23-26 OCTOBER 2023

Trellix EMEA Partner Tech Summit 2023

Rome, Italy

XDR

Filippo Sitzia
Sr. Solutions Architect

November 10, 2023

Trellix

Agenda

- Product Line Pitching
- Demonstration Guidance
- Pre-Sales Resources

Product Line Pitching

Trellix

Today's SOC challenges

	Siloed tools that don't work together	Limited org resources and expertise	Too many alerts and missed threats
Today	Weeks	Stretched, under-resourced	Inability to determine, prioritize top threats

Result: Organizational risk increases

What is XDR?

“XDR…integrates, correlates, and contextualizes data and alerts from multiple security prevention, detection, and response components”

– Gartner

X D R

Extended Detection Response

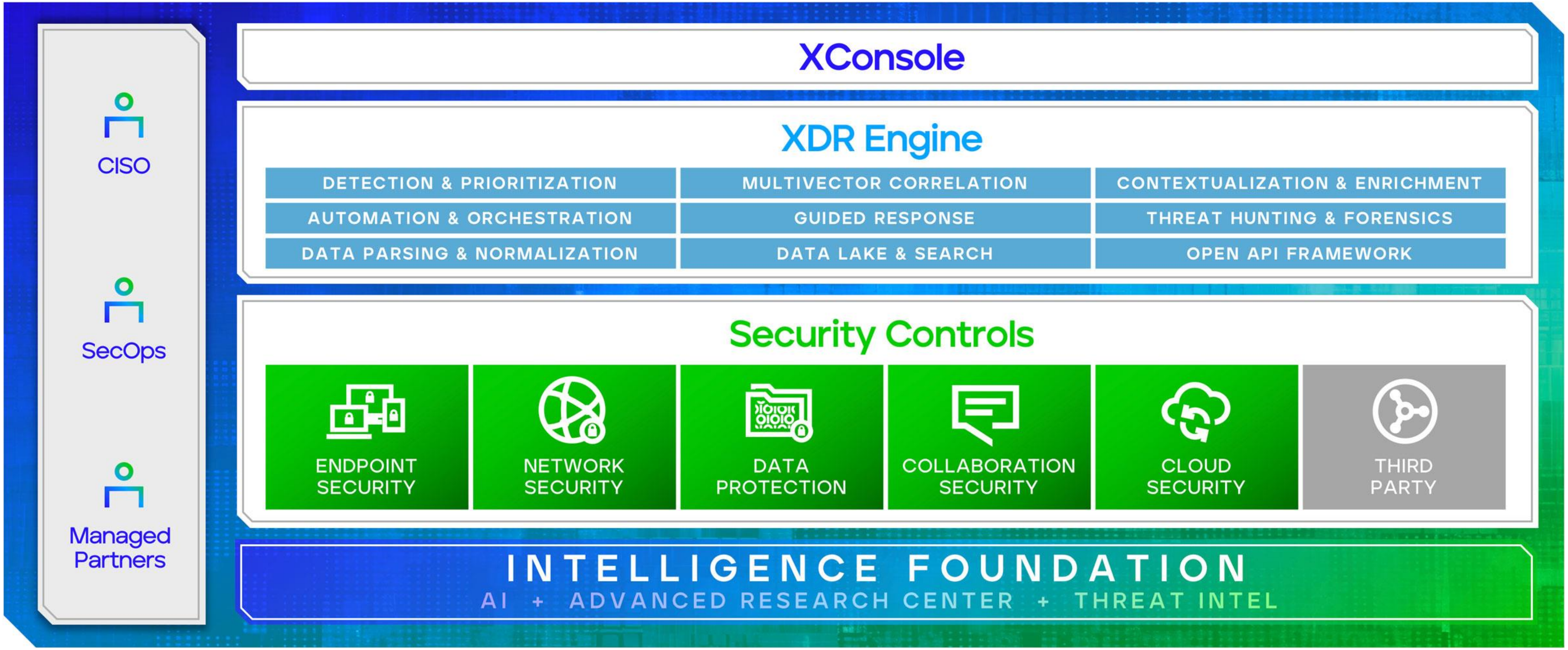
Trellix XDR Impact

	Time to Resolution	SOC Resources	Threat Coverage
Before	Days - Weeks	Stretched, under-resourced	Inability to determine, prioritize top threats
After	Hours - Minutes	Effective, efficient, optimized	Ability to determine, prioritize top threats

Result: A simplified and insightful security operations experience to rapidly stop attacks

Trellix

Trellix XDR Impact



CISO

SecOps

Managed Partners

XConsole

XDR Engine

DETECTION & PRIORITIZATION	MULTIVECTOR CORRELATION	CONTEXTUALIZATION & ENRICHMENT
AUTOMATION & ORCHESTRATION	GUIDED RESPONSE	THREAT HUNTING & FORENSICS
DATA PARSING & NORMALIZATION	DATA LAKE & SEARCH	OPEN API FRAMEWORK

Security Controls

- ENDPOINT SECURITY
- NETWORK SECURITY
- DATA PROTECTION
- COLLABORATION SECURITY
- CLOUD SECURITY
- THIRD PARTY

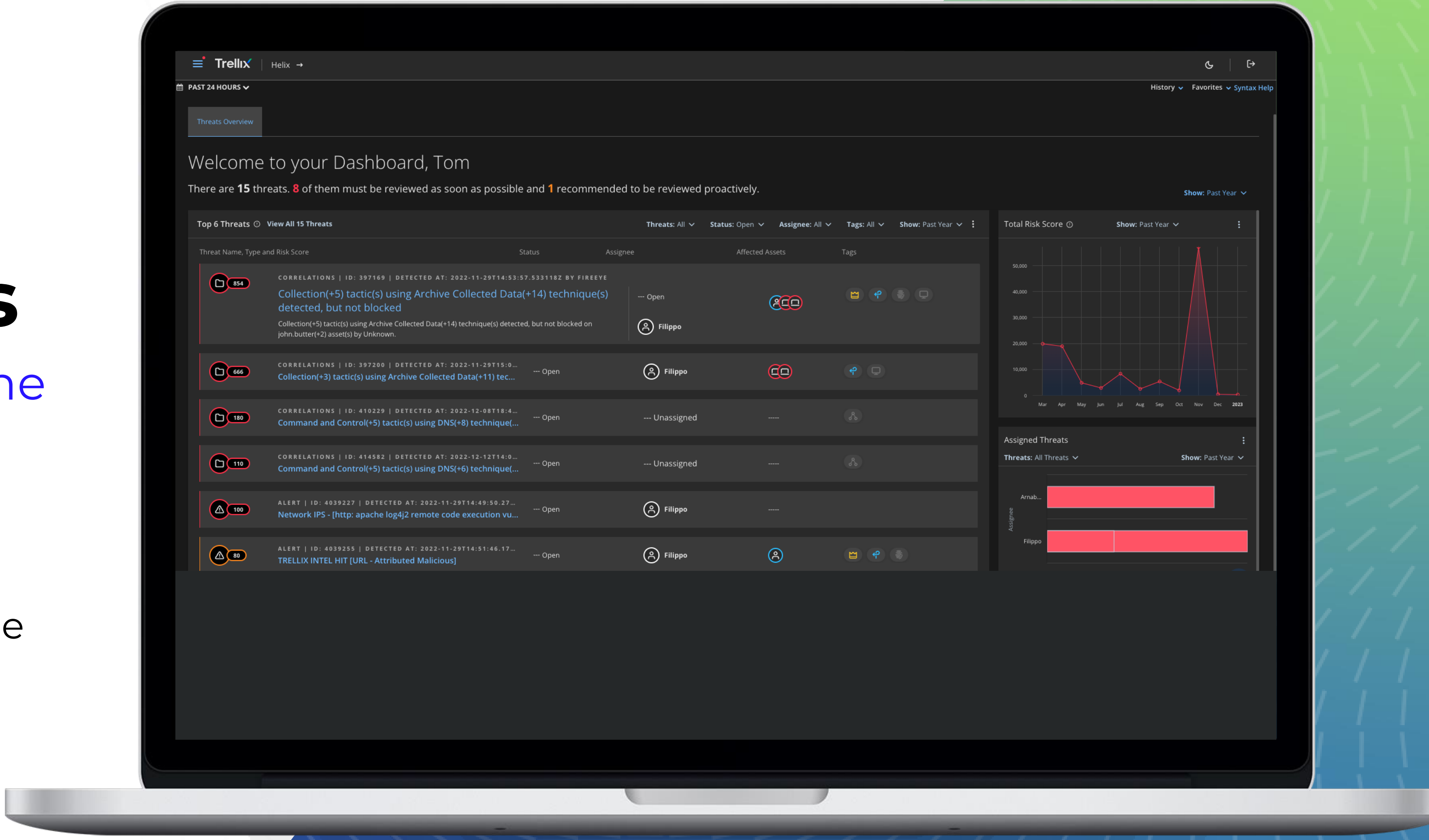
INTELLIGENCE FOUNDATION

AI + ADVANCED RESEARCH CENTER + THREAT INTEL

Detection effectiveness-prioritized alerts / threats

Surface and focus on the most critical alerts

- Layered machine learning detection intercepts multiple points in the kill chain
- Stack ranking of priority alerts
- Quick drill down on details



Welcome to your Dashboard, Tom

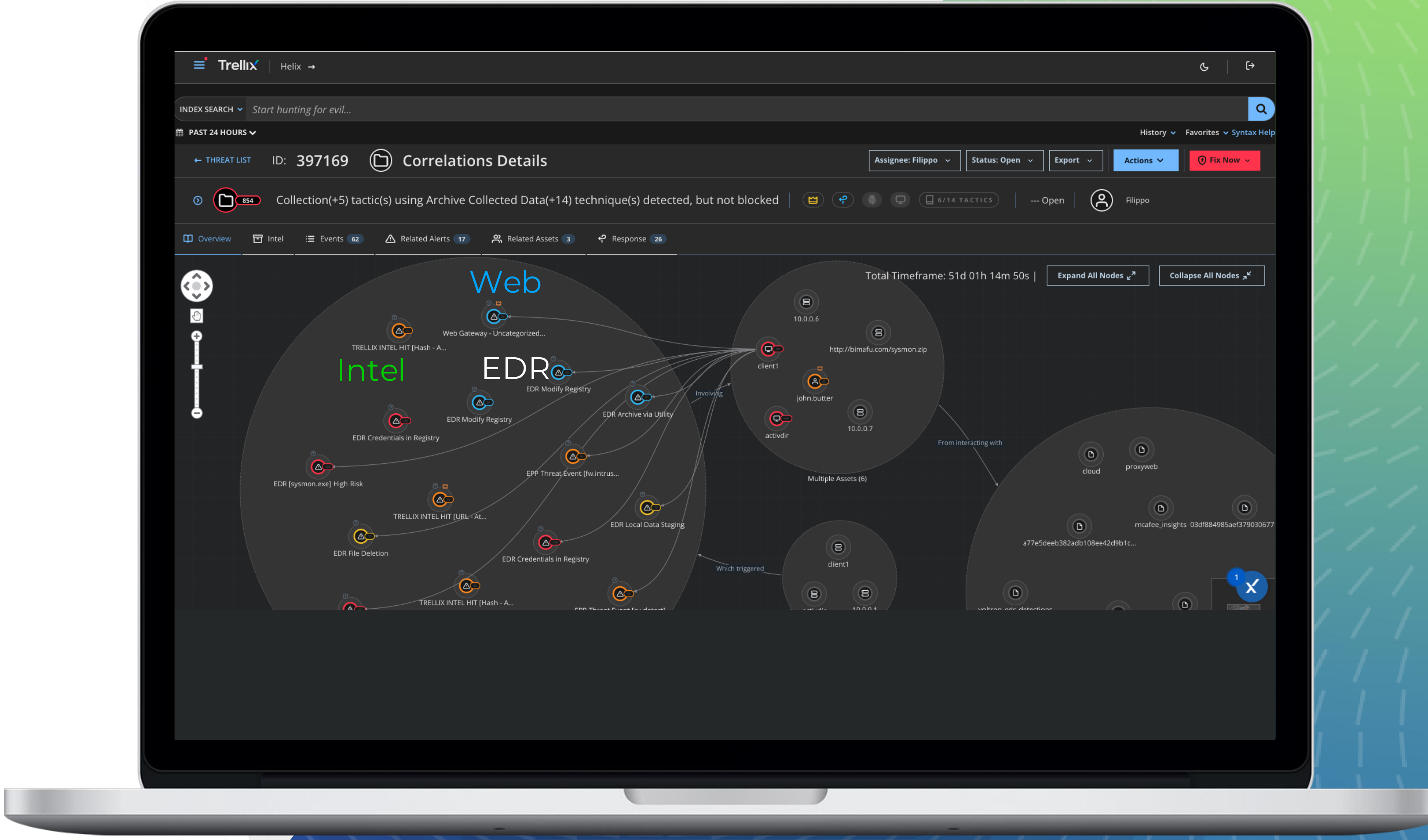
There are **15** threats. **8** of them must be reviewed as soon as possible and **1** recommended to be reviewed proactively.

Threat Name, Type and Risk Score	Status	Assignee	Affected Assets	Tags
854 CORRELATIONS | ID: 397169 | DETECTED AT: 2022-11-29T14:53:57.533118Z BY FIREEYE Collection(+5) tactic(s) using Archive Collected Data(+14) technique(s) detected, but not blocked Collection(+5) tactic(s) using Archive Collected Data(+14) technique(s) detected, but not blocked on john.butter(+2) asset(s) by Unknown.	--- Open	Filippo		
666 CORRELATIONS | ID: 397200 | DETECTED AT: 2022-11-29T15:0... Collection(+3) tactic(s) using Archive Collected Data(+11) tec...	--- Open	Filippo		
180 CORRELATIONS | ID: 410229 | DETECTED AT: 2022-12-08T18:4... Command and Control(+5) tactic(s) using DNS(+8) technique(...	--- Open	--- Unassigned	-----	
110 CORRELATIONS | ID: 414582 | DETECTED AT: 2022-12-12T14:0... Command and Control(+5) tactic(s) using DNS(+6) technique(...	--- Open	--- Unassigned	-----	
100 ALERT | ID: 4039227 | DETECTED AT: 2022-11-29T14:49:50.27... Network IPS - [http: apache log4j2 remote code execution vu...	--- Open	Filippo	-----	
80 ALERT | ID: 4039255 | DETECTED AT: 2022-11-29T14:51:46.17... TRELLIX INTEL HIT [URL - Attributed Malicious]	--- Open	Filippo		

Correlations across multiple data sources

View the entire threat story across environments

- Cross-correlations with web, endpoint and intelligence
- Easily view related alerts and assets
- Zoom in and out on the storyboard



THREAT LIST ID: 397169 Correlations Details

Assignee: Filippo Status: Open

Collection(+5) tactic(s) using Archive Collected Data(+14) technique(s) detected, but not blocked

6/14 TACTICS --- Open Filippo

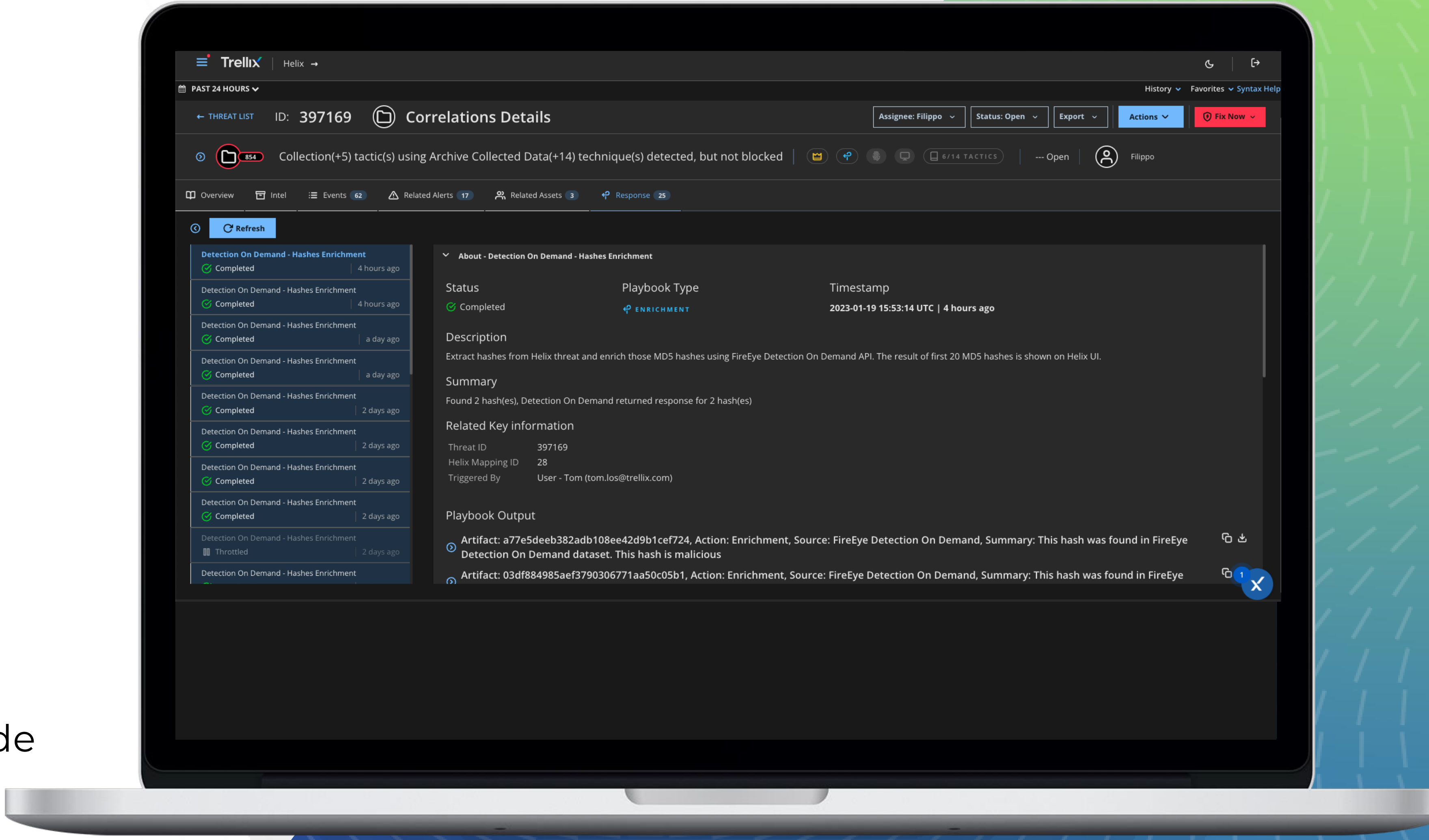
Total Timeframe: 51d 01h 14m 50s |

Trellix

Automate attack mitigation & prevention

Streamline threat mitigation and prevention

- Range of playbooks from investigation enrichment to containment
- Embedded expertise to guide better decisions
- Status on tasks progress and completions



ID: 397169 Correlations Details

Collection(+5) tactic(s) using Archive Collected Data(+14) technique(s) detected, but not blocked

Detection On Demand - Hashes Enrichment
Completed | 4 hours ago

Detection On Demand - Hashes Enrichment
Completed | 4 hours ago

Detection On Demand - Hashes Enrichment
Completed | a day ago

Detection On Demand - Hashes Enrichment
Completed | a day ago

Detection On Demand - Hashes Enrichment
Completed | 2 days ago

Detection On Demand - Hashes Enrichment
Completed | 2 days ago

Detection On Demand - Hashes Enrichment
Completed | 2 days ago

Detection On Demand - Hashes Enrichment
Completed | 2 days ago

Detection On Demand - Hashes Enrichment
Throttled | 2 days ago

Detection On Demand - Hashes Enrichment

About - Detection On Demand - Hashes Enrichment

Status	Playbook Type	Timestamp
Completed	ENRICHMENT	2023-01-19 15:53:14 UTC | 4 hours ago

Description

Extract hashes from Helix threat and enrich those MD5 hashes using FireEye Detection On Demand API. The result of first 20 MD5 hashes is shown on Helix UI.

Summary

Found 2 hash(es), Detection On Demand returned response for 2 hash(es)

Related Key information

Threat ID	397169
Helix Mapping ID	28
Triggered By	User - Tom (tom.los@trellix.com)

Playbook Output

Artifact: a77e5deeb382adb108ee42d9b1cef724, Action: Enrichment, Source: FireEye Detection On Demand, Summary: This hash was found in FireEye Detection On Demand dataset. This hash is malicious

Artifact: 03df884985aef3790306771aa50c05b1, Action: Enrichment, Source: FireEye Detection On Demand, Summary: This hash was found in FireEye

Trellix

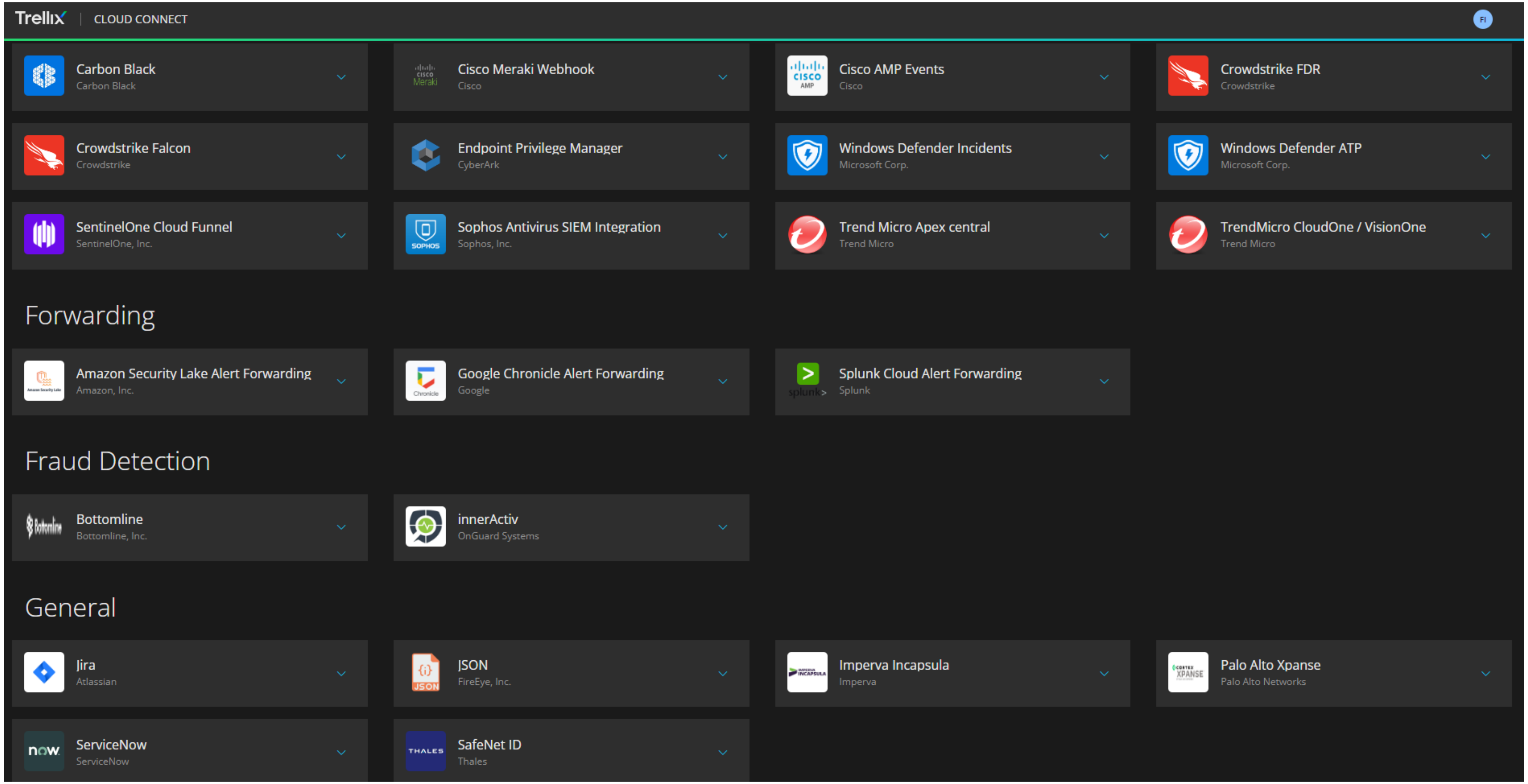
Demonstration Guidance (and Use cases)

Integrations

- Cloud Connect
- Communication Broker

Cloud Connect portal

XDR cloud connections allow events and logs from Trellix products and security products from other vendors to be sent to XDR through API connections.



Trellix | CLOUD CONNECT

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

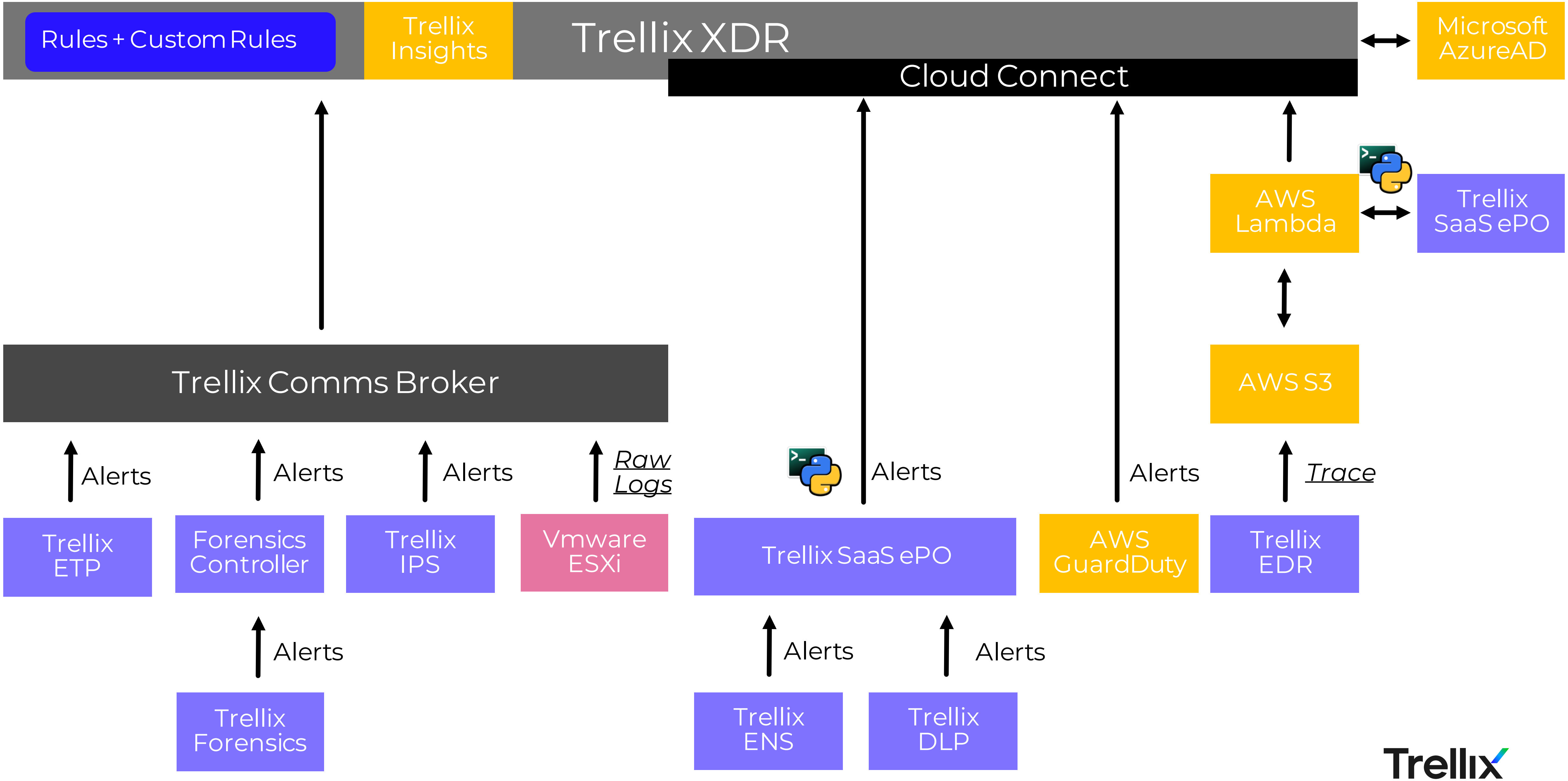
ServiceNow
ServiceNow

SafeNet ID
Thales

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.

Lab Mapping



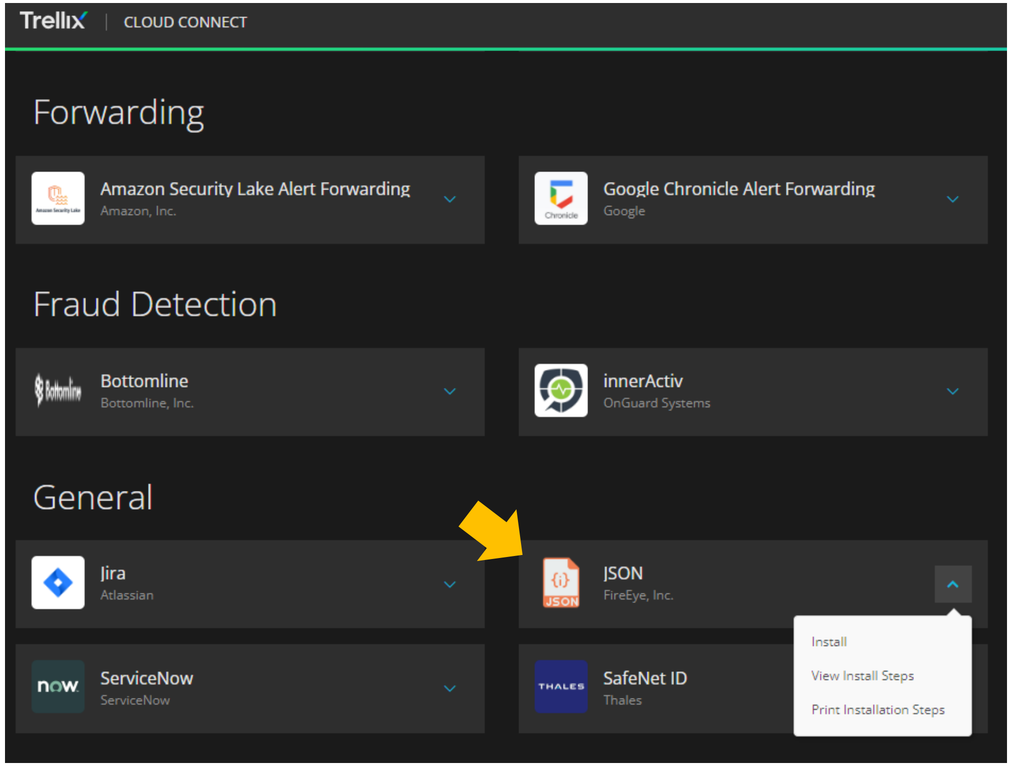
Rules + Custom Rules
Trellix Insights
Trellix XDR
Cloud Connect
Microsoft AzureAD
AWS Lambda
Trellix SaaS ePO
AWS S3
Trellix Comms Broker
Alerts
Alerts
Alerts
Raw Logs
Alerts
Alerts
Trace
Trellix ETP
Forensics Controller
Trellix IPS
Vmware ESXi
Trellix SaaS ePO
AWS GuardDuty
Trellix EDR
Alerts
Alerts
Alerts
Trellix Forensics
Trellix ENS
Trellix DLP

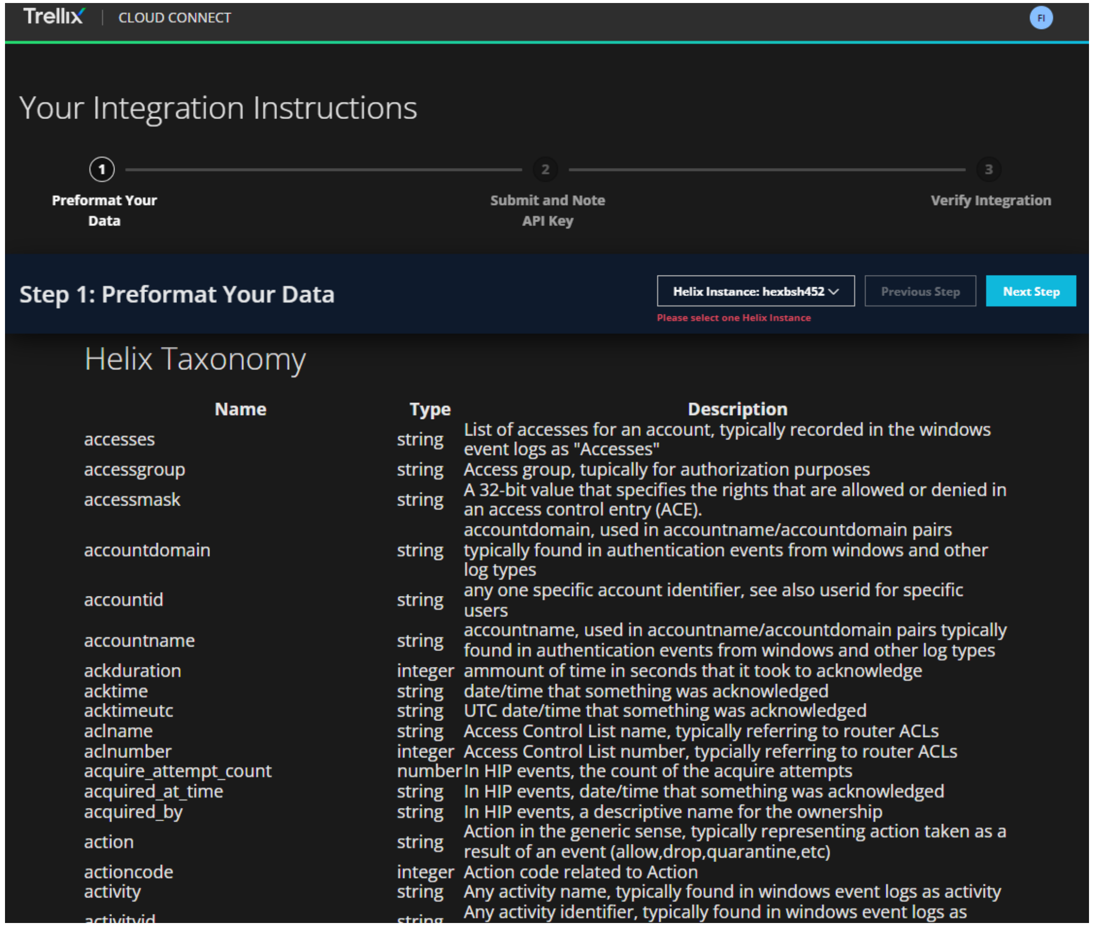
Events

- Taxonomy
- Parsers
- Alerts
- Distinguishers
- Correlations

Events - Taxonomy

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





Your Integration Instructions

Step 1: Preformat Your Data

Helix Taxonomy

Name	Type	Description
accesses	string	List of accesses for an account, typically recorded in the windows event logs as "Accesses"
accessgroup	string	Access group, tupically for authorization purposes
accessmask	string	A 32-bit value that specifies the rights that are allowed or denied in an access control entry (ACE).
accountdomain	string	accountdomain, used in accountname/accountdomain pairs typically found in authentication events from windows and other log types
accountid	string	any one specific account identifier, see also userid for specific users
accountname	string	accountname, used in accountname/accountdomain pairs typically found in authentication events from windows and other log types
ackduration	integer	ammount of time in seconds that it took to acknowledge
acktime	string	date/time that something was acknowledged
acktimeutc	string	UTC date/time that something was acknowledged
aclname	string	Access Control List name, typically referring to router ACLs
aclnumber	integer	Access Control List number, typcially referring to router ACLs
acquire_attempt_count	number	In HIP events, the count of the acquire attempts
acquired_at_time	string	In HIP events, date/time that something was acknowledged
acquired_by	string	In HIP events, a descriptive name for the ownership
action	string	Action in the generic sense, typically representing action taken as a result of an event (allow,drop,quarantine,etc)
actioncode	integer	Action code related to Action
activity	string	Any activity name, typically found in windows event logs as activity
activityid	string	Any activity identifier, typically found in windows event logs as

Events – 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
- md5 : 4373CF0D42926B15F95E35683D883A1C
- malwaretype : ransomware

Alert Rule class=myav malwaretype=ransomware

Alert Parameters [name= Ransomware Alert] [TAGS= T1204.002, T1486] [Distinguishers= md5]

Events

Generic AV log

Alert Rule

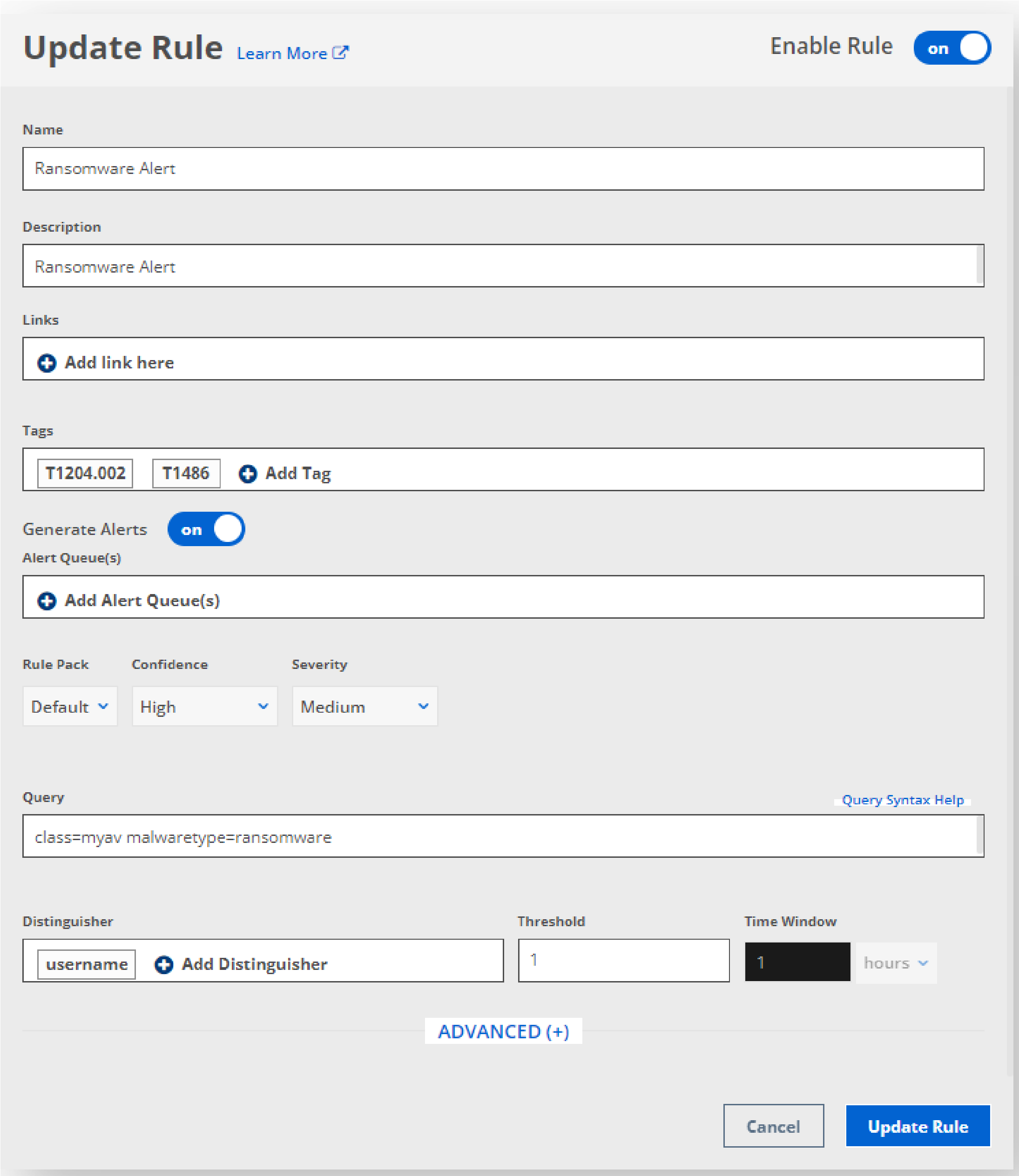
class=myav malwaretype=malware

Alert Parameters

[name= Ransomware Alert]

[TAGS= T1204.002, T1486]

[Distinguishers= username]



Update Rule

Enable Rule: on

Name: Ransomware Alert

Description: Ransomware Alert

Links:

Tags: T1204.002, T1486

Generate Alerts: on

Alert Queue(s):

Rule Pack: Default

Confidence: High

Severity: Medium

Query: class=myav malwaretype=ransomware

Distinguisher: username

Threshold: 1

Time Window: 1 hours

Events – Generic DLP Log

LOG {”violation” : ”credentialaccess”, ”victimaddress” : ”192.168.54.3”, ”user” : ”jessica.salt”}

Class mydlp

Parser {"violation":"policy", " victimaddress ":“hostname", "user":"username"}

PARSED_LOG

- hostname : client65
- policy : credentialaccess
- username : jessica.salt

Alert Rule class=mydlp policy=credentialaccess

Alert Parameters [name= Credential Access] [TAGS= TA0006] [Distinguishers= username]

Events

Generic DLP Log

Alert Rule

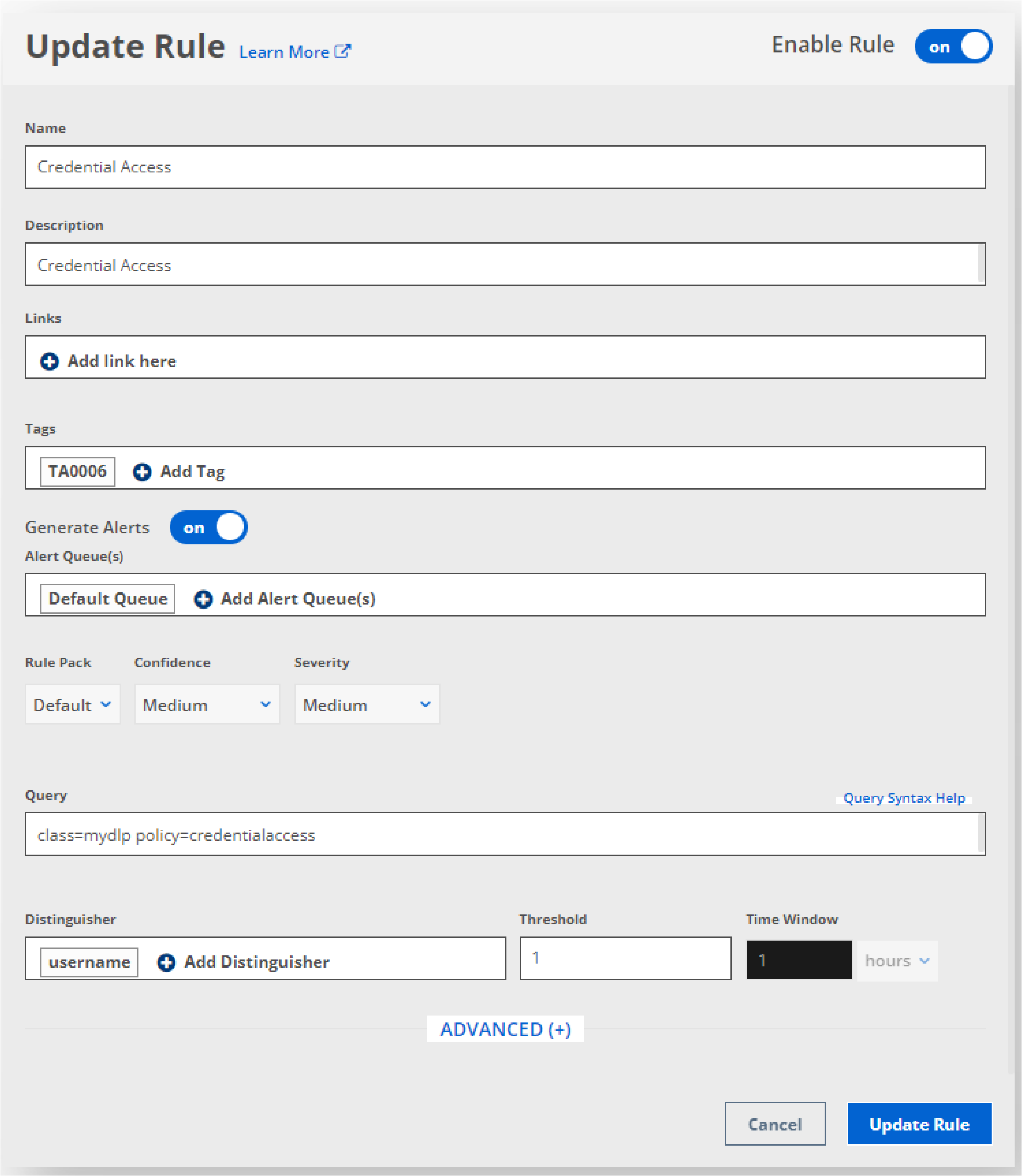
class=mydlp policy=credentialaccess

Alert Parameters

[name= Credential Access]

[TAGS= TA0006]

[Distinguishers= username]



Update Rule

Enable Rule on

Name: Credential Access

Description: Credential Access

Links

Tags: TA0006

Generate Alerts: on

Alert Queue(s): Default Queue

Rule Pack: Default

Confidence: Medium

Severity: Medium

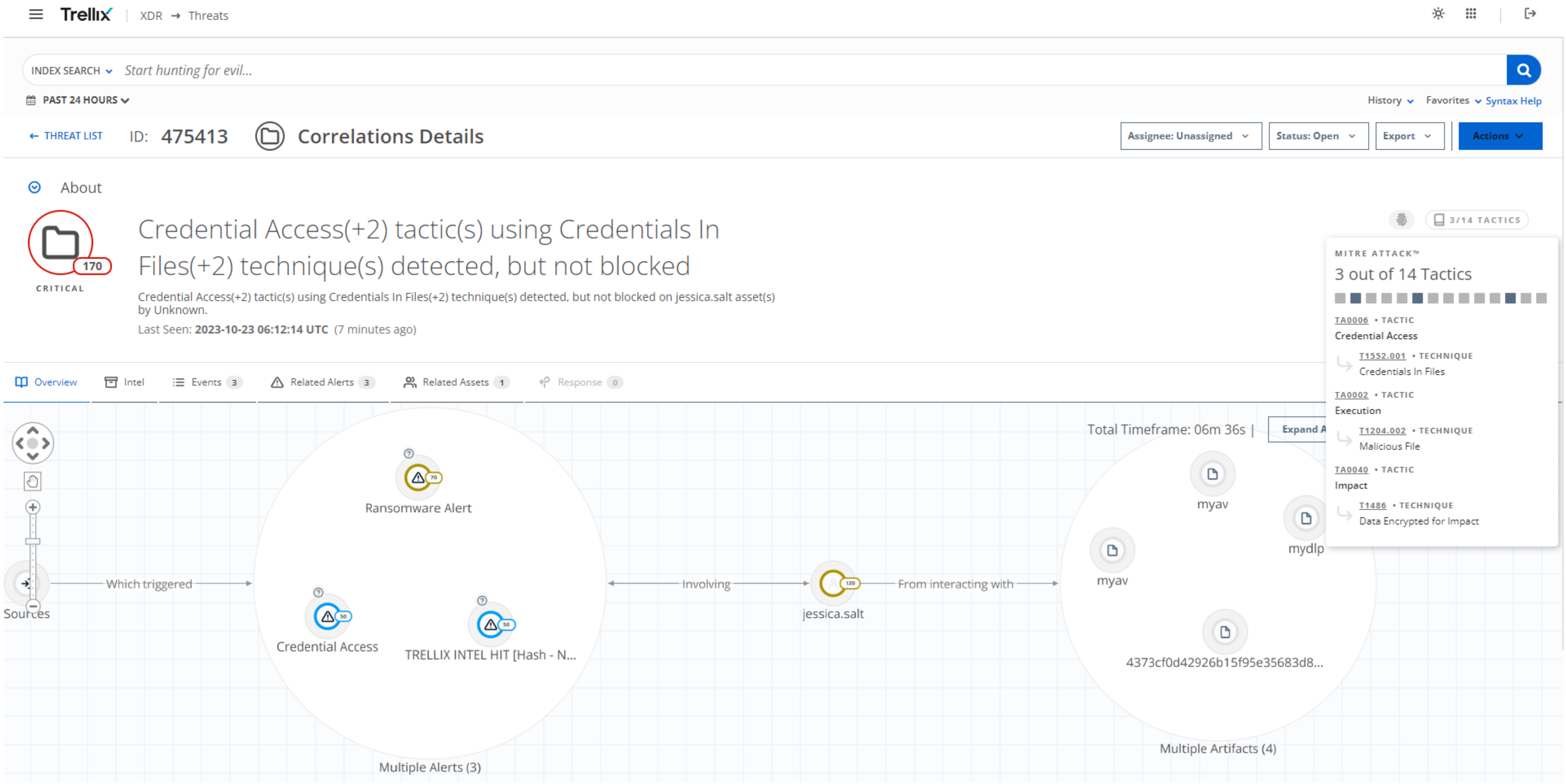
Query: class=mydlp policy=credentialaccess

Distinguisher: username

Threshold: 1

Time Window: 1 hours

Events – Trellix XDR



ID: 475413 Correlations Details

Credential Access(+2) tactic(s) using Credentials In Files(+2) technique(s) detected, but not blocked

Credential Access(+2) tactic(s) using Credentials In Files(+2) technique(s) detected, but not blocked on jessica.salt asset(s) by Unknown.

Last Seen: **2023-10-23 06:12:14 UTC** (7 minutes ago)

MITRE ATTACK™

3 out of 14 Tactics

TA0006 • TACTIC
Credential Access
T1552.001 • TECHNIQUE
Credentials In Files

TA0002 • TACTIC
Execution
T1204.002 • TECHNIQUE
Malicious File

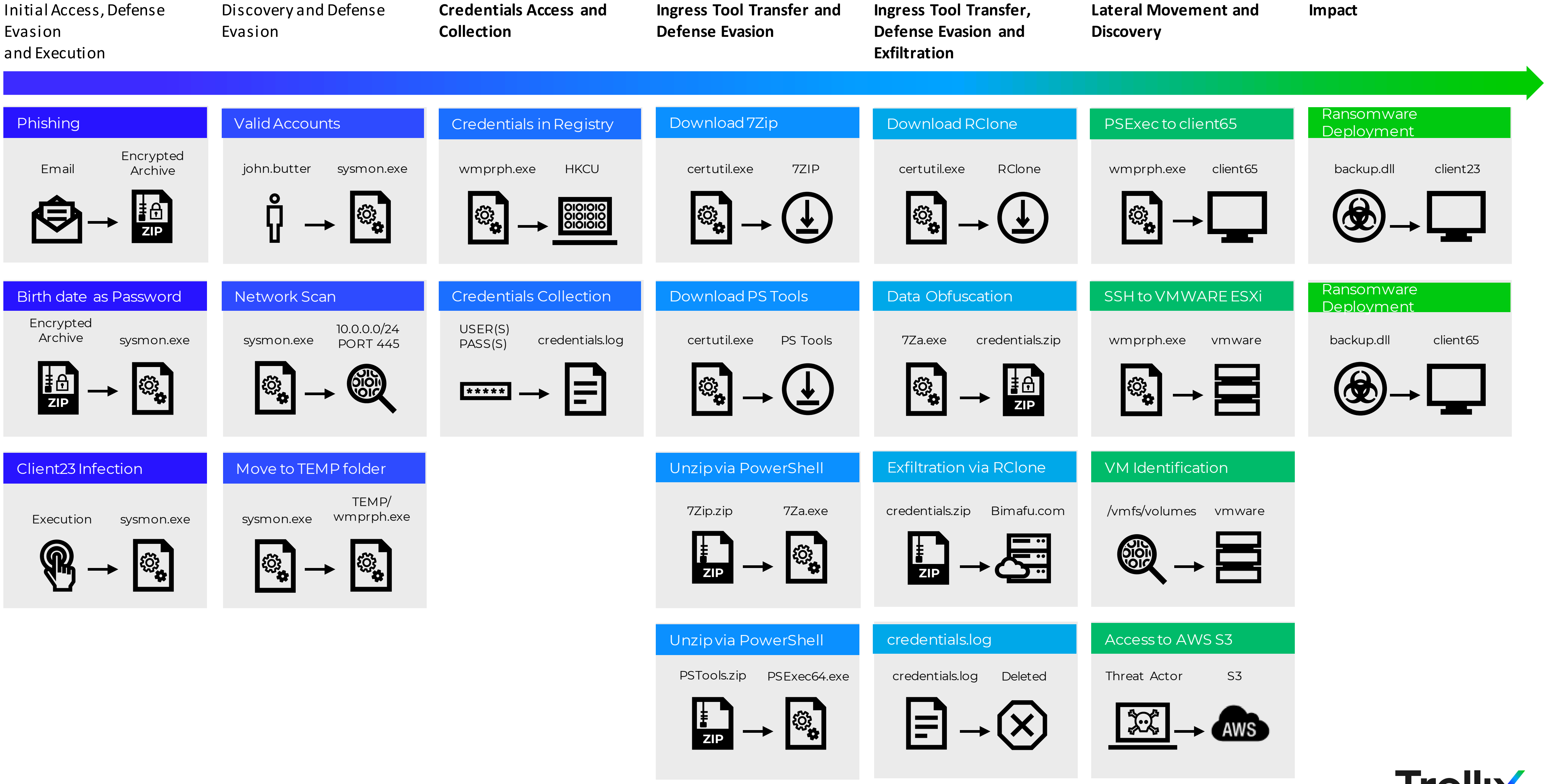
TA0040 • TACTIC
Impact
T1486 • TECHNIQUE
Data Encrypted for Impact

XDR Purple Team Exercise

Conti Ransomware Simulation

Trellix

Ransomware Kill chain



Initial Access, Defense Evasion and Execution

Phishing
Email → Encrypted Archive

Birth date as Password
Encrypted Archive → sysmon.exe

Client23 Infection
Execution → sysmon.exe

Discovery and Defense Evasion

Valid Accounts
john.butter → sysmon.exe

Network Scan
sysmon.exe → 10.0.0.0/24 PORT 445

Move to TEMP folder
sysmon.exe → TEMP/ wmprph.exe

Credentials Access and Collection

Credentials in Registry
wmprph.exe → HKCU

Credentials Collection
USER(S) PASS(S) → credentials.log

Ingress Tool Transfer and Defense Evasion

Download 7Zip
certutil.exe → 7ZIP

Download PS Tools
certutil.exe → PS Tools

Unzip via PowerShell
7Zip.zip → 7Za.exe

Unzip via PowerShell
PSTools.zip → PSExec64.exe

Ingress Tool Transfer, Defense Evasion and Exfiltration

Download RClone
certutil.exe → RClone

Data Obfuscation
7Za.exe → credentials.zip

Exfiltration via RClone
credentials.zip → Bimafu.com

credentials.log
credentials.log → Deleted

Lateral Movement and Discovery

PSExec to client65
wmprph.exe → client65

SSH to VMWARE ESXi
wmprph.exe → vmware

VM Identification
/vmfs/volumes → vmware

Access to AWS S3
Threat Actor → S3

Impact

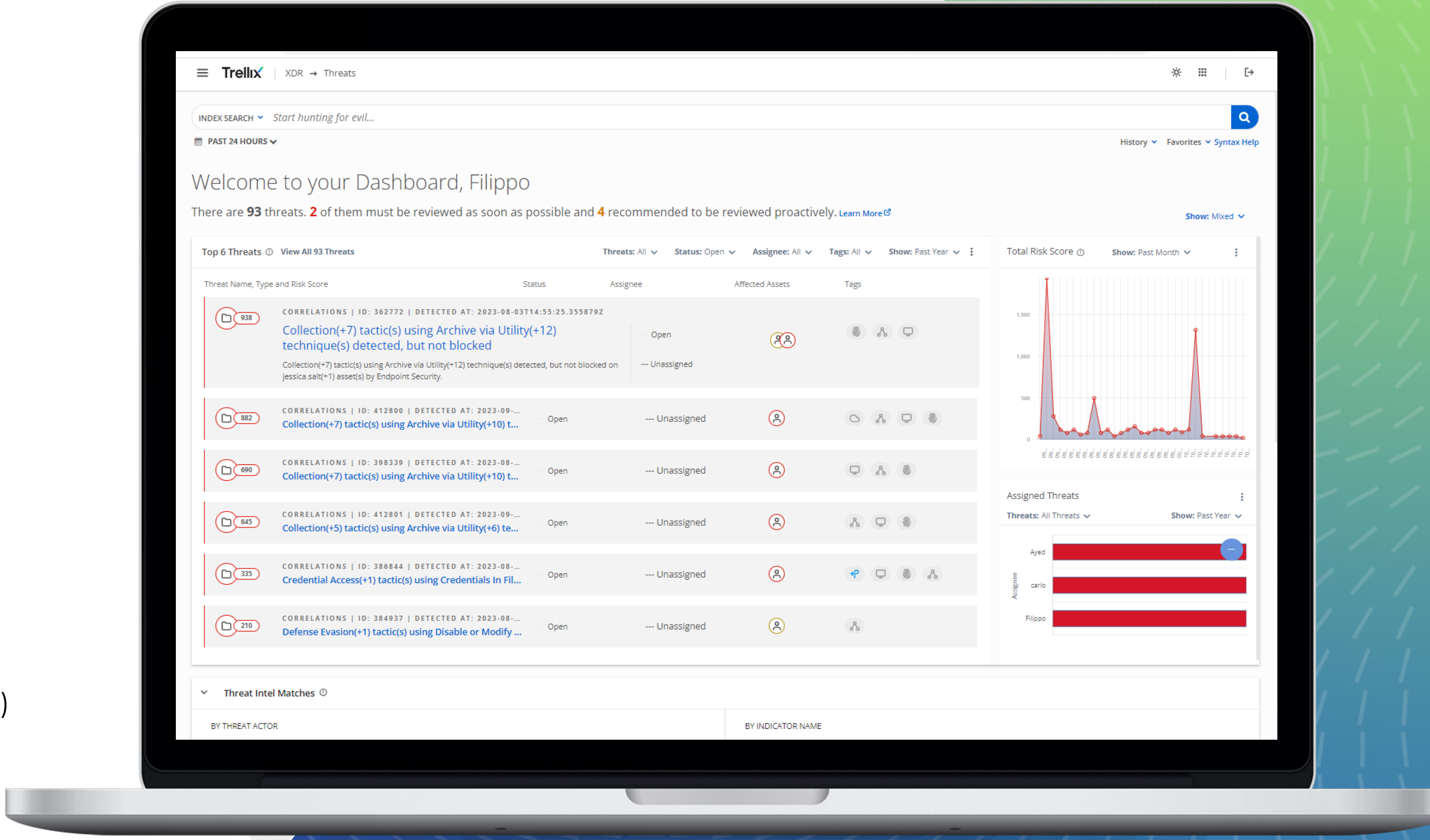
Ransomware Deployment
backup.dll → client23

Ransomware Deployment
backup.dll → client65

Demo

Demo Checkpoints

- XConsole switcher
- Search and TQL (ex MQL)
- MITRE
- Sources
- Assets
- Risk Score
- Case management
- Intelligence
- Events, Alerts, Correlations
- Actions (Playbooks)
- Alert Rules (don't forget analytics)
- Reporting
- Investigative Tips
- Cloud Connect



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

Show: Mixed

Top 6 Threats · View All 93 Threats · Threats: All · Status: Open · Assignee: All · Tags: All · Show: Past Year

Threat Name, Type and Risk Score	Status	Assignee	Affected Assets	Tags
938 CORRELATIONS | ID: 362772 | DETECTED AT: 2023-08-03T14:55:25.355879Z 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 jessica.salt(+1) asset(s) by Endpoint Security.	Open	--- Unassigned		
882 CORRELATIONS | ID: 412800 | DETECTED AT: 2023-09-... Collection(+7) tactic(s) using Archive via Utility(+10) t...	Open	--- Unassigned		
690 CORRELATIONS | ID: 398339 | DETECTED AT: 2023-08-... Collection(+7) tactic(s) using Archive via Utility(+10) t...	Open	--- Unassigned		
645 CORRELATIONS | ID: 412801 | DETECTED AT: 2023-09-... Collection(+5) tactic(s) using Archive via Utility(+6) te...	Open	--- Unassigned		
335 CORRELATIONS | ID: 386844 | DETECTED AT: 2023-08-... Credential Access(+1) tactic(s) using Credentials In Fil...	Open	--- Unassigned		
210 CORRELATIONS | ID: 384937 | DETECTED AT: 2023-08-... Defense Evasion(+1) tactic(s) using Disable or Modify ...	Open	--- Unassigned		

Total Risk Score · Show: Past Month

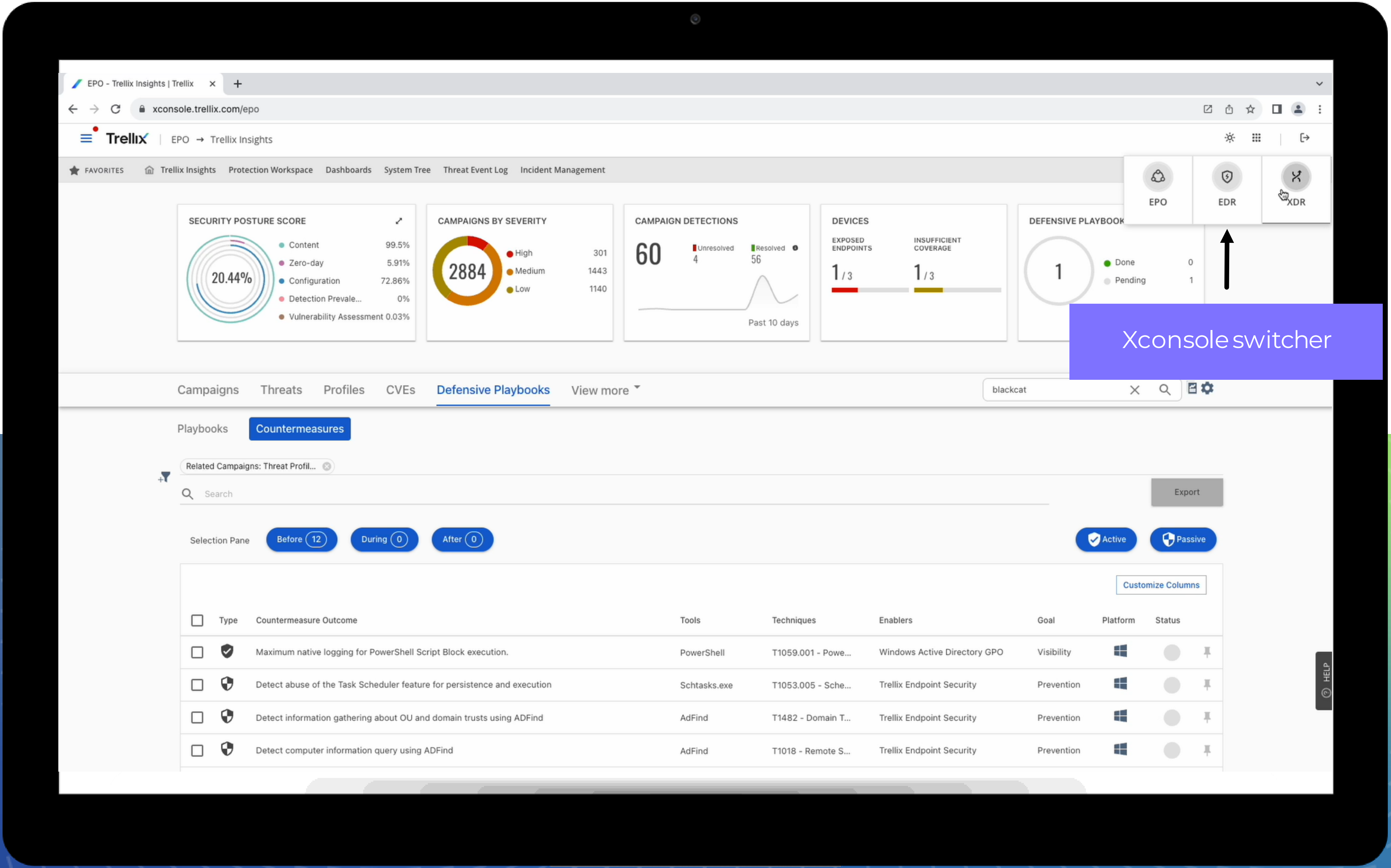
Assigned Threats · Threats: All Threats · Show: Past Year

Threat Intel Matches

BY THREAT ACTOR

BY INDICATOR NAME

Trellix



SECURITY POSTURE SCORE

20.44%

Content	99.5%
Zero-day	5.91%
Configuration	72.86%
Detection Prevale...	0%
Vulnerability Assessment	0.03%

CAMPAIGNS BY SEVERITY

2884

High	301
Medium	1443
Low	1140

CAMPAIGN DETECTIONS

60

Unresolved 4

Resolved 56

Past 10 days

DEVICES

EXPOSED ENDPOINTS 1 / 3

INSUFFICIENT COVERAGE 1 / 3

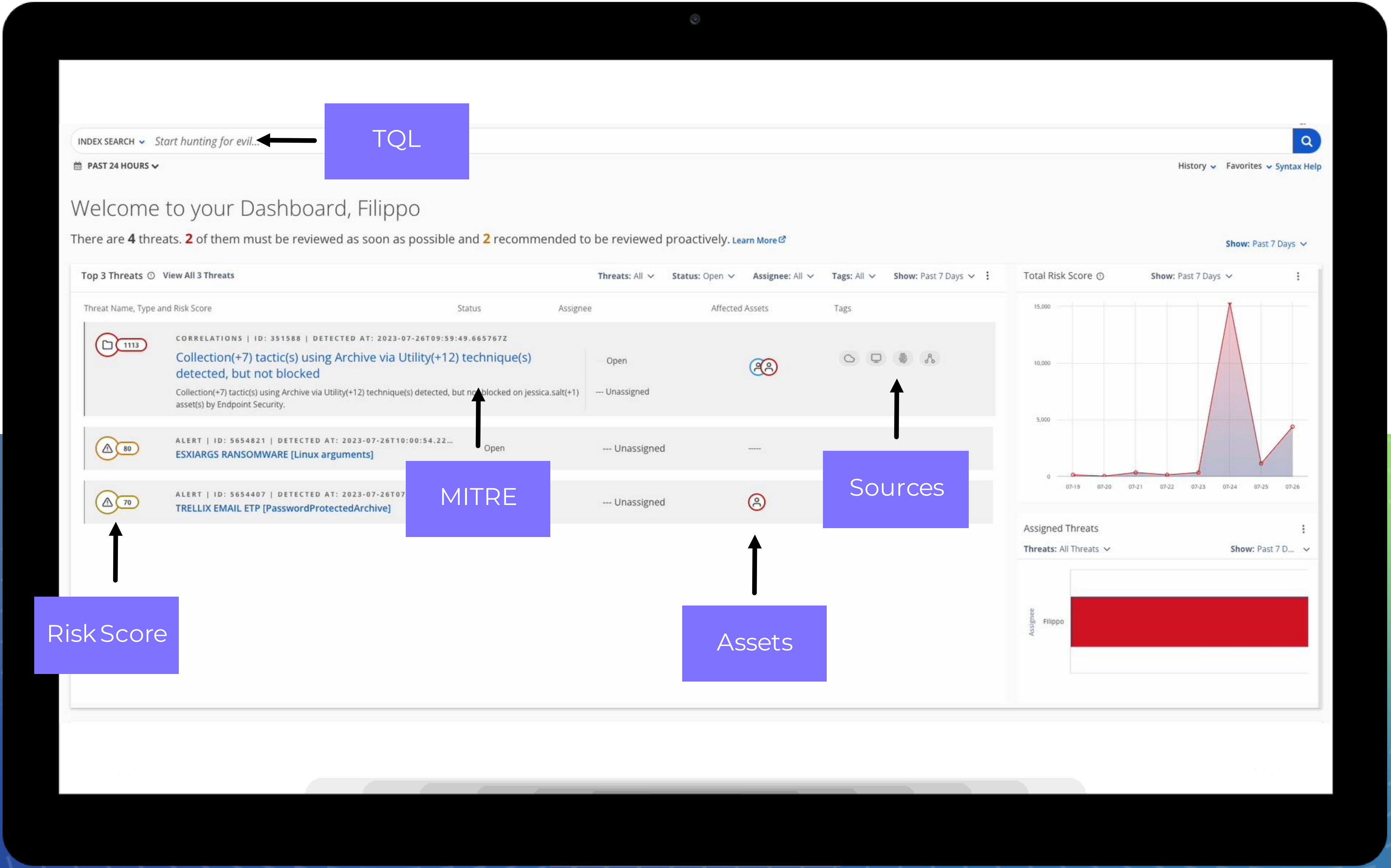
DEFENSIVE PLAYBOOK

1

Done	0
Pending	1

	Type	Countermeasure Outcome	Tools	Techniques	Enablers	Goal	Platform	Status
□		Maximum native logging for PowerShell Script Block execution.	PowerShell	T1059.001 - Powe...	Windows Active Directory GPO	Visibility		
□		Detect abuse of the Task Scheduler feature for persistence and execution	Schtasks.exe	T1053.005 - Sche...	Trellix Endpoint Security	Prevention		
□		Detect information gathering about OU and domain trusts using ADFind	AdFind	T1482 - Domain T...	Trellix Endpoint Security	Prevention		
□		Detect computer information query using ADFind	AdFind	T1018 - Remote S...	Trellix Endpoint Security	Prevention		

Xconsole switcher



INDEX SEARCH ⌄ *Start hunting for evil...*

PAST 24 HOURS ⌄

History ⌄ Favorites ⌄ Syntax Help

TQL

Welcome to your Dashboard, Filippo

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

Show: Past 7 Days ⌄

Top 3 Threats ⓘ View All 3 Threats

Threats: All ⌄ **Status:** Open ⌄ **Assignee:** All ⌄ **Tags:** All ⌄ **Show:** Past 7 Days ⌄

Threat Name, Type and Risk Score	Status	Assignee	Affected Assets	Tags
1113 CORRELATIONS | ID: 351588 | DETECTED AT: 2023-07-26T09:59:49.665767Z 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 jessica.salt(+1) asset(s) by Endpoint Security.	Open	--- Unassigned		
80 ALERT | ID: 5654821 | DETECTED AT: 2023-07-26T10:00:54.22... ESXIARGS RANSOMWARE [Linux arguments]	Open	--- Unassigned	-----	
70 ALERT | ID: 5654407 | DETECTED AT: 2023-07-26T07 TRELLIX EMAIL ETP [PasswordProtectedArchive]		--- Unassigned		

Total Risk Score ⓘ **Show:** Past 7 Days ⌄

Assigned Threats

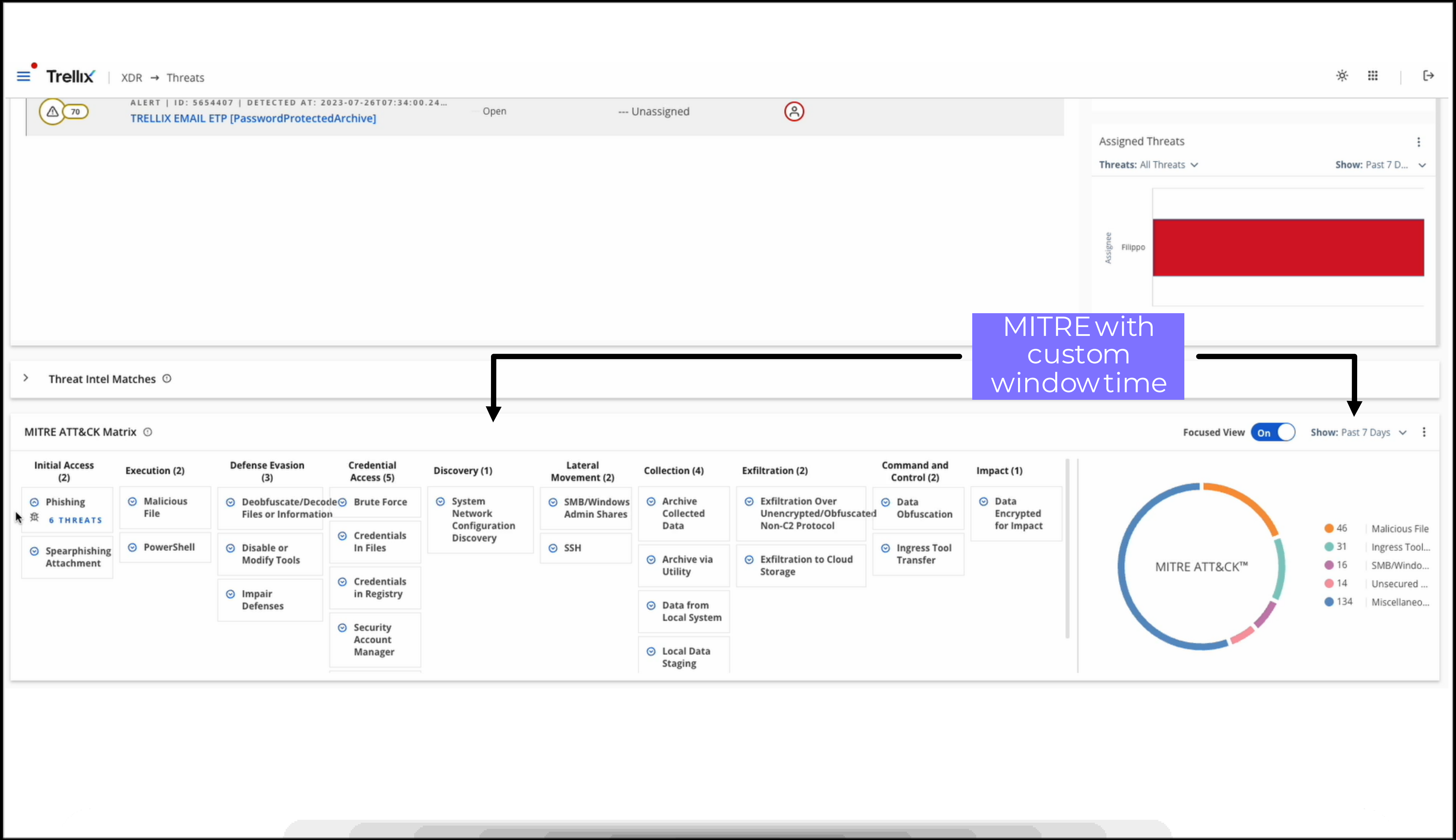
Threats: All Threats ⌄ **Show:** Past 7 D... ⌄

MITRE

Sources

Risk Score

Assets



Trellix | XDR → Threats

ALERT | ID: 5654407 | DETECTED AT: 2023-07-26T07:34:00.24…
70 TRELLIX EMAIL ETP [PasswordProtectedArchive]
Open
--- Unassigned

Assigned Threats
Threats: All Threats
Show: Past 7 D...

MITRE with custom windowtime

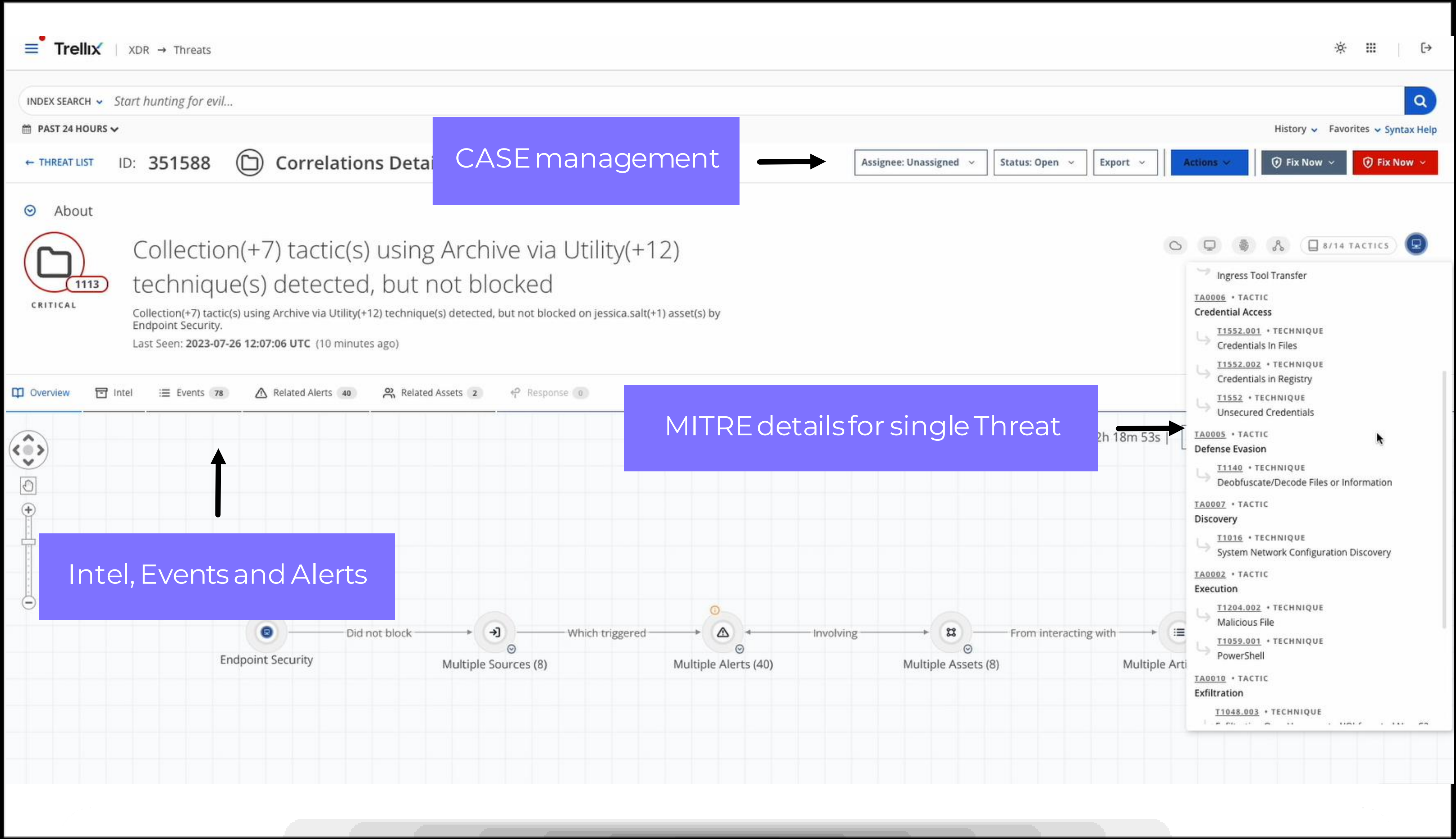
Threat Intel Matches

MITRE ATT&CK Matrix

Focused View On
Show: Past 7 Days

Initial Access (2)	Execution (2)	Defense Evasion (3)	Credential Access (5)	Discovery (1)	Lateral Movement (2)	Collection (4)	Exfiltration (2)	Command and Control (2)	Impact (1)
Phishing 6 THREATS	Malicious File	Deobfuscate/Decode Files or Information	Brute Force	System Network Configuration Discovery	SMB/Windows Admin Shares	Archive Collected Data	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Data Obfuscation	Data Encrypted for Impact
Spearphishing Attachment	PowerShell	Disable or Modify Tools	Credentials In Files		SSH	Archive via Utility	Exfiltration to Cloud Storage	Ingress Tool Transfer	
		Impair Defenses	Credentials in Registry			Data from Local System			
			Security Account Manager			Local Data Staging			

46	Malicious File
31	Ingress Tool...
16	SMB/Windo...
14	Unsecured ...
134	Miscellaneo...



Trellix | XDR → Threats

INDEX SEARCH ⌄ *Start hunting for evil...*

PAST 24 HOURS ⌄

History ⌄ Favorites ⌄ Syntax Help

← THREAT LIST ID: 351588 Correlations Detai

Assignee: Unassigned ⌄ | Status: Open ⌄ | Export ⌄ | Actions ⌄ | Fix Now ⌄ | Fix Now ⌄

About

1113 CRITICAL

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 jessica.salt(+1) asset(s) by Endpoint Security.

Last Seen: **2023-07-26 12:07:06 UTC** (10 minutes ago)

8/14 TACTICS

Ingress Tool Transfer

TA0006 • TACTIC
Credential Access

T1552.001 • TECHNIQUE
Credentials In Files

T1552.002 • TECHNIQUE
Credentials in Registry

T1552 • TECHNIQUE
Unsecured Credentials

TA0005 • TACTIC
Defense Evasion

T1140 • TECHNIQUE
Deobfuscate/Decode Files or Information

TA0007 • TACTIC
Discovery

T1016 • TECHNIQUE
System Network Configuration Discovery

TA0002 • TACTIC
Execution

T1204.002 • TECHNIQUE
Malicious File

T1059.001 • TECHNIQUE
PowerShell

TA0010 • TACTIC
Exfiltration

T1048.003 • TECHNIQUE

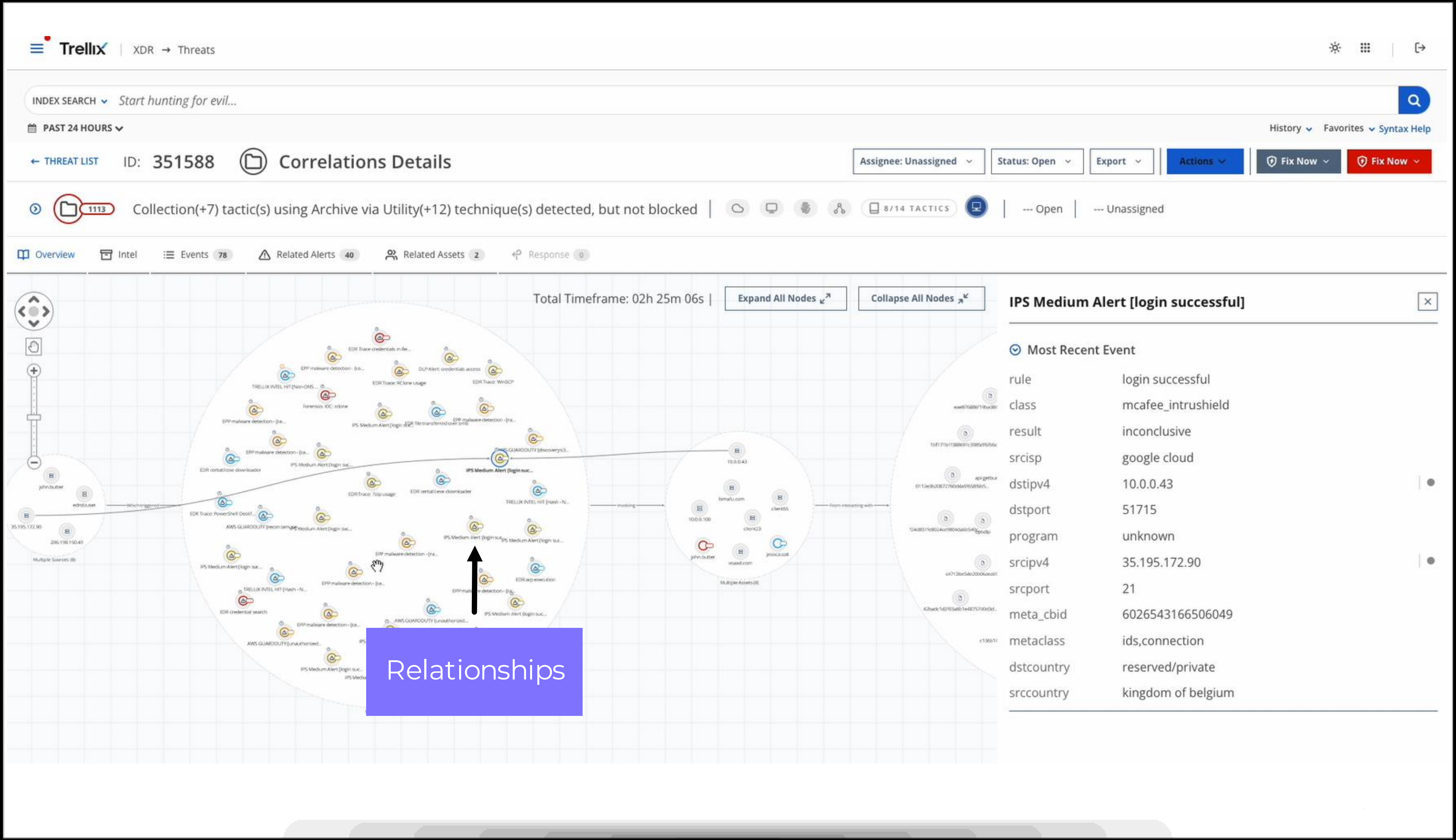
Overview | Intel | Events 78 | Related Alerts 40 | Related Assets 2 | Response 0

2h 18m 53s |

CASE management

MITRE details for single Threat

Intel, Events and Alerts



ID: 351588 Correlations Details

Collection(+7) tactic(s) using Archive via Utility(+12) technique(s) detected, but not blocked

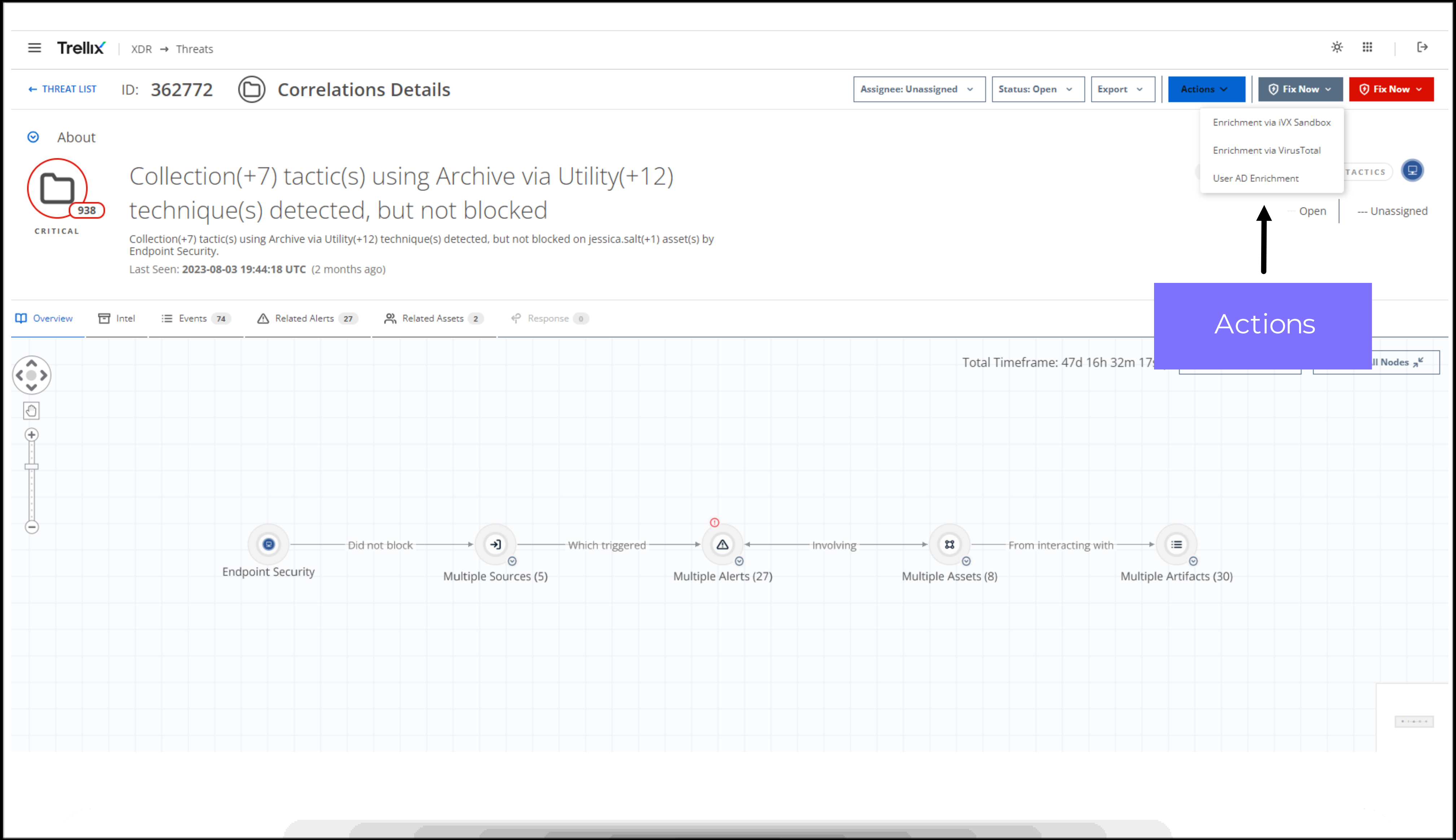
Total Timeframe: 02h 25m 06s |

IPS Medium Alert [login successful]

Most Recent Event

rule	login successful
class	mcafee_intrushield
result	inconclusive
srcisp	google cloud
dstipv4	10.0.0.43
dstport	51715
program	unknown
srcipv4	35.195.172.90
srcport	21
meta_cbid	6026543166506049
metaclass	ids,connection
dstcountry	reserved/private
srccountry	kingdom of belgium

Relationships



ID: 362772 Correlations Details

Collection(+7) tactic(s) using Archive via Utility(+12) technique(s) detected, but not blocked

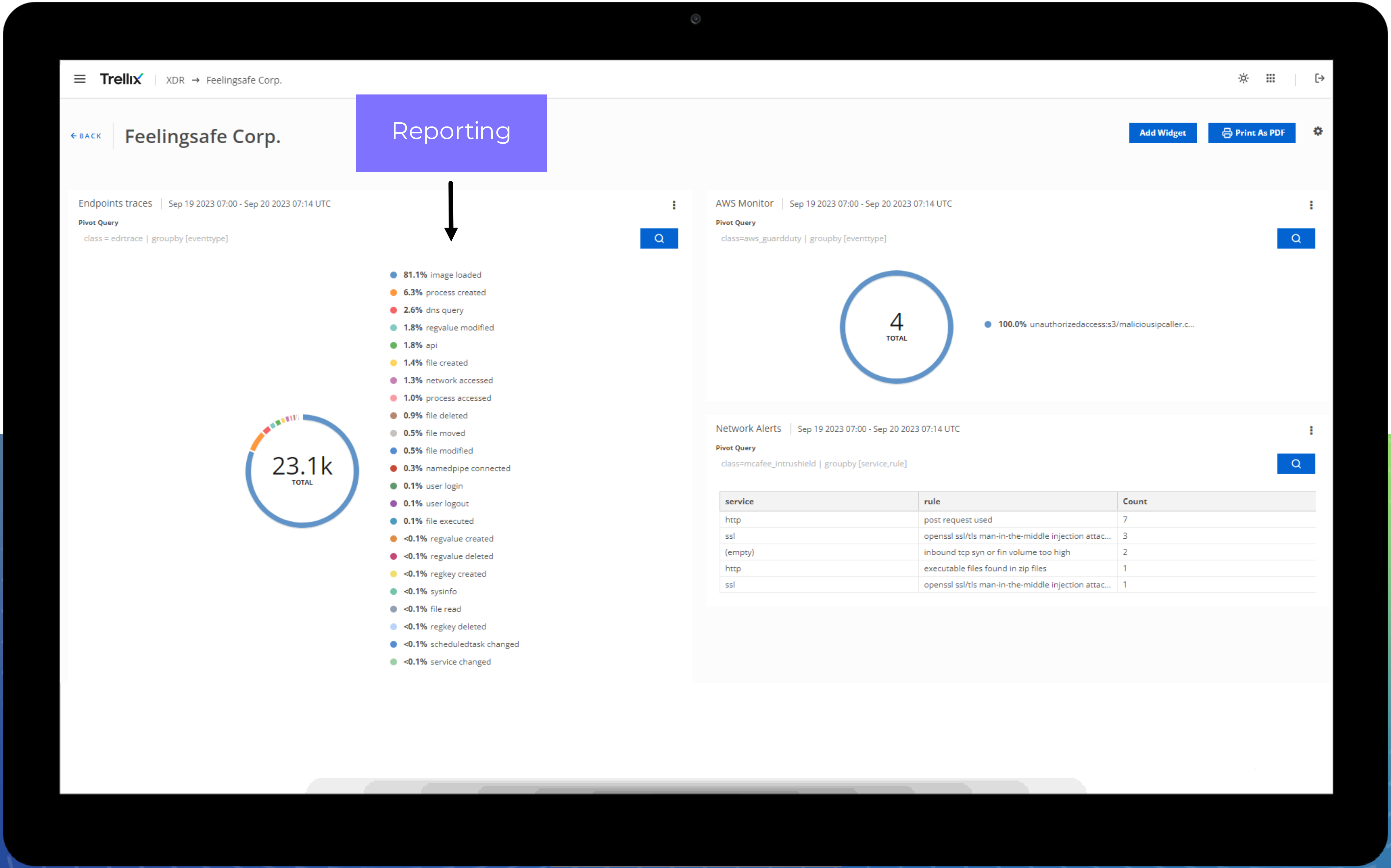
Collection(+7) tactic(s) using Archive via Utility(+12) technique(s) detected, but not blocked on jessica.salt(+1) asset(s) by Endpoint Security.

Last Seen: **2023-08-03 19:44:18 UTC** (2 months ago)

Total Timeframe: 47d 16h 32m 17

Actions

Reporting



☰ Trellix | XDR → Feelingsafe Corp.

← BACK

Feelingsafe Corp.

Add Widget | Print As PDF

Endpoints traces | Sep 19 2023 07:00 - Sep 20 2023 07:14 UTC

Pivot Query

class = edrtrace | groupby [eventtype]

- ● **81.1%** image loaded
- ● **6.3%** process created
- ● **2.6%** dns query
- ● **1.8%** regvalue modified
- ● **1.8%** api
- ● **1.4%** file created
- ● **1.3%** network accessed
- ● **1.0%** process accessed
- ● **0.9%** file deleted
- ● **0.5%** file moved
- ● **0.5%** file modified
- ● **0.3%** namedpipe connected
- ● **0.1%** user login
- ● **0.1%** user logout
- ● **0.1%** file executed
- ● **<0.1%** regvalue created
- ● **<0.1%** regvalue deleted
- ● **<0.1%** regkey created
- ● **<0.1%** sysinfo
- ● **<0.1%** file read
- ● **<0.1%** regkey deleted
- ● **<0.1%** scheduledtask changed
- ● **<0.1%** service changed

AWS Monitor | Sep 19 2023 07:00 - Sep 20 2023 07:14 UTC

Pivot Query

class=aws_guardduty | groupby [eventtype]

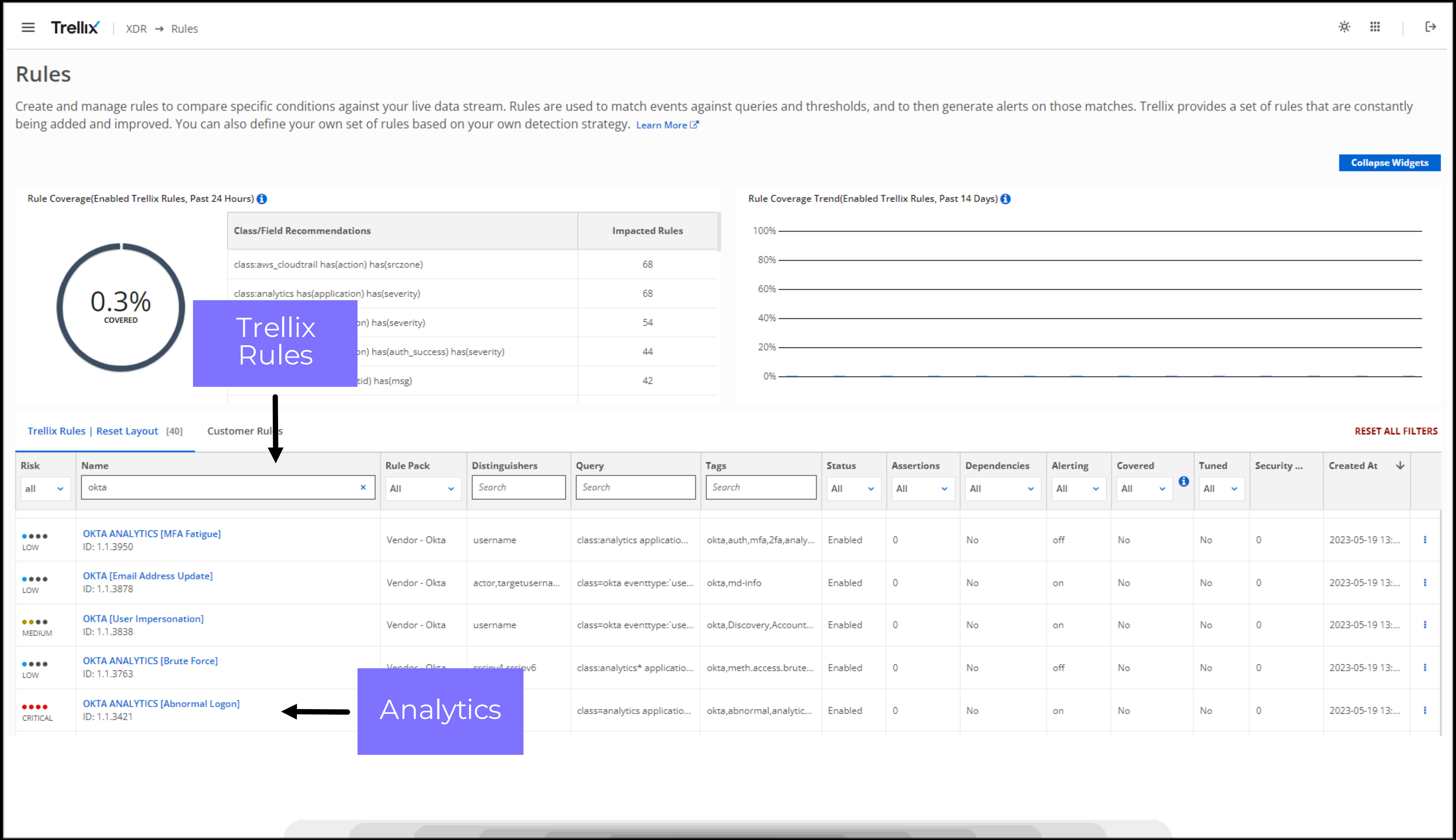
- ● **100.0%** unauthorizedaccess:s3/maliciousipcaller.c...

Network Alerts | Sep 19 2023 07:00 - Sep 20 2023 07:14 UTC

Pivot Query

class=mcafee_intrushield | groupby [service,rule]

service	rule	Count
http	post request used	7
ssl	openssl ssl/tls man-in-the-middle injection attac...	3
(empty)	inbound tcp syn or fin volume too high	2
http	executable files found in zip files	1
ssl	openssl ssl/tls man-in-the-middle injection attac...	1



Rules

Create and manage rules to compare specific conditions against 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 that are constantly being added and improved. You can also define your own set of rules based on your own detection strategy. Learn More

Rule Coverage(Enabled Trellix Rules, Past 24 Hours)

0.3% COVERED

Class/Field Recommendations	Impacted Rules
class:aws_cloudtrail has(action) has(srczone)	68
class:analytics has(application) has(severity)	68
on) has(severity)	54
on) has(auth_success) has(severity)	44
tid) has(msg)	42

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

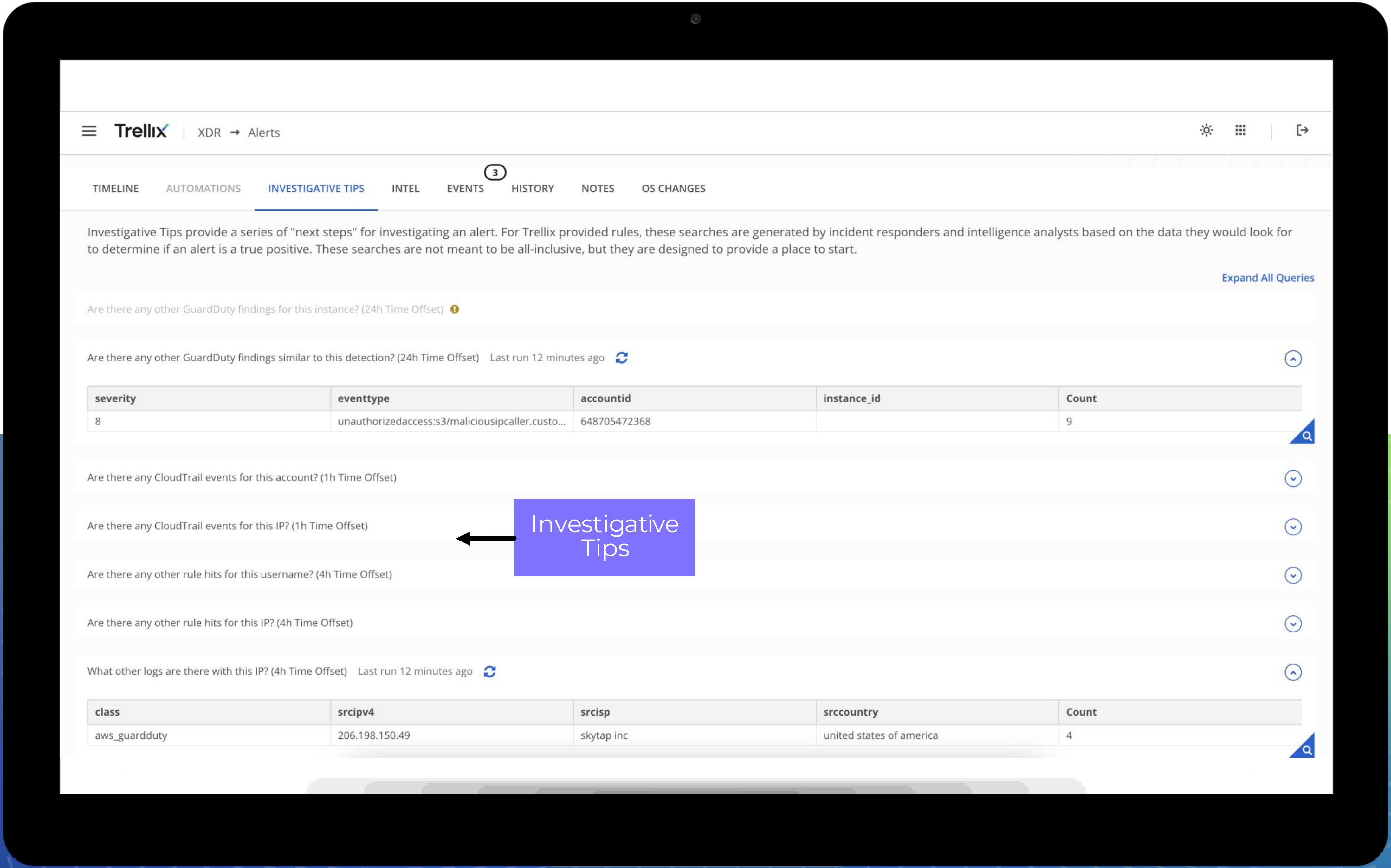
Trellix Rules

Trellix Rules | Reset Layout [40] Customer Rules

RESET ALL FILTERS

Risk	Name	Rule Pack	Distinguishers	Query	Tags	Status	Assertions	Dependencies	Alerting	Covered	Tuned	Security ...	Created At ↓
all	okta	All	Search	Search	Search	All	All	All	All	All	All		
●●●● LOW	OKTA ANALYTICS [MFA Fatigue] ID: 1.1.3950	Vendor - Okta	username	class:analytics applicatio...	okta,auth,mfa,2fa,analy...	Enabled	0	No	off	No	No	0	2023-05-19 13:...
●●●● LOW	OKTA [Email Address Update] ID: 1.1.3878	Vendor - Okta	actor,targetuserna...	class=okta eventtype:`use...	okta,md-info	Enabled	0	No	on	No	No	0	2023-05-19 13:...
●●●● MEDIUM	OKTA [User Impersonation] ID: 1.1.3838	Vendor - Okta	username	class=okta eventtype:`use...	okta,Discovery,Account...	Enabled	0	No	on	No	No	0	2023-05-19 13:...
●●●● LOW	OKTA ANALYTICS [Brute Force] ID: 1.1.3763	Vendor - Okta	srcipv4,srcipv6	class:analytics* applicatio...	okta,meth.access.brute...	Enabled	0	No	off	No	No	0	2023-05-19 13:...
●●●● CRITICAL	OKTA ANALYTICS [Abnormal Logon] ID: 1.1.3421			class=analytics applicatio...	okta,abnormal,analytic...	Enabled	0	No	on	No	No	0	2023-05-19 13:...

Analytics



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. These searches are not meant to be all-inclusive, but they are designed to provide a place to start.

Are there any other GuardDuty findings for this instance? (24h Time Offset)

Are there any other GuardDuty findings similar to this detection? (24h Time Offset) Last run 12 minutes ago

severity	eventtype	accountid	instance_id	Count
8	unauthorizedaccess:s3/maliciousipcaller.custo...	648705472368		9

Are there any CloudTrail events for this account? (1h Time Offset)

Are there any CloudTrail events for this IP? (1h Time Offset)

Are there any other rule hits for this username? (4h Time Offset)

Are there any other rule hits for this IP? (4h Time Offset)

What other logs are there with this IP? (4h Time Offset) Last run 12 minutes ago

class	srcipv4	srcisp	srccountry	Count
aws_guardduty	206.198.150.49	skytap inc	united states of america	4

Investigative Tips

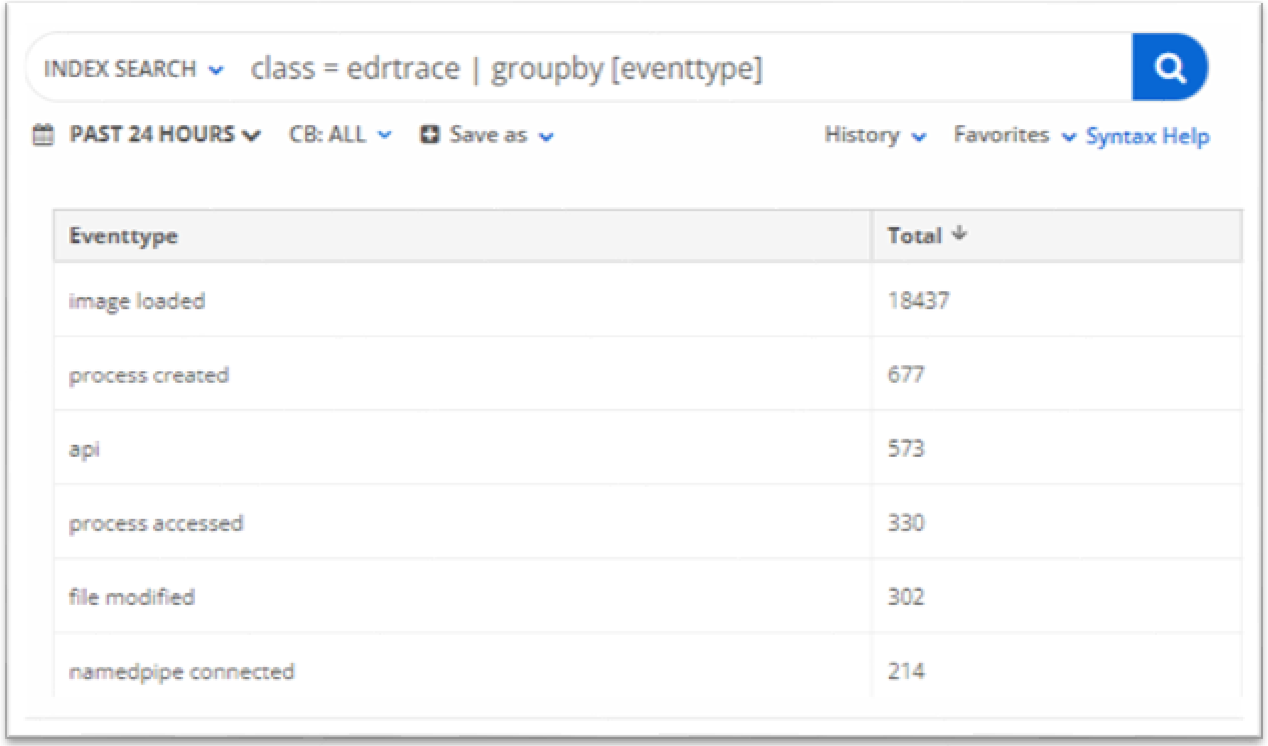
Trellix Query Language (TQL)

Trellix 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.

Anatomy of a TQL query

High-level anatomy of an TQL query:

<filter section> | <transform section>



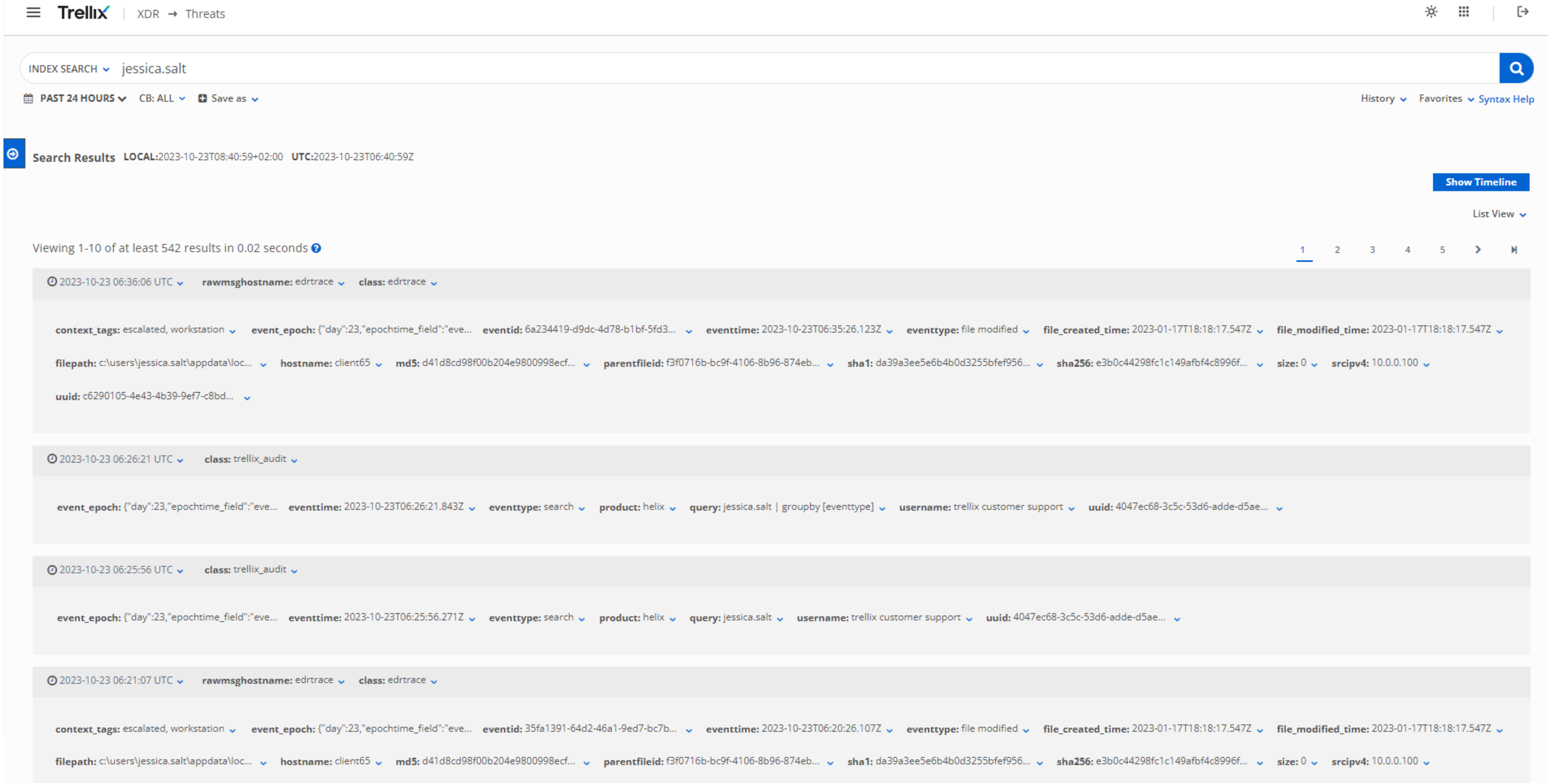
```
class = edrtrace | groupby [eventtype]
```

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



INDEX SEARCH jessica.salt

PAST 24 HOURS CB: ALL Save as

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...
```

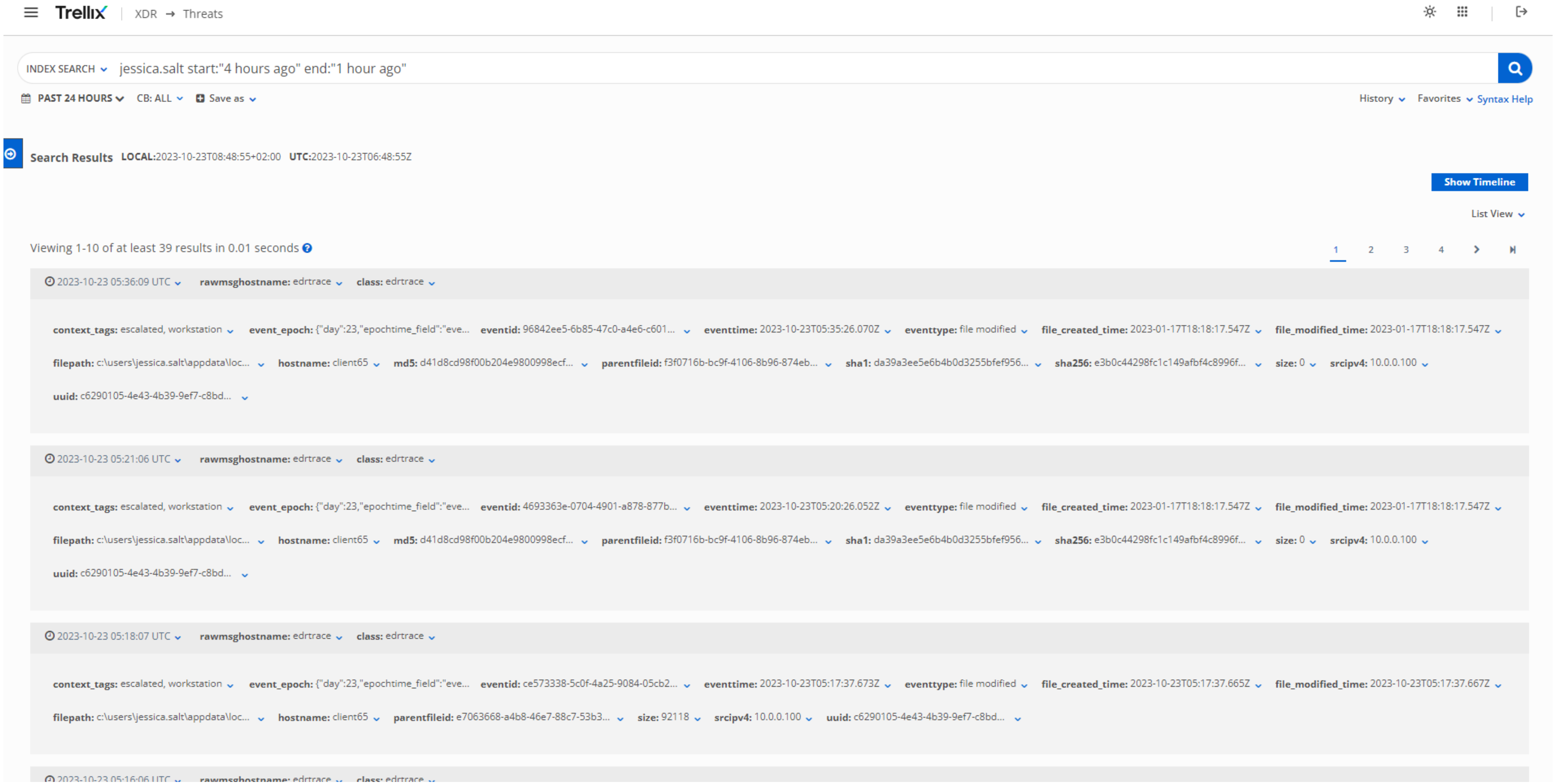
```
2023-10-23 06:25:56 UTC   class: trellix_audit

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 - Examples



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

PAST 24 HOURS CB: ALL Save as

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...

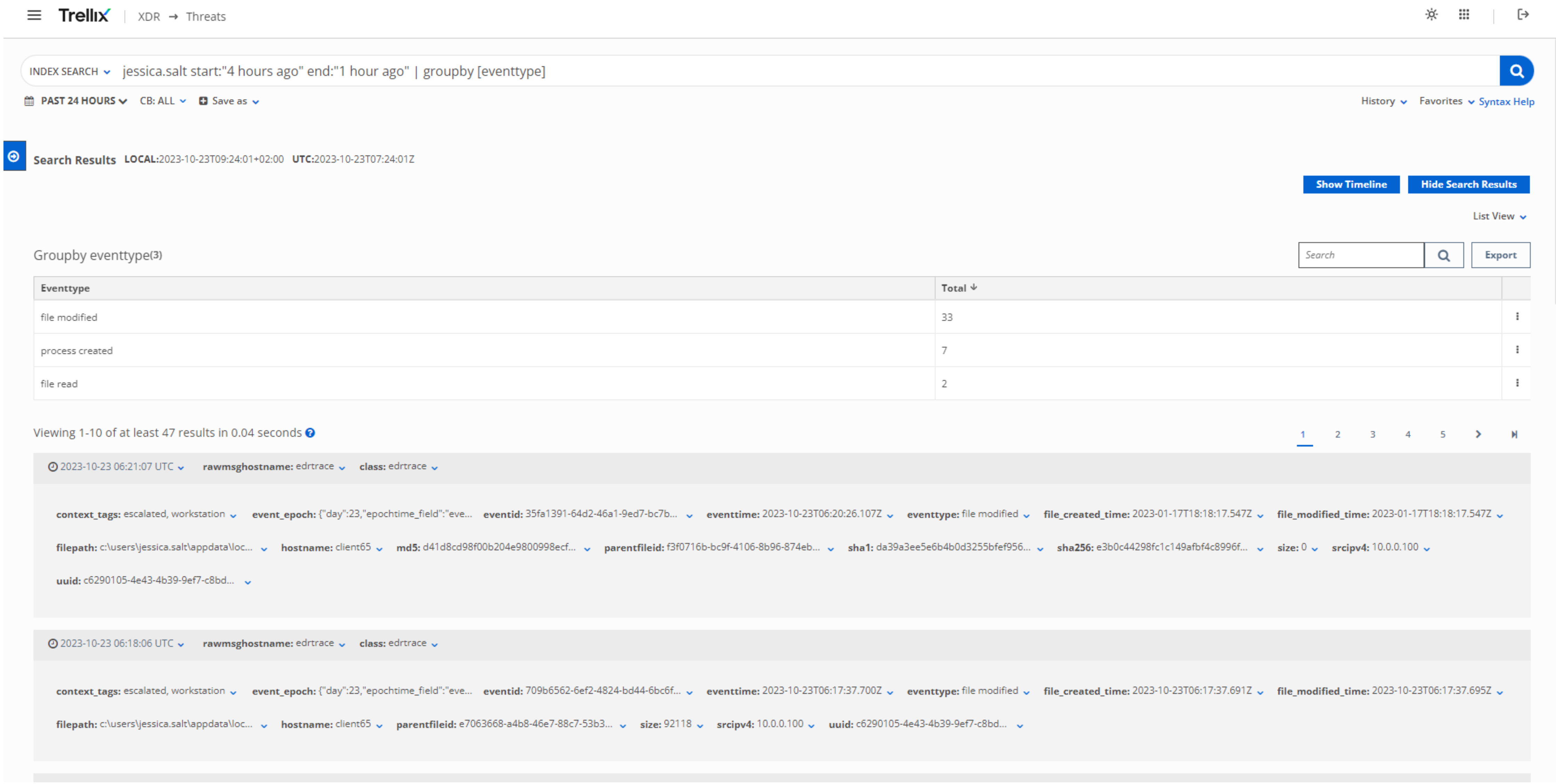
2023-10-23 05:18:07 UTC **rawmsghostname:** edrtrace **class:** edrtrace

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 - 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:** 35fa1391-64d2-46a1-9ed7-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...

Pre-Sales Resources

POV Guideline and Process

Trellix

Data Sources for XDR

XDR effectiveness depends on the data sources available for analysis. The log data that you send determines XDR's detection capability (such as use cases available). From the perspective of effective use of XDR, there are varying types of log data.

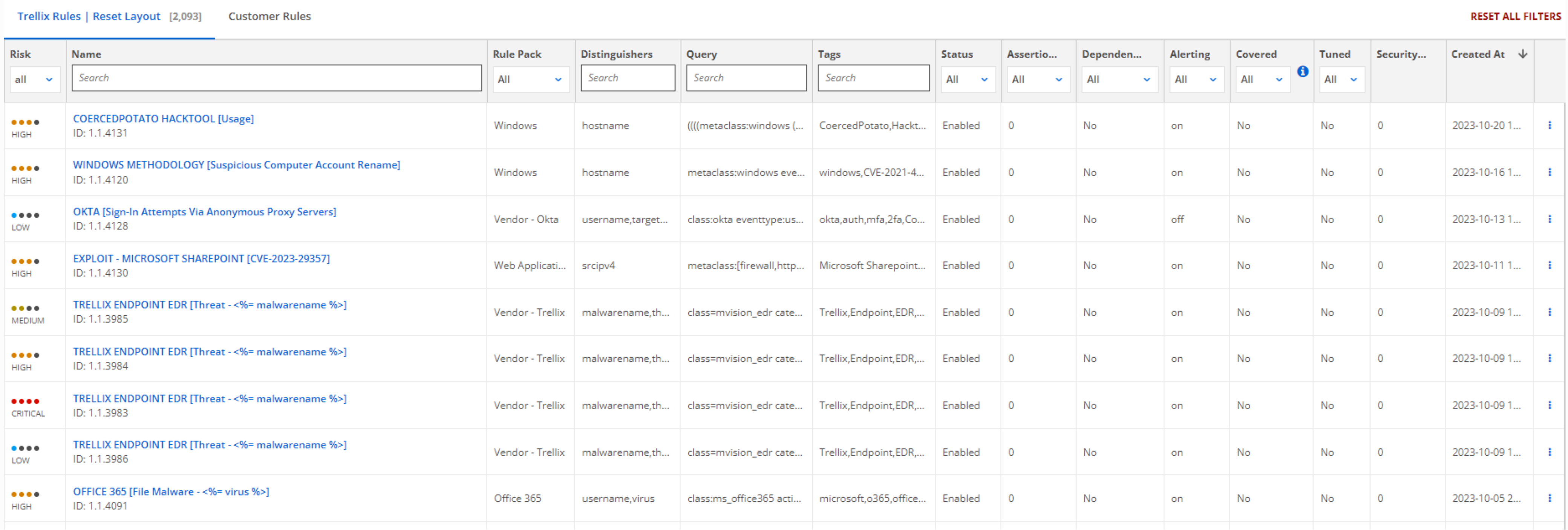
- Threat Detection Appliances
- Web Proxy (with user tracking)
- DNS Resolution and Relay events
- Authentication Events
- AD/LDAP, Wireless, VPN, etc.
- Firewalls (including NAT logs)
- Email server and transactions
- Endpoint Security
- Operating System events
- IDS / IPS
- Database Security/Audit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

Trellix Rules VS Customer Rules

There are two types of rules in XDR:

Trellix rules: Rules created by Trellix experts that detect a wide range of malicious activity. These rules are created and updated regularly.

Customer rules: Rules that you define, which detect events specific to your environment and organizational needs.



Trellix Rules | Reset Layout [2,093]   Customer Rules   RESET ALL FILTERS

Risk	Name	Rule Pack	Distinguishers	Query	Tags	Status	Assertio...	Dependen...	Alerting	Covered	Tuned	Security...	Created At ↓	
all	Search	All	Search	Search	Search	All	All	All	All	All	All			
●●●● HIGH	COERCEDPOTATO HACKTOOL [Usage] ID: 1.1.4131	Windows	hostname	((((metaclass:windows (...	CoercedPotato,Hackt...	Enabled	0	No	on	No	No	0	2023-10-20 1...	⋮
●●●● HIGH	WINDOWS METHODOLOGY [Suspicious Computer Account Rename] ID: 1.1.4120	Windows	hostname	metaclass:windows eve...	windows,CVE-2021-4...	Enabled	0	No	on	No	No	0	2023-10-16 1...	⋮
●●●● LOW	OKTA [Sign-In Attempts Via Anonymous Proxy Servers] ID: 1.1.4128	Vendor - Okta	username,target...	class:okta eventtype:us...	okta,auth,mfa,2fa,Co...	Enabled	0	No	off	No	No	0	2023-10-13 1...	⋮
●●●● HIGH	EXPLOIT - MICROSOFT SHAREPOINT [CVE-2023-29357] ID: 1.1.4130	Web Applicati...	srcipv4	metaclass:[firewall,http...	Microsoft Sharepoint...	Enabled	0	No	on	No	No	0	2023-10-11 1...	⋮
●●●● MEDIUM	TRELLIX ENDPOINT EDR [Threat - <%= malwarename %>] ID: 1.1.3985	Vendor - Trellix	malwarename,th...	class=mvision_edr cate...	Trellix,Endpoint,EDR,...	Enabled	0	No	on	No	No	0	2023-10-09 1...	⋮
●●●● HIGH	TRELLIX ENDPOINT EDR [Threat - <%= malwarename %>] ID: 1.1.3984	Vendor - Trellix	malwarename,th...	class=mvision_edr cate...	Trellix,Endpoint,EDR,...	Enabled	0	No	on	No	No	0	2023-10-09 1...	⋮
●●●● CRITICAL	TRELLIX ENDPOINT EDR [Threat - <%= malwarename %>] ID: 1.1.3983	Vendor - Trellix	malwarename,th...	class=mvision_edr cate...	Trellix,Endpoint,EDR,...	Enabled	0	No	on	No	No	0	2023-10-09 1...	⋮
●●●● LOW	TRELLIX ENDPOINT EDR [Threat - <%= malwarename %>] ID: 1.1.3986	Vendor - Trellix	malwarename,th...	class=mvision_edr cate...	Trellix,Endpoint,EDR,...	Enabled	0	No	on	No	No	0	2023-10-09 1...	⋮
●●●● HIGH	OFFICE 365 [File Malware - <%= virus %>] ID: 1.1.4091	Office 365	username,virus	class:ms_office365 acti...	microsoft,o365,office...	Enabled	0	No	on	No	No	0	2023-10-05 2...	⋮

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.

If the customer cannot provide a clear EPS number, then guidance is: **1 EPS per user**

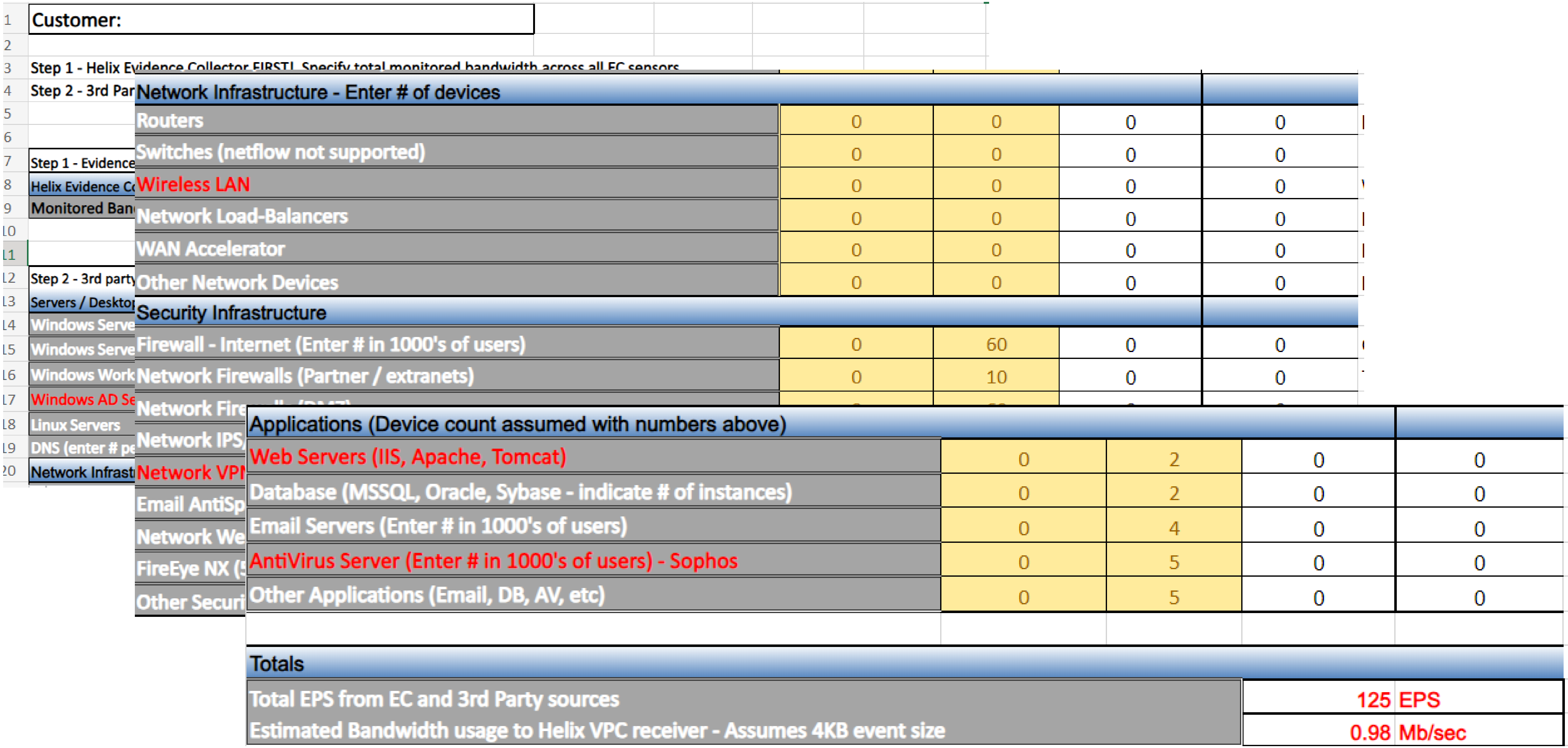
- 2,500 EPS – (2500 * 4096 * (1 – 0.75))/1,048,576 = 2.4 MB/sec
- 5,000 EPS – (5000 *4096 * (1 – 0.75))/1,048,576 = 4.9 MB/sec
- 10,000 EPS - (10000 *4096 * (1 – 0.75))/1,048,576 = 9.8 MB/sec
- 40,000 EPS - (40000 *4096 * (1 – 0.75))/1,048,576 = 39.1 MB/sec

Sizing Questionnaire

- What is the total number EPS (events per second) you expect to send based on logs generated from your infrastructure?

- Number of devices you will be sending logs from?
  - Servers? (like AD, DNS etc..)
  - Routers?
  - Firewalls?
  - Switches?
  - IPS/IDS?
  - VPN?
  - Proxy?
  - Email Antispam?
  - Load balancers?
  - EDR/Anti-Virus servers?
  - Web Servers?
  - Databases?
  - Wireless LAN?
  - Other Security devices?

Helix EPS and Bandwidth Usage Calculator



Customer:

Step 1 - Helix Evidence Collector FIRST! Specify total monitored bandwidth across all EC sensors

Step 2 - 3rd Par

Step 1 - Evidence

Helix Evidence Co

Monitored Ban

Step 2 - 3rd party

Servers / Desktop

Windows Serve

Windows Serve

Windows Work

Windows AD Se

Linux Servers

DNS (enter # pe

Network Infrast

Network Infrastructure - Enter # of devices				
Routers	0	0	0	0
Switches (netflow not supported)	0	0	0	0
Wireless LAN	0	0	0	0
Network Load-Balancers	0	0	0	0
WAN Accelerator	0	0	0	0
Other Network Devices	0	0	0	0
Security Infrastructure				
Firewall - Internet (Enter # in 1000's of users)	0	60	0	0
Network Firewalls (Partner / extranets)	0	10	0	0
Network Fire				
Network IPS				
Network VPN				
Email AntiSp				
Network We				
FireEye NX (5				
Other Securi				

Applications (Device count assumed with numbers above)				
Web Servers (IIS, Apache, Tomcat)	0	2	0	0
Database (MSSQL, Oracle, Sybase - indicate # of instances)	0	2	0	0
Email Servers (Enter # in 1000's of users)	0	4	0	0
AntiVirus Server (Enter # in 1000's of users) - Sophos	0	5	0	0
Other Applications (Email, DB, AV, etc)	0	5	0	0

Totals	
Total EPS from EC and 3rd Party sources	125 EPS
Estimated Bandwidth usage to Helix VPC receiver - Assumes 4KB event size	0.98 Mb/sec

Trellix Differentiators

SentinelOne

	Requirement	Trellix	SentinelOne	Outcomes / Customer Benefit
Strategic Security Vendor	Portfolio for Strategic Security Initiatives	☑	⊠	**Trellix** is security platform with capabilities across endpoint, email, network, cloud, data and vast threat intelligence. **SentinelOne** is endpoint centric with limited threat intelligence.
	Integrated Threat Intelligence	☑	⊠	**Trellix Insights** exposes rich actionable and customizable Threat Intel (by industry and country). **SentinelOne** claims their own threat intelligence but it isn't exposed to customers and they promote leveraging 3rd party threat intelligence like RecordedFuture.
	Open and Native XDR	☑	⊠	**Trellix** is truly Open and Native XDR has far more 3rd party integrations and far more native integrations with control points like email and network. **SentinelOne** is endpoint centric and doesn't have any many integrations as Trellix with only 15 premium integrations.
Detect and Respond	Automatic alert prioritization	☑	☑	**Trellix XDR** prioritizes alerts by showing context that matters to customers. **SentinelOne Endpoint** AI does prioritize alerts, though largely based on endpoint telemetry.
	Investigation Workflow	☑	⊠	**Trellix XDR** has intuitive workflow allowing customers to get high level attack visualization and drill into details. **SentinelOne** investigation workflow for endpoint is not bad but with XDR remains rudimentary.
	Out of box and customizable playbooks	☑	☒	**Trellix XDR** has many out of box and customizable playbooks to help responders automate tasks with many integrations. **SentinelOne** points to SIEM integrations for customizable playbooks since their own automation is extremely limited to endpoint custom rules.
Operational Efficiency	SOC Analyst UX	☑	⊠	**Trellix** workflow for SOC Analysts gives high-level overview and progression of an incident and has quick pivots into context for needed details. **SentinelOne** is focused on Endpoint SOC Analysts with very limited context beyond endpoint in the UI.
	Deeper context through native integration	☑	☒	**Trellix** built-in native integrations with endpoint, email, and network provide deeper expertise on cross control use cases. **SentinelOne** "native" integrations are all endpoint only with no network or email.
	Persona-centric views	☑	☑	Personal based Helix UI is focused on providing optimized usability experiences for different personas. SentinelOne RBAC is quite granular for different user roles.

Legend	☑	Full Coverage	⊠	Partial Coverage	☒	No Coverage

Microsoft

	Requirement	Trellix	Microsoft	Outcomes / Customer Benefit	Legend
Strategic Security Vendor	**Portfolio for Strategic Security Initiatives**	☑	☑	Both vendors offer coverage beyond Endpoint. Trellix is security focused and independent of the productivity platform. Microsoft missing network coverage and isn't singularly focused on security.	☑ Full Coverage
	Integrated Threat Intelligence	☑	⊠	Trellix Insights exposes far more actionable and customizable Threat Intel (by industry and country) than MS Threat Analytics which isn't customizable for customer relevance	
	Open and Native XDR	☑	⊠	Trellix is Open and Native XDR has far more integrations than M365 Defender. MS customers either can't leverage existing investments or need to deploy MS Sentinel and accompanying SIEM complexity and costs for broader integrations.	
Detect and Respond	**Automatic alert prioritization**	☑	☑	Trellix XDR prioritizes alerts by showing context that matters to customers. Microsoft has icons and filters to give visibility to areas for responders to focus on.	⊠ Partial Coverage
	Investigation Workflow	☑	⊠	Trellix XDR has intuitive workflow allowing customers to get high level attack visualization and drill into details. Microsoft investigative workflow is confusing and not prescriptive in understanding next steps.	
	Out of box and customizable playbooks	☑	☒	Trellix XDR has many out of box and customizable playbooks to help responders automate tasks with many integrations. M365 Defender doesn't have playbooks. Customers need MS Sentinel to build playbooks which add technical complexity and pricing unpredictability.	
Operational Efficiency	**SOC Analyst UX**	☑	⊠	Trellix workflow for SOC Analysts gives high-level overview and progression of an incident and has quick pivots into context for needed details. Microsoft SecOps UX in MS Defender and Sentinel are very complex for practitioners.	☒ No Coverage
	Deeper context through native integration	☑	☑	Built-in native integrations with endpoint, email, and network provide deeper expertise on cross control use cases. Microsoft has email and identity native integrations, but network and cloud workloads requires MS Sentinel.	
	Persona-centric views	☑	⊠	Personal based Helix UI is focused on providing optimized usability experiences for different personas. Microsoft is limited to basic security operator personas based more on role-based access than usability.	

Paloalto

	Requirement	Trellix	paloalto	Outcomes / Customer Benefit	Legend
Strategic Security Vendor	Portfolio for Strategic Security Initiatives	☑	☑	Both vendors offer coverage beyond Endpoint. Trellix is security focused and independent of the productivity platform. Palo Alto has 3 major platforms to support customers for strategic security initiatives.	☑
	Integrated Threat Intelligence	☑	☒	Trellix Insights exposes far more actionable and customizable Threat Intel (by industry and country) and is included in our XDR offering. Threat Intelligence is an extra cost and more closely positioned with their SOAR solution, separate from XDR.	Full Coverage
	Open and Native XDR	☑	☒	Trellix is Open and Native XDR has far more integrations than Palo Alto Cortex XDR. Their SOAR solution, XSOAR, has a comparable number of integrations as an industry leading SOAR solution, but is separate and a separate cost.	
Detect and Respond	Automatic Alert Prioritization	☑	☒	Trellix XDR prioritizes alerts by showing context that matters to customers. Palo Alto has a very busy interface with lots of details making it difficult for SOC Analysts to prioritize alert triage.	☒
	Investigation Workflow	☑	☒	Trellix XDR has intuitive workflow allowing customers to get high level attack visualization and drill into details. Palo Alto investigative workflow is complex to navigate. Minimal automation.	
	Out of box and customizable playbooks	☑	☒	Trellix XDR has many out of box and customizable playbooks to help responders automate tasks with many integrations. Palo Alto has a strong SOAR solution but it is separate from Cortex XDR and is high cost and complex.	Partial Coverage
Operational Efficiency	SOC Analyst UX	☑	☒	Trellix workflow for SOC Analysts gives high-level overview and progression of an incident and has quick pivots into context for needed details. Palo Alto SOC Analyst	✖
	Deeper Context Through Native Integration	☑	☒	Built-in native integrations with endpoint, email, and network provide deeper expertise on cross control use cases. Palo Alto has native integration with network, ueba, and cloud but is missing important native integration with email. Also missing data protection.	No Coverage
	Persona-centric Views	☑	☒	Personal based Helix UI is focused on providing optimized usability experiences for different personas. Palo Alto has RBAC controls for Cortex XDR admins that are granular and complex.	

Crowdstrike

	Requirement	Trellix	CROWDSTRIKE	Outcomes / Customer Benefit
Strategic Security Vendor	Portfolio for Strategic Security Initiatives	☑	⊠	**Trellix** is security platform with capabilities across endpoint, email, network, cloud, data and vast threat intelligence. **CrowdStrike** is endpoint-centric and has no proper DLP solution.
	Integrated Threat Intelligence	☑	☑	**Trellix Insights** exposes rich actionable and customizable Threat Intel (by industry and country). **CrowdStrike** threat intelligence is a strength, customizable by industry and country and enriches alerting in the flacon platform.
	Open and Native XDR	☑	⊠	**Trellix** is truly Open and Native XDR has far more 3rd party integrations and far more native integrations with control points like email and network. **CrowdStrike** is endpoint centric and doesn't have any many integrations as Trellix with only 20 integrations.
Detect and Respond	Automatic alert prioritization	☑	☑	**Trellix XDR** prioritizes alerts by showing context that matters to customers. **CrowdStrike** has graphical UI to show high priority alerts and utilizes CrowdScore for additional prioritization on threat levels.
	Investigation Workflow	☑	⊠	**Trellix XDR** has intuitive workflow allowing customers to get high level attack visualization and drill into details. **CrowdStrike** investigative workflow is complex, but does include graphical representations of incidents involving multiple data sources.
	Out of box and customizable playbooks	☑	⊠	**Trellix XDR** has many out of box and customizable playbooks to help responders automate tasks with many integrations. **CrowdStrike Fusion** is included with Falcon Insights EDR/XDR and allows for simple endpoint centric playbooks with a ServiceNow integration.
Operational Efficiency	SOC Analyst UX	☑	⊠	**Trellix** workflow for SOC Analysts gives high-level overview and progression of an incident and has quick pivots into context for needed details. **CrowdStrike** is advanced at providing high levels of details for expert users but is complex for many SOC Analysts.
	Deeper context through native integration	☑	☒	Built-in native integrations with endpoint, email, and network provide deeper expertise on cross control use cases. **CrowdStrike** "native" integrations are endpoint-centric with no network or email.
	Persona-centric views	☑	⊠	Personal based Helix UI is focused on providing optimized usability experiences for different personas. **CrowdStrike** user roles options are quite granular for different user roles.

Legend	☑	Full coverage	⊠	Partial Coverage	☒	No Coverage

Trellix

Contact and Docs

Partner Care Team here to help with:

Partner Care

partnercareemea@trellix.com

- Partner Portal & Service Portal
- Product/Licensing queries
- Profitability programs
- Partner Registration
- Partner Update/Certification
- NFR Depot
- Reports
- Training/Partner Onboarding
- Lab Access

MSP Partner Care
msppartnercare@trellix.com

- iAsset access
- Partner training: iAsset, PBC, MSP program, Download center
- Partner Business center (PBC), Reporting
- Product & Licensing
- BPS Portal
- Billing
- Tenant
- Name and address updation on MSP accounts

Trellix

Partner SE Technical Bookmarks

Product Technical Documentation Portal

- Product Documentation:
- https://docs.trellix.com/

- Administratorion Guides
- Deployment Guides
- System Security Guides
- Release Notes
- Hardware Guides
- Reference Guides

Cloud Lab

- CrossFire (ASH):
- https://login.trellix.com/

Communication

Partner Care Team

- partnercareemea@trellix.com

- MSP Partner Care Team
- **msppartnercare@trellix.com**

Expert Center

Knowledge Base

Forum

- Trellix-F Community:
- https://community.fireeye.com/
- Trellix-M Community:
- https://communitym.trellix.com/
  Consolidation in progress…

Trellix

Thank You!