

Trellix

XDR – the Trellix Advantage

Learn how Trellix is leapfrogging with its XDR Platform

June 3, 2024



Speaker Intro



Henrik Olsson

Senior Product Manager
Sweden



Josef Gillhuber

Senior Solutions Engineer
CISSP
Germany

Agenda

- Market Trends & Challenges
- The need for XDR
- This is Trellix XDR
- Trellix XDR Roadmap

Today's Challenges

72

Average number of security tools

62%

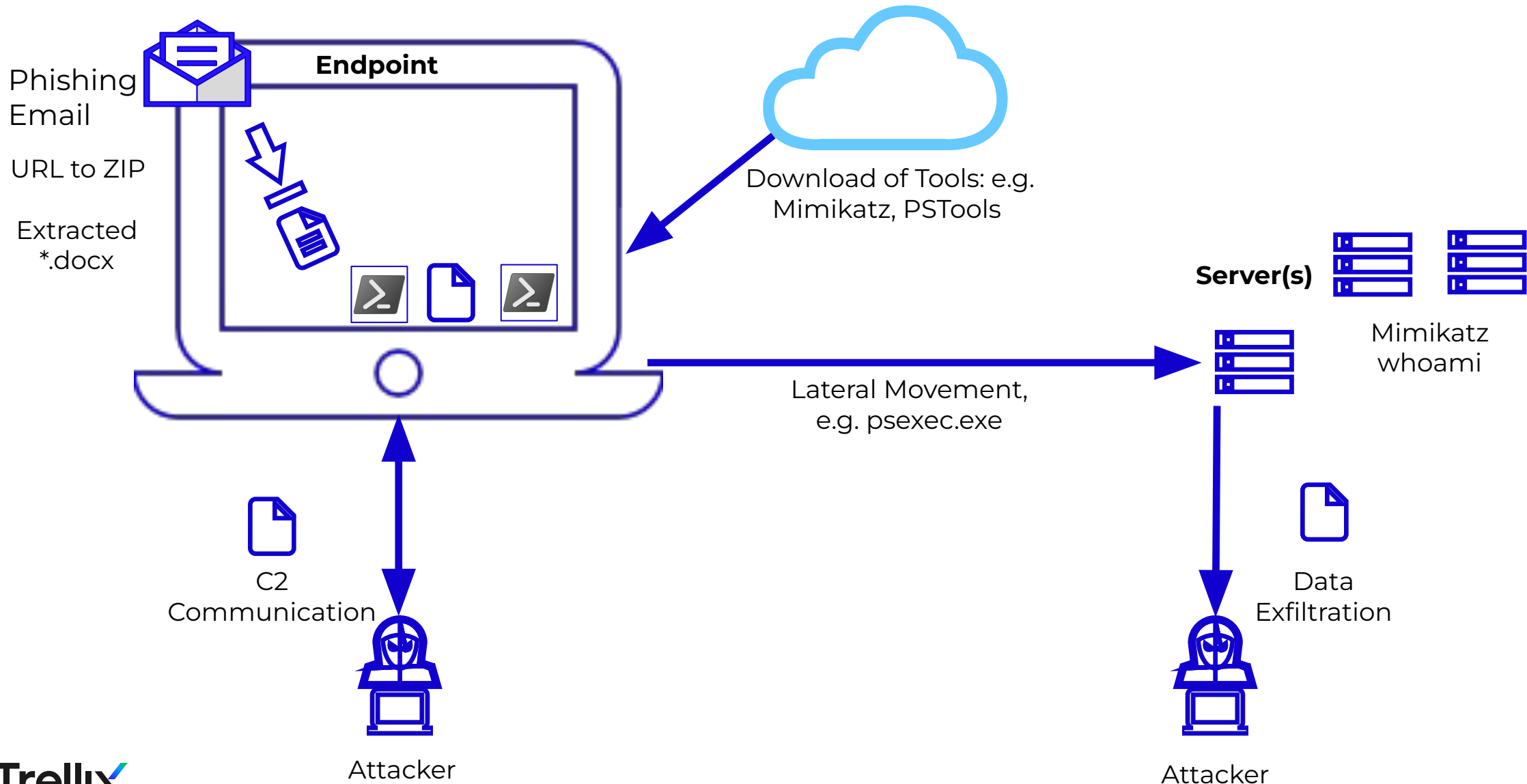
increase in attack surface over 2 years

74%

employees willing to bypass cybersecurity guidance

....and a Talent gap of 4 million people


Sample Attack



Today's SOC solutions are inadequate

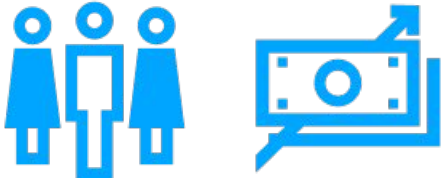
Today

Siloed tools that don't work together



Weeks

Limited org resources and expertise



Stretched, under-resourced

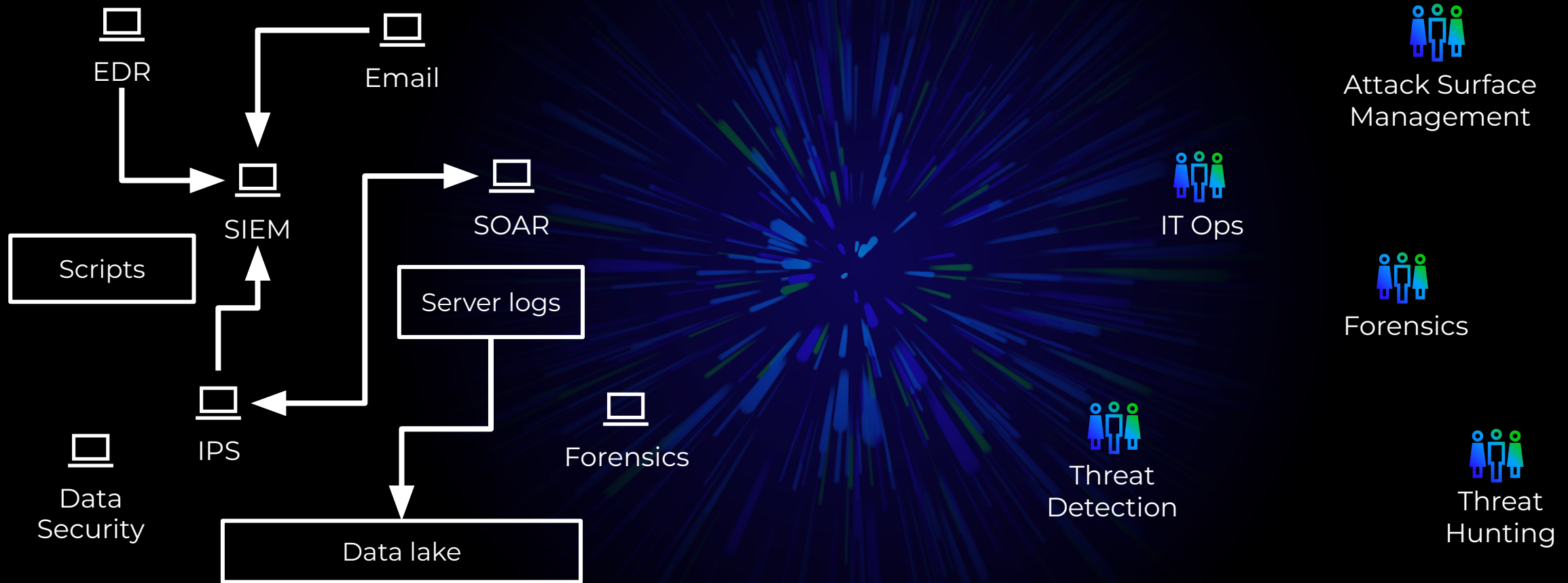
Too many alerts and missed threats



Inability to determine, prioritize top threats

**SOCs struggle to keep up with threat landscape of multi-vector attacks.
> Result: Organizational risk increases**

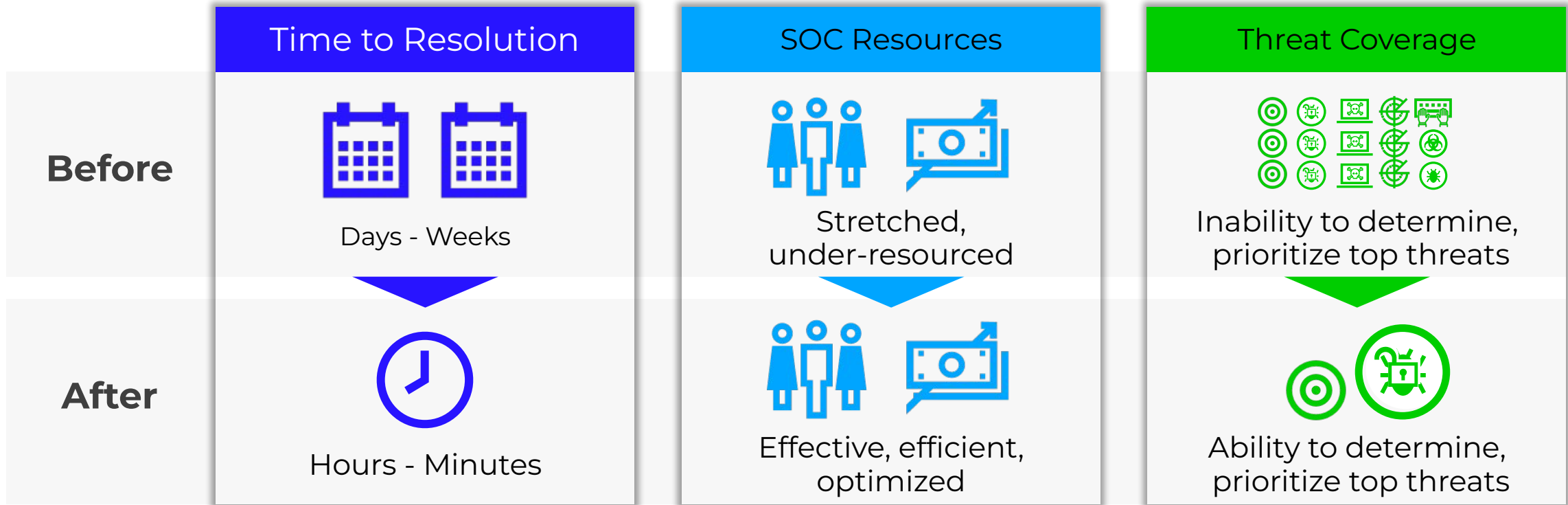
Challenges



Accelerated SOC Maturity



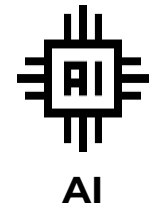
Trellix XDR Impact



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

Security Needs a Platform

Powered by:



AI



Automation



Analytics

Trellix

95%

CISOs agree their major cybersecurity incident would have been prevented with XDR

Why journey to XDR?

Mind of CISO: Behind the Breach Nov 2023 n= 500

Based on your understanding of XDR as a platform that connects your tools, to what extent do you agree or disagree

Trellix

This is Trellix XDR



What is XDR?



Extended goes across several security vectors including endpoints, network, data, cloud, email and other third-party products.

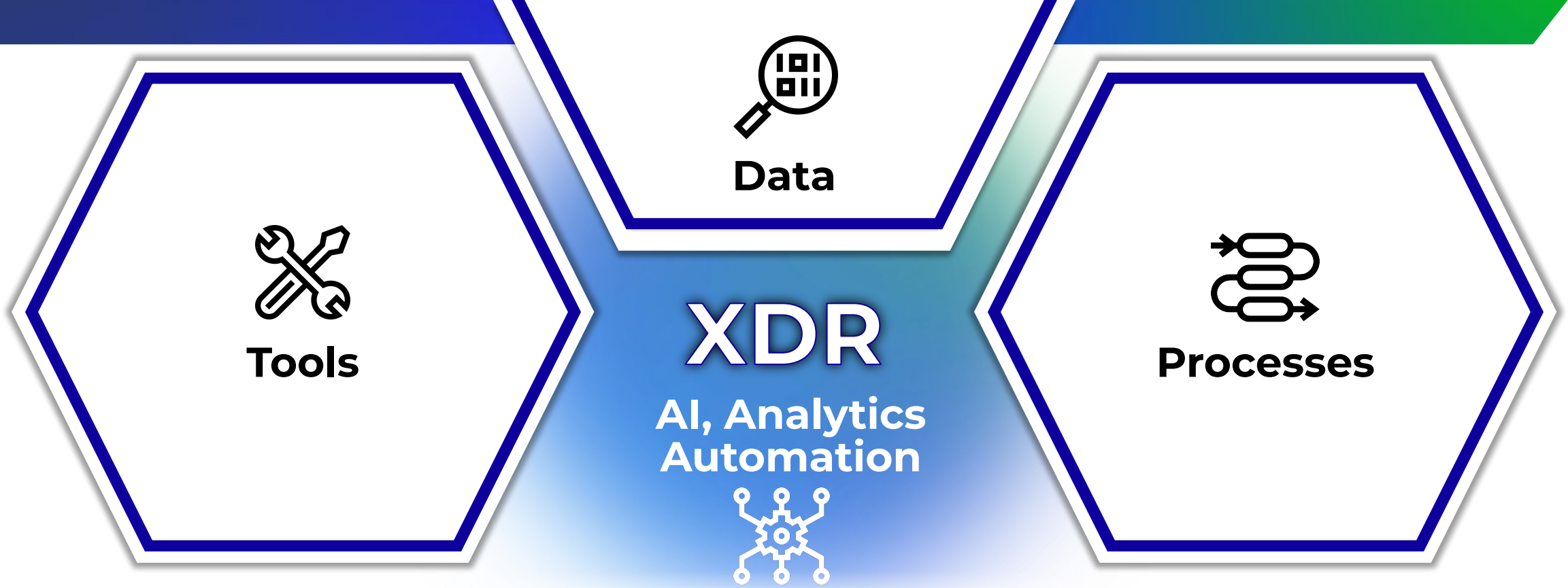


Detection comes from the ability to detect, correlate, and prioritize threats across multiple vectors the moment they arise.



Response enables your organization to be better prepared to respond effectively to attacks in real time.

XDR: the Convergence of Security



A platform to respond across your open, connected enterprise

Shut Down Threat Actors with Helix Connect

Rapid, Global Context

We turn "noise"
into **prioritized actions**

Correlated with
pre-built Analytics

Enriched with
Global Intelligence

Playbook Automation
Guided Response
Orchestration

MTTD, MTI,
MTTR in
minutes

Broad Integration

We meet you where
you are **today**...

Streamlined Workflows

We make your
team **proactive**

490+
third parties

...because minutes matter

How Helix Connect Works

1. Broad data Ingestion

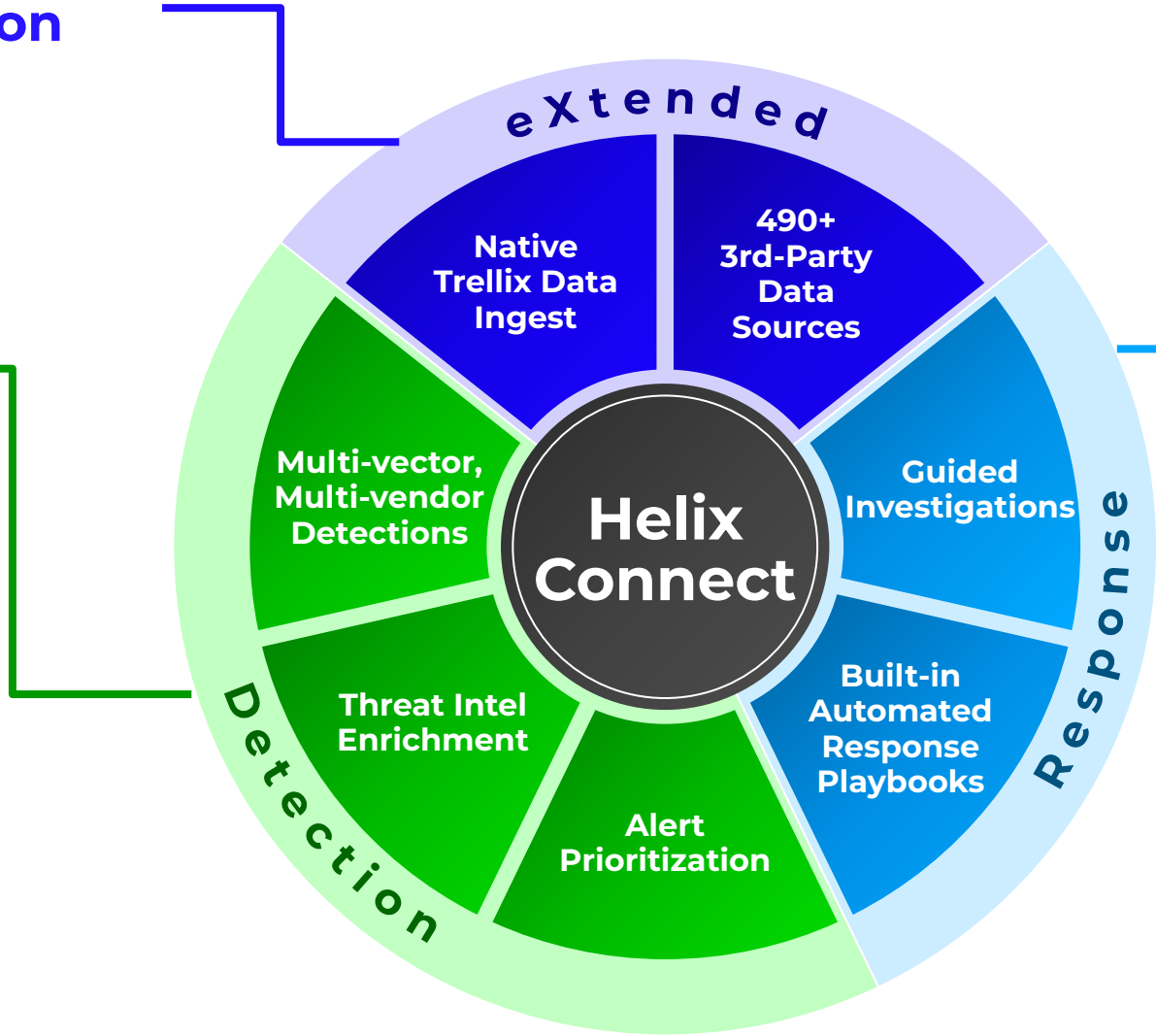
Open and native integrations

2. Detections:

- Analytics
- Automated threat elimination
- Noise suppression
- Enrichment
- Prioritization

3. Response

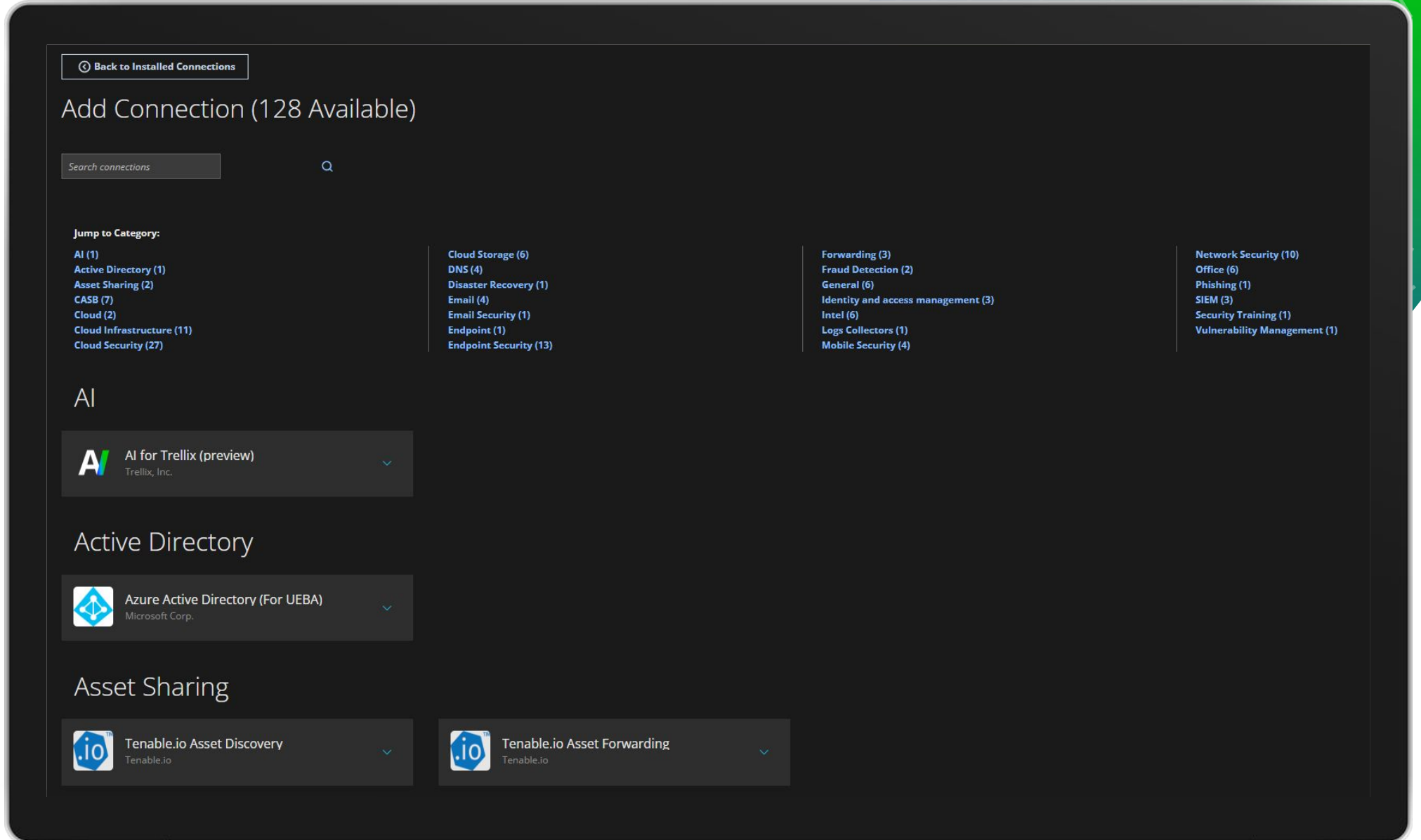
- On-prem / cloud orchestration and response
- AI-guidance
- Pre-built, customizable playbooks



Quickly Integrate Data

490+
3rd-party
sources

100+
different
SaaS
solutions
across
multiple
domains



Surface New Detections within Hours

2000+
rules,
integrated
intelligence
matching

50+
analytics

The screenshot displays the Trellix Helix Rules management interface. At the top, there's a navigation bar with 'Helix → Rules' and a search bar containing 'Start hunting for evil...'. Below the search bar, filters for 'PAST 24 HOURS' and 'ORGANIZATIONS: ALL' are visible. The main content area is titled 'Rules' and includes a brief description of rule functionality. Two charts are present: a circular gauge showing '67.8% COVERED' and a bar chart titled 'Rule Coverage Trend(Enabled Trellix Rules, Past 14 Days)' showing consistent coverage over time. A table titled 'Class/Field Recommendations' lists impacted rules with their respective counts. At the bottom, a table lists individual rules with columns for Risk, Name, Rule Pack, Distinguishers, Query, Tags, Status, Assertions, Dependencies, Alerting, Covered, Tuned, Security Orc..., and Created At.

Risk	Name	Rule Pack	Distinguishers	Query	Tags	Status	Assertions	Dependencies	Alerting	Covered	Tuned	Security Orc...	Created At
LOW	WINDOWS DEFENDER ... ID: 1.1.4231	Windows Defender	category,eventid	class=ms_windows_defender_...	windows_defender_microsof...	Enabled	0	No	off	No	No	0	2024-05-31 18:35 ...
HIGH	WINDOWS DEFENDER ... ID: 1.1.4230	Windows Defender	category,eventid	class=ms_windows_defender_...	windows_defender_microsof...	Enabled	0	No	on	No	No	0	2024-05-31 18:35 ...
MEDIUM	WINDOWS DEFENDER ... ID: 1.1.4229	Windows Defender	category,eventid	class=ms_windows_defender_...	windows_defender_microsof...	Enabled	0	No	on	No	No	0	2024-05-31 18:35 ...
LOW	WINDOWS DEFENDER ... ID: 1.1.4228	Windows Defender	category,eventid	class=ms_windows_defender_...	windows_defender_microsof...	Enabled	0	No	off	No	No	0	2024-05-31 18:35 ...
MEDIUM	LIGHTSPY MALWARE [...] ID: 1.1.4216	MacOS	hostname	((class:fireeye_hx_ioc assets.pr...	macos_methodology_malwa...	Enabled	0	No	on	No	No	0	2024-05-24 18:35 ...

Automatically Prioritize Threats

Address
the
most
critical
threats first

The screenshot displays the Trellix Helix Threats dashboard. At the top, it shows the Trellix logo and navigation options. A search bar is present with the text "Start hunting for evil...". Below the search bar, there are filters for "PAST 24 HOURS" and "ORGANIZATIONS: ALL". The main content area is titled "Welcome to your Dashboard, JGI" and provides a summary: "There are 13,543 threats. 3 of them must be reviewed as soon as possible and 78 recommended to be reviewed proactively." Below this, a table lists the "Top 6 Threats" with columns for "Threat Name, Type and Risk Score", "Status", "Assignee", "Affected Assets", and "Tags". The first threat (ID: 1547) is a "CORRELATIONS" type, detected on 2024-05-31T14:00:10.259829Z, with a status of "Open" and "Unassigned". The second threat (ID: 1489) is also a "CORRELATIONS" type, detected on 2024-05-28T16:30:00.000000Z, with a status of "Open" and "Unassigned". The third threat (ID: 1209) is a "CORRELATIONS" type, detected on 2024-06-03T12:40:00.000000Z, with a status of "Open" and "Unassigned". The fourth threat (ID: 878) is a "CORRELATIONS" type, detected on 2024-05-28T16:30:00.000000Z, with a status of "Open" and "Unassigned". The fifth threat (ID: 708) is a "CORRELATIONS" type, detected on 2024-05-30T04:00:00.000000Z, with a status of "Open" and "Unassigned". The sixth threat (ID: 671) is a "CORRELATIONS" type, detected on 2024-05-31T04:00:00.000000Z, with a status of "Open" and "Unassigned". To the right of the table, there is a "Total Risk Score" graph showing a peak in risk score around 20,000 on 05-30. Below the graph, there is an "Assigned Threats" section showing a bar chart for "Assigned Threats" with two bars for "RonKe..." and "David...".

Map the Complete Threat Journey

Mapped to MITRE ATT&CK tactics

The screenshot shows the Trellix Helix interface for threat analysis. The main content area displays a correlation graph for threat ID 106996. The graph shows a flow from security tools to multiple sources, which triggered multiple alerts, involving multiple assets. A sidebar on the right lists 11 out of 14 MITRE ATT&CK tactics:

- TA0011 - TACTIC: Command and Control
 - T1090.002 - TECHNIQUE: External Proxy
 - T1105 - TECHNIQUE: Ingress Tool Transfer
 - T1000 - TECHNIQUE: Proxy
 - T1071.001 - TECHNIQUE: Web Protocols
- TA0006 - TACTIC: Credential Access
 - T1111 - TECHNIQUE: Two-Factor Authentication Interception
- TA0005 - TACTIC: Defense Evasion
 - T1548 - TECHNIQUE: Abuse Elevation Control Mechanism
 - T1548.002 - TECHNIQUE: Bypass User Account Control
 - T1140 - TECHNIQUE: Deobfuscate/Decode Files or Information
 - T1553.004 - TECHNIQUE: [Unreadable]

Automatically take Action

Detections trigger responses in your tools

The screenshot displays a security dashboard interface. At the top, a critical alert is shown with a folder icon and a '325' badge. The alert text reads: 'Defense Evasion(+4) tactic(s) using Bypass User Account Control(+10) technique(s) with fe_trojan_win64_generic_24(+5) malware(s) detected, but not blocked'. Below the alert, it states: 'Defense Evasion(+4) tactic(s) using Bypass User Account Control(+10) technique(s) with fe_trojan_win64_generic_24(+5) malware(s) detected, but not blocked on elazar.broad asset(s) by Network Security and Email Security. Last Seen: 2023-09-08 23:34:52 UTC (9 months ago)'. The user 'Elazar' is logged in.

The dashboard includes a navigation bar with 'Overview', 'Intel', 'Events 32', 'Related Alerts 8', 'Related Assets 1', and 'Response 7'. A 'Refresh' button is visible. The main content area is divided into two columns. The left column shows a list of completed actions:

- Trellix ePO - SaaS: Apply Tags (Completed, 2 months ago)
- Trellix Intelligent Virtual Execution (IVX): Hashes Enrichment (Completed, 8 months ago)
- Trellix ePO - SaaS: Apply Tags (Completed, 8 months ago)
- Microsoft Azure: Disable Users (Completed, 9 months ago)
- Trellix ePO - SaaS: Apply Tags (Completed, 9 months ago)
- VirusTotal - Indicator Enrichment (Completed, 9 months ago)

The right column shows details for the 'Microsoft Azure: Disable Users' response:

Status	Playbook Type	Timestamp
Completed	REMEDIAATION	2023-09-11 15:05:47 UTC 9 months ago

Description
Extracts users from threats where Azure is the asset source and the risk score >=80. Disables such users in Azure AD.

Summary
Disabled 1 user(s) successfully.


Related Key information

Threat ID	653690
Mapping ID	26

Leverage AI-guided Investigations

Enable
and
upskill
more of
your
team

i The results of investigation tips may be restricted due to your assigned role or an applied data policy. Please

What other Okta logs are there for this user? (4h Time Offset) Last run a day ago 

username	msg	result
demo.user	reset all factor for user	success

What other Okta logs are there for this source? (4h Time Offset) Search not yet run


What failed Okta logs are there for this source? (4h Time Offset) Search not yet run

What successful Okta logs are there for this source? (4h Time Offset) Search not yet run

Leverage AI-guided Investigations

Investigative Tips provide a series of "next steps" for investigating an alert. For Trellix provided rules, these searches are generated by incident responders and intelligence analysts based on their experience and are not meant to be all-inclusive, but they are designed to provide a place to start.

i The results of investigation tips may be restricted due to your assigned role or an applied data policy. Please contact your administrator for more information.

Were there any other rules that fired for this source IP? (60m Time Offset) Last run 12 hours ago 

detect_rulenames	Count
trellix mvision [<%= category %>]	336
trellix network nx [smartvision-event]	78
fireeye hx ioc match	48
trellix endpoint hx [malware detected: <%= virus %>]	48
trellix endpoint hx [<%= iocnames %>]	36
malware methodology [certutil user-agent]	18
trellix endpoint hx [ioc alert - <%= iocnames %>]	12
trellix intel hit [non-dns fqdn - non-attributed malicious (tips)]	6
trellix intel hit [non-dns fqdn]	6
trellix network nx [infection-match]	6

What Trellix HX - IOC Registry Key Events are available for this process? (1h Time Offset) Search not yet run

What Trellix HX - IOC DNS Lookup Events are available for this process? (1h Time Offset) Search not yet run

What Trellix HX - IOC URL Monitor Events are available for this process? (1h Time Offset) Search not yet run

What Trellix HX - IOC Image Load Events are available for this process? (1h Time Offset) Search not yet run

Enable
and
upskill
more of
your
team

Trellix

XDR Roadmap

New and upcoming features & timelines



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



XDR Journey and Beyond

Fully Capable XDR 2024

- Multi data source integration
- Cross source correlation (multi-vendor, multi-vector)
- Integrated playbooks and response actions
- Trellix threat intel

Simplified XDR

Beta: Q1'24 GA: 2H'24

Full SOAR experience

- Create, add, run and edit response actions/playbooks

Enhance SecOps UX

- New Alerting, Search, Rule Mgt, Case Mgt, Tasks & Automation Apps

Broaden Integrations

- Broadened data Integrations and Response actions
- Easily integrate Trellix Products

New XDR Cross Vector Detections

- New detection engine (ACE)

Beyond XDR

2025 +

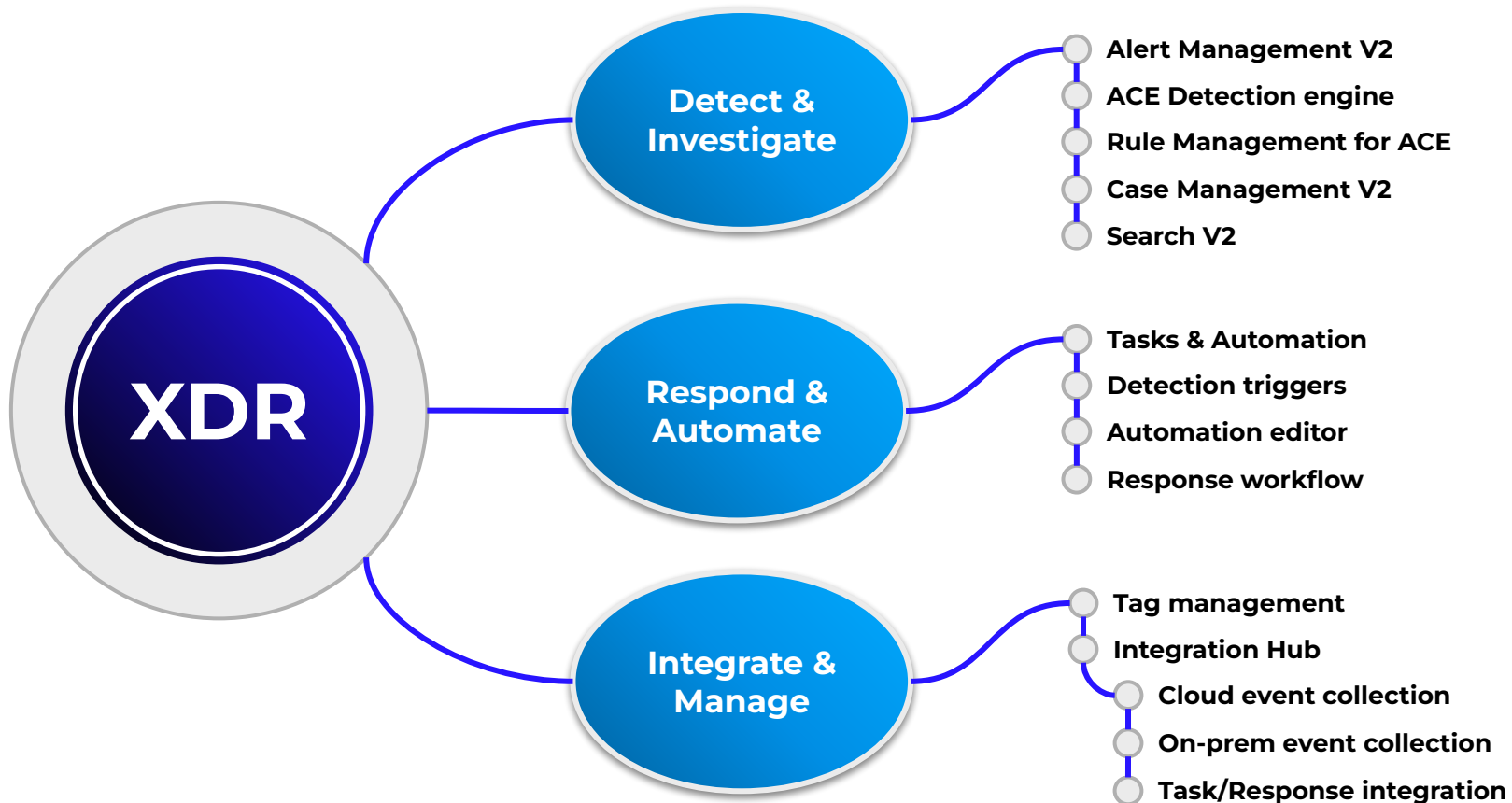
Enable Hybrid Architecture

- Hybrid On-Prem / Cloud solution that enables enterprise customer environments (data ingest / orchestration).
- Integrated single on-premise component that's cloud managed

Unlock Data Ownership

- Pluggable storage architecture and Bring Your Own Storage (BYOS)
- Augment existing Event Lakes (Splunk, Azure Sentinel, etc)

Major areas of improvement



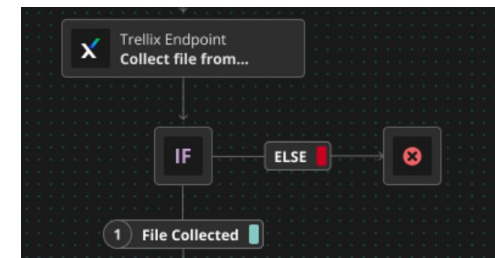
Alerts

Triage XDR alerts by viewing a summary of what happened, investigating the timeline of events, a

Filter

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

Severity	Alert Created	Alert Name
100 CRIT	06/12/2023 05:53:22 AM P1	Spearfishing Activity Attributed To Campaign APT 28 ID: #0271 Affected Assets: 43
99 CRIT	06/24/2023	Unauthorized Access Attempt



Available Integrations

Extend the capabilities of your SecOps environment, including monitoring, analy

Filter

Features: All Category: All

Akamai SIEM Monitor for suspicious activity in your account. SIEM	Atlassian JIRA Monitor for suspicious activity in your account. Ticketing
--	--

Detect & Investigate

The screenshot shows the Trellix XConsole Alerts page. At the top, there's a filter bar with 'Filter', 'Export', and 'Actions' buttons. Below that, there are dropdowns for 'Time Range: Last 7 Days', 'Assignee: Me, Unassigned', and 'Status: New'. The main table has columns for Severity, Alert Created, Alert Name, Assigned To, Status, Generated By, Data Sources, Intel, and Tags. Three alerts are visible, with their severity levels circled in red: 100 CRIT, 92 CRIT, and 96 CRIT.

Severity	Alert Created	Alert Name	Assigned To	Status	Generated By	Data Sources	Intel	Tags
100 CRIT	06/12/2023 09:39:22 AM PT	Spearphishing Activity Attributed To Campaign APT 28 ID: 40271 Affected Assets: 43	Unassigned	New	Trellix	✉ 🖥	🔍	🏷️ APT28
92 CRIT	06/24/2023 11:49:32 PM PT	Unauthorized Access Attempt ID: 61953 Affected Assets: 18	EM Cassidy Mar...	New	Trellix	✉ 🖥	🔍	
96 CRIT	06/19/2023 06:55:28 PM PT	Malware Infiltration Detected ID: 49018 Affected Assets: 20	FO Felicity O Co...	New	Trellix	✉ 🖥	🔍	

The screenshot shows the details for a 'CRITICAL' alert with a score of 98. The title is 'Spearphishing activity related to APT 28 campaign'. Below the title, there are tabs for 'Summary', 'Alert Timeline', and 'Respond'. The 'Summary' tab is active, showing 'How was the alert triggered?' (9 alerts triggered in these sources: EMAIL, ENDPOINT, NETWORK), 'Which assets are affected?' (43 affected assets: USERS, ENDPOINTS, EMAILS), and 'What actions should I take?' (Recommended actions: Quarantine the Device, Quarantine the Malicious File).

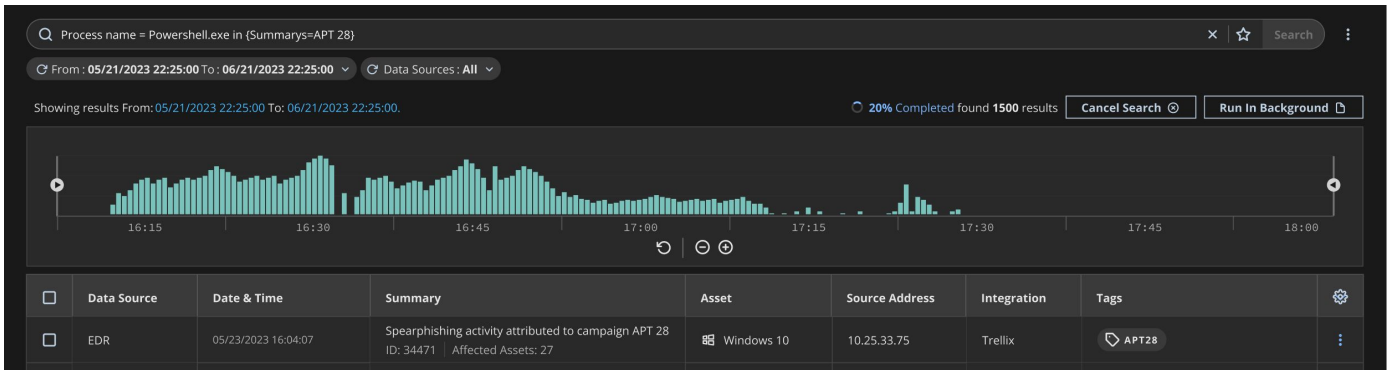
The screenshot shows the 'Alert Timeline' for the alert. It features a bar chart at the top showing activity over time from 15:30 to 19:00. Below the chart, there are filters and a table of events. Two events are visible: 'Spearphishing email received on a VIP account' (Risk Score: 24, LOW) and 'Endpoint: File was executed'. The timeline shows the relationship between these events.

- Manage incoming alerts
- Assign, acknowledge
- Sort, order, filter

- Quickly see
 - Assets involved
 - Why it's triggered
 - What to do next

- Scan through alert timeline
- See the attack lifecycle

Detect & Investigate



Conditions

```
1 id: 47-4000161
2 name: Attack - Possible DDoS Against Single Host - TCP - Flow
3 groupby: DEST_IP
4 require: 1
5 within: 10s
6 items:
7 - type: deviation
8   item:
9   - type: event
10  match: >
11    PROTOCOL == 6 66 CONTEXT == 2 66
12    DEST_IP != [192.0.2.0/24,198.51.100.0/24,203.0.113.0/2] 66
13    DEST_IP == [$var8,$var181,$var5,$var22,$var19]
14 field: SRC_IP
15 aggregate: cardinality
16 condition: stddev > 5
17 bucketSize: 60m
18 bucketCount: 60
```

Test IPs (27 IPs) maps to SRC_IP

AND UXers (12 Users) maps to USERNAME

Mission Critical (13 IPs) maps to Select Field

ID: 34471

Employee reporting possible malware

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

SEVERITY: Medium | ASSIGNEE: Kyle | STATUS: Open

MITRE ATT&CK

Summary | Case Timeline | Respond

Intel | Sandbox | MITRE | Related Activity | History | Notes

Key Milestones

Case Created: 05/18/2023 03:52:08 PM

Kyle Steffan

Case Contains

Data Sources: 4

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

- Search events, logs and all other collected data to complete investigation
- Build custom detection rules
- Organise alerts, events, searches, tasks into cases

Integrate & Manage

Available Integrations

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

Filter

Features: All Category: All Showing 185 of 372 integrations

- Akamai SIEM: Monitor for suspicious activity in your account. Category: SIEM.
- Atlassian JIRA: Monitor for suspicious activity in your account. Category: Ticketing.
- AWS CloudTrail: Continuous security monitoring for AWS. Category: Cloud Security.
- AWS CloudWatch: Continuous security monitoring for AWS. Category: Cloud Security.
- AWS GuardDuty: Continuous security monitoring for AWS. Category: Cloud Security.
- AWS DNS: Continuous security monitoring for AWS. Category: Cloud Security.
- Box Events: Inspect network traffic for signs of suspicious behavior. Category: Data Management.
- Cloudflare Logs: Inspect network traffic for signs of suspicious behavior. Category: Security.
- Duo Auth
- Google GSuite Audit
- Google GSuite
- Google Cloud

- Easily integrate with native and 3rd party products
- Ingest (event collection)
- Tasking response integrations

Your Integrations

Configure your 3rd party and custom integrations to ingest data and configure response actions.

Filter MITRE Coverage + Add New Integration

Features: All Status: All Category: All Showing 11 of 11 integrations

Integration	Features	Usage	Unique Configuration	Category	Tags
aws AWS S3 Germany	Ingest: Enabled Tasking: 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: Enabled Tasking: Enabled	11.2 TB	Bucket ID: trx-de-42wxdf7u88	Category	Slack

- Shows integrations already installed
- Change settings
- Monitor

Respond & Automate

The screenshot shows the 'Task and Automation Library' in the Trellix XCONSOLE. It features a search bar, a 'Filter' dropdown, and a 'Sort By: Date Created' menu. A table lists tasks with columns for Name, In Automations, Categories, and Tags. Two tasks are visible: 'Palo Alto: Add To Blocklist' and 'Palo Alto: Add Rule'. A detailed view for 'Quarantine Device' is shown on the right, with a description: 'Collect all the files and if any malicious file found, quarantine the device.' Buttons for 'Task And Automation Monitor' and 'Create Automation' are at the top right.

- Tasks from integrations shows up here
- Can be executed ad-hoc
- Can be part of automations

The screenshot shows the 'Create Custom Task' wizard. It has a progress bar on the left with three steps: 'Step 1: XDR Task - Rest Integration chosen.', 'Step 2: Basic Auth chosen.', and 'Step 3: Add Settings'. The main area is titled 'Add Settings' and contains an 'API Endpoint' section with 'HTTP Method' (Get) and 'URL' (https://dummy.restapiexample.com/api/v1/employees). Below is a 'Parameters' section with a table for defining task inputs.

Label	Type	Name	
Company	Static	Enter value	✕
User	Dynamic	User	✕
		Username you want to target	
Name	Dynamic	Remediation	✕
		Task input name	Description
			This is a sample long text for description of the task

- Non-supported integrations
- DIY tasks

Respond & Automate

The screenshot shows the Trellix XCONSOLE AUTOMATION interface. The main workspace displays a workflow diagram for "Manual analysis of a file on an endpoint". The workflow starts with a "Trigger Rules" step, followed by a "Trellix Endpoint Collect file from..." step. An "IF" step follows, with an "ELSE" branch leading to a red error icon. The main path continues to a "File Collected" step, then an "XDR Task Submit file to DaaS" step, and finally an "XDR Task Get analysis result for..." step. On the right, a "Version History" panel shows a list of versions (v.4 to v.7) with user names (Hans Zimmer) and timestamps. A "Save" button and other controls are visible at the top.

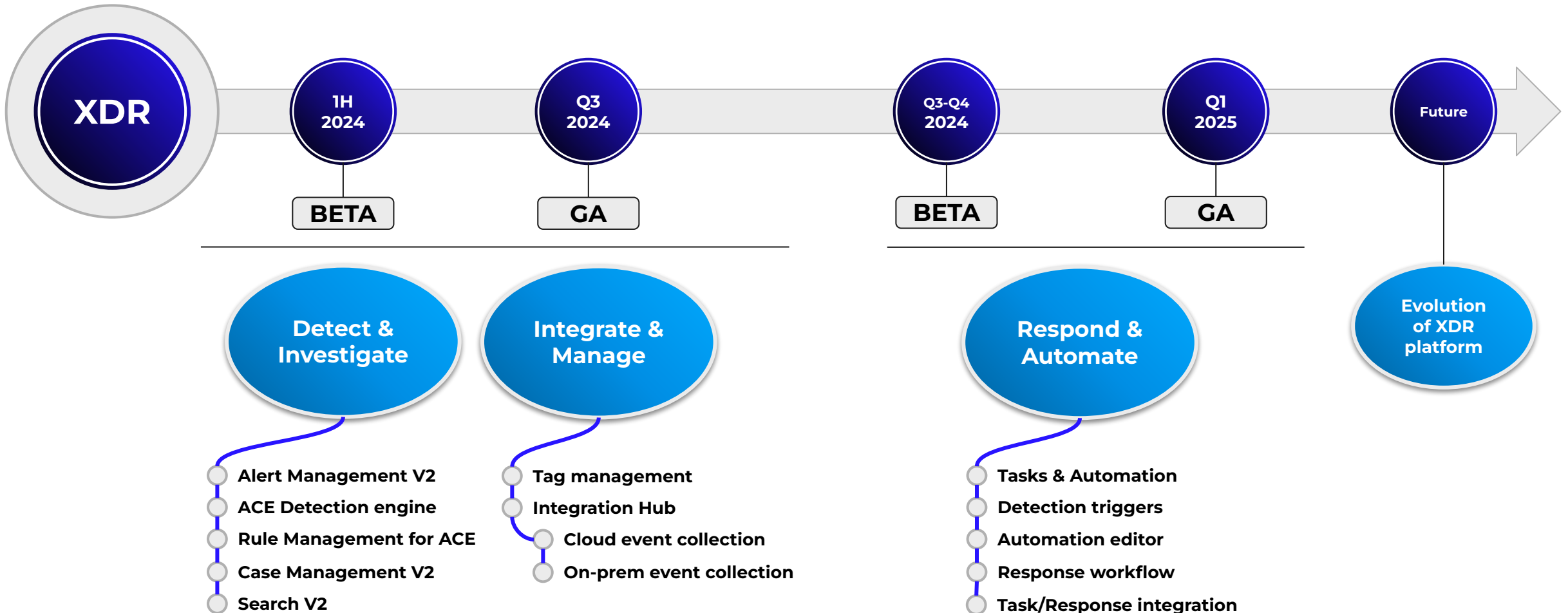
- Build custom automations/playbooks
- Can be run ad-hoc or automatically via detection events
- Easy to use UI

The screenshot shows the Trellix XCONSOLE interface displaying a critical alert. The alert is titled "Spearphishing activity attributed to campaign APT28" and is marked as "CRITICAL". The alert description states: "Spearphishing activity related to APT28 involving C2 and Credential harvesting with 4 assets affected... This text can be a maximum of 2 lines". The alert is associated with "Campaign APT28" and has a "MITRE ATT&CK" score of 98/100. The interface shows tabs for "Summary", "Alert Timeline", and "Respond". Below the alert, there are sections for "Recommended Actions", "Actions Monitor", "Task & Automation Library", and "Preventative Measures". A "Filter" input and a "Run Actions" button are visible. A table shows 25 out of 3000 results for recommended actions.

Automation Name	Artifacts	Tags	Integration	Category
<input type="checkbox"/> Quarantine Device	HZ HZ HZ HZ +99	Tag Tag	Trellix Email	Email Security
<input type="checkbox"/> Quarantine Malicious File	notepad.exe	Tag Tag	Trellix Email	Email Security
<input type="checkbox"/> Block Suspicious Domain	000.00.00.00	Tag Tag	Trellix Email	Email Security

- Recommendations for alerts, configurable and customizable

Release Timeline



Key Takeaways

**Broadest
Native
Controls**

**Largest open
XDR with
490+ data
sources**

**Fastest Path
to XDR**

We meet you where you are, help you realize XDR faster and align to your future



Trellix