Trellix

APJ Partner Summit'24

Partnering for a Secure Future

Join us at the APJ Partner Summit

Phuket, Thailand

10-12 JULY 2024

Trellix

Trellix Helix Connect

APJ Partner Summit 2024

July 8, 2024

Speakers for Today

Ron Wang
Sr Director, APJ SE

Hidemitsu Sakurai
Sr Director, Japan SE

Manish Sinha
Director, India SE

Carl Thaw
Global Enablement

Trellix

What factors does your consider most important when evaluating different XDR solutions?

Agenda

1) **Why the need for Trellix Helix Connect?**
Challenges it solves

2) **How does Trellix solve the problem?**
How we are different

3) **About the Trellix solution**
Overview & Demo

4) **Personas**
Who to target

5) **Proof Points**
Customer Case Study

6) **Product Packaging**
Product SKUs

7) **Upsell and Cross-Sell**
Positioning the solution to customers

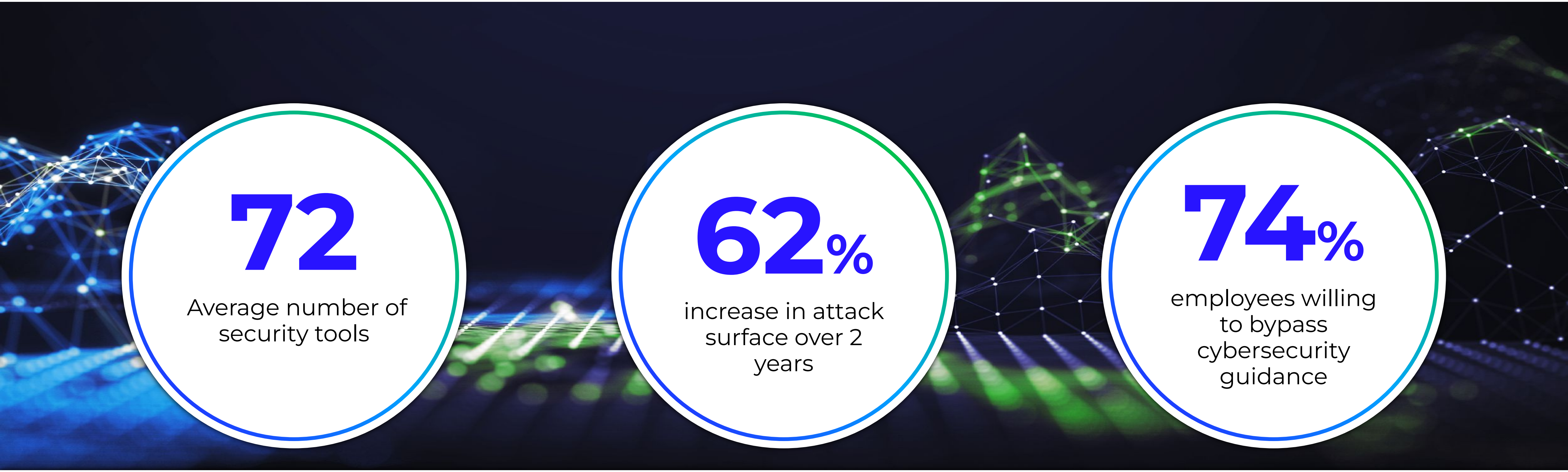
Trellix

Trellix

Why Trellix Helix Connect?

The challenges

Today’s Challenges



72

Average number of security tools

62%

increase in attack surface over 2 years

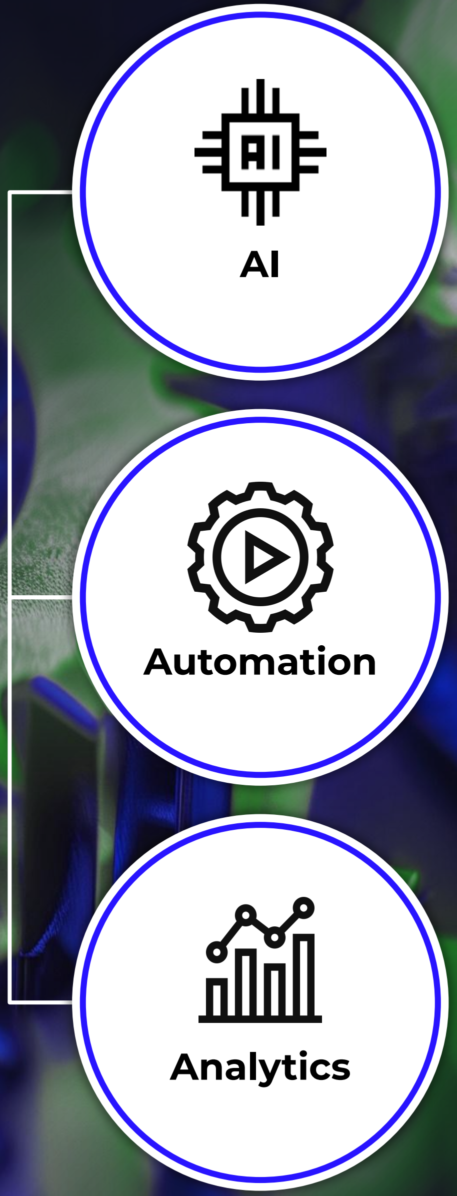
74%

employees willing to bypass cybersecurity guidance

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

Security Needs a Platform

Powered by:

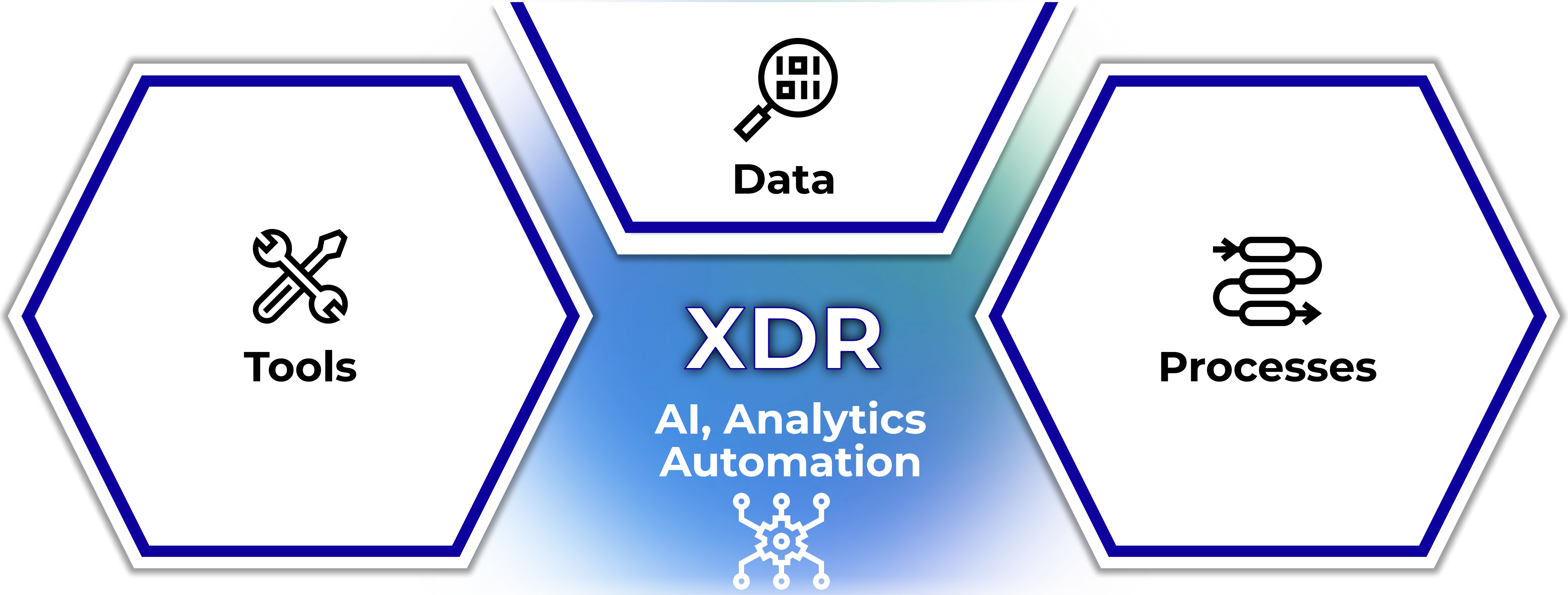


AI

Automation

Analytics

XDR: the Convergence of Security



A platform to respond across your open, connected enterprise

Why the Need for XDR solution?

↑ **MTTD**

Less false positives, prioritized alerts

↑ **MTTR**

AI - guided investigations, repair in minutes

>20 to 1

Decrease your vendor footprint

Respond faster:

20x increased SOC efficiency

Trellix

What if we dont change - status quo?

Staff Burnout

Turnover and burnout of teams from alert fatigue

Constantly Reacting

Missed detections leading to long, expensive firefights

Increased MTTD/MTTR

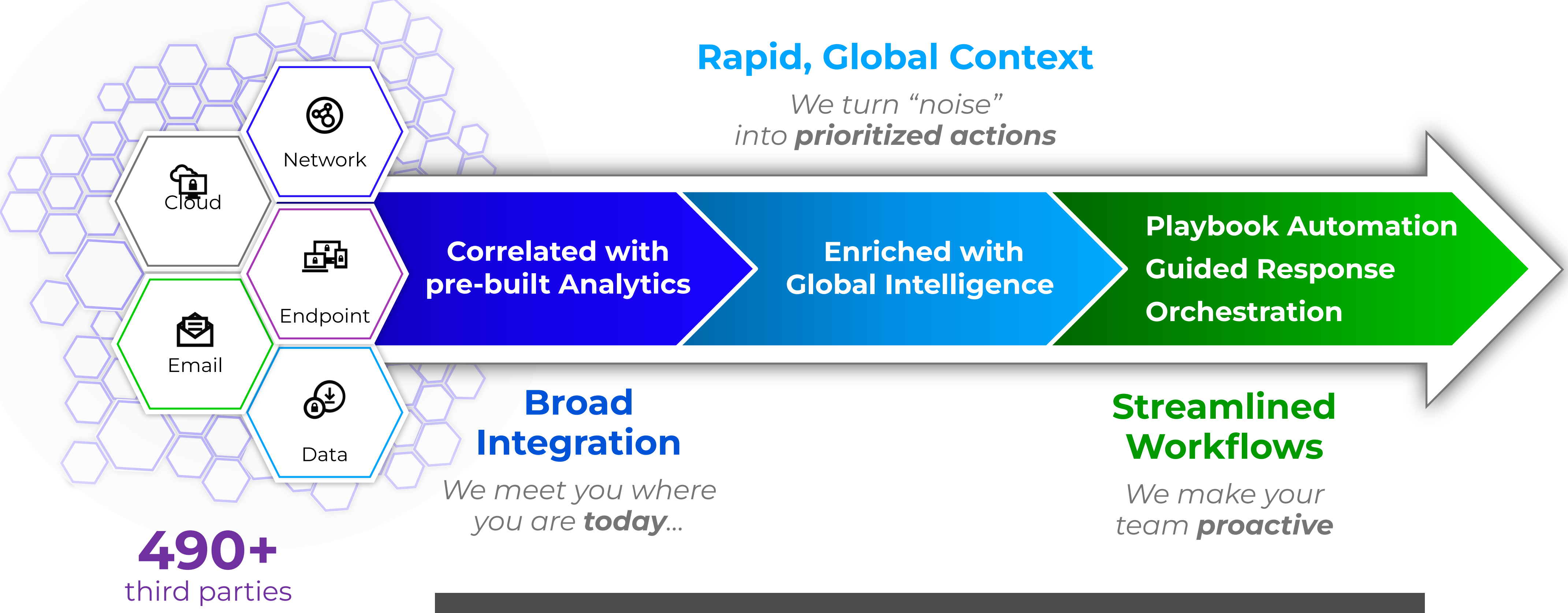
Siloed tools and data prolonging expensive manual processes

Trellix

How Trellix Helix Connect solves it

How we are different

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, MTTI, MTTR in minutes

Broad Integration

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

Streamlined Workflows

We make your
team ***proactive***

...because minutes matter

Trellix

What Makes Trellix Unique?

Broadest Native Controls

35+ capabilities replaces 6+ controls

3X More Integrations

500+ across 230+ vendors

Fastest Path to XDR

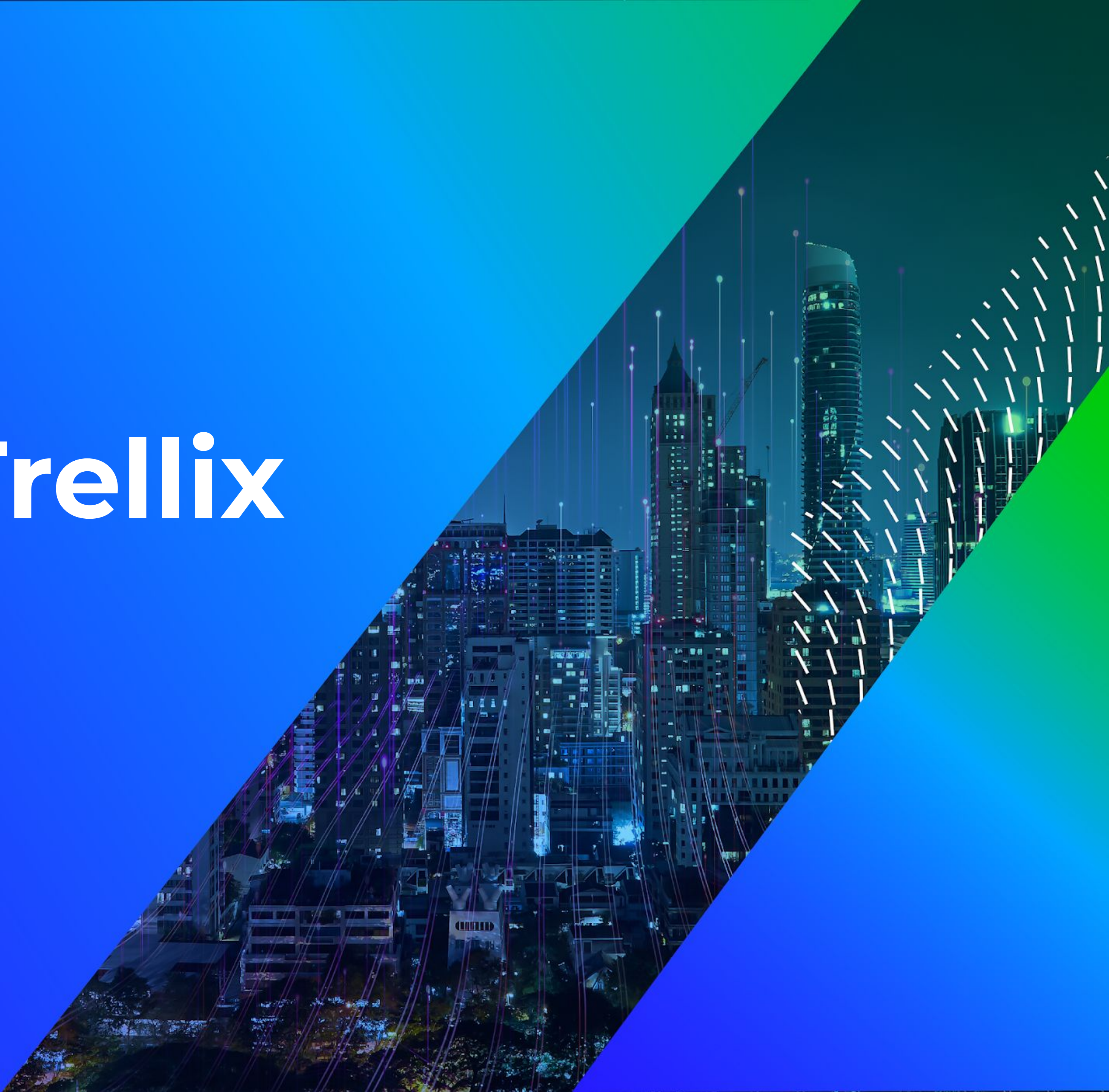
<1 week to deploy, months of built-in engineering

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

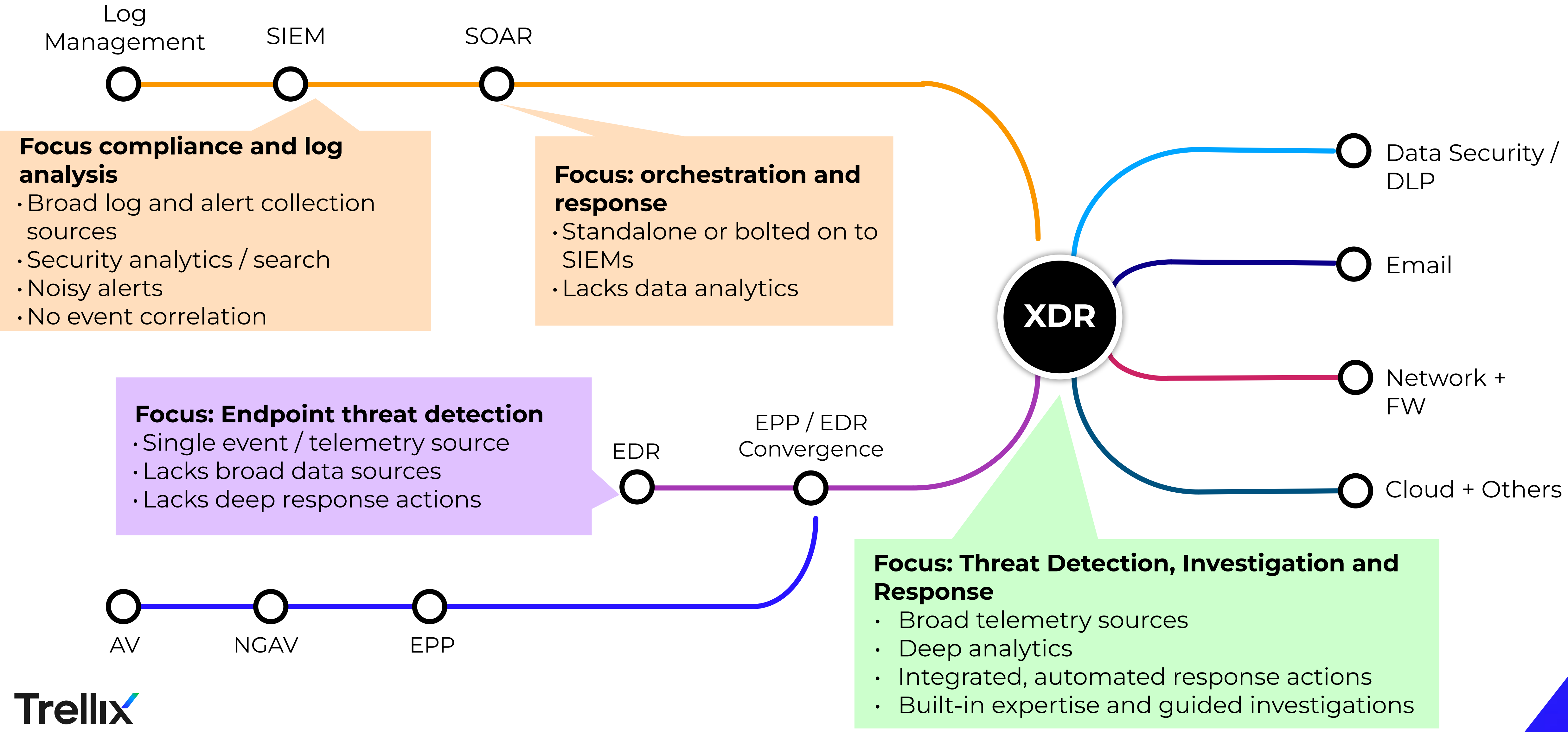
Trellix

About the Trellix solution

How we are different



Point Solutions are Incomplete



Focus compliance and log analysis

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

Focus: orchestration and response

- Standalone or bolted on to SIEMs
- Lacks data analytics

Focus: Endpoint threat detection

- Single event / telemetry source
- Lacks broad data sources
- Lacks deep response actions

Focus: Threat Detection, Investigation and Response

- Broad telemetry sources
- Deep analytics
- Integrated, automated response actions
- Built-in expertise and guided investigations

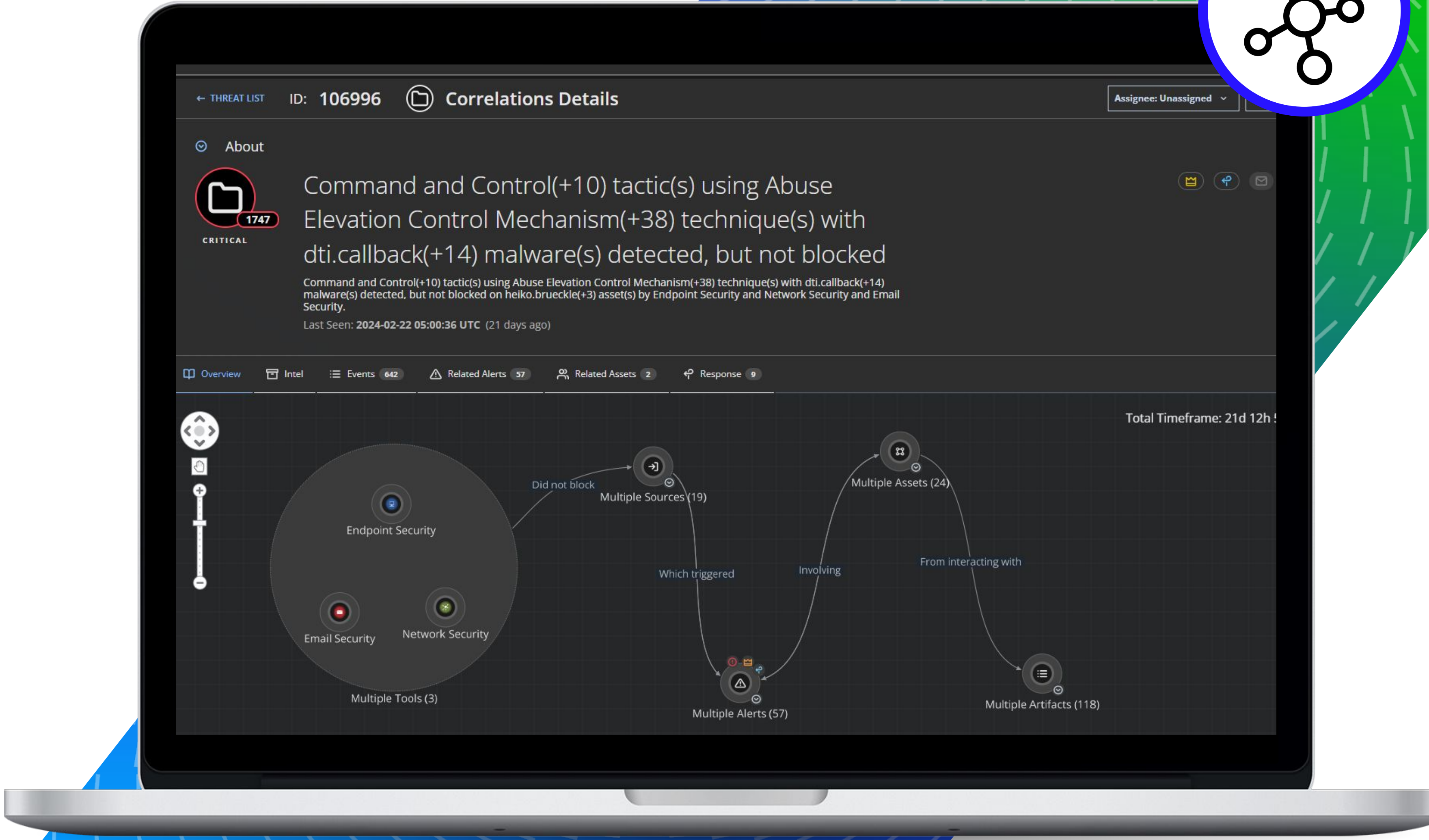
Why XDR is needed?

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

Minimize MTTR and increase SOC efficacy across the connected enterprise

Trellix Helix Connect

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



← THREAT LIST ID: 106996 Correlations Details

Assignee: Unassigned

About

1747

CRITICAL

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

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

Last Seen: **2024-02-22 05:00:36 UTC** (21 days ago)

Trellix

How Trellix Helix Connect Works

1. Broad data Ingestion

Open and
native integrations

2. Detections:

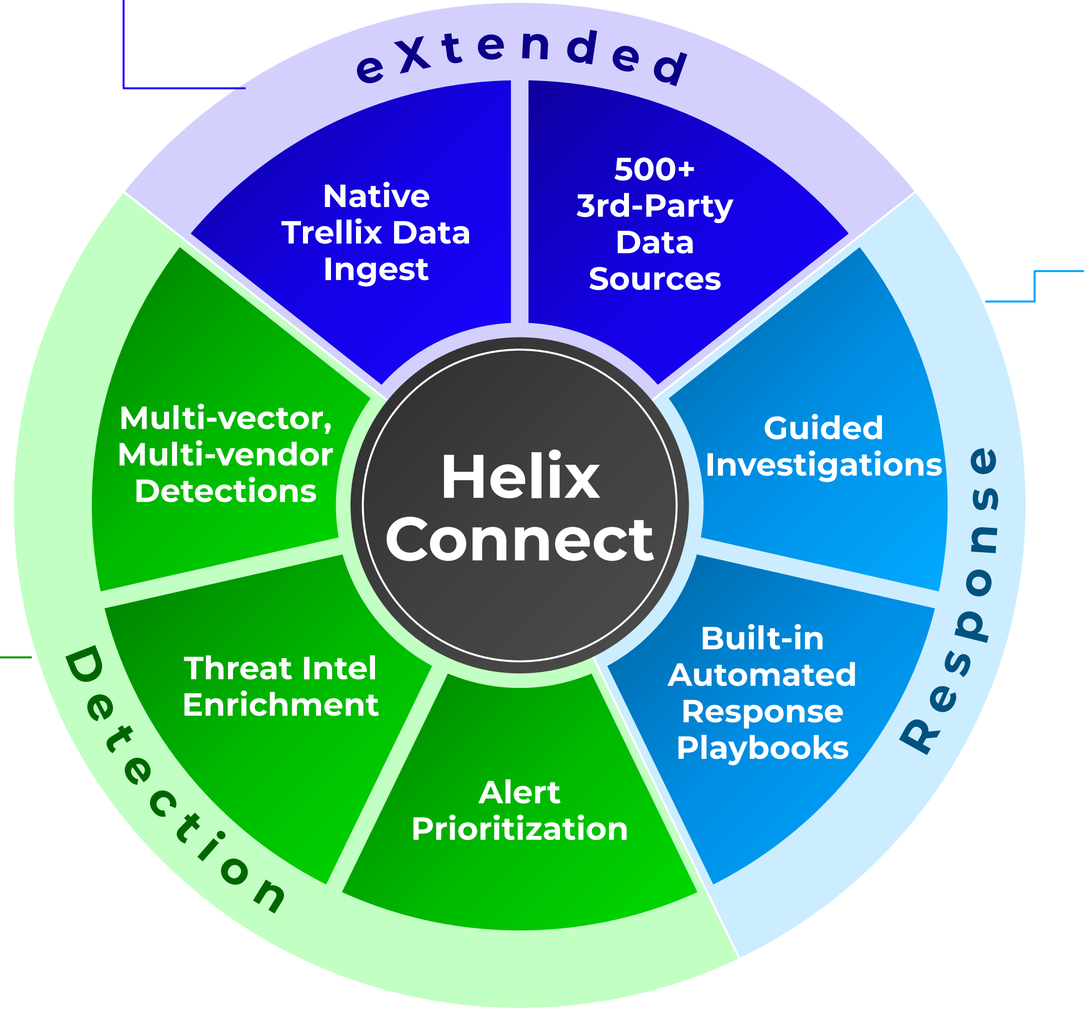
Analytics

Automated
threat elimination

Noise suppression

Enrichment

Prioritization



eXtended
Native Trellix Data Ingest
500+ 3rd-Party Data Sources
Helix Connect
Multi-vector, Multi-vendor Detections
Threat Intel Enrichment
Alert Prioritization
Detection
Guided Investigations
Built-in Automated Response Playbooks
Response

3. Response

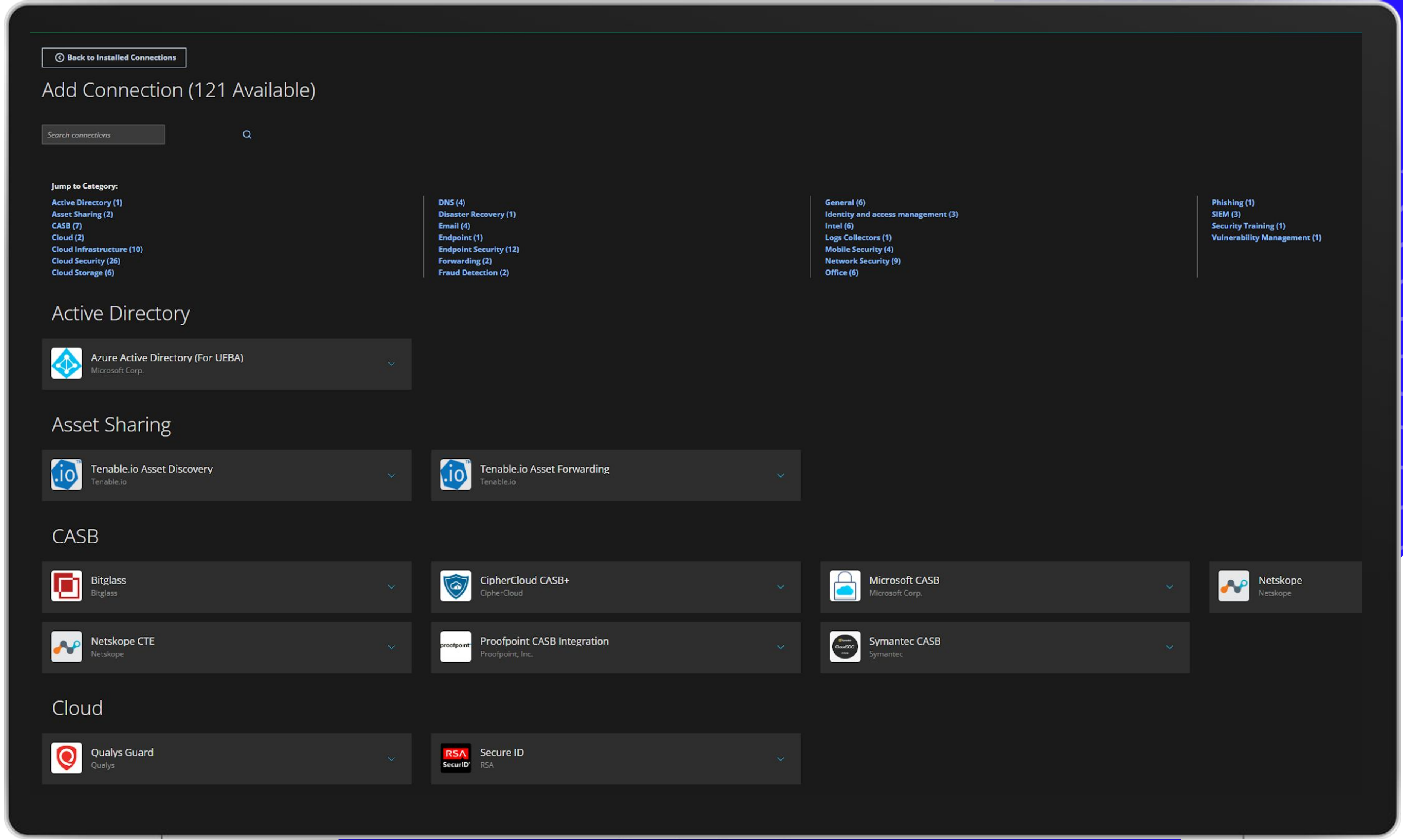
On-prem / cloud
orchestration
and response

AI-guidance

Pre-built,
customizable
playbooks

Trellix

Quickly Integrate Data



Back to Installed Connections

Add Connection (121 Available)

Search connections

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 (2)
Fraud Detection (2)

General (6)
Identity and access management (3)
Intel (6)
Logs Collectors (1)
Mobile Security (4)
Network Security (9)
Office (6)

Phishing (1)
SIEM (3)
Security Training (1)
Vulnerability Management (1)

Active Directory

Azure Active Directory (For UEBA)
Microsoft Corp.

Asset Sharing

Tenable.io Asset Discovery
Tenable.io

Tenable.io Asset Forwarding
Tenable.io

CASB

Bitglass
Bitglass

CipherCloud CASB+
CipherCloud

Microsoft CASB
Microsoft Corp.

Netskope
Netskope

Netskope CTE
Netskope

Proofpoint CASB Integration
Proofpoint, Inc.

Symantec CASB
Symantec

Cloud

Qualys Guard
Qualys

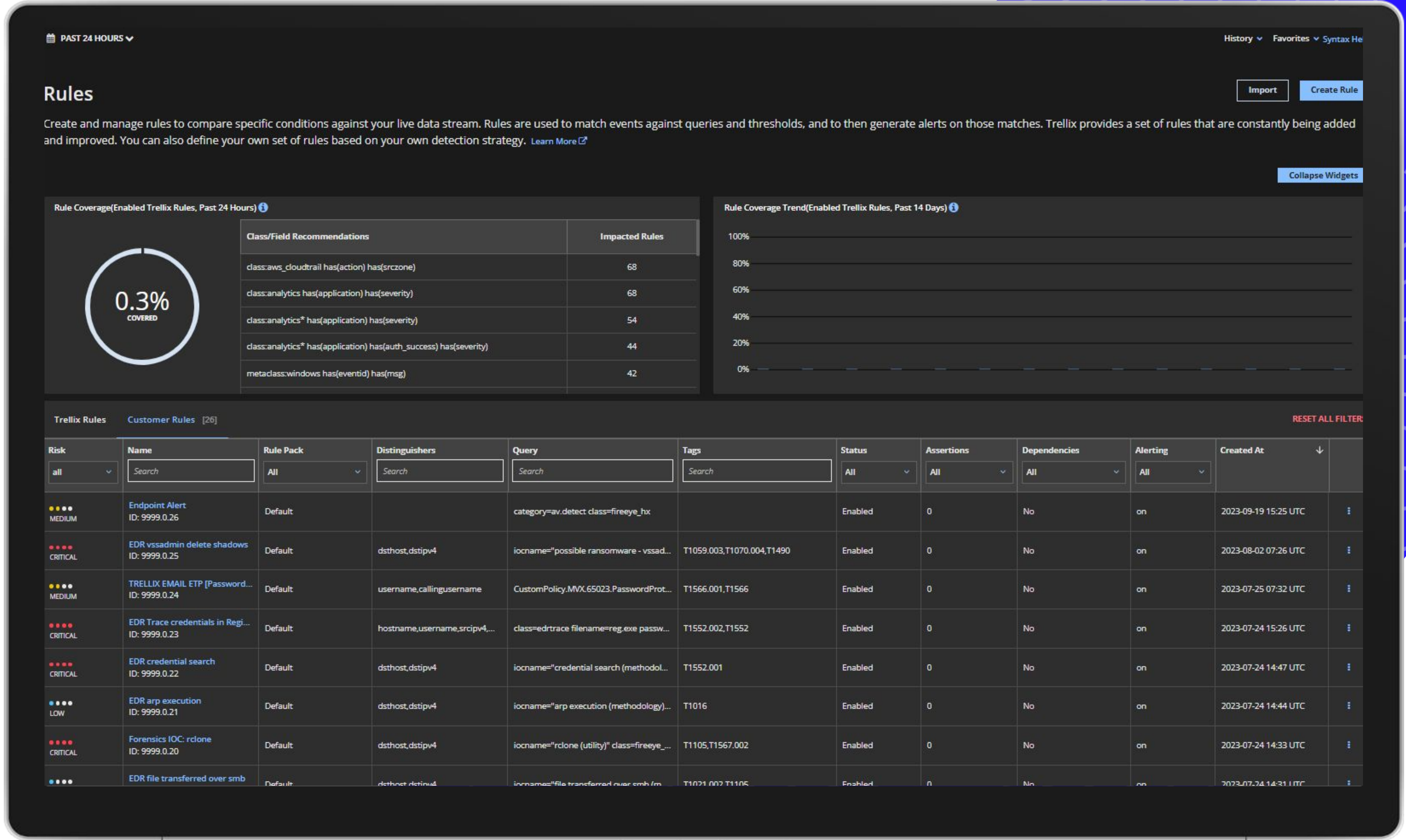
Secure ID
RSA

500+
3rd-party sources

100+
different SaaS solutions across multiple domains

Trellix

Surface New Detections within Hours



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:aws_cloudtrail has(action) has(srczone)	68
class:analytics has(application) has(severity)	68
class:analytics* has(application) has(severity)	54
class:analytics* has(application) has(auth_success) has(severity)	44
metaclass:windows has(eventid) has(msg)	42

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

Trellix Rules   Customer Rules [26]

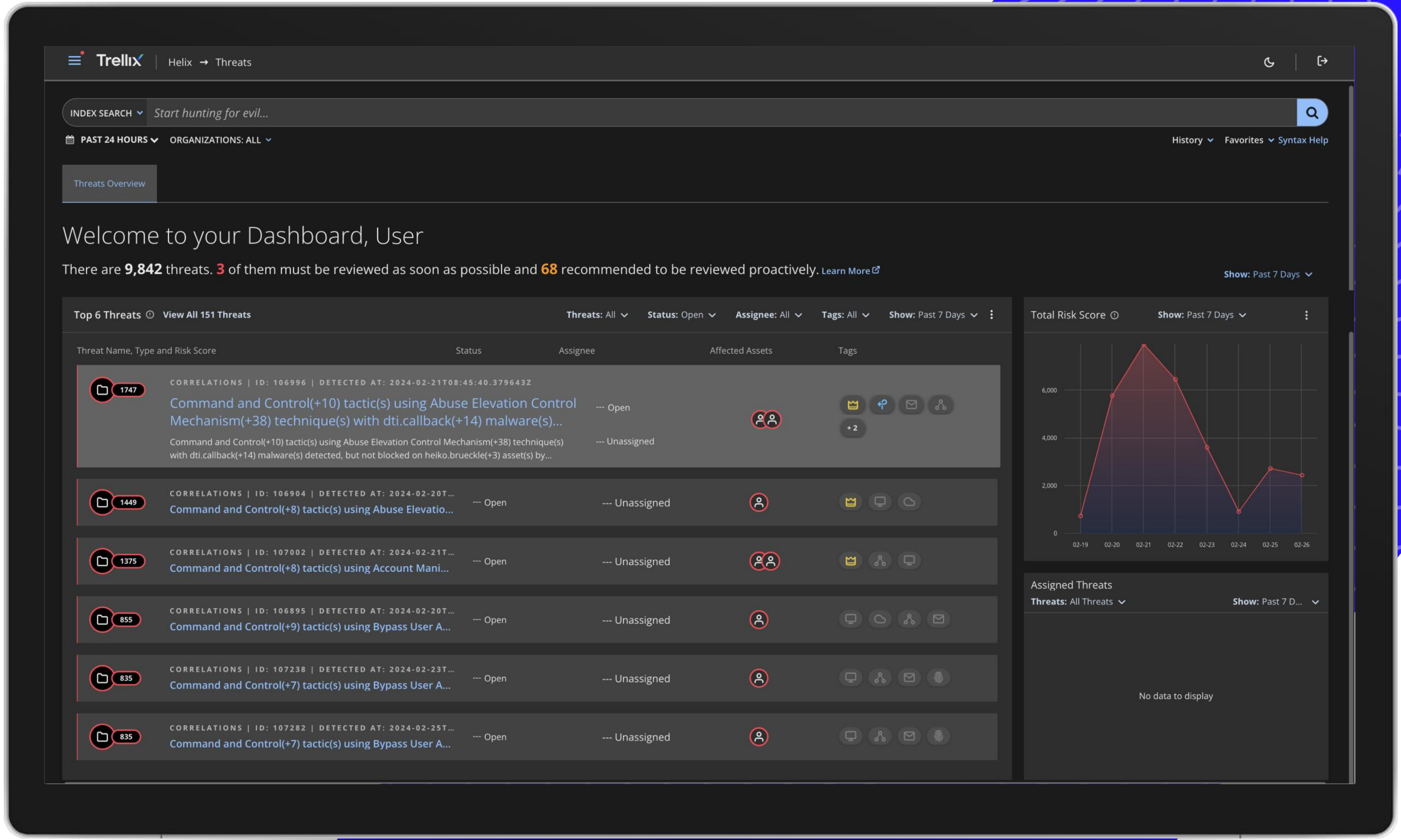
Risk	Name	Rule Pack	Distinguishers	Query	Tags	Status	Assertions	Dependencies	Alerting	Created At
all	Search	All	Search	Search	Search	All	All	All	All	
●●●● MEDIUM	Endpoint Alert ID: 9999.0.26	Default		category=av.detect class=fireeye_hx		Enabled	0	No	on	2023-09-19 15:25 UTC
●●●● CRITICAL	EDR vssadmin delete shadows ID: 9999.0.25	Default	dsthost,dstipv4	iocname="possible ransomware - vssad...	T1059.003,T1070.004,T1490	Enabled	0	No	on	2023-08-02 07:26 UTC
●●●● MEDIUM	TRELLIX EMAIL ETP [Password... ID: 9999.0.24	Default	username,callingusername	CustomPolicy.MVX.65023.PasswordProt...	T1566.001,T1566	Enabled	0	No	on	2023-07-25 07:32 UTC
●●●● CRITICAL	EDR Trace credentials in Regi... ID: 9999.0.23	Default	hostname,username,srcipv4,...	class=edrtrace filename=reg.exe passw...	T1552.002,T1552	Enabled	0	No	on	2023-07-24 15:26 UTC
●●●● CRITICAL	EDR credential search ID: 9999.0.22	Default	dsthost,dstipv4	iocname="credential search (methodol...	T1552.001	Enabled	0	No	on	2023-07-24 14:47 UTC
●●●● LOW	EDR arp execution ID: 9999.0.21	Default	dsthost,dstipv4	iocname="arp execution (methodology)...	T1016	Enabled	0	No	on	2023-07-24 14:44 UTC
●●●● CRITICAL	Forensics IOC: rclone ID: 9999.0.20	Default	dsthost,dstipv4	iocname="rclone (utility)" class=fireeye_...	T1105,T1567.002	Enabled	0	No	on	2023-07-24 14:33 UTC
●●●●	EDR file transferred over smb	Default	dsthost,dstipv4	iocname="file transferred over smb (m	T1021.002,T1105	Enabled	0	No	on	2023-07-24 14:31 UTC

2000+ rules, integrated intelligence matching

50+ analytics

Trellix

Automatically Prioritize Threats



Welcome to your Dashboard, User

There are **9,842** threats. **3** of them must be reviewed as soon as possible and **68** recommended to be reviewed proactively. Learn More

Show: Past 7 Days

Top 6 Threats · View All 151 Threats

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

Threat Name, Type and Risk Score	Status	Assignee	Affected Assets	Tags
1747 CORRELATIONS | ID: 106996 | DETECTED AT: 2024-02-21T08:45:40.379643Z Command and Control(+10) tactic(s) using Abuse Elevation Control Mechanism(+38) technique(s) with dti.callback(+14) malware(s)... Command and Control(+10) tactic(s) using Abuse Elevation Control Mechanism(+38) technique(s) with dti.callback(+14) malware(s) detected, but not blocked on heiko.brueckle(+3) asset(s) by...	--- Open	--- Unassigned		+2
1449 CORRELATIONS | ID: 106904 | DETECTED AT: 2024-02-20T... Command and Control(+8) tactic(s) using Abuse Elevatio...	--- Open	--- Unassigned		
1375 CORRELATIONS | ID: 107002 | DETECTED AT: 2024-02-21T... Command and Control(+8) tactic(s) using Account Mani...	--- Open	--- Unassigned		
855 CORRELATIONS | ID: 106895 | DETECTED AT: 2024-02-20T... Command and Control(+9) tactic(s) using Bypass User A...	--- Open	--- Unassigned		
835 CORRELATIONS | ID: 107238 | DETECTED AT: 2024-02-23T... Command and Control(+7) tactic(s) using Bypass User A...	--- Open	--- Unassigned		
835 CORRELATIONS | ID: 107282 | DETECTED AT: 2024-02-25T... Command and Control(+7) tactic(s) using Bypass User A...	--- Open	--- Unassigned		

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

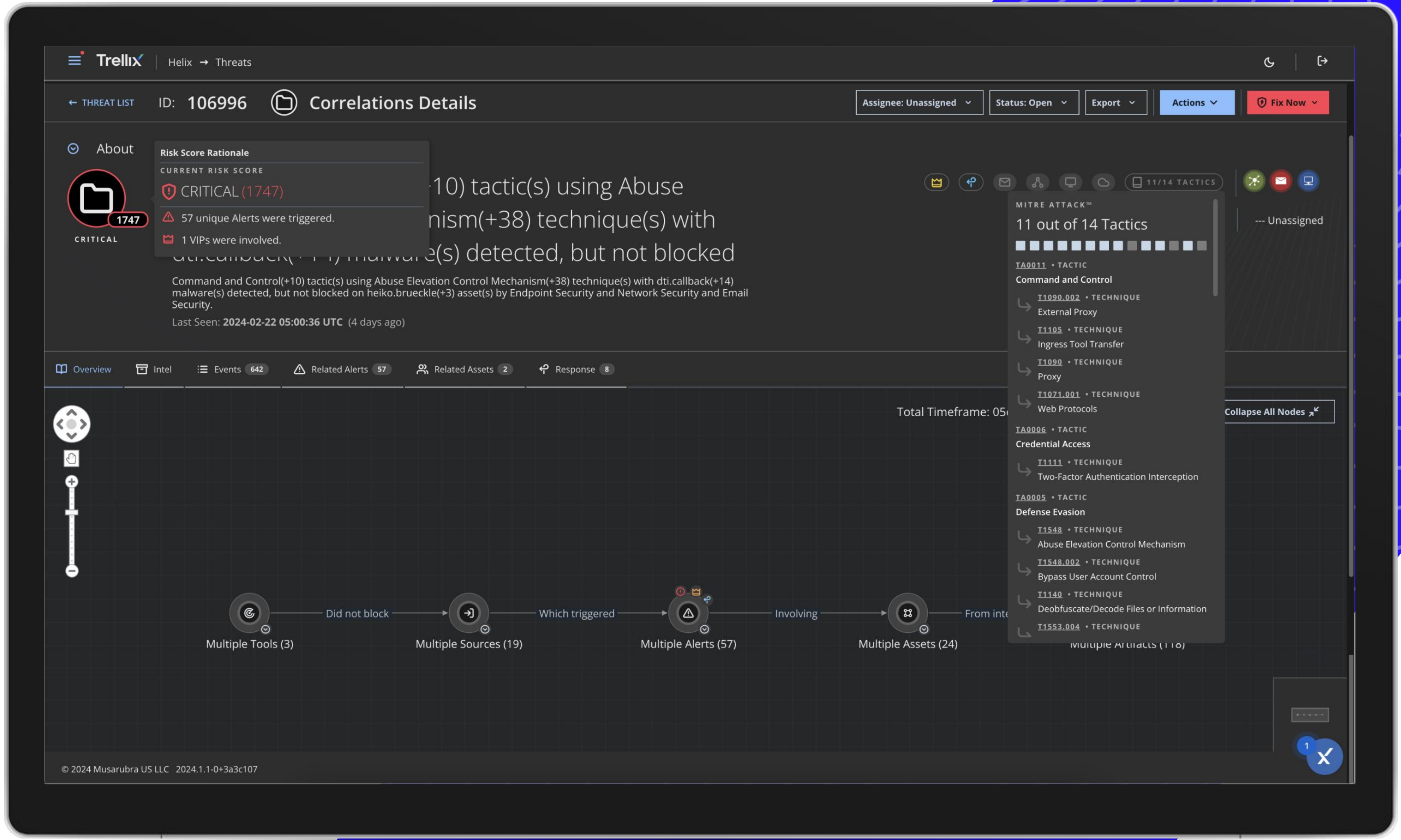
Assigned Threats

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

No data to display

Address the most critical threats first

Map the Complete Threat Journey



ID: 106996 Correlations Details

About

1747
CRITICAL

Risk Score Rationale

CURRENT RISK SCORE

CRITICAL (1747)

57 unique Alerts were triggered.

1 VIPs were involved.

-10) tactic(s) using Abuse
nism(+38) technique(s) with
e(s) detected, but not blocked

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

Last Seen: **2024-02-22 05:00:36 UTC** (4 days ago)

Total Timeframe: 05

MITRE ATTACK™

11 out of 14 Tactics

TA0011 • TACTIC
Command and Control

T1090.002 • TECHNIQUE
External Proxy

T1105 • TECHNIQUE
Ingress Tool Transfer

T1090 • 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

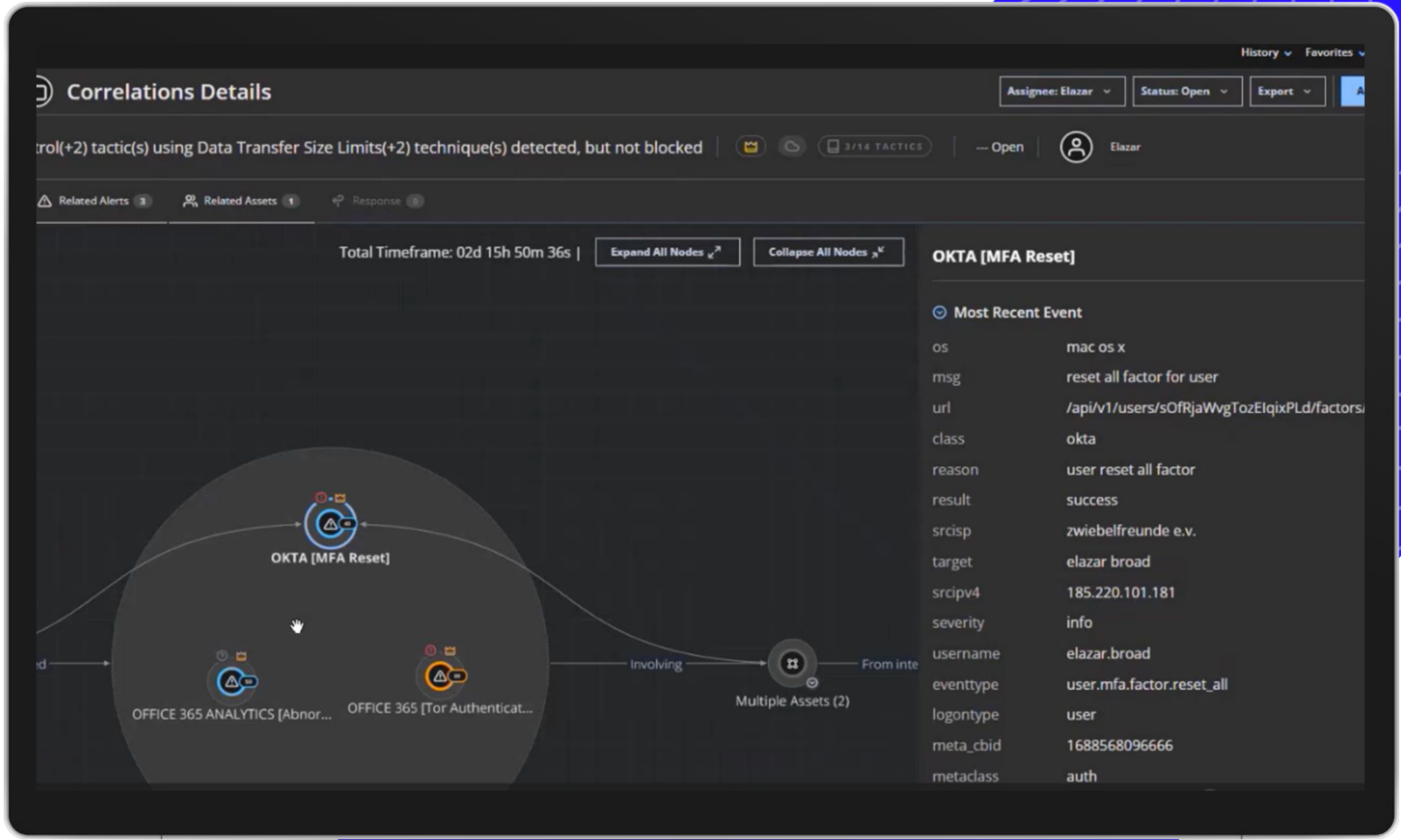
T1140 • TECHNIQUE
Deobfuscate/Decode Files or Information

T1553.004 • TECHNIQUE

© 2024 Musarubra US LLC 2024.1.1-0+3a3c107

Mapped to MITRE ATT&CK tactics

Automatically take Action



Correlations Details

trol(+2) tactic(s) using Data Transfer Size Limits(+2) technique(s) detected, but not blocked

--- Open

Elazar

Total Timeframe: 02d 15h 50m 36s |

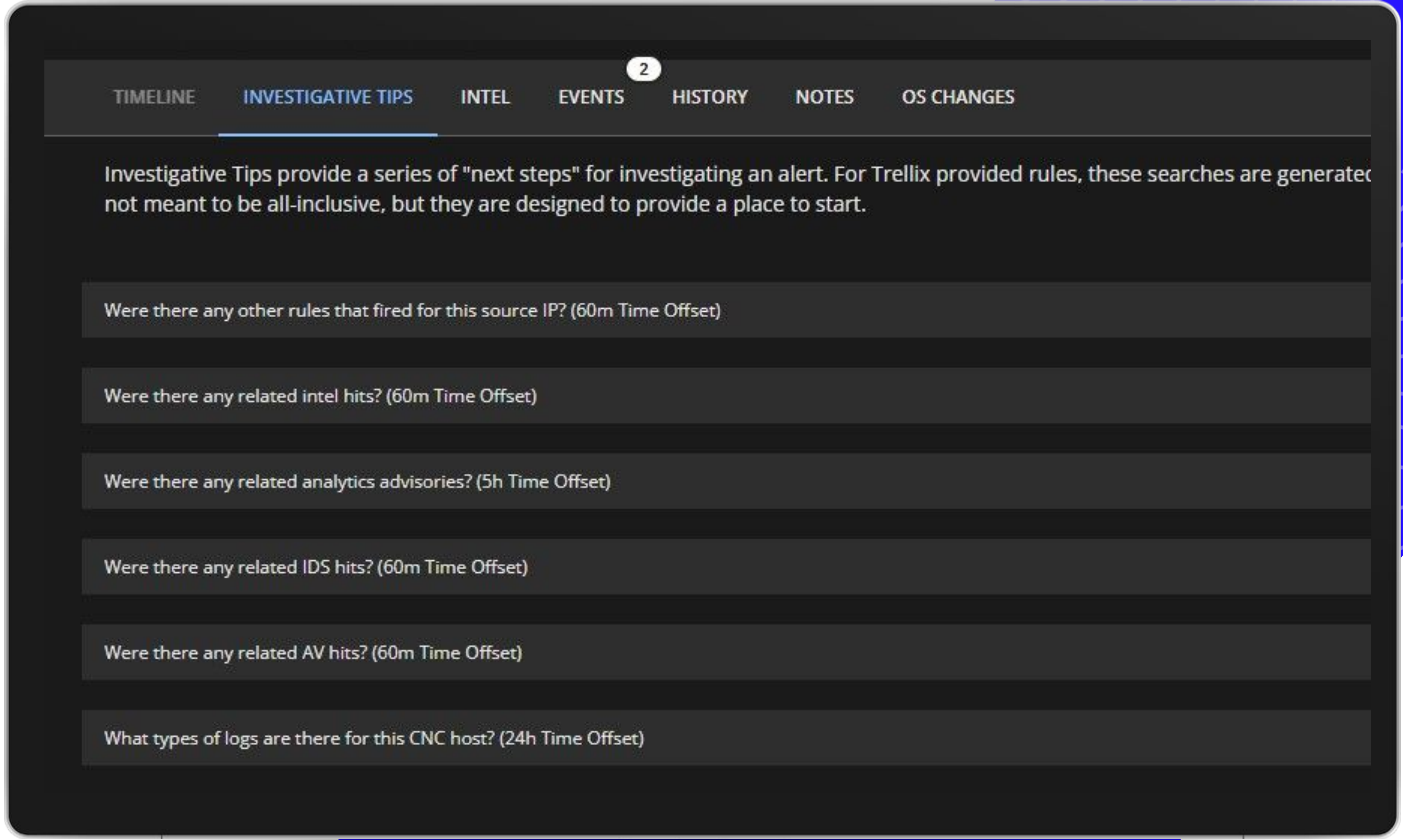
OKTA [MFA Reset]

Most Recent Event

os	mac os x
msg	reset all factor for user
url	/api/v1/users/sOfRjaWvgTozElqixPLd/factors/
class	okta
reason	user reset all factor
result	success
srcisp	zwiebelfreunde e.v.
target	elazar broad
srcipv4	185.220.101.181
severity	info
username	elazar.broad
eventtype	user.mfa.factor.reset_all
logontype	user
meta_cbid	1688568096666
metaclass	auth

Detections trigger responses in your tools

Leverage AI-guided Investigations



Investigative Tips provide a series of "next steps" for investigating an alert. For Trellix provided rules, these searches are generatec not meant to be all-inclusive, but they are designed to provide a place to start.

Were there any other rules that fired for this source IP? (60m Time Offset)

Were there any related intel hits? (60m Time Offset)

Were there any related analytics advisories? (5h Time Offset)

Were there any related IDS hits? (60m Time Offset)

Were there any related AV hits? (60m Time Offset)

What types of logs are there for this CNC host? (24h Time Offset)

Enable and upskill more of your team

What Can Helix Connect do for You?

40-60+
siloed tools

4-10K
unranked alerts a day

30 minutes
to begin remediations

1
location to view correlated data

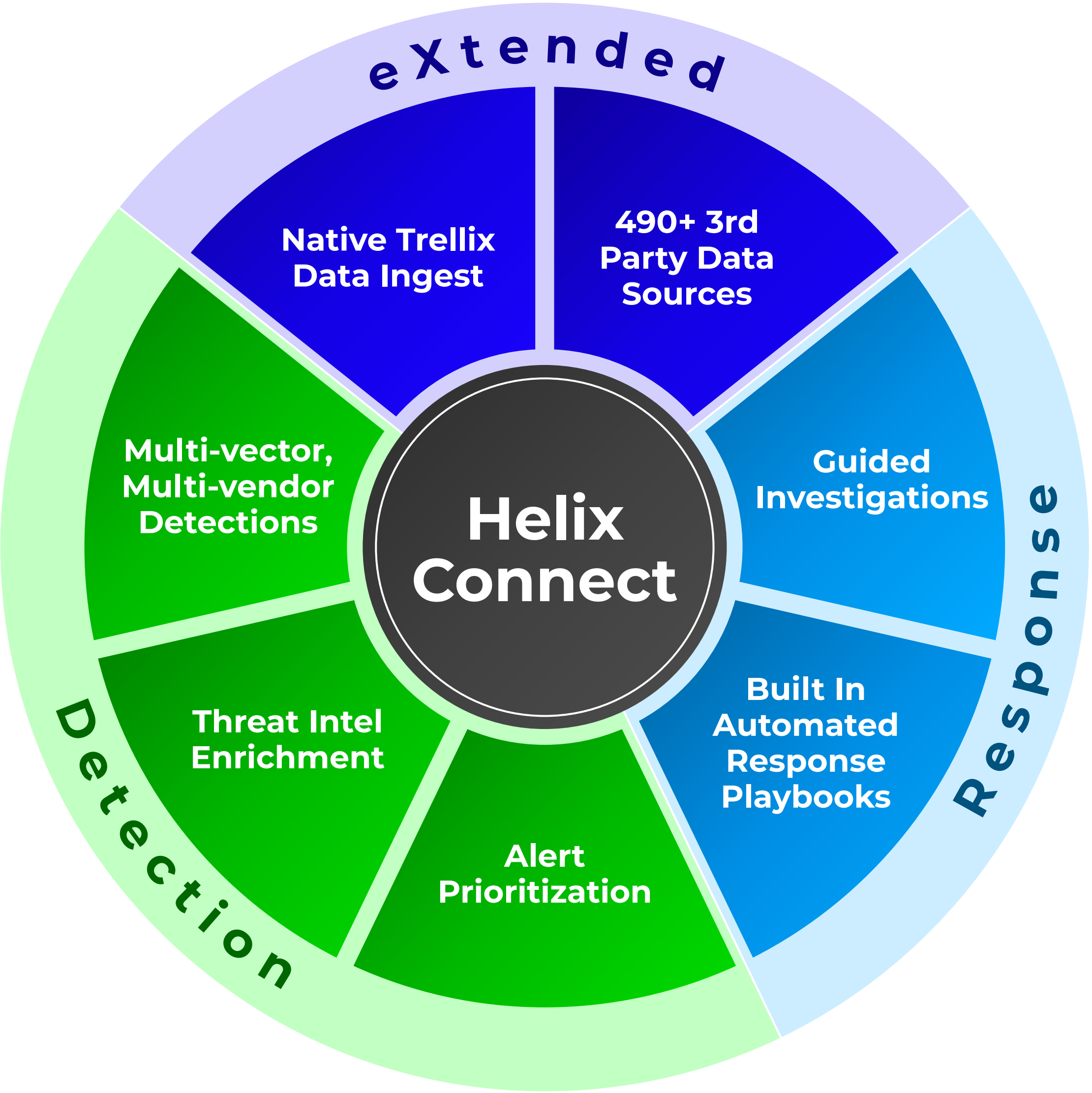
>70%
less false positives and events prioritized by impact

5
minutes or less to remediation actions

Trellix

Trellix Helix Connect

- Optimize SecOps Efficiency rapidly investigate and remediate threats minimizing MTTR
- Largest open XDR with 500+ data sources
- Detect attacks missed by silo security controls
- Contextualize threats with intel automatically
- Mitigate attacks with on-premises / cloud orchestration and response


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

Trellix

DEMO

Trellix

Personas

Who to target

Economic Buyer - CISO

Priorities:

- Operational Efficiency
- Reduce MTTD, MTTR
- Faster Response Cycles

Before Scenario:

- Limited SOC budget and too many incidents are costly
- Utilizing siloed security solutions, out of the box and open source,
  to secure the entire enterprise and digital assets; multiple vendors increases cost and deluge of alerts
- Utilizing shared IT personnel resources to monitor enterprise
- SIEM is cumbersome to manage and costly for data ingestion
  and storage
- C-Levels / Board are constantly asking about cyber risk

Positive Business Outcomes:

- Improved SOC efficiency and leveraging multiple native controls and vendor consolidation
- Managed risk and cost better
- Decreased breaches
- Better positioned for strategic SOC initiatives
- Increased prevention with a better security posture
- Improved Security Operations and SOC staff productivity (move quickly from a sea of alerts to prioritized incidents – removing repetitive tasks)
- Faster incident response cycles

Trellix

Technical Buyer - Director, Information Technology

Priorities:

- Minimize Risk
- Minimize Cost
- Increase Coverage

Before Scenario:

- Limited visibility
- Deluge of alerts creating inability to make effective decisions in a sea of noise
- Legacy-siloed security architectures and IT assets can’t keep up with rapidly advancing adversaries
- Manually pivoting between tools, cutting and pasting – further inhibiting proactive visibility and efficiency
- Seeking threat intelligence manually or through cumbersome search
- Long detect and response cycles offering dwell time to adversary

Positive Business Outcomes:

- Increased SOC productivity and morale
- Decreased SOC attribution
- Minimized cyber risk
- Gained comprehensive visibility and control with a prioritized focus on what matters most
- Shorter incident detection and response cycles
- Improved efficacy
- Increased proactive efforts to preempt threats

Trellix

Champion - SOC Manager

Priorities:

- Risk Management and Prevention
- Reduce MTTD, MTTR
- Increase SOC Productivity and Morale

Before Scenario:

- Excessive alerts; constantly deleting alerts without reviewing them
- Too many things on the screen
- Too much time spent firefighting and not enough time to spend looking for unknown threats using hunting mechanisms
- Reactive workflows investigating alerts
- Not fully understanding the threat landscape
- Growing risk around the undetectable
- Overwhelmed / burnt out SOC team

Positive Business Outcomes:

- Less time spent per incident and more time for strategic activities and threat hunting
- Prioritization of critical alerts and incidents; guiding others around more investigation or containment
- Gained a better overall SOC-team efficiency and effectiveness

Pain Points and Discovery Questions

Pain Points	Discovery Questions
Too many siloed tools fragment visibility, control, and cause alert fatigue	● Describe how your team correlates data from multiple sources? ● Do you think your current security tools are adequately protecting your organization? ● What visibility do you have into your security infrastructure? ● How many different consoles do you use for your daily activities? How many different consoles do you use when dealing with a cybersecurity incident? ● How much time do you spend dealing with false positives? ● How many alerts is your team able to review and triage in a day? ● What is your target response time for high-priority alerts? How often do you hit that goal?

Pain Points and Discovery Questions

Pain Points	Discovery Questions
Sophisticated threats continue to go undetected by point tools alone	● What detection and prioritization methods would you like to add, including those to prioritize alerts? ● What do you do when your team misses critical alerts? How often do you believe it happens? ● What gaps do you have in covering your attack surfaces? How do you ensure coverage over those gaps? ● What are your priorities for reducing human error? ● How would it improve your security posture to understand better, monitor, and deal with sophisticated threats?

Pain Points and Discovery Questions

Pain Points	Discovery Questions
Limited organizational resources and expertise	● What kind of automated tools do you have? ● What resources do you need to better mitigate attacks? ● What challenges do you face when trying to hire for your SOC positions? ● What challenges to improving your organization's security productivity are you seeking to overcome? Where do you think your gaps may be (e.g. resources, processes, tools)? ● How would you describe a better or preferred SOC environment? ● What are the significant concerns for your SOC team? Are they overworked? Do they feel they have the right tools to do their job?

Trellix

Proof Points

Customer Case Studies

Retailer Gains Deep Visibility and Efficient Incident Response

Customer Success Story: Proactively defends against cyberattacks

Industry: Retail Clothing | **Trellix Products:** Trellix Endpoint Security, Helix Connect

CHALLENGES

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

SOLUTIONS

- Trellix Endpoint Security incorporates mixture of next generation antivirus protection and data encryption, providing proactive defense against intrusion and keeping their data secure.
- Trellix Helix Connect integrates, correlates and simplifies visibility of threats while empowering less experienced staff to perform incident response

RESULTS

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

"Helix is extremely valuable to me for investigating and managing incidents.
The platform provides easy, immediate access and deep visibility into every endpoint across the enterprise,"
— Security Manager, High-profile Luxury Goods Retailer

Full Service Financial Institution Modernizes their SOC

Customer Success Story: Trellix helps to stop threats faster and lower costs

Industry: Banking / Financial | **Trellix Products:** Helix Connect, Trellix XDR Platform (NX, IVX)

CHALLENGES

- Mature organization, but weak detection using current tools
- Attempted to build a modern SOC themselves, but found costs were too high trying to connect and integrate tools themselves
- Alert fatigue and overwhelmed teams

SOLUTIONS

- Trellix Helix Connect delivers hundreds of integrations with native and third party tools to create deep, multi-vector, multi-vendor detections
- The Trellix Helix Connect offers the deepest number of native security controls in the industry spanning endpoint, network, email, data security and more.

RESULTS

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

Trellix was selected from a list of 14 world class integrators and service providers not only because of our integrations and abilities to lower costs, but because of our relationship with the customer who said “we buy from people.”

Trellix

Product Packaging

What SKUs

Packaging

Helix Connect has SKUs for the product and for add-ons to data ingestion and retention. It can be sold with components of the Trellix XDR platform, or a customer can use Helix Connect with the third-party (competitive) controls they already own.

SKU	Capabilities	Data Ingestion	Retention
1 Year of Thrive Essential Included in XDR Subscription (Matching 1-year Thrive SKU for each)			
XDR	Helix Connect (SaaS) licensed per user (100 minimum). Retention extensible to 13 months with add-on	100 MB per user/ per month	90 days
OXDR-nn**GB-ADDON**	Extends Helix Connect data ingest to accommodate 3rd-party data sources	50, 100, 250 GB and 1 TB options per day	90 days
OXDR-nn**GB-10M-ADDON**	Extends Helix Connect Event retention to 13 months. Requires matching OXDR-nnGB-ADDON SKU	50, 100, 250 GB and 1 TB options	13 months

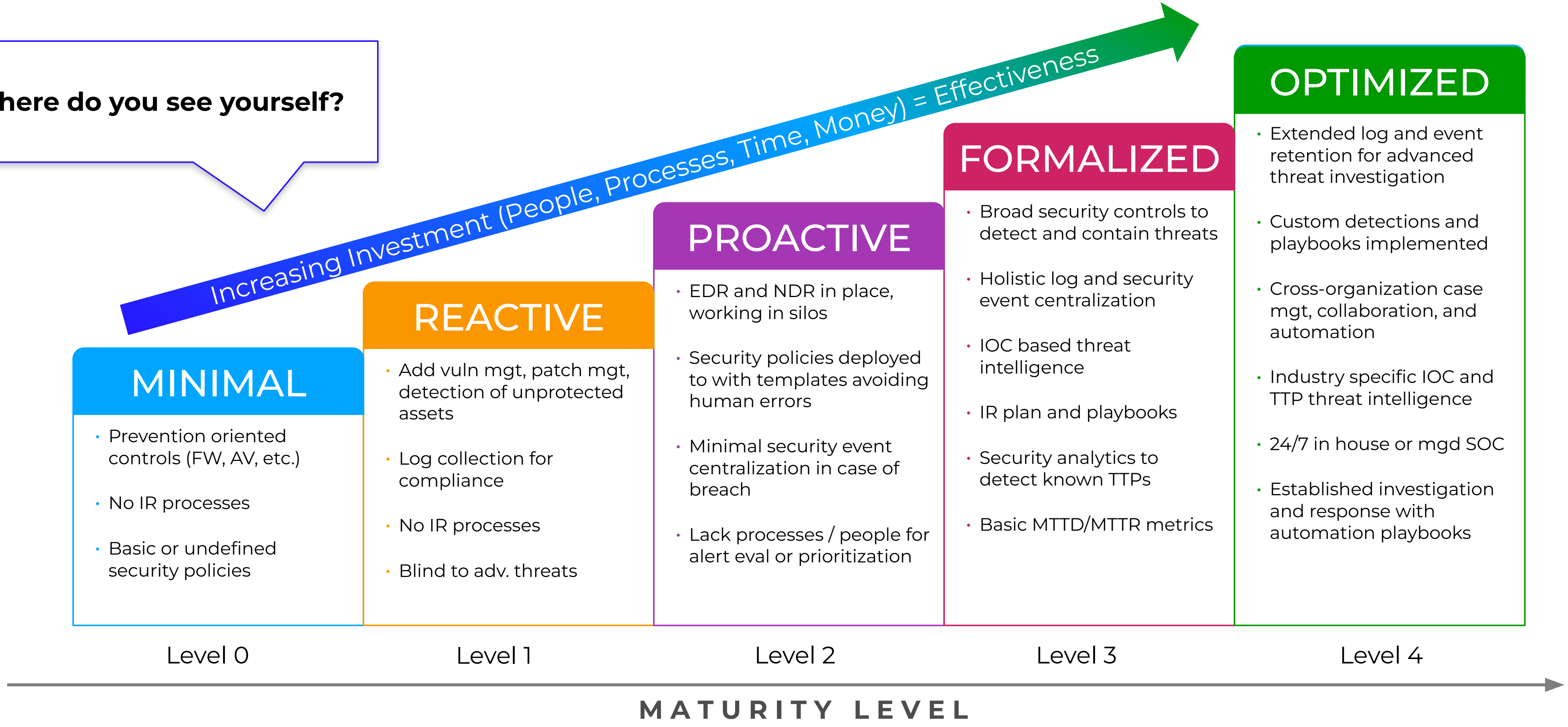
Trellix

UpSell and Cross-Sell

What to position to customers

Organizational SecOps Maturity

Where do you see yourself?



Increasing Investment (People, Processes, Time, Money) = Effectiveness

MINIMAL

- Prevention oriented controls (FW, AV, etc.)
- No IR processes
- Basic or undefined security policies

Level 0

REACTIVE

- Add vuln mgt, patch mgt, detection of unprotected assets
- Log collection for compliance
- No IR processes
- Blind to adv. threats

Level 1

PROACTIVE

- EDR and NDR in place, working in silos
- Security policies deployed to with templates avoiding human errors
- Minimal security event centralization in case of breach
- Lack processes / people for alert eval or prioritization

Level 2

FORMALIZED

- Broad security controls to detect and contain threats
- Holistic log and security event centralization
- IOC based threat intelligence
- IR plan and playbooks
- Security analytics to detect known TTPs
- Basic MTTD/MTTR metrics

Level 3

OPTIMIZED

- Extended log and event retention for advanced threat investigation
- Custom detections and playbooks implemented
- Cross-organization case mgt, collaboration, and automation
- Industry specific IOC and TTP threat intelligence
- 24/7 in house or mgd SOC
- Established investigation and response with automation playbooks

Level 4

MATURITY LEVEL

Go with MDR?

XDR Highest Fit L1-L3
Turnkey Solution to Help Increase Maturity With Minimal Investment

Stick with existing investments

Trellix

Target Customers Ready for XDR

XDR for New Customers

XDR, XDR Add-ons

Why Buy?
Unlock your data
and turn it into prioritized, correlated detections.

Eliminate time spent manually performing detection,
response,
and threat hunting
with automation,
AI, and orchestration.

Multi-vector, multi-vendor detections with no minimum Trellix native tool requirement - XDR that meets you where you are today!

Why they need it:
Easier entry to XDR
with faster time to value
Additional Upsell: Email, NDR, EDR

NDR / EMAIL

NDR -T, EMCL, EMCA

Why Buy?
Leverage investments in Trellix Network and email tools to make event data more visible, accessible and improve your efficiency

Why they need it:
Faster pivot across tools means faster investigations (MTTI)
More context of network data with endpoint. Faster, more accurate scoping.

Additional Upsell: EDR

SIEM/SOAR

McAfee ESM, Splunk, LogRhythm, etc.

Why Buy?
Augment or replace the SIEM with deeper detections, orchestration and automation capabilities designed for multiple levels of expertise

Makes threat hunting accessible and easier for small teams with analytics, and AI guidance

Why they need it
SIEMs are great at collecting data, but do not resolve alert fatigue. They lack automation, orchestration and require specialized skills for threat hunting.

Additional Upsell: Email, NDR, EDR

EDR

MV2/MV6, TRXE (SaaS), TRXHX (On-prem)

Why Buy?
Go beyond Endpoint detections with network, email, data security and more correlated and prioritized for reduced MTTD, MTTR

Integrate your non-Trellix tools to get more value from existing investments

Why they need it

Get more from your Trellix EDR by integrating with Helix Connect for deeper threat hunting capabilities

Additional Upsell: NDR / Email

Each Pathway Leads to XDR

Selling Helix Connect to New Customers

Leveraging our integrations and open platform to land and expand

Target customers:

- Those with competing Endpoint, EDR, Email, Network or other technologies who don't want to replace them to gain XDR
- Any advancing from medium-high security maturity, wanting more automation and orchestration
- Teams overloaded by alerts from multiple tools looking to unlock their data
- Those looking to get more value from existing investments

Customer benefits:

- Helix Connect integrates with the tools they already own making multi-vector, multi-vendor detection possible without any requirement to rip or replace their current tools
- Built-in automation, expertise and AI-guidance to make data across environments and tools actionable
- Automatic false positive elimination and prioritized alerts make analysts more efficient
- Trellix Helix Connect meets them where they are unlocking the data they own

SKU	Value Add	Value Messaging	Customer Positive Outcomes	Discovery Questions
XDR	**XDR meets them where they are**	• XDR with no rip and replace required • Get more value from your existing Endpoint, EDR, Network, Email, etc. investments	• XDR that is ready out of the box to surface missed detections from your tools improving MTTD • Prioritized alerts, multi-vector, multi-vendor detections and AI-guidance make analysts more effective and efficient	• How many tools are required to fully investigate threats in your environment? • Can you collect and analyze data from your security tools automatically or is it a manual process?

Benefits for Sales

- Beachhead for future displacement opportunities with our XDR platform
- Continue to engage in and deepen strategic customer conversations as trusted security advisor; upsell with services

Cautions

- **Don't leave displacement off the table, but lead with XDR**
- **Make sure to line up data / retention needs**

Selling to NDR and Email Customers

Leveraging customers to sell XDR into mixed vendor environments

Target customers:

- Current Email customers with mixed Trellix/third party controls
- NDR customers who want to expand detection and response across tools and environments

Customer benefits:

- Email customers can integrate their third party tools without an additional Trellix native control realizing XDR faster..
- NDR customers can automate detection and response across additional vectors

Current SKUs	Value Add	Value Messaging	Customer Positive Outcomes	Discovery Questions
NDR-T, EMCL, EMCA	**Augmenting current environments with XDR**	• 490+ integrations for your current tools • Deeper detection and response across your environment	• Reduce manual work with automated analysis • Leverage email and your other controls • Faster investigations and responses with correlation beyond network alone	• How do you connect alerts from email to your other tools? • How much time would you save by extending detection and response to more than just your network?

Benefits for Sales

- Existing relationships you can expand
- Can leverage NDR realized values as a driver for XDR
- Creates more visibility into third parties for future displacement

Cautions

- **Don’t position as a replacement to NDR and be mindful of renewal timelines when approaching them**

Trellix

Selling to SIEM / SOAR Customers

Augmenting or replacing a SIEM with Helix Connect

Target customers:

- Current ESM customers or those heavily committed to Splunk, LogRhythm or other leading SIEMs
- Large customers struggling to get orchestration and automation out of their SIEM
- Customers with smaller teams, less experienced staff they would like to enable to perform detection, response and investigations

Customer benefits:

- Increase the volume of automation and orchestration available to them making them more efficient
- Upskill and leverage less experienced staff to be improve MTTD, MTTR
- SIEM investment cost recovered by reducing dependency and footprint

Current SKU	Value Add	Value Messaging	Customer Positive Outcomes	Discovery Questions
ESM & 3rd parties	**Augment the SIEM**	• Trellix XDR can ingest and aggregate insights from many existing SIEM products. It distills and filters the insights from SIEM and other sources so you spend less time manually investigating while increasing your automation and orchestration abilities	• Offload more manual and repetitive tasks increasing efficiency • Focus more time on remediation, less time manually analyzing and determining which alerts are most important • Enable more of your team to detect, respond and hunt for threats using AI-guidance, prebuilt playbooks and automation	• How do you prioritize alerts from your SIEM? • How manual is your triage process today? • How many tools beyond your SIEM are involved in an investigation?

Benefits for Sales

- Existing relationships you can leverage to add XDR value
- Cross-sell oppts with endpoint, EDR
- Future competitive displacement oppts.

Cautions

- **Don’t position XDR as a full replacement to SIEM to larger Enterprise customers**
- **SIEMS can offer SOAR capabilities, explore if / how they’re using what they have**

Upselling Helix Connect to EDR Customers

Extending Detection and Response Beyond the Endpoint to Rapidly Stop Multi-Vector Attacks

Target Customers:

- Organizations with mature endpoint risk management (prevention, protection, and endpoint detection and response) practices looking to continue progressing their security maturity journey
- Mid-market to large organizations with mid-maturity level (developing) SOCs likely with a few analysts and limited SOC processes in place

Customer benefits:

- XDR would help further extend detection and response alongside gain visibility and control across **multiple threat vectors**
- Maximizes endpoint security maturity journey by leveraging existing EDR investment

Current SKU	Value Add	Value Messaging	Customer Positive Outcomes	Discovery Questions
MV2/MV6 TRXE, TRXHX	**View the entire threat story across environments**	• Detect and remediate faster and cheaper with faster responses, leveraged investments, orchestration and automation. • Trellix XDR goes beyond the endpoint for detection and response. This is helpful with more advanced threats that leverage a multi-vector approach	• Streamline existing endpoint tools • Improved understanding of security posture as higher-level SOC maturity better reduces risk thanks to the SOC gaining comprehensive visibility and control across vectors • Automated correlation and prioritized alerts across all vectors; allowing analysts to focus on what matters • Centralized access to critical controls telemetry and data improves efficiency and reduces risk	• Are your current capabilities covering your attack surfaces? • What detection and prioritization methods would you like to add? • How would better visibility impact your security operations? • How is your team dealing with the daily number of alerts? • What resources do you need to mitigate attacks?

Benefits for Sales

- EDR is the #1 path to XDR, as 70% of XDR customers will buy XDR through their EDR vendor.
- Increases retention, stickiness
- Continue to engage in and deepen strategic customer conversations as trusted their security advisor
- Cross-sell opportunities: paths to XDR, Network, Email

Cautions

- **Remember that Helix Connect does not replace their EPP/EDR and that customers should retain their EPP product to maximize the value of the integration.**

What are your key takeaways from the session?

Trellix