

Trellix

3-6 November 2025

EMEA & LTAM Tech Summit

Madrid, Spain



Trellix

Helix

Get AI-powered context across
all threat vectors and security
tools — and respond in minutes



Speakers



**Christoph
Kiechle**

Solutions Engineer



**Enrico
Chirico Pisacane**

Solutions Engineer



**Henrik
Olsson**

Senior Director of Product
Management

Trellix

Solution Presentation



Market trends

Siloed Tools

76

Organizations with over 5,000 employees manage an average of 76 discrete security tools¹

Understaffed Teams

59%

Of cybersecurity teams being understaffed caused by burnout and a talent gap of 4 million professionals²

Blind Spots

66%

Of IT environments can be monitored by global organizations³

Attack Surface

62%

Increase in attack surface over the past 2 years⁴



1. [JupiterOne](#) | 2. [New ISACA Research](#) | 3. [Exabeam and IDC Study](#) | 4. [Techtarget](#)

SOC Barriers to Efficacy and Efficiency



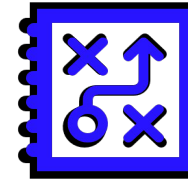
Noise vs. Signals

Low-level “noise” needs to be correlated and analyzed to become “signal.”



Atomic vs. Behavioral

True threats have to be manually pieced together into a narrative from disparate alerts.



Tuning Detection Rules

Time consuming but necessary to stop false positives and alert noise

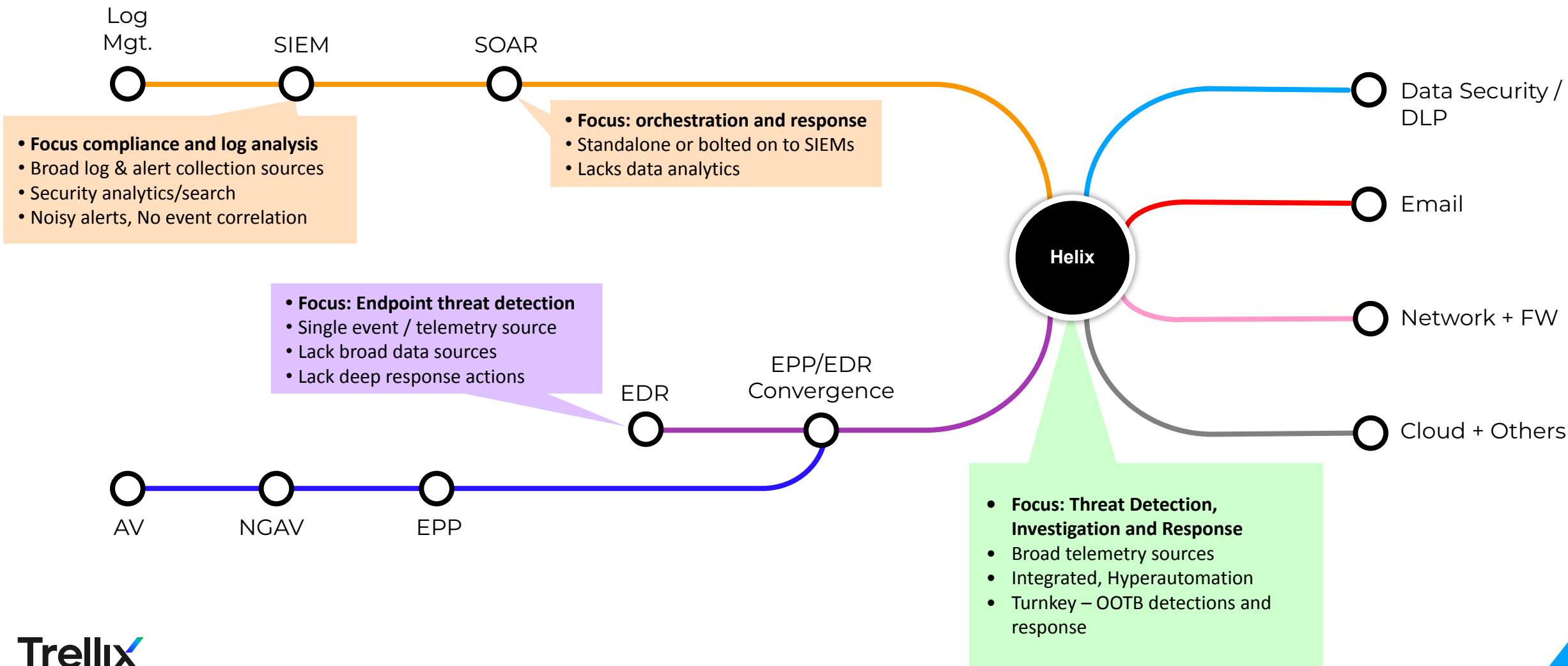


Limited Correlation

Alerts from the same activity appearing as separate, unrelated

How do you surface what matters quickly & accurately?

Evolution of SecOps Visibility



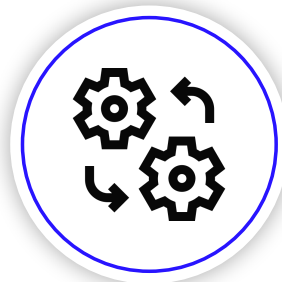
Simplify SecOps with Trellix

Turn Noise Into Insight



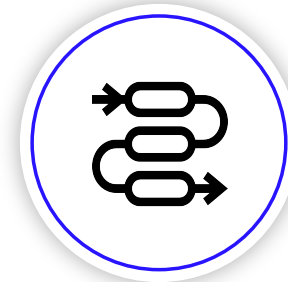
**Triage Every Alert
and Prioritize Threats**

Get the Full Story



**Deep analytics,
Pre-built Detection
Rules**

Minimize MTTD, MTTR



**Low-code
Automation, GenAI
Powered Processes
& Expertise**

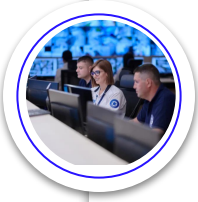
Detect and respond across your environment

Trellix Helix Benefits



Speed MTTD, MTTR

Deep analytics, advanced correlations, AI, and user-friendly analyst experience, the average time spent investigating threats and taking response actions is under 10 minutes



Make Security Teams more efficient and productive

Through the elimination of point product pivot across an efficiency boost of up to 20% is achieved.

Valuable Time is saved as 50% to 70% of FPs are halted before they arrive.

Correlation prioritizes the alerts that matter, saving hours or days.



Close security talent and skills gaps, and automate

With more pre-built automation workflows than competing solutions and the ability to customize them using Hyperautomation no-code SOAR, Helix helps upskill less experienced analysts.

Click through correlation details and be led through best practices to perform data enrichment or remediation steps, improving expertise.

Helix delivers

- Faster Investigation
- Less Product Pivots
- Fewer False Positives
- Faster Responses

How Helix Works

1. Data Ingestion:

Open and Native integrations

2. Detections:

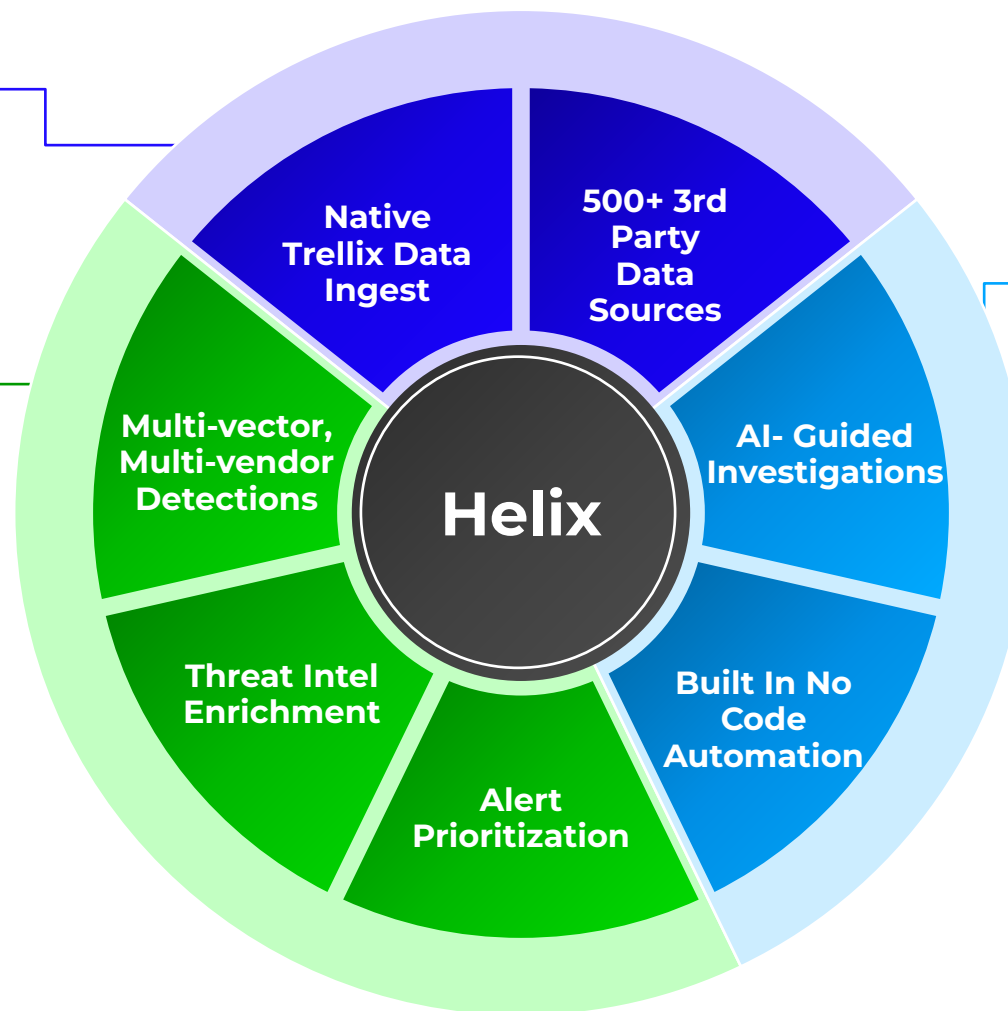
Analytics

Automated threat elimination

Noise suppression

Enrichment

Prioritization

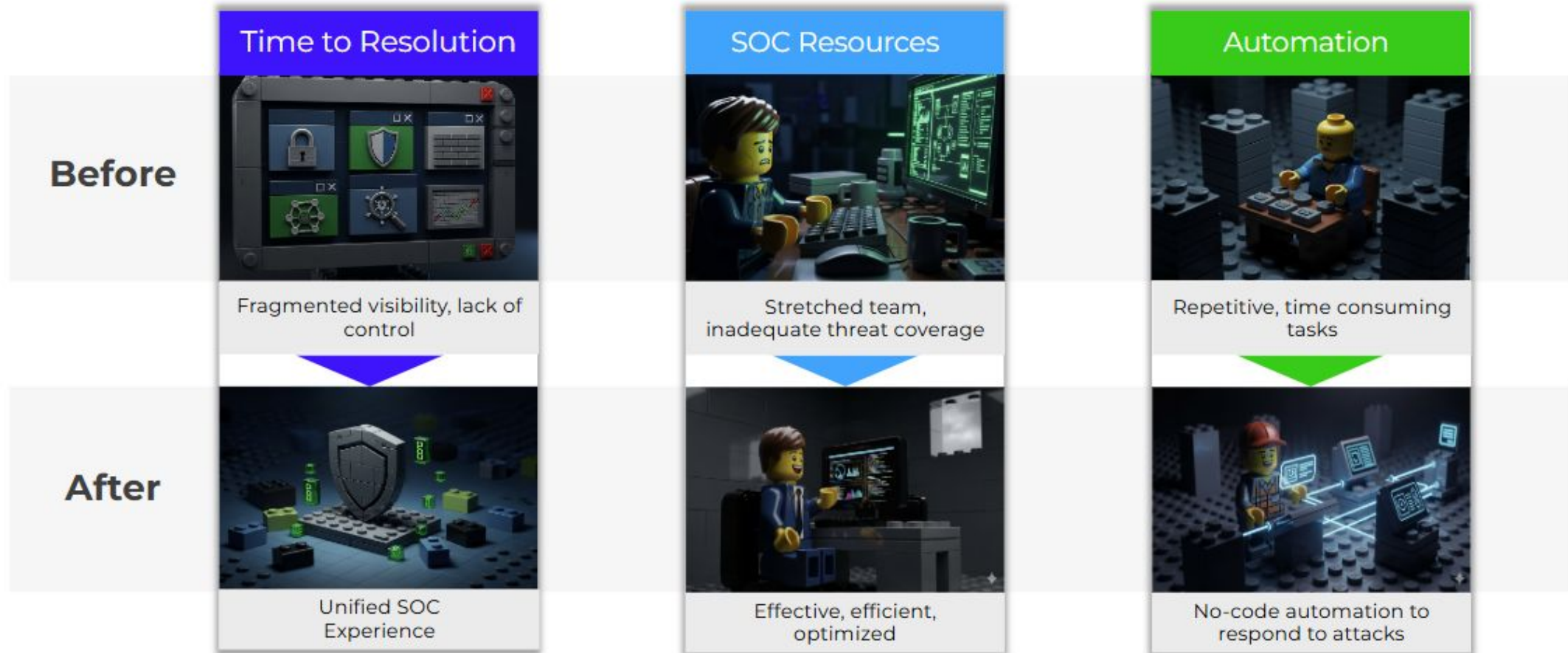


3. Response:

AI Guided Investigations

On-prem/cloud HyperAutomation orchestration and response

The Helix Impact



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

Driving Decisions With Wise AI

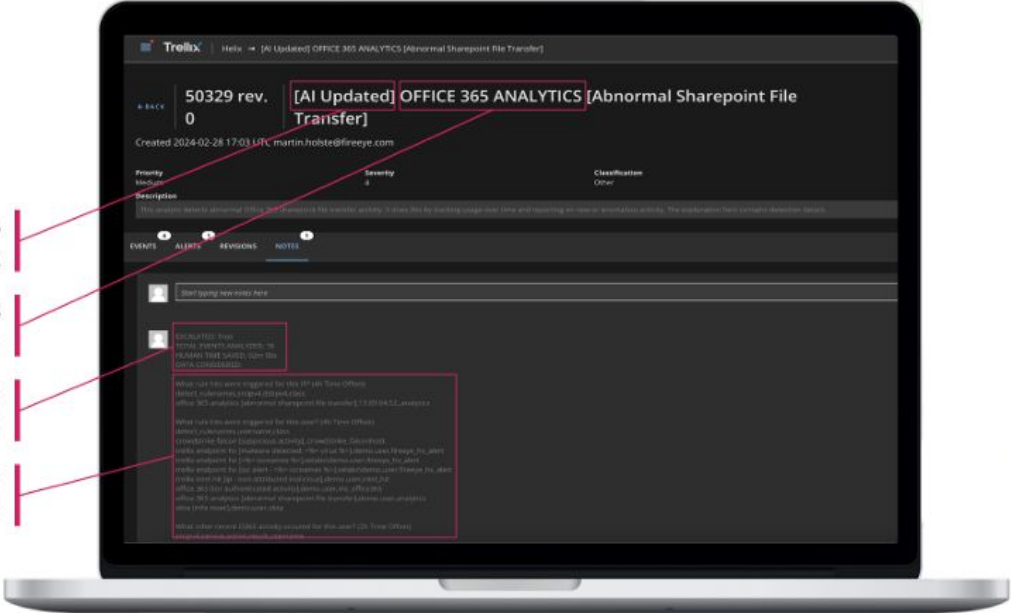
Helix with Wise performs the work of 12 8-hour SOC shifts

Auto-investigates every alert

Leverages our integrations + ML AI for detection

Makes decisions and records stats on time saved

Provides detailed explanation of decision



An answer to alert fatigue and skills gaps:

100%
of Alerts investigated in <3 min

40x
Faster Detection

8hrs
SOC work recovered per 100 alerts investigated

Trellix Helix with Wise



Multi- vector Machine Learning Models

Across Endpoint, Email,
Network, and Sandbox
products

Operational Threat Intelligence

Using 60 billion queries
a day on malicious
activity

Workflows And Analytics

Trained by decades of
expertise and large data
volumes

GenAI

Content creation with
everyday language, Alert
Scoring and
Prioritization,
Automated escalations
and Reporting for
recovered time

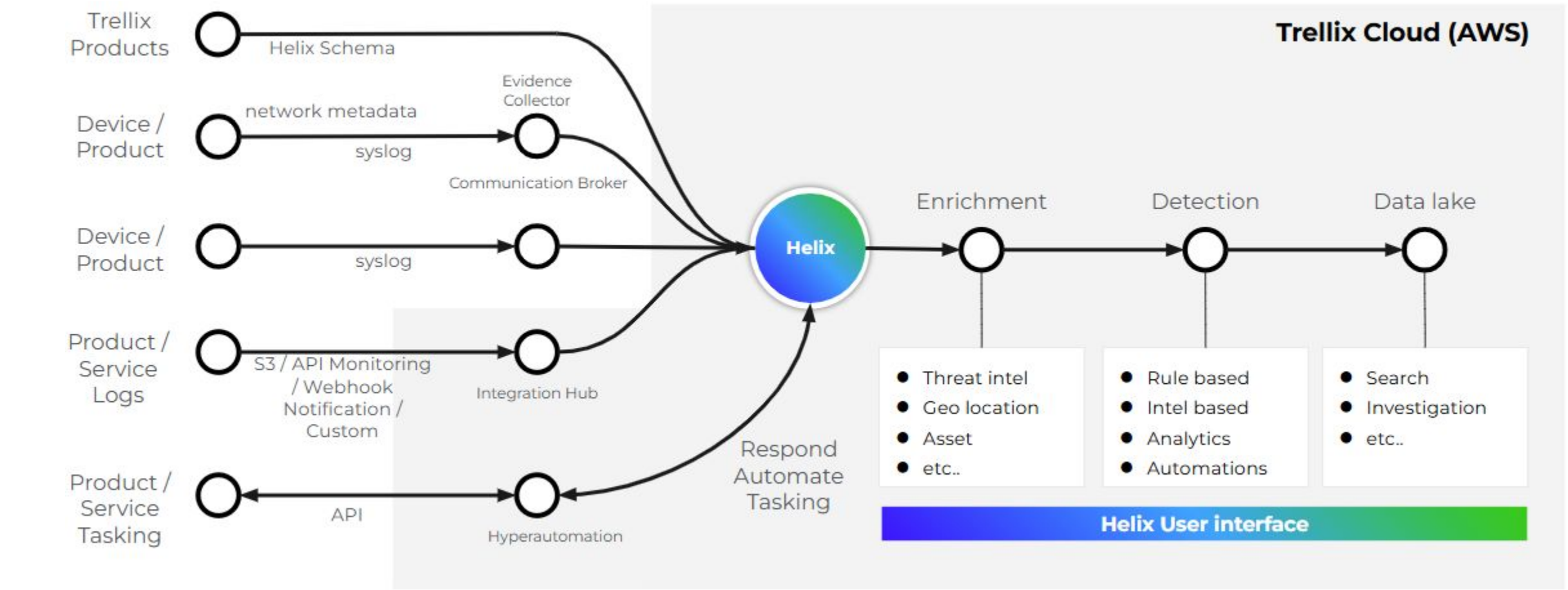
Trellix

Architecture



Helix Reference Architecture

Onboarding data sources for threat detection, investigation and retention



Trellix Out-of-the-box integrations for common data sources and data mapping for custom log sources

Trellix

Key Use-cases



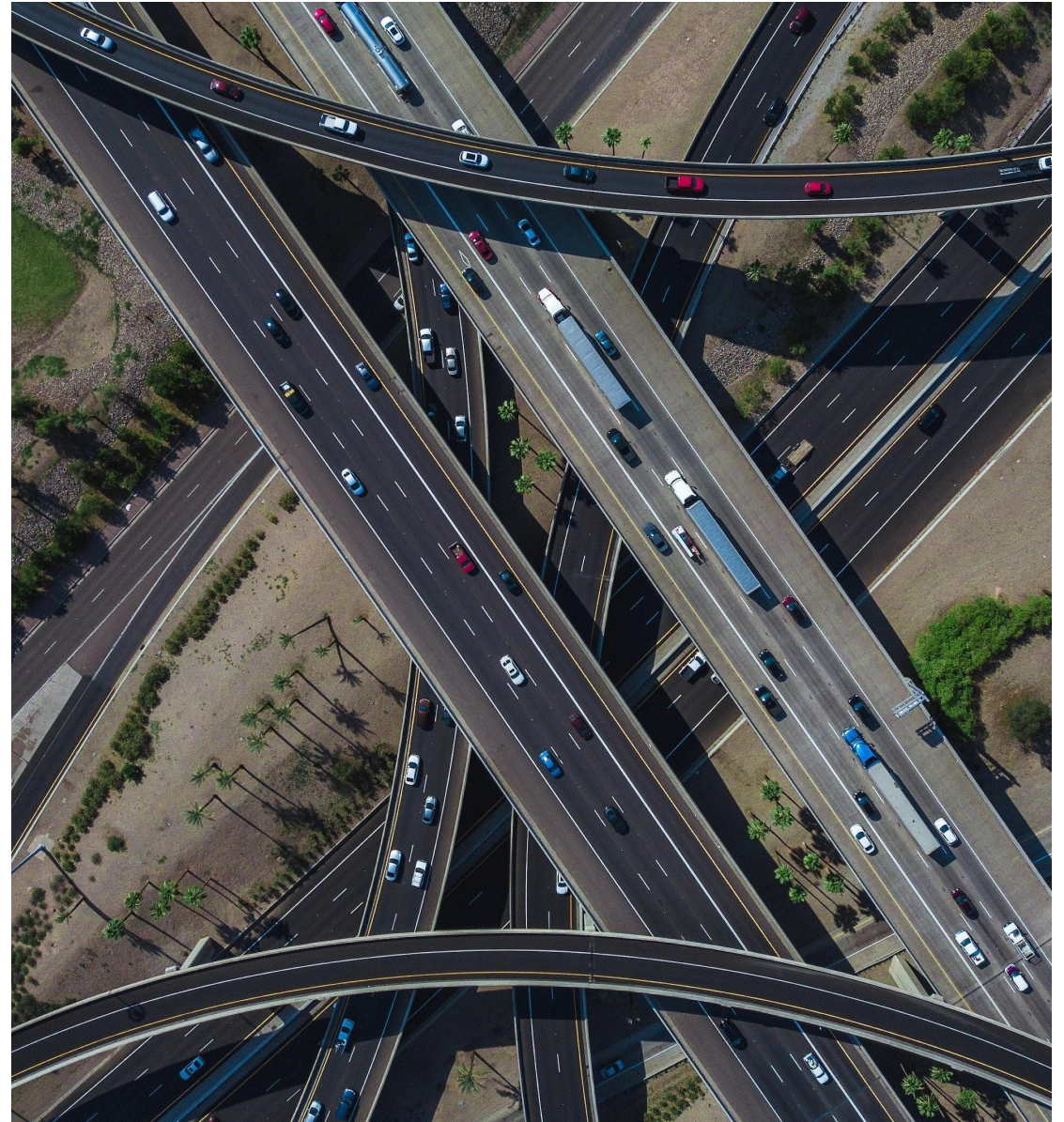
Integrations



Integration Hub

Communications Broker

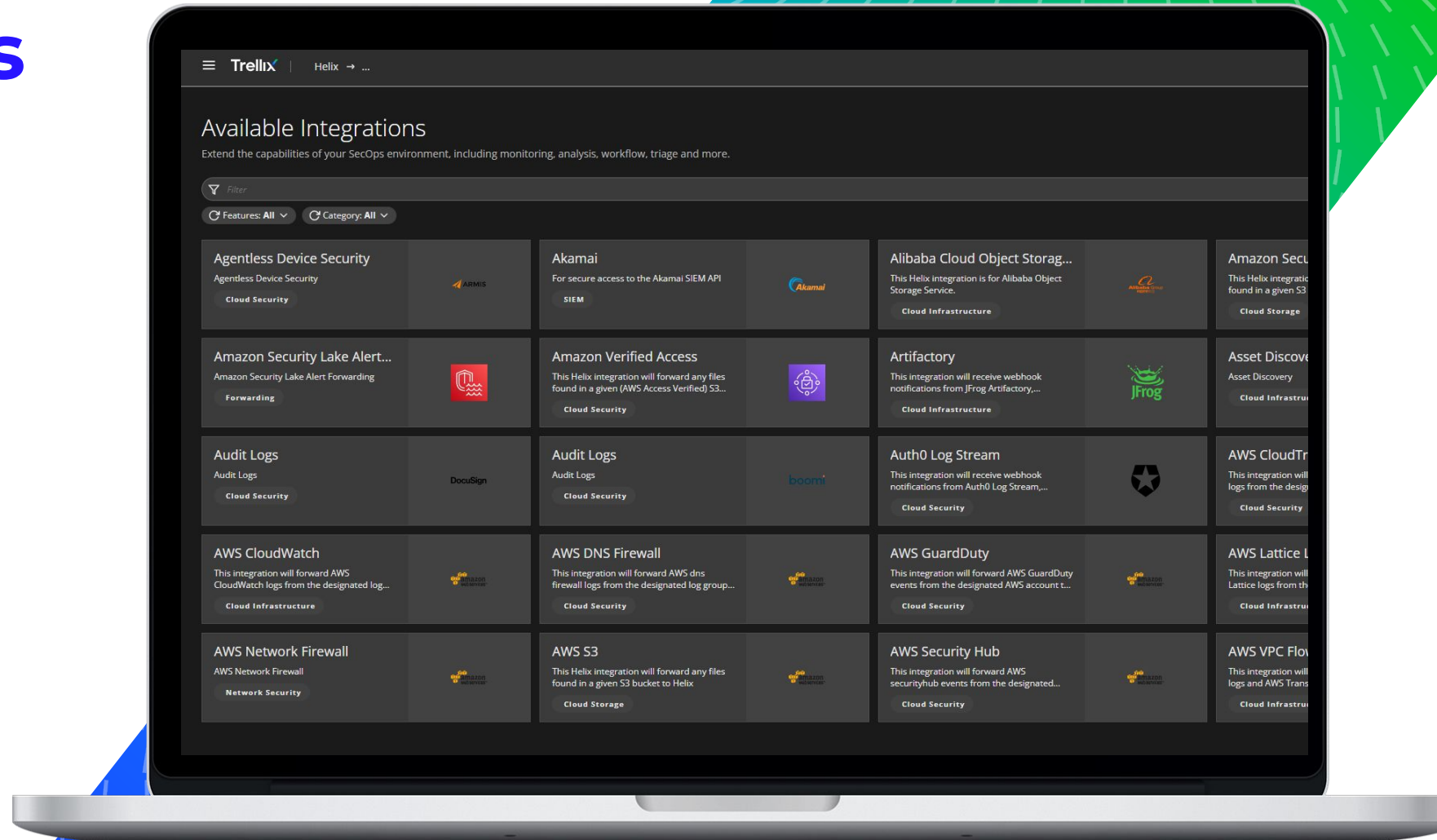
Data Sources



Integrate your Data and Tools

500+
third parties

120+
SaaS solutions
across multiple
domains



Integration Hub

Allow ingestion and response actions performed through API connections.

Agentless Device Security Agentless Device Security Cloud Security		Akamai For secure access to the Akamai SIEM API SIEM		Alibaba Cloud Object Storage Service This Helix integration is for Alibaba Object Storage Service. Cloud Infrastructure		Amazon Security Lake This Helix integration will forward any files found in a given S3 bucket to Helix Cloud Storage	
Amazon Security Lake Alert Forwarding Amazon Security Lake Alert Forwarding Forwarding		Amazon Verified Access This Helix integration will forward any files found in a given (AWS Access Verified) S3 bucket to Helix Cloud Security		Artifactory This integration will receive webhook notifications from JFrog Artifactory,... Cloud Infrastructure		Asset Discovery Asset Discovery Cloud Infrastructure	
Audit Logs Audit Logs Cloud Security		Audit Logs Audit Logs Cloud Security		Auth0 Log Stream This integration will receive webhook notifications from Auth0 Log Stream,... Cloud Security		AWS CloudTrail This integration will forward AWS CloudTrail logs from the designated bucket into... Cloud Security	
AWS CloudWatch This integration will forward AWS CloudWatch logs from the designated log group to Helix Cloud Infrastructure		AWS DNS Firewall This integration will forward AWS dns firewall logs from the designated log group to Helix Cloud Security		AWS GuardDuty This integration will forward AWS GuardDuty events from the designated Amazon S3 bucket to Helix Cloud Security		AWS Lattice Logs This integration will forward AWS VPC Lattice logs from the designated bucket into... Cloud Infrastructure	
AWS Network Firewall AWS Network Firewall Network Security		AWS S3 This Helix integration will forward any files found in a given S3 bucket to Helix Cloud Storage		AWS Security Hub This integration will forward AWS securityhub events from the designated Amazon S3 bucket to Helix Cloud Security		AWS VPC Flow Logs This integration will forward AWS VPC Flow logs and AWS Transit Gateway flow logs... Cloud Infrastructure	

1 - 20 of 128 < 1 2 3 4 5 >

Evidence Collector

Allow traffic, events and logs to be sent to Helix.

- **Evidence Collector** is a virtual network security sensor. It is the default Helix network security sensor running on a simplified virtual Network Security appliance that uses Suricata to generate L7 metadata events from network traffic and streams these to Helix.
- Evidence Collector can also stream third-party logs directly to Helix. It supports the Tapsender, Communications Broker, event filter, and data streaming features. It does not offer detection.
- It can also be enabled on a physical Network Security appliance.

Communication Broker

Allow events and logs to be sent to Helix through syslog.

- Helix uses the **Communication Broker (Commbroker) 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 receiver component present in the customer's environment 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.

Data Sources for Helix

SecOps effectiveness depends on the data sources available for analysis

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

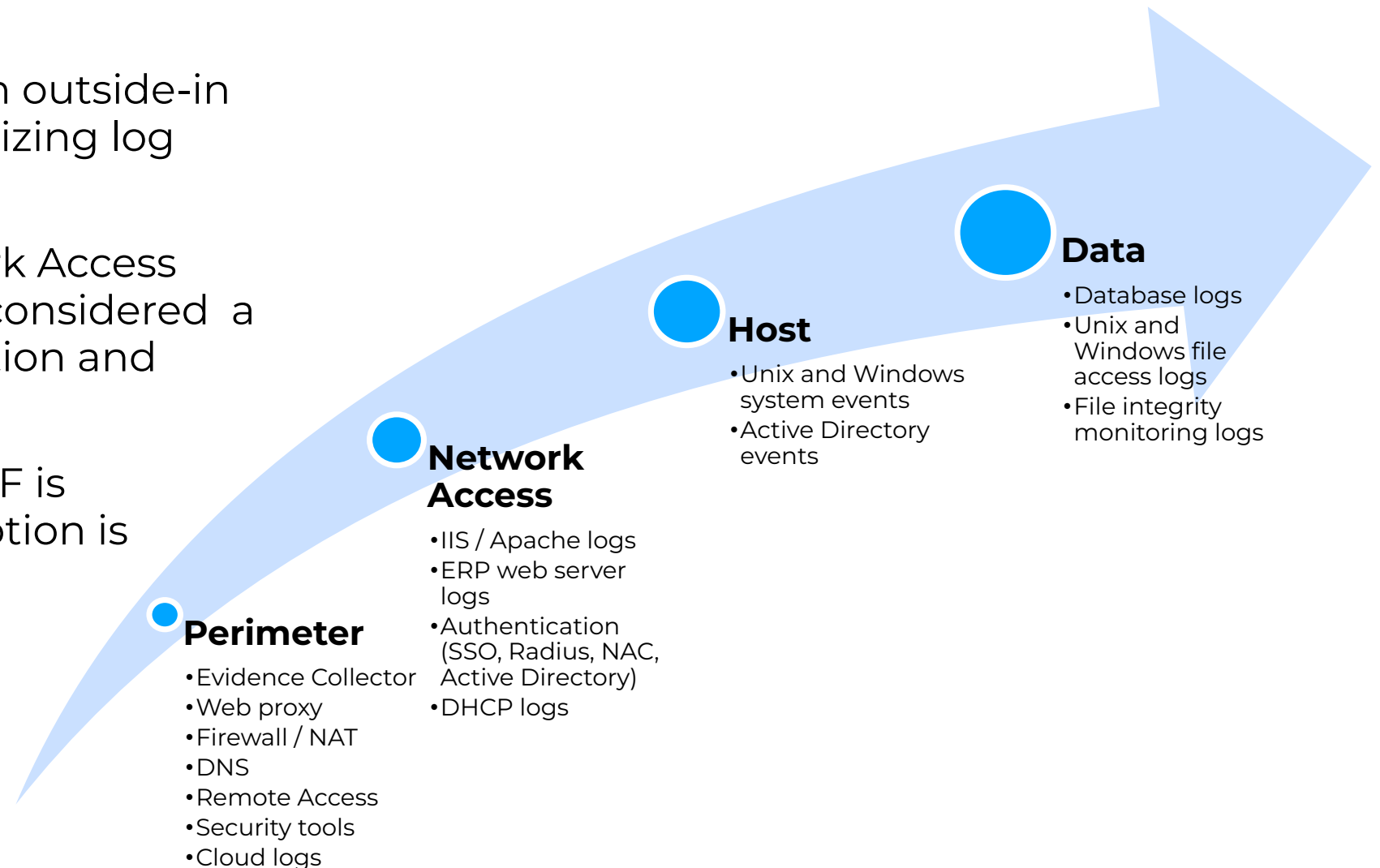
Critical Data Sources

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

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

Data Sources by Priority

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



Event Data

Format Data
TQL



Event Format

meta_ts	Raw & Parsed
2025-10-20 12:12:31 UTC ▾	1427116186.019480 C73ZO2ThDIOt77xo5 10.224.72.20 21729 23.99.20.198 443 1 GET 23.99.20.198 /image001.gif - Mozilla/5.0 (Windows NT 6.1; rv:36.0) Gecko/20100101 Firefox/36.0 0 75264 200 OK - -- (empty) ----- F6owdI3BUrc0kvzpWi application/x-dosexec class: bro_http ▾ connectionid: c73zo2thdlot77xo5 ▾ depth: 1 ▾ domain: 23.99.20.198 ▾ dstcity: san francisco ▾ dstcountry: united states of america ▾ dstcountrycode: 840 ▾ dstdomain: microsoft.com ▾ dstipv4: 23.99.20.198 ▾ dstisp: microsoft corp ▾ dstlatitude: 37.720001220703125 ▾ dstlongitude: -122.44000244140625 ▾ dstport: 443 ▾ dstregion: california ▾ event_epoch: {"day":23,"hour":13,"year":2015,"month":3,"minute":9,"second":46,"weekday":"monday","timezone":"utc","epochtime_field":"eventtimeutc"} ▾ eventtimeutc: 2015-03-23T13:09:46.019Z ▾ httpmethod: get ▾ meta_cbid: 10121144 ▾ meta_cbname: xfire-hexcbh829-xdr ▾ meta_i: 10.12.1.144/514/tcp ▾ meta_omh: <23>Mar 1 22:17:27 broworker3 bro_http: ▾ meta_oml: 293 ▾ meta_rts: 2025-10-20T12:12:31.665Z ▾ meta_rule: bro_http-2223679616 ▾ meta_sip4: 10.12.1.226 ▾ meta_sp: 49980 ▾ meta_ts: 2025-10-20 12:12:31 UTC ▾ metaclass: http_proxy ▾ program: bro_http ▾ raw_pri: 23 ▾ rawmsg: "1427116186.019480\tC73ZO2ThDIOt77xo5\t10.224.72.20\t21729\t23.99.20.198\t443\t1\tGET\t23.99.20.198\t/image001.gif\t\tMozilla/5.0 (Windows NT 6.1; rv:36.0) Gecko/2010... ▾ rawmsghostname: broworker3 ▾ rawsrchostname: 10.12.1.226 ▾ rcvdbodybytes: 75264 ▾ rcvdfileid: f6owdi3burc0kvzpw ▾ rcvdmimetype: application/x-dosexec ▾ sentbodybytes: 0 ▾ srccity: private ▾ srccountry: reserved/private ▾ srccountrycode: 999 ▾ srcipv4: 10.224.72.20 ▾ srcport: 21729 ▾ srcregion: reserved/private ▾ statuscode: 200 ▾ statusmsg: ok ▾ tags: (empty) ▾ uri: /image001.gif ▾ _eventid: 10d32742-adae-11f0-b981-9f4bbc084043#2 ▾ uri_parsed: /image001.gif ▾ useragent: mozilla/5.0 (windows nt 6.1; rv:36.0) gecko/20100101 firefox/36.0 ▾ __metadata__: {"id":"10d32742-adae-11f0-b981-9f4bbc084043#2","batch_id":"10d32742-adae-11f0-b981-9f4bbc084043","received":"2025-10-20T12:12:36.000Z","data_type":"syslog","num_... ▾

Events

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

The screenshot shows the 'Add New Integrations' interface. On the left, three blue boxes with labels 'Sender Name', 'Field Mapping', and 'Class Name' have arrows pointing to specific fields in the 'Feature Settings' section. The 'Sender Name' box points to the 'Sender Name' field. The 'Field Mapping' box points to the '(Optional) Field Mapping' field. The 'Class Name' box points to the '(Optional) Helix Class Name' field.

Add New Integrations Cancel Add & Verify Integration

Details

Integration Name *

Description

Tags

Feature Settings

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

Sender Name ⓘ

(Optional) Field Mapping ⓘ

(Optional) Helix Class Name ⓘ

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

Preformat Your Data

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

Submit and Note API Key

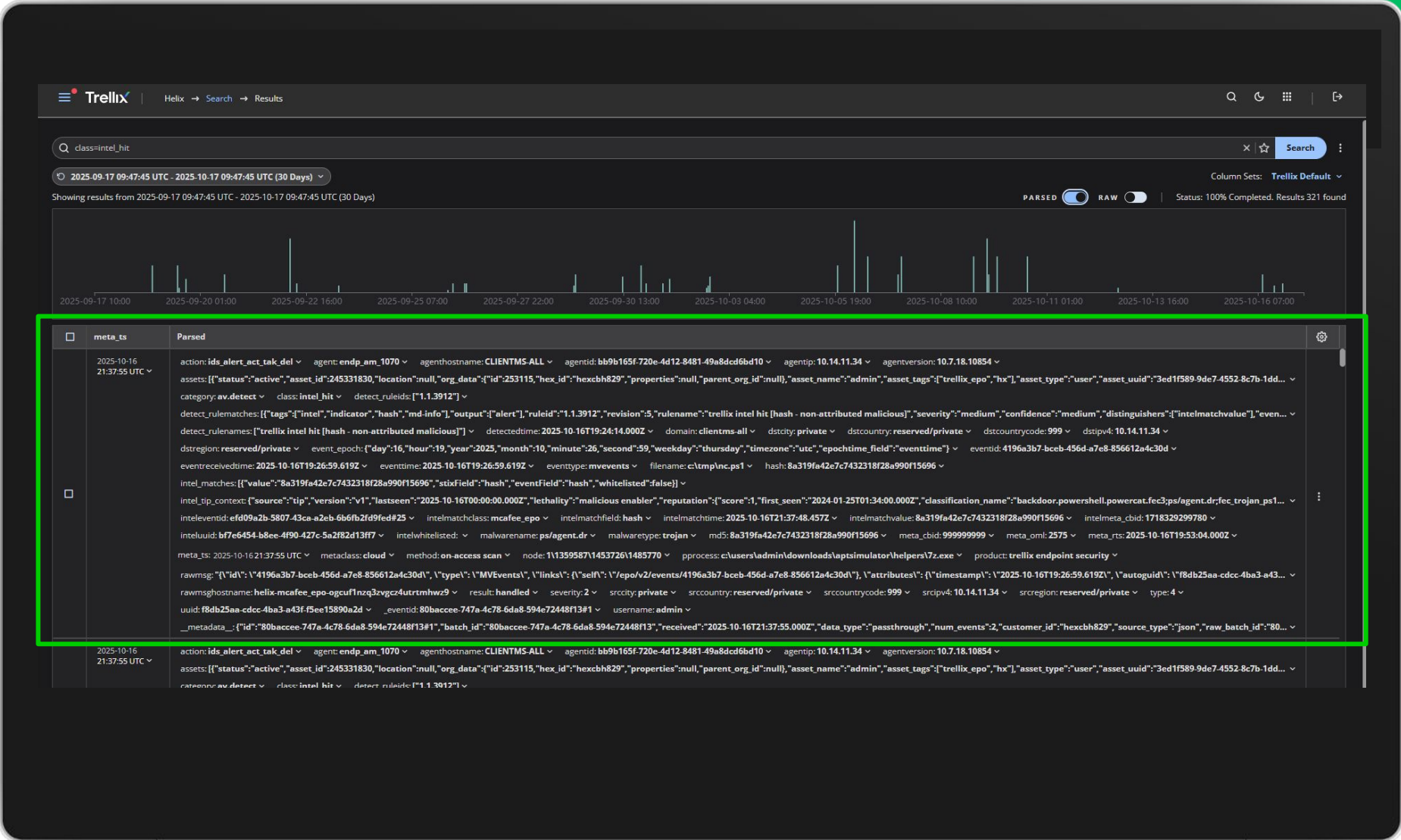
1. Note the URL and example curl command below. This will allow you to send JSON-formatted events into the Helix ID you have selected.
2. After clicking Submit and Verify, you will be presented with the API key to use. Please record it and use it in place of the \$APIKEY variable as shown below.
3. Example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

Events

Parsed / Indexed Fields

Geographic Fields

Metadata Fields



Parsing

Event Classes (Past 24 Hours)

fireeye_nx	1.7m	ms_windows_event	54.4k	aws_cloudwatch	10.2k	mvision_edr	9.9k	crowdstrike	9.1k
cisco_pix	6.9k	fireeye_hx_sysinfo	3.4k	slack	3.0k	trellix_audit	1.7k	unknown	1.7k
aws_vpc_flow	1.4k	appliance_health	1.2k	intel_hit	1.1k	ms_office365	631	fireeye_stats	598
mcafee_epo	500	aws_cloudtrail	404	fireeye_hx_alert	223	alerts	214	crowdstrike_falconhost	168
fireeye_nx_alert	164	fireeye_dod	111	bro_conn	108	bro_files	108	aws_guardduty	92
bro_http	84	analytics_beta	48	fireeye	48	ms_dns	48	bro_smtp	24
mandiant_mso	24	analytics	16	okta	7	fireeye_localsig	3	web_server	3
salesforce_appomni	2								

Class and Metaclass

- Critical for rule function
- Class is device / technology specific
- Metaclass buckets like devices/technologies
- Class=unknown means no matching parser

Native parsers out of the box

- Control over parsing ensures rule consistency

Custom parsers can be built by customers

- Typically needed for unknown syslog / CEF
- Complex

Trellix Query Language

Trellix Query Language (TQL) is a data analysis language used in queries to retrieve events for further analysis.

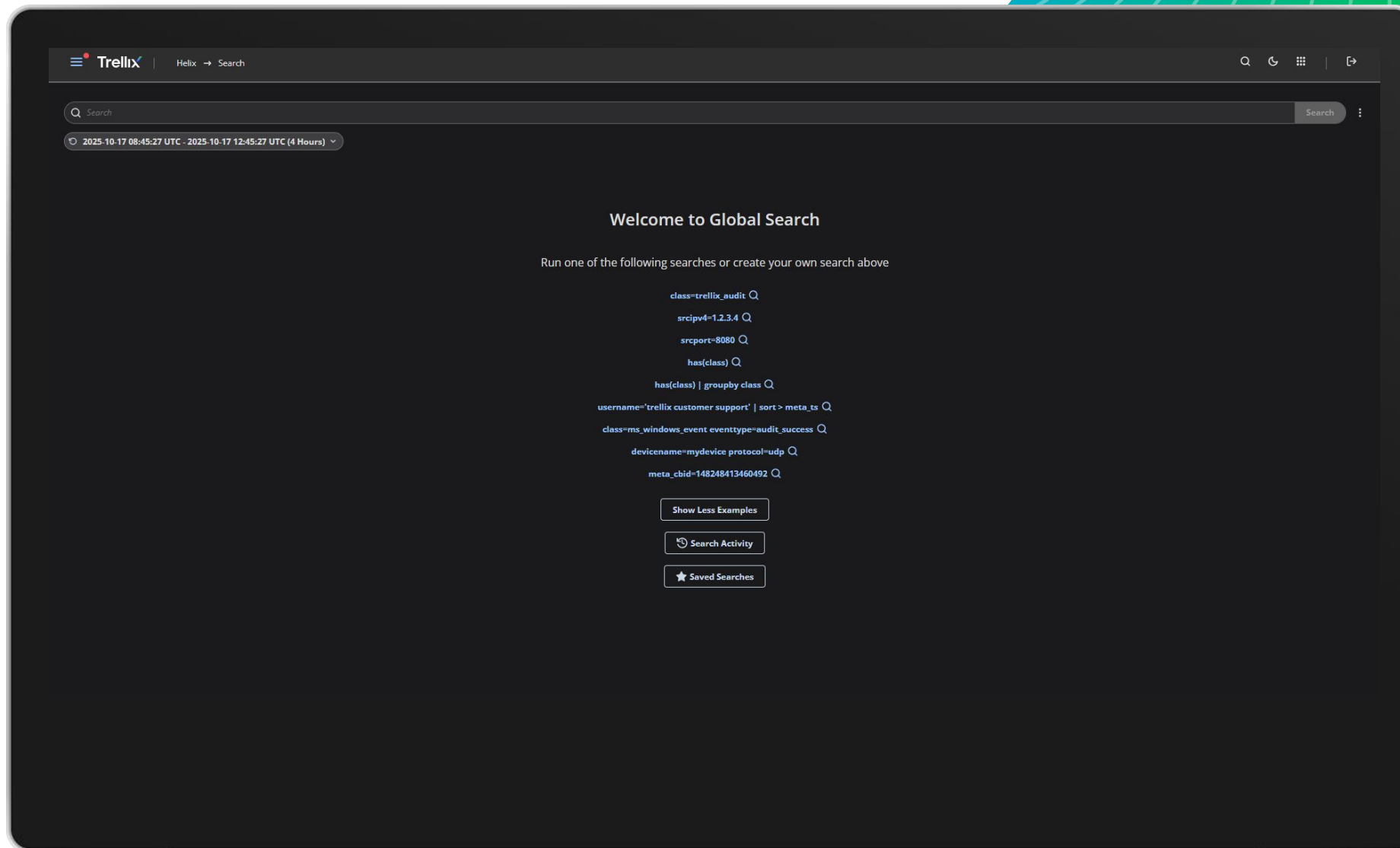
The screenshot displays the Trellix Helix Search interface. At the top, the Trellix logo and 'Helix → Search' are visible. Below the header, a search bar contains the query 'class="bro_http"'. To the right of the search bar are icons for search, settings, and a grid. Below the search bar, a date range filter is set to '2025-10-20 10:48:59 UTC - 2025-10-20 14:48:59 UTC (4 Hours)'. To the right of the date range, the column sets are set to 'Trellix Default'. The main content area is titled 'Welcome to Global Search' and includes the instruction 'Run one of the following searches or create your own search above'. Below this, a list of example queries is provided, each with a magnifying glass icon: 'class=trellix_audit', 'srcip4=1.2.3.4', 'srcport=8080', 'has(class)', 'has(class) | groupby class', 'username='trellix customer support' | sort > meta_ts', 'class=ms_windows_event eventtype=audit_success', 'devicename=mydevice protocol=udp', and 'meta_cbid=148248413460492'. At the bottom of the interface, there are three buttons: 'Show Less Examples', 'Search Activity', and 'Saved Searches'.

TQL Search

Trellix
Query
Language

Search
across all
indexed /
parsed
fields

Rules use
the same
syntax
(with
caveats)



Anatomy of a TQL Query

High-level anatomy of an TQL query:
<filter section> | <transform section>

Q class=ms_office365 | groupby [username]

2025-10-17 00:50:52 UTC - 2025-10-17 12:50:52 UTC (12 Hours)

Showing results from 2025-10-17 00:50:52 UTC - 2025-10-17 12:50:52 UTC (12 Hours) | Status: 100% Completed. Results 232 found

username	Count
extuser@extld.com	148
mr.smith@fetld.com	4
intuser@fetld.com	3
cwilliams@holmes.org	2
danielwong@yahoo.com	2
dominguezerika@hotmail.com	2

TQL query can use two types of clauses:

- **Searches:** data to be located based on exact matches, comparisons, ranges, and expressions.
- **Transforms:** allow you to modify the way that your query results are returned and displayed [Groupby, Sort,]

TQL - Examples

Trellix

Helix → Search → Results

extuser

2025-10-17 00:50:52 UTC - 2025-10-17 12:50:52 UTC (12 Hours)

PARSED RAW

Status: 100% Completed. Results 148 found

00:5101:1601:4102:0602:3102:5603:2103:4604:1104:3605:0105:2605:5106:1606:4107:0607:3107:5608:2108:4609:1109:3610:0110:2610:5111:1611:4112:0612:31

meta_ts	Parsed
2025-10-17 12:00:07 UTC	accountid: not available action: userloginfailed class: ms_office365 detect_ruleids: ["1.1.2663", "1.1.2664"] detect_rulenames: ["office 365 [brute force attempt by user]", "office 365 [brute force attempt by ip]"] event_epoch: {"day": 17, "hour": 12, "year": 2025, "month": 10, "minute": 0, "second": 7, "weekday": "friday", "timezone": "utc", "epochtime_field": "meta_ts"} eventid: 10c11e45-ef17-4507-bd80-959a8b66940f eventtype: 1 meta_cbid: 10121144 meta_cbname: xfire-hexcbh829-xdr meta_i: 10.12.1.144/512/tcp meta_oml: 4267 meta_rts: 2025-10-17T12:00:07.399Z meta_rule: ms_office365-ss-0.1.2 meta_sip4: 10.12.1.226 meta_sp: 56402 meta_ts: 2025-10-17 12:00:07 UTC metaclass: app_transaction object: unknown rawmsg: {"username": "extuser@extld.com", "meta_sip4": "10.12.1.1", "eventid": "abc123-def456-11e1-aa2bb3cc4#751", "rawmsg": {"creationtime": "2019-01-09t03:22:15", "id": "10c11e45-ef17-4507-bd80-959a8b66940f", "operation": "userloginfailed", "source": "extuser@extld.com", "target": "10.12.1.144/512/tcp", "type": "userloginfailed"}, "rawmsg_ghostname": "10.12.1.226", "rawsrchostname": "10.12.1.226", "result": "failed", "service": "azureactivedirectory", "srccity": "nantong", "srccountry": "china", "srccountrycode": "cn", "srcdomain": "telecom.com.cn", "srcip": "114.216.106.130", "srcip4": "114.216.106.130", "srcip6": "2601:100:0000:0000:0000:0000:0000:0000", "srcip8": "2601:100:0000:0000:0000:0000:0000:0000", "srcip16": "2601:100:0000:0000:0000:0000:0000:0000", "srcip32": "2601:100:0000:0000:0000:0000:0000:0000", "srcip64": "2601:100:0000:0000:0000:0000:0000:0000", "srcip128": "2601:100:0000:0000:0000:0000:0000:0000", "srcip256": "2601:100:0000:0000:0000:0000:0000:0000", "srcip512": "2601:100:0000:0000:0000:0000:0000:0000", "srcip1024": "2601:100:0000:0000:0000:0000:0000:0000", "srcip2048": "2601:100:0000:0000:0000:0000:0000:0000", "srcip4096": "2601:100:0000:0000:0000:0000:0000:0000", "srcip8192": "2601:100:0000:0000:0000:0000:0000:0000", "srcip16384": "2601:100:0000:0000:0000:0000:0000:0000", "srcip32768": "2601:100:0000:0000:0000:0000:0000:0000", "srcip65536": "2601:100:0000:0000:0000:0000:0000:0000", "srcip131072": "2601:100:0000:0000:0000:0000:0000:0000", "srcip262144": "2601:100:0000:0000:0000:0000:0000:0000", "srcip524288": "2601:100:0000:0000:0000:0000:0000:0000", "srcip1048576": "2601:100:0000:0000:0000:0000:0000:0000", "srcip2097152": "2601:100:0000:0000:0000:0000:0000:0000", "srcip4194304": "2601:100:0000:0000:0000:0000:0000:0000", "srcip8388608": "2601:100:0000:0000:0000:0000:0000:0000", "srcip16777216": "2601:100:0000:0000:0000:0000:0000:0000", "srcip33554432": "2601:100:0000:0000:0000:0000:0000:0000", "srcip67108864": "2601:100:0000:0000:0000:0000:0000:0000", "srcip134217728": "2601:100:0000:0000:0000:0000:0000:0000", "srcip268435456": "2601:100:0000:0000:0000:0000:0000:0000", "srcip536870912": "2601:100:0000:0000:0000:0000:0000:0000", "srcip1073741824": "2601:100:0000:0000:0000:0000:0000:0000", "srcip2147483648": "2601:100:0000:0000:0000:0000:0000:0000", "srcip4294967296": "2601:100:0000:0000:0000:0000:0000:0000", "srcip8589934592": "2601:100:0000:0000:0000:0000:0000:0000", "srcip17179869184": "2601:100:0000:0000:0000:0000:0000:0000", "srcip34359738368": "2601:100:0000:0000:0000:0000:0000:0000", "srcip68719476736": "2601:100:0000:0000:0000:0000:0000:0000", "srcip137438953472": "2601:100:0000:0000:0000:0000:0000:0000", "srcip274877906944": "2601:100:0000:0000:0000:0000:0000:0000", "srcip549755813888": "2601:100:0000:0000:0000:0000:0000:0000", "srcip1099511627776": "2601:100:0000:0000:0000:0000:0000:0000", "srcip2199023255552": "2601:100:0000:0000:0000:0000:0000:0000", "srcip4398046511104": "2601:100:0000:0000:0000:0000:0000:0000", "srcip8796093022208": "2601:100:0000:0000:0000:0000:0000:0000", "srcip17592186044416": "2601:100:0000:0000:0000:0000:0000:0000", "srcip35184372088832": "2601:100:0000:0000:0000:0000:0000:0000", "srcip70368744177664": "2601:100:0000:0000:0000:0000:0000:0000", "srcip140737488355328": "2601:100:0000:0000:0000:0000:0000:0000", "srcip281474976710656": "2601:100:0000:0000:0000:0000:0000:0000", "srcip562949953421312": "2601:100:0000:0000:0000:0000:0000:0000", "srcip1125899906842624": "2601:100:0000:0000:0000:0000:0000:0000", "srcip2251799813685248": "2601:100:0000:0000:0000:0000:0000:0000", "srcip4503599627370496": "2601:100:0000:0000:0000:0000:0000:0000", "srcip9007199254740992": "2601:100:0000:0000:0000:0000:0000:0000", "srcip18014398509481984": "2601:100:0000:0000:0000:0000:0000:0000", "srcip36028797018963968": "2601:100:0000:0000:0000:0000:0000:0000", "srcip72057594037927936": "2601:100:0000:0000:0000:0000:0000:0000", "srcip144115188075855872": "2601:100:0000:0000:0000:0000:0000:0000", "srcip288230376151711744": "2601:100:0000:0000:0000:0000:0000:0000", "srcip576460752303423488": "2601:100:

TQL - Transform Examples #1

 Helix → Search → Results

Q

class="fireeye_etp" | groupby [objecttype]

× ☆ Search ⋮

🕒 2025-09-23 10:15:24 UTC - 2025-10-23 10:15:24 UTC (30 Days) ▼

Showing results from 2025-09-23 10:15:24 UTC - 2025-10-23 10:15:24 UTC (30 Days)

🔄

Status: Running. 50% Completed. Results 12.9K found

objecttype	Count
url ▼	2023
zip ▼	219
docx ▼	115
file ▼	75
xlsx ▼	54
ppt ▼	53
pdf ▼	17
doc ▼	11

TQL - Transform Examples #2

 Trellix

Helix → Search → Results



 class="fireeye_etp" | groupby [objecttype, result]

 Search 

 2025-09-23 10:15:24 UTC - 2025-10-23 10:15:24 UTC (30 Days) 

Showing results from 2025-09-23 10:15:24 UTC - 2025-10-23 10:15:24 UTC (30 Days)

 Status: Running. 50% Completed. Results 12.9K found

objecttype	result	Count
url 	non-malicious 	1972
zip 	malicious 	164
docx 	malicious 	114
zip 	non-malicious 	55
xlsx 	non-malicious 	54
url 	malicious 	51
ppt 	non-malicious 	50
file 	non-malicious 	45



TQL - Functions Examples #1

Trellix

Helix → Search → Results

🔍 ↻ 🗖️ | 🔗

🔍 class="fireeye_etp" has:domain result:"malicious"

✕ ☆ Search ⋮

🕒 2025-09-23 10:15:24 UTC - 2025-10-23 10:15:24 UTC (30 Days) ▾

Column Sets: EmailSecurity ▾

Showing results from 2025-09-23 10:15:24 UTC - 2025-10-23 10:15:24 UTC (30 Days)

PARSED ☒ RAW ☐ |

🔄 Status: Running. 50% Completed. Results 51 found

☐	meta_ts	class	metaclass	domain	result	⚙️
☐	2025-10-20 11:50:17 UTC ▾	fireeye_etp ▾	email ▾	assets.bbhub.io ▾	malicious ▾	⋮
☐	2025-10-20 11:49:31 UTC ▾	fireeye_etp ▾	email ▾	assets.bbhub.io ▾	malicious ▾	⋮
☐	2025-10-20 11:49:13 UTC ▾	fireeye_etp ▾	email ▾	assets.bbhub.io ▾	malicious ▾	⋮
☐	2025-10-20 11:48:30 UTC ▾	fireeye_etp ▾	email ▾	assets.bbhub.io ▾	malicious ▾	⋮
☐	2025-10-17 04:46:26 UTC ▾	fireeye_etp ▾	email ▾	foodhubrichingspark.org ▾	malicious ▾	⋮
☐	2025-10-17 03:53:19 UTC ▾	fireeye_etp ▾	email ▾	go.ginobillard.com ▾	malicious ▾	⋮

Rows

50 100 500 1000

1 - 50 of 51 < 1 2 >

Alerting

Rules
Analytics
Correlations
UEBA
Cases



Rules

Rules

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

Actions

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

Analytics

50+ deployed analytics

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

Trellix Rules | Reset Layout [13] Customer Rules

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

Rule creation tool

Trellix

Helix → Rules → Create Custom Rule

Q ↺ ⋮ ⌕

Create Custom Rule

CancelSave

Definition & Settings

Definition

Rule ID

--

Name

Recon - Recon Events from a Local Host

Description (Optional)

Description of rule

Severity

Unknown

1 Write your condition here

Settings

Enable Rule

Exclude these lists

Search Lists to exclude

Tags

Search tags...

Trellix

ACE – Advanced Correlation Engine

Example 01 – A Simple Rule

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

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

ACE – Advanced Correlation Engine

Example 02 – A Simple Rule with a Threshold

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

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

ACE – Advanced Correlation Engine

Example 03 – A Simple Rule with Groupby

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

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

ACE – Advanced Correlation Engine

Example 04 – A Rule that correlates multiple events.

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

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

ACE – Advanced Correlation Engine

Example 05 – A Rule with Cardinality

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

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

Lateral Movement: Suspicious File Write To WindowsApps Folder

Detected a known malware process writing a file to the WindowsApps directory. This action is associated with preparing for lateral movement by exploiting DCOM application objects.

```
groupby: srcipv4
require: 2
within: 1h
ordered: true
items:
- type: correlation
  require: 1
  within: 120s
  items:
  - type: fields
    groupby: "field(\"source\", string)"
    match: "xpod_ds_name == \"ace\" && rule_id == [\"1.1.4004\", \"2.2.0013\", \"\"2.1.0067\", \"2.2.0014\"]"
  - type: fields
    groupby: srcipv4
    match: "xpod_ds_name != \"ace\" && class == \"mcafee_epo\" && category == \"av.detect\" && !(srcipv4 inWatchlist \"exclusions.global.srcipv4\")"
  - type: fields
    groupby: srcipv4
    match: "xpod_ds_name != \"ace\" && class == \"fireeye_nx_alert\" && eventlog == \"malware-object\" && !(srcipv4 inWatchlist \"exclusions.global.srcipv4\")"
- type: fields
  groupby: agentip
  match: "(filename == [\"foxprow.exe\", \"schdplus.exe\", \"winproj.exe\"] && ((class\\
    \\ == \"fireeye_hx_ioc\" && iocnames == \"file write to network share (methodology)\"\\
    \\ && filepath contains \"\\\\\\\\appdata\\\\\\\\local\\\\\\\\microsoft\\\\\\\\windowsapps\\\\\\\\\"\\
    \\ || (metaclass containsNoCase \"windows\" && eventid =~ \"5140\" && severity\\
    \\ =~ \"failure audit\" && filename contains \"\\\\\\\\appdata\\\\\\\\local\\\\\\\\microsoft\\\\\\\\
    \\\\windowsapps\\\\\\\\\"))) || (metaclass containsNoCase \"windows\" && pprocess containsNoCase\\
    \\ [\"\\\\\\\\winword.exe\", \"\\\\\\\\excel.exe\", \"\\\\\\\\powerpnt.exe\", \"\\\\\\\\eqndt32.exe\",
    \\ \"\\\\\\\\onenote.exe\", \"\\\\\\\\Graph.exe\", \"\\\\\\\\MSAccess.exe\", \"\\\\\\\\MSPub.exe\",
    \\ \"\\\\\\\\PowerPoint.exe\", \"\\\\\\\\Visio.exe\", \"\\\\\\\\WinProj.exe\", \"\\\\\\\\WinWord.exe\",
    \\ \"\\\\\\\\Wordpad.exe\"] && process containsNoCase [\"foxprow.exe\", \"schdplus.exe\",
    \\ \"winproj.exe\"])"
```

```
output:
- field: $.source
  value: agentip
metadata:
  attacks:
  - tactics:
    - name: Lateral Movement
      uid: TA0008
    technique:
      name: Lateral Tool Transfer
      uid: T1570
    version: "1.4"
  - tactics:
    - name: Lateral Movement
      uid: TA0008
    technique:
      name: SMB/Windows Admin Shares
      uid: T1021.002
    version: "1.3"
  - tactics:
    - name: Lateral Movement
      uid: TA0008
    technique:
      name: Distributed Component Object Model
      uid: T1021.003
    version: "1.3"
  - tactics:
    - name: Execution
      uid: TA0002
    technique:
      name: Malicious File
      uid: T1204.002
    version: "1.5"
  created: "1730719351"
  recommended_action:
  - 2.1.1
  - 2.1.5
  - 3.2.4
  - 3.2.5
  - 2.3.3
  revision: 3
```

Lat Mov: Susp File Write To WindowsApps Folder - Detail 1/8

Detected a known malware process writing a file to the WindowsApps directory. This action is associated with preparing for lateral movement by exploiting DCOM application objects.

```
groupby: srcipv4
require: 2
within: 1h
ordered: true
items:
```

- all events need to have the same source ipv4 address (otherwise a new instance is forked)
- two of the following items (Detail 2-5 AND Detail 6)
 - need to match for the rule to trigger
 - within 1 hour
 - order does matter

Lat Mov: Susp File Write To WindowsApps Folder - Detail 2/8

Detected a known malware process writing a file to the WindowsApps directory. This action is associated with preparing for lateral movement by exploiting DCOM application objects.

- type: correlation
 - require: 1
 - within: 120s
 - items:
 - This rule is of the type "standard rule correlation"
 - this item needs
 - one occurrence
 - of the following (see next three slides) to happen
 - within 120 seconds

Lat Mov: Susp File Write To WindowsApps Folder - Detail 3/8

Detected a known malware process writing a file to the WindowsApps directory. This action is associated with preparing for lateral movement by exploiting DCOM application objects.

```
- type: fields
  groupby: "field(\"source\", string)"
  match: "xpod_ds_name == \"ace\" && rule_id == [\"1.1.4004\", \"2.2.0013\", \"2.1.0067\", \"2.2.0014\"]"
```

- matches on fields (of events)
- Event needs to
 - originate from the data source (xpod_ds_name) ACE
 - AND
 - must have rule_id 1.1.4004 or 2.2.0013 or 2.1.0067 or 2.2.0014

Lat Mov: Susp File Write To WindowsApps Folder - Detail 4/8

Detected a known malware process writing a file to the WindowsApps directory. This action is associated with preparing for lateral movement by exploiting DCOM application objects.

```
- type: fields
  groupby: srcipv4
  match: xpod_ds_name != "ace" && class == "mcafee_epo" && category == "av.detect"
        && !(srcipv4 inWatchlist "exclusions.global.srcipv4")
```

- matches on fields (of events)
- Event needs to
 - originate NOT from the data source (xpod_ds_name) ACE
 - AND
 - have class "mcafee_epo"
 - AND
 - have category "av.detect"
 - AND
 - must NOT have sourceipv4 present in watchlist exclusions.global.sourceipv4

Lat Mov: Susp File Write To WindowsApps Folder - Detail 5/8

Detected a known malware process writing a file to the WindowsApps directory. This action is associated with preparing for lateral movement by exploiting DCOM application objects.

```
- type: fields
  groupby: srcipv4
  match: xpod_ds_name != "ace" && class == "fireeye_nx_alert" && eventlog == "malware-object"
        && !(srcipv4 inWatchlist "exclusions.global.srcipv4")
```

- matches on fields (of events)
- Event needs to
 - originate NOT from the data source (xpod_ds_name) ACE
 - AND
 - have class "fireeye_nx_alert"
 - AND
 - have eventlog "malware-object"
 - AND
 - must NOT have sourceipv4 present in watchlist exclusions.global.sourceipv4

Lat Mov: Susp File Write To WindowsApps Folder - Detail 6/8

Detected a known malware process writing a file to the WindowsApps directory. This action is associated with preparing for lateral movement by exploiting DCOM application objects.

```
- type: fields
  groupby: agentip
  match: "(filename == [\"foxprow.exe\", \"schdplus.exe\", \"winproj.exe\"] && ((class\\
    \\ == \"fireeye_hx_ioc\" && iocnames == \"file write to network share (methodology)\"\\
    \\ && filepath contains \"\\\\\\\\appdata\\\\\\\\local\\\\\\\\microsoft\\\\\\\\windowsapps\\\\\\\\\\\\\\\\\"
  ) || (metaclass containsNoCase \"windows\" && eventid =~ \"5140\" && severity\\
    \\ =~ \"failure audit\" && filename contains \"\\\\\\\\\\\\\\\\appdata\\\\\\\\\\\\\\\\local\\\\\\\\\\\\\\\\microsoft\\\\\\\\
    \\\\windowsapps\\\\\\\\\\\\\\\\\"))) || (metaclass containsNoCase \"windows\" && pprocess containsNoCase\\
    \\ [\"\\\\\\\\\\\\\\\\winword.exe\", \"\\\\\\\\\\\\\\\\excel.exe\", \"\\\\\\\\\\\\\\\\powerpnt.exe\", \"\\\\\\\\\\\\\\\\eqnedt32.exe\"\\
    , \"\\\\\\\\\\\\\\\\onenote.exe\", \"\\\\\\\\\\\\\\\\Graph.exe\", \"\\\\\\\\\\\\\\\\MSAccess.exe\", \"\\\\\\\\\\\\\\\\MSPub.exe\"\\
    , \"\\\\\\\\\\\\\\\\PowerPoint.exe\", \"\\\\\\\\\\\\\\\\Visio.exe\", \"\\\\\\\\\\\\\\\\WinProj.exe\", \"\\\\\\\\\\\\\\\\WinWord.exe\"\\
    , \"\\\\\\\\\\\\\\\\Wordpad.exe\"] && process containsNoCase [\"foxprow.exe\", \"schdplus.exe\"\\
    , \"winproj.exe\"])"
```

- ~~On this case, the process is not identified as a malware process~~ AND process is
- ~~AND the severity is high and the event is failure and the file name is methodology~~ AND file name is methodology AND file path is \\appdata\\local\\microsoft\\windowsapps\\exe or MSAppdata\\local\\microsoft\\windowsapps\\exe or WinProj.exe or WinWord.exe or Wordpad.exe AND process contains (case insensitive) foxprow.exe or schdplus.exe or winproj.exe



Lat Mov: Susp File Write To WindowsApps Folder - Detail 7/8

Detected a known malware process writing a file to the WindowsApps directory. This action is associated with preparing for lateral movement by exploiting DCOM application objects.

output:

```
- field: $.source  
  value: agentip
```

- add field "source"
- with value of field "agentip"
- to correlated event

Lat Mov: Susp File Write To WindowsApps Folder - Detail 8/8

Detected a known malware process writing a file to the WindowsApps directory. This action is associated with preparing for lateral movement by exploiting DCOM application objects.

```
metadata:
  attacks:
    - tactics:
      - name: Lateral Movement
        uid: TA0008
    technique:
      name: Lateral Tool Transfer
      uid: T1570
      version: "1.4"
  ...
  created: "1730719351"
  recommended_action:
    - 2.1.1
  ...
  revision: 3
```

- add metadata
 - MITRE mappings
 - creation date (automatic)
 - recommended actions
 - revision information (automatic)

Lateral Movement: Suspicious File Write To WindowsApps Folder

Detected a known malware process writing a file to the WindowsApps directory. This action is associated with preparing for lateral movement by exploiting DCOM application objects.

```
groupby: srcipv4
require: 2
within: 1h
ordered: true
items:
- type: correlation
  require: 1
  within: 120s
  items:
  - type: fields
    groupby: "field(\"source\", string)"
    match: "xpod_ds_name == \"ace\" && rule_id == [\"1.1.4004\", \"2.2.0013\", \"\"2.1.0067\", \"2.2.0014\"]"
  - type: fields
    groupby: srcipv4
    match: "xpod_ds_name != \"ace\" && class == \"mcafee_epo\" && category == \"av.detect\" && !(srcipv4 inWatchlist \"exclusions.global.srcipv4\")"
  - type: fields
    groupby: srcipv4
    match: "xpod_ds_name != \"ace\" && class == \"fireeye_nx_alert\" && eventlog == \"malware-object\" && !(srcipv4 inWatchlist \"exclusions.global.srcipv4\")"
- type: fields
  groupby: agentip
  match: "(filename == [\"foxprow.exe\", \"schdplus.exe\", \"winproj.exe\"] && ((class\\
    \\ == \"fireeye_hx_ioc\" && iocnames == \"file write to network share (methodology)\\\"\\
    \\ && filepath contains \"\\\\\\\\appdata\\\\\\\\local\\\\\\\\microsoft\\\\\\\\windowsapps\\\\\\\\\\\\\\\\\\
    \\ || (metaclass containsNoCase \"windows\" && eventid =~ \"5140\" && severity\\
    \\ =~ \"failure audit\" && filename contains \"\\\\\\\\appdata\\\\\\\\local\\\\\\\\microsoft\\\\\\\\
    \\\\windowsapps\\\\\\\\\\\\\\\\\\\"))) || (metaclass containsNoCase \"windows\" && pprocess containsNoCase\\
    \\ [\"\\\\\\\\winword.exe\", \"\\\\\\\\excel.exe\", \"\\\\\\\\powerpnt.exe\", \"\\\\\\\\eqndt32.exe\", \\
    , \"\\\\\\\\onenote.exe\", \"\\\\\\\\Graph.exe\", \"\\\\\\\\MSAccess.exe\", \"\\\\\\\\MSPub.exe\", \\
    , \"\\\\\\\\PowerPoint.exe\", \"\\\\\\\\Visio.exe\", \"\\\\\\\\WinProj.exe\", \"\\\\\\\\WinWord.exe\", \\
    , \"\\\\\\\\Wordpad.exe\", \"&& process containsNoCase [\"foxprow.exe\", \"schdplus.exe\", \\
    , \"winproj.exe\"])"
```

```
output:
- field: $.source
  value: agentip
metadata:
  attacks:
  - tactics:
    - name: Lateral Movement
      uid: TA0008
    technique:
      name: Lateral Tool Transfer
      uid: T1570
    version: "1.4"
  - tactics:
    - name: Lateral Movement
      uid: TA0008
    technique:
      name: SMB/Windows Admin Shares
      uid: T1021.002
    version: "1.3"
  - tactics:
    - name: Lateral Movement
      uid: TA0008
    technique:
      name: Distributed Component Object Model
      uid: T1021.003
    version: "1.3"
  - tactics:
    - name: Execution
      uid: TA0002
    technique:
      name: Malicious File
      uid: T1204.002
    version: "1.5"
  created: "1730719351"
  recommended_action:
  - 2.1.1
  - 2.1.5
  - 3.2.4
  - 3.2.5
  - 2.3.3
  revision: 3
```

User & Entity Behavior Analytics

Monitor user and entity activity over time to identify anomalies

Examples

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

Investigation



Alerts

Cases

Wise for Helix



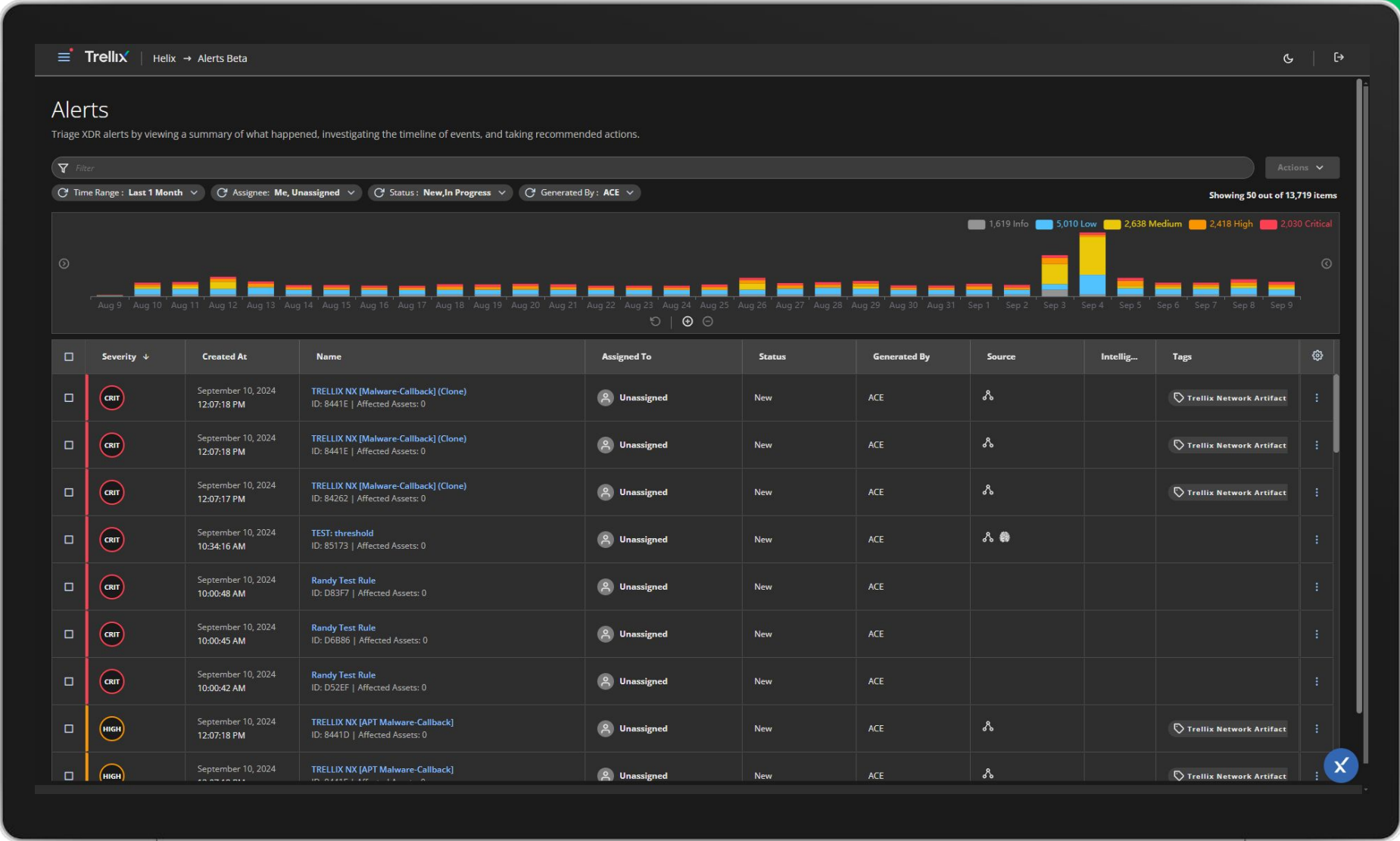
Alerts

Alert
Based
Triage

Traditional
Approach

Who?
What?
Where?

Correlated
and
Aggregated



Managing Alerts

Helix → Alerts → Lateral Movement: PsExec Execution Detected

ALERT 1F0AA | RULE 2.2.0030

Lateral Movement: PsExec Execution Detected

Detected the use of PsExec to move laterally between systems. Adversaries use this legitimate administration tool to execute code on remote hosts.

Correlation
Methodology
Multi-Vector

MEDIUM

CASE: -
ASSIGNEE: -
STATUS: New

MITRE ATT&CK

Summary
Alert Details
Respond

Intelligence
MITRE
Assets
History
Notes

GROUP BY
ALERTS 2
CHILD EVENTS
STANDALONE EVENTS
ACTIONS 0

srcipv4: 10.14.65.167
agentip: 10.14.65.167
2
2
2
0

Timeline
Table

Severity: All
Source: All

NETWORK
2025-10-16 16:22:16 UTC
2

EVENT | MITRE System Services
Trellix NX identified suspicious smartvision-event

action: notified
dstipv4: 65.87.182.33
dstport: 445
srcipv4: 10.14.65.167

ENDPOINT
2025-10-16 16:22:16 UTC
1

MED
ALERT 1F0AA | RULE 1.1.2399 | MITRE Ingress Tool Transfer
Trellix Endpoint HX: IOC Alert - certutil.exe downloader a (utility)
Trellix Endpoint Security (HX) detected a process execution that corresponds to a defined IOC, signaling a potential security event.

agentip: 10.14.65.167
process: certutil.exe
username: selabs\pablo.aguilar
agenthostname: 150655-paguilar-Marketing

ENDPOINT
2025-10-16 16:22:16 UTC
1

MED
ALERT 1F0AA | RULE 1.1.2399 | MITRE PowerShell
Trellix Endpoint HX: IOC Alert - suspicious powershell usage (methodology)
Trellix Endpoint Security (HX) detected a process execution that corresponds to a defined IOC, signaling a potential security event.

agentip: 10.14.65.167
process: powershell.exe
username: selabs\pablo.aguilar
agenthostname: 150655-paguilar-Marketing

Cases

Promote Alerts and Threats to Cases

Assign Cases

TrellixHelix → Cases Beta

Cases

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

Filter

Actions

Create Case

Assignee: Me, Unassigned

Status: All

Time Filter: All Time

Showing 32 out of 32 results

☐	Severity	Case Name	Assigned To	Status	Created By	Case Created	Last Updated	Tags	
☐	MED	Case TK-01 ID: 49 Affected Assets:	UN Unassigned	Open	TK tkaimoto	06/25/2024 07:26:19 PM	09/10/2024 12:13:08 PM	Test	
☐	CRIT	Alert_DAE4A ID: 48 Affected Assets:	UN Unassigned	Open	RA Randy	06/25/2024 06:08:35 PM	08/27/2024 02:09:43 PM	Test	
☐	LOW	Alert_6CC3D ID: 45 Affected Assets:	UN Unassigned	Open	RA Randy	06/20/2024 08:17:45 AM	07/29/2024 08:58:43 AM	Cases_tag1 SE	
☐	CRIT	Alert_DD955 ID: 47 Affected Assets:	UN Unassigned	Open	TK tkaimoto	06/23/2024 06:27:41 PM	06/24/2024 07:07:47 AM	Test	
☐	CRIT	Alert_42B53 ID: 46 Affected Assets:	UN Unassigned	Open	HE HenrikPM	06/20/2024 10:33:29 AM	06/20/2024 10:33:29 AM		
☐	LOW	Randy demo ID: 27 Affected Assets:	UN Unassigned	Closed	RA Randy	05/02/2024 08:49:00 AM	06/18/2024 04:24:31 PM	Trellix Atomic	
☐	LOW	Alert_3BC2D ID: 40 Affected Assets:	UN Unassigned	Open	MA MariaAlarcon	06/10/2024 04:40:23 AM	06/11/2024 08:31:34 AM	Cases_tag1 SE	
☐	HIGH	Alert_4D2B0 ID: 38 Affected Assets:	UN Unassigned	Open	RA Randy	06/05/2024 07:26:39 AM	06/10/2024 03:29:43 AM	E2e_prod_nx	
☐	CRIT	Alert_4D2B0 ID: 37 Affected Assets:	UN Unassigned	Open	RA Randy	06/05/2024 07:24:39 AM	06/05/2024 07:24:39 AM		
☐	MED	Alert_4956A ID: 36 Affected Assets:	UN Unassigned	Open	RA Randy	05/31/2024 12:17:38 PM	06/03/2024 11:17:08 AM	Trellix Atomic	
☐		Alerts Koi demo							

Rows 501005001000

1 - 32 of 32 < 1 >

Case Details

Trellix

Helix → Cases → Ransom CONTI Detected

Q

🔄

⌵

⌵

MED

MEDIUM

ID: 2808

Ransom CONTI Detected

Intel Hit from Trellix Threat Intel associated with an OAS run by ENS

Passthrough

Endpoint

SEVERITY

Medium

ASSIGNEE

Unassigned

STATUS

Open

⋮

MITRE ATT&CK

Summary

Case Timeline

Intelligence

MITRE

Related Assets

Related Alerts

History

Notes

Key Milestones

Case Created

2025-10-02 15:16:19 UTC

6 days 17 hours 37 minutes

MS Matteo Spiga

Last Updated

2025-10-09 08:54:07 UTC

SD Suopas Detchwilairuang

Added Alert

Estimated Time Spent

43 minutes

Case Contains

Data Sources

0

Alerts

2

Assets

4

Tasks and Automations

0

Search Results

0

Notes

1

Related Cases

0

Case Summary

Case created by Analyst to track the remediation activities.

Recent Activity

Suopas Detchwilairuang added alert on 2025-10-02 15:16:48 UTC

Matteo Spiga added alert on 2025-10-02 15:16:48 UTC

Matteo Spiga created case on 2025-10-02 15:16:19 UTC

61

Trellix

Wise

1 No alert left behind;
100% investigated

2 Automate SOC
investigation and
response workflows

3 Improve analyst
efficiency by 5x

4 Reduce MTTD and
MTTR by 50%

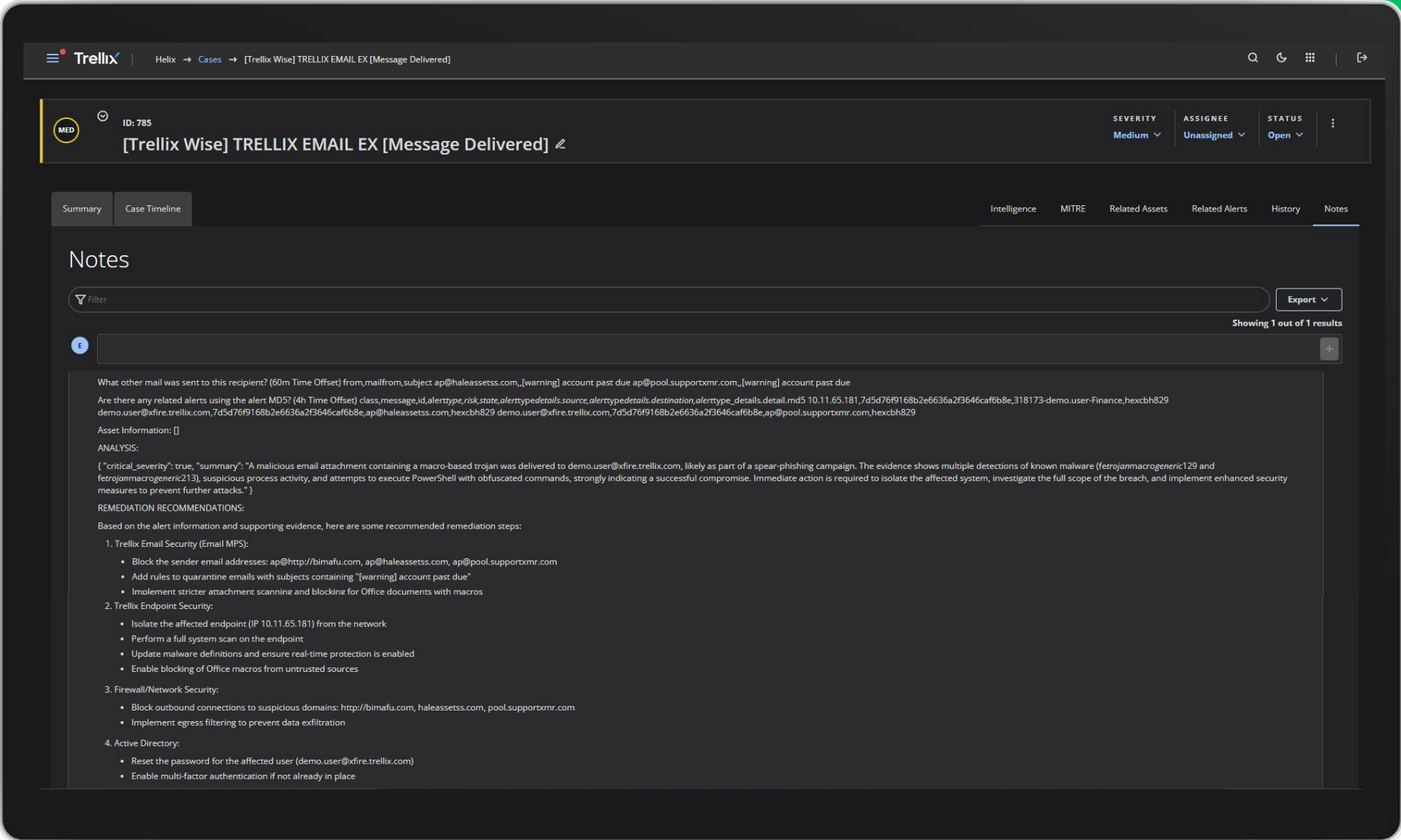
Trellix Wise for Helix

Running in Background

Upskill Teams

Auto-Prioritized Alerts

Suggested Remediations



Response



Hyperautomation

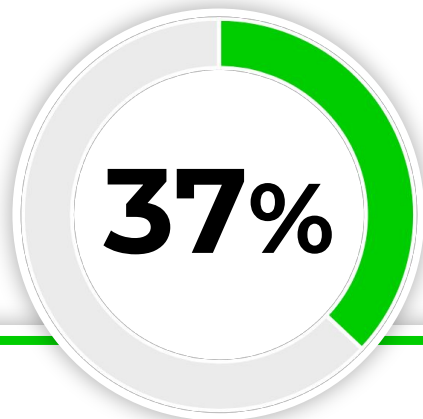


Why is Automation Essential to SecOps?



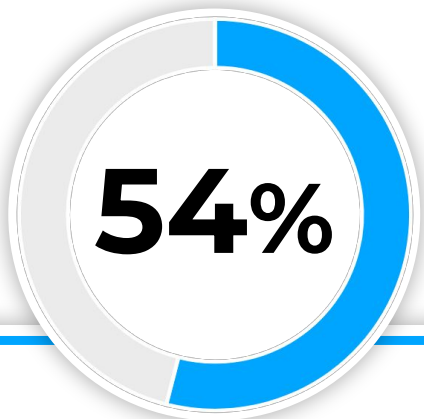
of CISOs agree
ransomware
incorporating AI is
a significant risk

EFFICACY



of CISOs would like
increased levels of
automation to help
perform their
responsibilities more
effectively

EFFICIENCY



Of workers say heavy
workloads are a top
stressor while **43%**
cite long hours

WORKLOADS

What is Hyperautomation?

“Hyperautomation is a business-driven, disciplined approach that organizations use to rapidly identify, vet and automate as many business and IT processes as possible.”

Security Hyperautomation involves the orchestrated use of multiple technologies, tools or platforms, including: artificial intelligence (AI), low-code/no-code tools, packaged software, and other types of decision, process and task automation tools.”

Gartner Research

SOAR vs. Hyperautomation

Why aren't traditional automation solutions enough?

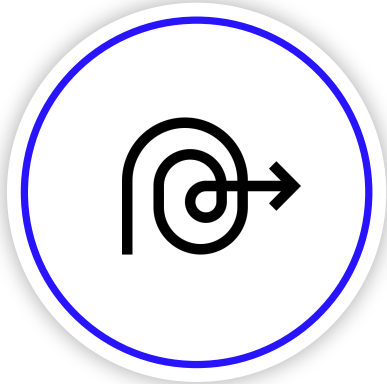
SOAR

- Coding Expertise Required
- Restricted automation capabilities
- Limited AI
- Challenging to integrate products
- High implementation and maintenance costs

Hyperautomation

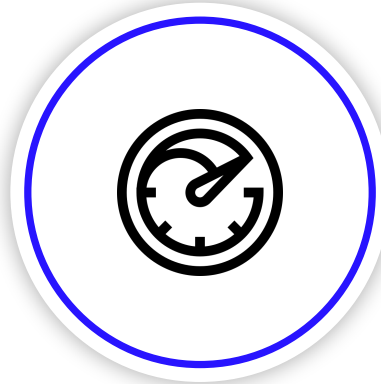
- Low-code, no-code solution
- Automation across tools, environments
- Deeper AI integration capabilities
- broader , simplified integrations
- Faster implementation, low maintenance

How Does Hyperautomation Help Response Times ?



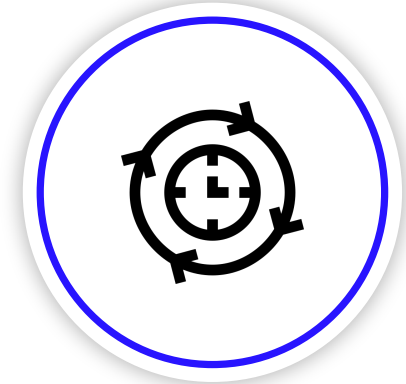
Reducing Complexity

Integrating data from tools to unite SecOps workflows



Enhancing speed and accuracy

Automated responses, analysis, intelligence enrichment



Improving Efficiency

Offloading repeat tasks, empowering more analysts to create automation

Rapid response, minimal manual intervention

How do you Make Automation Successful?



UNIFY

Pre-built, app
agnostic
integrations



SIMPLIFY

Standardized,
shareable
workflows



AMPLIFY

Low-code,
team-focused
automation

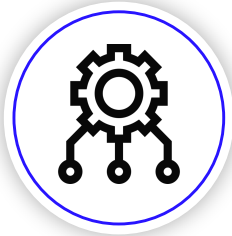


Low cost, low
risk architecture



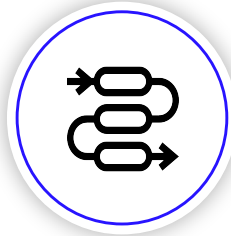
Speed visibility, drive efficiency & shift to “automate-first”

Speed Workflows and Amplify Outcomes with Trellix



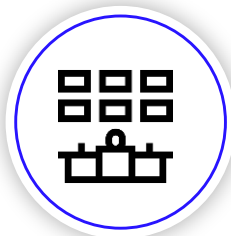
Trellix & 3rd Party Integrations

Pre-built or build your own



No-Code Workflows

Drag and drop, shareable



Cross Function Collaboration

Designed for Fusion teams



Data Privacy & Efficiency

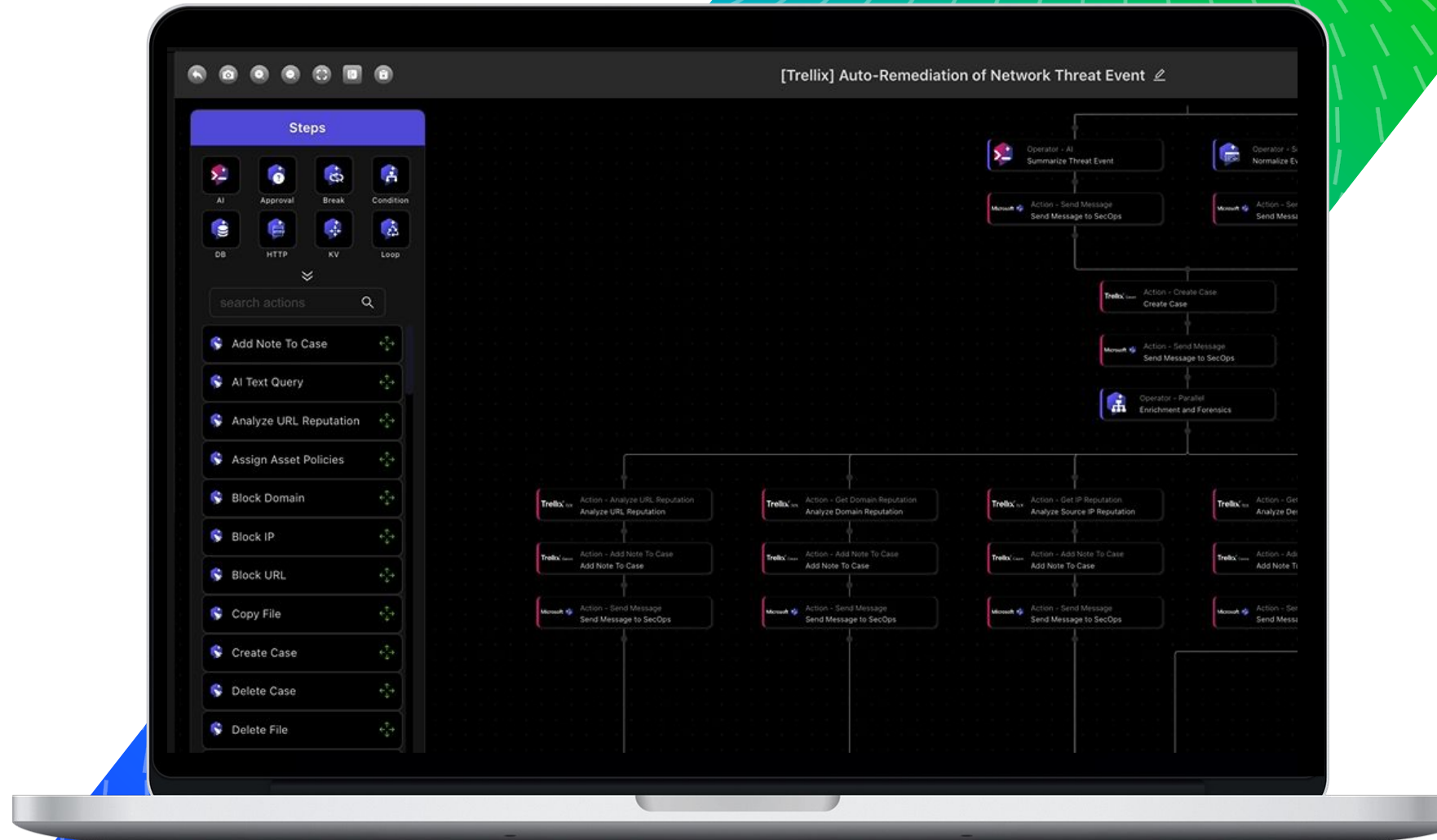
Lower Cost, Lower Risk

Trellix Hyperautomation

**Drag-and-drop
workflow builder**

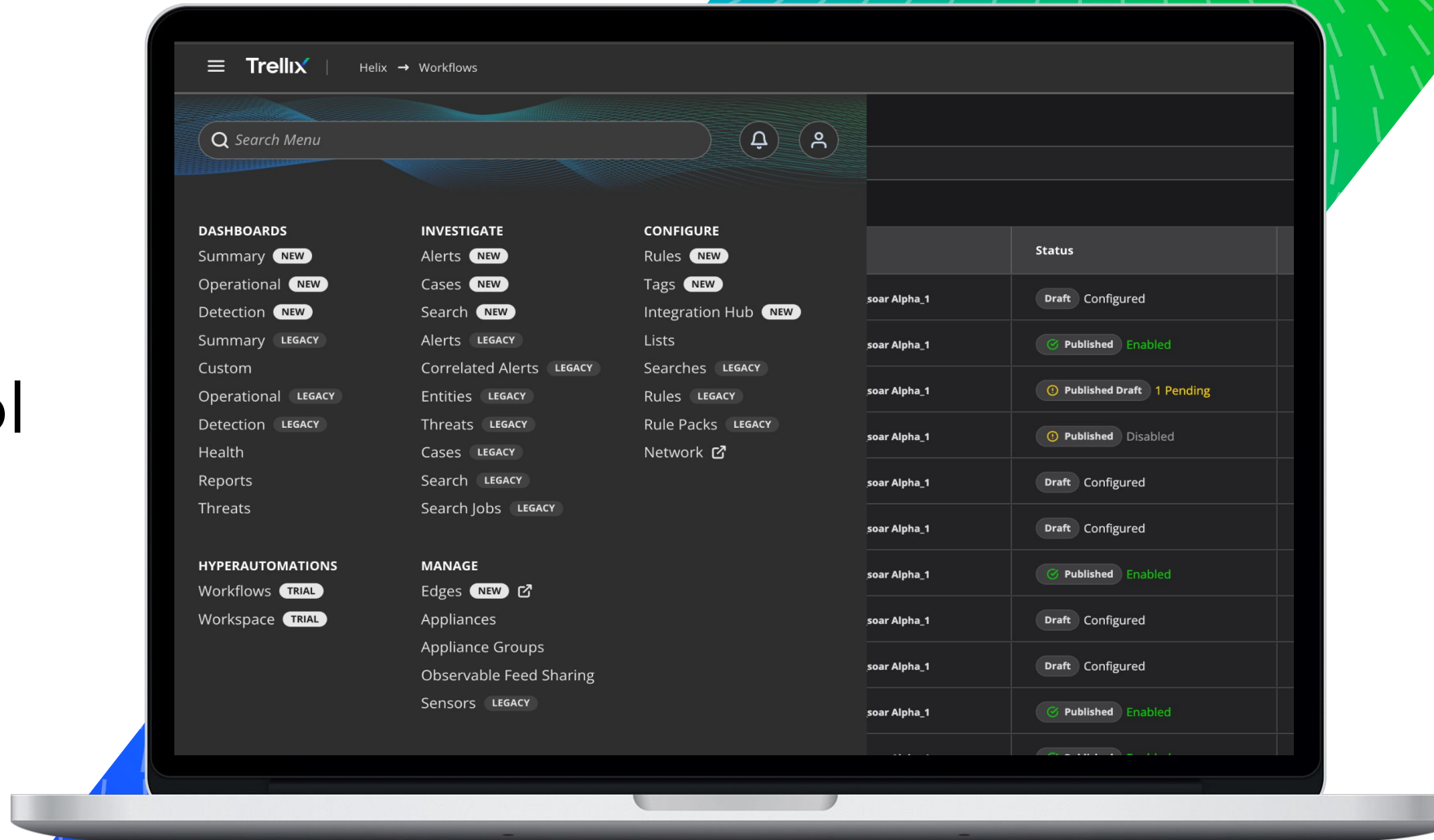
**Edges to take
action in multiple
environments**

**Integrate nearly
anything with
an API**

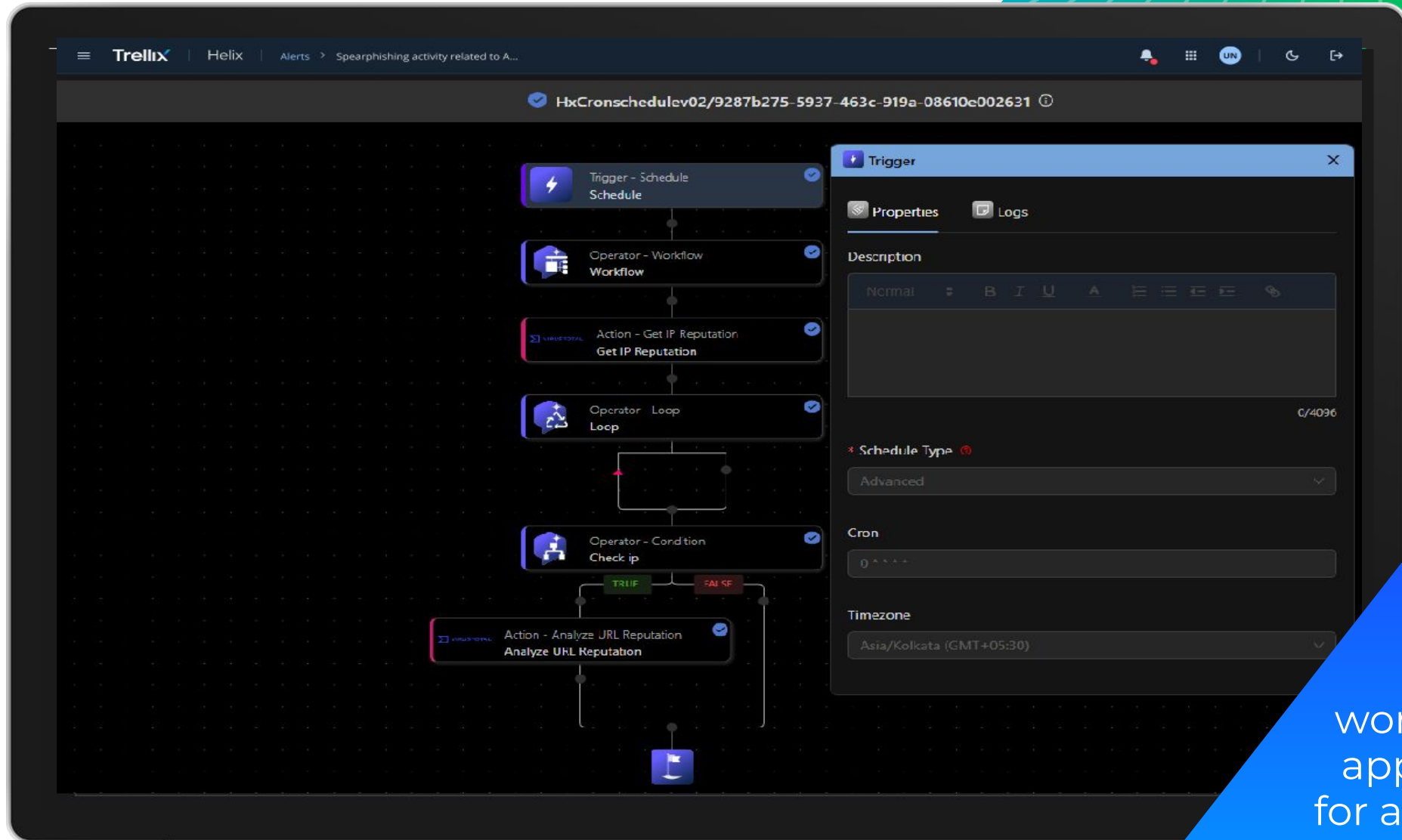


Integrated Directly into Helix

Our SecOps tool
for connecting
solutions,
detection,
response,
and hunting

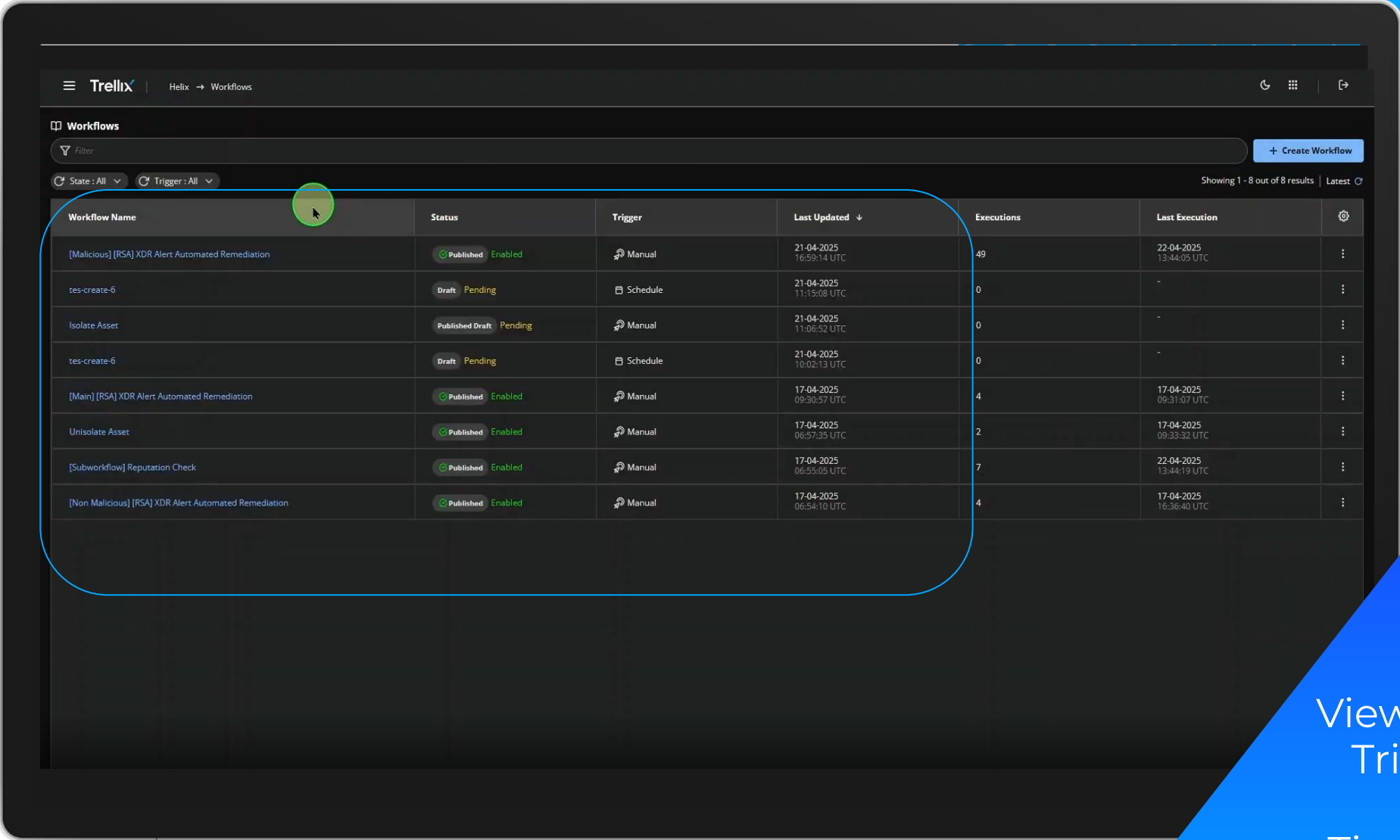


Makes Automated Responses Easy



Create workflows and apply triggers for actions using low-code editing

Easily View Workflow Status

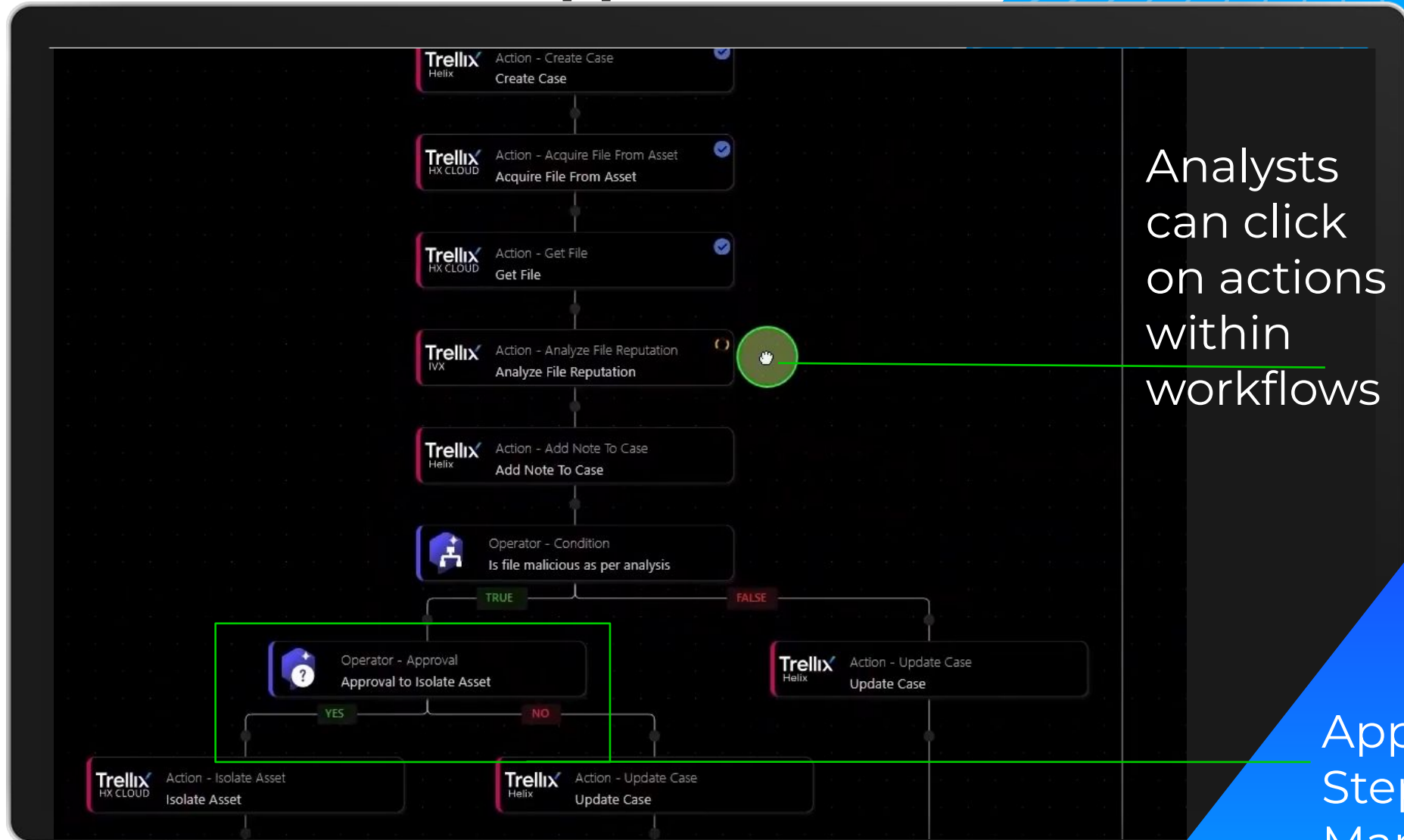


The screenshot displays the Trellix Helix Workflows management interface. At the top, the breadcrumb navigation shows 'Helix → Workflows'. Below this, there's a 'Filter' input field and a '+ Create Workflow' button. The main content area shows a table of workflows with columns for 'Workflow Name', 'Status', 'Trigger', 'Last Updated', 'Executions', and 'Last Execution'. A green circle highlights the 'Workflow Name' column header. The table lists eight workflows, including '[Malicious] [RSA] XDR Alert Automated Remediation', 'tes-create-6', 'Isolate Asset', '[Main] [RSA] XDR Alert Automated Remediation', 'Unisolate Asset', '[Subworkflow] Reputation Check', and '[Non Malicious] [RSA] XDR Alert Automated Remediation'. Each row shows the workflow's status (e.g., Published, Draft), trigger type (e.g., Manual, Schedule), last updated timestamp, number of executions, and last execution timestamp.

Workflow Name	Status	Trigger	Last Updated ↓	Executions	Last Execution
[Malicious] [RSA] XDR Alert Automated Remediation	Published Enabled	Manual	21-04-2025 16:59:14 UTC	49	22-04-2025 13:44:05 UTC
tes-create-6	Draft Pending	Schedule	21-04-2025 11:15:08 UTC	0	-
Isolate Asset	Published Draft Pending	Manual	21-04-2025 11:06:52 UTC	0	-
tes-create-6	Draft Pending	Schedule	21-04-2025 10:02:13 UTC	0	-
[Main] [RSA] XDR Alert Automated Remediation	Published Enabled	Manual	17-04-2025 09:30:57 UTC	4	17-04-2025 09:31:07 UTC
Unisolate Asset	Published Enabled	Manual	17-04-2025 06:57:35 UTC	2	17-04-2025 09:33:32 UTC
[Subworkflow] Reputation Check	Published Enabled	Manual	17-04-2025 06:55:05 UTC	7	22-04-2025 13:44:19 UTC
[Non Malicious] [RSA] XDR Alert Automated Remediation	Published Enabled	Manual	17-04-2025 06:54:10 UTC	4	17-04-2025 16:36:40 UTC

View the Status,
Trigger Type
and
Timestamps of
Workflows

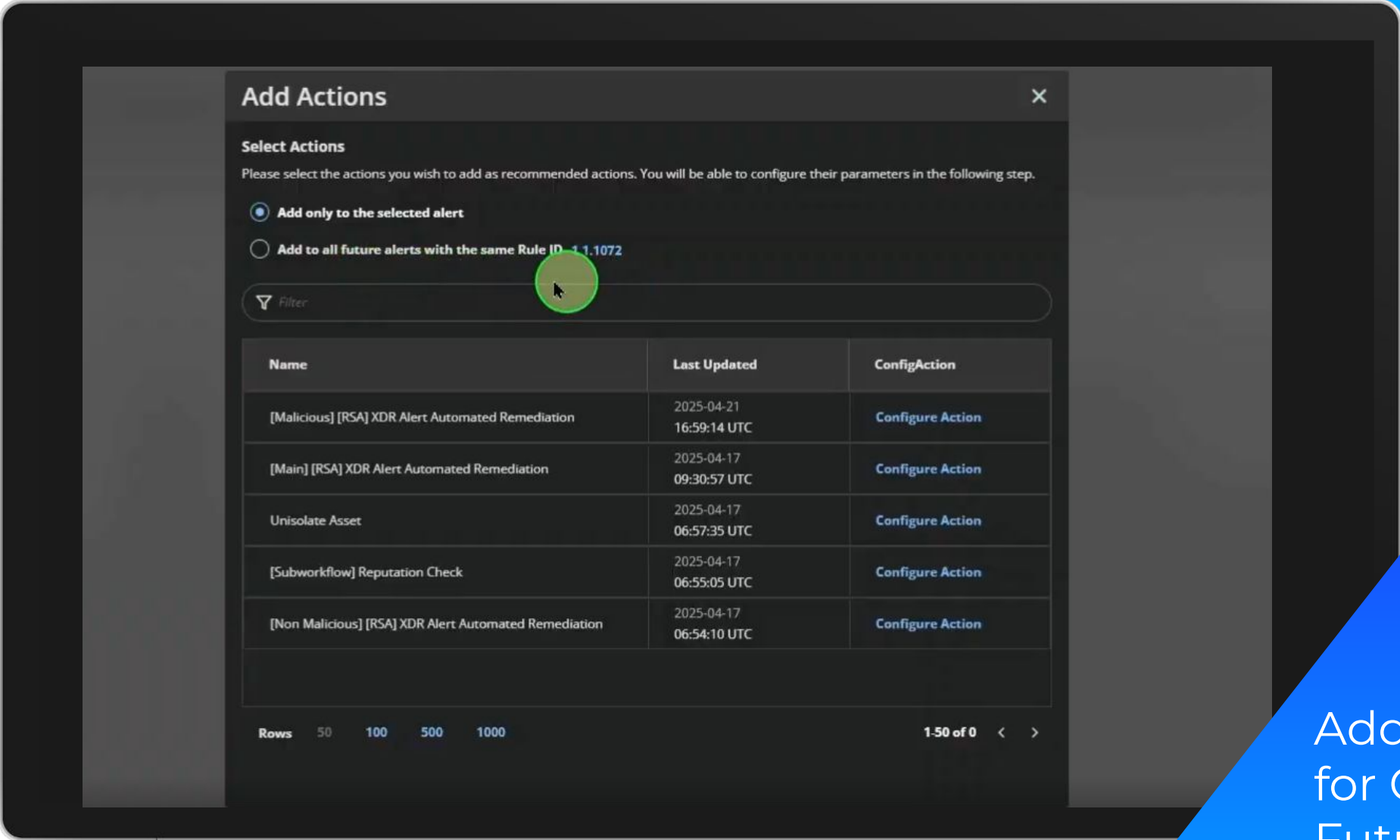
Workflow Actions and Approvals



Guided Responses

<

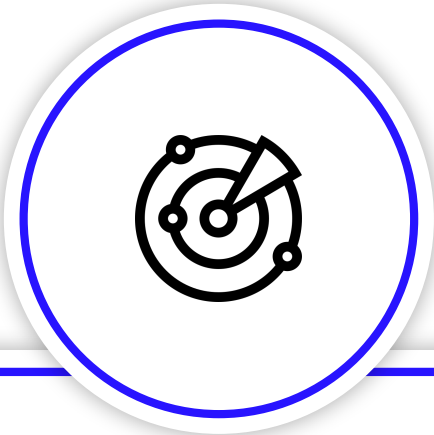
Manage, Add and Configure Actions



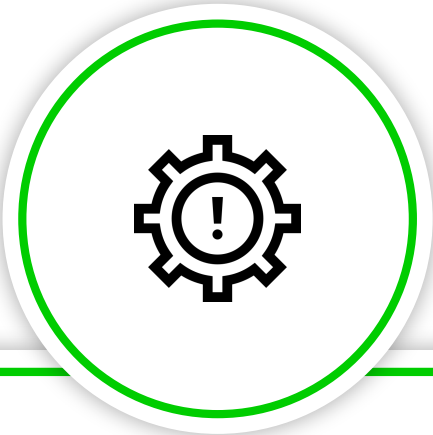
Add Actions
for Current or
Future Alerts

Use Cases

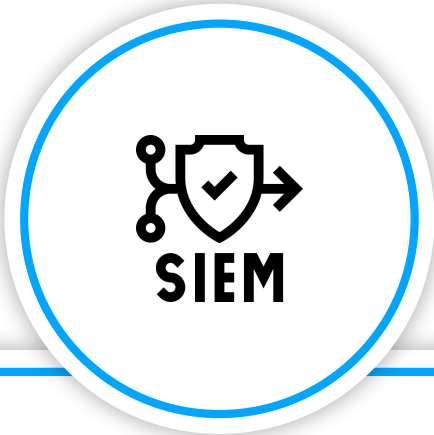
Common applications of Trellix Hyperautomation for SecOps



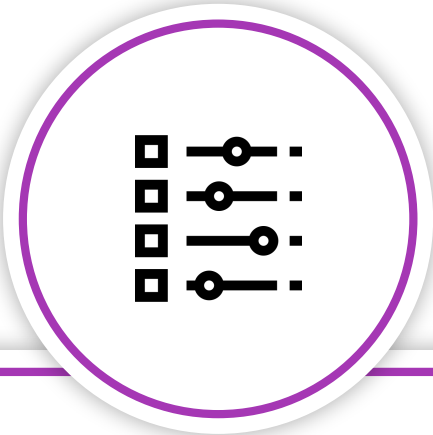
**Threat
Intelligence
Enrichment**



**Automated
Incident
Response &
Remediation**

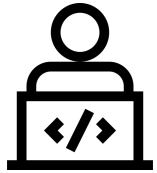


**SIEM &
Ticketing
Integration**

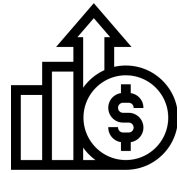


**Asset and
Configuration
Management
Integration**

Why Choose Trellix Hyper Automation?



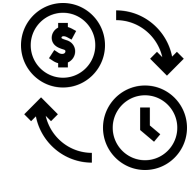
**Enable More
of Your team
to Create
Automation**



**Get More
From Your
Current
Investments**



**Avoid
Vendor
Lock-in**



**Enhance
Operational
Efficiency and
Reduce Costs**

Why Choose Trellix for your Hyperautomation Needs?



Lower Cost

Reduce cloud costs by lowering data transfer



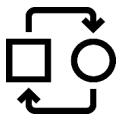
Shared Visibility

Integrate tools, unite team processes



Data Privacy

Retain complete datasets at the source and limit data duplication.



Realize a Cross-org Automation Strategy

Integrate and apply across more of your tools with application agnostic, 1-click swap, no-code workflows

Use Cases

Examples

Business Value

Customer Success Stories



Example Use Cases

Operationalize threat intelligence across the business

- Real-time global insights across a range of what used to be separate products
- Push/pull from native data sources with a much higher volume
- Make actionable intelligence reports

Reduce vendors, tools & operational overhead

- Pre-built integrations
- Single platform/vendor to replace multiple tools
- Built-in automation and orchestration

Automate workflows across the extended platform

- Signal other controls from inside Helix
- Threat correlation and prioritization
- Immediate mitigation across controls, guided workflows

Augment the SIEM with SOAR capabilities

- Pre-built or user created orchestration & automation
- Automated forensics & threat hunting
- Automated remediation actions

Trellix Helix - Business Value



Security Effectiveness

- Reduce risk by increasing visibility, seeing what point solutions miss
- Multi-vector, Multi-vendor threat detections



Security Effectiveness

- Recover valuable time by reducing manual pivots using a unified analyst experience that helps you spend 90% less time on non-response activities



Security Efficiency

- Reduce MTTD, MTTR by empowering analysts of any skill level with pre-built automation playbooks, AI-guided detection and threat hunting



Security Efficiency

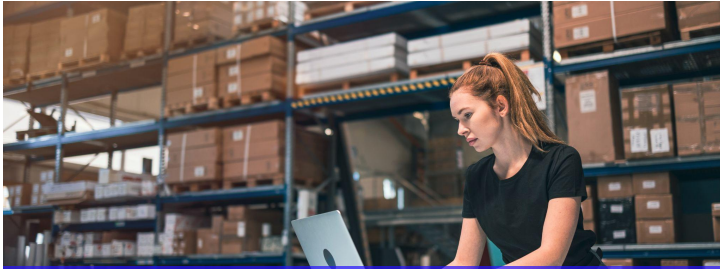
- Relieve alert fatigue with automatic false positive suppression and prioritized alerts
- Reduce vendor and tool footprint by leveraging one platform with 35+ capabilities



Reduced Expense

- Increase value from existing investments by unlocking data with 490+ out of the box integrations, prebuilt analytics that save months of detection engineering

Customer Success Stories



Global Luxury Retailer

Challenges:

- Protecting customer data and intellectual property.
- Unfilled security team positions, unable to empower current members effectively.
- Visibility beyond SIEM tools.

Results:

- Significant reduction of false positives.
- Simplified management and consolidated incident response.
- Improved incident response efficiency of SOC teams.



Law Firm

Challenges:

- Too many disparate tools to effectively detect and respond to threats.
- Compliance and reporting requirements.
- Small team with ad hoc infrastructure.

Results:

- Better visibility and simplified procedures by integrating tools and data.
- Prioritized alerts and responses.
- Reduced exposure to large fines from breaches where customer data is exposed.



Financial Institution

Challenges:

- Mature organization but weak detection using current tools translating to alert fatigue.
- Attempted to build a modern SOC themselves but found costs were too high trying to connect and integrate tools themselves.

Results:

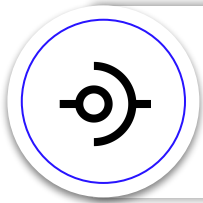
- Faster, lower cost integrations.
- Reduced MTTD and MTTR.
- An Integrated, single architecture that modernized their SOC and improved the efficiency of the SOC team..

Trellix

Trellix
differentiators

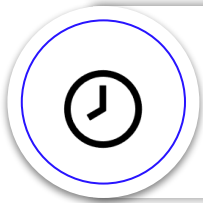


Trellix Helix Differentiators



Depth of integrations

500+ integrations across 230 vendors to onboard the data you already own.



Out-of-the-box multi-vector multi-source detections

Data is ingested in real time with over 2,000 rules and 50 analytics creating context without the need for months of detection engineering.



GenAI alert triage

Investigate 100% of alerts, prioritize threats and get updates as related events are ingested



Designed for unique environments

With more pre-built automation workflows than competing solutions and the ability to customize them using Hyperautomation no-code SOAR, Helix helps upskill less experienced analysts.

What makes Helix unique?



Trellix