2. Enter a valid operator: Valid operators are "=", "!=", ">", ">=", "<", "<=", "in", "contains", "starts with", "ends with"
3. Enter a valid value that is appropriate for the type of key selected.

For example, to search for all findings that have a source address of 192.168.1.4, enter *saddr=192.168.1.4* in the search bar and click **Search**. All findings that have that source address are displayed in the *Findings* widget.

Casebooks

The *Casebooks* dashboard displays the casebooks and the findings assigned to each casebook in the time-frame configured in the *Date/Time Picker*. A casebook is a collection of findings. A casebook can have multiple findings; however, a finding can only be associated with one casebook.



Sep 29, 2022 14:26Z → Sep 30, 2022 14:26Z

[redacted]

Sort by: Status

TIMESTAMP	TYPE	MESSAGE	HOSTNAME	SOURCE ADDRESS	DEST ADDRESS	CATEGORY	DOMAIN	FLOW COUNT	TAGS
No Data									

Casebooks

The *Casebooks* widget allows you to create, sort, add, tag, edit, and delete casebooks.

- *Enter your request here*: The *Enter your request here* text box allows you to filter casebooks by various clauses.
- *Sort by*: You can sort the list of casebooks by clicking the drop-down arrow and selecting either *Status* or *Name*.
- *Elipsis* (...): Click the elipsis to view the following options:
  - *Add*: Select to add a new casebook.
  - *Tags*: Select to select a tag for the casebook
  - *Delete*: Select to delete the selected casebooks.
- *Check Box*: Click to select the casebook. Click the check box at the top of the column to select or deselect the entire list of casebooks.
- *Edit*: Click to edit the details and comments of the casebook.
- *Delete*: Click to delete the casebook.

Findings By Time

The *Findings By Time* widget displays a bar graph of the distribution of findings for the findings listed below. This graph helps to shows how often your environment is targeted and when it has been targeted. Click the up and down arrow to show or hide the bar graph.

- *Count of records*: Displays the Y-Axis of number of findings.
- *Recon*: Displays the findings that are of a *Recon* type.
- *Exploit*: Displays the findings that are of an *Exploit* type.
- *Lateral Movement*: Displays the of findings that are of a *Lateral Movement* type.
- *C2*: Displays findings that are of a *C2* type.
- *Execute*: Displays the findings that are of an *Execute* type.

Note See *Mitre Attack* on page 19 for descriptions of the various types of attacks displayed in the *Findings By Time* widget.

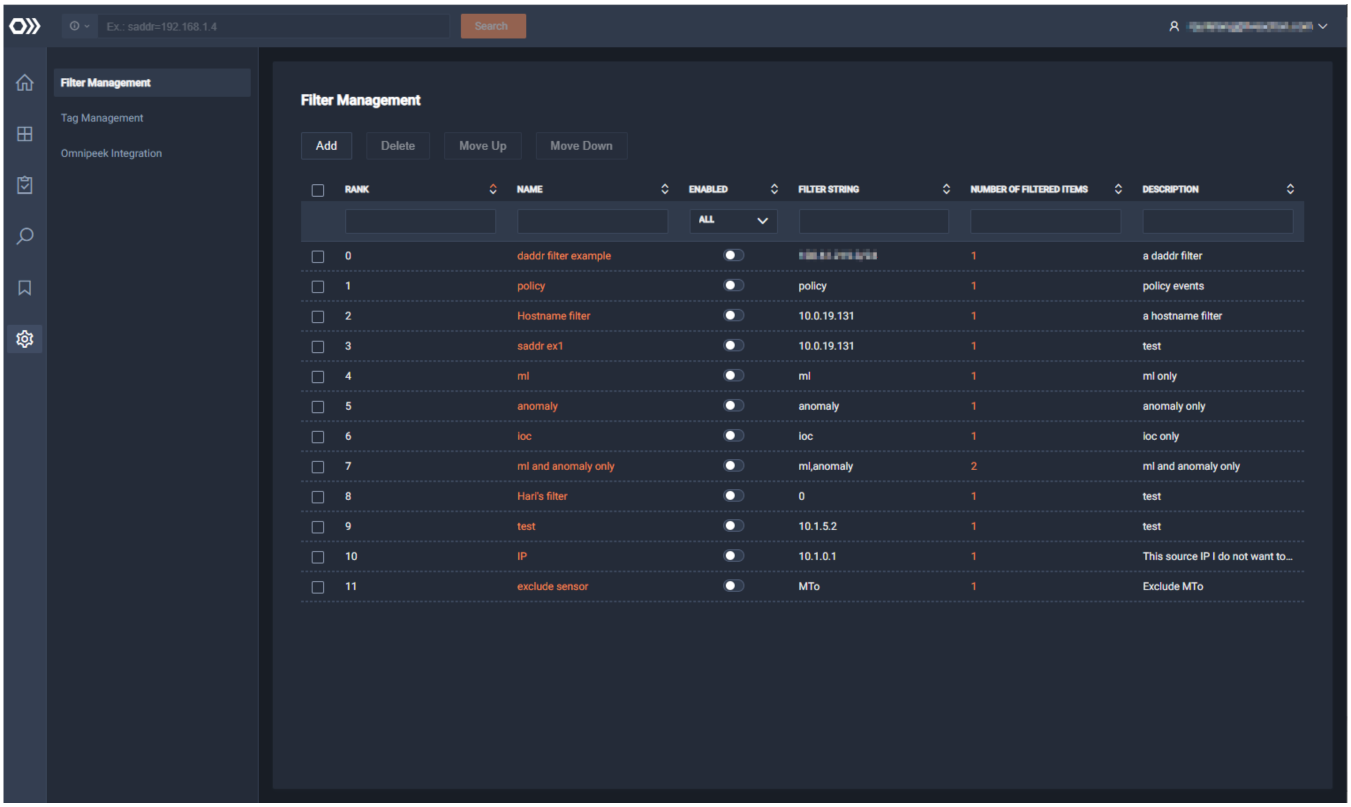
Findings

The *Findings* widget is a table that displays each finding with information that can help you see more detailed information. Only 5000 of the total results can be displayed in the table.

- *Timestamp*: The date and time of the finding.
- *Type*: The type of threat.
- *Message*: The name of the threat.
- *Hostname*: The hostname from where the finding originated.
- *Source Address*: The source IP address of the finding.
- *Dest Address*: The destination IP address of the finding.
- *Category*: The category of the finding which tells the analyst the type of attack.
- *Disposition*: The outcome of the research set by analyst.
- *Domain*: The domain of the finding.
- *Flow Count*: The number of flows that include the finding.
- *Tags*: The tags that help the analyst search on the type of finding.
- *Magnifying Glass (icon)*: Click the magnifying glass icon to view the details of the finding. (*Details*, *Flows*, *Finding JSON*, *PassiveDNS*, *Intelligence*, *Comments*).

Settings

The *Settings* dashboard allows you to edit *Filter*, *Tag*, and *Omnipeek Integration* settings. The *Settings* dashboard is only available to users that have been assigned an Administrator role in ThreatEye.



□	RANK	NAME	ENABLED	FILTER STRING	NUMBER OF FILTERED ITEMS	DESCRIPTION
			ALL			
□	0	daddr filter example	○	[redacted]	1	a daddr filter
□	1	policy	○	policy	1	policy events
□	2	Hostname filter	○	10.0.19.131	1	a hostname filter
□	3	saddr ex1	○	10.0.19.131	1	test
□	4	ml	○	ml	1	ml only
□	5	anomaly	○	anomaly	1	anomaly only
□	6	ioc	○	ioc	1	ioc only
□	7	ml and anomaly only	○	ml,anomaly	2	ml and anomaly only
□	8	Hari's filter	○	0	1	test
□	9	test	○	10.1.5.2	1	test
□	10	IP	○	10.1.0.1	1	This source IP I do not want to...
□	11	exclude sensor	○	MTo	1	Exclude MTo

Filter Management

The *Filter Management* widget lets you restrict the data presented in the ThreatEye interface. Filters are only applied to the results displayed on the *Findings Explorer* dashboard. All other widgets are never filtered.

- *Add*: Click to add a new filter to the system.
  - *Filter Name*: Type a name for the filter.
  - *Key*: Select a key for the filter.
  - *Operator*: Select an operator for the filter.
  - *Value*: Type a value for the filter.
  - *Description*: Type a description for the filter.
- *Delete*: Click to delete selected filters.
- *Move Up*: Click to move up the rank of selected filters in the list of filters. The rank determines how filters are displayed throughout ThreatEye interface.
- *Move Down*: Click to move down the rank of selected filters in the list of filters. The rank determines how filters are displayed throughout ThreatEye interface.
- *Check box*: Select the check box of the filter to modify. Selecting the check box at the top of the check box column allows you to select or deselect all filters in the list.
- *Rank*: Displays the rank of the filter
- *Name*: The name of the filter. Click the filter to edit the filter.

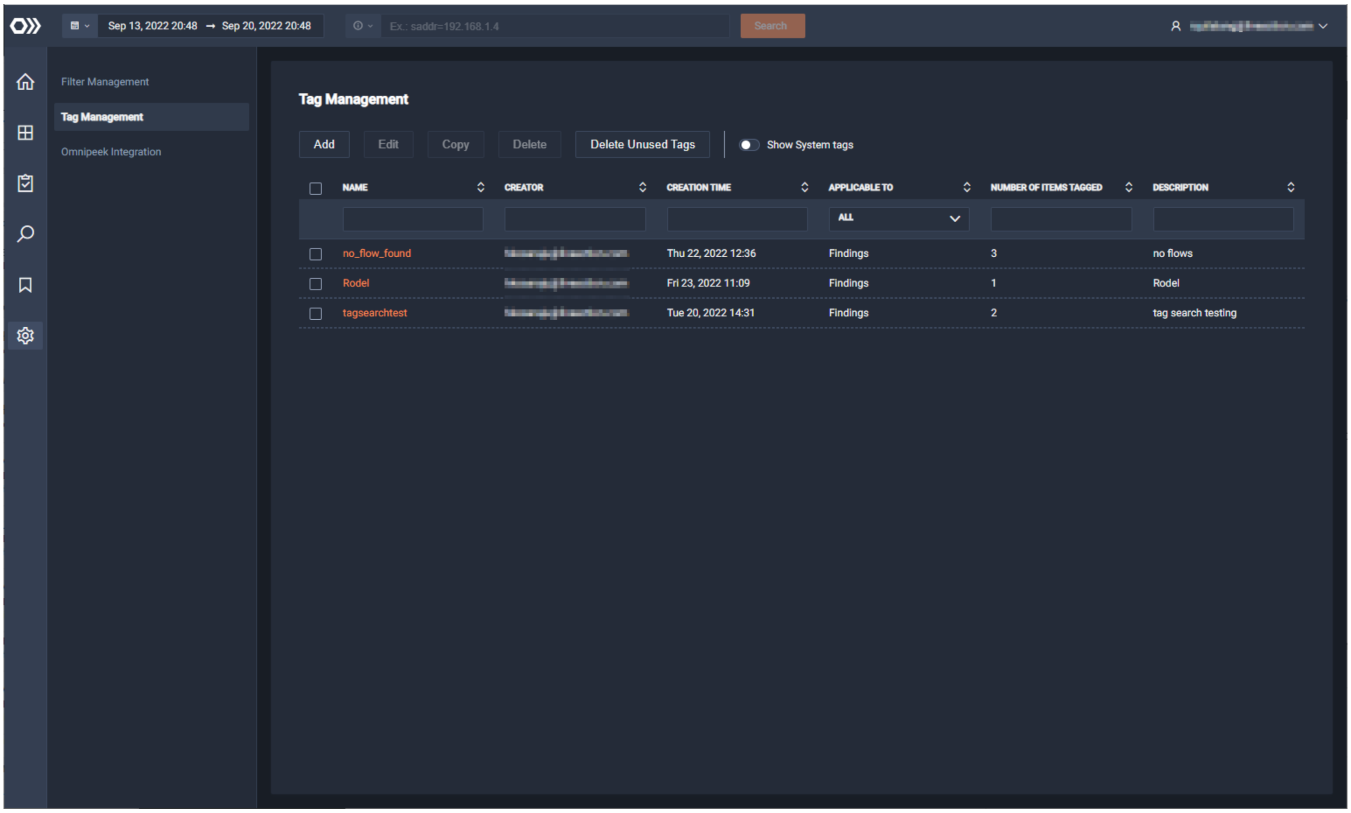
- *Enabled*: Click to toggle whether a filter is *Enabled* or *Disabled*.
- *Filter String*: Displays the filter string.
- *Number of Filtered Items*: Displays the number of filtered items.
- *Description*: Displays the description of the filter.

Note You can use the column filtering box below each of the column headings to filter for more targeted results. Simply enter a text string in the desired text box to display values matching the text string.

Tag Management

The *Tag Management* widget lets you manage the tags created in ThreatEye. Tags can be added to either casebooks or findings. Tags allow teams to add their own workflow to ThreatEye. Administrators can create tags in the *Tag Management* widget. Analysts or administrators can then apply tags.

You can search for a tag using the keyword “tags” in the search bar. For example, *tags=windows_server*. There are both system and user tags used in ThreatEye. System tags cannot be edited or deleted.



Tag Management

☐	NAME	CREATOR	CREATION TIME	APPLICABLE TO	NUMBER OF ITEMS TAGGED	DESCRIPTION
				ALL		
☐	no_flow_found	[redacted]	Thu 22, 2022 12:36	Findings	3	no flows
☐	Rodel	[redacted]	Fri 23, 2022 11:09	Findings	1	Rodel
☐	tagsearchtest	[redacted]	Tue 20, 2022 14:31	Findings	2	tag search testing

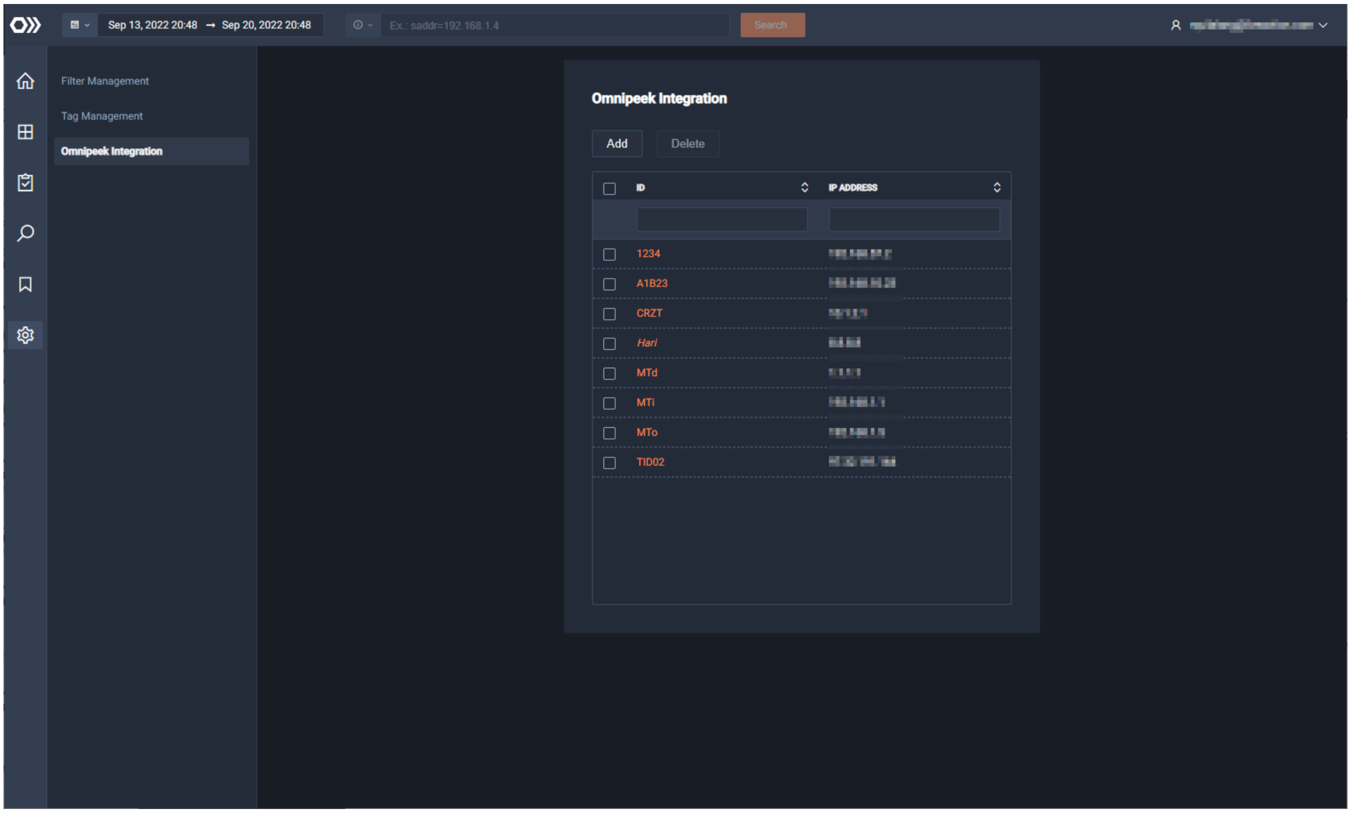
- *Add*: Click to add a new tag to the system.
- *Copy*: Click to copy the selected tag and its properties. Only one tag can be copied at a time.
- *Delete*: Click to delete the selected tags.
- *Delete Unused Tags*: Click to delete all tags which are not associated to a finding.
- *Show System Tags:* Use this toggle to show *System tags*.
- *Check box*: Select the check box of the tag to select the tag. Selecting the check box at the top of the column allows you to select or deselect all tags in the list. All system tags will not have a check box and cannot be selected.
- *Name*: The name of the tag.

- *Creator*: The user that created the tag.
- *Creation Time*: The date and time the tag was created.
- *Applicable To*: Displays whether the tag is applicable to casebooks or findings.
- *Number of Items Tagged*: The number of findings in a tag.
- *Description*: The description of the tag.

> **Note** You can use the column filtering box below each of the column headings to filter for more targeted results. Simply enter a text string in the desired text box to display values matching the text string.

Omnipeek Integration

The *Omnipeek Integration* widget lets you map the source field in the findings to an IP address of a Live-Wire appliance. These settings are for integrating flow data from LiveWire which allows you to perform detailed packet analysis.



Omnipeek Integration

Add Delete

□	ID	IP ADDRESS
□	1234	[redacted]
□	A1B23	[redacted]
□	CRZT	[redacted]
□	*Hari*	[redacted]
□	MTd	[redacted]
□	MTi	[redacted]
□	MTo	[redacted]
□	TID02	[redacted]

- *Add*: Click to add an Omnipeek integration. You will need to specify a unique ID and the IP address of the LiveWire appliance providing flow data.
- *Delete*: Click to delete the selected Omnipeek integrations.
- *ID*: The ID specified for the integration. See also *Monitor ID* in *Updating Your ThreatEye License* on page 5.
- *IP Address*: The IP address of the LiveWire appliance providing flow data.