Trellix

24-26 OCTOBER 2023

EMEA Security Summit

Rome, Italy

Trellix

Elevating the SOC Analyst Experience with XDR

Tanja Hofmann
Principal Solutions Engineer

Henrik Olsson
Senior Product Line Manager

November 10, 2023

The typical SOC environment

Too many alerts:

10k

Typical company's daily alerts

Too many ignored alerts:

35%

Alerts that are ignored

Too many tools:

85

Average number of security tools in use

Lack of visibility:

99days

Average time to discover a breach

Lack of fast responses:

32days

Average time to respond to a breach

Slow triage:

30min

Average time to triage a single alert

Trellix

And SOCs struggle to keep up with threat landscape

Siloed tools that don't work together

Fragmented visibility and control

Limited org resources and expertise

Over-worked teams and insufficient threat coverage

Too many alerts and missed threats

Alert fatigue and high-risk exposure

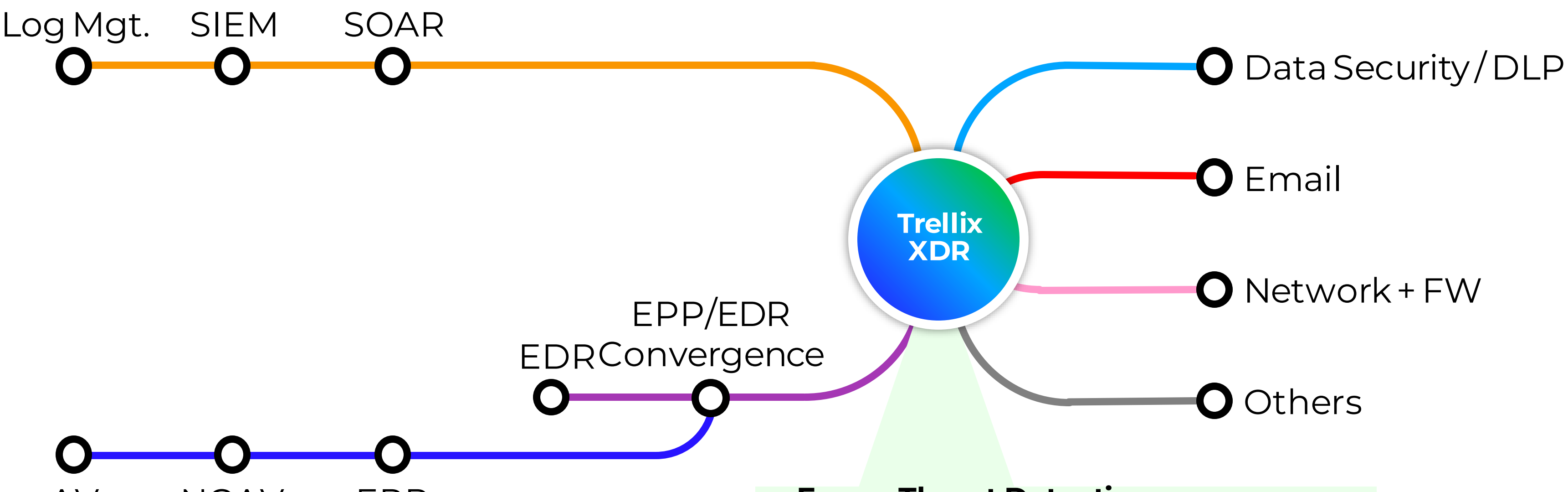
Expensive infrastructure

Costly to maintain and operate

Result = Increased Risk to the Organization

XDR Market Dynamics

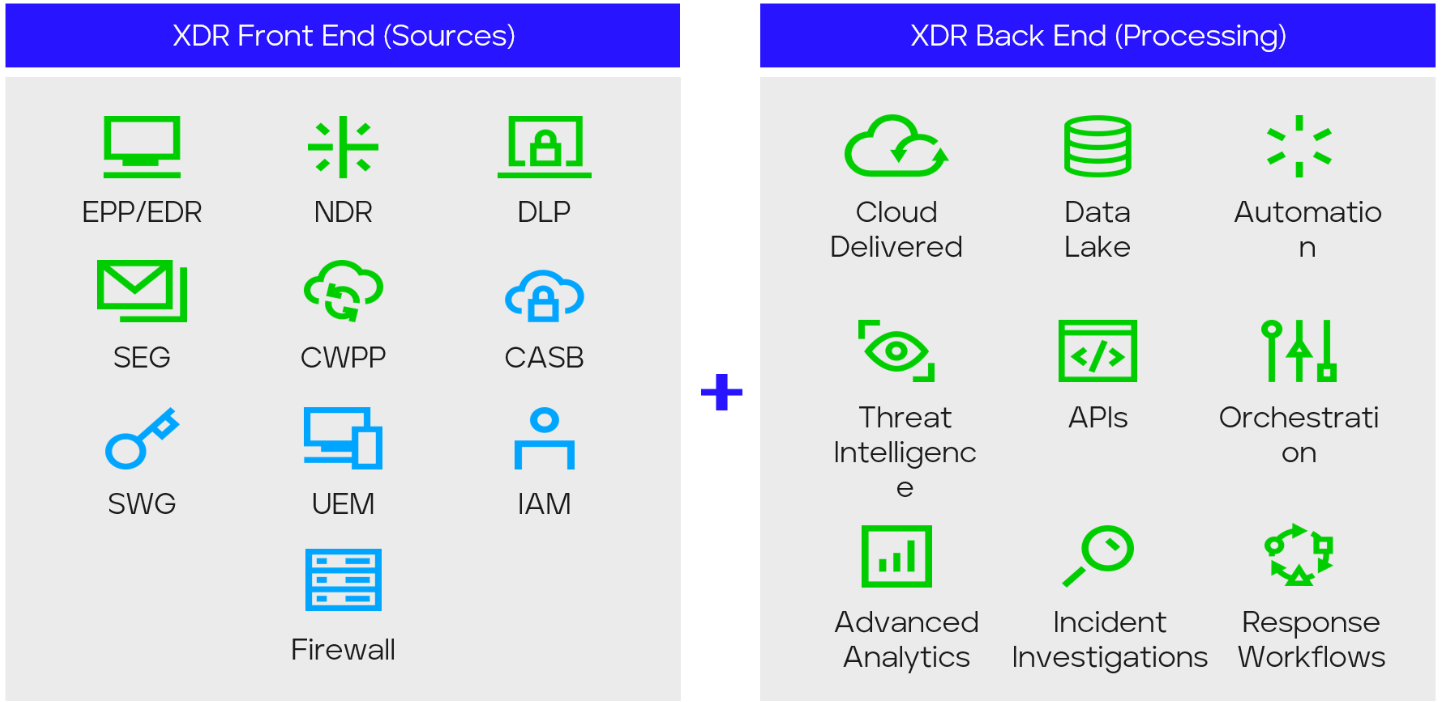
XDR represents an evolutionary convergence EPP/EDR/NDR/AV as well as SIEM/SOAR capabilities to offer better threat intelligence, detection, response and remediation



- **Focus: Threat Detection, Investigation and Response**
- Broad telemetry sources
- Integrated, automated response actions
- Turnkey – OOTB detections and response
- Open / Native XDR

XDR – Merges Controls, Control Management and Sec Ops Capability

Gartner's Point of view



XDR Front End (Sources)

EPP/EDR

NDR

DLP

SEG

CWPP

CASB

SWG

UEM

IAM

Firewall

+

XDR Back End (Processing)

Cloud
Delivered

Data
Lake

Automatio
n

Threat
Intelligenc
e

APIs

Orchestrati
on

Advanced
Analytics

Incident
Investigations

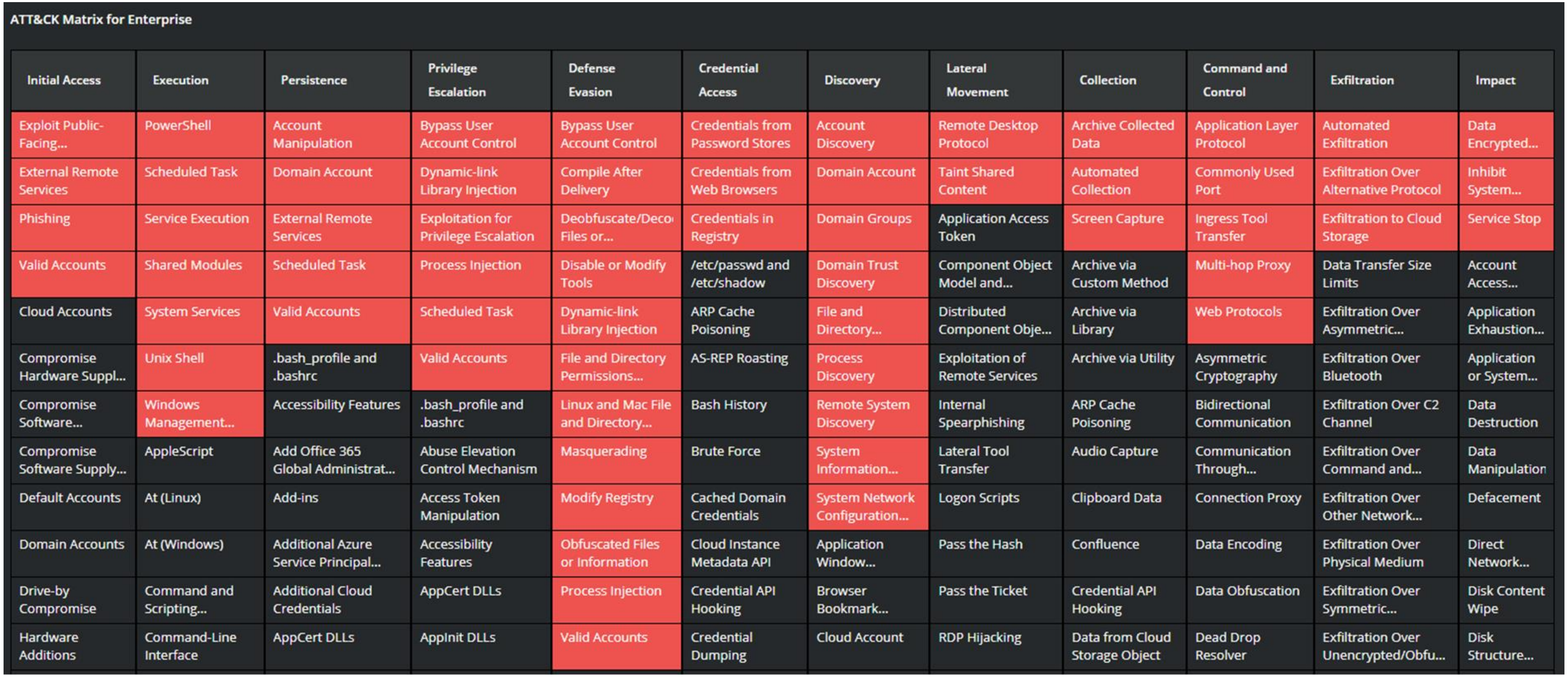
Response
Workflows

Gartner XDR Market Guide 2021

🟩 Native Trellix Capability

🟦 Partner Opportunity

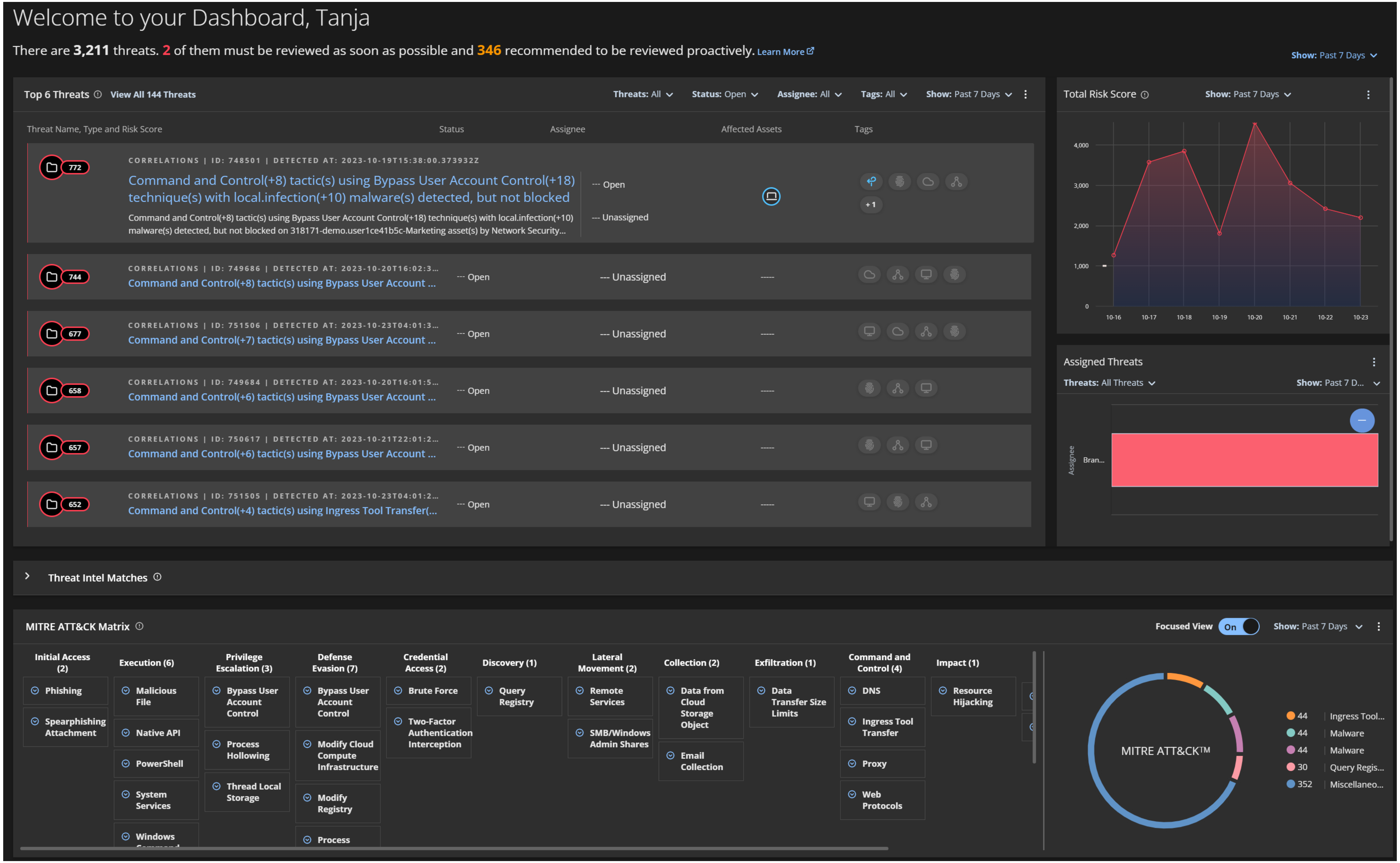
Threat Actor – MITRE ATT&CK Matrix



ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
🟥 Exploit Public-Facing...	🟥 PowerShell	🟥 Account Manipulation	🟥 Bypass User Account Control	🟥 Bypass User Account Control	🟥 Credentials from Password Stores	🟥 Account Discovery	🟥 Remote Desktop Protocol	🟥 Archive Collected Data	🟥 Application Layer Protocol	🟥 Automated Exfiltration	🟥 Data Encrypted...
🟥 External Remote Services	🟥 Scheduled Task	🟥 Domain Account	🟥 Dynamic-link Library Injection	🟥 Compile After Delivery	🟥 Credentials from Web Browsers	🟥 Domain Account	🟥 Taint Shared Content	🟥 Automated Collection	🟥 Commonly Used Port	🟥 Exfiltration Over Alternative Protocol	🟥 Inhibit System...
🟥 Phishing	🟥 Service Execution	🟥 External Remote Services	🟥 Exploitation for Privilege Escalation	🟥 Deobfuscate/Deco Files or...	🟥 Credentials in Registry	🟥 Domain Groups	Application Access Token	🟥 Screen Capture	🟥 Ingress Tool Transfer	🟥 Exfiltration to Cloud Storage	🟥 Service Stop
🟥 Valid Accounts	🟥 Shared Modules	🟥 Scheduled Task	🟥 Process Injection	🟥 Disable or Modify Tools	/etc/passwd and /etc/shadow	🟥 Domain Trust Discovery	Component Object Model and...	Archive via Custom Method	🟥 Multi-hop Proxy	Data Transfer Size Limits	Account Access...
Cloud Accounts	🟥 System Services	🟥 Valid Accounts	🟥 Scheduled Task	🟥 Dynamic-link Library Injection	ARP Cache Poisoning	🟥 File and Directory...	Distributed Component Obje...	Archive via Library	🟥 Web Protocols	Exfiltration Over Asymmetric...	Application Exhaustion...
Compromise Hardware Suppl...	🟥 Unix Shell	.bash_profile and .bashrc	🟥 Valid Accounts	🟥 File and Directory Permissions...	AS-REP Roasting	🟥 Process Discovery	Exploitation of Remote Services	Archive via Utility	Asymmetric Cryptography	Exfiltration Over Bluetooth	Application or System...
Compromise Software...	🟥 Windows Management...	Accessibility Features	.bash_profile and .bashrc	🟥 Linux and Mac File and Directory...	Bash History	🟥 Remote System Discovery	Internal Spearphishing	ARP Cache Poisoning	Bidirectional Communication	Exfiltration Over C2 Channel	Data Destruction
Compromise Software Supply...	AppleScript	Add Office 365 Global Administrat...	Abuse Elevation Control Mechanism	🟥 Masquerading	Brute Force	🟥 System Information...	Lateral Tool Transfer	Audio Capture	Communication Through...	Exfiltration Over Command and...	Data Manipulation
Default Accounts	At (Linux)	Add-ins	Access Token Manipulation	🟥 Modify Registry	Cached Domain Credentials	🟥 System Network Configuration...	Logon Scripts	Clipboard Data	Connection Proxy	Exfiltration Over Other Network...	Defacement
Domain Accounts	At (Windows)	Additional Azure Service Principal...	Accessibility Features	🟥 Obfuscated Files or Information	Cloud Instance Metadata API	Application Window...	Pass the Hash	Confluence	Data Encoding	Exfiltration Over Physical Medium	Direct Network...
Drive-by Compromise	Command and Scripting...	Additional Cloud Credentials	AppCert DLLs	🟥 Process Injection	Credential API Hooking	Browser Bookmark...	Pass the Ticket	Credential API Hooking	Data Obfuscation	Exfiltration Over Symmetric...	Disk Content Wipe
Hardware Additions	Command-Line Interface	AppCert DLLs	AppInit DLLs	🟥 Valid Accounts	Credential Dumping	Cloud Account	RDP Hijacking	Data from Cloud Storage Object	Dead Drop Resolver	Exfiltration Over Unencrypted/Obfu...	Disk Structure...

DEMO



Welcome to your Dashboard, Tanja

There are **3,211** threats. **2** of them must be reviewed as soon as possible and **346** recommended to be reviewed proactively. Learn More

Show: Past 7 Days

Top 6 Threats ⓘ **View All 144 Threats**

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

Threat Name, Type and Risk Score	Status	Assignee	Affected Assets	Tags
772 CORRELATIONS | ID: 748501 | DETECTED AT: 2023-10-19T15:38:00.373932Z Command and Control(+8) tactic(s) using Bypass User Account Control(+18) technique(s) with local.infection(+10) malware(s) detected, but not blocked Command and Control(+8) tactic(s) using Bypass User Account Control(+18) technique(s) with local.infection(+10) malware(s) detected, but not blocked on 318171-demo.user1ce41b5c-Marketing asset(s) by Network Security...	--- Open	--- Unassigned		+1
744 CORRELATIONS | ID: 749686 | DETECTED AT: 2023-10-20T16:02:3... Command and Control(+8) tactic(s) using Bypass User Account ...	--- Open	--- Unassigned	-----	
677 CORRELATIONS | ID: 751506 | DETECTED AT: 2023-10-23T04:01:3... Command and Control(+7) tactic(s) using Bypass User Account ...	--- Open	--- Unassigned	-----	
658 CORRELATIONS | ID: 749684 | DETECTED AT: 2023-10-20T16:01:5... Command and Control(+6) tactic(s) using Bypass User Account ...	--- Open	--- Unassigned	-----	
657 CORRELATIONS | ID: 750617 | DETECTED AT: 2023-10-21T22:01:2... Command and Control(+6) tactic(s) using Bypass User Account ...	--- Open	--- Unassigned	-----	
652 CORRELATIONS | ID: 751505 | DETECTED AT: 2023-10-23T04:01:2... Command and Control(+4) tactic(s) using Ingress Tool Transfer(...	--- Open	--- Unassigned	-----	

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

Assigned Threats

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

› **Threat Intel Matches** ⓘ

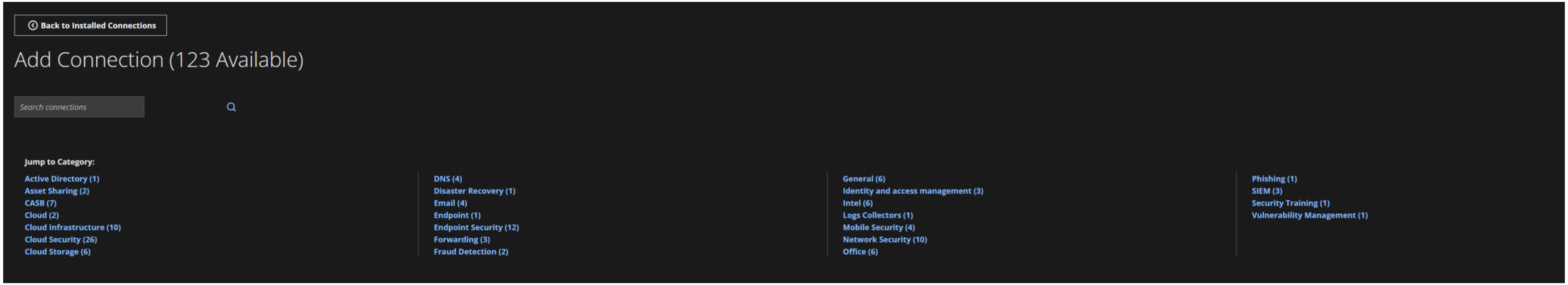
MITRE ATT&CK Matrix ⓘ

Focused View On **Show:** Past 7 Days

Initial Access (2)	Execution (6)	Privilege Escalation (3)	Defense Evasion (7)	Credential Access (2)	Discovery (1)	Lateral Movement (2)	Collection (2)	Exfiltration (1)	Command and Control (4)	Impact (1)
Phishing	Malicious File	Bypass User Account Control	Bypass User Account Control	Brute Force	Query Registry	Remote Services	Data from Cloud Storage Object	Data Transfer Size Limits	DNS	Resource Hijacking
Spearphishing Attachment	Native API	Process Hollowing	Modify Cloud Compute Infrastructure	Two-Factor Authentication Interception		SMB/Windows Admin Shares	Email Collection		Ingress Tool Transfer	
	PowerShell	Thread Local Storage	Modify Registry						Proxy	
	System Services		Process						Web Protocols	
	Windows									

🟠	44	Ingress Tool...
🟢	44	Malware
🟣	44	Malware
🔴	30	Query Regis...
🔵	352	Miscellaneo...

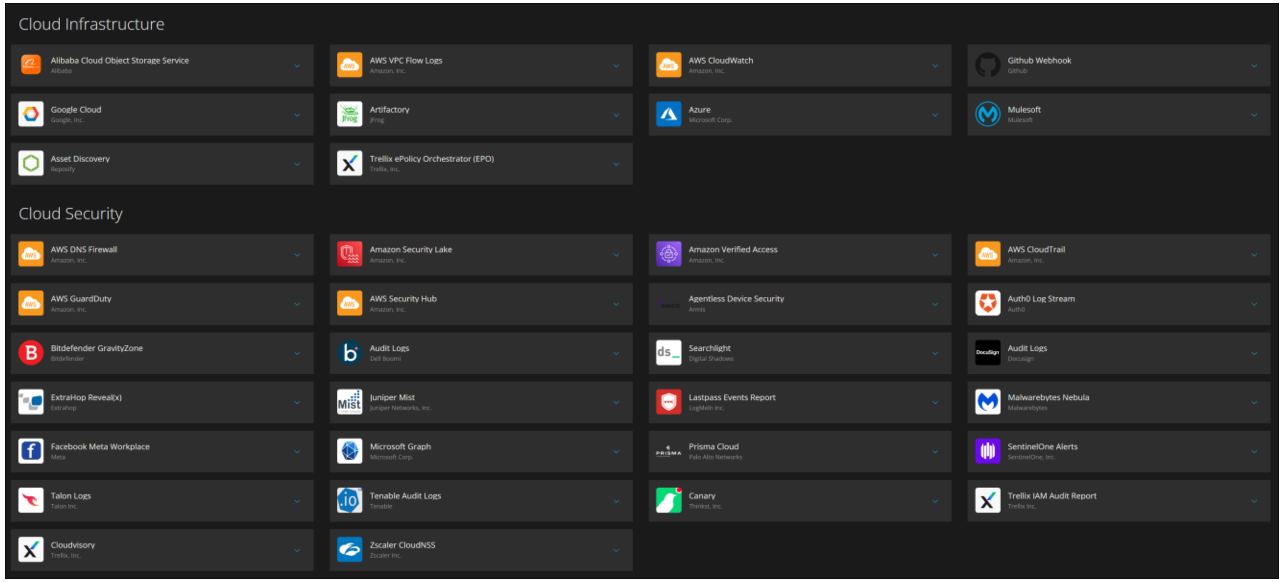
Trellix



Add Connection (123 Available)

Jump to Category:

- Active Directory (1)
- Asset Sharing (2)
- CASB (7)
- Cloud (2)
- Cloud Infrastructure (10)
- Cloud Security (26)
- Cloud Storage (6)
- DNS (4)
- Disaster Recovery (1)
- Email (4)
- Endpoint (1)
- Endpoint Security (12)
- Forwarding (3)
- Fraud Detection (2)
- General (6)
- Identity and access management (3)
- Intel (6)
- Logs Collectors (1)
- Mobile Security (4)
- Network Security (10)
- Office (6)
- Phishing (1)
- SIEM (3)
- Security Training (1)
- Vulnerability Management (1)

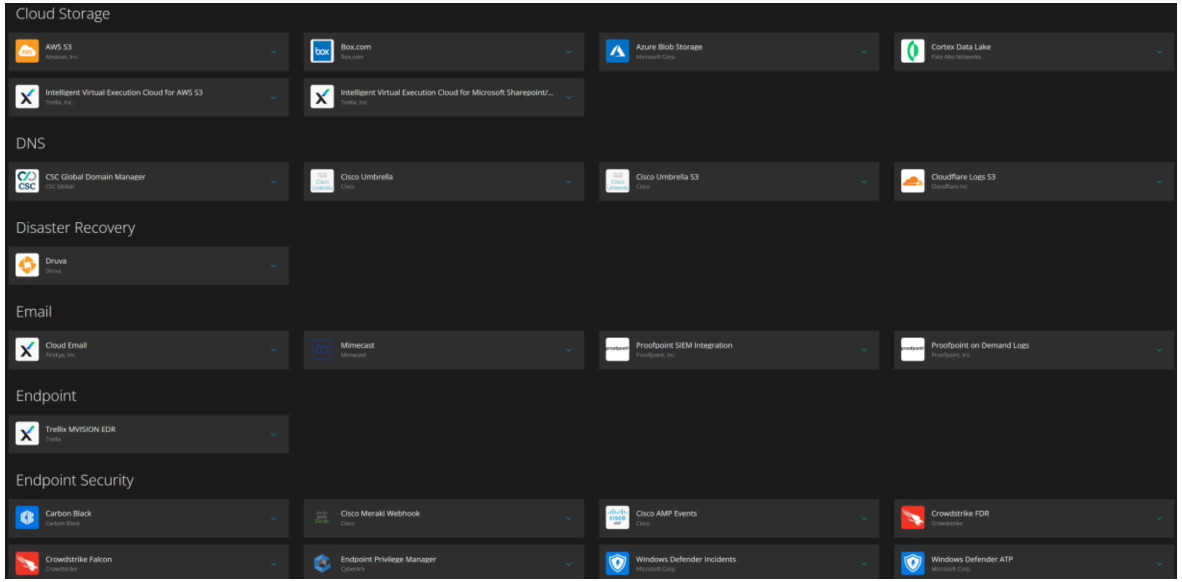


Cloud Infrastructure

- Alibaba Cloud Object Storage Service
  Alibaba
- AWS VPC Flow Logs
  Amazon, Inc.
- AWS CloudWatch
  Amazon, Inc.
- Github Webhook
  Github
- Google Cloud
  Google, Inc.
- Artifactory
  JFrog
- Azure
  Microsoft Corp.
- Mulesoft
  Mulesoft
- Asset Discovery
  Reposify
- Trellix ePolicy Orchestrator (EPO)
  Trellix, Inc.

Cloud Security

- AWS DNS Firewall
  Amazon, Inc.
- Amazon Security Lake
  Amazon, Inc.
- Amazon Verified Access
  Amazon, Inc.
- AWS CloudTrail
  Amazon, Inc.
- AWS GuardDuty
  Amazon, Inc.
- AWS Security Hub
  Amazon, Inc.
- Agentless Device Security
  Armis
- Auth0 Log Stream
  Auth0
- Bitdefender GravityZone
  Bitdefender
- Audit Logs
  Dell Boomi
- Searchlight
  Digital Shadows
- Audit Logs
  Docusign
- ExtraHop Reveal(x)
  Extrahop
- Juniper Mist
  Juniper Networks, Inc.
- Lastpass Events Report
  LogMeIn Inc.
- Malwarebytes Nebula
  Malwarebytes
- Facebook Meta Workplace
  Meta
- Microsoft Graph
  Microsoft Corp.
- Prisma Cloud
  Palo Alto Networks
- SentinelOne Alerts
  SentinelOne, Inc.
- Talon Logs
  Talon Inc.
- Tenable Audit Logs
  Tenable
- Canary
  Thinkst, Inc.
- Trellix IAM Audit Report
  Trellix Inc.
- Cloudvisory
  Trellix, Inc.
- Zscaler CloudNSS
  Zscaler Inc.



Cloud Storage

- AWS S3
  Amazon, Inc.
- Box.com
  Box.com
- Azure Blob Storage
  Microsoft Corp.
- Cortex Data Lake
  Palo Alto Networks
- Intelligent Virtual Execution Cloud for AWS S3
  Trellix, Inc.
- Intelligent Virtual Execution Cloud for Microsoft Sharepoint/...
  Trellix, Inc.

DNS

- CSC Global Domain Manager
  CSC Global
- Cisco Umbrella
  Cisco
- Cisco Umbrella S3
  Cisco
- Cloudflare Logs S3
  Cloudflare Inc

Disaster Recovery

- Druva
  Druva

Email

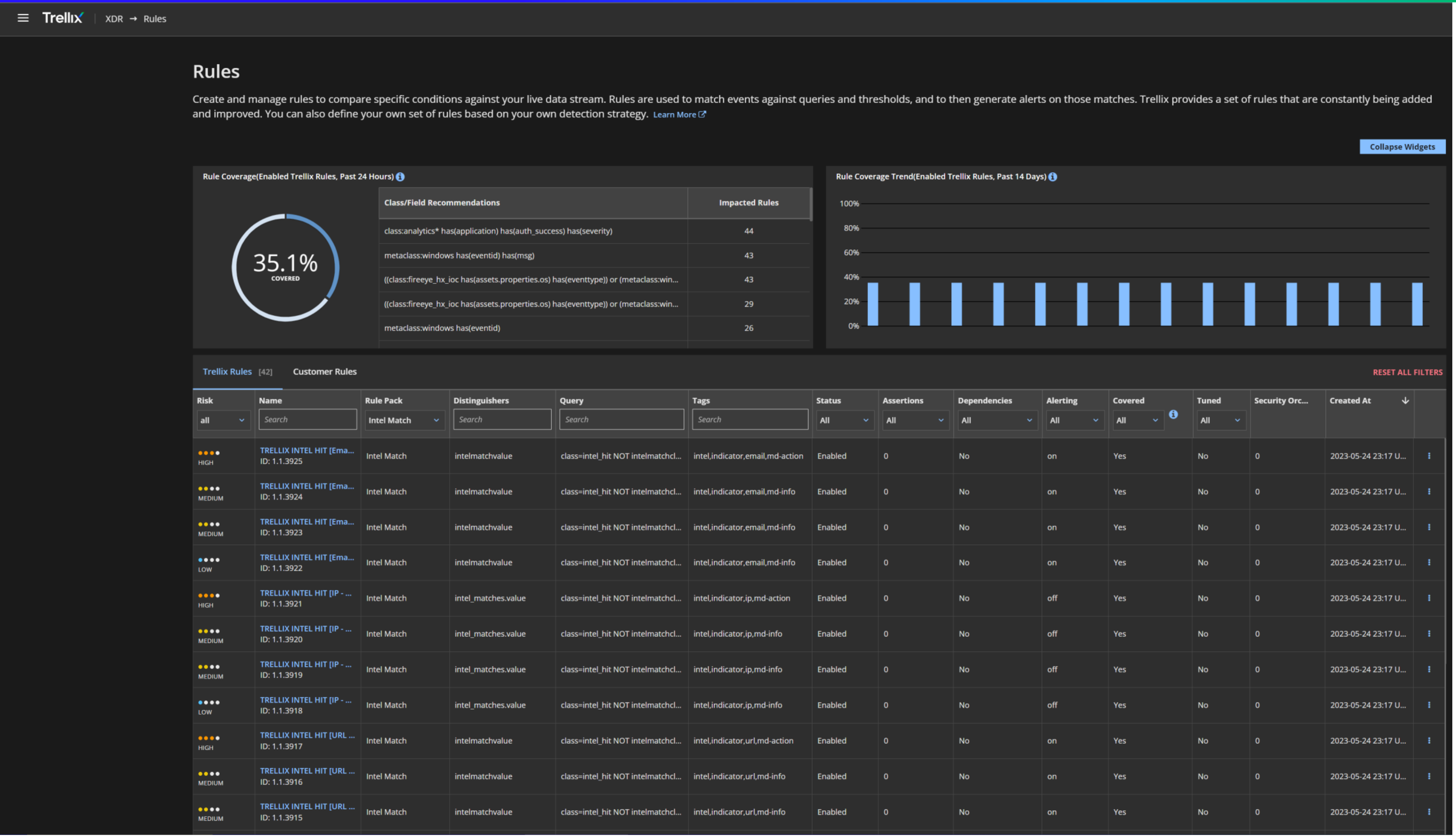
- Cloud Email
  FireEye, Inc.
- Mimecast
  Mimecast
- Proofpoint SIEM Integration
  Proofpoint, Inc.
- Proofpoint on Demand Logs
  Proofpoint, Inc.

Endpoint

- Trellix MVISION EDR
  Trellix

Endpoint Security

- 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.



Rules

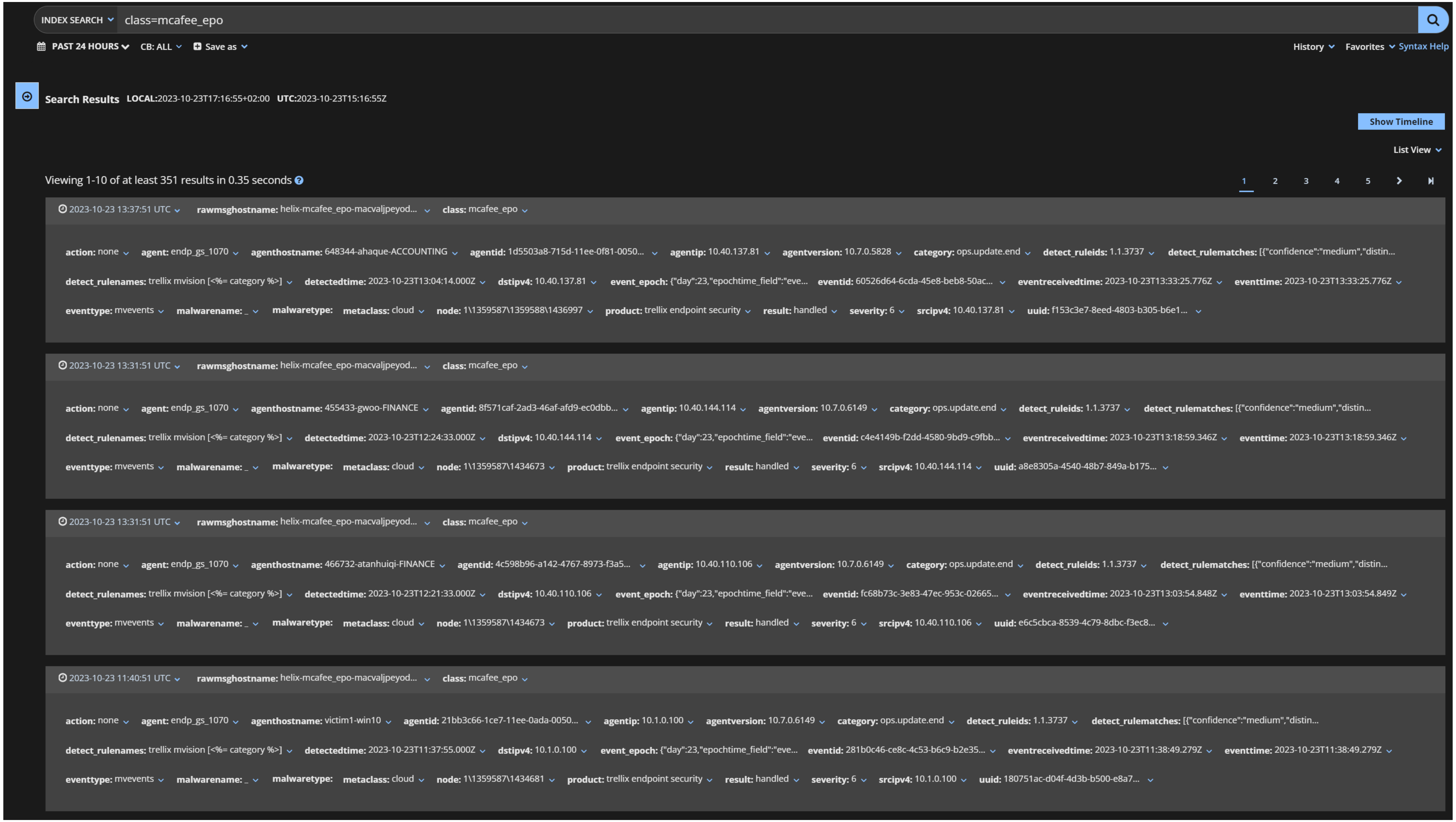
Create and manage rules to compare specific conditions against your live data stream. Rules are used to match events against queries and thresholds, and to then generate alerts on those matches. Trellix provides a set of rules that are constantly being added and improved. You can also define your own set of rules based on your own detection strategy. Learn More

Rule Coverage(Enabled Trellix Rules, Past 24 Hours)

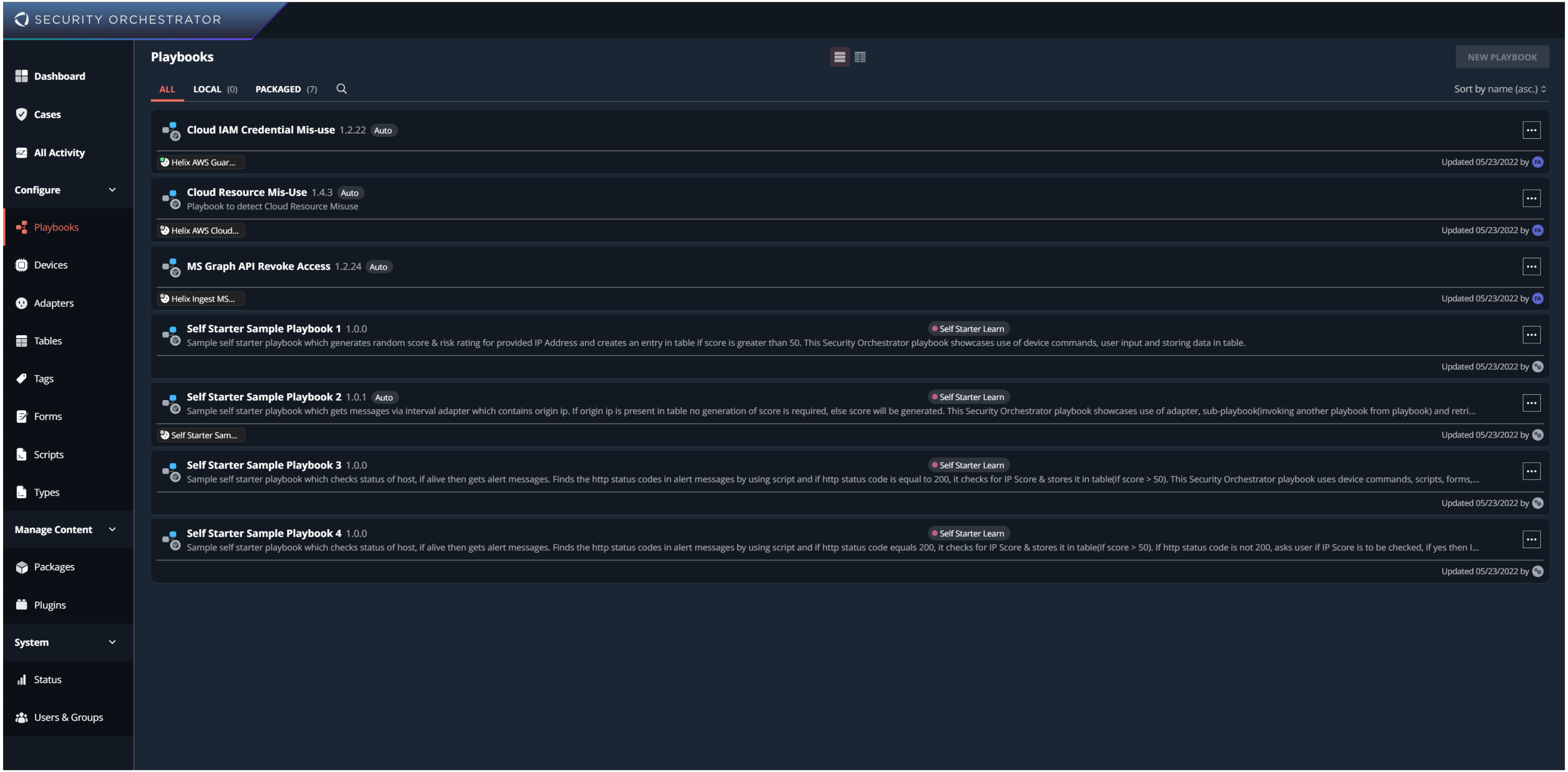
Class/Field Recommendations	Impacted Rules
class:analytics* has(application) has(auth_success) has(severity)	44
metaclass:windows has(eventid) has(msg)	43
((class:fireeye_hx_ioc has(assets.properties.os) has(eventtype)) or (metaclass:win...	43
((class:fireeye_hx_ioc has(assets.properties.os) has(eventtype)) or (metaclass:win...	29
metaclass:windows has(eventid)	26

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

Risk	Name	Rule Pack	Distinguishers	Query	Tags	Status	Assertions	Dependencies	Alerting	Covered	Tuned	Security Orc...	Created At
all	Search	Intel Match	Search	Search	Search	All	All	All	All	All	All		
●●●● HIGH	TRELLIX INTEL HIT [Ema... ID: 1.1.3925	Intel Match	intelmatchvalue	class=intel_hit NOT intelmatchcl...	intel,indicator,email,md-action	Enabled	0	No	on	Yes	No	0	2023-05-24 23:17 U...
●●●● MEDIUM	TRELLIX INTEL HIT [Ema... ID: 1.1.3924	Intel Match	intelmatchvalue	class=intel_hit NOT intelmatchcl...	intel,indicator,email,md-info	Enabled	0	No	on	Yes	No	0	2023-05-24 23:17 U...
●●●● MEDIUM	TRELLIX INTEL HIT [Ema... ID: 1.1.3923	Intel Match	intelmatchvalue	class=intel_hit NOT intelmatchcl...	intel,indicator,email,md-info	Enabled	0	No	on	Yes	No	0	2023-05-24 23:17 U...
●●●● LOW	TRELLIX INTEL HIT [Ema... ID: 1.1.3922	Intel Match	intelmatchvalue	class=intel_hit NOT intelmatchcl...	intel,indicator,email,md-info	Enabled	0	No	on	Yes	No	0	2023-05-24 23:17 U...
●●●● HIGH	TRELLIX INTEL HIT [IP - ... ID: 1.1.3921	Intel Match	intel_matches.value	class=intel_hit NOT intelmatchcl...	intel,indicator,ip,md-action	Enabled	0	No	off	Yes	No	0	2023-05-24 23:17 U...
●●●● MEDIUM	TRELLIX INTEL HIT [IP - ... ID: 1.1.3920	Intel Match	intel_matches.value	class=intel_hit NOT intelmatchcl...	intel,indicator,ip,md-info	Enabled	0	No	off	Yes	No	0	2023-05-24 23:17 U...
●●●● MEDIUM	TRELLIX INTEL HIT [IP - ... ID: 1.1.3919	Intel Match	intel_matches.value	class=intel_hit NOT intelmatchcl...	intel,indicator,ip,md-info	Enabled	0	No	off	Yes	No	0	2023-05-24 23:17 U...
●●●● LOW	TRELLIX INTEL HIT [IP - ... ID: 1.1.3918	Intel Match	intel_matches.value	class=intel_hit NOT intelmatchcl...	intel,indicator,ip,md-info	Enabled	0	No	off	Yes	No	0	2023-05-24 23:17 U...
●●●● HIGH	TRELLIX INTEL HIT [URL ... ID: 1.1.3917	Intel Match	intelmatchvalue	class=intel_hit NOT intelmatchcl...	intel,indicator,url,md-action	Enabled	0	No	on	Yes	No	0	2023-05-24 23:17 U...
●●●● MEDIUM	TRELLIX INTEL HIT [URL ... ID: 1.1.3916	Intel Match	intelmatchvalue	class=intel_hit NOT intelmatchcl...	intel,indicator,url,md-info	Enabled	0	No	on	Yes	No	0	2023-05-24 23:17 U...
●●●● MEDIUM	TRELLIX INTEL HIT [URL ... ID: 1.1.3915	Intel Match	intelmatchvalue	class=intel_hit NOT intelmatchcl...	intel,indicator,url,md-info	Enabled	0	No	on	Yes	No	0	2023-05-24 23:17 U...



```
LOCAL:2023-10-23T17:16:55+02:00  UTC:2023-10-23T15:16:55Z

Viewing 1-10 of at least 351 results in 0.35 seconds

2023-10-23 13:37:51 UTC   rawmsghostname: helix-mcafee_epo-macvaljpeyod...   class: mcafee_epo

action: none   agent: endp_gs_1070   agenthostname: 648344-ahaque-ACCOUNTING   agentid: 1d5503a8-715d-11ee-0f81-0050...   agentip: 10.40.137.81   agentversion: 10.7.0.5828   category: ops.update.end   detect_ruleids: 1.1.3737   detect_rulematches: [{"confidence":"medium","distin...
detect_rulenames: trellix mvision [<%= category %>]   detectedtime: 2023-10-23T13:04:14.000Z   dstipv4: 10.40.137.81   event_epoch: {"day":23,"epochtime_field":"eve...   eventid: 60526d64-6cda-45e8-beb8-50ac...   eventreceivedtime: 2023-10-23T13:33:25.776Z   eventtime: 2023-10-23T13:33:25.776Z
eventtype: mvevents   malwarename: _   malwaretype:   metaclass: cloud   node: 1\1359587\1359588\1436997   product: trellix endpoint security   result: handled   severity: 6   srcipv4: 10.40.137.81   uuid: f153c3e7-8eed-4803-b305-b6e1...

2023-10-23 13:31:51 UTC   rawmsghostname: helix-mcafee_epo-macvaljpeyod...   class: mcafee_epo

action: none   agent: endp_gs_1070   agenthostname: 455433-gwoo-FINANCE   agentid: 8f571caf-2ad3-46af-afd9-ec0dbb...   agentip: 10.40.144.114   agentversion: 10.7.0.6149   category: ops.update.end   detect_ruleids: 1.1.3737   detect_rulematches: [{"confidence":"medium","distin...
detect_rulenames: trellix mvision [<%= category %>]   detectedtime: 2023-10-23T12:24:33.000Z   dstipv4: 10.40.144.114   event_epoch: {"day":23,"epochtime_field":"eve...   eventid: c4e4149b-f2dd-4580-9bd9-c9fbb...   eventreceivedtime: 2023-10-23T13:18:59.346Z   eventtime: 2023-10-23T13:18:59.346Z
eventtype: mvevents   malwarename: _   malwaretype:   metaclass: cloud   node: 1\1359587\1434673   product: trellix endpoint security   result: handled   severity: 6   srcipv4: 10.40.144.114   uuid: a8e8305a-4540-48b7-849a-b175...

2023-10-23 13:31:51 UTC   rawmsghostname: helix-mcafee_epo-macvaljpeyod...   class: mcafee_epo

action: none   agent: endp_gs_1070   agenthostname: 466732-atanhuiqi-FINANCE   agentid: 4c598b96-a142-4767-8973-f3a5...   agentip: 10.40.110.106   agentversion: 10.7.0.6149   category: ops.update.end   detect_ruleids: 1.1.3737   detect_rulematches: [{"confidence":"medium","distin...
detect_rulenames: trellix mvision [<%= category %>]   detectedtime: 2023-10-23T12:21:33.000Z   dstipv4: 10.40.110.106   event_epoch: {"day":23,"epochtime_field":"eve...   eventid: fc68b73c-3e83-47ec-953c-02665...   eventreceivedtime: 2023-10-23T13:03:54.848Z   eventtime: 2023-10-23T13:03:54.849Z
eventtype: mvevents   malwarename: _   malwaretype:   metaclass: cloud   node: 1\1359587\1434673   product: trellix endpoint security   result: handled   severity: 6   srcipv4: 10.40.110.106   uuid: e6c5cbca-8539-4c79-8dbc-f3ec8...

2023-10-23 11:40:51 UTC   rawmsghostname: helix-mcafee_epo-macvaljpeyod...   class: mcafee_epo

action: none   agent: endp_gs_1070   agenthostname: victim1-win10   agentid: 21bb3c66-1ce7-11ee-0ada-0050...   agentip: 10.1.0.100   agentversion: 10.7.0.6149   category: ops.update.end   detect_ruleids: 1.1.3737   detect_rulematches: [{"confidence":"medium","distin...
detect_rulenames: trellix mvision [<%= category %>]   detectedtime: 2023-10-23T11:37:55.000Z   dstipv4: 10.1.0.100   event_epoch: {"day":23,"epochtime_field":"eve...   eventid: 281b0c46-ce8c-4c53-b6c9-b2e35...   eventreceivedtime: 2023-10-23T11:38:49.279Z   eventtime: 2023-10-23T11:38:49.279Z
eventtype: mvevents   malwarename: _   malwaretype:   metaclass: cloud   node: 1\1359587\1434681   product: trellix endpoint security   result: handled   severity: 6   srcipv4: 10.1.0.100   uuid: 180751ac-d04f-4d3b-b500-e8a7...
```



Playbooks

Cloud IAM Credential Mis-use 1.2.22 Auto
Helix AWS Guar...
Updated 05/23/2022 by

Cloud Resource Mis-Use 1.4.3 Auto
Playbook to detect Cloud Resource Misuse
Helix AWS Cloud...
Updated 05/23/2022 by

MS Graph API Revoke Access 1.2.24 Auto
Helix Ingest MS...
Updated 05/23/2022 by

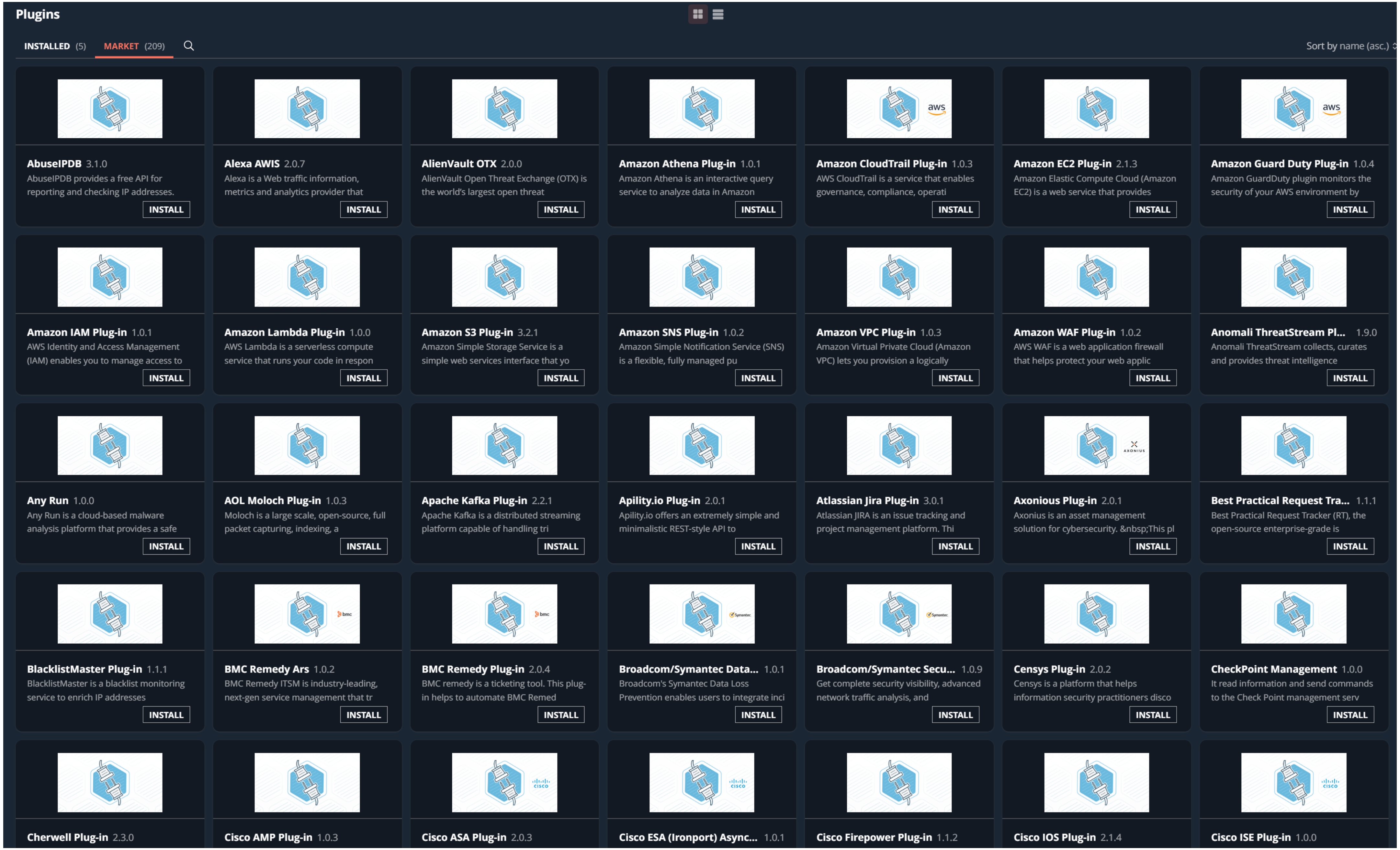
Self Starter Sample Playbook 1 1.0.0 Self Starter Learn
Sample self starter playbook which generates random score & risk rating for provided IP Address and creates an entry in table if score is greater than 50. This Security Orchestrator playbook showcases use of device commands, user input and storing data in table.
Updated 05/23/2022 by

Self Starter Sample Playbook 2 1.0.1 Auto Self Starter Learn
Sample self starter playbook which gets messages via interval adapter which contains origin ip. If origin ip is present in table no generation of score is required, else score will be generated. This Security Orchestrator playbook showcases use of adapter, sub-playbook(invoking another playbook from playbook) and retri...
Self Starter Sam...
Updated 05/23/2022 by

Self Starter Sample Playbook 3 1.0.0 Self Starter Learn
Sample self starter playbook which checks status of host, if alive then gets alert messages. Finds the http status codes in alert messages by using script and if http status code is equal to 200, it checks for IP Score & stores it in table(if score > 50). This Security Orchestrator playbook uses device commands, scripts, forms,...
Updated 05/23/2022 by

Self Starter Sample Playbook 4 1.0.0 Self Starter Learn
Sample self starter playbook which checks status of host, if alive then gets alert messages. Finds the http status codes in alert messages by using script and if http status code equals 200, it checks for IP Score & stores it in table(if score > 50). If http status code is not 200, asks user if IP Score is to be checked, if yes then I...
Updated 05/23/2022 by

Trellix



Plugins

INSTALLED (5) MARKET (209)

Sort by name (asc.)

AbuseIPDB 3.1.0
AbuseIPDB provides a free API for reporting and checking IP addresses.
INSTALL

Alexa AWIS 2.0.7
Alexa is a Web traffic information, metrics and analytics provider that
INSTALL

AlienVault OTX 2.0.0
AlienVault Open Threat Exchange (OTX) is the world's largest open threat
INSTALL

Amazon Athena Plug-in 1.0.1
Amazon Athena is an interactive query service to analyze data in Amazon
INSTALL

Amazon CloudTrail Plug-in 1.0.3
AWS CloudTrail is a service that enables governance, compliance, operati
INSTALL

Amazon EC2 Plug-in 2.1.3
Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides
INSTALL

Amazon Guard Duty Plug-in 1.0.4
Amazon GuardDuty plugin monitors the security of your AWS environment by
INSTALL

Amazon IAM Plug-in 1.0.1
AWS Identity and Access Management (IAM) enables you to manage access to
INSTALL

Amazon Lambda Plug-in 1.0.0
AWS Lambda is a serverless compute service that runs your code in respon
INSTALL

Amazon S3 Plug-in 3.2.1
Amazon Simple Storage Service is a simple web services interface that yo
INSTALL

Amazon SNS Plug-in 1.0.2
Amazon Simple Notification Service (SNS) is a flexible, fully managed pu
INSTALL

Amazon VPC Plug-in 1.0.3
Amazon Virtual Private Cloud (Amazon VPC) lets you provision a logically
INSTALL

Amazon WAF Plug-in 1.0.2
AWS WAF is a web application firewall that helps protect your web applic
INSTALL

Anomali ThreatStream Pl... 1.9.0
Anomali ThreatStream collects, curates and provides threat intelligence
INSTALL

Any Run 1.0.0
Any Run is a cloud-based malware analysis platform that provides a safe
INSTALL

AOL Moloch Plug-in 1.0.3
Moloch is a large scale, open-source, full packet capturing, indexing, a
INSTALL

Apache Kafka Plug-in 2.2.1
Apache Kafka is a distributed streaming platform capable of handling tri
INSTALL

Apility.io Plug-in 2.0.1
Apility.io offers an extremely simple and minimalistic REST-style API to
INSTALL

Atlassian Jira Plug-in 3.0.1
Atlassian JIRA is an issue tracking and project management platform. Thi
INSTALL

Axonious Plug-in 2.0.1
Axonius is an asset management solution for cybersecurity. This pl
INSTALL

Best Practical Request Tra... 1.1.1
Best Practical Request Tracker (RT), the open-source enterprise-grade is
INSTALL

BlacklistMaster Plug-in 1.1.1
BlacklistMaster is a blacklist monitoring service to enrich IP addresses
INSTALL

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

BMC Remedy Plug-in 2.0.4
BMC remedy is a ticketing tool. This plug-in helps to automate BMC Remed
INSTALL

Broadcom/Symantec Data... 1.0.1
Broadcom's Symantec Data Loss Prevention enables users to integrate inci
INSTALL

Broadcom/Symantec Secu... 1.0.9
Get complete security visibility, advanced network traffic analysis, and
INSTALL

Censys Plug-in 2.0.2
Censys is a platform that helps information security practitioners disco
INSTALL

CheckPoint Management 1.0.0
It read information and send commands to the Check Point management serv
INSTALL

Cherwell Plug-in 2.3.0

Cisco AMP Plug-in 1.0.3

Cisco ASA Plug-in 2.0.3

Cisco ESA (Ironport) Async... 1.0.1

Cisco Firepower Plug-in 1.1.2

Cisco IOS Plug-in 2.1.4

Cisco ISE Plug-in 1.0.0

Trellix

Trellix

XDR Roadmap & Future

Henrik Olsson

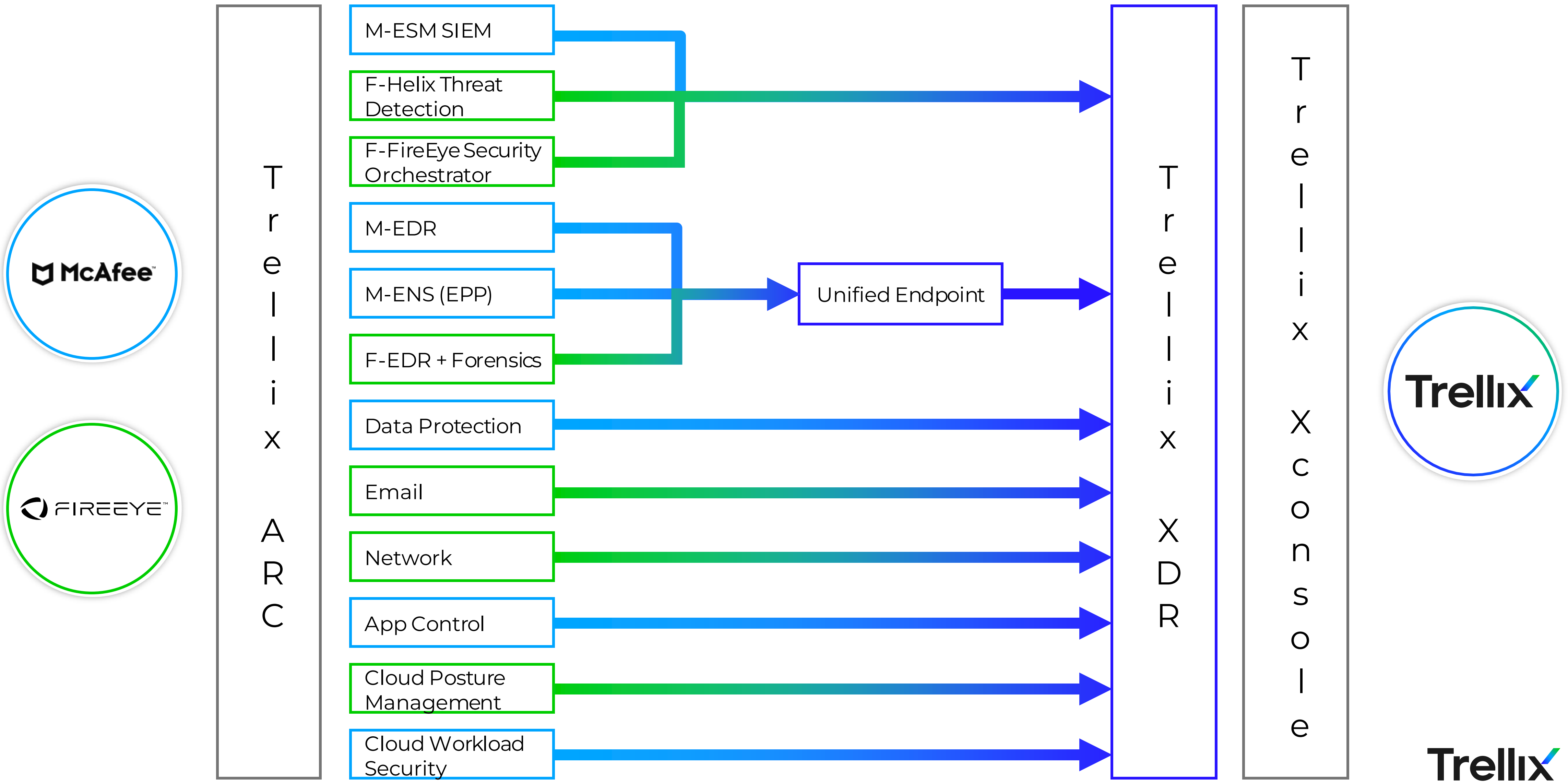
Senior Product Line Manager

Safe Harbor Statement

This slide deck may include roadmap information, projections or other information that might be considered forward-looking. While these forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ.r

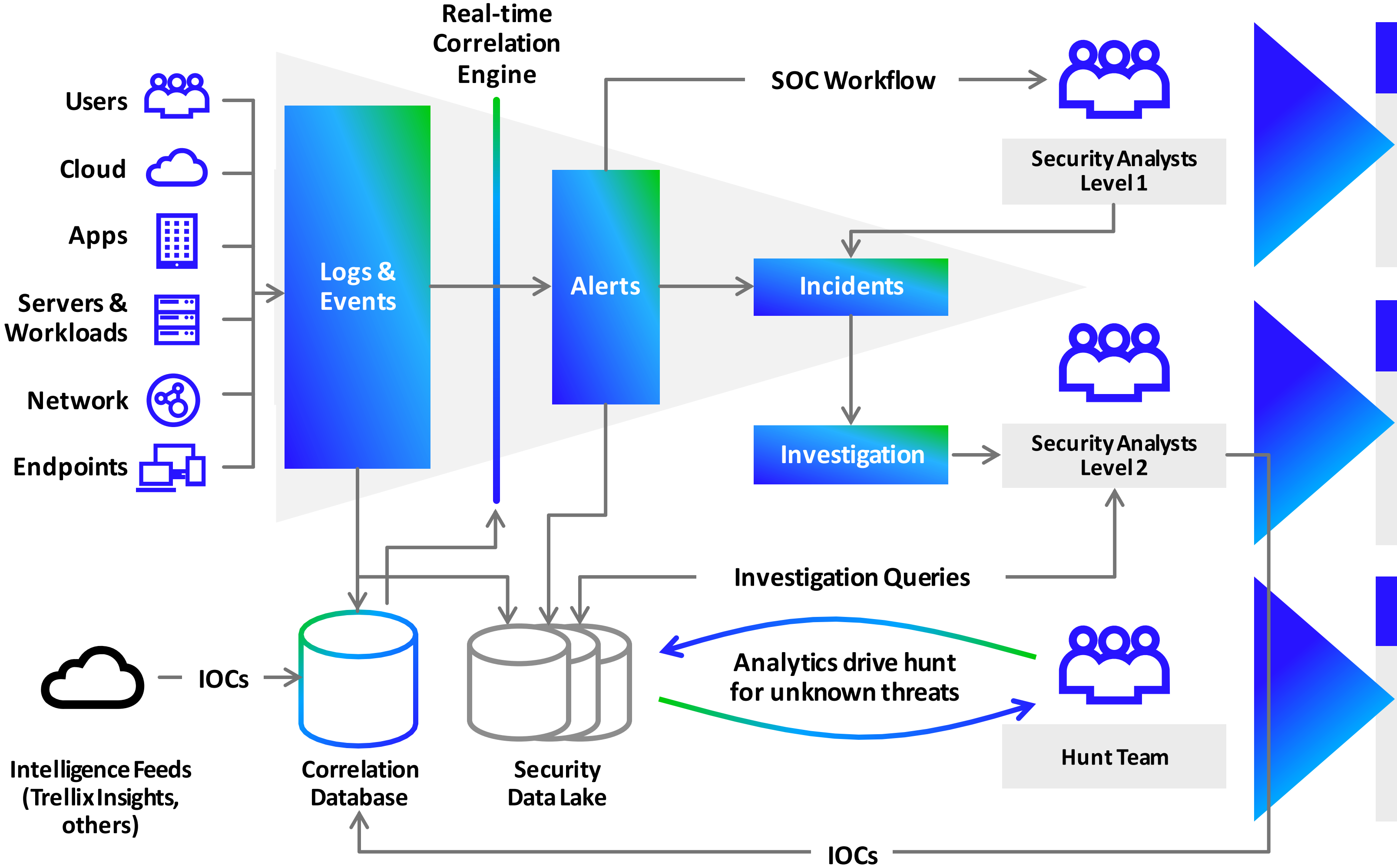
Trellix

Trellix Unified Security Stack



Trellix

SOC Personas and Workflows



SOC Admin

- Configure integrations
- Setups Tasks/Playbooks
- Tune alerts/manage rules

L1: Alert Management

- Monitor alerts
- Identify TP/FP alerts
- Enriched alerts with context
- Acknowledge in < 5 mins

L2: Investigation

- Assess risks and respond
- Run queries across the environment
- Determine attack origin / impact
- Take action

L3: Hunt

- Hunt for unknown threats with deep analytics and machine learning
- Identify new IOCs to improve monitoring

Trellix

XConsole New Unified Apps

Common apps across Unified Endpoint and XDR

Alerting

- Prioritized alerts
- Automatically enriched
- Designed for SOC (multi-monitor etc.)
- Auto respond / Click to respond

Search and Forensics

- Search across data lakes
- Threat intel and enrichment integration
- Saved queries and threat rule creation
- Endpoint data retrieval

Rule Management

- Create monitoring, mitigation and whitelist rules
- Import from standard formats

Integrations Hub

- Click to integrate different sources (data ingest, enrichment, workflow, response, custom)
- Create tasks per integration automatically

Tasks and Playbooks

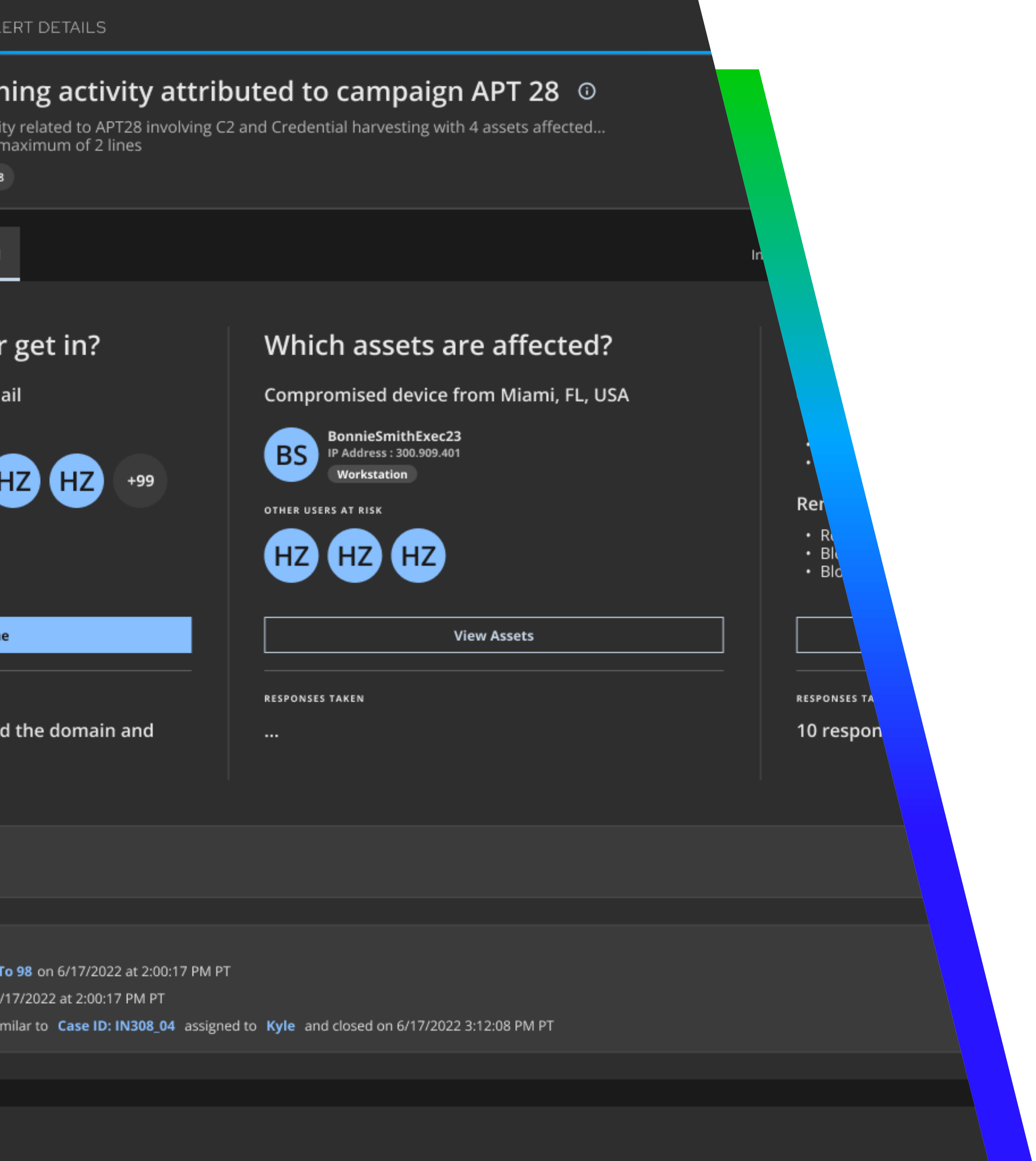
- Low code actions
- Create custom tasks
- Combine tasks into playbooks
- Integrate actions into alerts and rules

Case Management

- Collaboration space
- Assign actions to colleagues
- Integrate and create third party cases

Integrated Workflows Between Apps

Trellix



ERT DETAILS

hing activity attributed to campaign APT 28

ity related to APT28 involving C2 and Credential harvesting with 4 assets affected...
maximum of 2 lines

r get in?

ail

d the domain and

Which assets are affected?

Compromised device from Miami, FL, USA

BonnieSmithExec23
IP Address : 300.909.401
Workstation

OTHER USERS AT RISK

RESPONSES TAKEN

...

Rer
- R
- Bl
- Blo

RESPONSES TA

10 respon

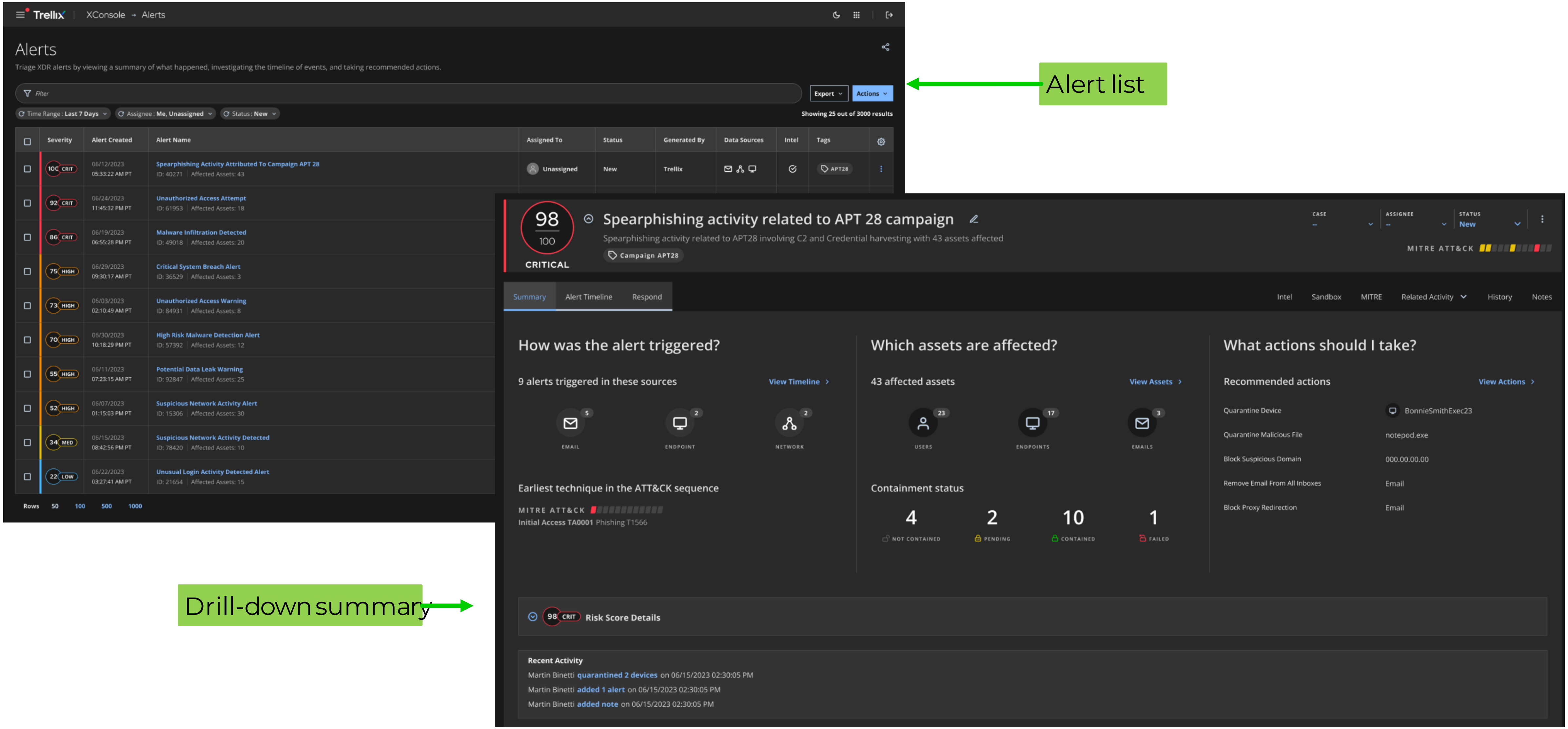
To 98 on 6/17/2022 at 2:00:17 PM PT

/17/2022 at 2:00:17 PM PT

milar to Case ID: IN308_04 assigned to Kyle and closed on 6/17/2022 3:12:08 PM PT

What’s Included – Detailed List

Alerts



Alerts

Triage XDR alerts by viewing a summary of what happened, investigating the timeline of events, and taking recommended actions.

Time Range : Last 7 Days | Assignee : Me, Unassigned | Status : New

Showing 25 out of 3000 results

□	Severity	Alert Created	Alert Name	Assigned To	Status	Generated By	Data Sources	Intel	Tags
□	100 CRIT	06/12/2023 05:33:22 AM PT	Spearphishing Activity Attributed To Campaign APT 28 ID: 40271 | Affected Assets: 43	Unassigned	New	Trellix	✉	✓	APT28
□	92 CRIT	06/24/2023 11:45:32 PM PT	Unauthorized Access Attempt ID: 61953 | Affected Assets: 18						
□	86 CRIT	06/19/2023 06:55:28 PM PT	Malware Infiltration Detected ID: 49018 | Affected Assets: 20						
□	75 HIGH	06/29/2023 09:30:17 AM PT	Critical System Breach Alert ID: 36529 | Affected Assets: 3						
□	73 HIGH	06/03/2023 02:10:49 AM PT	Unauthorized Access Warning ID: 84931 | Affected Assets: 8						
□	70 HIGH	06/30/2023 10:18:29 PM PT	High Risk Malware Detection Alert ID: 57392 | Affected Assets: 12						
□	55 HIGH	06/11/2023 07:23:15 AM PT	Potential Data Leak Warning ID: 92847 | Affected Assets: 25						
□	52 HIGH	06/07/2023 01:15:03 PM PT	Suspicious Network Activity Alert ID: 15306 | Affected Assets: 30						
□	34 MED	06/15/2023 08:42:56 PM PT	Suspicious Network Activity Detected ID: 78420 | Affected Assets: 10						
□	22 LOW	06/22/2023 03:27:41 AM PT	Unusual Login Activity Detected Alert ID: 21654 | Affected Assets: 15						

Rows 50 100 500 1000

98 / 100 CRITICAL

Spearphishing activity related to APT 28 campaign

Spearphishing activity related to APT28 involving C2 and Credential harvesting with 43 assets affected

Campaign APT28

CASE: -- | ASSIGNEE: -- | STATUS: New

How was the alert triggered?

9 alerts triggered in these sources — View Timeline >

EMAIL 5 | ENDPOINT 2 | NETWORK 2

Earliest technique in the ATT&CK sequence

MITRE ATT&CK

Initial Access TA0001 Phishing T1566

Which assets are affected?

43 affected assets — View Assets >

USERS 23 | ENDPOINTS 17 | EMAILS 3

Containment status

4 NOT CONTAINED | 2 PENDING | 10 CONTAINED | 1 FAILED

What actions should I take?

Recommended actions — View Actions >

Quarantine Device	BonnieSmithExec23
Quarantine Malicious File	notepod.exe
Block Suspicious Domain	000.00.00.00
Remove Email From All Inboxes	Email
Block Proxy Redirection	Email

98 CRIT Risk Score Details

Recent Activity

Martin Binetti quarantined 2 devices on 06/15/2023 02:30:05 PM

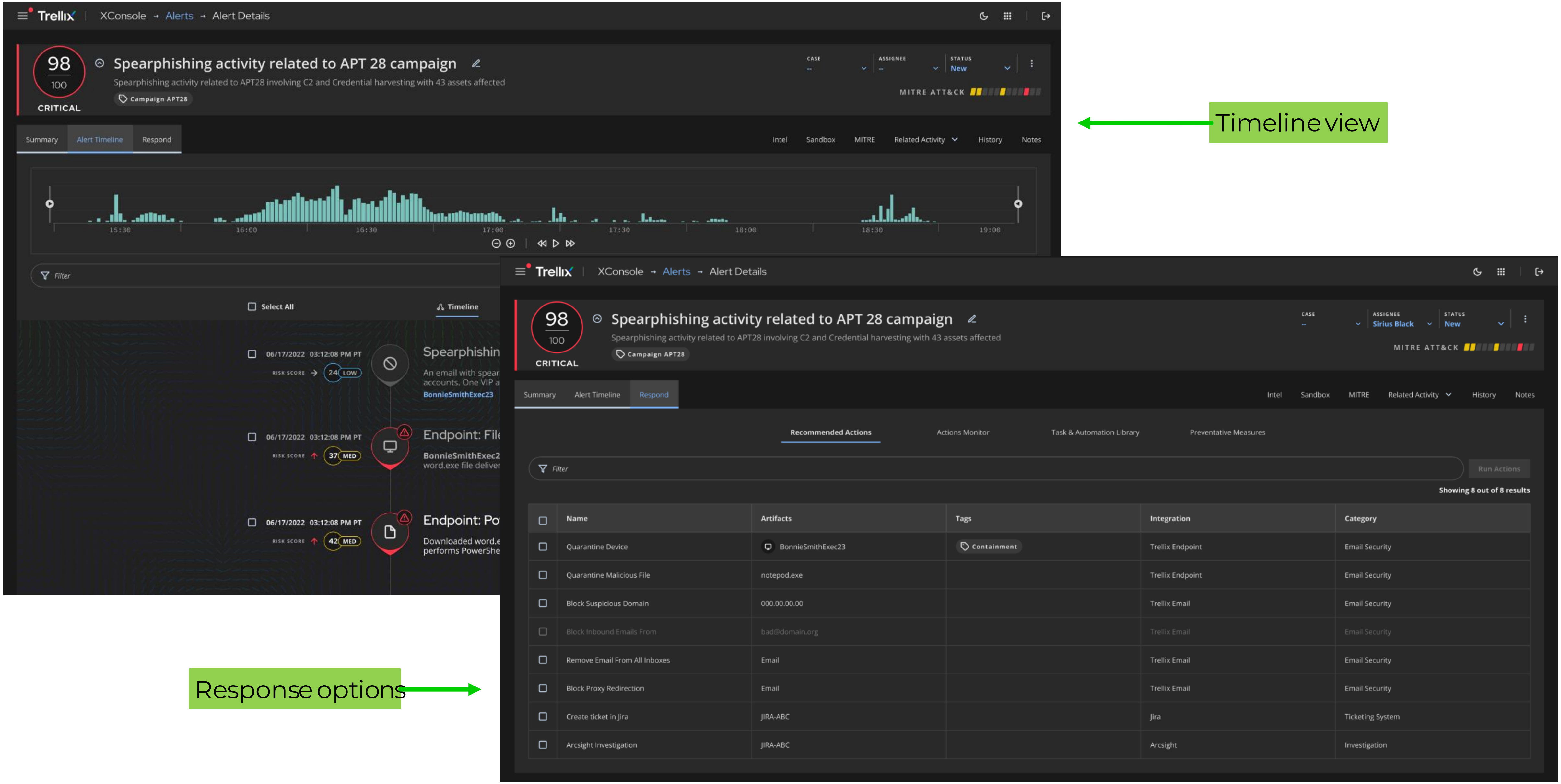
Martin Binetti added 1 alert on 06/15/2023 02:30:05 PM

Martin Binetti added note on 06/15/2023 02:30:05 PM

Alert list

Drill-down summary

Alerts



Spearphishing activity related to APT 28 campaign

Spearphishing activity related to APT28 involving C2 and Credential harvesting with 43 assets affected

Campaign APT28

CASE: --

ASSIGNEE: --

STATUS: New

□ 06/17/2022 03:12:08 PM PT — RISK SCORE → 24 LOW — Spearphishin
An email with spear
accounts. One VIP a
BonnieSmithExec23

□ 06/17/2022 03:12:08 PM PT — RISK SCORE ↑ 37 MED — Endpoint: File
BonnieSmithExec2
word.exe file deliver

□ 06/17/2022 03:12:08 PM PT — RISK SCORE ↑ 42 MED — Endpoint: Po
Downloaded word.e
performs PowerShe

Spearphishing activity related to APT 28 campaign

Spearphishing activity related to APT28 involving C2 and Credential harvesting with 43 assets affected

Campaign APT28

CASE: --

ASSIGNEE: Sirius Black

STATUS: New

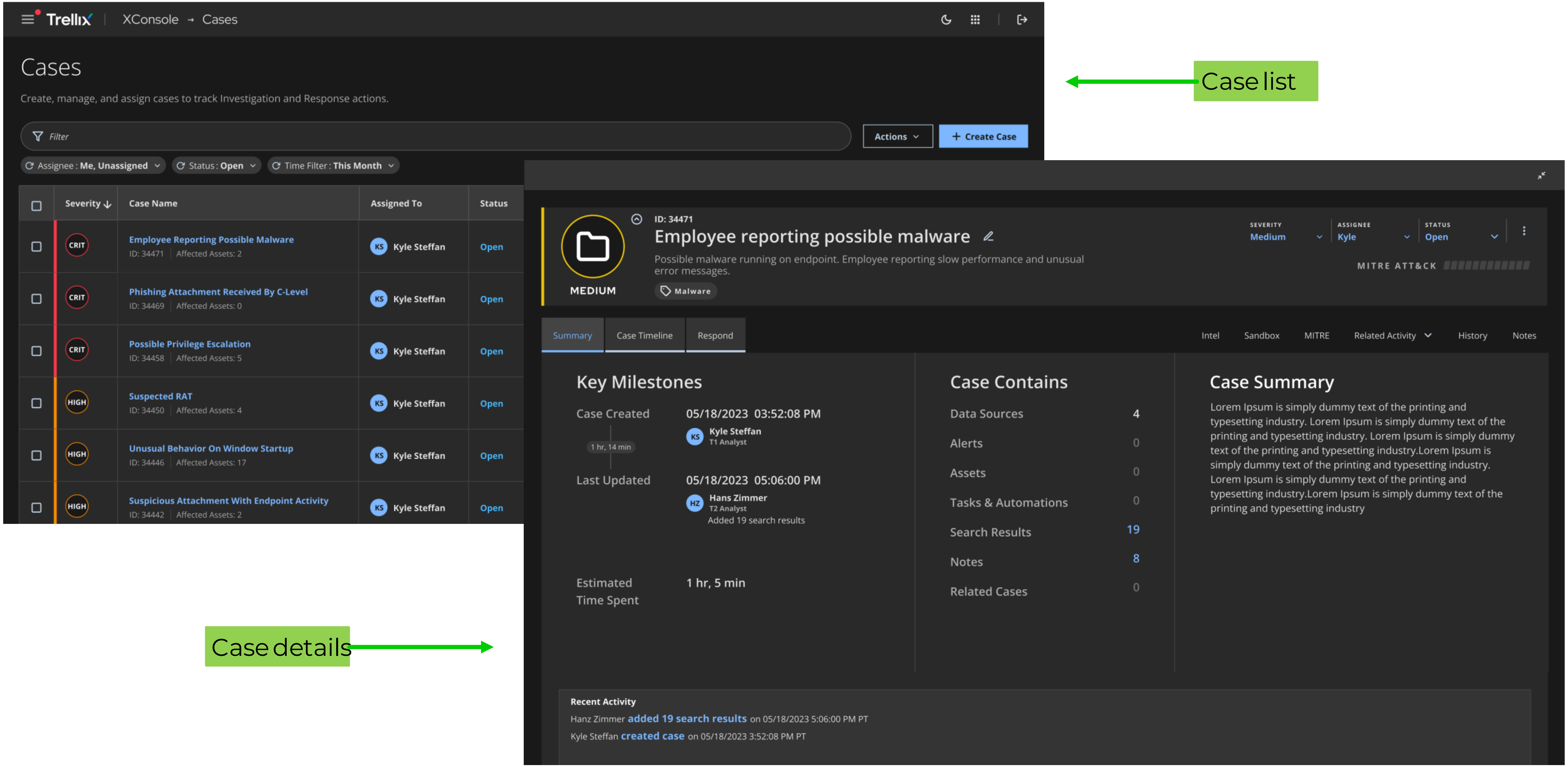
Showing 8 out of 8 results

□	Name	Artifacts	Tags	Integration	Category
□	Quarantine Device	BonnieSmithExec23	Containment	Trellix Endpoint	Email Security
□	Quarantine Malicious File	notepod.exe		Trellix Endpoint	Email Security
□	Block Suspicious Domain	000.00.00.00		Trellix Email	Email Security
□	Block Inbound Emails From	bad@domain.org		Trellix Email	Email Security
□	Remove Email From All Inboxes	Email		Trellix Email	Email Security
□	Block Proxy Redirection	Email		Trellix Email	Email Security
□	Create ticket in Jira	JIRA-ABC		Jira	Ticketing System
□	Arcsight Investigation	JIRA-ABC		Arcsight	Investigation

Timeline view

Response options

Case Management



Cases

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

Assignee : Me, Unassigned · Status : Open · Time Filter : This Month

☐	Severity ↓	Case Name	Assigned To	Status
☐	CRIT	Employee Reporting Possible Malware ID: 34471 | Affected Assets: 2	KS Kyle Steffan	Open
☐	CRIT	Phishing Attachment Received By C-Level ID: 34469 | Affected Assets: 0	KS Kyle Steffan	Open
☐	CRIT	Possible Privilege Escalation ID: 34458 | Affected Assets: 5	KS Kyle Steffan	Open
☐	HIGH	Suspected RAT ID: 34450 | Affected Assets: 4	KS Kyle Steffan	Open
☐	HIGH	Unusual Behavior On Window Startup ID: 34446 | Affected Assets: 17	KS Kyle Steffan	Open
☐	HIGH	Suspicious Attachment With Endpoint Activity ID: 34442 | Affected Assets: 2	KS Kyle Steffan	Open

ID: 34471

Employee reporting possible malware

MEDIUM

Possible malware running on endpoint. Employee reporting slow performance and unusual error messages.

Malware

SEVERITY: Medium · ASSIGNEE: Kyle · STATUS: Open

MITRE ATT&CK

Key Milestones

Case Created: 05/18/2023 03:52:08 PM
KS Kyle Steffan, T1 Analyst

1 hr, 14 min

Last Updated: 05/18/2023 05:06:00 PM
HZ Hans Zimmer, T2 Analyst
Added 19 search results

Estimated Time Spent: 1 hr, 5 min

Case Contains

Data Sources	4
Alerts	0
Assets	0
Tasks & Automations	0
Search Results	19
Notes	8
Related Cases	0

Case Summary

Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum is simply dummy text of the printing and typesetting industry.Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum is simply dummy text of the printing and typesetting industry.Lorem Ipsum is simply dummy text of the printing and typesetting industry

Recent Activity

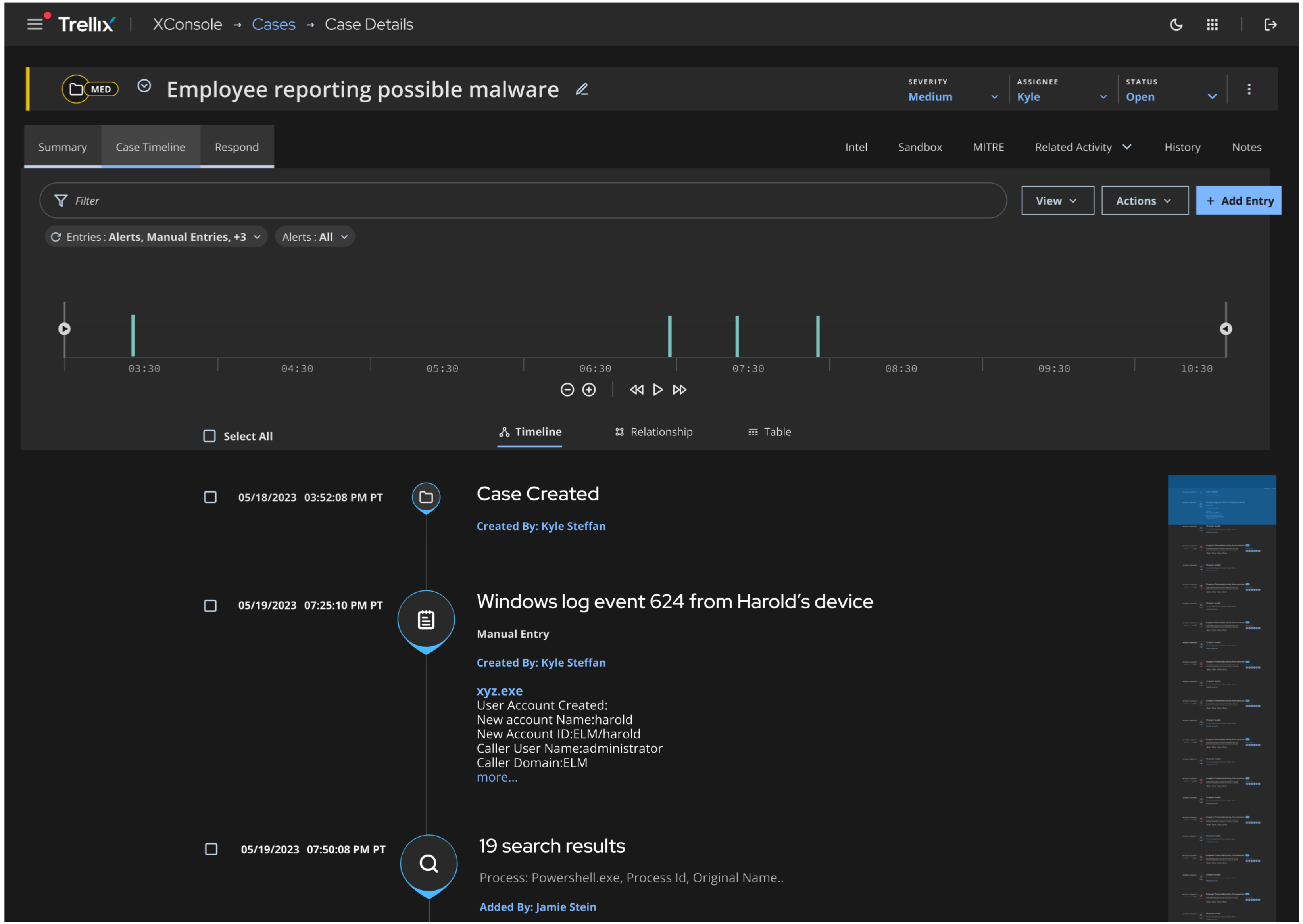
Hanz Zimmer added 19 search results on 05/18/2023 5:06:00 PM PT

Kyle Steffan created case on 05/18/2023 3:52:08 PM PT

Case list

Case details

Case Management



Employee reporting possible malware

SEVERITY: Medium
ASSIGNEE: Kyle
STATUS: Open

Entries : Alerts, Manual Entries, +3
Alerts : All

□ 05/18/2023 03:52:08 PM PT

Case Created

Created By: Kyle Steffan

□ 05/19/2023 07:25:10 PM PT

Windows log event 624 from Harold's device

Manual Entry

Created By: Kyle Steffan

xyz.exe
User Account Created:
New account Name:harold
New Account ID:ELM/harold
Caller User Name:administrator
Caller Domain:ELM
more...

□ 05/19/2023 07:50:08 PM PT

19 search results

Process: Powershell.exe, Process Id, Original Name..

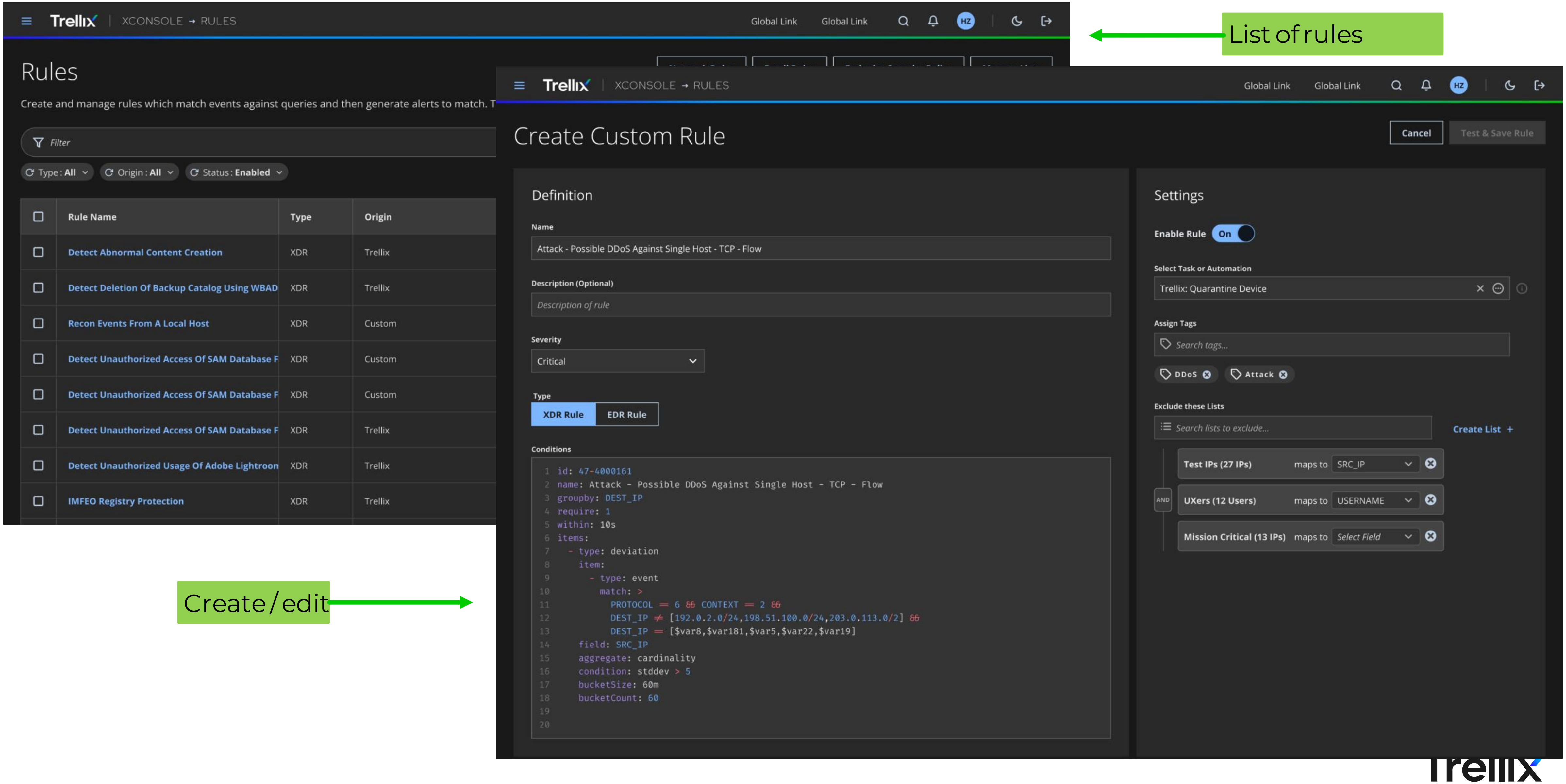
Added By: Jamie Stein

Case Timeline

Manual entry

Add data from other apps

Rule Management



Rules

Create and manage rules which match events against queries and then generate alerts to match. T

□	Rule Name	Type	Origin
□	Detect Abnormal Content Creation	XDR	Trellix
□	Detect Deletion Of Backup Catalog Using WBAD	XDR	Trellix
□	Recon Events From A Local Host	XDR	Custom
□	Detect Unauthorized Access Of SAM Database F	XDR	Custom
□	Detect Unauthorized Access Of SAM Database F	XDR	Custom
□	Detect Unauthorized Access Of SAM Database F	XDR	Trellix
□	Detect Unauthorized Usage Of Adobe Lightroon	XDR	Trellix
□	IMFEO Registry Protection	XDR	Trellix

Create Custom Rule

Definition

Name: Attack - Possible DDoS Against Single Host - TCP - Flow

Description (Optional): *Description of rule*

Severity: Critical

Type: XDR Rule | EDR Rule

Conditions

```
id: 47-4000161
name: Attack - Possible DDoS Against Single Host - TCP - Flow
groupby: DEST_IP
require: 1
within: 10s
items:
  - type: deviation
    item:
      - type: event
        match: >
          PROTOCOL == 6 && CONTEXT == 2 &&
          DEST_IP ≠ [192.0.2.0/24,198.51.100.0/24,203.0.113.0/2] &&
          DEST_IP == [$var8,$var181,$var5,$var22,$var19]
    field: SRC_IP
    aggregate: cardinality
    condition: stddev > 5
    bucketSize: 60m
    bucketCount: 60


```

Settings

Enable Rule: On

Select Task or Automation: Trellix: Quarantine Device

Assign Tags: *Search tags...*

DDoS ⊗ Attack ⊗

Exclude these Lists: *Search lists to exclude...*

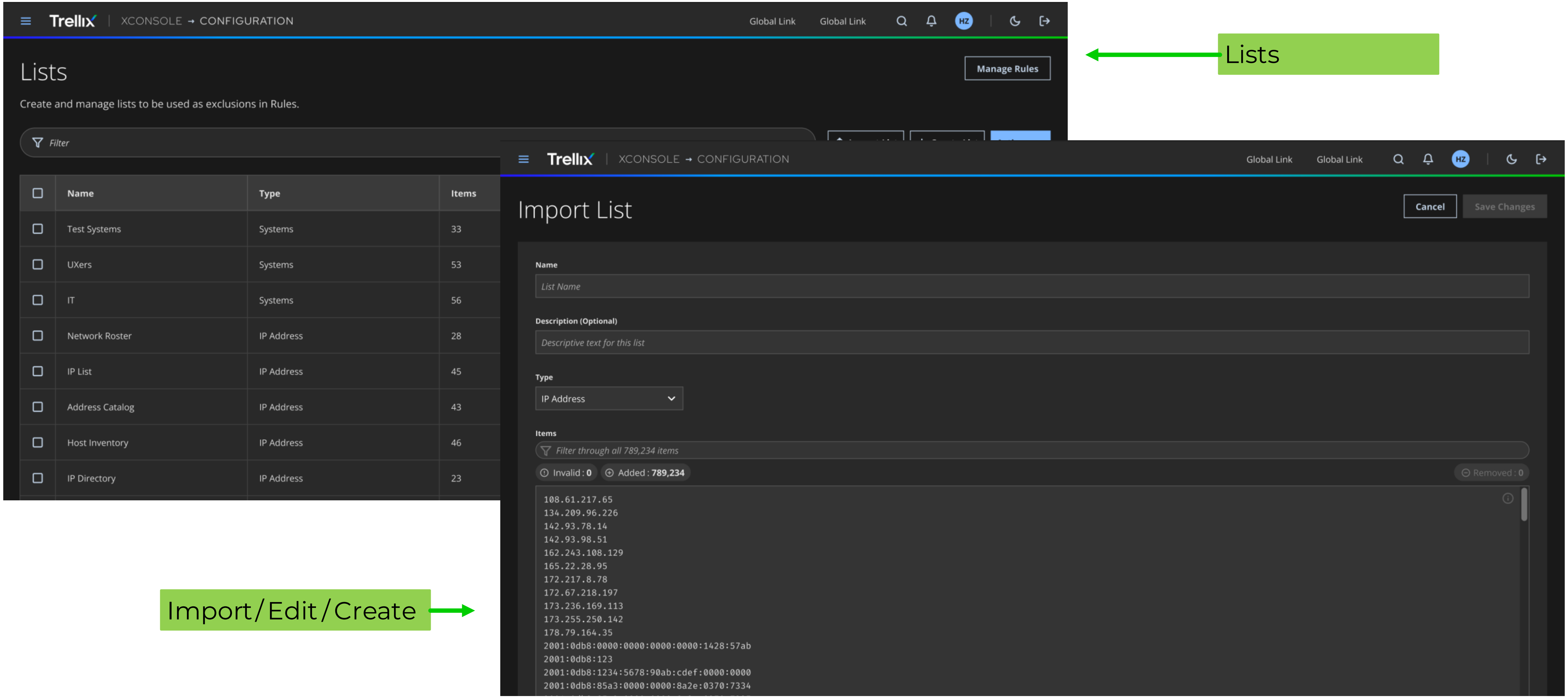
AND

- Test IPs (27 IPs) maps to SRC_IP ⊗
- UXers (12 Users) maps to USERNAME ⊗
- Mission Critical (13 IPs) maps to *Select Field* ⊗

List of rules

Create/edit

Rule Management



Lists

Create and manage lists to be used as exclusions in Rules.

□	Name	Type	Items
□	Test Systems	Systems	33
□	UXers	Systems	53
□	IT	Systems	56
□	Network Roster	IP Address	28
□	IP List	IP Address	45
□	Address Catalog	IP Address	43
□	Host Inventory	IP Address	46
□	IP Directory	IP Address	23

Import List

Name: List Name

Description (Optional): Descriptive text for this list

Type: IP Address

Items: Filter through all 789,234 items

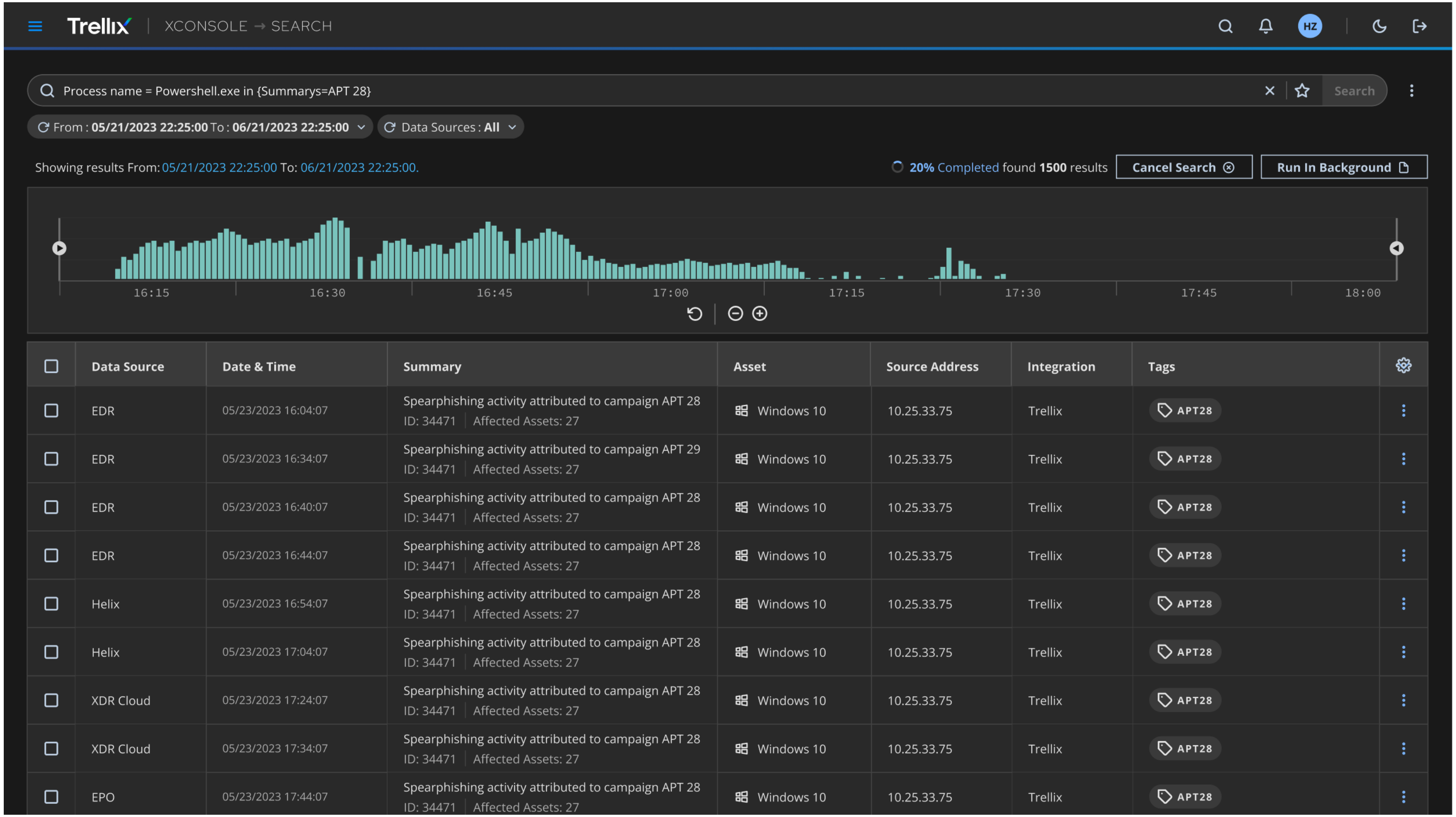
Invalid : 0 — Added : 789,234 — Removed : 0

```
108.61.217.65
134.209.96.226
142.93.78.14
142.93.98.51
162.243.108.129
165.22.28.95
172.217.8.78
172.67.218.197
173.236.169.113
173.255.250.142
178.79.164.35
2001:0db8:0000:0000:0000:0000:1428:57ab
2001:0db8:123
2001:0db8:1234:5678:90ab:cdef:0000:0000
2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

Lists

Import/Edit/Create

Search



Process name = Powershell.exe in {Summarys=APT 28}

Showing results From: 05/21/2023 22:25:00 To: 06/21/2023 22:25:00.

20% Completed found 1500 results

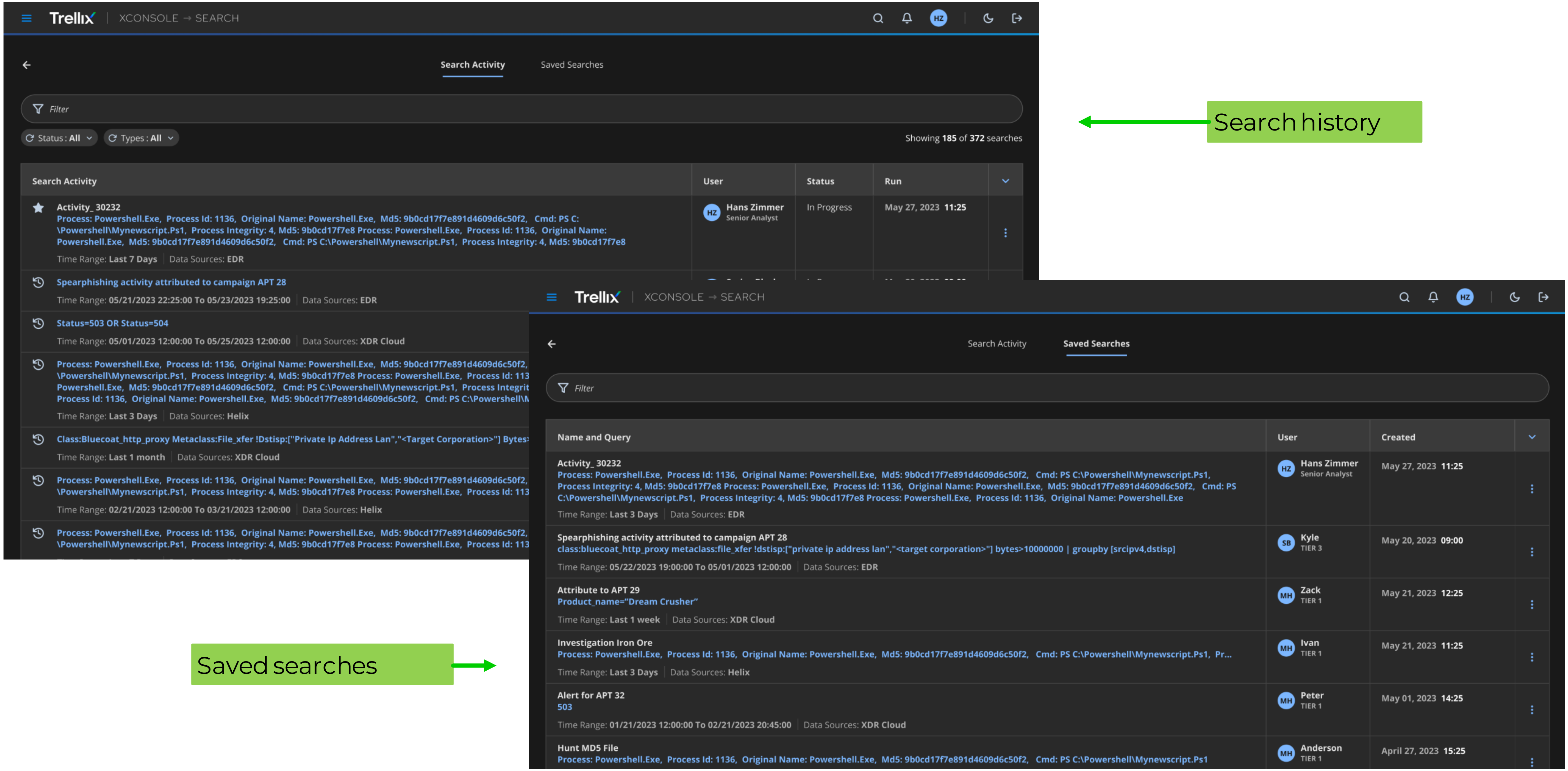
□	Data Source	Date & Time	Summary	Asset	Source Address	Integration	Tags
□	EDR	05/23/2023 16:04:07	Spearphishing activity attributed to campaign APT 28 ID: 34471 | Affected Assets: 27	Windows 10	10.25.33.75	Trellix	APT28
□	EDR	05/23/2023 16:34:07	Spearphishing activity attributed to campaign APT 29 ID: 34471 | Affected Assets: 27	Windows 10	10.25.33.75	Trellix	APT28
□	EDR	05/23/2023 16:40:07	Spearphishing activity attributed to campaign APT 28 ID: 34471 | Affected Assets: 27	Windows 10	10.25.33.75	Trellix	APT28
□	EDR	05/23/2023 16:44:07	Spearphishing activity attributed to campaign APT 28 ID: 34471 | Affected Assets: 27	Windows 10	10.25.33.75	Trellix	APT28
□	Helix	05/23/2023 16:54:07	Spearphishing activity attributed to campaign APT 28 ID: 34471 | Affected Assets: 27	Windows 10	10.25.33.75	Trellix	APT28
□	Helix	05/23/2023 17:04:07	Spearphishing activity attributed to campaign APT 28 ID: 34471 | Affected Assets: 27	Windows 10	10.25.33.75	Trellix	APT28
□	XDR Cloud	05/23/2023 17:24:07	Spearphishing activity attributed to campaign APT 28 ID: 34471 | Affected Assets: 27	Windows 10	10.25.33.75	Trellix	APT28
□	XDR Cloud	05/23/2023 17:34:07	Spearphishing activity attributed to campaign APT 28 ID: 34471 | Affected Assets: 27	Windows 10	10.25.33.75	Trellix	APT28
□	EPO	05/23/2023 17:44:07	Spearphishing activity attributed to campaign APT 28 ID: 34471 | Affected Assets: 27	Windows 10	10.25.33.75	Trellix	APT28

Trellix Query Language

Query results

Smart columns

Search



Search Activity | Saved Searches

Filter

Status : All · Types : All

Showing 185 of 372 searches

Search Activity	User	Status	Run
★ Activity_ 30232 Process: Powershell.Exe, Process Id: 1136, Original Name: Powershell.Exe, Md5: 9b0cd17f7e891d4609d6c50f2, Cmd: PS C:\Powershell\Mynewscript.Ps1, Process Integrity: 4, Md5: 9b0cd17f7e8 Process: Powershell.Exe, Process Id: 1136, Original Name: Powershell.Exe, Md5: 9b0cd17f7e891d4609d6c50f2, Cmd: PS C:\Powershell\Mynewscript.Ps1, Process Integrity: 4, Md5: 9b0cd17f7e8 Time Range: Last 7 Days | Data Sources: EDR	HZ Hans Zimmer Senior Analyst	In Progress	May 27, 2023 11:25
Spearphishing activity attributed to campaign APT 28 Time Range: 05/21/2023 22:25:00 To 05/23/2023 19:25:00 | Data Sources: EDR			
Status=503 OR Status=504 Time Range: 05/01/2023 12:00:00 To 05/25/2023 12:00:00 | Data Sources: XDR Cloud			
Process: Powershell.Exe, Process Id: 1136, Original Name: Powershell.Exe, Md5: 9b0cd17f7e891d4609d6c50f2, \Powershell\Mynewscript.Ps1, Process Integrity: 4, Md5: 9b0cd17f7e8 Process: Powershell.Exe, Process Id: 113 Powershell.Exe, Md5: 9b0cd17f7e891d4609d6c50f2, Cmd: PS C:\Powershell\Mynewscript.Ps1, Process Integrit Process Id: 1136, Original Name: Powershell.Exe, Md5: 9b0cd17f7e891d4609d6c50f2, Cmd: PS C:\Powershell\M Time Range: Last 3 Days | Data Sources: Helix			
Class:Bluecoat_http_proxy Metaclass:File_xfer !Dstisp:["Private Ip Address Lan","<Target Corporation>"] Bytes Time Range: Last 1 month | Data Sources: XDR Cloud			
Process: Powershell.Exe, Process Id: 1136, Original Name: Powershell.Exe, Md5: 9b0cd17f7e891d4609d6c50f2, \Powershell\Mynewscript.Ps1, Process Integrity: 4, Md5: 9b0cd17f7e8 Process: Powershell.Exe, Process Id: 113 Time Range: 02/21/2023 12:00:00 To 03/21/2023 12:00:00 | Data Sources: Helix			
Process: Powershell.Exe, Process Id: 1136, Original Name: Powershell.Exe, Md5: 9b0cd17f7e891d4609d6c50f2, \Powershell\Mynewscript.Ps1, Process Integrity: 4, Md5: 9b0cd17f7e8 Process: Powershell.Exe, Process Id: 113			

Search Activity | Saved Searches

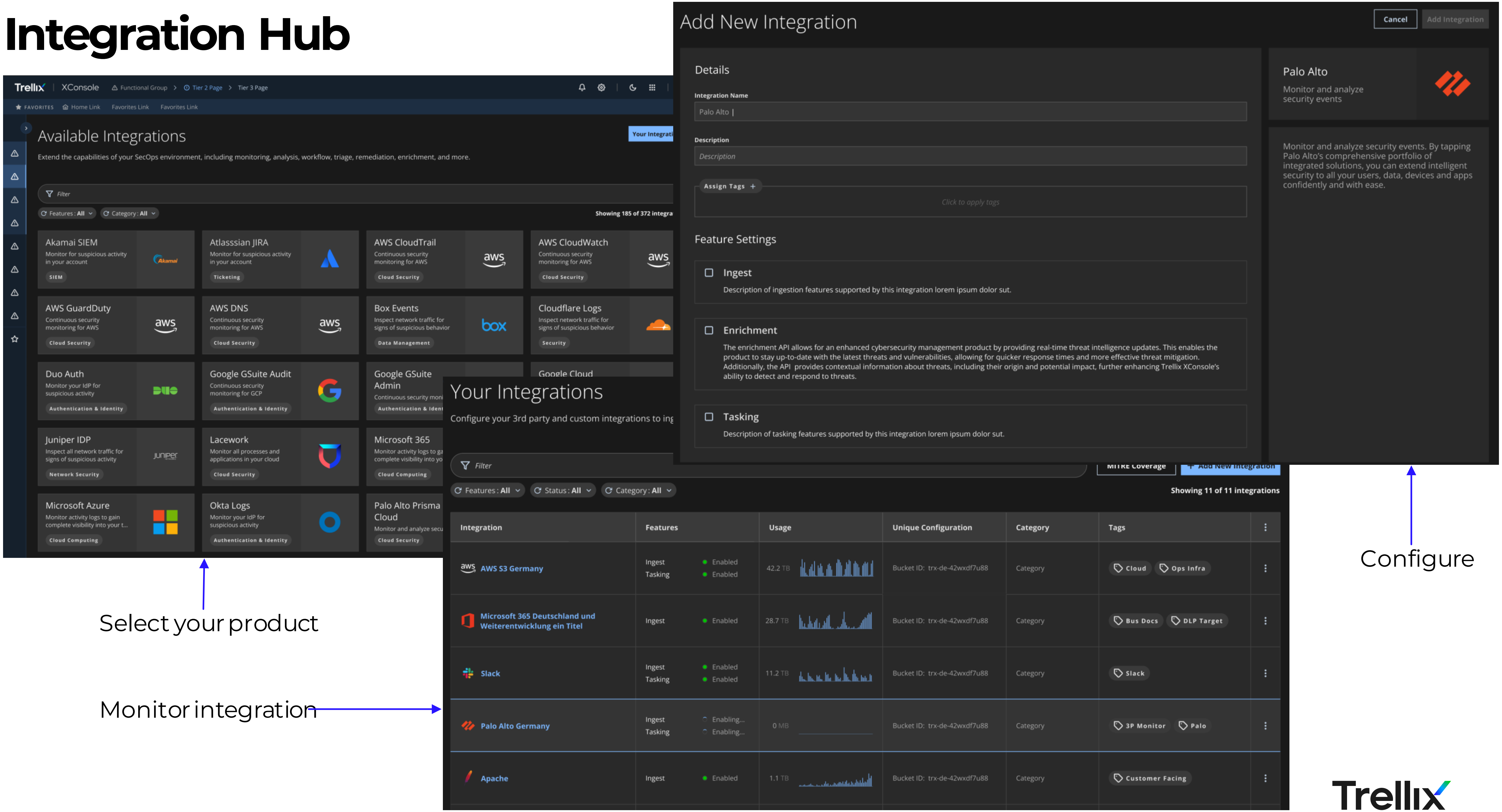
Filter

Name and Query	User	Created
Activity_ 30232 Process: Powershell.Exe, Process Id: 1136, Original Name: Powershell.Exe, Md5: 9b0cd17f7e891d4609d6c50f2, Cmd: PS C:\Powershell\Mynewscript.Ps1, Process Integrity: 4, Md5: 9b0cd17f7e8 Process: Powershell.Exe, Process Id: 1136, Original Name: Powershell.Exe, Md5: 9b0cd17f7e891d4609d6c50f2, Cmd: PS C:\Powershell\Mynewscript.Ps1, Process Integrity: 4, Md5: 9b0cd17f7e8 Process: Powershell.Exe, Process Id: 1136, Original Name: Powershell.Exe Time Range: Last 3 Days | Data Sources: EDR	HZ Hans Zimmer Senior Analyst	May 27, 2023 11:25
Spearphishing activity attributed to campaign APT 28 class:bluecoat_http_proxy metaclass:file_xfer !dstisp:["private ip address lan","<target corporation>"] bytes>10000000 | groupby [srcipv4,dstisp] Time Range: 05/22/2023 19:00:00 To 05/01/2023 12:00:00 | Data Sources: EDR	SB Kyle TIER 3	May 20, 2023 09:00
Attribute to APT 29 Product_name="Dream Crusher" Time Range: Last 1 week | Data Sources: XDR Cloud	MH Zack TIER 1	May 21, 2023 12:25
Investigation Iron Ore Process: Powershell.Exe, Process Id: 1136, Original Name: Powershell.Exe, Md5: 9b0cd17f7e891d4609d6c50f2, Cmd: PS C:\Powershell\Mynewscript.Ps1, Pr... Time Range: Last 3 Days | Data Sources: Helix	MH Ivan TIER 1	May 21, 2023 11:25
Alert for APT 32 503 Time Range: 01/21/2023 12:00:00 To 02/21/2023 20:45:00 | Data Sources: XDR Cloud	MH Peter TIER 1	May 01, 2023 14:25
Hunt MD5 File Process: Powershell.Exe, Process Id: 1136, Original Name: Powershell.Exe, Md5: 9b0cd17f7e891d4609d6c50f2, Cmd: PS C:\Powershell\Mynewscript.Ps1	MH Anderson TIER 1	April 27, 2023 15:25

Search history

Saved searches

Integration Hub



Available Integrations

Extend the capabilities of your SecOps environment, including monitoring, analysis, workflow, triage, remediation, enrichment, and more.

Showing 185 of 372 integra

Akamai SIEM – Monitor for suspicious activity in your account – SIEM

Atlasssian JIRA – Monitor for suspicious activity in your account – Ticketing

AWS CloudTrail – Continuous security monitoring for AWS – Cloud Security

AWS CloudWatch – Continuous security monitoring for AWS – Cloud Security

AWS GuardDuty – Continuous security monitoring for AWS – Cloud Security

AWS DNS – Continuous security monitoring for AWS – Cloud Security

Box Events – Inspect network traffic for signs of suspicious behavior – Data Management

Cloudflare Logs – Inspect network traffic for signs of suspicious behavior – Security

Duo Auth – Monitor your IdP for suspicious activity – Authentication & Identity

Google GSuite Audit – Continuous security monitoring for GCP – Authentication & Identity

Google GSuite Admin – Continuous security moni – Authentication & Ident

Google Cloud

Juniper IDP – Inspect all network traffic for signs of suspicious activity – Network Security

Lacework – Monitor all processes and applications in your cloud – Cloud Security

Microsoft 365 – Monitor activity logs to ga complete visibility into yo – Cloud Computing

Microsoft Azure – Monitor activity logs to gain complete visibility into your t... – Cloud Computing

Okta Logs – Monitor your IdP for suspicious activity – Authentication & Identity

Palo Alto Prisma Cloud – Monitor and analyze secu – Cloud Security

Your Integrations

Configure your 3rd party and custom integrations to ing

Showing 11 of 11 integrations

Integration	Features		Usage	Unique Configuration	Category	Tags
AWS S3 Germany	Ingest Tasking	Enabled Enabled	42.2 TB	Bucket ID: trx-de-42wxdf7u88	Category	Cloud Ops Infra
Microsoft 365 Deutschland und Weiterentwicklung ein Titel	Ingest	Enabled	28.7 TB	Bucket ID: trx-de-42wxdf7u88	Category	Bus Docs DLP Target
Slack	Ingest Tasking	Enabled Enabled	11.2 TB	Bucket ID: trx-de-42wxdf7u88	Category	Slack
Palo Alto Germany	Ingest Tasking	Enabling... Enabling...	0 MB	Bucket ID: trx-de-42wxdf7u88	Category	3P Monitor Palo
Apache	Ingest	Enabled	1.1 TB	Bucket ID: trx-de-42wxdf7u88	Category	Customer Facing

Add New Integration

Details

Integration Name: Palo Alto |

Description: Description

Assign Tags +
Click to apply tags

Feature Settings

☐ **Ingest**
Description of ingestion features supported by this integration lorem ipsum dolor sut.

☐ **Enrichment**
The enrichment API allows for an enhanced cybersecurity management product by providing real-time threat intelligence updates. This enables the product to stay up-to-date with the latest threats and vulnerabilities, allowing for quicker response times and more effective threat mitigation. Additionally, the API provides contextual information about threats, including their origin and potential impact, further enhancing Trellix XConsole's ability to detect and respond to threats.

☐ **Tasking**
Description of tasking features supported by this integration lorem ipsum dolor sut.

Palo Alto
Monitor and analyze security events

Monitor and analyze security events. By tapping Palo Alto's comprehensive portfolio of integrated solutions, you can extend intelligent security to all your users, data, devices and apps confidently and with ease.

Select your product

Monitor integration

Configure

Benefits of XDRv2 vs XDRv1

Tasks are now separate and can be run stand-alone from an automation

- Directly access single tasks without wrapping them in a full automation
- Immidiate value without having to understand automations

Automation Editor

- Edit automations we ship with the product or create new custom automations for your use cases
- Reimagined editor to enable low-code experience
- Limitless possibility to automate most things for mature customers and power users

Custom XDR Tasks

- Build your own tasks using REST and Webhook
- Extend SOAR to currently unsupported 3rd party products yourself

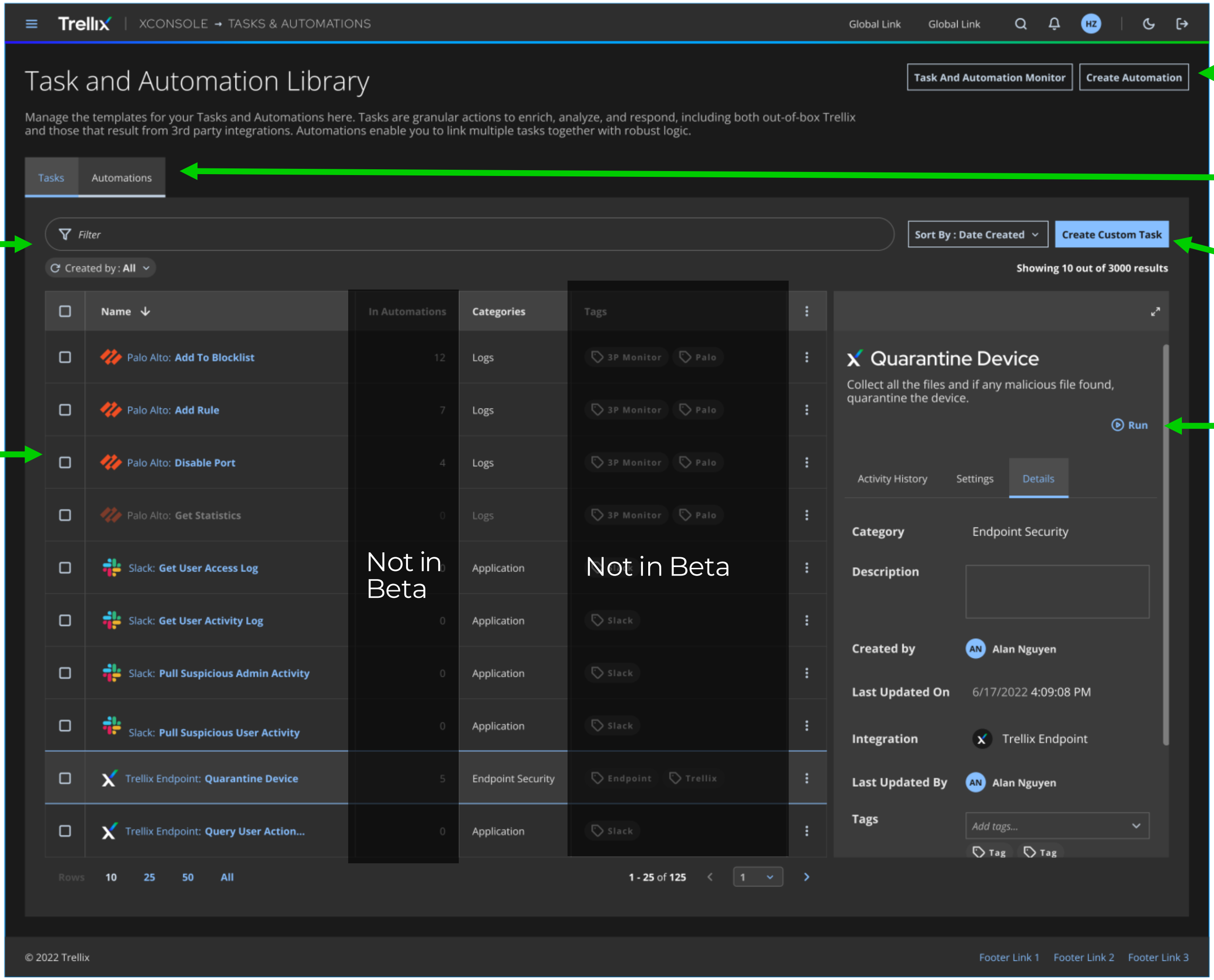
Integrated workflows in Alert management & Case management

- Launch tasks and automations directly from an alert or case without pivoting
- Respond and remediate with the click of a button

XDR internal tasks now exposed as tasks

- Allow automations to interact with our own platform
- Create cases, create alerts, search data in the DB, create rules and much more…
- Extend our XDR platform via custom automations

Task Library



Task and Automation Library

Manage the templates for your Tasks and Automations here. 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.

Showing 10 out of 3000 results

□	Name ↓	In Automations	Categories	Tags
□	Palo Alto: **Add To Blocklist**	12	Logs	3P Monitor, Palo
□	Palo Alto: **Add Rule**	7	Logs	3P Monitor, Palo
□	Palo Alto: **Disable Port**	4	Logs	3P Monitor, Palo
□	Palo Alto: **Get Statistics**	0	Logs	3P Monitor, Palo
□	Slack: **Get User Access Log**	Not in Beta	Application	Not in Beta
□	Slack: **Get User Activity Log**	0	Application	Slack
□	Slack: **Pull Suspicious Admin Activity**	0	Application	Slack
□	Slack: **Pull Suspicious User Activity**	0	Application	Slack
□	Trellix Endpoint: **Quarantine Device**	5	Endpoint Security	Endpoint, Trellix
□	Trellix Endpoint: **Query User Action...**	0	Application	Slack

Rows 10 25 50 All 1 - 25 of 125 ‹ 1 ›

Quarantine Device

Collect all the files and if any malicious file found, quarantine the device.

Category	Endpoint Security
Description	
Created by	AN Alan Nguyen
Last Updated On	6/17/2022 4:09:08 PM
Integration	Trellix Endpoint
Last Updated By	AN Alan Nguyen
Tags	Add tags... Tag Tag

© 2022 Trellix

Create new automation

Separate tables for Tasks and Automations

Type-ahead filter

Create custom task

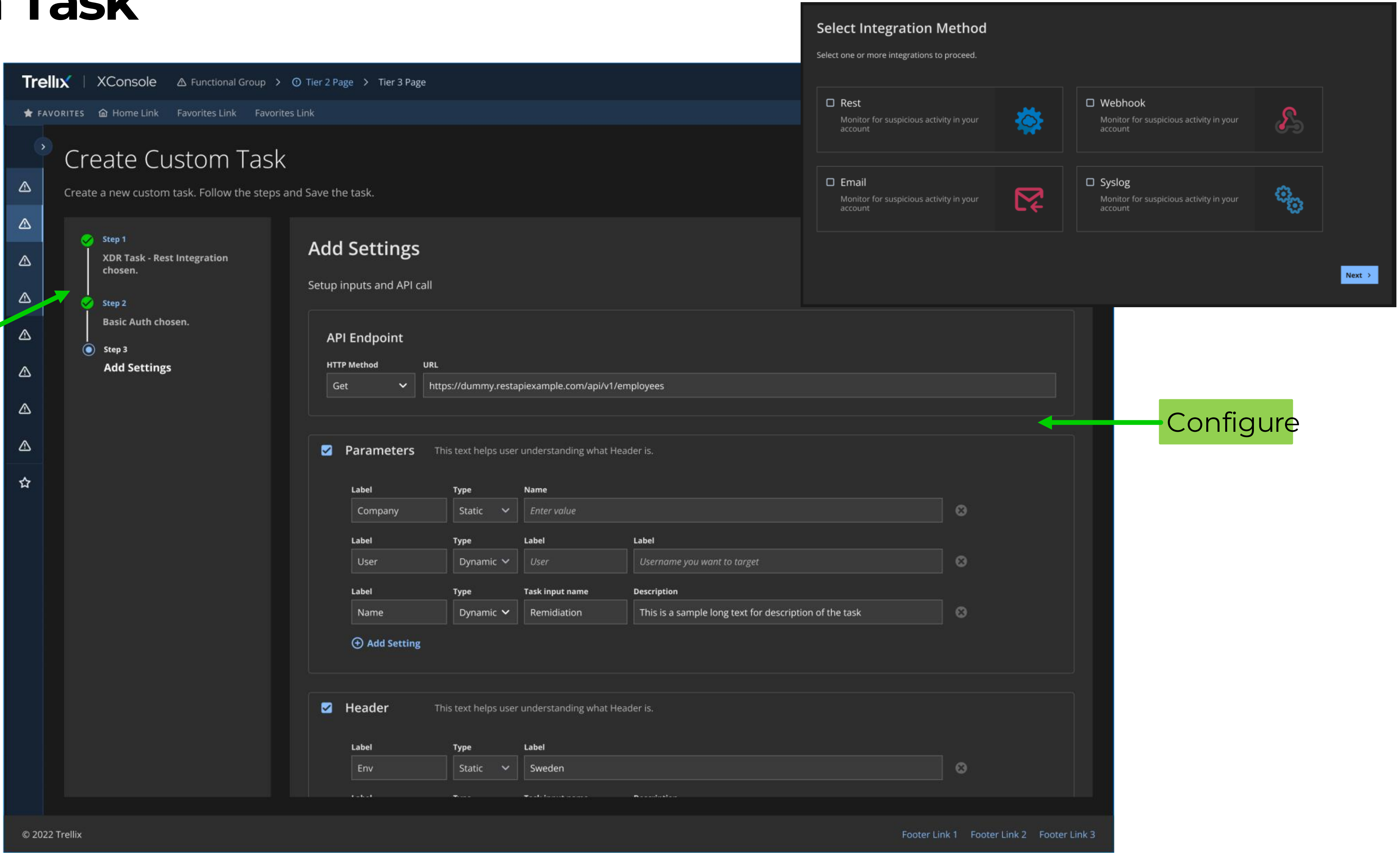
3rd party tasks from integration hub

Run task ad-hoc

XDR Custom Task

Wizard

- Naming and type
- Auth method
- REST/WebHook config



Create Custom Task

Create a new custom task. Follow the steps and Save the task.

Step 1 — XDR Task - Rest Integration chosen.

Step 2 — Basic Auth chosen.

Step 3 — Add Settings

Add Settings

Setup inputs and API call

API Endpoint

HTTP Method	URL
Get	https://dummy.restapiexample.com/api/v1/employees

☑ **Parameters** This text helps user understanding what Header is.

Label	Type	Name	
Company	Static	Enter value	

Label	Type	Label	Label
User	Dynamic	User	Username you want to target

Label	Type	Task input name	Description
Name	Dynamic	Remidiation	This is a sample long text for description of the task

⊕ Add Setting

☑ **Header** This text helps user understanding what Header is.

Label	Type	Label
Env	Static	Sweden

Select Integration Method

Select one or more integrations to proceed.

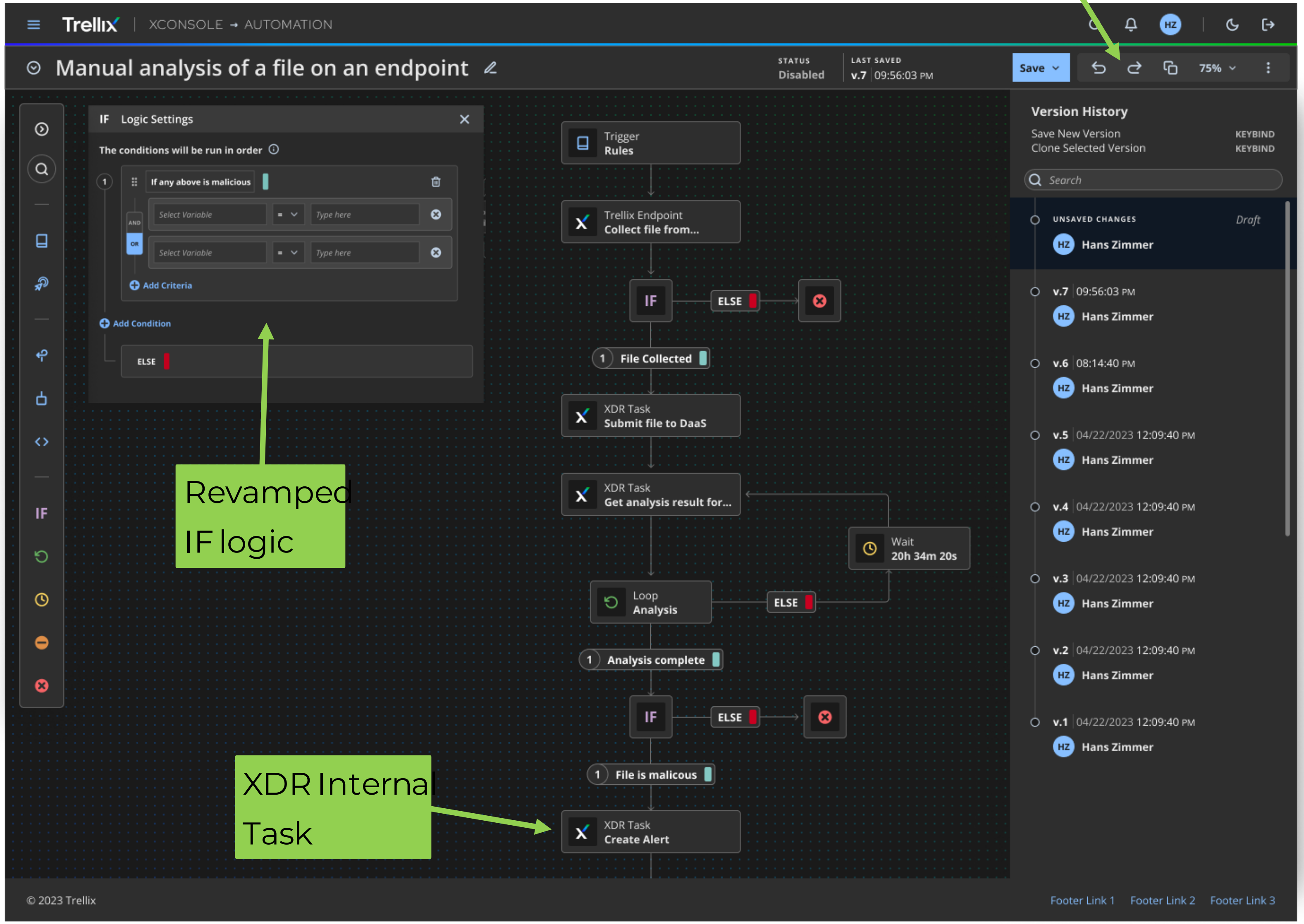
- □ Rest — Monitor for suspicious activity in your account
- □ Webhook — Monitor for suspicious activity in your account
- □ Email — Monitor for suspicious activity in your account
- □ Syslog — Monitor for suspicious activity in your account

Configure

Note: A simplified version of this workflow will be available at next release!

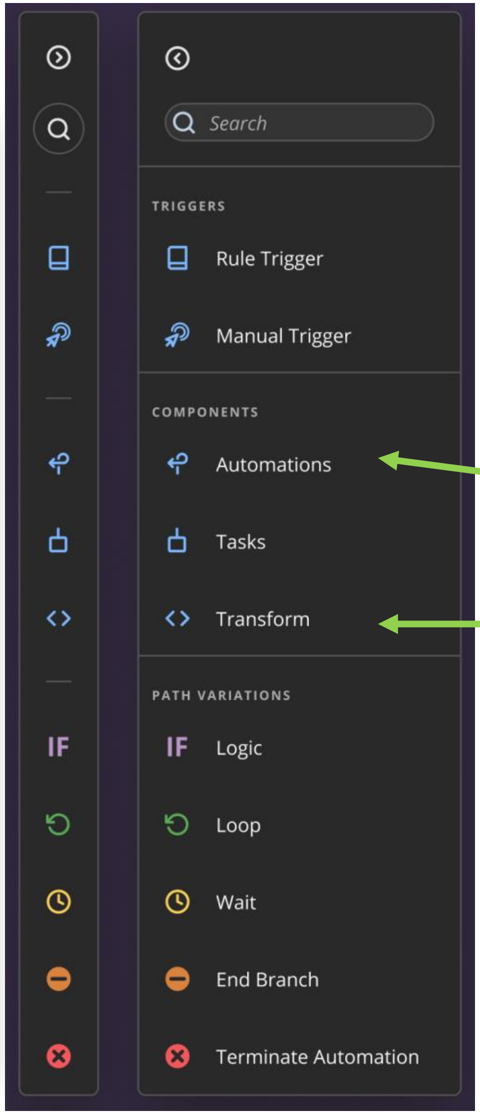
Automation Editor

Undo/Redo



Revamped IF logic

XDR Internal Task



Run another automation

Script

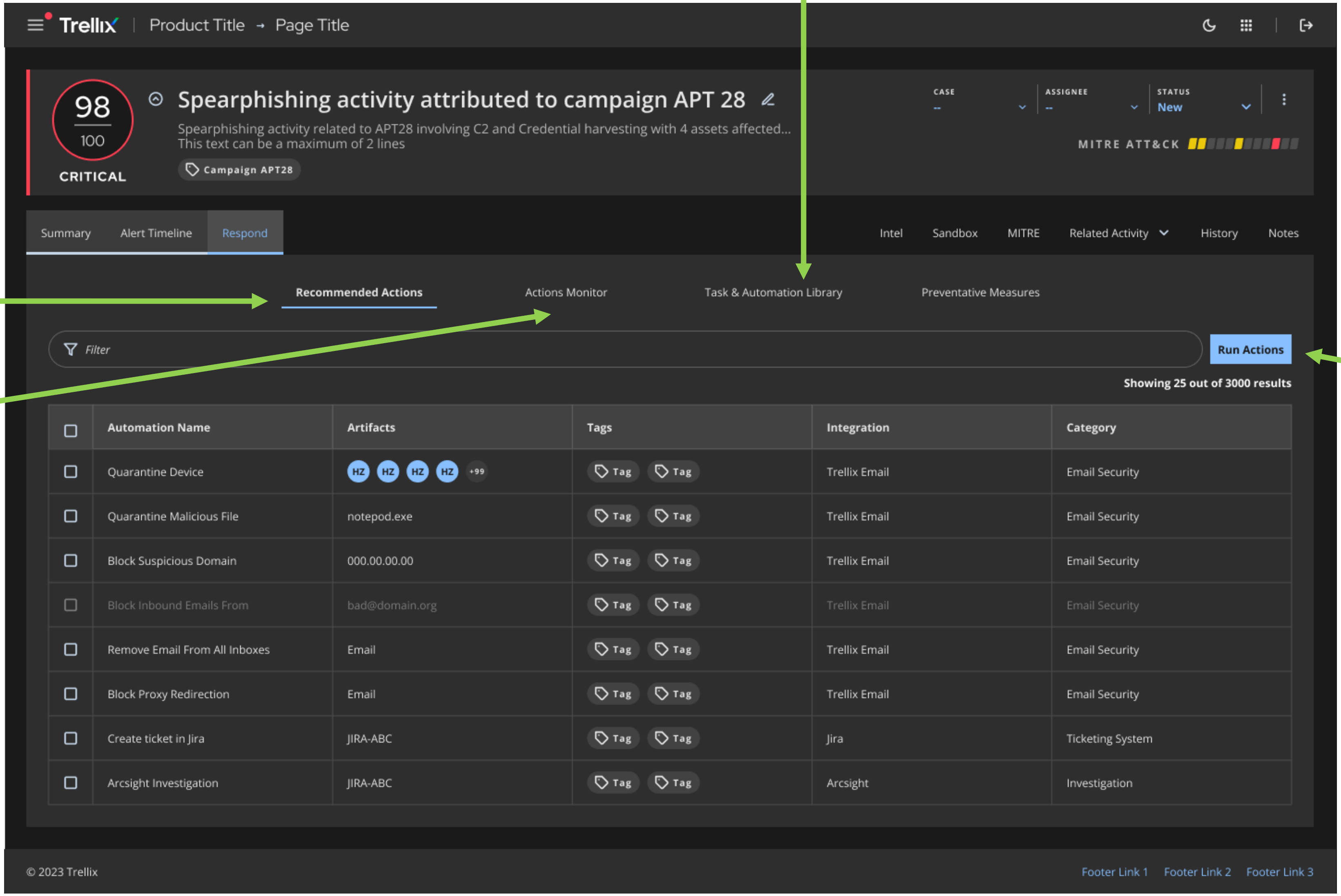
Alert Workflow integration

Full Library

Filtered list from task library

Filtered list from task monitor

Execute selected Tasks & Automations



98
100
CRITICAL

Spearphishing activity attributed to campaign APT 28

Spearphishing activity related to APT28 involving C2 and Credential harvesting with 4 assets affected...
This text can be a maximum of 2 lines

Campaign APT28

CASE --
ASSIGNEE --
STATUS New

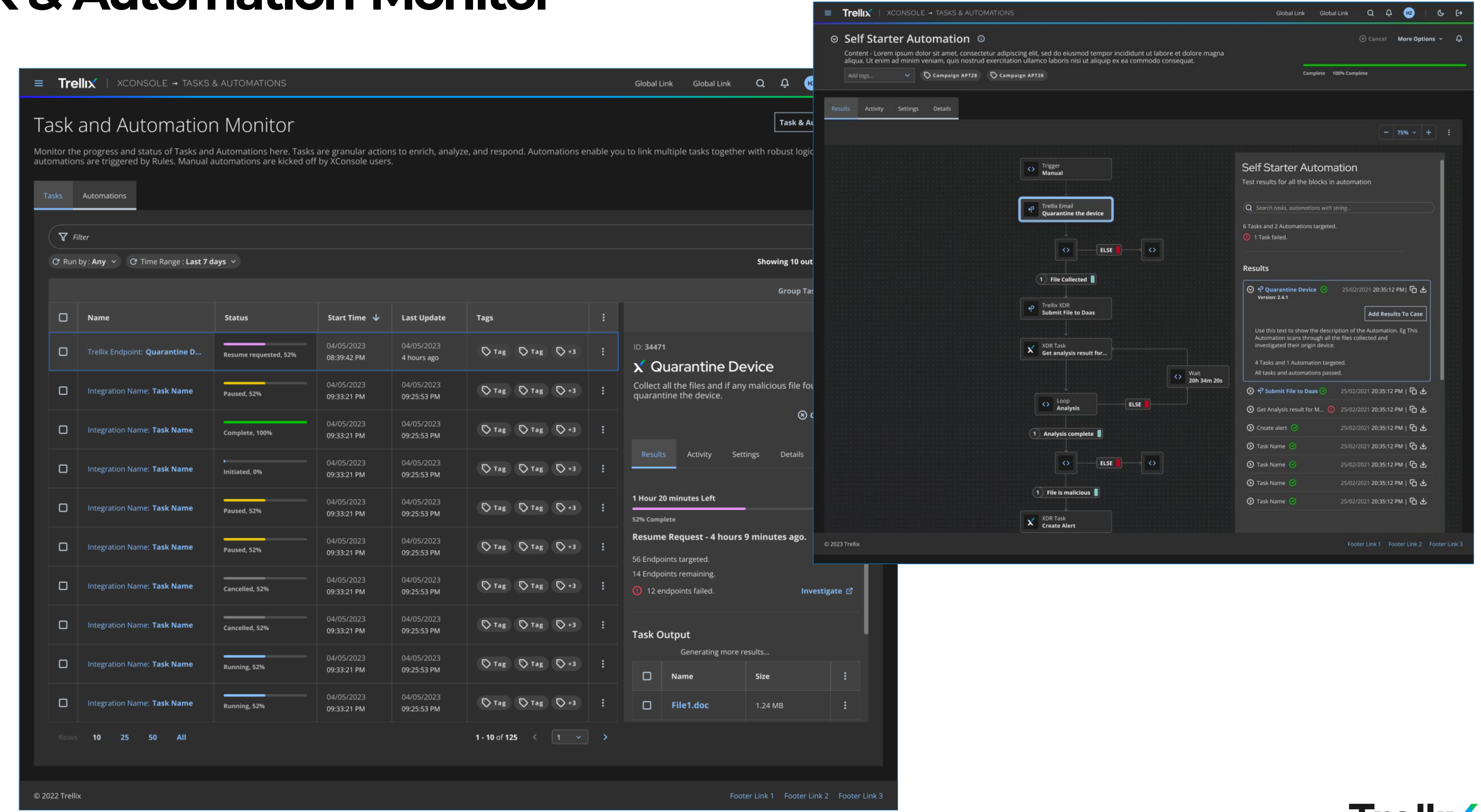
MITRE ATT&CK

Showing 25 out of 3000 results

□	Automation Name	Artifacts	Tags	Integration	Category
□	Quarantine Device	HZ HZ HZ HZ +99	Tag Tag	Trellix Email	Email Security
□	Quarantine Malicious File	notepod.exe	Tag Tag	Trellix Email	Email Security
□	Block Suspicious Domain	000.00.00.00	Tag Tag	Trellix Email	Email Security
□	Block Inbound Emails From	bad@domain.org	Tag Tag	Trellix Email	Email Security
□	Remove Email From All Inboxes	Email	Tag Tag	Trellix Email	Email Security
□	Block Proxy Redirection	Email	Tag Tag	Trellix Email	Email Security
□	Create ticket in Jira	JIRA-ABC	Tag Tag	Jira	Ticketing System
□	Arcsight Investigation	JIRA-ABC	Tag Tag	Arcsight	Investigation

© 2023 Trellix

Task & Automation Monitor



Task and Automation Monitor

Monitor the progress and status of Tasks and Automations here. Tasks are granular actions to enrich, analyze, and respond. Automations enable you to link multiple tasks together with robust logic automations are triggered by Rules. Manual automations are kicked off by XConsole users.

Name	Status	Start Time	Last Update	Tags
Trellix Endpoint: Quarantine D...	Resume requested, 52%	04/05/2023 08:39:42 PM	04/05/2023 4 hours ago	Tag Tag +3
Integration Name: Task Name	Paused, 52%	04/05/2023 09:33:21 PM	04/05/2023 09:25:53 PM	Tag Tag +3
Integration Name: Task Name	Complete, 100%	04/05/2023 09:33:21 PM	04/05/2023 09:25:53 PM	Tag Tag +3
Integration Name: Task Name	Initiated, 0%	04/05/2023 09:33:21 PM	04/05/2023 09:25:53 PM	Tag Tag +3
Integration Name: Task Name	Paused, 52%	04/05/2023 09:33:21 PM	04/05/2023 09:25:53 PM	Tag Tag +3
Integration Name: Task Name	Paused, 52%	04/05/2023 09:33:21 PM	04/05/2023 09:25:53 PM	Tag Tag +3
Integration Name: Task Name	Cancelled, 52%	04/05/2023 09:33:21 PM	04/05/2023 09:25:53 PM	Tag Tag +3
Integration Name: Task Name	Cancelled, 52%	04/05/2023 09:33:21 PM	04/05/2023 09:25:53 PM	Tag Tag +3
Integration Name: Task Name	Running, 52%	04/05/2023 09:33:21 PM	04/05/2023 09:25:53 PM	Tag Tag +3
Integration Name: Task Name	Running, 52%	04/05/2023 09:33:21 PM	04/05/2023 09:25:53 PM	Tag Tag +3

ID: 34471

Quarantine Device

Collect all the files and if any malicious file fou quarantine the device.

1 Hour 20 minutes Left

52% Complete

Resume Request - 4 hours 9 minutes ago.

56 Endpoints targeted.

14 Endpoints remaining.

12 endpoints failed.

Task Output

Generating more results...

Name	Size
File1.doc	1.24 MB

© 2022 Trellix

Self Starter Automation

Content - Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Self Starter Automation

Test results for all the blocks in automation

6 Tasks and 2 Automations targeted.

1 Task failed.

Results

Quarantine Device ✓ 25/02/2021 20:35:12 PM |
Version: 2.4.1

Use this text to show the description of the Automation. Eg This Automation scans through all the files collected and investigated their origin device.

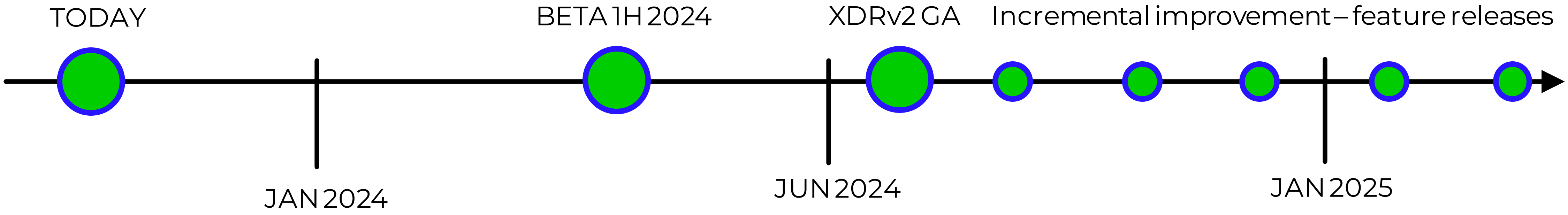
4 Tasks and 1 Automation targeted.

All tasks and automations passed.

Submit File to Daas ✓ 25/02/2021 20:35:12 PM |
Get Analysis result for M... ! 25/02/2021 20:35:12 PM |
Create alert ✓ 25/02/2021 20:35:12 PM |
Task Name ✓ 25/02/2021 20:35:12 PM |
Task Name ✓ 25/02/2021 20:35:12 PM |
Task Name ✓ 25/02/2021 20:35:12 PM |
Task Name ✓ 25/02/2021 20:35:12 PM |

© 2023 Trellix

Roadmap



TODAY

BETA 1H 2024

XDRv2 GA

Incremental improvement – feature releases

JAN 2024

JUN 2024

JAN 2025

Trellix

Thank You!