Trellix

21 – 24 OCTOBER 2024

EMEA & LTAM Partner Tech Summit

Lisbon, Portugal

Helix Connect

Open XDR Platform

Hello!

Henrik Olsson

Director, Product Management

Filippo Sitzia

Principal Solutions Architect

Trellix

Helix Connect

Open XDR Platform

Agenda

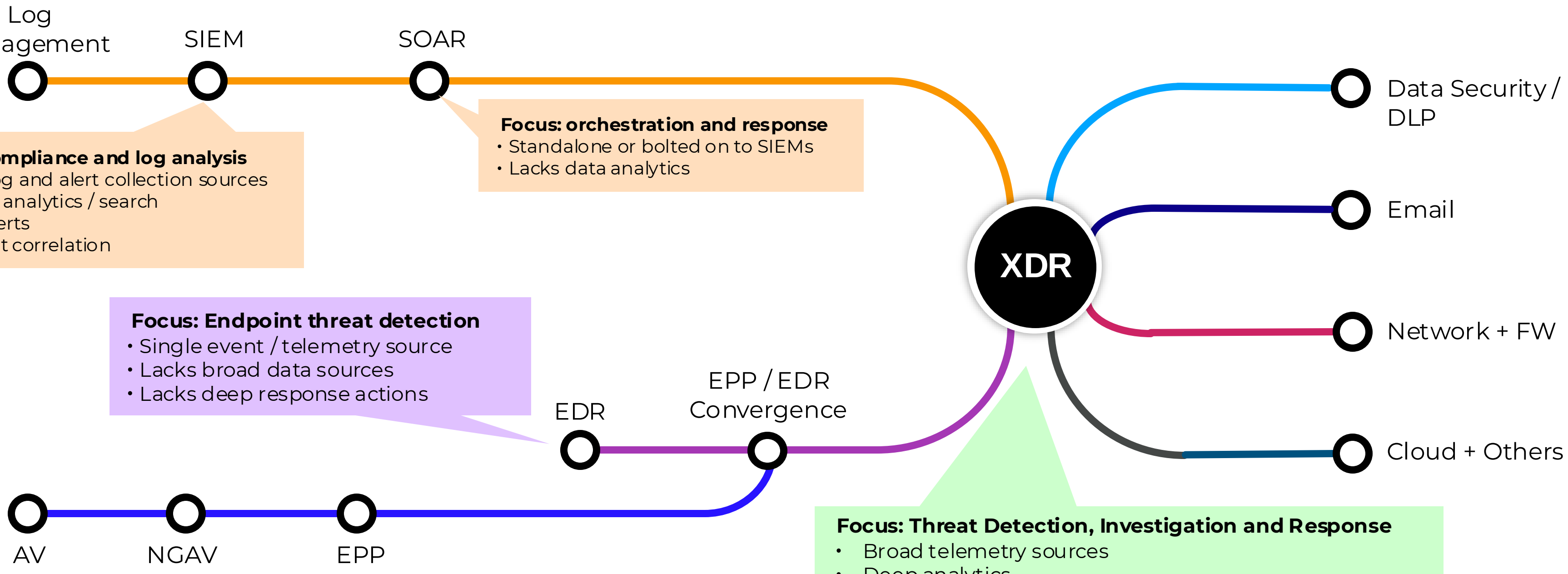
1) Intro and Sales Pitch
2) Technical Deep Dive
3) Roadmap
4) Hands-on exercises
5) Pre-Sales Resources

Trellix

Helix Connect

Open XDR Platform

Point Solutions are Incomplete



Focus compliance and log analysis
- Broad log and alert collection sources
- Security analytics / search
- Noisy alerts
- No event correlation

Focus: orchestration and response
- Standalone or bolted on to SIEMs
- Lacks data analytics

Focus: Endpoint threat detection
- Single event / telemetry source
- Lacks broad data sources
- Lacks deep response actions

Focus: Threat Detection, Investigation and Response
- Broad telemetry sources
- Deep analytics
- Integrated, automated response actions
- Built-in expertise and guided investigations

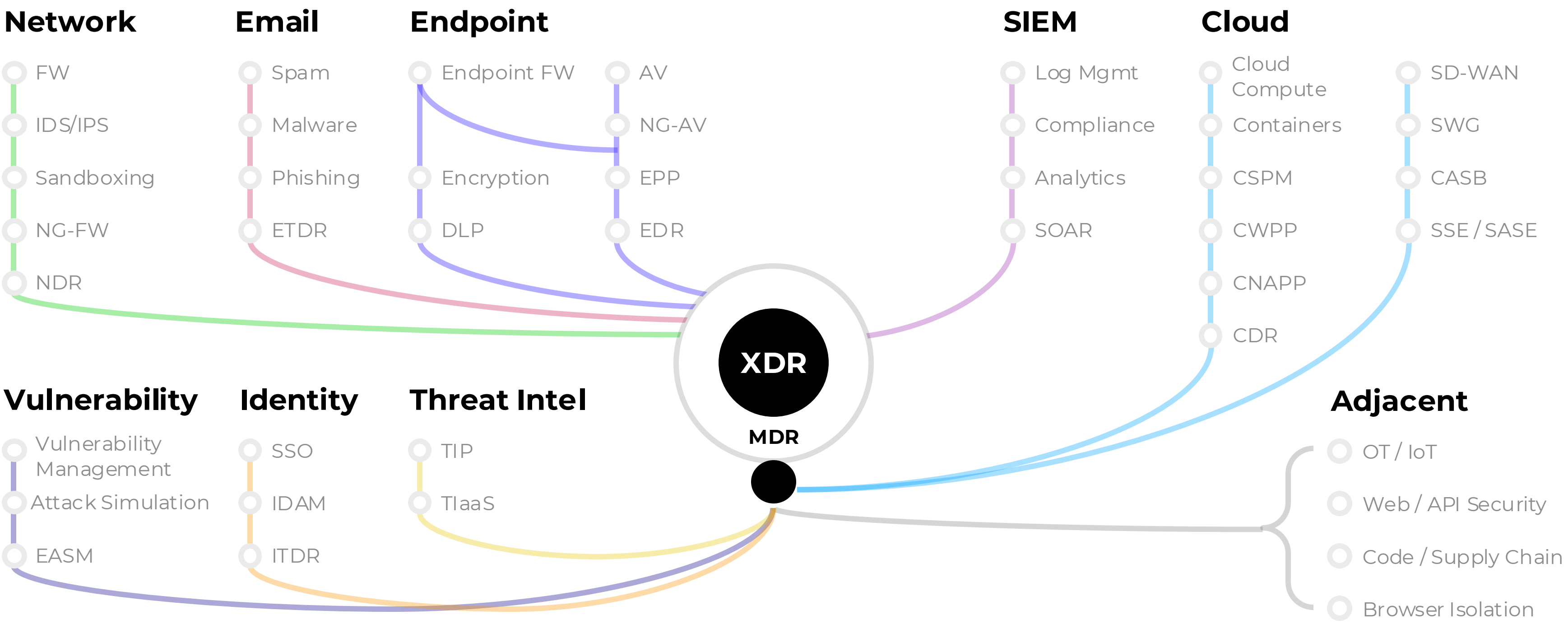
Trellix

Why do you need XDR?

ALERT FATIGUE	LONG, MANUAL PROCESSES	STAFF, SKILLS GAPS
Threat prioritization with analytics	**Built-in automation and orchestration**	**AI-driven processes and expertise**

Minimize MTTR and increase SOC efficacy across your connected enterprise

XDR: The Convergence of Point Technologies



Network
- FW
- IDS/IPS
- Sandboxing
- NG-FW
- NDR

Email
- Spam
- Malware
- Phishing
- ETDR

Endpoint
- Endpoint FW
- Encryption
- DLP
- AV
- NG-AV
- EPP
- EDR

SIEM
- Log Mgmt
- Compliance
- Analytics
- SOAR

Cloud
- Cloud Compute
- Containers
- CSPM
- CWPP
- CNAPP
- CDR
- SD-WAN
- SWG
- CASB
- SSE / SASE

XDR

MDR

Vulnerability
- Vulnerability Management
- Attack Simulation
- EASM

Identity
- SSO
- IDAM
- ITDR

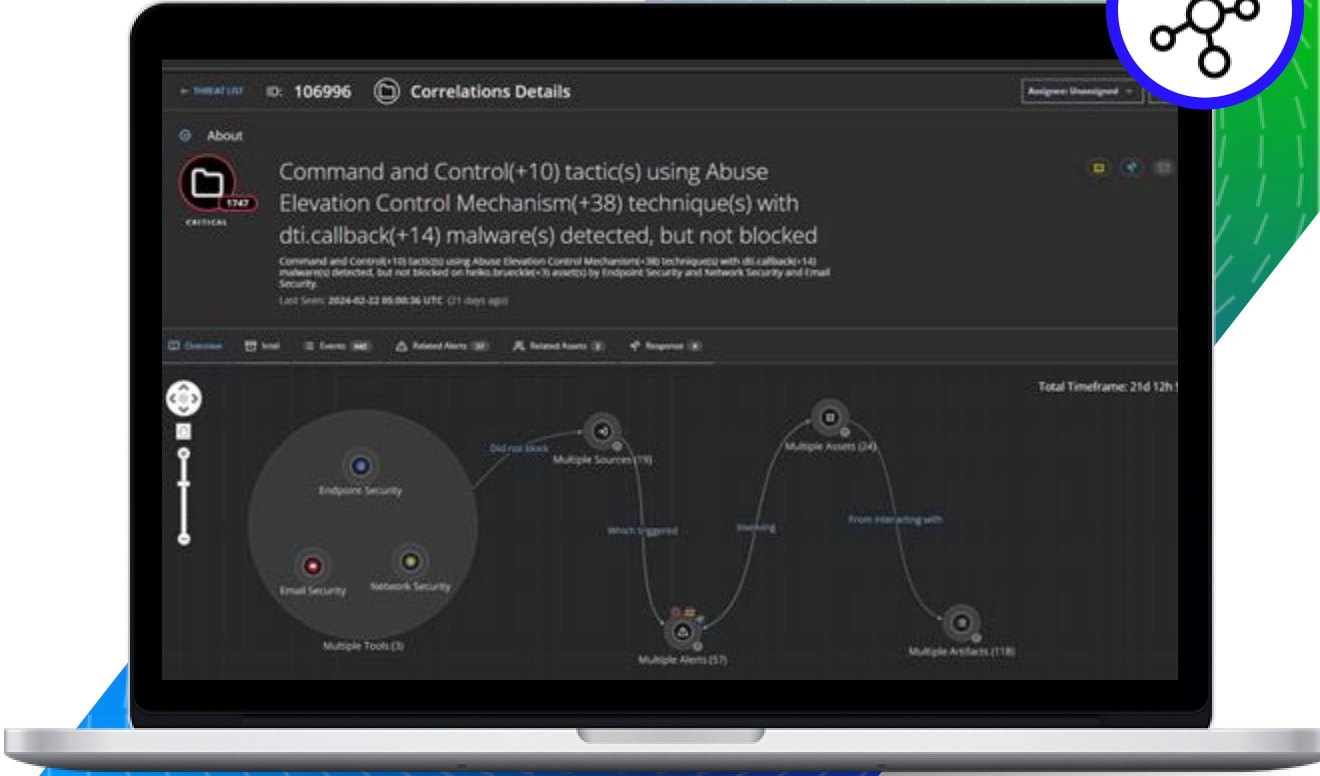
Threat Intel
- TIP
- TIaaS

Adjacent
- OT / IoT
- Web / API Security
- Code / Supply Chain
- Browser Isolation

Integrate + Analyze + Prioritize

Helix Connect

Speed detection and response with multi-vector, multi-vendor correlation



← THREAT LIST ID: 106996 Correlations Details

About

Command and Control(+10) tactic(s) using Abuse Elevation Control Mechanism(+38) technique(s) with dti.callback(+14) malware(s) detected, but not blocked

Command and Control(+10) tactic(s) using Abuse Elevation Control Mechanism(+38) technique(s) with dti.callback(+14) malware(s) detected, but not blocked on heiko.brueckle(+3) asset(s) by Endpoint Security and Network Security and Email Security.

Last Seen: 2024-02-22 00:00:36 UTC (21 days ago)

Total Timeframe: 21d 12h

Trellix

How Helix Connect Works

1. Broad data Ingestion

Open and
native integrations

2. Detections:

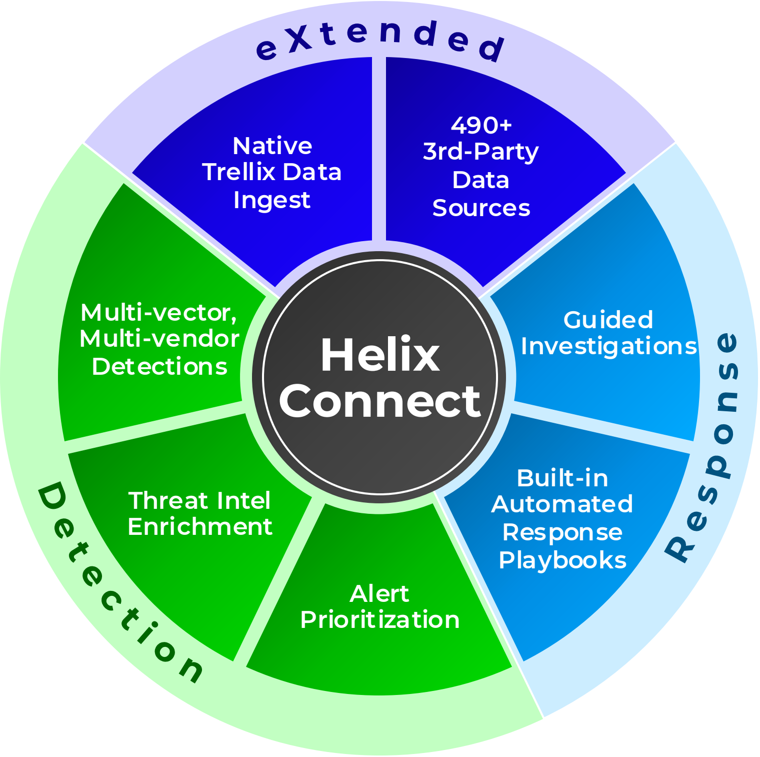
Analytics

Automated
threat elimination

Noise suppression

Enrichment

Prioritization


eXtended
Native Trellix Data Ingest
490+ 3rd-Party Data Sources
Helix Connect
Multi-vector, Multi-vendor Detections
Threat Intel Enrichment
Alert Prioritization
Guided Investigations
Built-in Automated Response Playbooks
Detection
Response

3. Response

On-prem / cloud
orchestration
and response

AI-guidance

Pre-built,
customizable
playbooks

Trellix

What Can Helix Connect do for You?

40-60+
siloed tools

4-10K
unranked alerts a day

30 minutes
to begin remediations

1
location to view correlated data

>70%
less false positives and events prioritized by impact

5
minutes or less to remediation actions

Trellix

Helix Connect

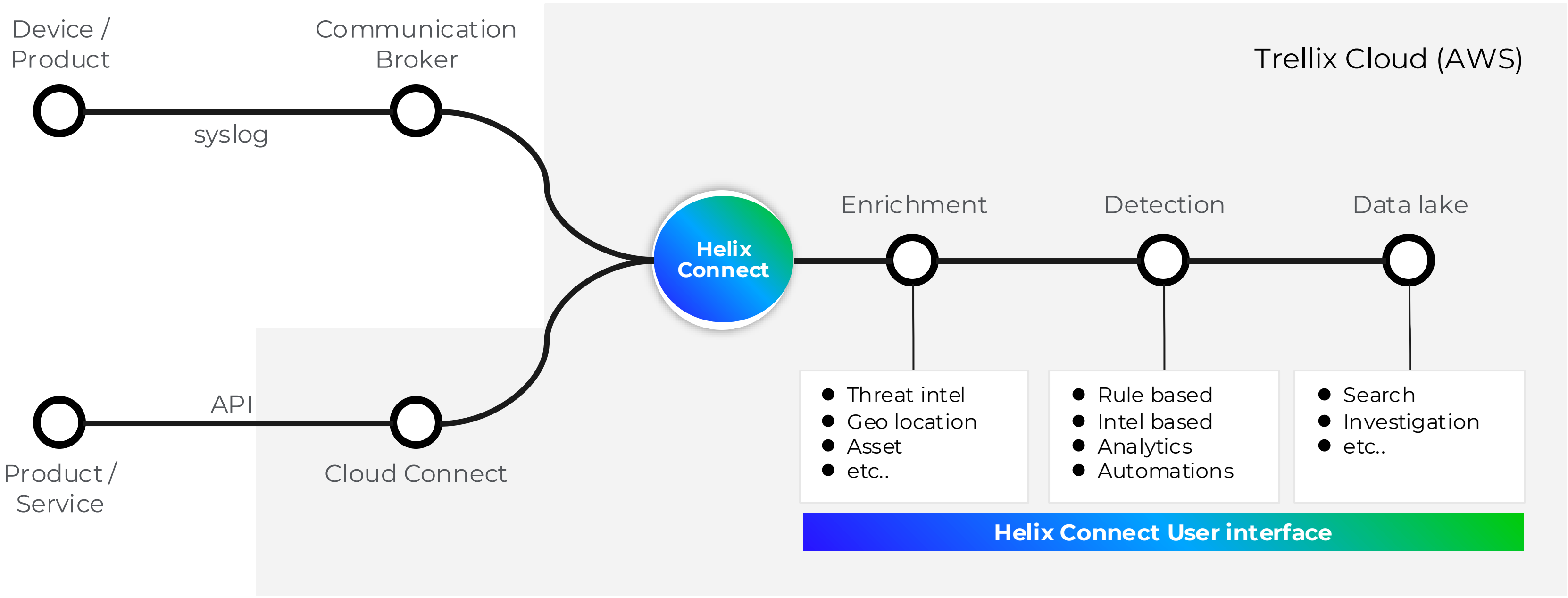
Technical Deep Dive

- Architecture and integrations
- Events data
- Alert mechanisms
- Response tools

Architecture and Integrations

- Architecture
- Integration Hub
- Communication Broker
- Apps

Helix Connect architecture



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

- Rule based
- Intel based
- Analytics
- Automations

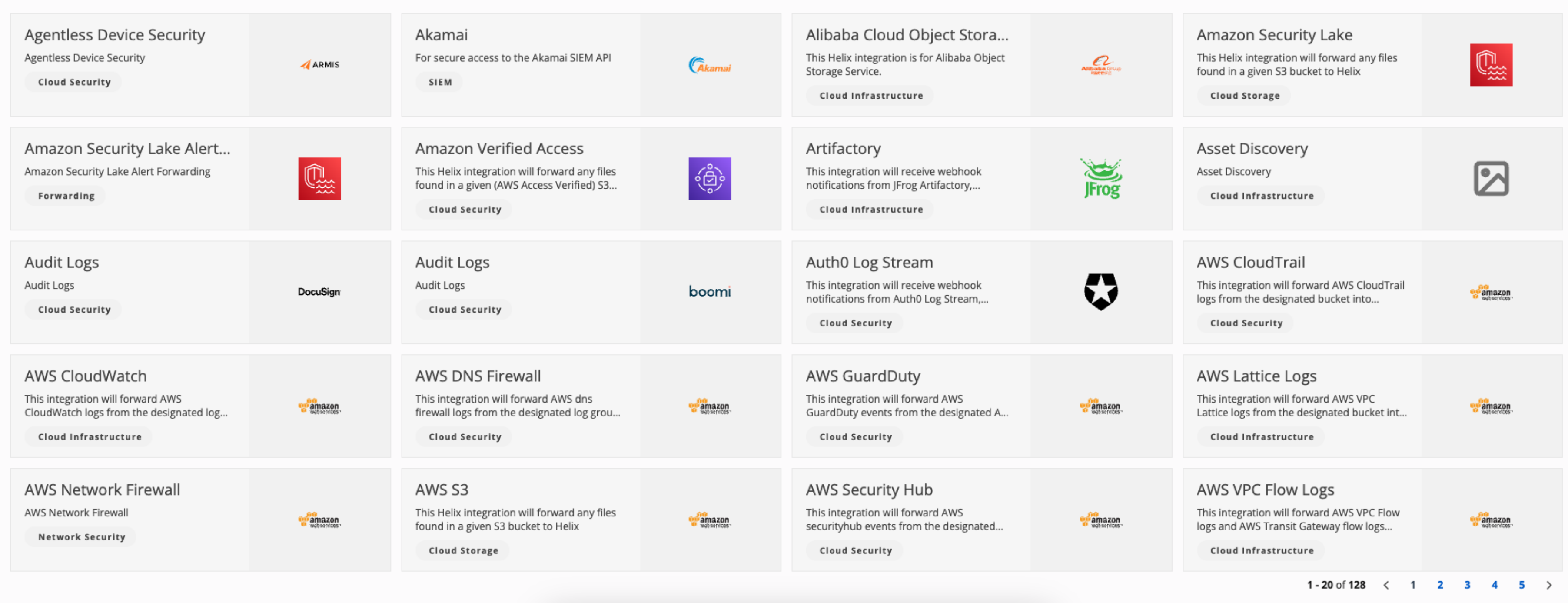
- Search
- Investigation
- etc..

Helix Connect User interface

Trellix

Integration Hub

Allow events and logs to be sent to Helix Connect through API connections.



Agentless Device Security
Agentless Device Security
Cloud Security

Akamai
For secure access to the Akamai SIEM API
SIEM

Alibaba Cloud Object Stora...
This Helix integration is for Alibaba Object Storage Service.
Cloud Infrastructure

Amazon Security Lake
This Helix integration will forward any files found in a given S3 bucket to Helix
Cloud Storage

Amazon Security Lake Alert...
Amazon Security Lake Alert Forwarding
Forwarding

Amazon Verified Access
This Helix integration will forward any files found in a given (AWS Access Verified) S3...
Cloud Security

Artifactory
This integration will receive webhook notifications from JFrog Artifactory,...
Cloud Infrastructure

Asset Discovery
Asset Discovery
Cloud Infrastructure

Audit Logs
Audit Logs
Cloud Security

Audit Logs
Audit Logs
Cloud Security

Auth0 Log Stream
This integration will receive webhook notifications from Auth0 Log Stream,...
Cloud Security

AWS CloudTrail
This integration will forward AWS CloudTrail logs from the designated bucket into...
Cloud Security

AWS CloudWatch
This integration will forward AWS CloudWatch logs from the designated log...
Cloud Infrastructure

AWS DNS Firewall
This integration will forward AWS dns firewall logs from the designated log grou...
Cloud Security

AWS GuardDuty
This integration will forward AWS GuardDuty events from the designated A...
Cloud Security

AWS Lattice Logs
This integration will forward AWS VPC Lattice logs from the designated bucket int...
Cloud Infrastructure

AWS Network Firewall
AWS Network Firewall
Network Security

AWS S3
This Helix integration will forward any files found in a given S3 bucket to Helix
Cloud Storage

AWS Security Hub
This integration will forward AWS securityhub events from the designated...
Cloud Security

AWS VPC Flow Logs
This integration will forward AWS VPC Flow logs and AWS Transit Gateway flow logs...
Cloud Infrastructure

1 - 20 of 128 ‹ 1 2 3 4 5 ›

Communication Broker

Allow events and logs to be sent to Helix Connect through syslogs.

- 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.

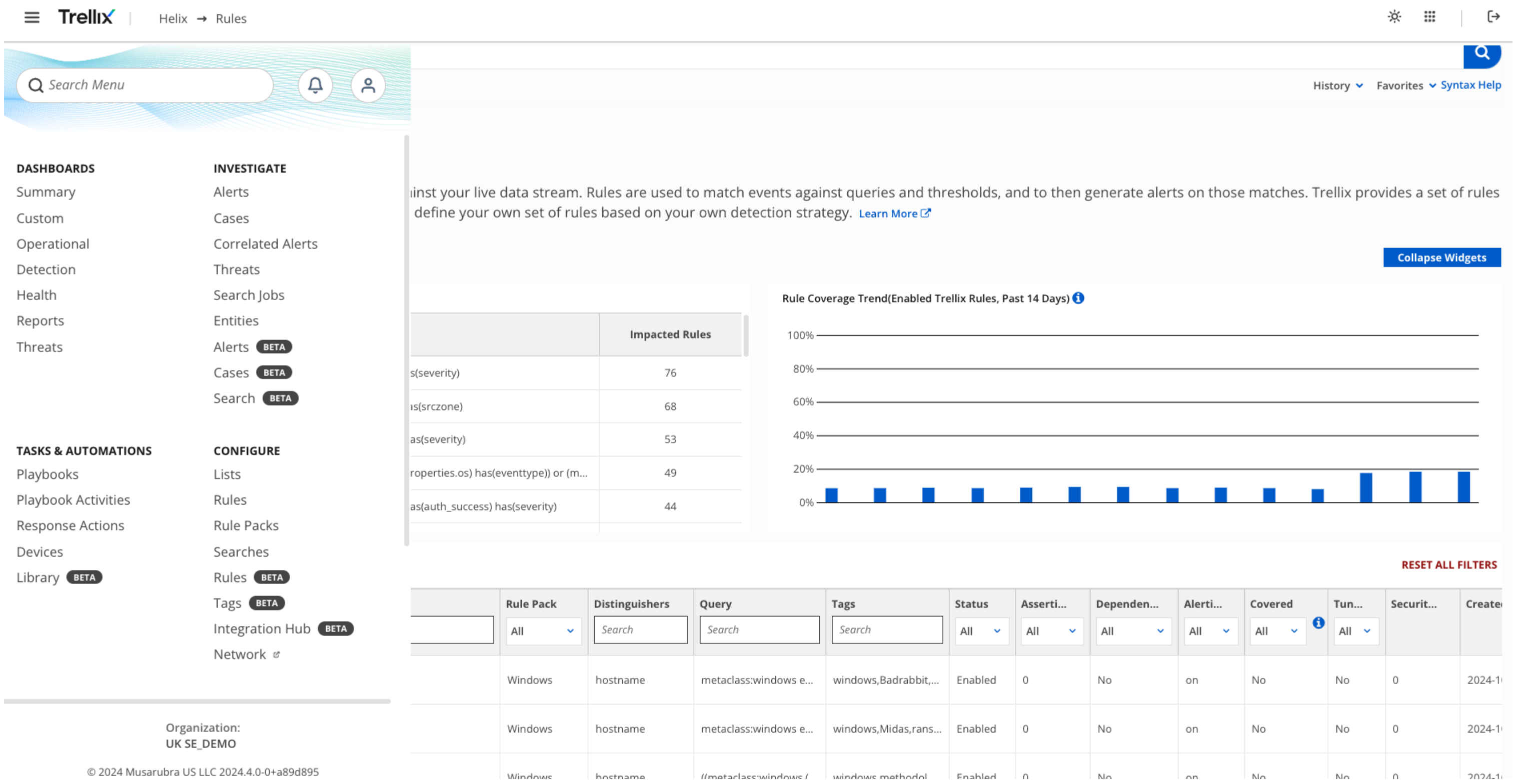
- The Comm Broker looks for events formatted as the following (in descending order of preference): JSON, CEF syslog, LEEF 1.0 & 2.0 syslog, RFC-5424 Syslog (https://tools.ietf.org/html/rfc5424), RFC-3164 Syslog (https://tools.ietf.org/html/rfc3164)

- 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.

Apps – New, Beta, Legacy



Organization:
UK SE_DEMO

© 2024 Musarubra US LLC 2024.4.0-0+a89d895

iinst 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
ıs(srczone)	68
as(severity)	53
roperties.os) has(eventtype)) or (m...	49
as(auth_success) has(severity)	44

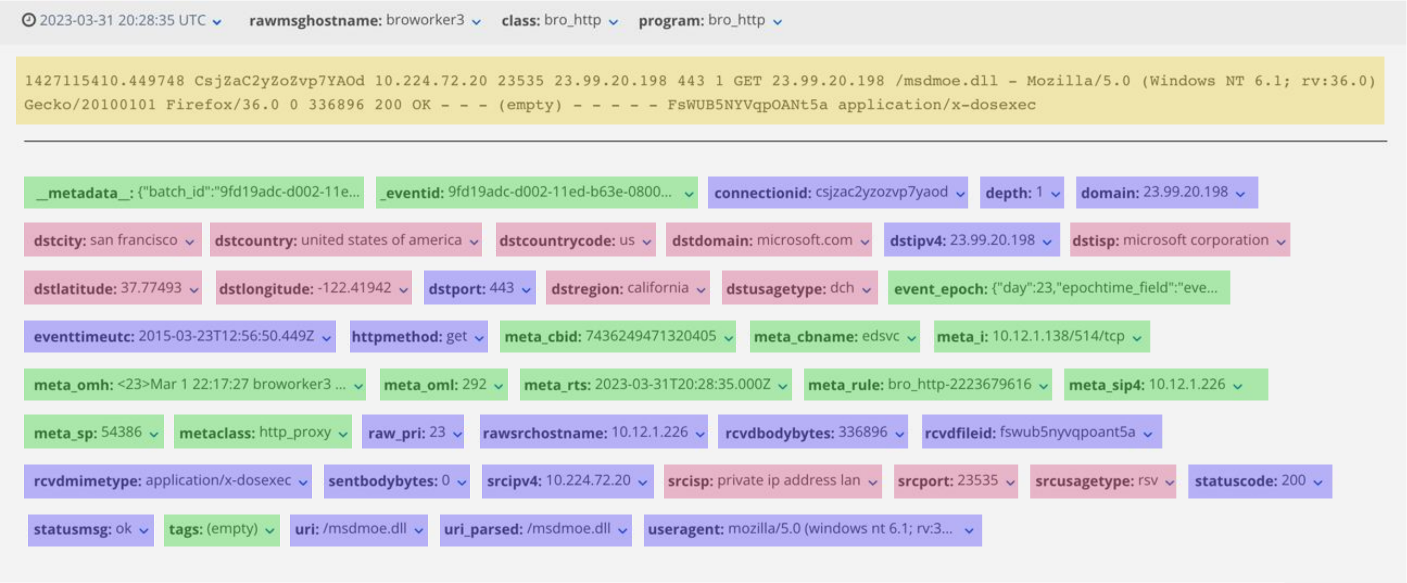
	Rule Pack	Distinguishers	Query	Tags	Status	Asserti...	Dependen...	Alerti...	Covered	Tun...	Securit...	Create
	All	Search	Search	Search	All	All	All	All	All	All		
	Windows	hostname	metaclass:windows e...	windows,Badrabbit,...	Enabled	0	No	on	No	No	0	2024-1
	Windows	hostname	metaclass:windows e...	windows,Midas,rans...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

Events data

- Format
- TQL

Trellix

Event Format



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

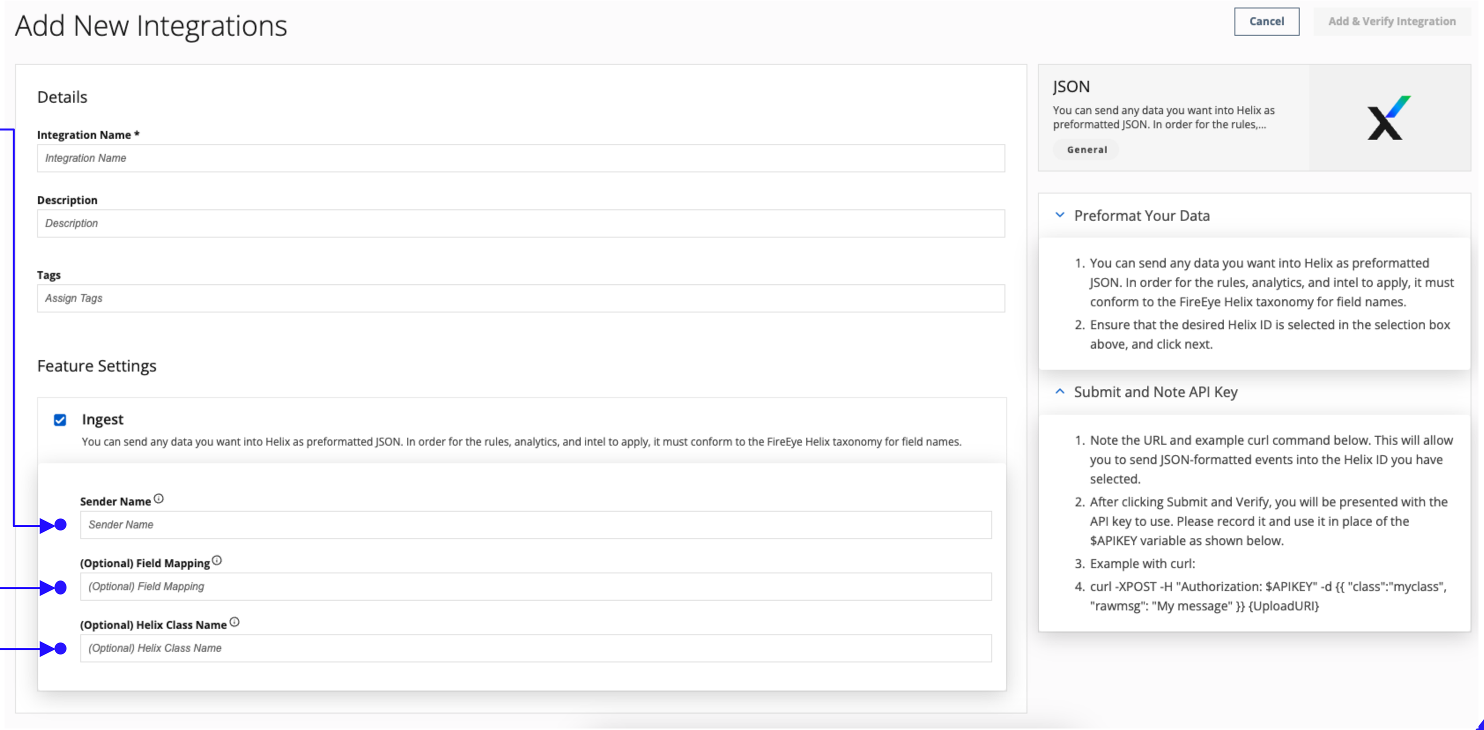
Events

You can send any data you want into Helix as preformatted JSON.
For the rules, analytics, and intel to apply, it must conform to the taxonomy.

Sender Name

Field Mapping

Class Name



Add New Integrations

Cancel | Add & Verify Integration

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}

Events

Example: Generic AV Log

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

Class myav

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

PARSED_LOG

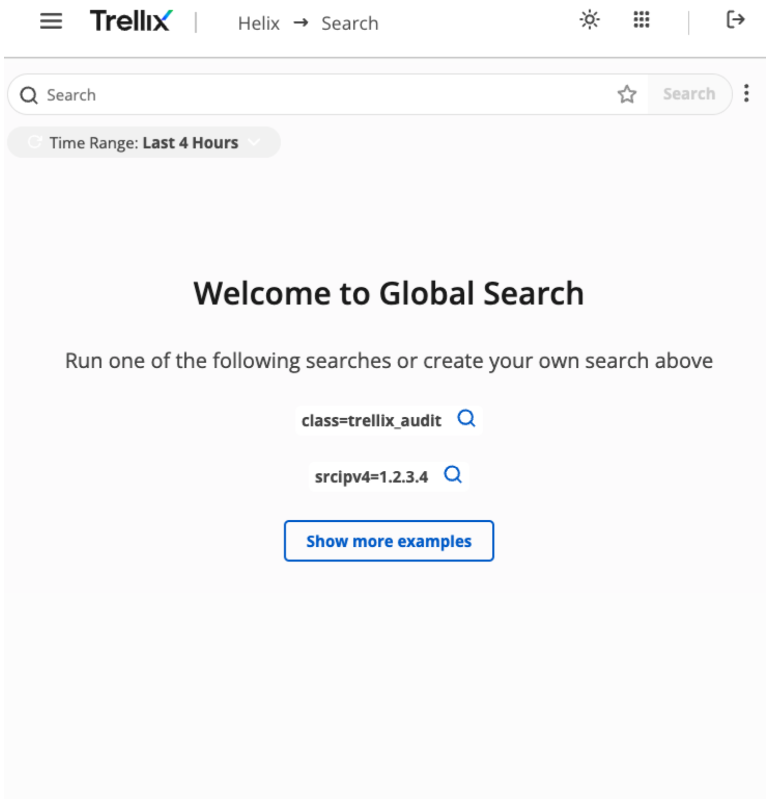
- username : jessica.salt
- md5hash : 4373CF0D42926B15F95E35683D883A1C
- malwaretype : ransomware

[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

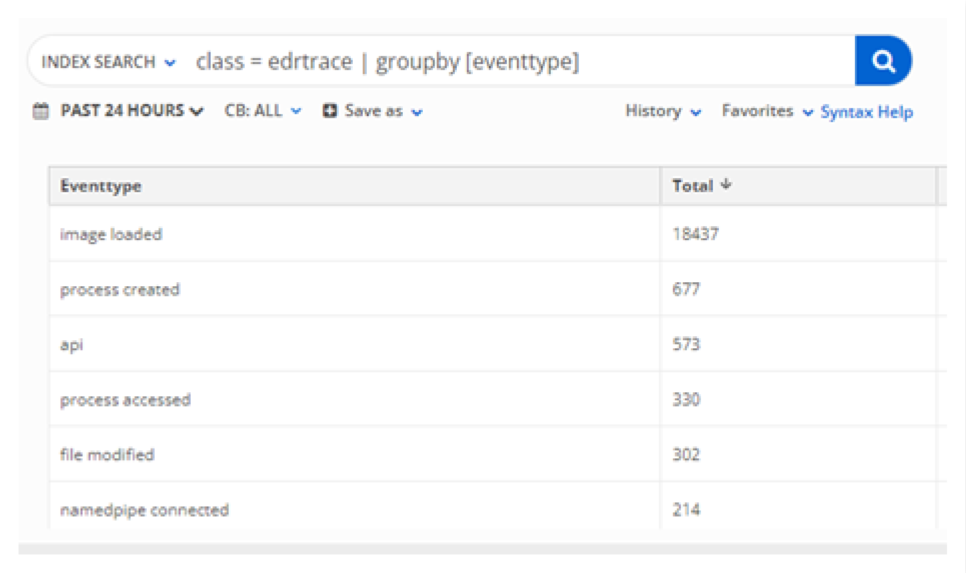
Run one of the following searches or create your own search above

```
class=trellix_audit
srcipv4=1.2.3.4
```

Anatomy of a TQL query

High-level anatomy of an TQL query:

<filter section> | <transform section>



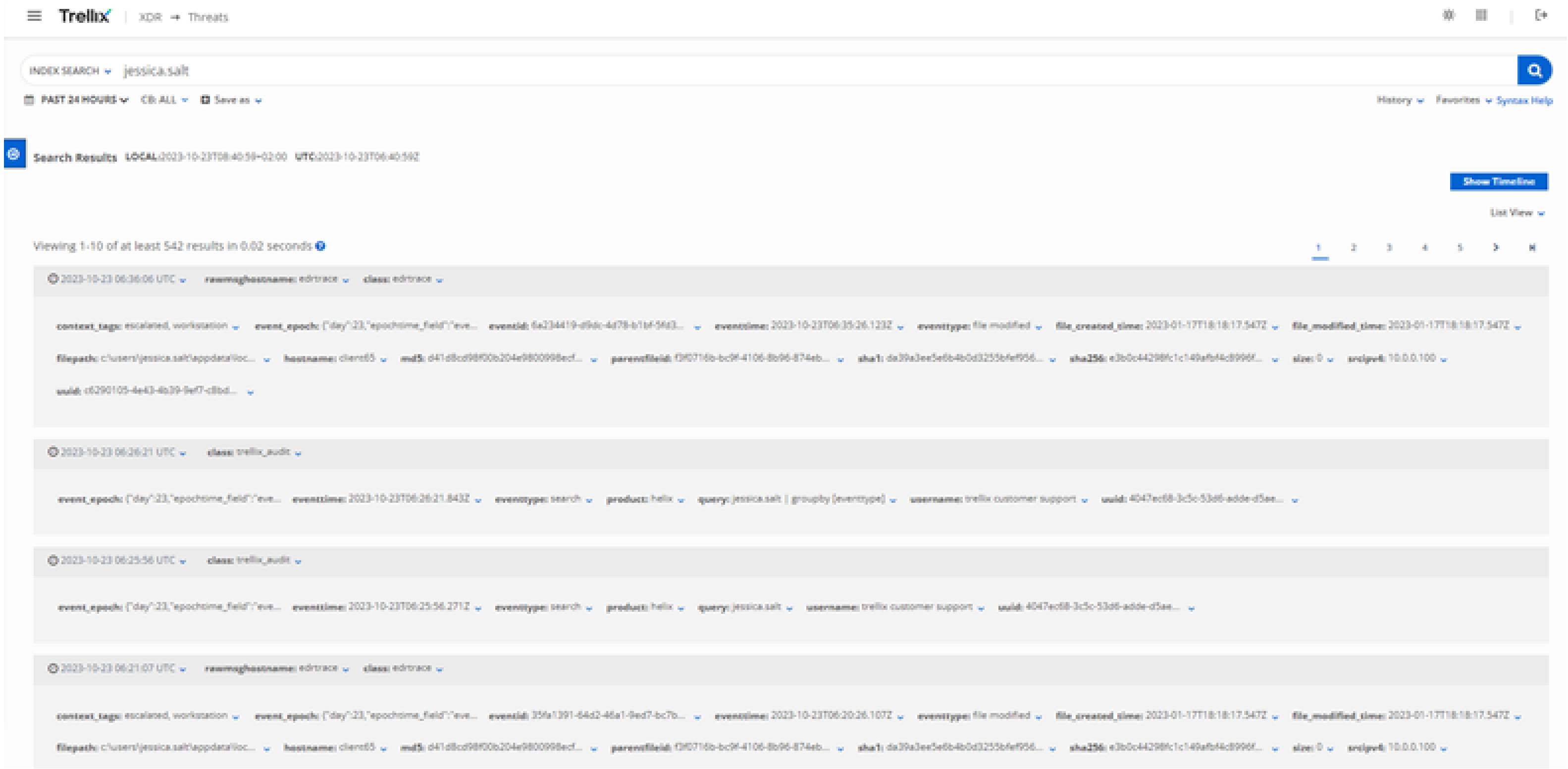
```
class = edrtrace | groupby [eventtype]
```

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

TQL query can use three types of clauses:

- **Searches:** data to be located based on exact matches, comparisons, ranges, and expressions
- **Directives:** modifiers that instruct the search engine how to query [Limit, Page_size, Offset, Start, End]
- **Transforms:** allow you to modify the way that your query results are returned and displayed [Groupby, Histogram, Sort, Table]

TQL - Examples



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: c6290105-4e63-4b39-9ef7-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-d5ee...

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

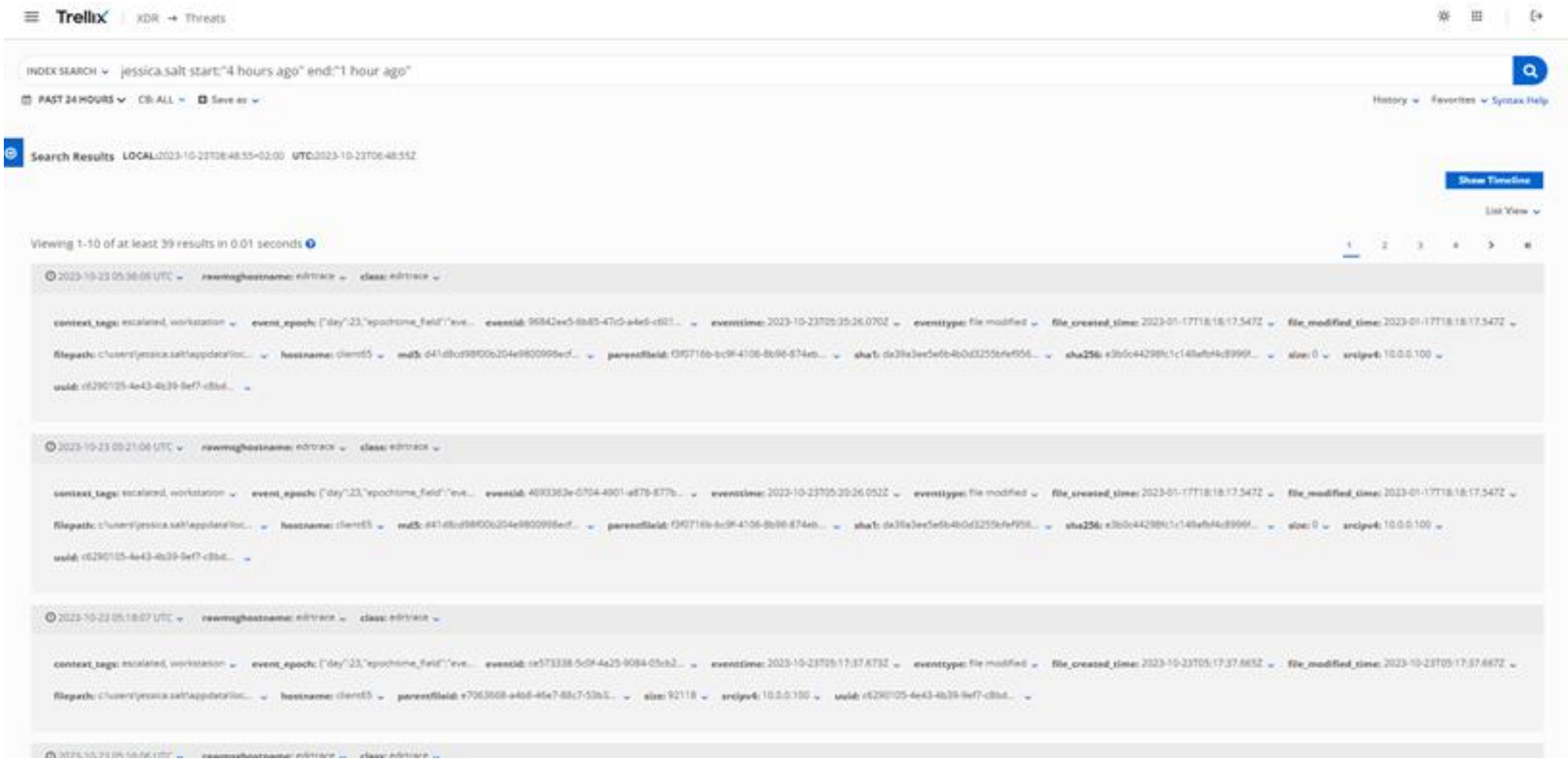
event_epoch: {"day":23,"epochtime_field":"eve... **eventtime:** 2023-10-23T06:25:56.271Z **eventtype:** search **product:** helix **query:** jessica.salt **username:** trellix customer support **uuid:** 4047ec68-3c5c-53d6-adde-d5ee...

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 - Examples



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 05:36:08 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...

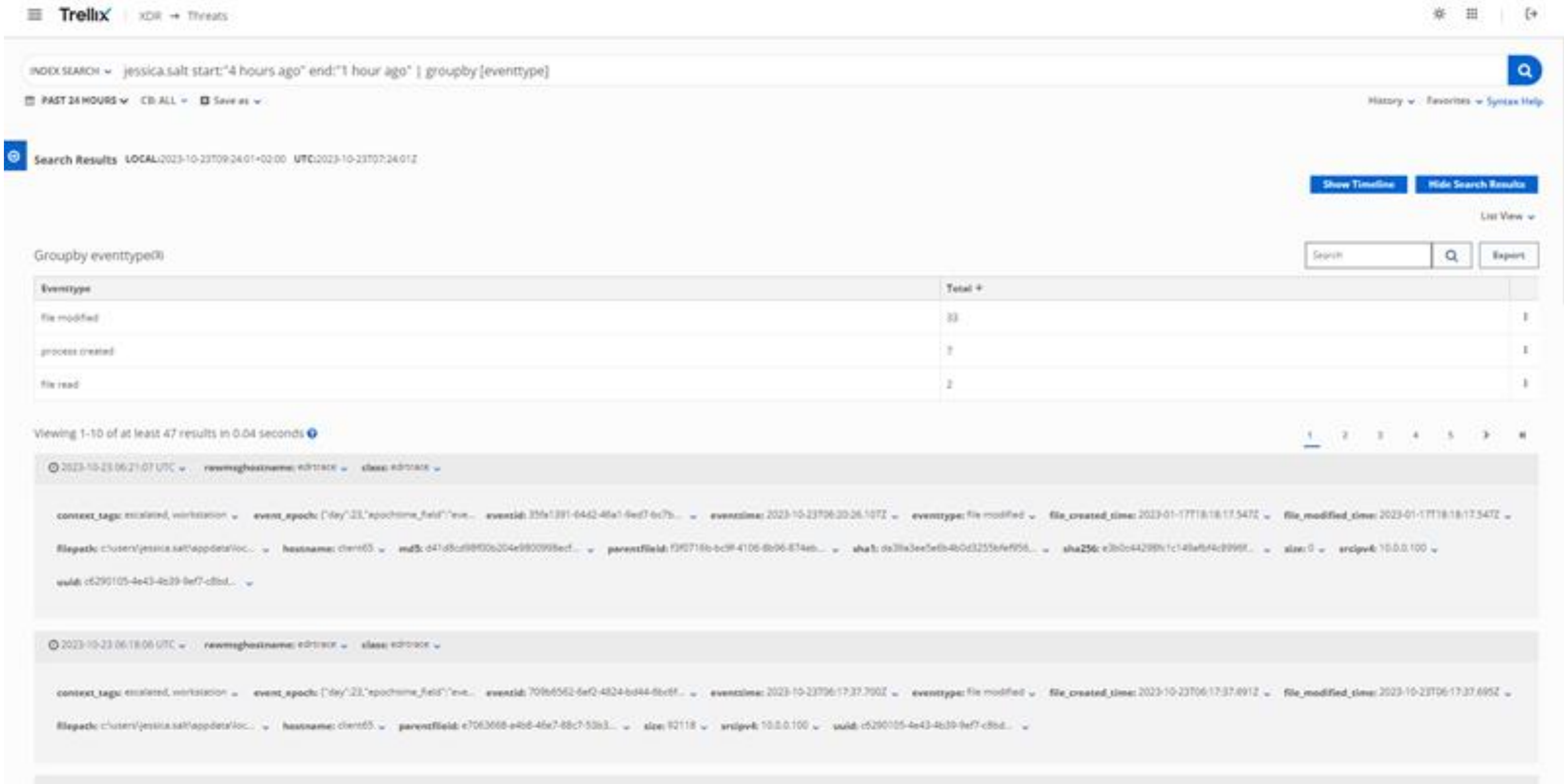
2023-10-23 05:18:07 UTC rawmsghostname: edrtrace class: edrtrace

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-a4b8-46e7-88c7-53b5... 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 - Examples



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

1 2 3 4 5

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

context_tags: escalated, workstation event_epoch: {"day":23,"epochtime_field":"eve... eventid: 35fa1391-6442-46a1-9ed7-6c7b... 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: f3f0718b-bc9f-4106-8b96-874eb... sha1: da39a3ee5e6b4b0d3255bfef956... sha256: e3b0c44298fc1c149afbf4c8996f... size: 0 srcipv4: 10.0.0.100
uuid: c6290105-4e43-4b39-9ef7-c8bd...

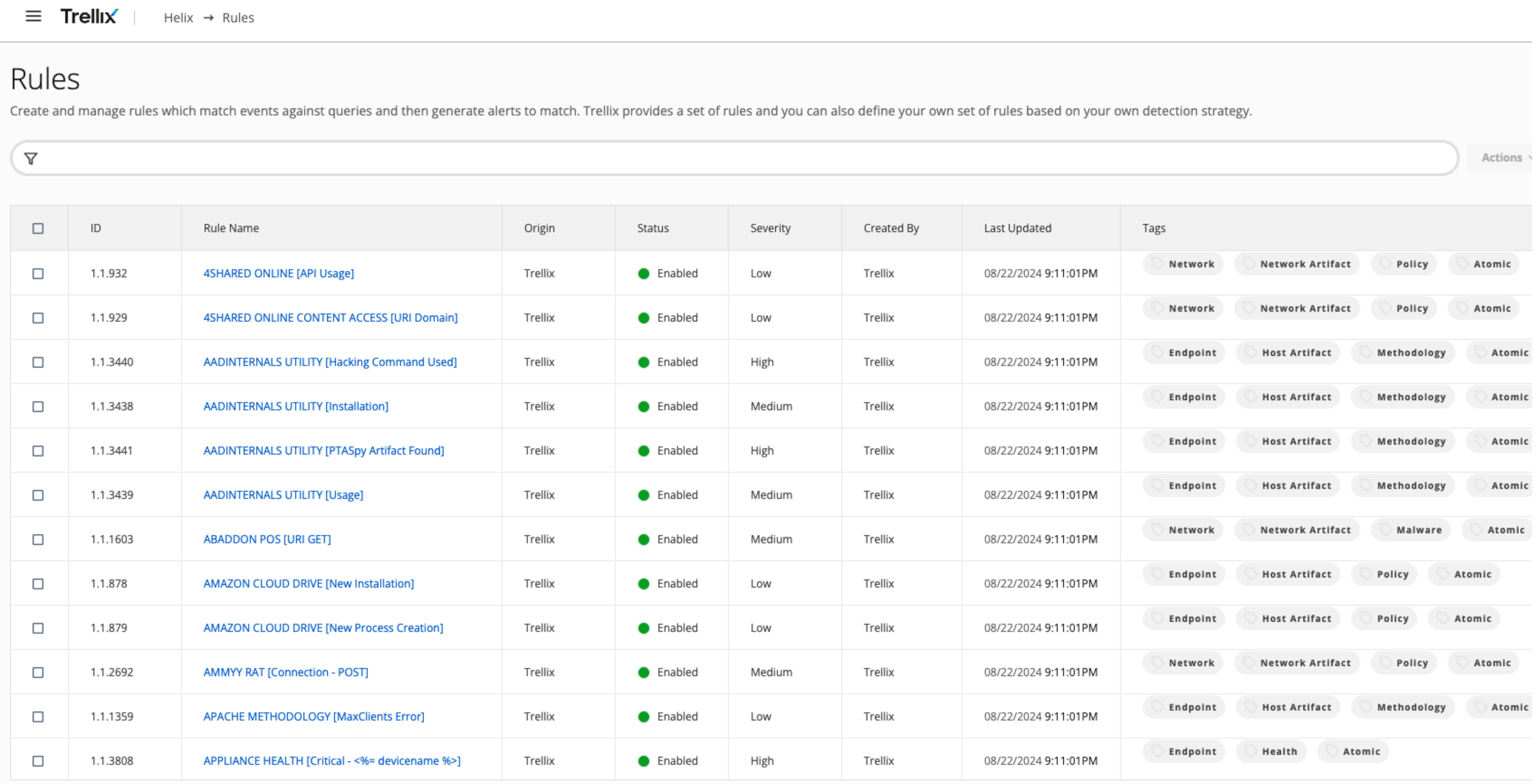
2023-10-23 06:18:06 UTC rawmsghostname: edrtrace class: edrtrace

context_tags: escalated, workstation event_epoch: {"day":23,"epochtime_field":"eve... eventid: 709b6562-6ef2-4824-bd44-8bc6f... 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
- Case management
- Wise

Rules



Rules

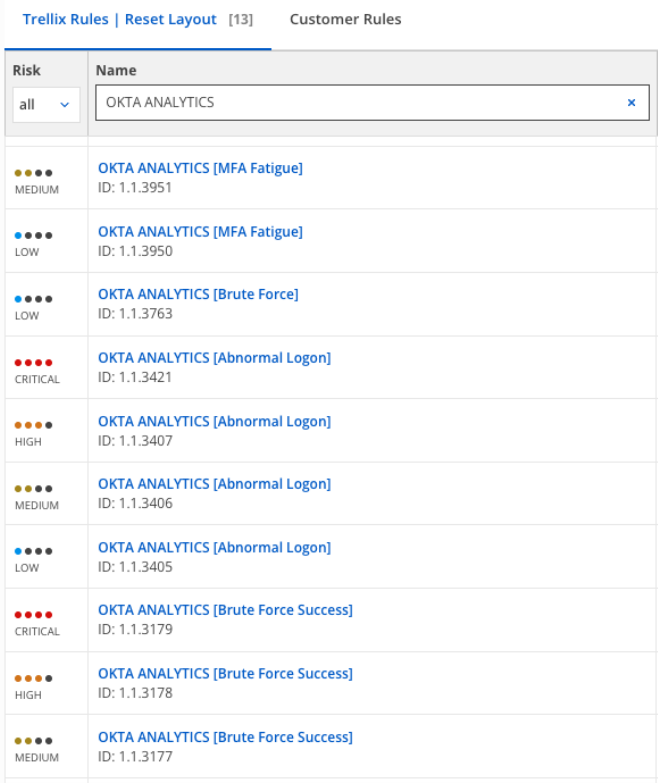
Create and manage rules which match events against queries and then generate alerts to match. Trellix provides a set of rules and you can also define your own set of rules based on your own detection strategy.

□	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



Trellix Rules | Reset Layout [13]   Customer Rules

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
```

Trellix

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
```

Trellix

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

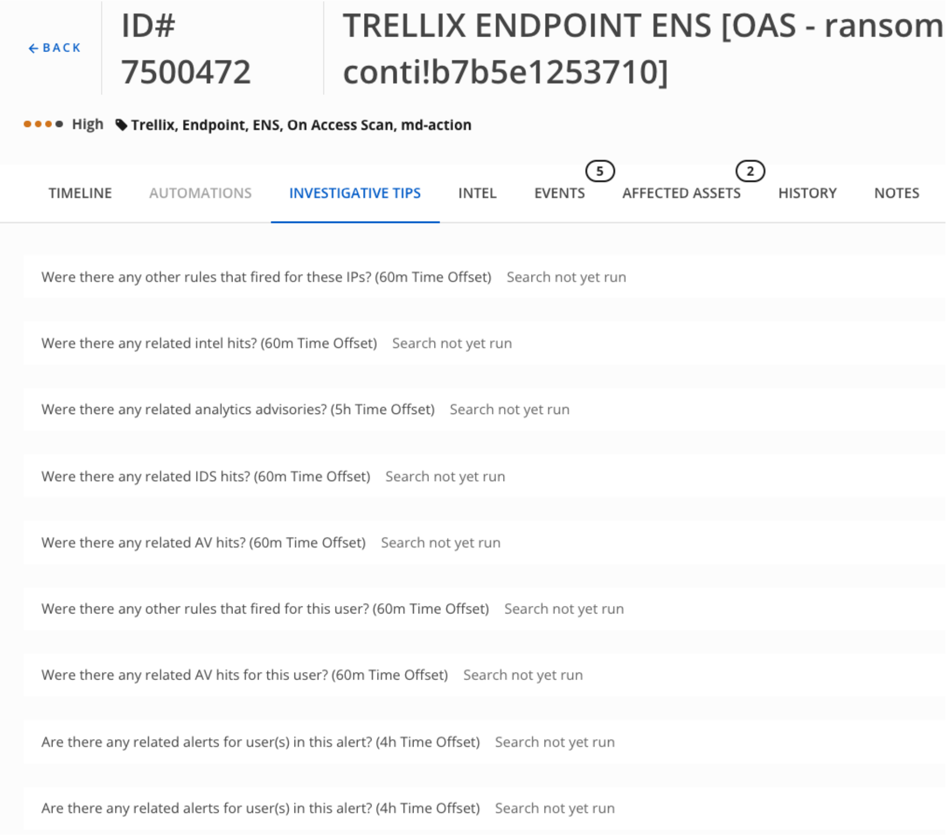
Monitor user and entity activity over time to identify anomalies

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

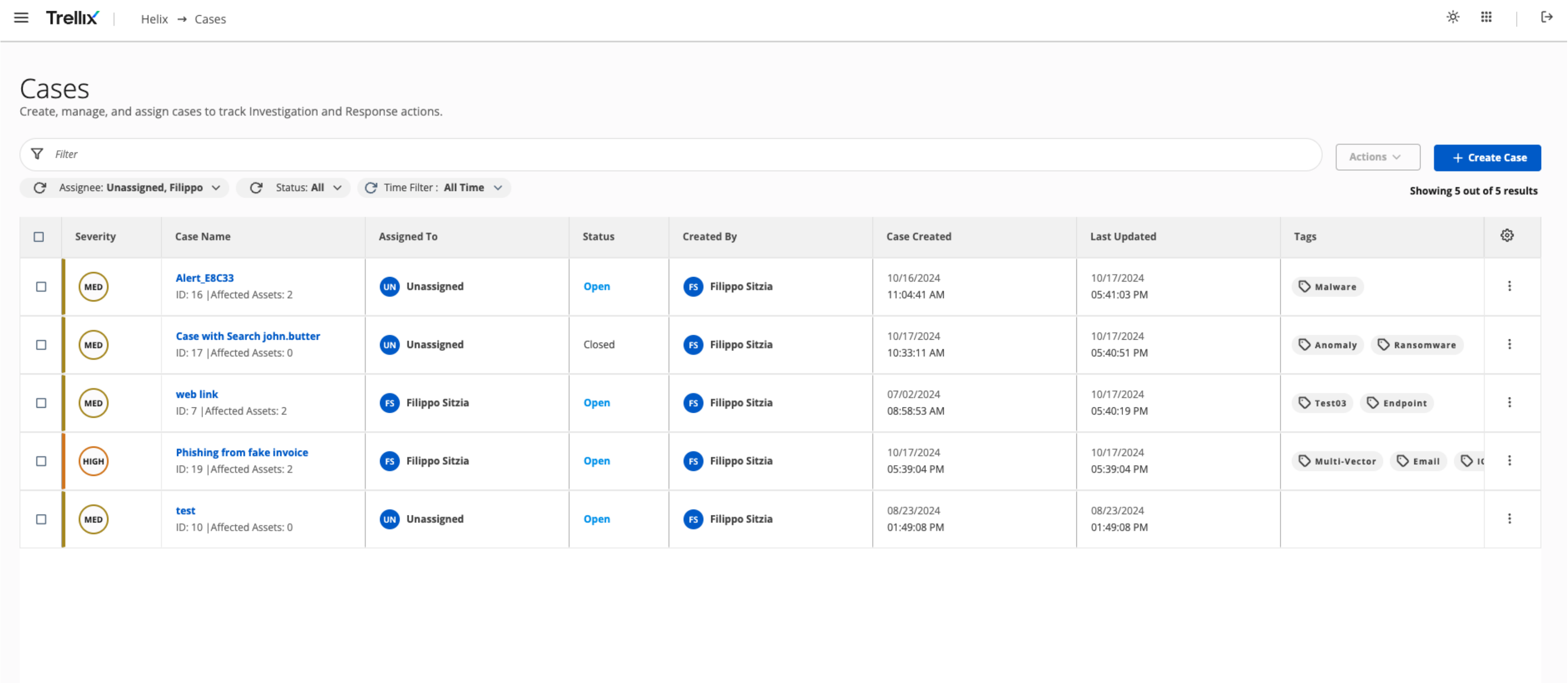
Were there any related AV hits for this user? (60m Time Offset) Search not yet run

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

Trellix

Case management



Cases

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

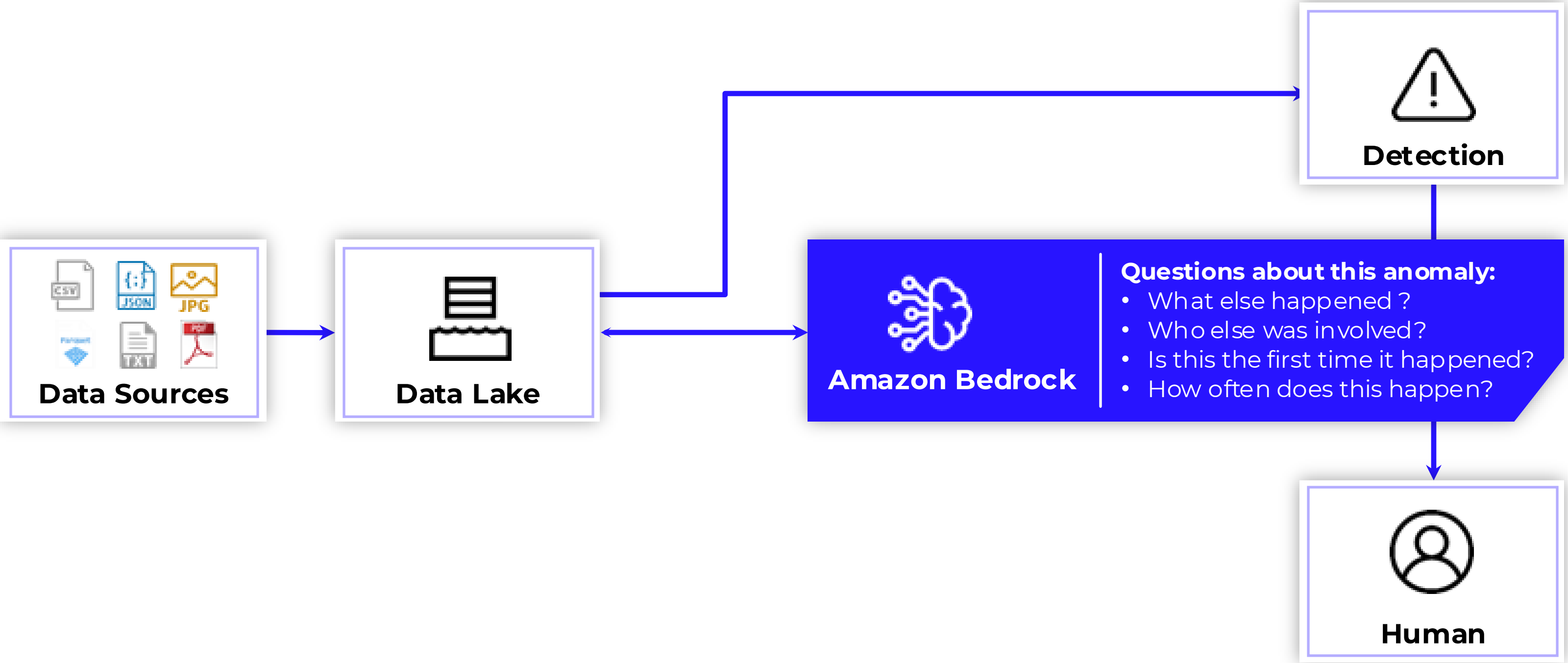
Assignee: **Unassigned, Filippo** | Status: **All** | Time Filter : **All Time**

Showing 5 out of 5 results

□	Severity	Case Name	Assigned To	Status	Created By	Case Created	Last Updated	Tags
□	MED	Alert_E8C33 ID: 16 |Affected Assets: 2	UN Unassigned	Open	FS Filippo Sitzia	10/16/2024 11:04:41 AM	10/17/2024 05:41:03 PM	Malware
□	MED	Case with Search john.butter ID: 17 |Affected Assets: 0	UN Unassigned	Closed	FS Filippo Sitzia	10/17/2024 10:33:11 AM	10/17/2024 05:40:51 PM	Anomaly Ransomware
□	MED	web link ID: 7 |Affected Assets: 2	FS Filippo Sitzia	Open	FS Filippo Sitzia	07/02/2024 08:58:53 AM	10/17/2024 05:40:19 PM	Test03 Endpoint
□	HIGH	Phishing from fake invoice ID: 19 |Affected Assets: 2	FS Filippo Sitzia	Open	FS Filippo Sitzia	10/17/2024 05:39:04 PM	10/17/2024 05:39:04 PM	Multi-Vector Email IC
□	MED	test ID: 10 |Affected Assets: 0	UN Unassigned	Open	FS Filippo Sitzia	08/23/2024 01:49:08 PM	08/23/2024 01:49:08 PM	

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?

Trellix

GenAI and customer data

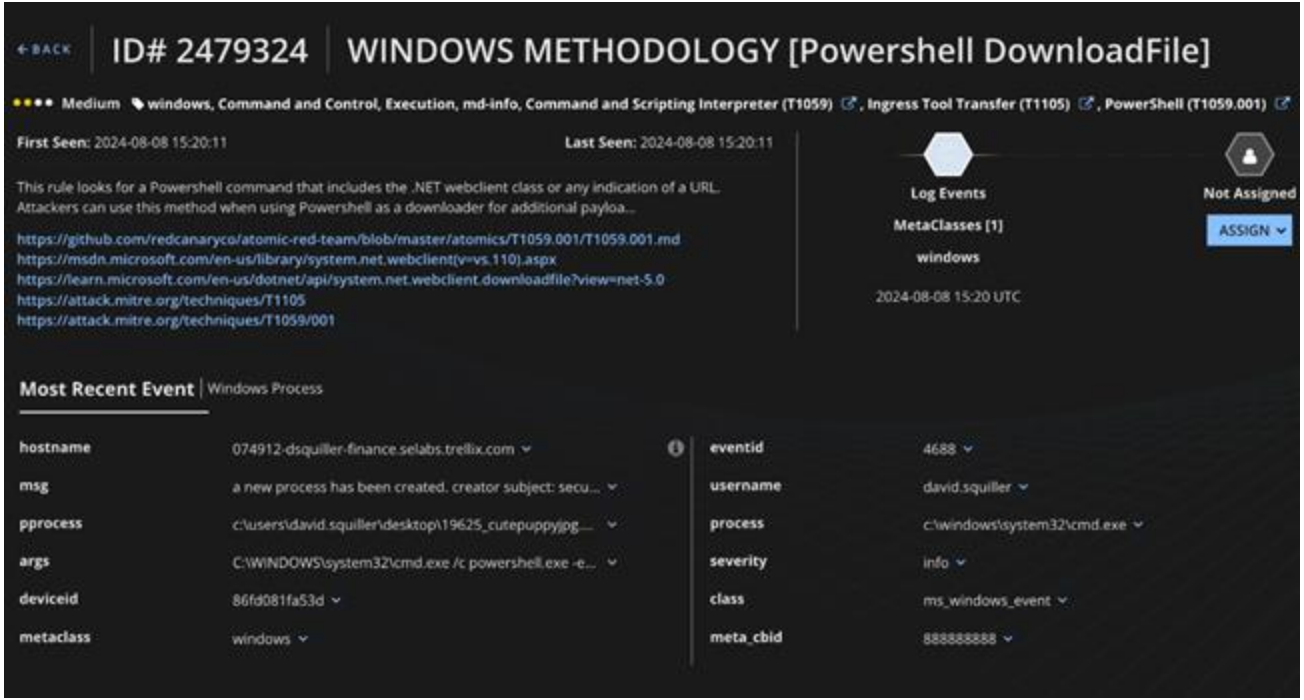
Does Trellix Wise use customer data to train models?

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**.

Auto Investigation: How good is it?

What does it look like when Trellix Wise investigates an alert?



ID# 2479324 WINDOWS METHODOLOGY [Powershell DownloadFile]

●●●● Medium windows, Command and Control, Execution, md-info, Command and Scripting Interpreter (T1059), Ingress Tool Transfer (T1105), PowerShell (T1059.001)

First Seen: 2024-08-08 15:20:11 **Last Seen:** 2024-08-08 15:20:11

This rule looks for a Powershell command that includes the .NET webclient class or any indication of a URL. Attackers can use this method when using Powershell as a downloader for additional payloa...

https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1059.001/T1059.001.md
https://msdn.microsoft.com/en-us/library/system.net.webclient(v=vs.110).aspx
https://learn.microsoft.com/en-us/dotnet/api/system.net.webclient.downloadfile?view=net-5.0
https://attack.mitre.org/techniques/T1105
https://attack.mitre.org/techniques/T1059/001

Log Events
MetaClasses [1]
windows
2024-08-08 15:20 UTC

Not Assigned

Most Recent Event | Windows Process

hostname	074912-dsquiller-finance.selabs.trellix.com	eventid	4688
msg	a new process has been created. creator subject: secu...	username	david.squiller
pprocess	c:\users\david.squiller\desktop\19625_cutepuppyjpg....	process	c:\windows\system32\cmd.exe
args	C:\WINDOWS\system32\cmd.exe /c powershell.exe -e...	severity	info
deviceid	86fd081fa53d	class	ms_windows_event
metaclass	windows	meta_cbid	888888888

Methodology alerts are not "good" or "bad," they must be investigated.

Was this use of Powershell malicious?

Auto Investigation: Who is involved?

Trellix Wise uses the rich context provided by integrations to understand the role of the user.

```
After analyzing the provided information, here is my assessment:
Explanation:
1. User profile: David Squiller is a Director in the Sales department, not a support account
or super user. His role doesn't typically involve running PowerShell scripts or executing
potentially malicious files.
2. IP profile: No specific IP address is provided for analysis.
3. Standard tools: The command executed is not a standard tool. It's a PowerShell command that
downloads and executes a script from a GitHub repository, which is highly suspicious.
4. Story in the data: The most plausible story is malicious activity. A file named
"19625_cutepuppyjpg.exe" (likely masquerading as an image) executed a command to run
PowerShell with bypassed execution policy, downloading and executing a script from GitHub.
This is a common technique used by attackers.
5. Evidence of success: The alert indicates the process was successfully created, suggesting
the malicious activity was likely successful in its initial stages.
6. Importance of target: While David Squiller is not marked as a VIP, he is a Director, which
makes him a potentially valuable target for attackers.
Given these factors, especially the successful execution of a suspicious PowerShell command
and the target being a Director, I believe this alert should be escalated to critical
severity.
```

Auto Investigation: What is normal?

Trellix Wise understands what tools are normal and if they are being used suspiciously.

```
After analyzing the provided information, here is my assessment:
Explanation:
1. User profile: David Squiller is a Director in the Sales department, not a support account
or super user. His role doesn't typically involve running PowerShell scripts or executing
potentially malicious files.
2. IP profile: No specific IP address is provided for analysis.
3. Standard tools: The command executed is not a standard tool. It's a PowerShell command that
downloads and executes a script from a GitHub repository, which is highly suspicious.
4. Story in the data: The most plausible story is malicious activity. A file named
"19625_cutepuppyjpg.exe" (likely masquerading as an image) executed a command to run
PowerShell with bypassed execution policy, downloading and executing a script from GitHub.
This is a common technique used by attackers.
5. Evidence of success: The alert indicates the process was successfully created, suggesting
the malicious activity was likely successful in its initial stages.
6. Importance of target: While David Squiller is not marked as a VIP, he is a Director, which
makes him a potentially valuable target for attackers.
Given these factors, especially the successful execution of a suspicious PowerShell command
and the target being a Director, I believe this alert should be escalated to critical
severity.
```

Auto Investigation: What happened?

Trellix Wise creates a complete story based on all of the evidence.

```
After analyzing the provided information, here is my assessment:
Explanation:
1. User profile: David Squiller is a Director in the Sales department, not a support account
or super user. His role doesn't typically involve running PowerShell scripts or executing
potentially malicious files.
2. IP profile: No specific IP address is provided for analysis.
3. Standard tools: The command executed is not a standard tool. It's a PowerShell command that
downloads and executes a script from a GitHub repository, which is highly suspicious.
4. Story in the data: The most plausible story is malicious activity. A file named
"19625_cutepuppyjpg.exe" (likely masquerading as an image) executed a command to run
PowerShell with bypassed execution policy, downloading and executing a script from GitHub.
This is a common technique used by attackers.
5. Evidence of success: The alert indicates the process was successfully created, suggesting
the malicious activity was likely successful in its initial stages.
6. Importance of target: While David Squiller is not marked as a VIP, he is a Director, which
makes him a potentially valuable target for attackers.
Given these factors, especially the successful execution of a suspicious PowerShell command
and the target being a Director, I believe this alert should be escalated to critical
severity.
```

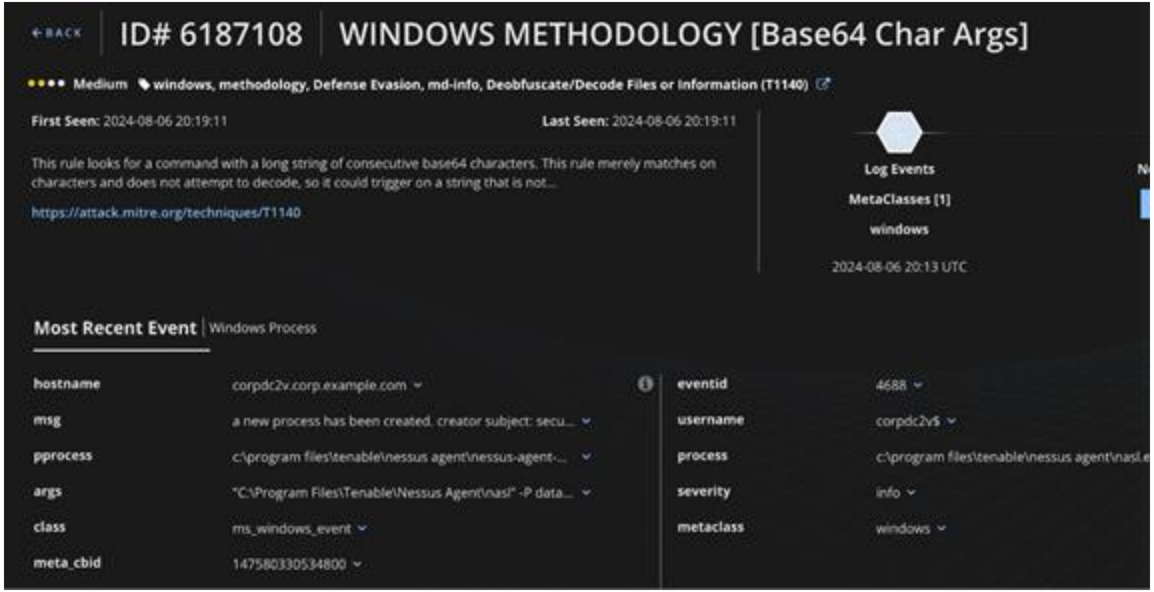
Auto Investigation: Do we care?

Trellix Wise considers everything and makes a decision.

```
After analyzing the provided information, here is my assessment:
Explanation:
1. User profile: David Squiller is a Director in the Sales department, not a support account
or super user. His role doesn't typically involve running PowerShell scripts or executing
potentially malicious files.
2. IP profile: No specific IP address is provided for analysis.
3. Standard tools: The command executed is not a standard tool. It's a PowerShell command that
downloads and executes a script from a GitHub repository, which is highly suspicious.
4. Story in the data: The most plausible story is malicious activity. A file named
"19625_cutepuppyjpg.exe" (likely masquerading as an image) executed a command to run
PowerShell with bypassed execution policy, downloading and executing a script from GitHub.
This is a common technique used by attackers.
5. Evidence of success: The alert indicates the process was successfully created, suggesting
the malicious activity was likely successful in its initial stages.
6. Importance of target: While David Squiller is not marked as a VIP, he is a Director, which
makes him a potentially valuable target for attackers.
Given these factors, especially the successful execution of a suspicious PowerShell command
and the target being a Director, I believe this alert should be escalated to critical
severity.
```

Deprioritizing Noisy Alerts

Trellix Wise declines to escalate this alert using a transparent decision making process.



ID# 6187108 WINDOWS METHODOLOGY [Base64 Char Args]

●●●● Medium windows, methodology, Defense Evasion, md-info, Deobfuscate/Decode Files or Information (T1140)

First Seen: 2024-08-06 20:19:11 Last Seen: 2024-08-06 20:19:11

This rule looks for a command with a long string of consecutive base64 characters. This rule merely matches on characters and does not attempt to decode, so it could trigger on a string that is not...

https://attack.mitre.org/techniques/T1140

Log Events
MetaClasses [1]
windows
2024-08-06 20:13 UTC

Most Recent Event | Windows Process

hostname	corpdc2v.corp.example.com	eventid	4688
msg	a new process has been created. creator subject: secu...	username	corpdc2v$
pprocess	c:\program files\tenable\nessus agent\nessus-agent-...	process	c:\program files\tenable\nessus agent\nasl.e
args	"C:\Program Files\Tenable\Nessus Agent\nasl" -P data...	severity	info
class	ms_windows_event	metaclass	windows
meta_cbid	147580330534800		

Trellix Wise is evaluating every alert to ensure it's ***not*** important.

But this only works if you can audit what it's doing.

It shows its work, walking you through its decision making process, step by step.

Trellix Wise fully understands the situation

It knows why the alert was triggered and what it was looking for.

Decision:

The alert was likely triggered due to the presence of a long base64 encoded string in the command line arguments of the Nessus Agent. However, this is expected behavior for this security scanning tool. The base64 string contains metadata about the system, including OS version, IP addresses, and Nessus plugin information.

Other rules that fired (like "powershell methodology [base64 string]" and "windows methodology [base64 char args]") are likely false positives triggered by the legitimate use of base64 encoding by the Nessus Agent.

Given that this appears to be normal activity from an authorized security tool, and there's no evidence of malicious intent or compromise, raising the severity to critical is not warranted. The current medium severity is appropriate, as it allows for investigation without causing undue alarm.

Trellix Wise fully understands the situation

It knows what behavior is expected in an enterprise environment.

Decision:

The alert was likely triggered due to the presence of a long base64 encoded string in the command line arguments of the Nessus Agent. However, this is expected behavior for this security scanning tool. The base64 string contains metadata about the system, including OS version, IP addresses, and Nessus plugin information.

Other rules that fired (like "powershell methodology [base64 string]" and "windows methodology [base64 char args]") are likely false positives triggered by the legitimate use of base64 encoding by the Nessus Agent.

Given that this appears to be normal activity from an authorized security tool, and there's no evidence of malicious intent or compromise, raising the severity to critical is not warranted. The current medium severity is appropriate, as it allows for investigation without causing undue alarm.

Trellix Wise fully understands the situation

It automatically decodes the base64 string and uses that in its decision.

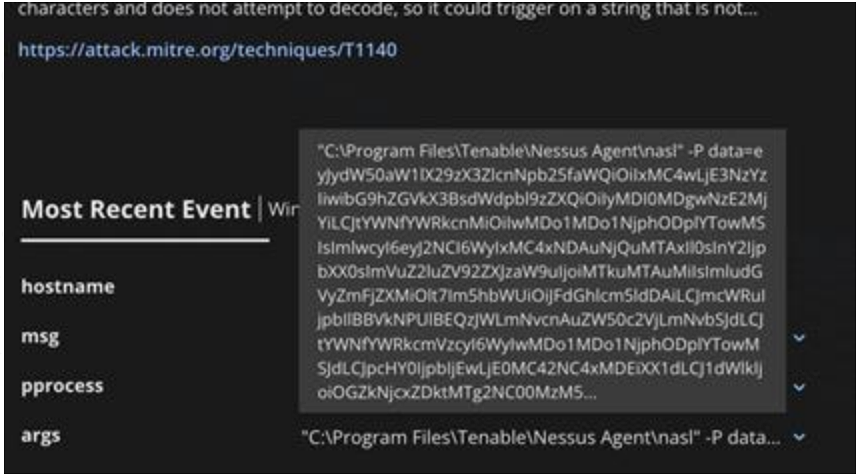
This is the moment where gen AI goes beyond what a human can do:

Decision:

The alert was likely triggered due to the presence of a long base64 encoded string in the command line arguments of the Nessus Agent. However, this is expected behavior for this security scanning tool. The base64 string contains metadata about the system, including OS version, IP addresses, and Nessus plugin information.

Other rules that fired (like "powersh
"windows methodology [base64 char args
triggered by the legitimate use of bas

Given that this appears to be normal
tool, and there's no evidence of malic
severity to critical is not warranted.
appropriate, as it allows for investig



characters and does not attempt to decode, so it could trigger on a string that is not...

https://attack.mitre.org/techniques/T1140

Most Recent Event | Wir

hostname

msg

pprocess

args: "C:\Program Files\Tenable\Nessus Agent\nasl" -P data...

```
"C:\Program Files\Tenable\Nessus Agent\nasl" -P data=e
yJydW50aW1lX29zX3ZlcnNpb25faWQiOilxMC4wLjE3NzYz
IiwibG9hZGVkX3BsdWdpbl9zZXQiOilyMDI0MDgwNzE2Mj
YiLCJtYWNfYWRkcnMiOilwMDo1MDo1NjphODplYTowMS
IsImlwcyI6eyJ2NCI6WyIxMC4xNDAuNjQuMTAxIl0sInY2Ijp
bXX0sImVuZ2luZV92ZXJzaW9uIjoiMTkuMTAuMiIsImludG
VyZmFjZXMiOlt7Im5hbWUiOiJFdGhlcm5ldDAiLCJmcWRuI
jpbIlBBVkNPUlBEQzJWLmNvcnAuZW50c2VjLmNvbSJdLCJ
tYWNfYWRkcmVzcyI6WyIwMDo1MDo1NjphODplYTowM
SJdLCJpcHY0IjpbIjEwLjE0MC42NC4xMDEiXX1dLCJ1dWlkIj
oiOGZkNjcxZDktMTg2NC00MzM5...
```

Trellix

Trellix Wise fully understands the situation

It puts this alert in the context of the other alerts for this host and realizes they are also false positives.

Decision:

The alert was likely triggered due to the presence of a long base64 encoded string in the command line arguments of the Nessus Agent. However, this is expected behavior for this security scanning tool. The base64 string contains metadata about the system, including OS version, IP addresses, and Nessus plugin information.

Other rules that fired (like "powershell methodology [base64 string]" and "windows methodology [base64 char args]") are likely false positives triggered by the legitimate use of base64 encoding by the Nessus Agent.

Given that this appears to be normal activity from an authorized security tool, and there's no evidence of malicious intent or compromise, raising the severity to critical is not warranted. The current medium severity is appropriate, as it allows for investigation without causing undue alarm.

Trellix Wise fully understands the situation

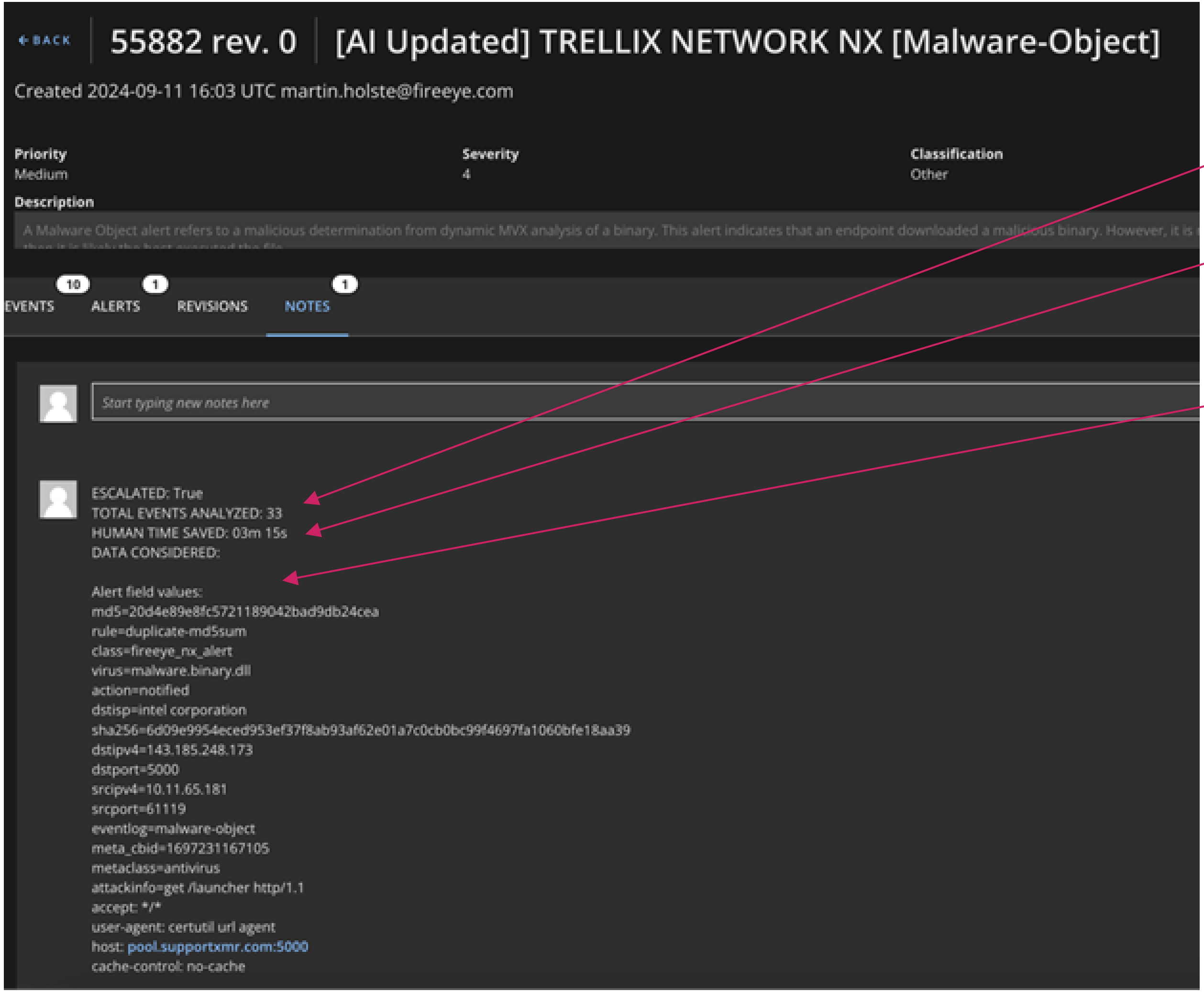
It knows what is worth investigating and what is not.

Decision:

The alert was likely triggered due to the presence of a long base64 encoded string in the command line arguments of the Nessus Agent. However, this is expected behavior for this security scanning tool. The base64 string contains metadata about the system, including OS version, IP addresses, and Nessus plugin information.

Other rules that fired (like "powershell methodology [base64 string]" and "windows methodology [base64 char args]") are likely false positives triggered by the legitimate use of base64 encoding by the Nessus Agent.

Given that this appears to be normal activity from an authorized security tool, and there's no evidence of malicious intent or compromise, raising the severity to critical is not warranted. The current medium severity is appropriate, as it allows for investigation without causing undue alarm.



55882 rev. 0 [AI Updated] TRELLIX NETWORK NX [Malware-Object]

Created 2024-09-11 16:03 UTC martin.holste@fireeye.com

Priority	Severity	Classification
Medium	4	Other

Description

A Malware Object alert refers to a malicious determination from dynamic MVX analysis of a binary. This alert indicates that an endpoint downloaded a malicious binary. However, it is

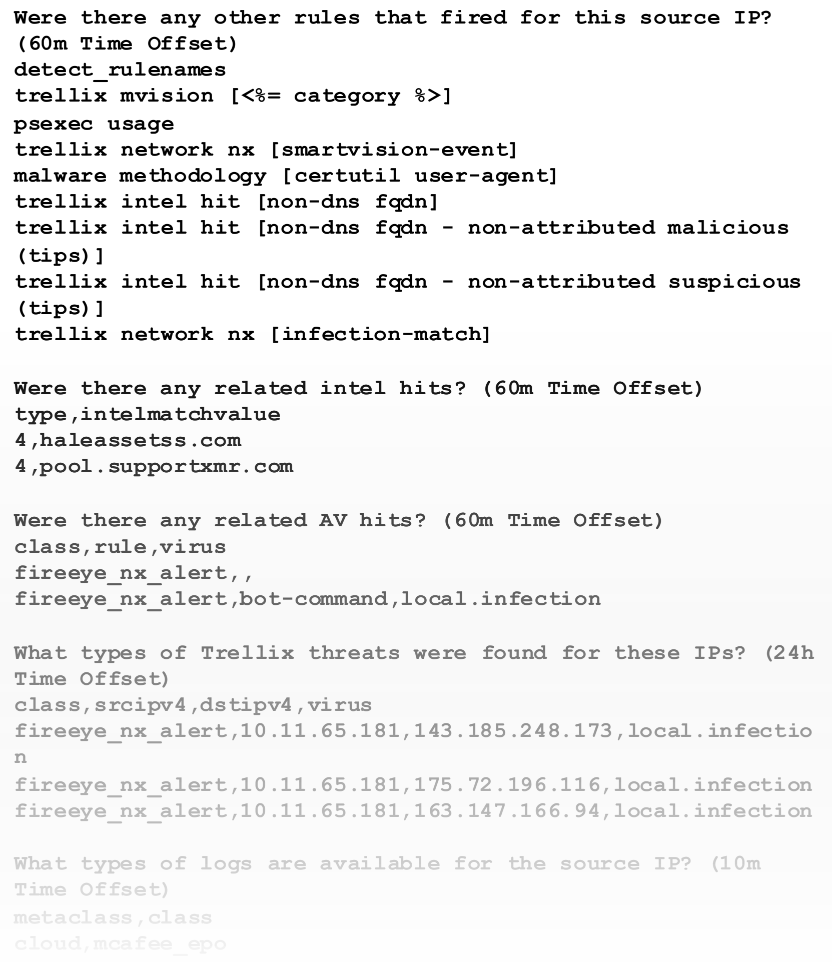
then it is likely the host executed the file

```
ESCALATED: True
TOTAL EVENTS ANALYZED: 33
HUMAN TIME SAVED: 03m 15s
DATA CONSIDERED:

Alert field values:
md5=20d4e89e8fc5721189042bad9db24cea
rule=duplicate-md5sum
class=fireeye_nx_alert
virus=malware.binary.dll
action=notified
dstisp=intel corporation
sha256=6d09e9954eced953ef37f8ab93af62e01a7c0cb0bc99f4697fa1060bfe18aa39
dstipv4=143.185.248.173
dstport=5000
srcipv4=10.11.65.181
srcport=61119
eventlog=malware-object
meta_cbid=1697231167105
metaclass=antivirus
attackinfo=get /launcher http/1.1
accept: */*
user-agent: certutil url agent
host: pool.supportxmr.com:5000
cache-control: no-cache
```

NX Auto Triage Example:

- **Complete**
  Analyzed 33 events
- **Valuable**
  Saved over 3 minutes of analyst time
- **Transparent**
  Provides data considered so analyst can audit the decision



```
Were there any other rules that fired for this source IP?
(60m Time Offset)
detect_rulenames
trellix mvision [<%= category %>]
psexec usage
trellix network nx [smartvision-event]
malware methodology [certutil user-agent]
trellix intel hit [non-dns fqdn]
trellix intel hit [non-dns fqdn - non-attributed malicious
(tips)]
trellix intel hit [non-dns fqdn - non-attributed suspicious
(tips)]
trellix network nx [infection-match]

Were there any related intel hits? (60m Time Offset)
type,intelmatchvalue
4,haleassetss.com
4,pool.supportxmr.com

Were there any related AV hits? (60m Time Offset)
class,rule,virus
fireeye_nx_alert,,
fireeye_nx_alert,bot-command,local.infection

What types of Trellix threats were found for these IPs? (24h
Time Offset)
class,srcipv4,dstipv4,virus
fireeye_nx_alert,10.11.65.181,143.185.248.173,local.infectio
n
fireeye_nx_alert,10.11.65.181,175.72.196.116,local.infection
fireeye_nx_alert,10.11.65.181,163.147.166.94,local.infection

What types of logs are available for the source IP? (10m
Time Offset)
metaclass,class
cloud,mcafee_epo
```

Data considered contains all of the questions and answers asked of the data:

- What other rules fired for this IP?
- Were there any intel hits?
- AV hits?
- What types of threats were found for these IP's?
- What types are logs are available for these IP's?
- Etc.

Human analyst has transparent view into all data the AI considered when making its decision.

Complete, correct analysis of the NX alert with decision to escalate:

1. User profile:
The username "demo.user" is mentioned, which suggests **this may be a test or demo account rather than a regular user.** There's no indication of it being a support or super user account.

2. IP address profile:
The source IP 10.11.65.181 is **an internal IP address.** It appears in multiple logs, suggesting it could be used by multiple users or be a **shared resource.**

3. Standard tools consideration:
The alert mentions "certutil url agent" in the user-agent string. **Certutil is a legitimate Windows tool, but its use to download files can be abused by attackers.** This usage is suspicious in this context.

4. Story from the data:
The data strongly suggests malicious activity:

- A malware object (meterpreter.dll) was downloaded
- Connection to a known malicious domain (pool.supportxmr.com)
- Multiple related alerts and intel hits for bot activity and infections
- **Use of certutil to download the malware**

5. Evidence of success:
While the initial alert states it's unknown if the file was executed, there are multiple subsequent alerts for "local.infection" associated with this IP, suggesting **the malware was likely executed successfully.**

6. Importance of target and success likelihood:
The target appears to be an internal system (based on the IP), and there's strong evidence of successful infection across multiple destinations.

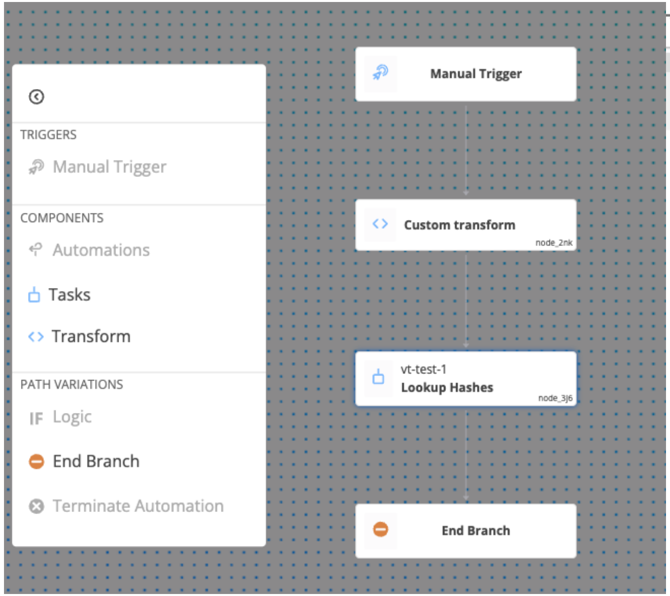
Given this analysis, I believe **this alert should be raised to critical severity.** The **evidence points to a successful malware infection** that has spread to multiple systems, indicating an active and potentially severe security incident.

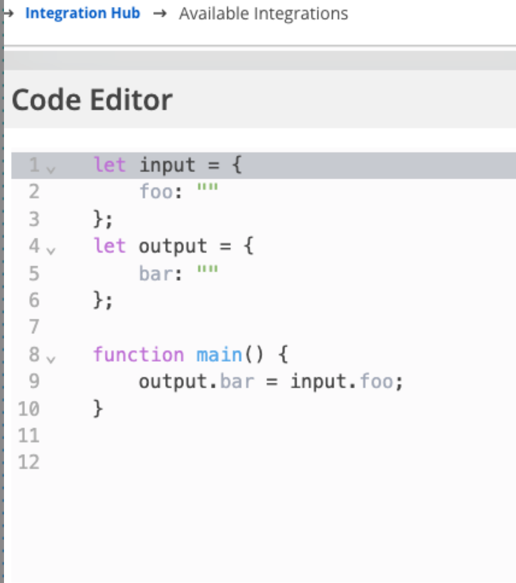
Response tools

- Tasks
- Triggers
- Transformations
- Automations

Tasks and Automations

- Tasks are granular actions to enrich, analyze, and respond, including both out-of-box Trellix and those that result from 3rd party integrations.
- Automations enable you to link multiple tasks together with robust logic.



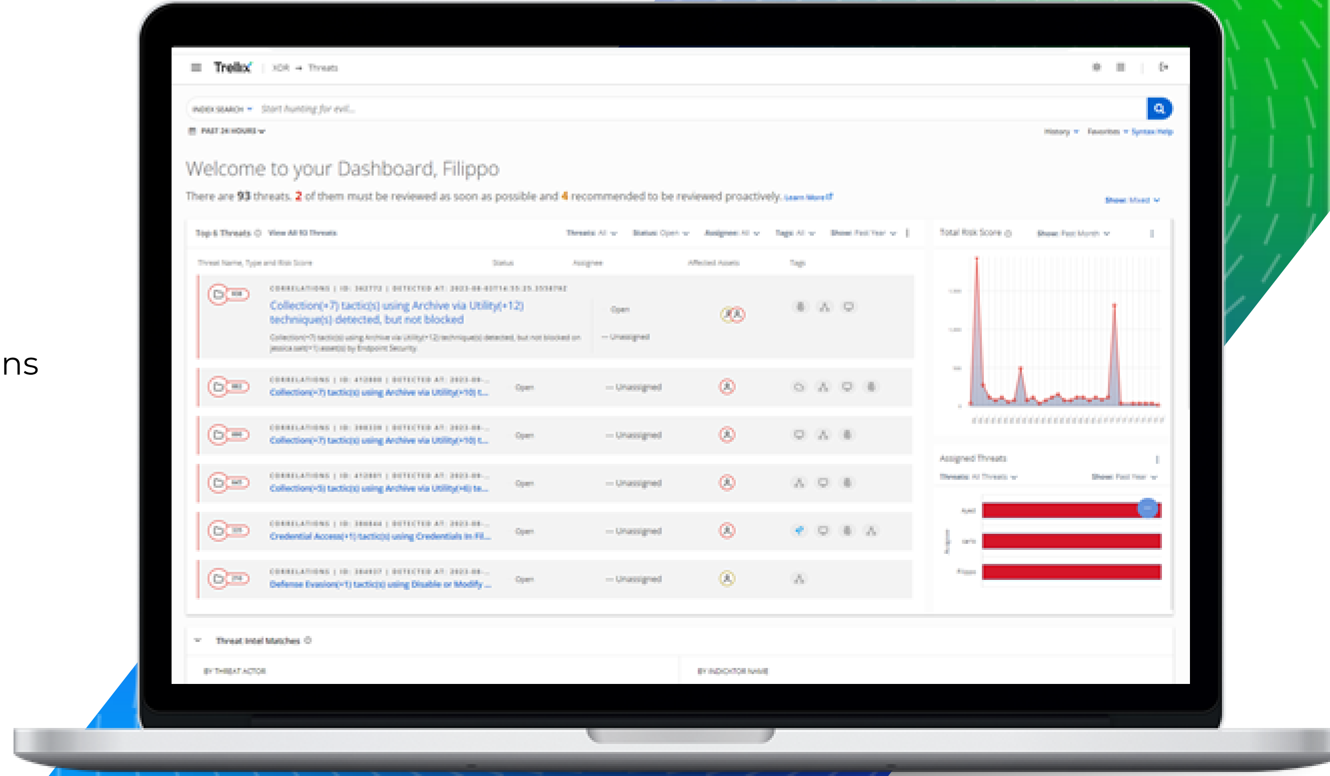


```
let input = {
    foo: ""
};
let output = {
    bar: ""
};

function main() {
    output.bar = input.foo;
}
```

Demo - Checkpoints

- Integration Hub
- Search and TQL
- Assets
- Risk Score
- Alert Rules
- Events, Alerts, Correlations
- Threat Intelligence
- Investigative Tips
- Tasks and Automations
- Case management
- Wise
- Reporting



Welcome to your Dashboard, Filippo

There are 93 threats. 2 of them must be reviewed as soon as possible and 4 recommended to be reviewed proactively. Learn More

Threat Name, Type and Risk Score	Status	Assignee	Affected Assets	Tags
CORRELATIONS | ID: [illegible] | DETECTED AT: 2023-08-[illegible] Collection(+7) tactic(s) using Archive via Utility(+12) technique(s) detected, but not blocked Collection(+7) tactic(s) using Archive via Utility(+12) technique(s) detected, but not blocked on [illegible] asset(s) by Endpoint Security	Open	— Unassigned		
CORRELATIONS | ID: [illegible] | DETECTED AT: 2023-08-... Collection(+7) tactic(s) using Archive via Utility(+10) t...	Open	— Unassigned		
CORRELATIONS | ID: [illegible] | DETECTED AT: 2023-08-... Collection(+7) tactic(s) using Archive via Utility(+10) t...	Open	— Unassigned		
CORRELATIONS | ID: [illegible] | DETECTED AT: 2023-08-... Collection(+5) tactic(s) using Archive via Utility(+6) te...	Open	— Unassigned		
CORRELATIONS | ID: [illegible] | DETECTED AT: 2023-08-... Credential Access(+1) tactic(s) using Credentials In Fil...	Open	— Unassigned		
CORRELATIONS | ID: [illegible] | DETECTED AT: 2023-08-... Defense Evasion(+1) tactic(s) using Disable or Modify ...	Open	— Unassigned		

Roadmap

Hands-on!!!

Search

PizzaHack APT uses FTP protocol

Let’s hunt!

- Port 21 connections
- External IPs
- Other suspicious ports
- Internal hosts involved

Entities

John Butter might be a target

Let’s hunt!

- Job profile
- Office location
- Risk score
- Relevant alerts

WinSCP usage found on the trace

Let’s hunt!

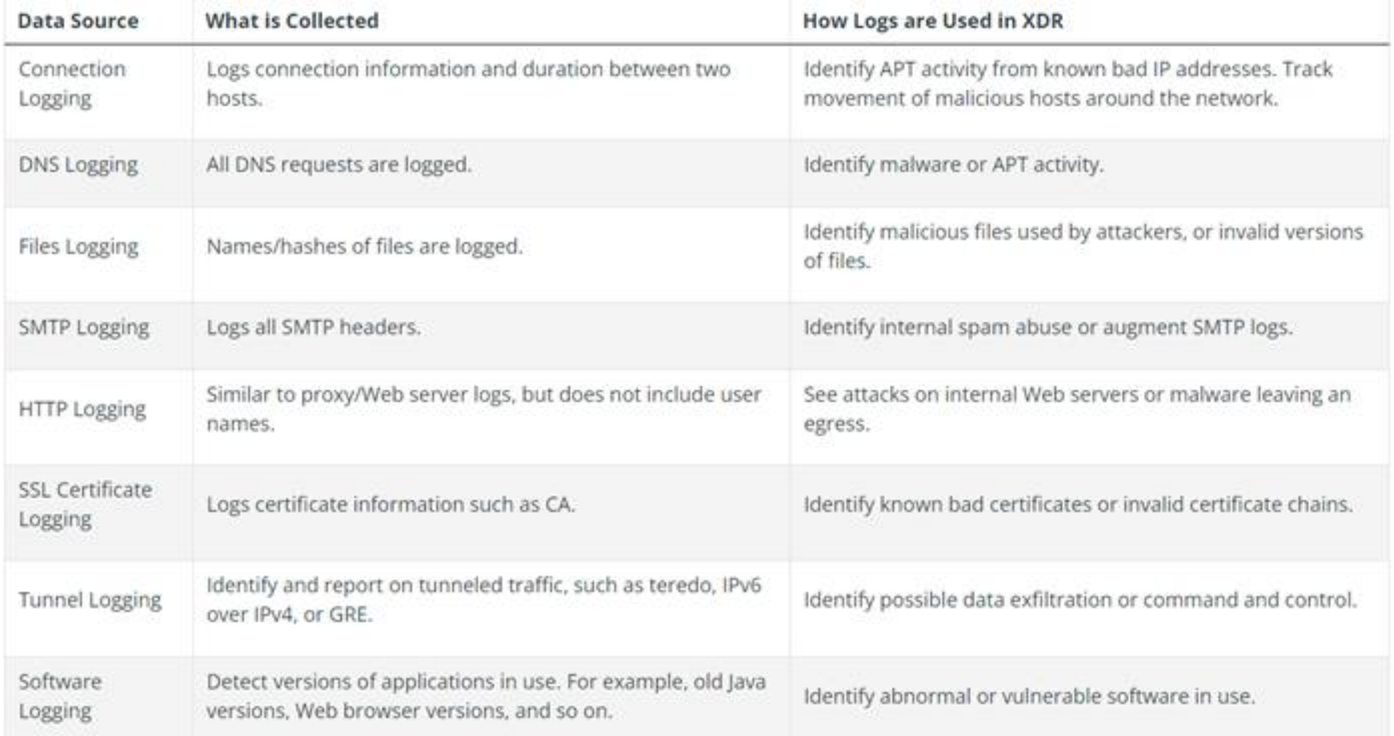
- Total events analyzed
- Human time saved
- Remediation recommendations

Pre-Sales Resources

POV Guideline

Data Sources for XDR

XDR effectiveness depends on the data sources available for analysis



Data Source	What is Collected	How Logs are Used in XDR
Connection Logging	Logs connection information and duration between two hosts.	Identify APT activity from known bad IP addresses. Track movement of malicious hosts around the network.
DNS Logging	All DNS requests are logged.	Identify malware or APT activity.
Files Logging	Names/hashes of files are logged.	Identify malicious files used by attackers, or invalid versions of files.
SMTP Logging	Logs all SMTP headers.	Identify internal spam abuse or augment SMTP logs.
HTTP Logging	Similar to proxy/Web server logs, but does not include user names.	See attacks on internal Web servers or malware leaving an egress.
SSL Certificate Logging	Logs certificate information such as CA.	Identify known bad certificates or invalid certificate chains.
Tunnel Logging	Identify and report on tunneled traffic, such as teredo, IPv6 over IPv4, or GRE.	Identify possible data exfiltration or command and control.
Software Logging	Detect versions of applications in use. For example, old Java versions, Web browser versions, and so on.	Identify abnormal or vulnerable software in use.

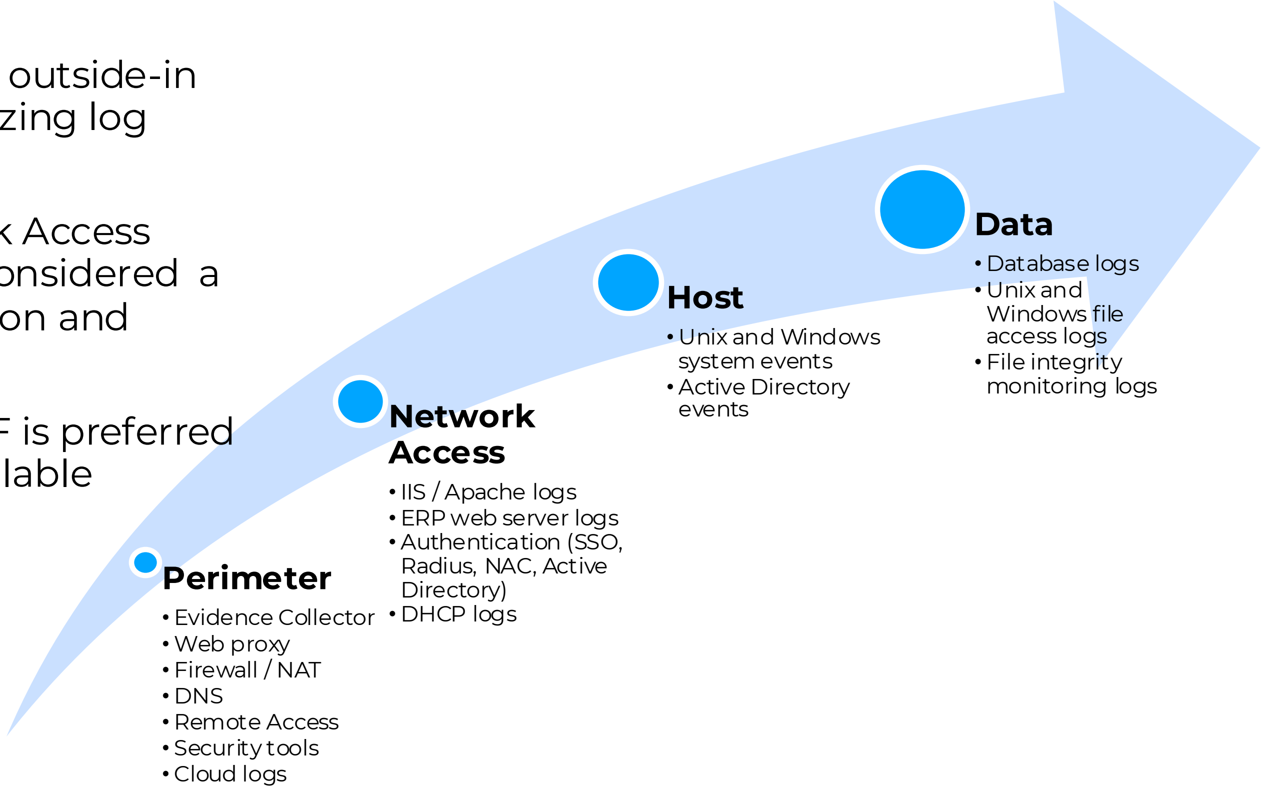
Critical Data Sources

A list of sources required to detect and respond to cyber attacks

- Threat Detection Appliances
- Web Proxy (with user tracking)
- DNS Resolution and Relay events
- Authentication Events
- AD/LDAP, Wireless, VPN, etc.
- Firewalls (including NAT logs)
- Email server and transactions
- Endpoint Security
- AV, HIPS, EDR, etc.
- DHCP Assignments
- Operating System events
- Windows, Linux, etc.
- Windows/Linux Process Tracking
- IDS / IPS
- Database Security/Audit events
- Email Filtering/Security events
- NAC events
- PowerShell logs
- Cloud Infrastructure

Data Sources by Priority

- Trellix recommends an outside-in approach when prioritizing log source collection
- Perimeter and Network Access categories should be considered a “must have” for detection and analytics efficacy
- Log Format – CEF/LEEF is preferred when the option is available



Perimeter

- Evidence Collector
- Web proxy
- Firewall / NAT
- DNS
- Remote Access
- Security tools
- Cloud logs

Network Access

- IIS / Apache logs
- ERP web server logs
- Authentication (SSO, Radius, NAC, Active Directory)
- DHCP logs

Host

- Unix and Windows system events
- Active Directory events

Data

- Database logs
- Unix and Windows file access logs
- File integrity monitoring logs

Trellix

Bandwidth calculation

Here are some rough calculations based on the Helix environment size.

(EPS * average message size * (1 - compression ratio)/ 1MB = megabytes/second transferred over WAN to the virtual private cloud.

Keep in mind that this is a worst-case calculation. The average message size we are using is 4 KB, but in practice this is closer to 2KB.

- **2,500 EPS** – (2500 * 4096 * (1 – 0.75))/ 1,048,576 = **2.4 MB/sec**
- **5,000 EPS** – (5000 *4096 * (1 – 0.75))/ 1,048,576 = **4.9 MB/sec**
- **10,000 EPS** - (10000 *4096 * (1 – 0.75))/ 1,048,576 = **9.8 MB/sec**
- **40,000 EPS** - (40000 *4096 * (1 – 0.75))/ 1,048,576 = **39.1 MB/sec**

EPS Calculations

- Be mindful of what the customer plans on sending to XDR. Our goal is to help the customer find evil, not become their ***digital attic***.

- Ensure that the log sources are those where we have good rules and analytics coverage and aren't simply going to fill up their EPS limit without benefit.

- Ensure that there isn't event duplication: for example, we don't need both network metadata from Evidence Collector or a Commbroker and their DNS logs, as the network devices already see those.

- If possible, use metrics from existing SIEM.

- If the customer cannot provide a clear EPS number, then guidance is as follows:
- **1 EPS per user.**
  - Beware of edge cases where this does not hold true. Publicly facing web servers, where event generation is going to be far higher than the customer's user counts.

Trellix