Trellix

21 – 24 OCTOBER 2024

EMEA & LTAM Partner Tech Summit

Lisbon, Portugal

Trellix

XDR

Fernando Segura

Principal Architect Professional Services

Oct 23, 2024

Agenda

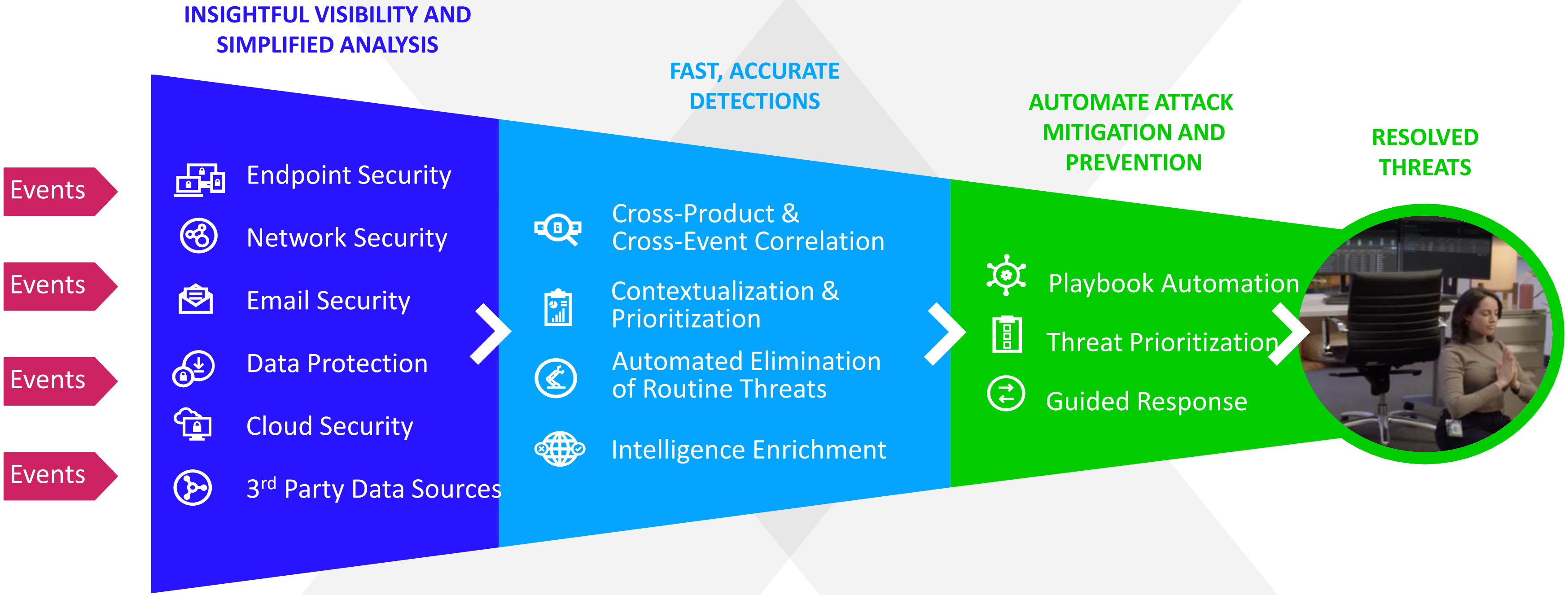
Acerca de nosotros
Introducción
Trellix XDR Solution resumen
Trellix XDR Architecture
Trellix XDR consideraciones de deployment
Trellix XDR Guia y demostración
(y casos de uso)

Acerca de nosotros

Fernando Segura

Principal Solutions
Architect Trellix
Professional Services

Introducción



INSIGHTFUL VISIBILITY AND SIMPLIFIED ANALYSIS

FAST, ACCURATE DETECTIONS

AUTOMATE ATTACK MITIGATION AND PREVENTION

RESOLVED THREATS

- Events
- Events
- Events
- Events

- Endpoint Security
- Network Security
- Email Security
- Data Protection
- Cloud Security
- 3rd Party Data Sources

- Cross-Product & Cross-Event Correlation
- Contextualization & Prioritization
- Automated Elimination of Routine Threats
- Intelligence Enrichment

- Playbook Automation
- Threat Prioritization
- Guided Response

Trellix

Trellix XDR Impacto en el cliente

	Time to Resolution	SOC Resources	Threat Coverage
ANTES	Semanas	Sobrecarga y recursos limitados	Imposibilidad de determinar, Prioriza las principales amenazas
DESPUÉS	Días	Eficaz, eficiente, Optimizado	Detecciones y mitigaciones rápidas y precisas para las alertas principales

Resultado: una experiencia de operaciones de seguridad simplificada y perspicaz para detener rápidamente los ataques

Cobertura XDR de Trellix

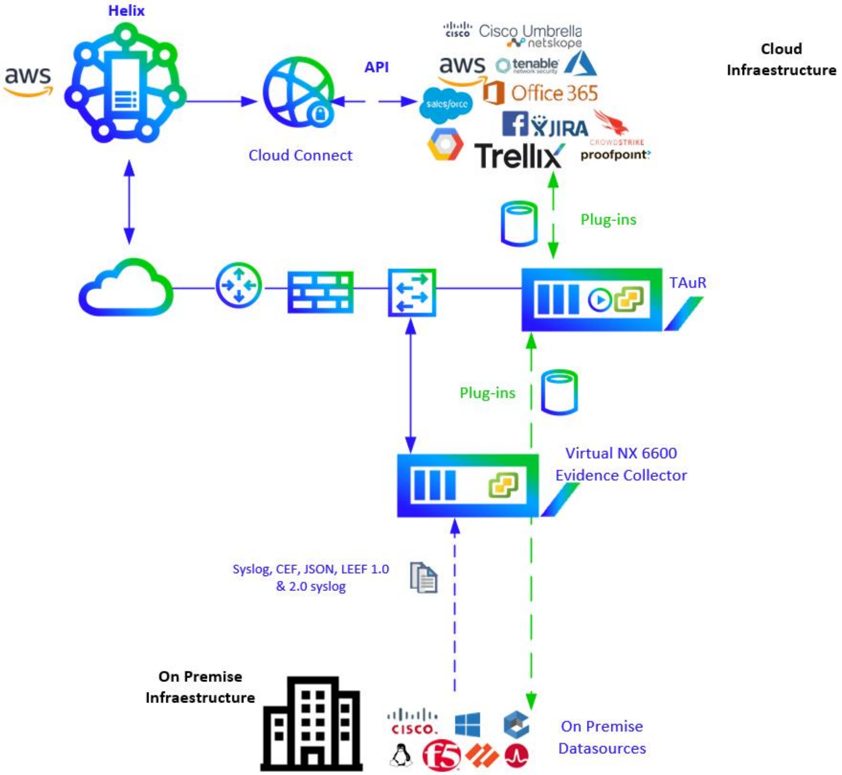
	Endpoint Security (EDR)	SIEMs	Trellix XDR
Telemetría y eventos enriquecidos	⊖	⊗	✓
Amplia gama de datos de terceros / Integración de alertas	⊗	✓	✓
Análisis de seguridad profundos	✓	✓	✓
Respuesta configurable Acciones	⊖	✓	✓
Información de amenazas nativas y de 3ª party	⊖	⊖	✓

Trellix

Arquitectura

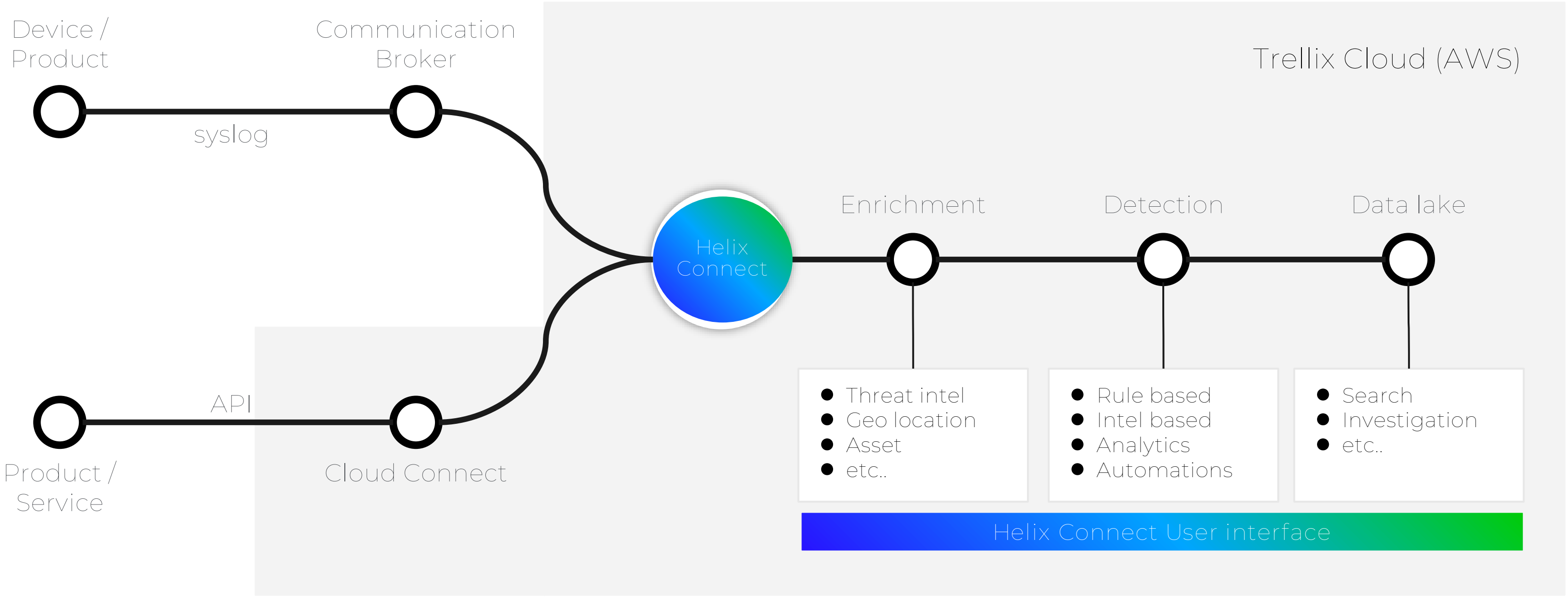
Arquitectura e Integraciones

Arquitectura



Trellix

Helix Connect arquitectura



- Threat intel
- Geo location
- Asset
- etc..

- Rule based
- Intel based
- Analytics
- Automations

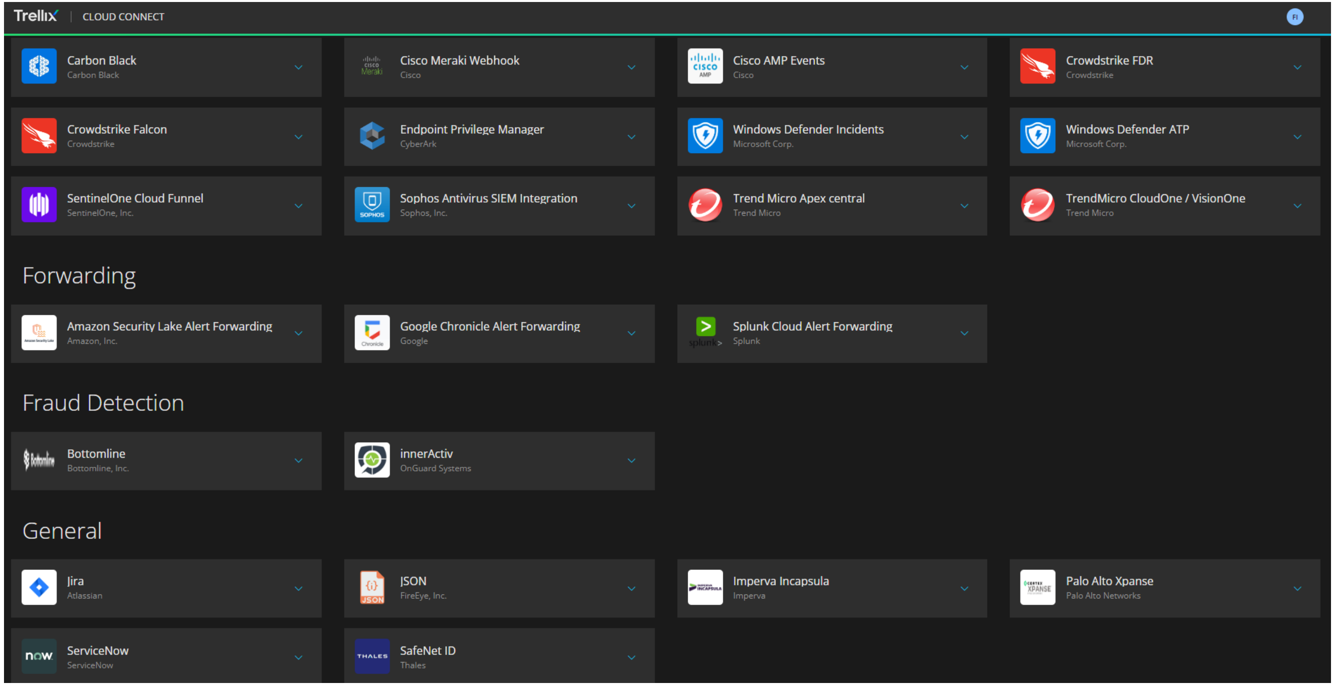
- Search
- Investigation
- etc..

Helix Connect User interface

Trellix

Cloud Connect portal

Las conexiones en la nube XDR permiten que los eventos y registros de los productos de Trellix y los productos de seguridad de otros proveedores se envíen a XDR a través de conexiones API.



Trellix | CLOUD CONNECT

FI

Carbon Black
Carbon Black

Cisco Meraki Webhook
Cisco

Cisco AMP Events
Cisco

Crowdstrike FDR
Crowdstrike

Crowdstrike Falcon
Crowdstrike

Endpoint Privilege Manager
CyberArk

Windows Defender Incidents
Microsoft Corp.

Windows Defender ATP
Microsoft Corp.

SentinelOne Cloud Funnel
SentinelOne, Inc.

Sophos Antivirus SIEM Integration
Sophos, Inc.

Trend Micro Apex central
Trend Micro

TrendMicro CloudOne / VisionOne
Trend Micro

Forwarding

Amazon Security Lake Alert Forwarding
Amazon, Inc.

Google Chronicle Alert Forwarding
Google

Splunk Cloud Alert Forwarding
Splunk

Fraud Detection

Bottomline
Bottomline, Inc.

innerActiv
OnGuard Systems

General

Jira
Atlassian

JSON
FireEye, Inc.

Imperva Incapsula
Imperva

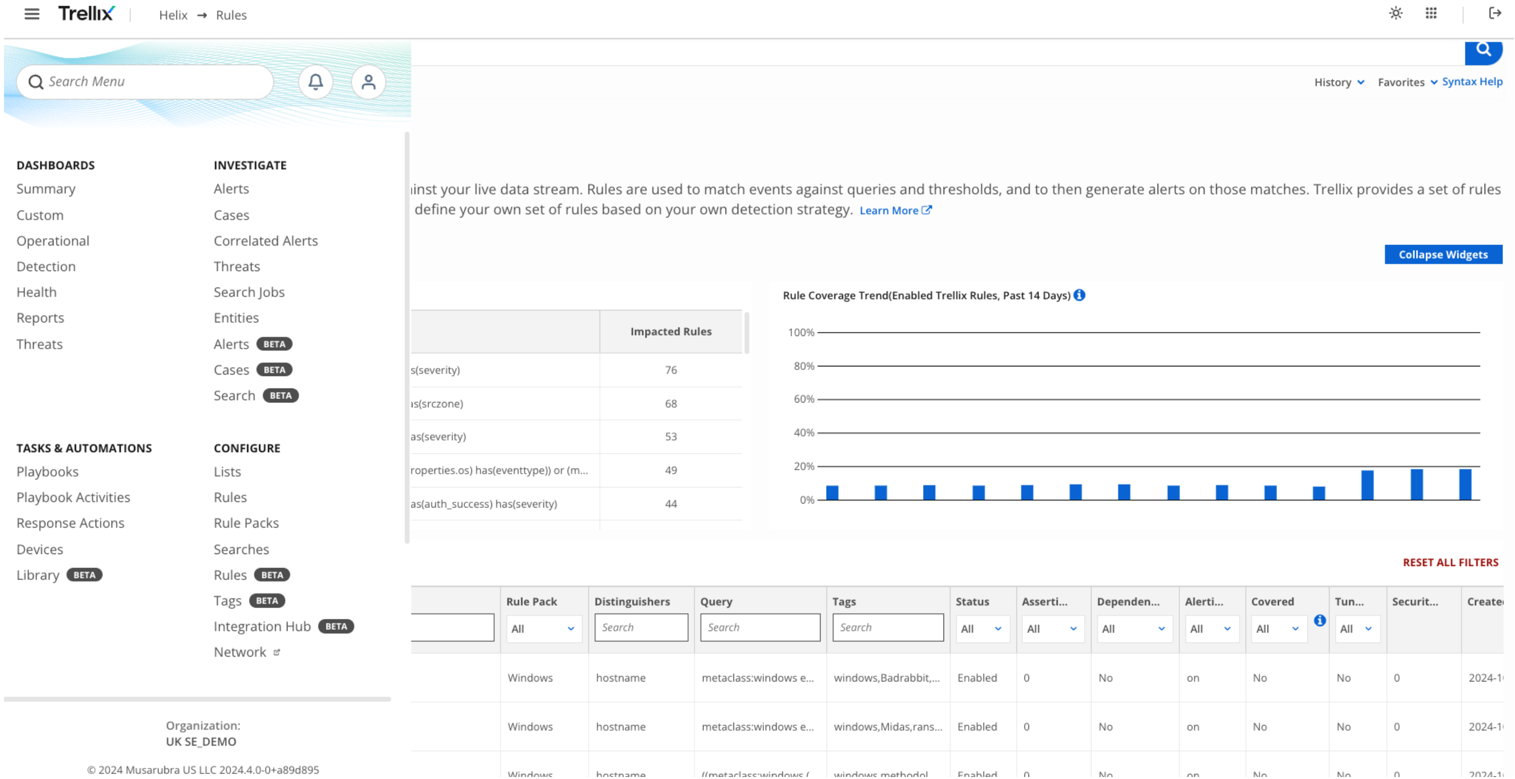
Palo Alto Xpanse
Palo Alto Networks

ServiceNow
ServiceNow

SafeNet ID
Thales

Trellix

Apps – Nuevas, Beta, Legacy



DASHBOARDS
- Summary
- Custom
- Operational
- Detection
- Health
- Reports
- Threats

INVESTIGATE
- Alerts
- Cases
- Correlated Alerts
- Threats
- Search Jobs
- Entities
- Alerts BETA
- Cases BETA
- Search BETA

TASKS & AUTOMATIONS
- Playbooks
- Playbook Activities
- Response Actions
- Devices
- Library BETA

CONFIGURE
- Lists
- Rules
- Rule Packs
- Searches
- Rules BETA
- Tags BETA
- Integration Hub BETA
- Network

Organization:
UK SE_DEMO

© 2024 Musarubra US LLC 2024.4.0-0+a89d895

ɪinst your live data stream. Rules are used to match events against queries and thresholds, and to then generate alerts on those matches. Trellix provides a set of rules define your own set of rules based on your own detection strategy. Learn More

	Impacted Rules
s(severity)	76
ɪs(srczone)	68
as(severity)	53
roperties.os) has(eventtype)) or (m...	49
as(auth_success) has(severity)	44

Rule Coverage Trend(Enabled Trellix Rules, Past 14 Days)

	Rule Pack	Distinguishers	Query	Tags	Status	Asserti...	Dependen...	Alerti...	Covered	Tun...	Securit...	Create
	All	Search	Search	Search	All	All	All	All	All	All		
	Windows	hostname	metaclass:windows e...	windows,Badrabbit,...	Enabled	0	No	on	No	No	0	2024-1
	Windows	hostname	metaclass:windows e...	windows,Midas,rans...	Enabled	0	No	on	No	No	0	2024-1
	Windows	hostname	((metaclass:windows (	windows,methodol	Enabled	0	No	on	No	No	0	2024-1

Communication Broker

- XDR uses the Communication Broker (Comm Broker) Sender to accept machine-generated messages and logs from hardware devices, operating systems, applications, security appliances, network devices, and databases through a variety of methods.

- The Comm Broker looks for events formatted as the following (in descending order of preference): JSON, CEF syslog, LEEF 1.0 & 2.0 syslog, RFC-5424 Syslog (https://tools.ietf.org/html/rfc5424), RFC-3164 Syslog (https://tools.ietf.org/html/rfc3164)

- Communications Broker resides on a Trellix Network Security appliance "NX" or may be installed as an "Unmanaged Comm Broker" on a customer-managed Linux host.

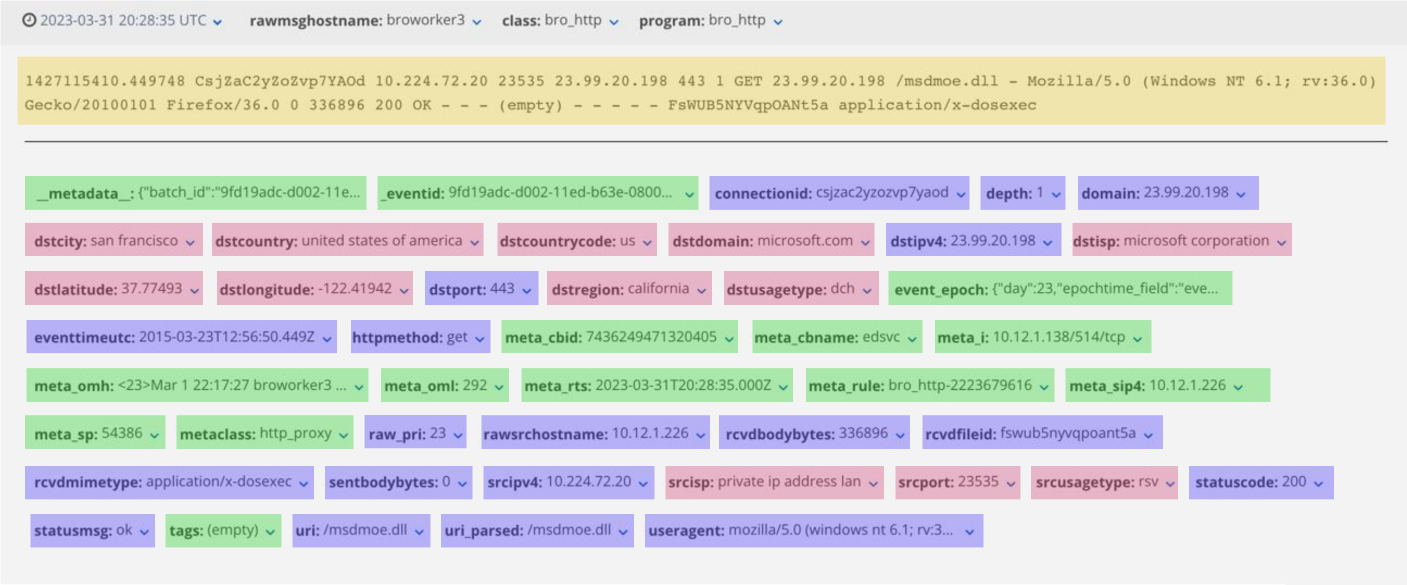
- The log messages received by the Comm Broker are compressed and encrypted for transport to the customer's Helix instance, which resides in an Amazon Web Services™ virtual private cloud (VPC).

- The receiver component present in the customer's VPC decrypts the received data and decompresses the log messages. At that point, the log messages are parsed, indexed, analyzed, and correlated with real-time threat intelligence from Trellix.

Eventos

- Formato
- TQL

Formato de eventos



2023-03-31 20:28:35 UTC ⌄ **rawmsghostname:** broworker3 ⌄ **class:** bro_http ⌄ **program:** bro_http ⌄

```
1427115410.449748 CsjZaC2yZoZvp7YAOd 10.224.72.20 23535 23.99.20.198 443 1 GET 23.99.20.198 /msdmoe.dll - Mozilla/5.0 (Windows NT 6.1; rv:36.0)
Gecko/20100101 Firefox/36.0 0 336896 200 OK - - - (empty) - - - - - FsWUB5NYVqpOANt5a application/x-dosexec
```

__metadata__: {"batch_id":"9fd19adc-d002-11e... **_eventid:** 9fd19adc-d002-11ed-b63e-0800... ⌄ **connectionid:** csjzac2yzozvp7yaod ⌄ **depth:** 1 ⌄ **domain:** 23.99.20.198 ⌄

dstcity: san francisco ⌄ **dstcountry:** united states of america ⌄ **dstcountrycode:** us ⌄ **dstdomain:** microsoft.com ⌄ **dstipv4:** 23.99.20.198 ⌄ **dstisp:** microsoft corporation ⌄

dstlatitude: 37.77493 ⌄ **dstlongitude:** -122.41942 ⌄ **dstport:** 443 ⌄ **dstregion:** california ⌄ **dstusagetype:** dch ⌄ **event_epoch:** {"day":23,"epochtime_field":"eve...

eventtimeutc: 2015-03-23T12:56:50.449Z ⌄ **httpmethod:** get ⌄ **meta_cbid:** 7436249471320405 ⌄ **meta_cbname:** edsvc ⌄ **meta_i:** 10.12.1.138/514/tcp ⌄

meta_omh: <23>Mar 1 22:17:27 broworker3 ... ⌄ **meta_oml:** 292 ⌄ **meta_rts:** 2023-03-31T20:28:35.000Z ⌄ **meta_rule:** bro_http-2223679616 ⌄ **meta_sip4:** 10.12.1.226 ⌄

meta_sp: 54386 ⌄ **metaclass:** http_proxy ⌄ **raw_pri:** 23 ⌄ **rawsrchostname:** 10.12.1.226 ⌄ **rcvdbodybytes:** 336896 ⌄ **rcvdfileid:** fswub5nyvqpoant5a ⌄

rcvdmimetype: application/x-dosexec ⌄ **sentbodybytes:** 0 ⌄ **srcipv4:** 10.224.72.20 ⌄ **srcisp:** private ip address lan ⌄ **srcport:** 23535 ⌄ **srcusagetype:** rsv ⌄ **statuscode:** 200 ⌄

statusmsg: ok ⌄ **tags:** (empty) ⌄ **uri:** /msdmoe.dll ⌄ **uri_parsed:** /msdmoe.dll ⌄ **useragent:** mozilla/5.0 (windows nt 6.1; rv:3... ⌄

Raw

Parsed

Metadata

Geo

Trellix

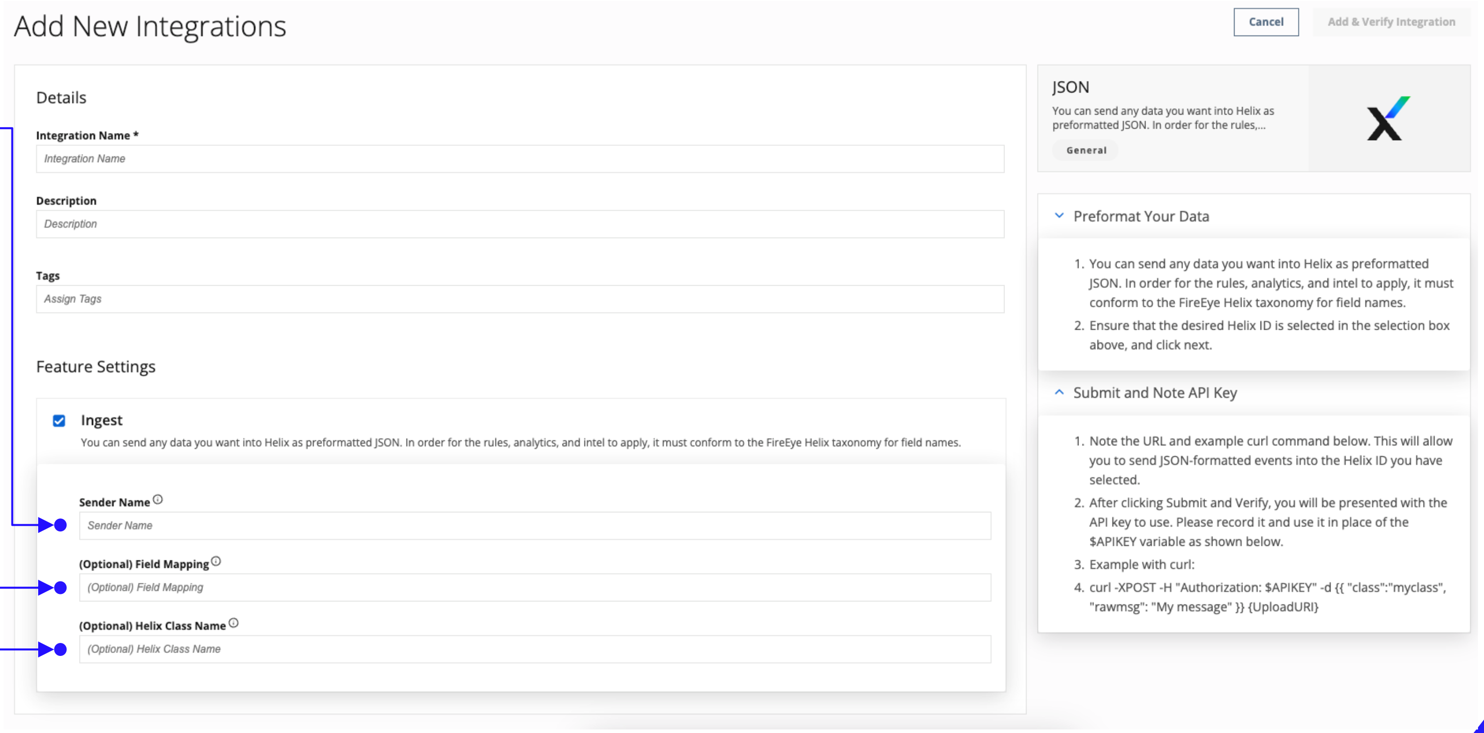
Eventos

Puede enviar cualquier dato que desee a Helix como JSON preformateado.
Para que las reglas, los análisis y la información se apliquen, deben ajustarse a la taxonomía.

Sender Name

Field Mapping

Class Name



Add New Integrations

Details

Integration Name *
Integration Name

Description
Description

Tags
Assign Tags

Feature Settings

☑ Ingest

You can send any data you want into Helix as preformatted JSON. In order for the rules, analytics, and intel to apply, it must conform to the FireEye Helix taxonomy for field names.

Sender Name ⓘ
Sender Name

(Optional) Field Mapping ⓘ
(Optional) Field Mapping

(Optional) Helix Class Name ⓘ
(Optional) Helix Class Name

JSON

You can send any data you want into Helix as preformatted JSON. In order for the rules,...

General

Preformat Your Data

1. You can send any data you want into Helix as preformatted JSON. In order for the rules, analytics, and intel to apply, it must conform to the FireEye Helix taxonomy for field names.
2. Ensure that the desired Helix ID is selected in the selection box above, and click next.

Submit and Note API Key

1. Note the URL and example curl command below. This will allow you to send JSON-formatted events into the Helix ID you have selected.
2. After clicking Submit and Verify, you will be presented with the API key to use. Please record it and use it in place of the $APIKEY variable as shown below.
3. Example with curl:
4. curl -XPOST -H "Authorization: $APIKEY" -d {{ "class":"myclass", "rawmsg": "My message" }} {UploadURI}

Eventos

Example: Generic AV Log

LOG {”victim” : ”jessica.salt”, ”md5hash” : ”4373CF0D42926B15F95E35683D883A1C”, ”type” : ”ransomware”}

Class myav

Parser {“victim": “username","md5hash": "md5","type":"malwaretype"}

PARSED_LOG

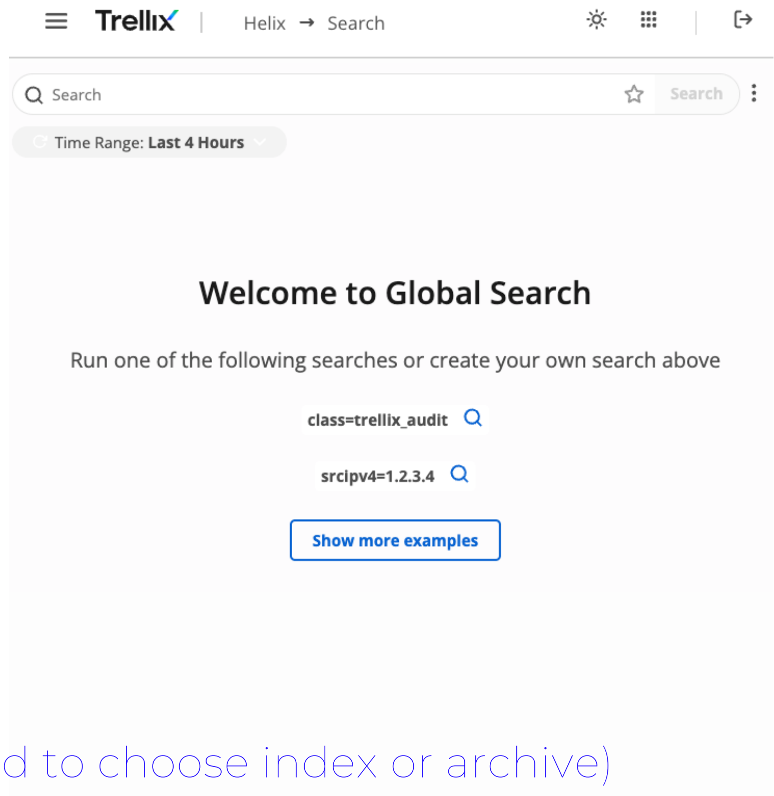
- username : jessica.salt
- md5hash : 4373CF0D42926B15F95E35683D883A1C
- malwaretype : ransomware

[Legacy] Alert Rule class=myav malwaretype=ransomware

[Legacy] Alert Parameters [name= Ransomware Alert] [TAGS= T1204.002, T1486] [Distinguishers= username]

TQL

- Query Language (TQL) is a data analysis language used in queries to retrieve events for further analysis.
- TQL queries are used in searches and rules in Helix, and other Trellix products.



Welcome to Global Search

Run one of the following searches or create your own search above

class=trellix_audit

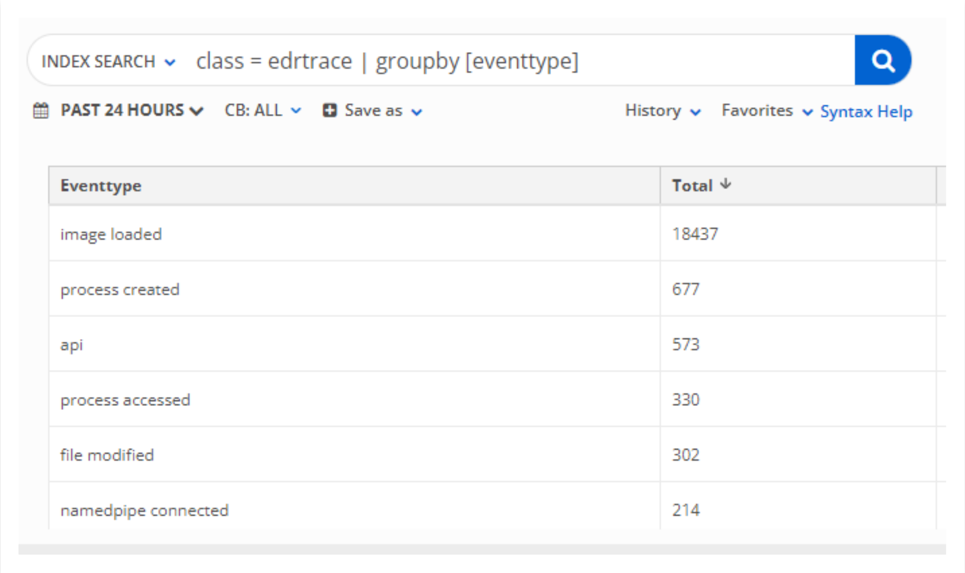
srcipv4=1.2.3.4

New search is unified (no longer need to choose index or archive)

Anatomía de una consulta TQL

High-level anatomy of an TQL query:

<filter section> | <transform section>



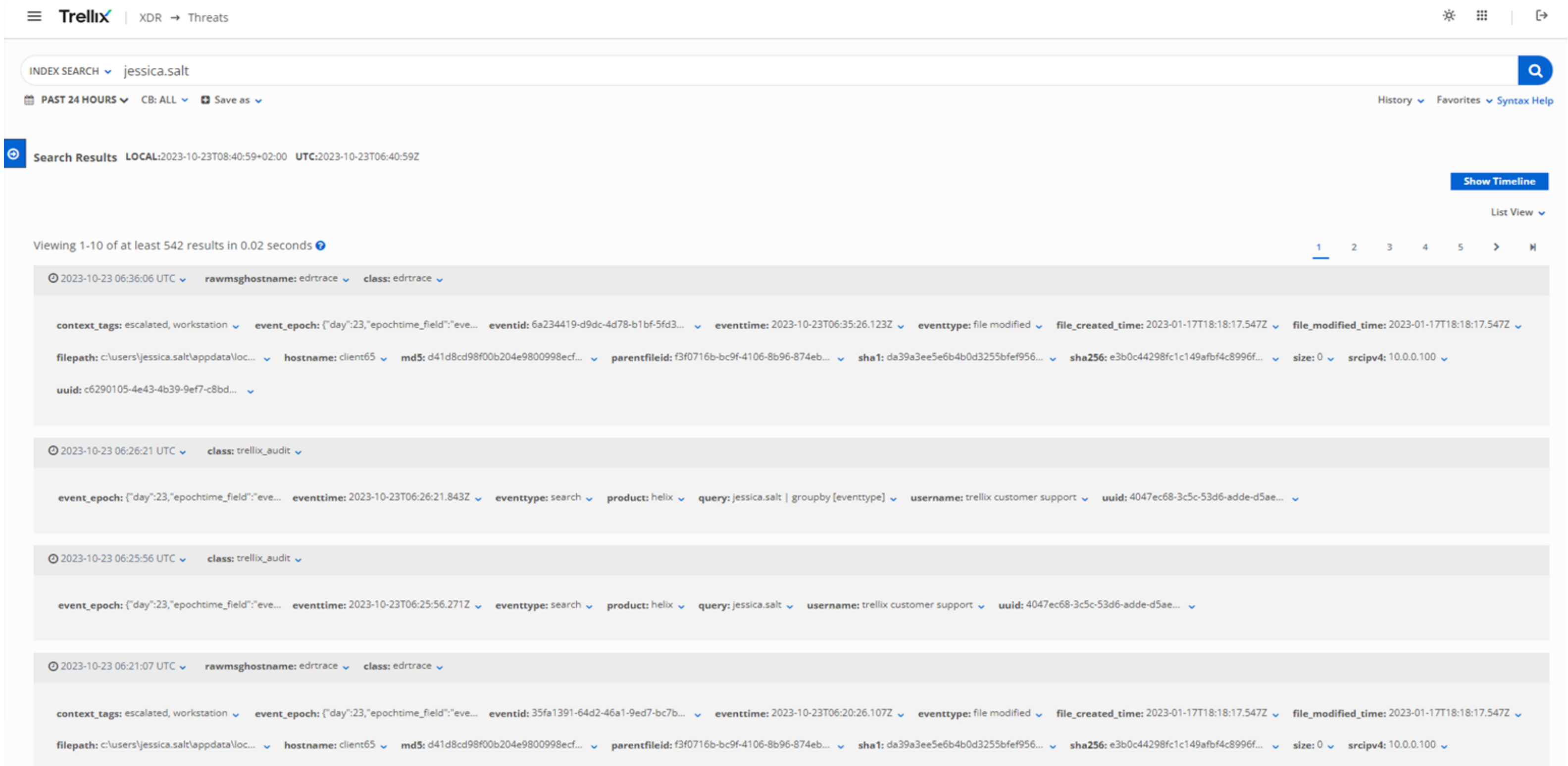
```
class = edrtrace | groupby [eventtype]
```

Eventtype	Total
image loaded	18437
process created	677
api	573
process accessed	330
file modified	302
namedpipe connected	214

Las consultas TQL puede usar tres tipos de cláusulas:

- Searches: Datos que se van a localizar en función de coincidencias exactas, comparaciones, rangos y expresiones
- Directives: modificadores que instruyen al motor de búsqueda cómo consultar [Limit, Page_size, Offset, Start, End]
- Transforms: le permiten modificar la forma en que se devuelven y muestran los resultados de su consulta [Groupby, Histogram, Sort, Table]

TQL - Ejemplos



jessica.salt

Search Results LOCAL:2023-10-23T08:40:59+02:00 UTC:2023-10-23T06:40:59Z

Viewing 1-10 of at least 542 results in 0.02 seconds

2023-10-23 06:36:06 UTC **rawmsghostname:** edrtrace **class:** edrtrace

context_tags: escalated, workstation **event_epoch:** {"day":23,"epochtime_field":"eve... **eventid:** 6a234419-d9dc-4d78-b1bf-5fd3... **eventtime:** 2023-10-23T06:35:26.123Z **eventtype:** file modified **file_created_time:** 2023-01-17T18:18:17.547Z **file_modified_time:** 2023-01-17T18:18:17.547Z

filepath: c:\users\jessica.salt\appdata\loc... **hostname:** client65 **md5:** d41d8cd98f00b204e9800998ecf... **parentfileid:** f3f0716b-bc9f-4106-8b96-874eb... **sha1:** da39a3ee5e6b4b0d3255bfef956... **sha256:** e3b0c44298fc1c149afbf4c8996f... **size:** 0 **srcipv4:** 10.0.0.100

uuid: c6290105-4e43-4b39-9ef7-c8bd...

2023-10-23 06:26:21 UTC **class:** trellix_audit

event_epoch: {"day":23,"epochtime_field":"eve... **eventtime:** 2023-10-23T06:26:21.843Z **eventtype:** search **product:** helix **query:** jessica.salt | groupby [eventtype] **username:** trellix customer support **uuid:** 4047ec68-3c5c-53d6-adde-d5ae...

2023-10-23 06:25:56 UTC **class:** trellix_audit

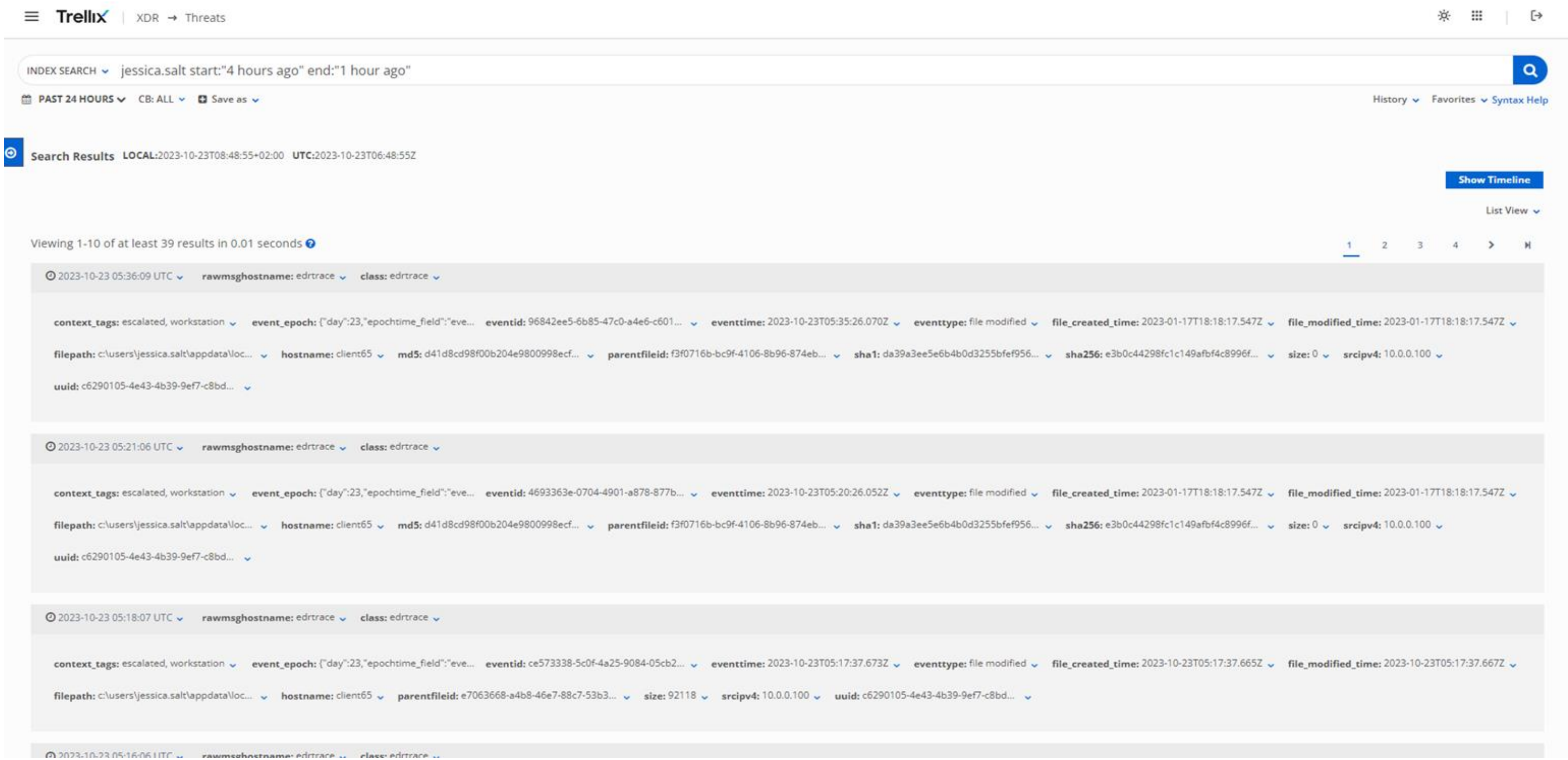
event_epoch: {"day":23,"epochtime_field":"eve... **eventtime:** 2023-10-23T06:25:56.271Z **eventtype:** search **product:** helix **query:** jessica.salt **username:** trellix customer support **uuid:** 4047ec68-3c5c-53d6-adde-d5ae...

2023-10-23 06:21:07 UTC **rawmsghostname:** edrtrace **class:** edrtrace

context_tags: escalated, workstation **event_epoch:** {"day":23,"epochtime_field":"eve... **eventid:** 35fa1391-64d2-46a1-9ed7-bc7b... **eventtime:** 2023-10-23T06:20:26.107Z **eventtype:** file modified **file_created_time:** 2023-01-17T18:18:17.547Z **file_modified_time:** 2023-01-17T18:18:17.547Z

filepath: c:\users\jessica.salt\appdata\loc... **hostname:** client65 **md5:** d41d8cd98f00b204e9800998ecf... **parentfileid:** f3f0716b-bc9f-4106-8b96-874eb... **sha1:** da39a3ee5e6b4b0d3255bfef956... **sha256:** e3b0c44298fc1c149afbf4c8996f... **size:** 0 **srcipv4:** 10.0.0.100

TQL - Ejemplos



INDEX SEARCH: jessica.salt start:"4 hours ago" end:"1 hour ago"

Search Results **LOCAL:**2023-10-23T08:48:55+02:00 **UTC:**2023-10-23T06:48:55Z

Viewing 1-10 of at least 39 results in 0.01 seconds

2023-10-23 05:36:09 UTC **rawmsghostname:** edrtrace **class:** edrtrace

context_tags: escalated, workstation **event_epoch:** {"day":23,"epochtime_field":"eve... **eventid:** 96842ee5-6b85-47c0-a4e6-c601... **eventtime:** 2023-10-23T05:35:26.070Z **eventtype:** file modified **file_created_time:** 2023-01-17T18:18:17.547Z **file_modified_time:** 2023-01-17T18:18:17.547Z

filepath: c:\users\jessica.salt\appdata\loc... **hostname:** client65 **md5:** d41d8cd98f00b204e9800998ecf... **parentfileid:** f3f0716b-bc9f-4106-8b96-874eb... **sha1:** da39a3ee5e6b4b0d3255bfef956... **sha256:** e3b0c44298fc1c149afbf4c8996f... **size:** 0 **srcipv4:** 10.0.0.100

uuid: c6290105-4e43-4b39-9ef7-c8bd...

2023-10-23 05:21:06 UTC **rawmsghostname:** edrtrace **class:** edrtrace

context_tags: escalated, workstation **event_epoch:** {"day":23,"epochtime_field":"eve... **eventid:** 4693363e-0704-4901-a878-877b... **eventtime:** 2023-10-23T05:20:26.052Z **eventtype:** file modified **file_created_time:** 2023-01-17T18:18:17.547Z **file_modified_time:** 2023-01-17T18:18:17.547Z

filepath: c:\users\jessica.salt\appdata\loc... **hostname:** client65 **md5:** d41d8cd98f00b204e9800998ecf... **parentfileid:** f3f0716b-bc9f-4106-8b96-874eb... **sha1:** da39a3ee5e6b4b0d3255bfef956... **sha256:** e3b0c44298fc1c149afbf4c8996f... **size:** 0 **srcipv4:** 10.0.0.100

uuid: c6290105-4e43-4b39-9ef7-c8bd...

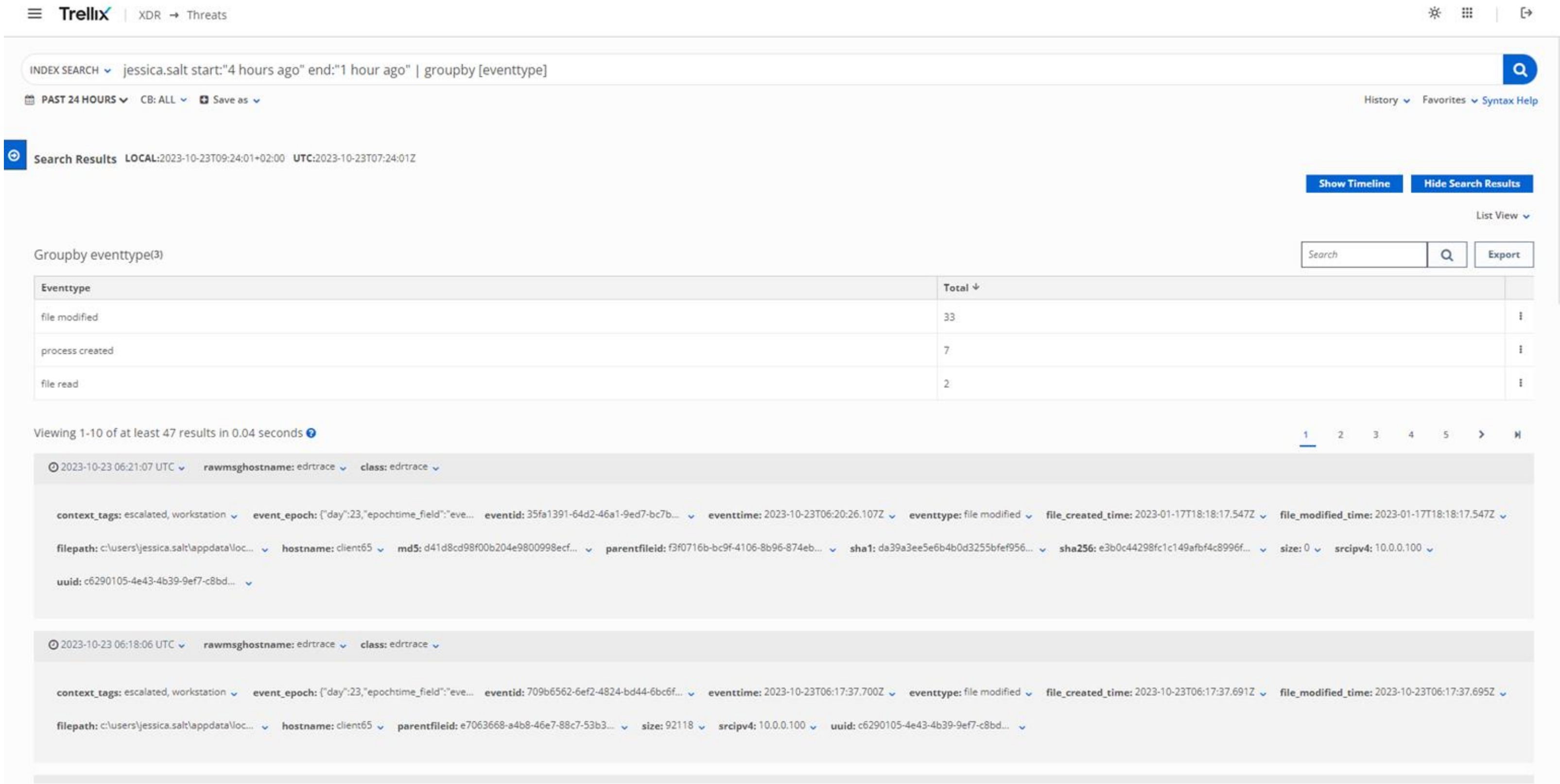
2023-10-23 05:18:07 UTC **rawmsghostname:** edrtrace **class:** edrtrace

context_tags: escalated, workstation **event_epoch:** {"day":23,"epochtime_field":"eve... **eventid:** ce573338-5c0f-4a25-9084-05cb2... **eventtime:** 2023-10-23T05:17:37.673Z **eventtype:** file modified **file_created_time:** 2023-10-23T05:17:37.665Z **file_modified_time:** 2023-10-23T05:17:37.667Z

filepath: c:\users\jessica.salt\appdata\loc... **hostname:** client65 **parentfileid:** e7063668-a4b8-46e7-88c7-53b3... **size:** 92118 **srcipv4:** 10.0.0.100 **uuid:** c6290105-4e43-4b39-9ef7-c8bd...

2023-10-23 05:16:06 UTC **rawmsghostname:** edrtrace **class:** edrtrace

TQL - Ejemplos



INDEX SEARCH jessica.salt start:"4 hours ago" end:"1 hour ago" | groupby [eventtype]

Search Results LOCAL:2023-10-23T09:24:01+02:00 UTC:2023-10-23T07:24:01Z

Groupby eventtype(3)

Eventtype	Total ↓
file modified	33
process created	7
file read	2

Viewing 1-10 of at least 47 results in 0.04 seconds

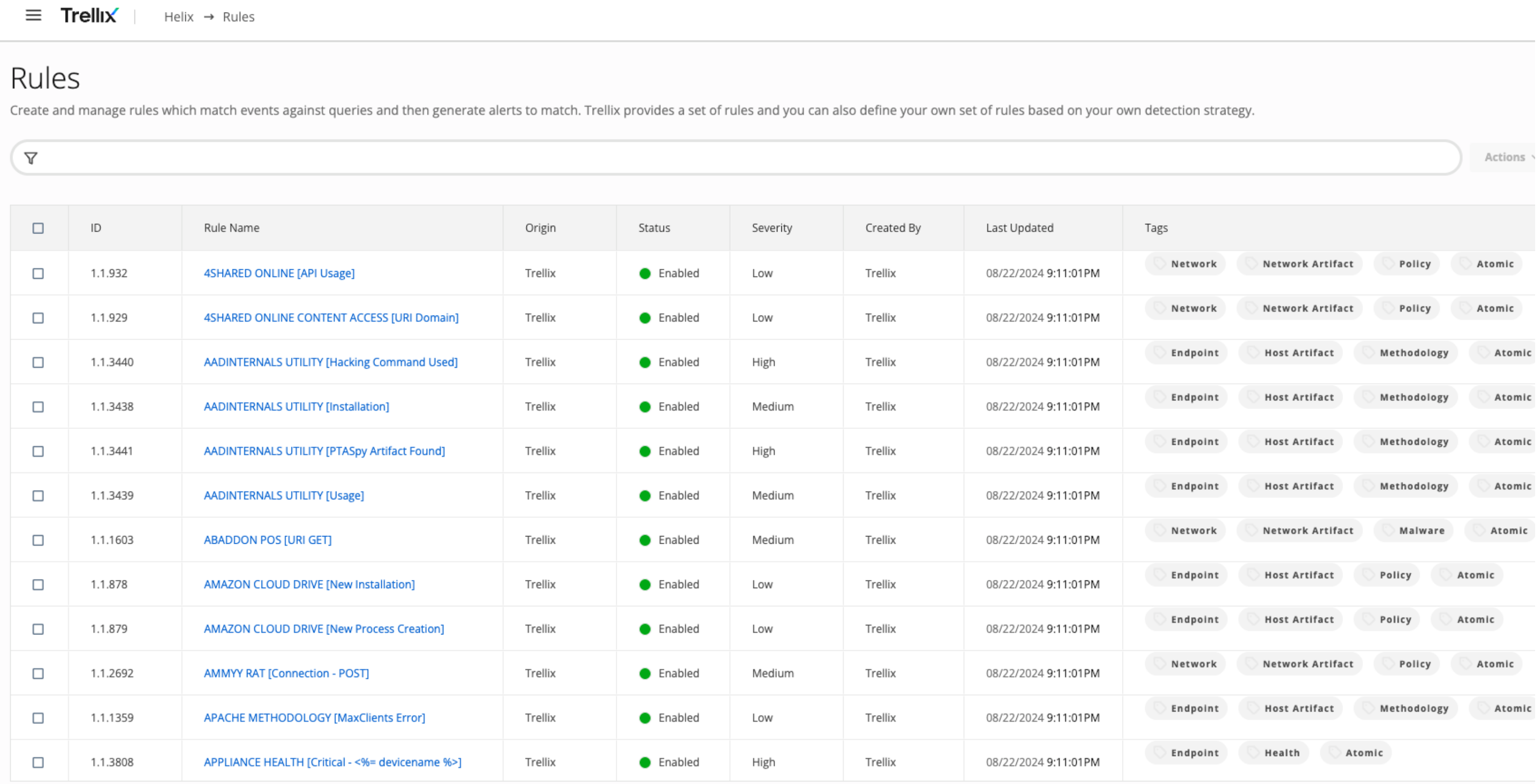
```
2023-10-23 06:21:07 UTC   rawmsghostname: edrtrace   class: edrtrace

context_tags: escalated, workstation   event_epoch: {"day":23,"epochtime_field":"eve...   eventid: 35fa1391-64d2-46a1-9ed7-bc7b...   eventtime: 2023-10-23T06:20:26.107Z   eventtype: file modified   file_created_time: 2023-01-17T18:18:17.547Z   file_modified_time: 2023-01-17T18:18:17.547Z
filepath: c:\users\jessica.salt\appdata\loc...   hostname: client65   md5: d41d8cd98f00b204e9800998ecf...   parentfileid: f3f0716b-bc9f-4106-8b96-874eb...   sha1: da39a3ee5e6b4b0d3255bfef956...   sha256: e3b0c44298fc1c149afbf4c8996f...   size: 0   srcipv4: 10.0.0.100
uuid: c6290105-4e43-4b39-9ef7-c8bd...

2023-10-23 06:18:06 UTC   rawmsghostname: edrtrace   class: edrtrace

context_tags: escalated, workstation   event_epoch: {"day":23,"epochtime_field":"eve...   eventid: 709b6562-6ef2-4824-bd44-6bc6f...   eventtime: 2023-10-23T06:17:37.700Z   eventtype: file modified   file_created_time: 2023-10-23T06:17:37.691Z   file_modified_time: 2023-10-23T06:17:37.695Z
filepath: c:\users\jessica.salt\appdata\loc...   hostname: client65   parentfileid: e7063668-a4b8-46e7-88c7-53b3...   size: 92118   srcipv4: 10.0.0.100   uuid: c6290105-4e43-4b39-9ef7-c8bd...
```

Alert mechanisms

- Rules
- Analytics
- Correlations
- UEBA
- Investigative tips
- Cases
- Wise

Trellix

Rules



☰ Trellix | Helix → Rules

Rules

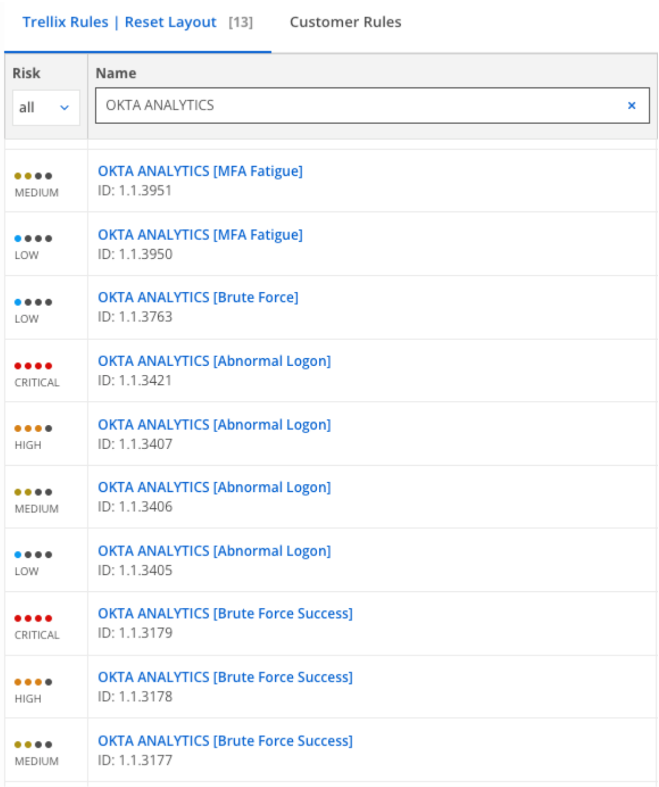
Create and manage rules which match events against queries and then generate alerts to match. Trellix provides a set of rules and you can also define your own set of rules based on your own detection strategy.

□	ID	Rule Name	Origin	Status	Severity	Created By	Last Updated	Tags
□	1.1.932	4SHARED ONLINE [API Usage]	Trellix	● Enabled	Low	Trellix	08/22/2024 9:11:01PM	Network Network Artifact Policy Atomic
□	1.1.929	4SHARED ONLINE CONTENT ACCESS [URI Domain]	Trellix	● Enabled	Low	Trellix	08/22/2024 9:11:01PM	Network Network Artifact Policy Atomic
□	1.1.3440	AADINTERNALS UTILITY [Hacking Command Used]	Trellix	● Enabled	High	Trellix	08/22/2024 9:11:01PM	Endpoint Host Artifact Methodology Atomic
□	1.1.3438	AADINTERNALS UTILITY [Installation]	Trellix	● Enabled	Medium	Trellix	08/22/2024 9:11:01PM	Endpoint Host Artifact Methodology Atomic
□	1.1.3441	AADINTERNALS UTILITY [PTASpy Artifact Found]	Trellix	● Enabled	High	Trellix	08/22/2024 9:11:01PM	Endpoint Host Artifact Methodology Atomic
□	1.1.3439	AADINTERNALS UTILITY [Usage]	Trellix	● Enabled	Medium	Trellix	08/22/2024 9:11:01PM	Endpoint Host Artifact Methodology Atomic
□	1.1.1603	ABADDON POS [URI GET]	Trellix	● Enabled	Medium	Trellix	08/22/2024 9:11:01PM	Network Network Artifact Malware Atomic
□	1.1.878	AMAZON CLOUD DRIVE [New Installation]	Trellix	● Enabled	Low	Trellix	08/22/2024 9:11:01PM	Endpoint Host Artifact Policy Atomic
□	1.1.879	AMAZON CLOUD DRIVE [New Process Creation]	Trellix	● Enabled	Low	Trellix	08/22/2024 9:11:01PM	Endpoint Host Artifact Policy Atomic
□	1.1.2692	AMMYY RAT [Connection - POST]	Trellix	● Enabled	Medium	Trellix	08/22/2024 9:11:01PM	Network Network Artifact Policy Atomic
□	1.1.1359	APACHE METHODOLOGY [MaxClients Error]	Trellix	● Enabled	Low	Trellix	08/22/2024 9:11:01PM	Endpoint Host Artifact Methodology Atomic
□	1.1.3808	APPLIANCE HEALTH [Critical - <%= devicename %>]	Trellix	● Enabled	High	Trellix	08/22/2024 9:11:01PM	Endpoint Health Atomic

Analytics

50+ deployed analytics

- Brute force
- Phishing
- Data exfiltration
- Suspicious domains
- Reconnaissance commands
- Login activity anomalies
- Process execution anomalies
- Cloud data/resource access
- Windows share access
- Account creation/deletion activity
- AWS resource scanning
- MFA fatigue activity
- Scheduled task backdoors



Risk all	Name OKTA ANALYTICS ×
●●●● MEDIUM	OKTA ANALYTICS [MFA Fatigue] ID: 1.1.3951
●●●● LOW	OKTA ANALYTICS [MFA Fatigue] ID: 1.1.3950
●●●● LOW	OKTA ANALYTICS [Brute Force] ID: 1.1.3763
●●●● CRITICAL	OKTA ANALYTICS [Abnormal Logon] ID: 1.1.3421
●●●● HIGH	OKTA ANALYTICS [Abnormal Logon] ID: 1.1.3407
●●●● MEDIUM	OKTA ANALYTICS [Abnormal Logon] ID: 1.1.3406
●●●● LOW	OKTA ANALYTICS [Abnormal Logon] ID: 1.1.3405
●●●● CRITICAL	OKTA ANALYTICS [Brute Force Success] ID: 1.1.3179
●●●● HIGH	OKTA ANALYTICS [Brute Force Success] ID: 1.1.3178
●●●● MEDIUM	OKTA ANALYTICS [Brute Force Success] ID: 1.1.3177

ACE – Advanced Correlation Engine

Example 01 – A Simple Rule

Create an alert every time we see an event from source IP 121.131.141.151

```
threshold:  1
within:  1m
items:
  -  type:  fields
     match:   srcipv4 == 121.131.141.151
require:  1
```

ACE – Advanced Correlation Engine

Example 02 – A Simple Rule with a Threshold

Create an alert if we see 10 events in a 1-minute window from source IP 121.131.141.151
1,000 events will generate 100 alerts.

```
threshold:  10
within:  1m
items:
  -  type:  fields
     match:   srcipv4 == 121.131.141.151
require:  1
```

ACE – Advanced Correlation Engine

Example 03 – A Simple Rule with Groupby

Create an alert on ten login failures for the same user within 60 seconds.

```
threshold:  10
within:  60s
groupby:  username
items:
  -  type:  fields
     match:   class==  “ms_windows_event”  &&  eventid==“4624”   &&.  event_type == “audit_failure”
require:  1
```

ACE – Advanced Correlation Engine

Example 04 – A Rule that correlates multiple events.

Create an alert when the same user has login success followed by failure within 60 seconds.

```
threshold:  1
within:  60s
groupby:  username
items:
  -  type:  fields
     match:   class==  “ms_windows_event”  &&  eventid==“4624”   &&.  event_type == “audit_failure”
  -  type:  fields
     match:   class==  “ms_windows_event”  &&  eventid==“4624”   &&.  event_type == “audit_success”
require:  2
ordered: true
```

ACE – Advanced Correlation Engine

Example 05 – A Rule with Cardinality

Create an alert when the same user has logs in from five different IP addresses in ten minutes.

```
threshold:  1
within:  600s
groupby:  username
items:
  -  type:  cardinality
     item:
     -  type:  fields
           match:   class==  "ms_office365"  &&  action contains "userloggedin"  &&  result == "success"
     require:  5
     cardinalityGroupby: srcipv4
```

User & Entity Behavior Analytics Analytics

Monitor user and entity activity over time to identify anomalies

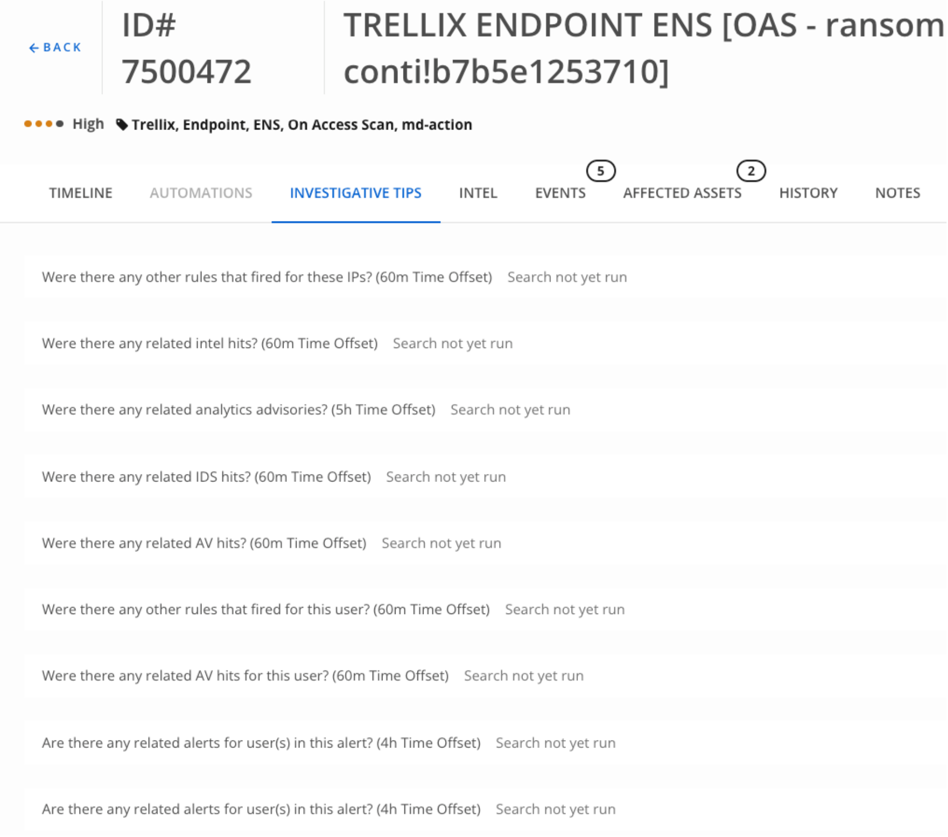
Examples

- Account logs in from a particular country for the first time
- Host executes a particular process for the first time
- Sum of byte count for host in past day is some standard deviations above daily average

Investigative tips

- Investigative Tips provide a series of "next steps" for investigating an alert.

- For Trellix provided rules, these searches are generated by incident responders and intelligence analysts based on the data they would look for to determine if an alert is a true positive.



ID# 7500472

TRELLIX ENDPOINT ENS [OAS - ransom conti!b7b5e1253710]

●●●● High Trellix, Endpoint, ENS, On Access Scan, md-action

Were there any other rules that fired for these IPs? (60m Time Offset) Search not yet run

Were there any related intel hits? (60m Time Offset) Search not yet run

Were there any related analytics advisories? (5h Time Offset) Search not yet run

Were there any related IDS hits? (60m Time Offset) Search not yet run

Were there any related AV hits? (60m Time Offset) Search not yet run

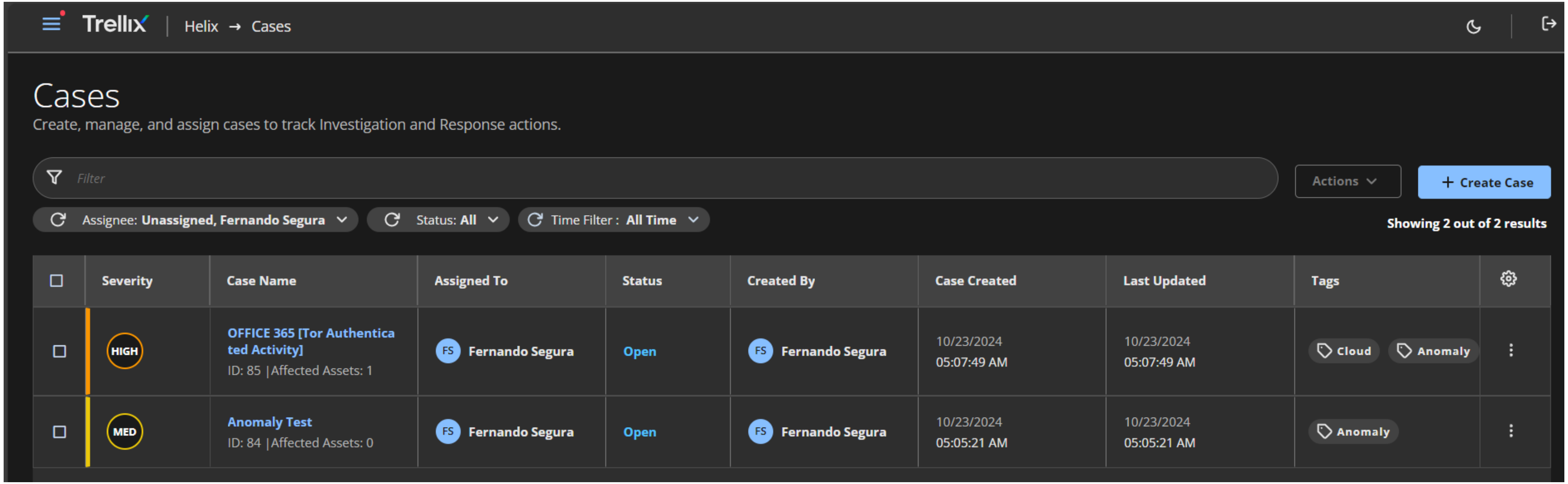
Were there any other rules that fired for this user? (60m Time Offset) Search not yet run

Were there any related AV hits for this user? (60m Time Offset) Search not yet run

Are there any related alerts for user(s) in this alert? (4h Time Offset) Search not yet run

Are there any related alerts for user(s) in this alert? (4h Time Offset) Search not yet run

Cases



Cases

Create, manage, and assign cases to track Investigation and Response actions.

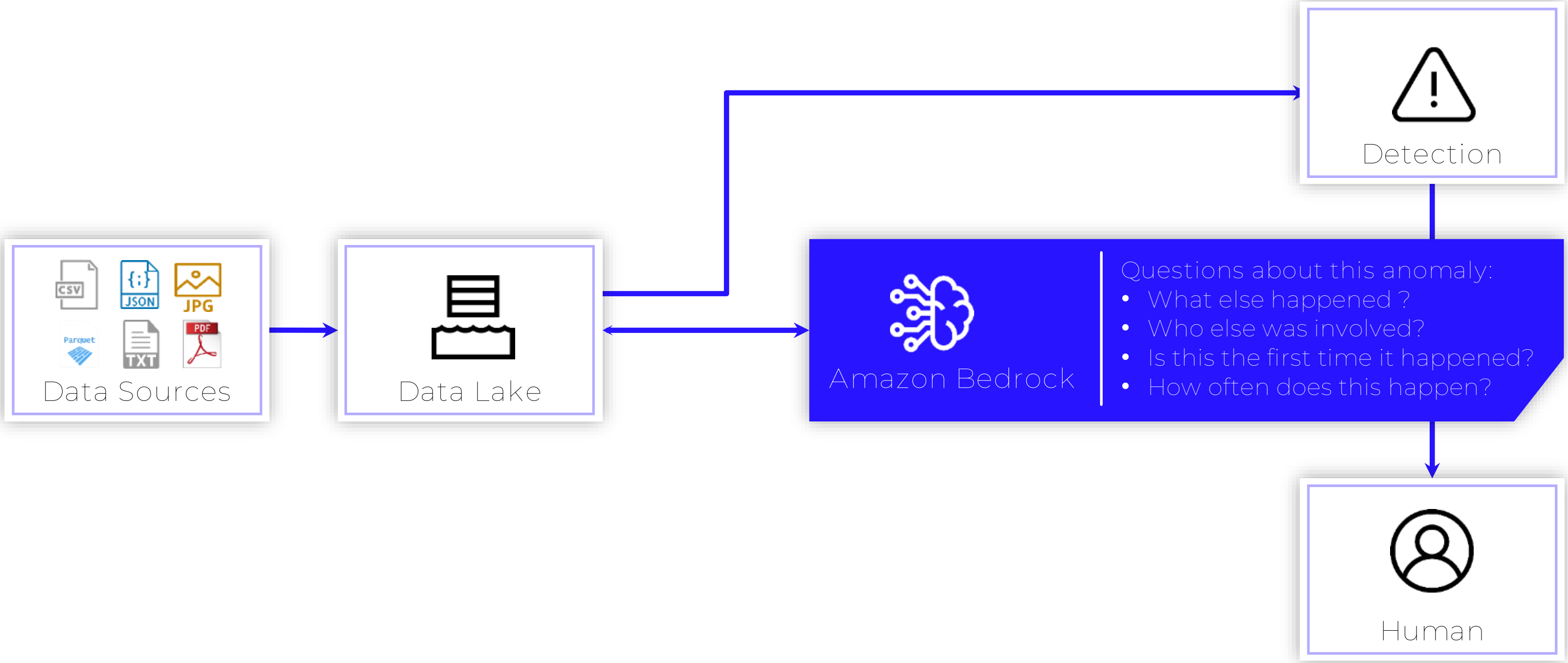
Assignee: **Unassigned, Fernando Segura** | Status: **All** | Time Filter : **All Time**

Showing 2 out of 2 results

□	Severity	Case Name	Assigned To	Status	Created By	Case Created	Last Updated	Tags
□	HIGH	OFFICE 365 [Tor Authenticated Activity] ID: 85 |Affected Assets: 1	FS Fernando Segura	Open	FS Fernando Segura	10/23/2024 05:07:49 AM	10/23/2024 05:07:49 AM	Cloud Anomaly
□	MED	Anomaly Test ID: 84 |Affected Assets: 0	FS Fernando Segura	Open	FS Fernando Segura	10/23/2024 05:05:21 AM	10/23/2024 05:05:21 AM	Anomaly

Trellix Wise for Helix Connect

Generative AI can ask key questions and understand answers



Questions about this anomaly:

- What else happened ?
- Who else was involved?
- Is this the first time it happened?
- How often does this happen?

GenAI y datos de clientes

Does Trellix Wise use customer data to train models?

Trellix Wise does NOT use customer data to train models or share data with third parties!

- GenAI models are already pre-trained on general security knowledge and do not need to be fine-tuned.
- Decisions are made solely based on the tactical information at hand, so they are not biased by previous occurrences or other situations.
- This ensures gen AI decisions are grounded and not hallucinations.

Consideraciones sobre la implementación

Optional subtitle

Hardware Requirements Specs

TAuR

- 32 GB memory
- 220 GB diskspace
  - Thin provisioned disks
- 2 Cores CPU minimum (ideally 64-bit quad-core processor)

- NOTE: For the lab your OVA will pre-define the specs to be used on the virtual machine (4 Cores, 8 GB Memory, 220 GB diskspace)

Install TAuR

TAuR

- Power on your VM
- Login to the VM with:
  - User: root
  - Password: eiX3Ci3qua
  - User: ixoperator
  - Password : changeme

NOTE: You'll be required to change these upon logging in. Remember what you set them to!

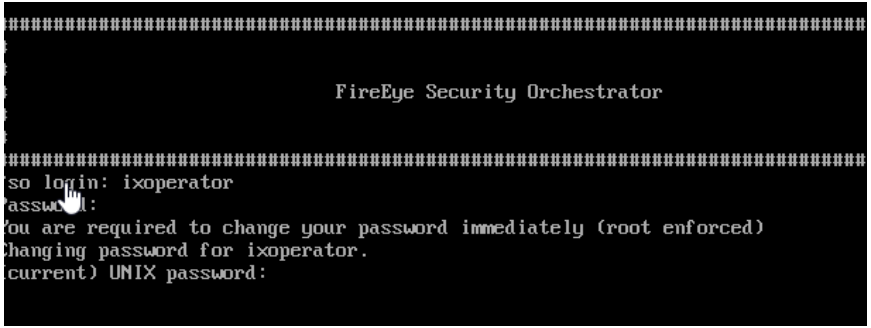
Install TAuR

Getting Started

Ejecute ifconfig como **root** y anote su dirección IP en el bloc de notas. ¡Necesitará esto para la configuración de su host!

Install TAuR

Initial Login



```
##############################################################################
#
#
#                    FireEye Security Orchestrator
#
#
##############################################################################
so login: ixoperator
assword:
ou are required to change your password immediately (root enforced)
hanging password for ixoperator.
current) UNIX password:
```

Step 1

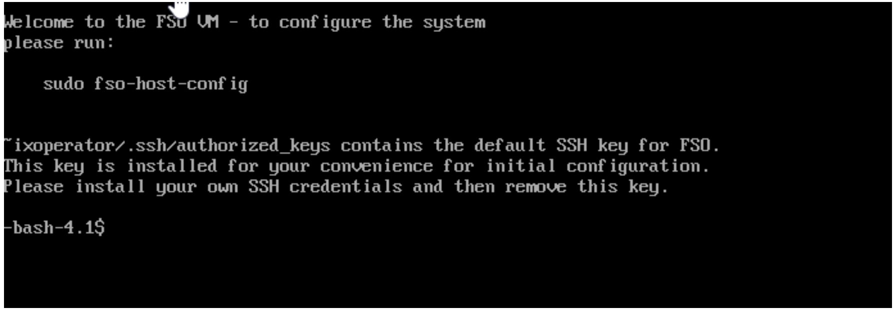
Login with “ixoperator” password “changeme”

You will be prompted for a new password

Step 2:

sudo fso-host-config

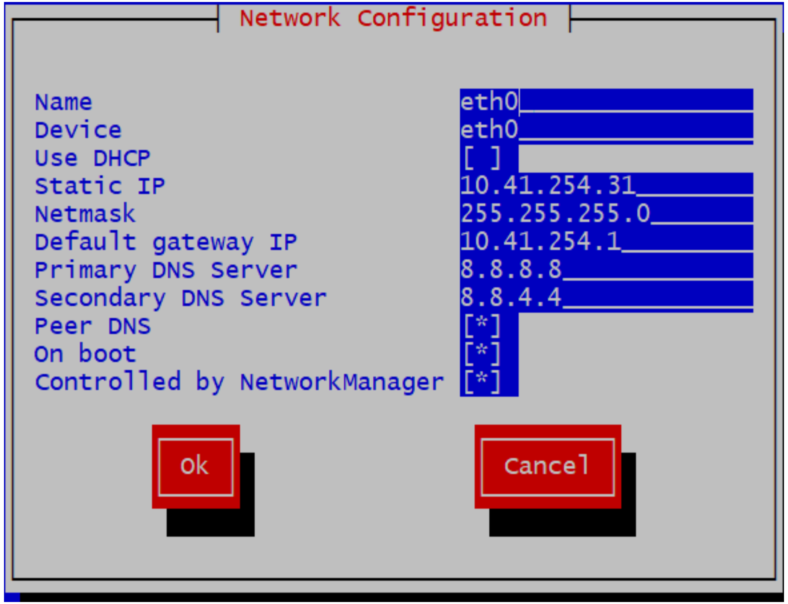
To trigger configuration wizard



```
Welcome to the FSO VM - to configure the system
please run:

   sudo fso-host-config


~ixoperator/.ssh/authorized_keys contains the default SSH key for FSO.
This key is installed for your convenience for initial configuration.
Please install your own SSH credentials and then remove this key.

-bash-4.1$
```

Install TAuR

Wizard View



```
Network Configuration

Name                           eth0
Device                         eth0
Use DHCP                       [ ]
Static IP                      10.41.254.31
Netmask                        255.255.255.0
Default gateway IP             10.41.254.1
Primary DNS Server             8.8.8.8
Secondary DNS Server           8.8.4.4
Peer DNS                       [*]
On boot                        [*]
Controlled by NetworkManager   [*]
```

Upon your first run of **fso-host-config**, you will be presented with an option to supply the DNS settings.

Make sure these match your network settings before you save.

After completing this step and saving, you'll be prompted to supply a hostname (FQDN) for TAuR. **Make sure you note that hostname.**

Install TAuR

Update Windows Hosts File

From your “admin workstation”, you’ll need to update your hosts settings to match whatever FQDN you supply. For Windows users:

Run notepad.exe as administrator

Browse to C:\Windows\System32\drivers\etc

Add the IP and FQN i.e. 192.168.65.133 fso.domain.com

Save the file

Install TAuR

Update Windows Hosts File

From your “admin workstation”, you’ll need to update your hosts settings to match whatever FQDN you supply. For Windows users:

Run notepad.exe as administrator

Browse to C:\Windows\System32\drivers\etc

Add the IP and FQN i.e. 192.168.65.133 fso.domain.com

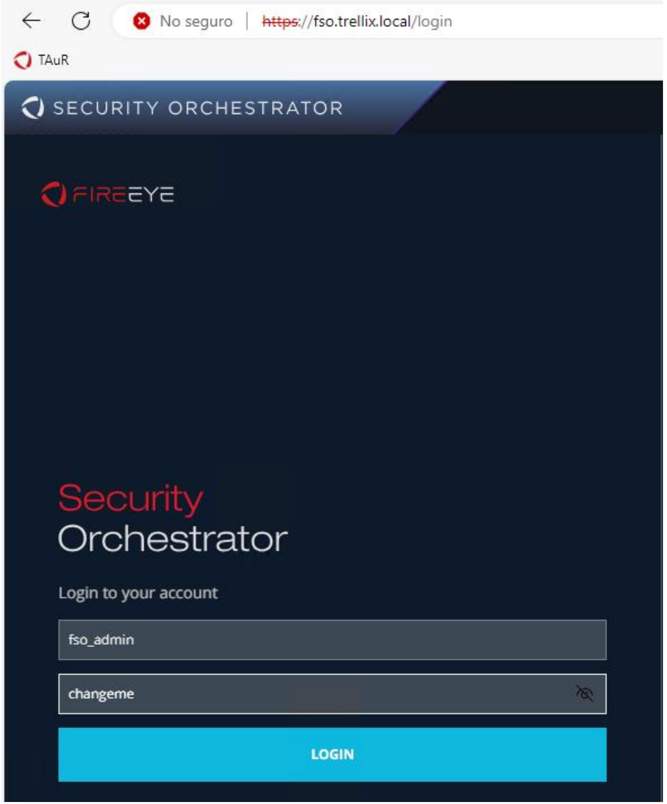
Save the file

Install TAuR

Logging into the Web UI

You’re all set! You should be able to access the Web UI via the FQDN you have now set up.
Note: Make sure that you use HTTPS, or it won’t resolve.

Login user : fso_admin
Password : changeme



No seguro | ~~https~~://fso.trellix.local/login

fso_admin

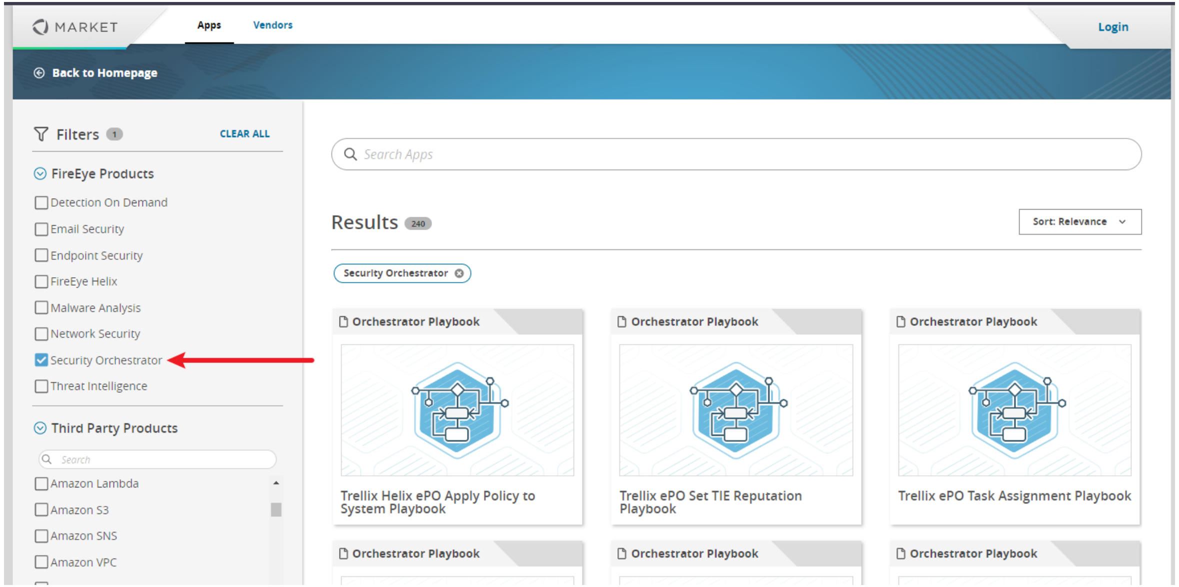
changeme

Demonstration Guidance (and Use cases)

Optional subtitle

Plug-ins installaton

https://fireeye.market/



Filters 1

FireEye Products

- ☐ Detection On Demand
- ☐ Email Security
- ☐ Endpoint Security
- ☐ FireEye Helix
- ☐ Malware Analysis
- ☐ Network Security
- ☑ Security Orchestrator
- ☐ Threat Intelligence

Third Party Products

Search

- ☐ Amazon Lambda
- ☐ Amazon S3
- ☐ Amazon SNS
- ☐ Amazon VPC

Results 240

Security Orchestrator ⊗

Orchestrator Playbook — Trellix Helix ePO Apply Policy to System Playbook

Orchestrator Playbook — Trellix ePO Set TIE Reputation Playbook

Orchestrator Playbook — Trellix ePO Task Assignment Playbook

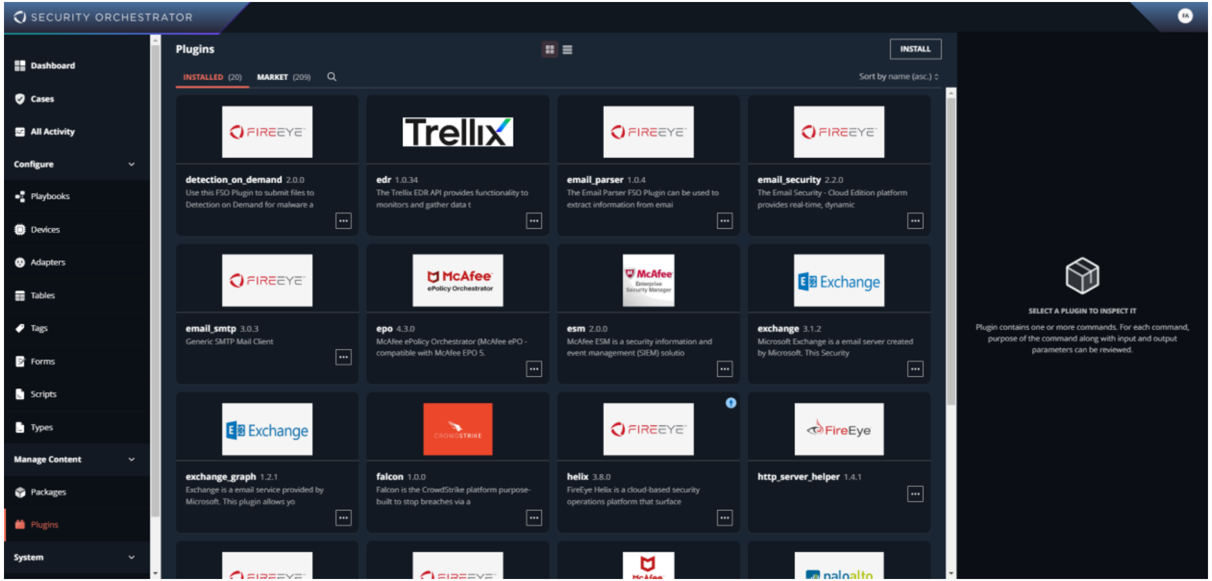
Orchestrator Playbook

Orchestrator Playbook

Orchestrator Playbook

Plug-ins installaton

TAuR Plugins



Plugins

detection_on_demand 2.0.0
Use this FSO Plugin to submit files to Detection on Demand for malware a

edr 1.0.34
The Trellix EDR API provides functionality to monitors and gather data t

email_parser 1.0.4
The Email Parser FSO Plugin can be used to extract information from emai

email_security 2.2.0
The Email Security - Cloud Edition platform provides real-time, dynamic

email_smtp 3.0.3
Generic SMTP Mail Client

epo 4.3.0
McAfee ePolicy Orchestrator (McAfee ePO - compatible with McAfee EPO 5.

esm 2.0.0
McAfee ESM is a security information and event management (SIEM) solutio

exchange 3.1.2
Microsoft Exchange is a email server created by Microsoft. This Security

exchange_graph 1.2.1
Exchange is a email service provided by Microsoft. This plugin allows yo

falcon 1.0.0
Falcon is the CrowdStrike platform purpose-built to stop breaches via a

helix 3.8.0
FireEye Helix is a cloud-based security operations platform that surface

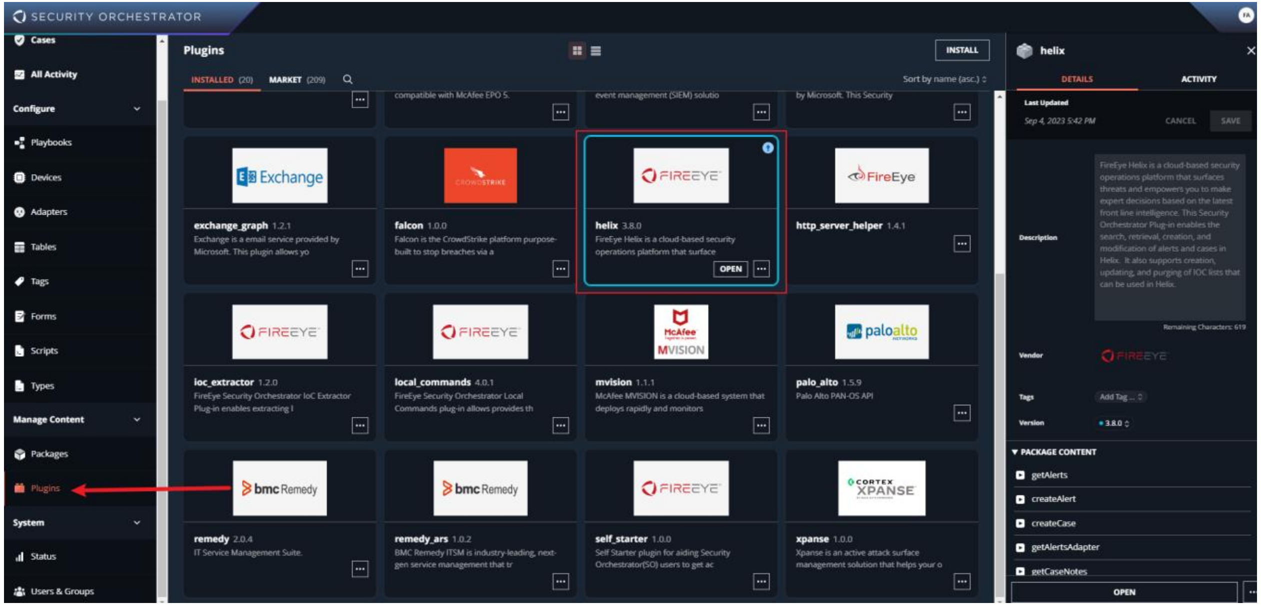
http_server_helper 1.4.1

SELECT A PLUGIN TO INSPECT IT

Plugin contains one or more commands. For each command, purpose of the command along with input and output parameters can be reviewed.

Plug-ins settings

Helix



compatible with McAfee EPO 5.

event management (SIEM) solutio

by Microsoft. This Security

exchange_graph 1.2.1
Exchange is a email service provided by Microsoft. This plugin allows yo

falcon 1.0.0
Falcon is the CrowdStrike platform purpose-built to stop breaches via a

helix 3.8.0
FireEye Helix is a cloud-based security operations platform that surface

http_server_helper 1.4.1

ioc_extractor 1.2.0
FireEye Security Orchestrator IoC Extractor Plug-in enables extracting I

local_commands 4.0.1
FireEye Security Orchestrator Local Commands plug-in allows provides th

mvision 1.1.1
McAfee MVISION is a cloud-based system that deploys rapidly and monitors

palo_alto 1.5.9
Palo Alto PAN-OS API

remedy 2.0.4
IT Service Management Suite.

remedy_ars 1.0.2
BMC Remedy ITSM is industry-leading, next-gen service management that tr

self_starter 1.0.0
Self Starter plugin for aiding Security Orchestrator(SO) users to get ac

xpanse 1.0.0
Xpanse is an active attack surface management solution that helps your o

Last Updated
Sep 4, 2023 5:42 PM

Description
FireEye Helix is a cloud-based security operations platform that surfaces threats and empowers you to make expert decisions based on the latest front line intelligence. This Security Orchestrator Plug-in enables the search, retrieval, creation, and modification of alerts and cases in Helix. It also supports creation, updating, and purging of IOC lists that can be used in Helix.

Remaining Characters: 619

Vendor FIREEYE

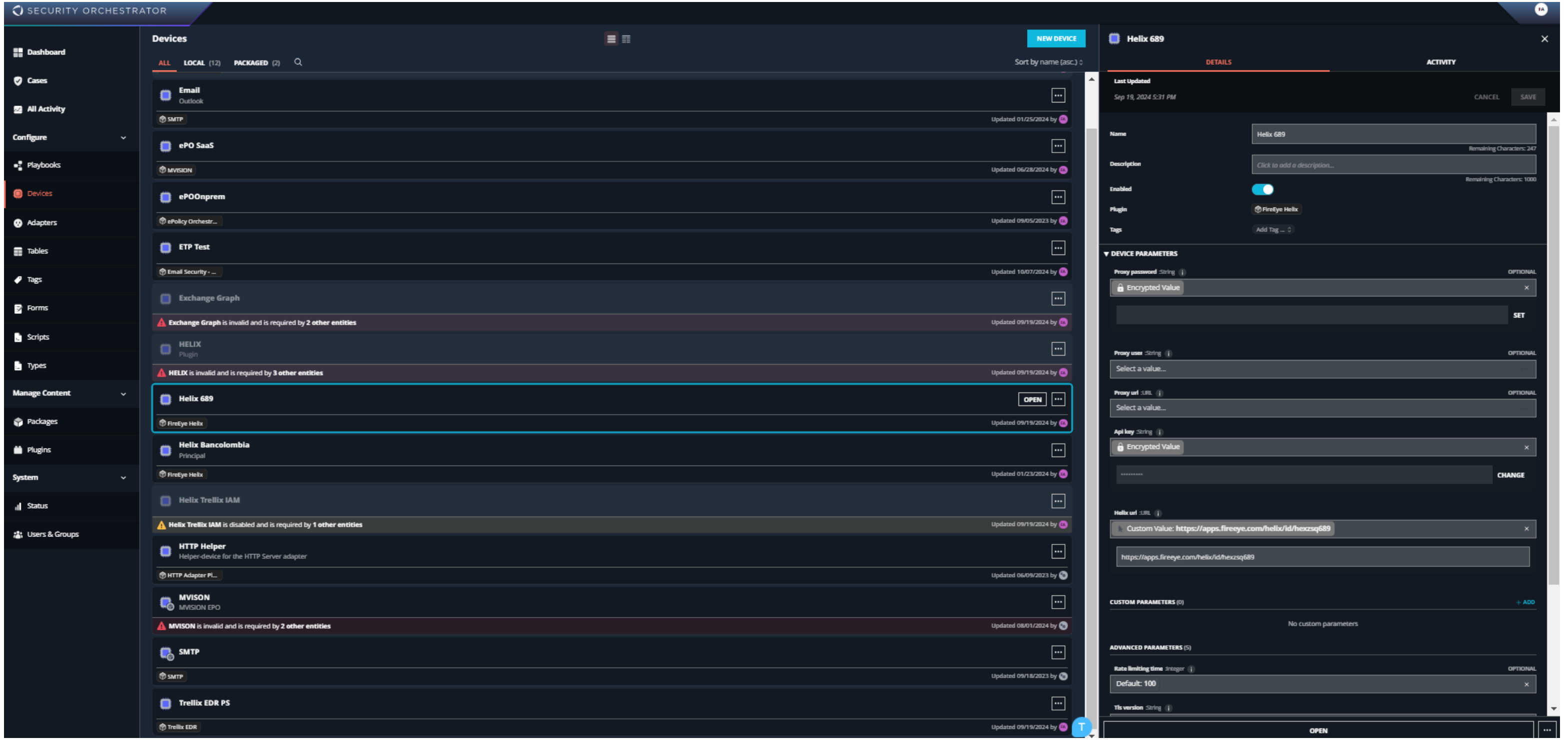
Tags Add Tag ...

Version 3.8.0

PACKAGE CONTENT
- getAlerts
- createAlert
- createCase
- getAlertsAdapter
- getCaseNotes

Plug-ins settings

Helix



Devices

ALL LOCAL (12) PACKAGED (2)

Sort by name (asc.)

Email
Outlook
SMTP — Updated 01/25/2024 by

ePO SaaS
MVISION — Updated 06/28/2024 by

ePOOnprem
ePolicy Orchestr... — Updated 09/05/2023 by

ETP Test
Email Security - ... — Updated 10/07/2024 by

Exchange Graph
Exchange Graph is invalid and is required by **2 other entities** — Updated 09/19/2024 by

HELIX
Plugin
HELIX is invalid and is required by **3 other entities** — Updated 09/19/2024 by

Helix 689
FireEye Helix — Updated 09/19/2024 by

Helix Bancolombia
Principal
FireEye Helix — Updated 01/23/2024 by

Helix Trellix IAM
Helix Trellix IAM is disabled and is required by **1 other entities** — Updated 09/19/2024 by

HTTP Helper
Helper-device for the HTTP Server adapter
HTTP Adapter Pl... — Updated 06/09/2023 by

MVISON
MVISION EPO
MVISON is invalid and is required by **2 other entities** — Updated 08/01/2024 by

SMTP
SMTP — Updated 09/18/2023 by

Trellix EDR PS
Trellix EDR — Updated 09/19/2024 by

Helix 689

Last Updated
Sep 19, 2024 5:31 PM

Name: Helix 689
Remaining Characters: 247

Description: Click to add a description...
Remaining Characters: 1000

Enabled

Plugin: FireEye Helix

Tags: Add Tag ...

▼ DEVICE PARAMETERS

Proxy password :String — OPTIONAL
Encrypted Value

Proxy user :String — OPTIONAL
Select a value...

Proxy url :URL — OPTIONAL
Select a value...

Api key :String
Encrypted Value
•••••••••

Helix url :URL
Custom Value: **https://apps.fireeye.com/helix/id/hexzsq689**
https://apps.fireeye.com/helix/id/hexzsq689

CUSTOM PARAMETERS (0)
No custom parameters

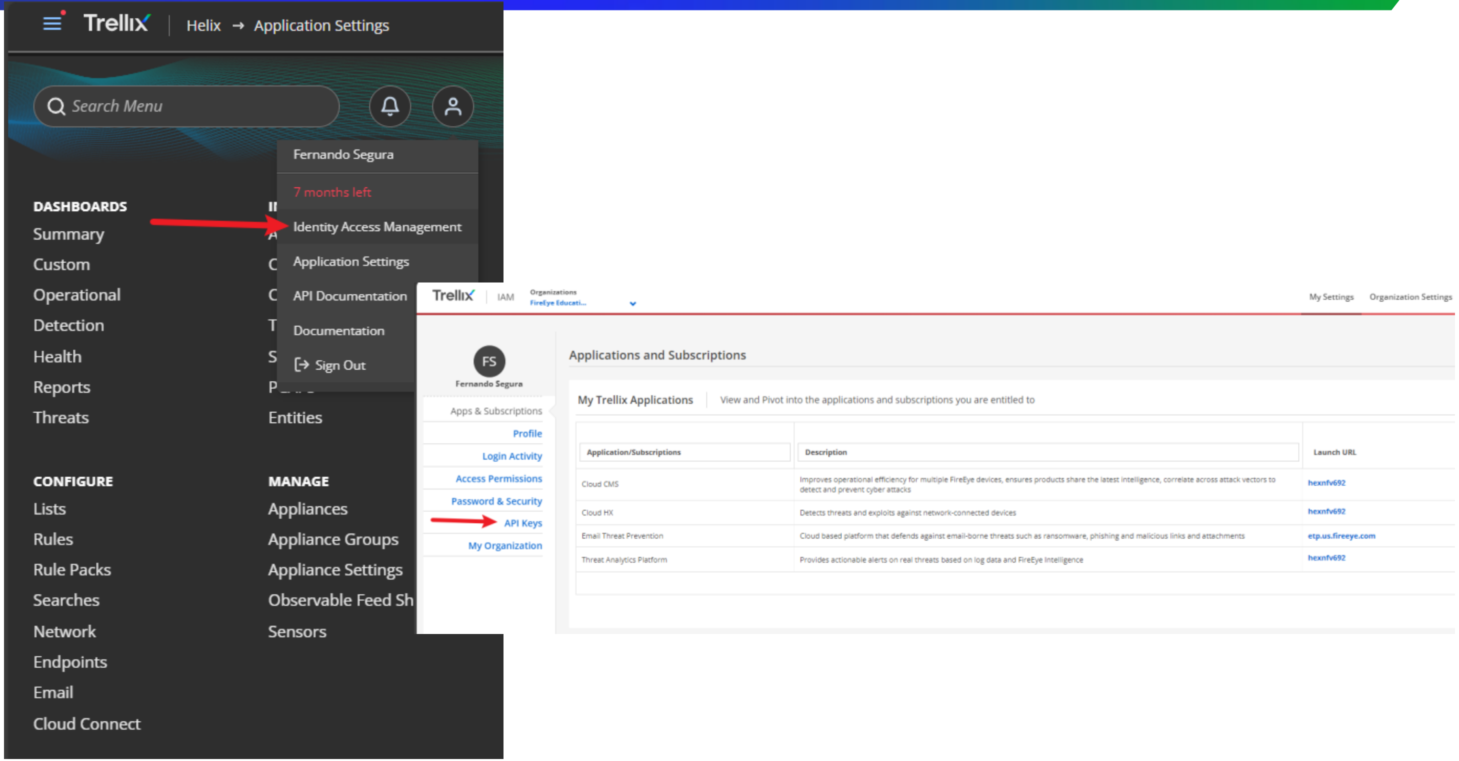
ADVANCED PARAMETERS (5)

Rate limiting time :Integer — OPTIONAL
Default: 100

Tls version :String

Use Case

Helix API key



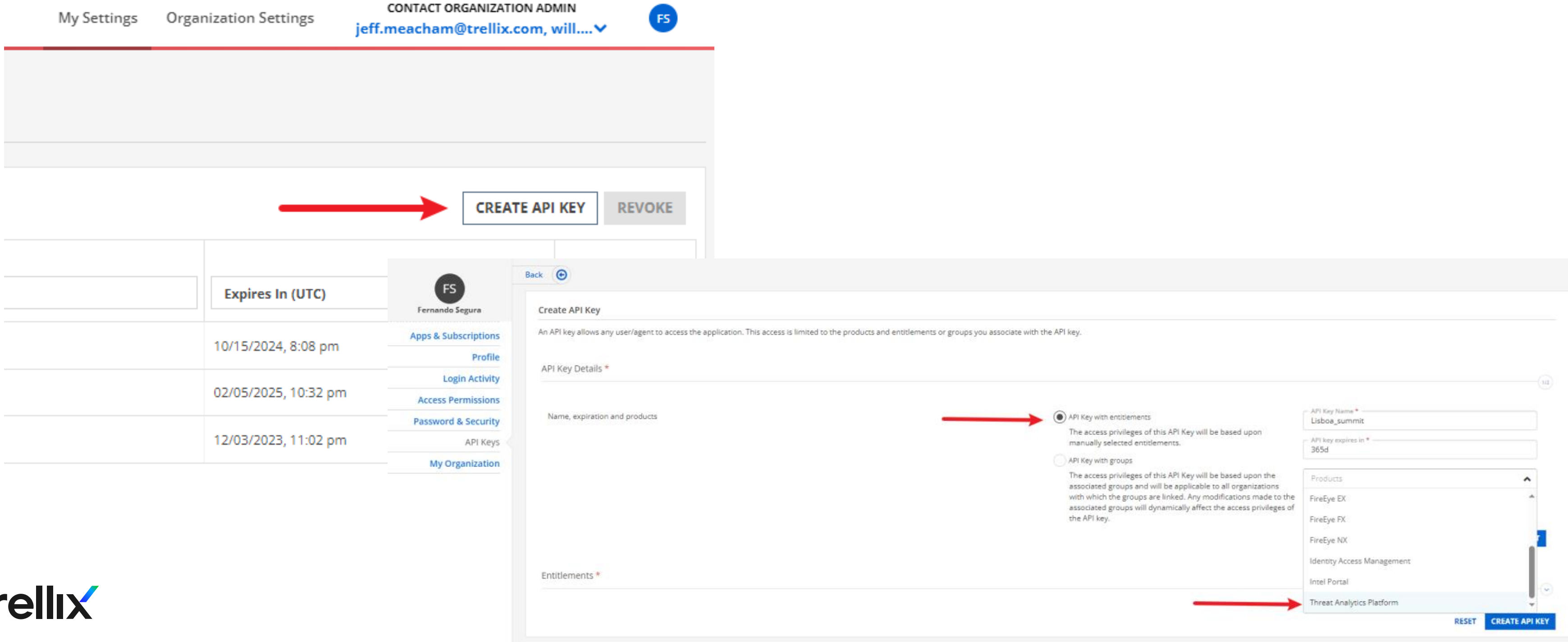
Applications and Subscriptions

My Trellix Applications | View and Pivot into the applications and subscriptions you are entitled to

Application/Subscriptions	Description	Launch URL
Cloud CMS	Improves operational efficiency for multiple FireEye devices, ensures products share the latest intelligence, correlate across attack vectors to detect and prevent cyber attacks	hexnfv692
Cloud HX	Detects threats and exploits against network-connected devices	hexnfv692
Email Threat Prevention	Cloud based platform that defends against email-borne threats such as ransomware, phishing and malicious links and attachments	etp.us.fireeye.com
Threat Analytics Platform	Provides actionable alerts on real threats based on log data and FireEye Intelligence	hexnfv692

Use Case

Helix API key



Expires In (UTC)
10/15/2024, 8:08 pm
02/05/2025, 10:32 pm
12/03/2023, 11:02 pm

Create API Key

An API key allows any user/agent to access the application. This access is limited to the products and entitlements or groups you associate with the API key.

API Key Details *

Name, expiration and products

● API Key with entitlements

The access privileges of this API Key will be based upon manually selected entitlements.

○ API Key with groups

The access privileges of this API Key will be based upon the associated groups and will be applicable to all organizations with which the groups are linked. Any modifications made to the associated groups will dynamically affect the access privileges of the API key.

API Key Name *: Lisboa_summit

API key expires in *: 365d

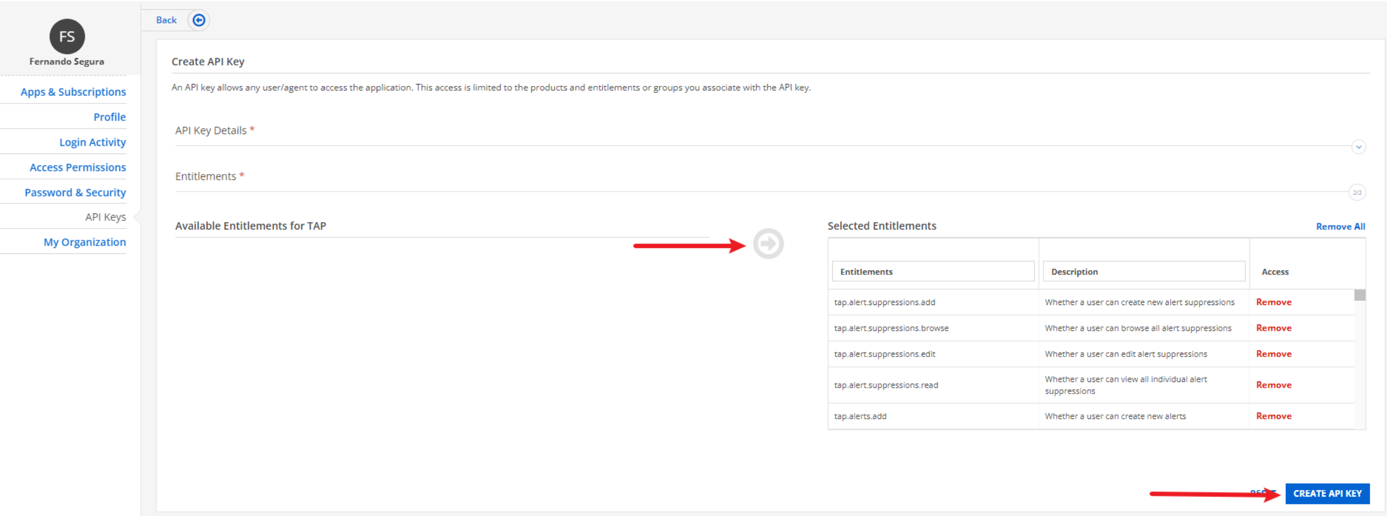
Products

- FireEye EX
- FireEye FX
- FireEye NX
- Identity Access Management
- Intel Portal
- Threat Analytics Platform

Entitlements *

Use Case

Helix API key



Create API Key

An API key allows any user/agent to access the application. This access is limited to the products and entitlements or groups you associate with the API key.

API Key Details *

Entitlements *

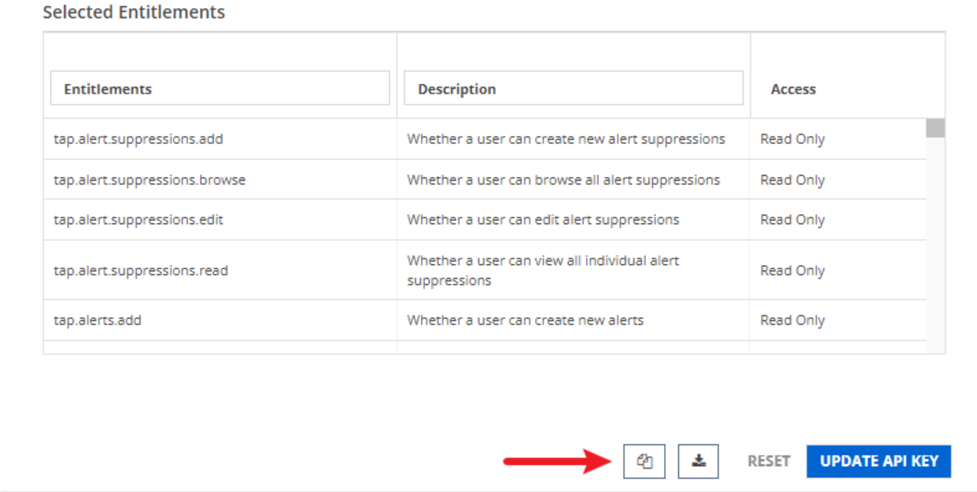
Available Entitlements for TAP

Selected Entitlements

Entitlements	Description	Access
tap.alert.suppressions.add	Whether a user can create new alert suppressions	Remove
tap.alert.suppressions.browse	Whether a user can browse all alert suppressions	Remove
tap.alert.suppressions.edit	Whether a user can edit alert suppressions	Remove
tap.alert.suppressions.read	Whether a user can view all individual alert suppressions	Remove
tap.alerts.add	Whether a user can create new alerts	Remove

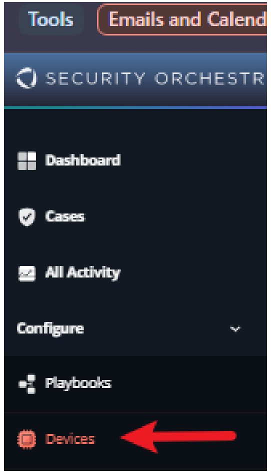
Use Case

Helix API key & plugin configuration



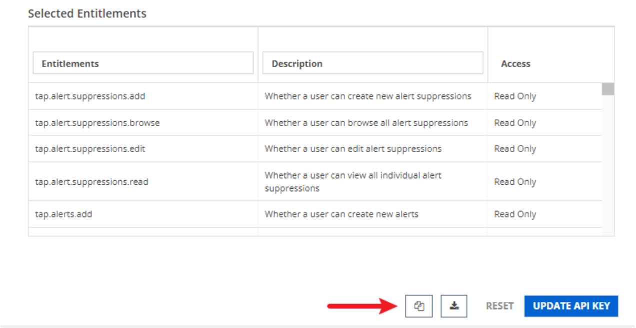
Selected Entitlements

Entitlements	Description	Access
tap.alert.suppressions.add	Whether a user can create new alert suppressions	Read Only
tap.alert.suppressions.browse	Whether a user can browse all alert suppressions	Read Only
tap.alert.suppressions.edit	Whether a user can edit alert suppressions	Read Only
tap.alert.suppressions.read	Whether a user can view all individual alert suppressions	Read Only
tap.alerts.add	Whether a user can create new alerts	Read Only



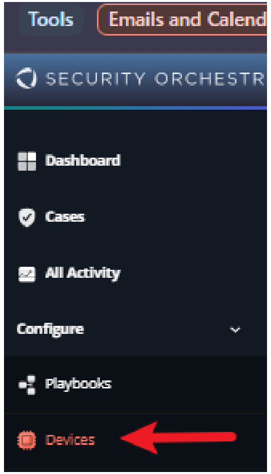
Use Case

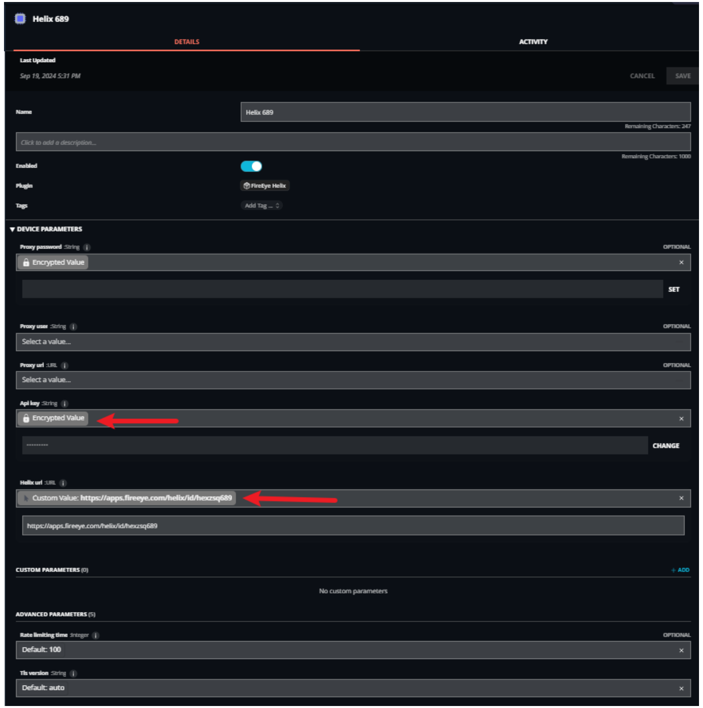
Helix API key & plugin configuration



Selected Entitlements

Entitlements	Description	Access
tap.alert.suppressions.add	Whether a user can create new alert suppressions	Read Only
tap.alert.suppressions.browse	Whether a user can browse all alert suppressions	Read Only
tap.alert.suppressions.edit	Whether a user can edit alert suppressions	Read Only
tap.alert.suppressions.read	Whether a user can view all individual alert suppressions	Read Only
tap.alerts.add	Whether a user can create new alerts	Read Only





Helix 689

Last Updated
Sep 19, 2024 5:31 PM

Name: Helix 689
Remaining Characters: 247

Click to add a description...
Remaining Characters: 1000

Enabled

Plugin: FireEye Helix

Tags: Add Tag ...

▼ DEVICE PARAMETERS

Proxy password :String — OPTIONAL
Encrypted Value ×
SET

Proxy user :String — OPTIONAL
Select a value...

Proxy url :URL — OPTIONAL
Select a value...

Api key :String
Encrypted Value ×
********* CHANGE

Helix url :URL
Custom Value: https://apps.fireeye.com/helix/id/hexzsq689 ×
https://apps.fireeye.com/helix/id/hexzsq689

CUSTOM PARAMETERS (0) + ADD

No custom parameters

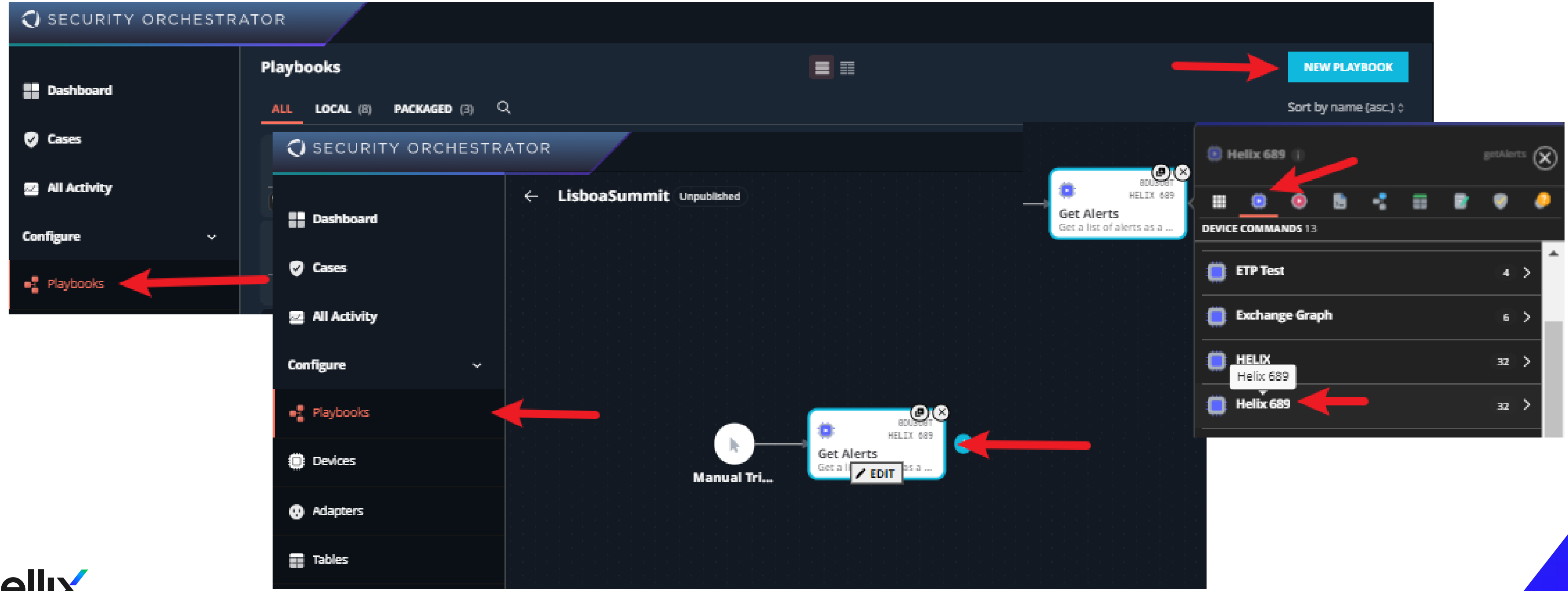
ADVANCED PARAMETERS (5)

Rate limiting time :Integer — OPTIONAL
Default: 100 ×

Tls version :String
Default: auto ×

Use Case

Identify Helix integration success



Trellix