The AI-Driven & Automation SecOps Transformation Platform

Tiến Nguyễn CISSP, CISM
Solutions Consultant at Palo Alto Networks

Now

SOC Mission

Defend our information and technology resources, intellectual property and ability to operate by disrupting our adversary's ability to conduct their operations and achieve their desired outcomes.

SOC SERVICES

THREAT MONITORING — THREAT HUNTING — INCIDENT RESPONSE

ROUGH SCOPE

19k USERS

400k SERVERS & VMs

19K LAPTOPS/DESKTOPS

ENDPOINTS

11 DATA CENTERS trending ▼

SECURITY SERVICES CONSUMED BY **85k+** CUSTOMERS

Human-Centered SOCs Can’t Stop AI-Fueled Threats

300%

Increase in attacks in 2025

25 min

Median time to exfiltrate data using AI

2-3 days

Median time to resolve (MTTR)

Sources: Unit 42 Global Incident Response Report, 2. 2025 Global Incident Response Report, Palo Alto Networks 3. XSIAM customer interviews and product telemetry

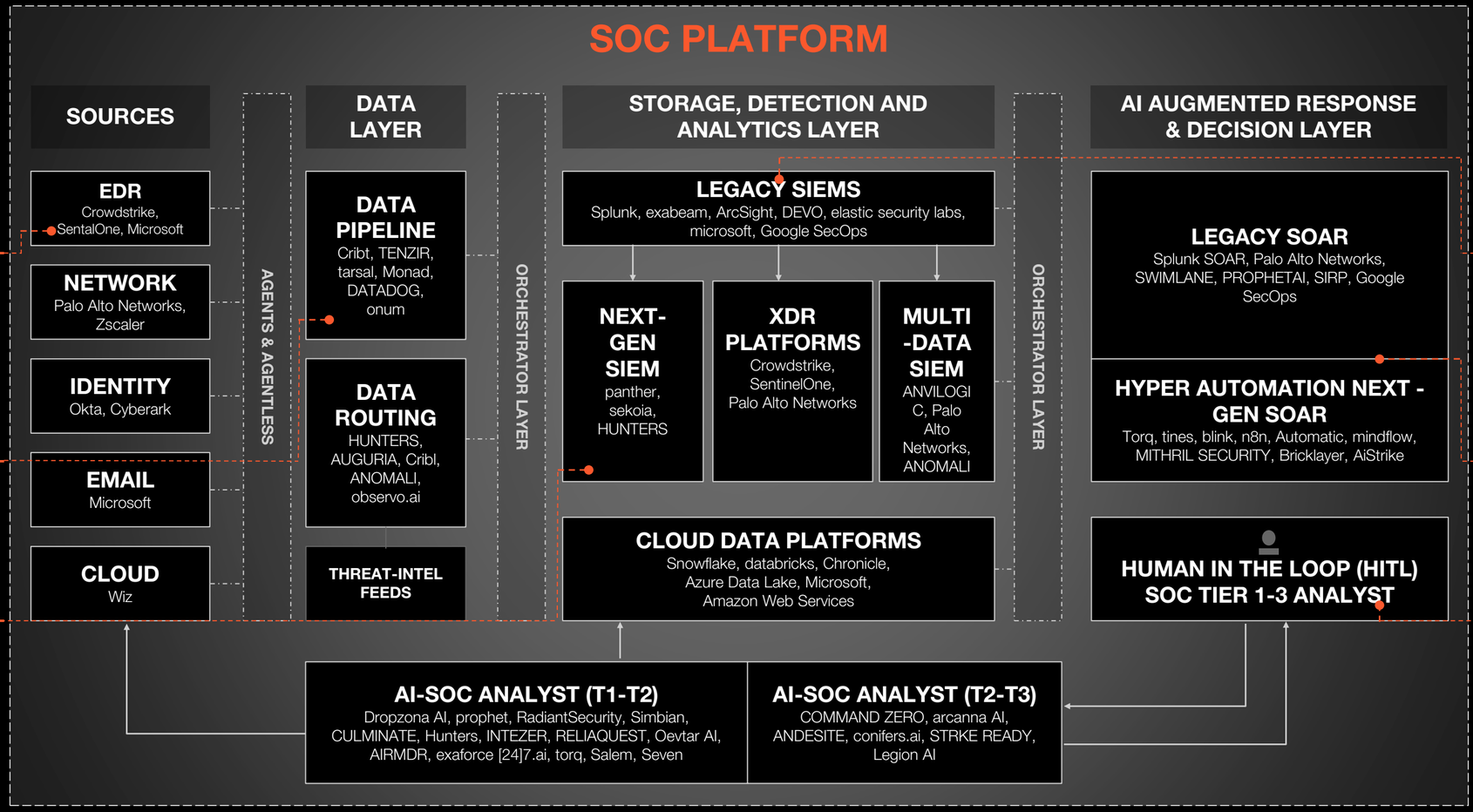
How Can The “Modern” SOC Possibly Work?

What one blog proposed as the “Modern” SOC…

Separate tools for detection

Separate data repositories

Manual, static correlation rules



Siloed Analytics

Separate, labor-intensive automation

No clear next steps

paloalto NETWORKS | CORTEX

Three primary challenges that SOCs face today

Siloed Tools and Data

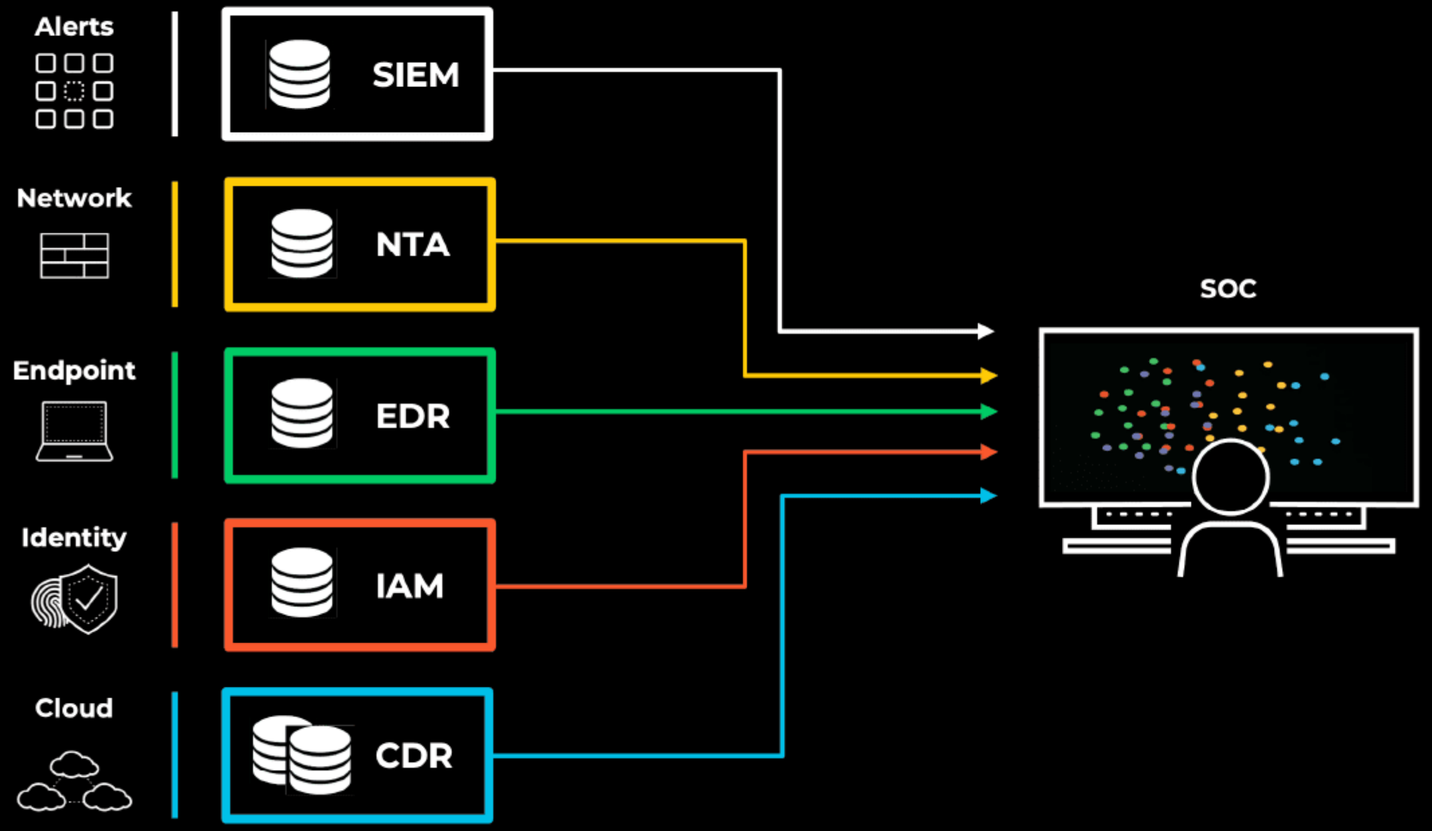
Too many data silos make it difficult to detect attacks

Inability to Stop Threats at Scale

Teams build and maintain detection content and use multiple tools to manually investigate and respond.

Heavy Reliance on Manual Work

Result: Low efficiency and performance



~11K
Alerts per day

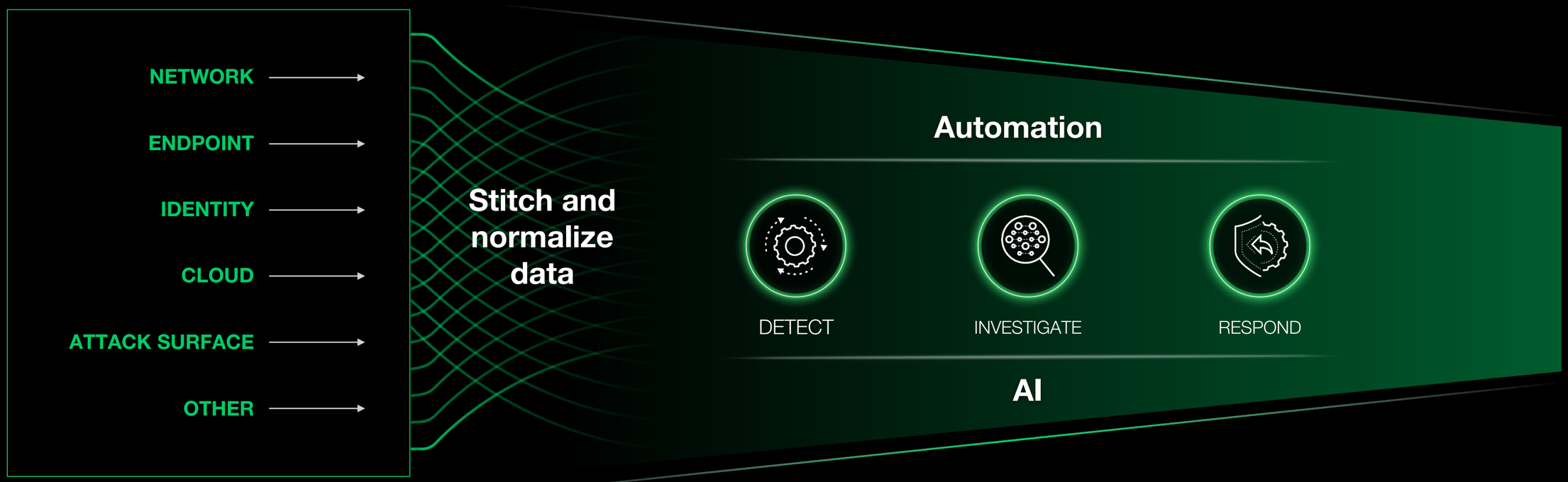
4+
Days to investigate

< 30%
of SOC teams meet KPI goals

212
Days of dwell time

The Solution: Rethink and Transform Security Operations

What’s Needed: One Platform Powered by AI & Automation

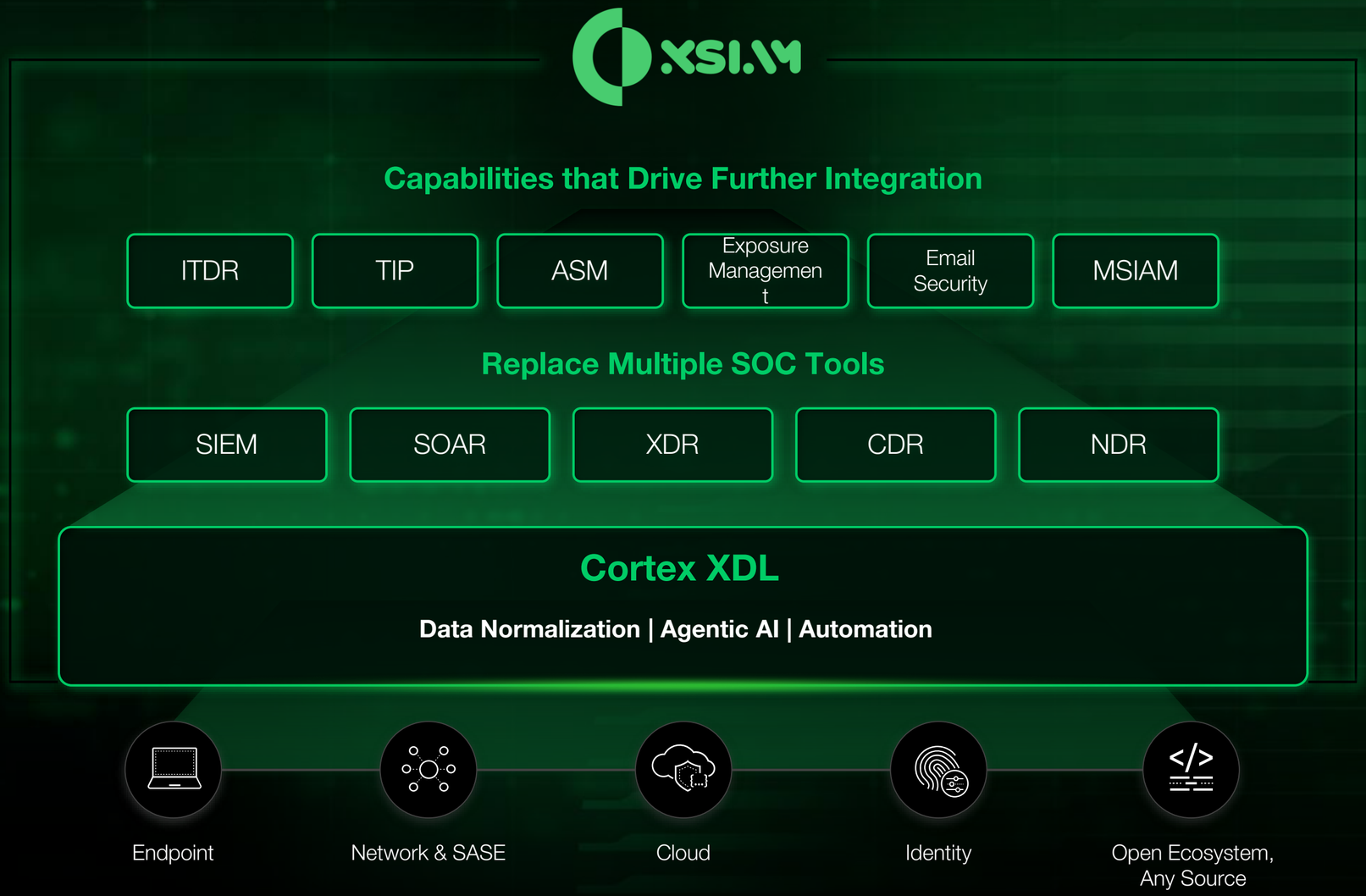


Massive data, with automated stitching and grouping

Automated detection and AI-guided investigation and response

Empowered analysts become more proactive

Cortex XSIAM: AI-Driven Security Operations



Unified SecOps
One platform. One user experience

AI-powered protection
Best-in-class 100% detection in MITRE

Industry-leading automation
1,000+ automation playbooks

AI-driven response
Up to 98% faster MTTR

paloalto NETWORKS | CORTEX

Delivering Unprecedented Results for the Largest Organizations Worldwide

Days → ~1 hour → Under 10 minutes

Drastically Reduced MTTR

Global logistics leader with ~300K employees

7→1

reduction in point products

Leading North American energy company

75%

reduction in incident volume

Leading home and business security company

92%

of alerts resolved automatically

Sources: Palo Alto Networks case studies

One Platform for Proactive & Reactive Security

paloalto NETWORKS | CORTEX

Data: Unified Tools & Data to Power AI and Automation

XSIAM

Data | AI | Automation

Any Data Source

- Endpoint
- Network
- Cloud
- Identity
- Email
- Other (kafka, Microsoft 365, Google Workspace, tenable, infoblox, proofpoint, zscaler, CYBERARK, CLOUDFLARE, slack, CISCO, salesforce, Dropbox)

Ingest raw data

Normalize data for AI

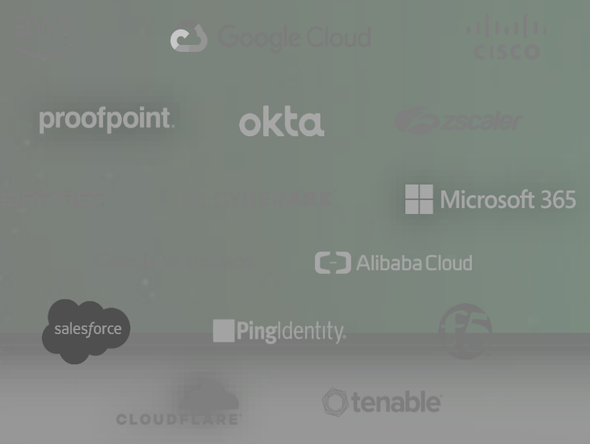
Enrich data with threat intelligence

Single, complete source of AI-ready data

Simplified new data source onboarding

Data onboarding | Ingest ANY data source

100s of 3rd-party OOTB integrations



...and many more

AUTOMATICALLY MAPPED

All other data

…with generic data onboarding

Palo Alto Networks products and services

Cortex®

Strata®

Prisma®

Unit 42®

...and many more

AUTOMATICALLY MAPPED

UNIFIED DATA MODEL FOR ANALYTICS

paloalto NETWORKS | CORTEX®

AI: AI-Powered Defense to Stop Threats in Minutes

XSIAM

Data | AI | Automation

Single, complete source of AI-ready data

Simplified new data source onboarding

10K Detectors
and over
2.6K+ ML models
continuously advancing

- Real-time prevention
- Precise causality and detection
- Full context of threats

100% Detection and industry-low false positives
in MITRE ATT&CK Round 6

paloalto NETWORKS | CORTEX

Automation: Automated Operations to Accelerate SOC Workflows

XSIAM

Data AI Automation

Alerts triggered and grouped; incident created → Impact assessed and contained → Incident remediated

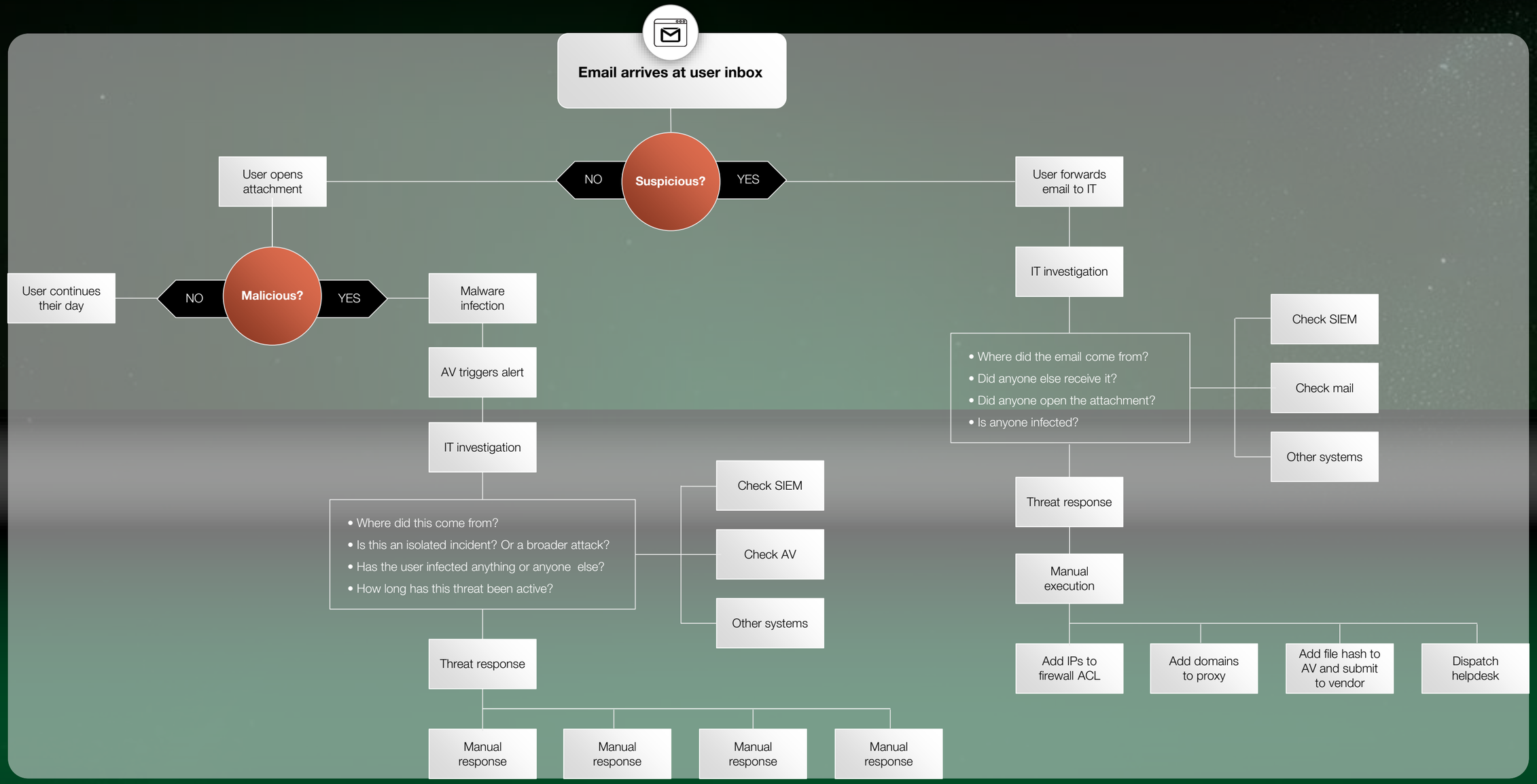
THOUSANDS OF INTEGRATIONS AND ACTIONS

75%
Fewer incidents requiring investigation*

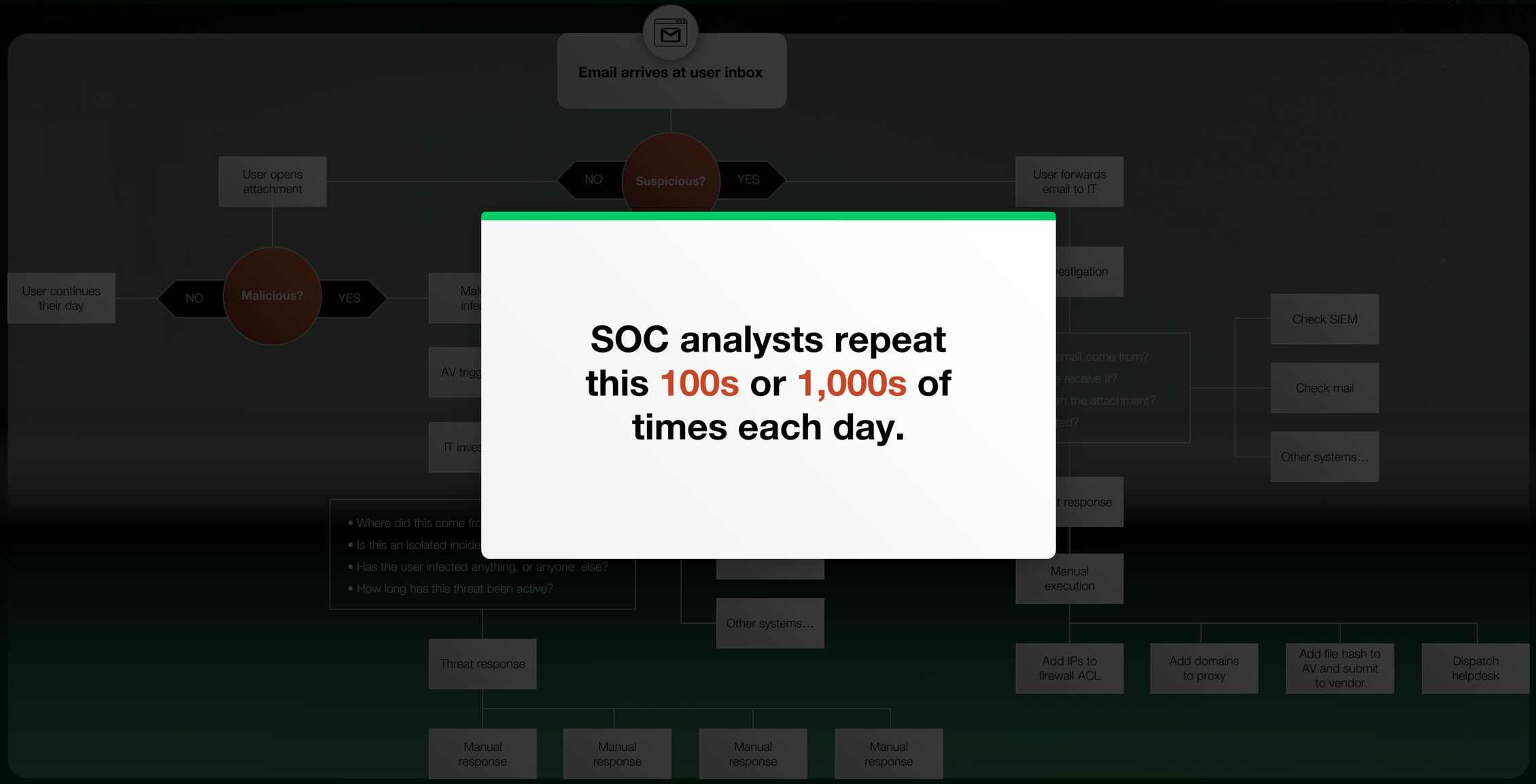
98%
Reduction in MTTR**

*Oil and Gas company case study **Boyne Resorts case study

The SOC without automation

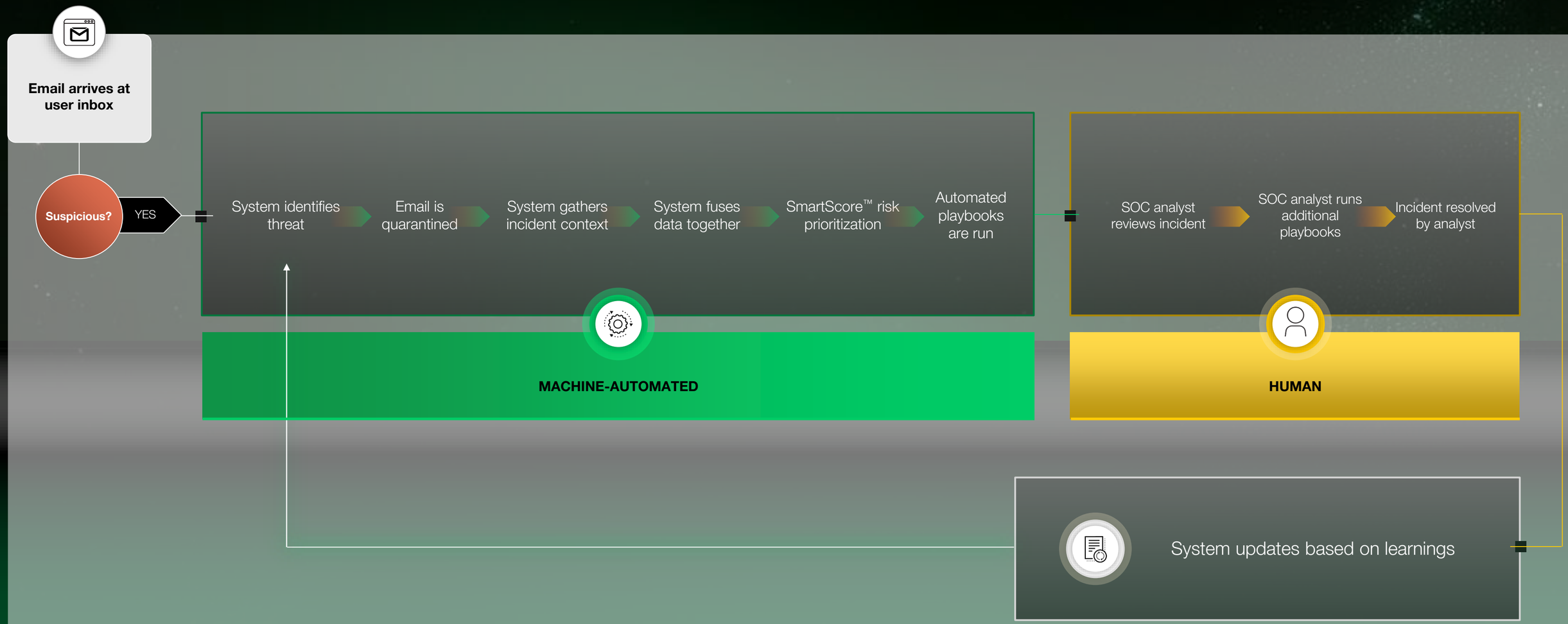


The SOC without automation



SOC analysts repeat this 100s or 1,000s of times each day.

What if automation can take on the heavy lifting for SOC teams?



paloalto NETWORKS | CORTEX

Two categories of automation in XSIAM

Alert enrichment to improve accuracy

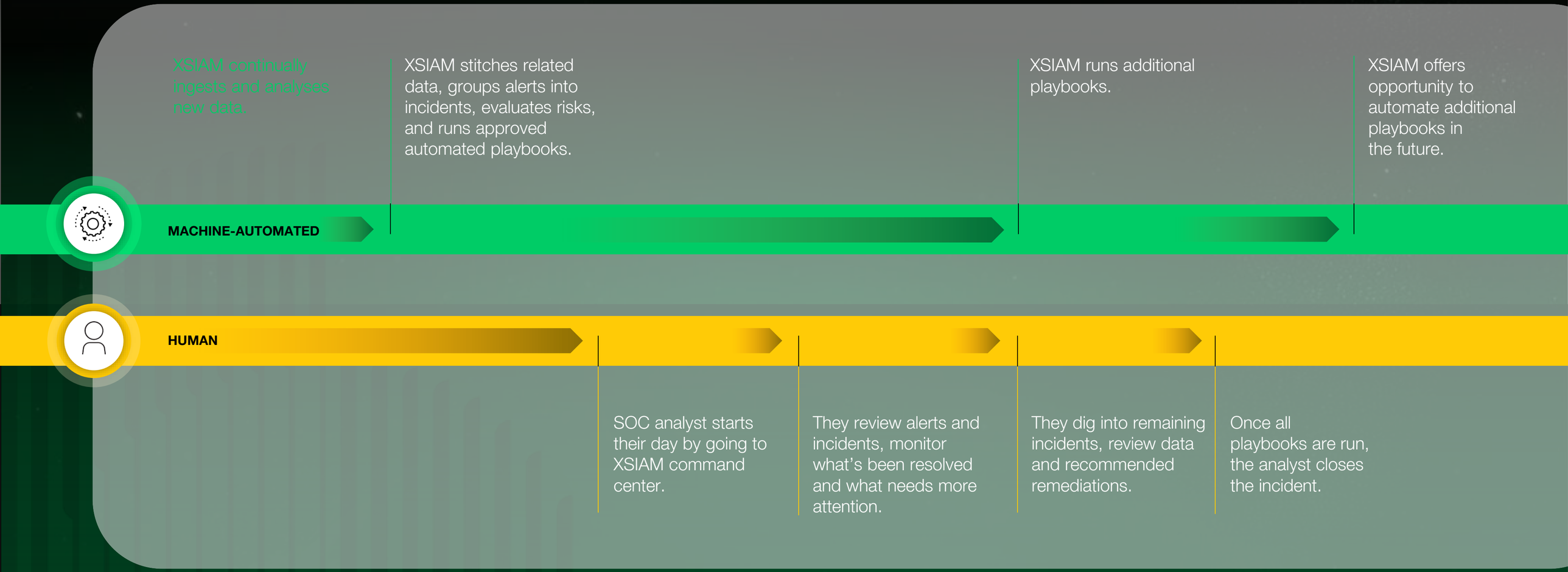
- Data stitching
- Auto analysis
- Alert grouping
- SmartScore™

+

Repetitive analyst tasks

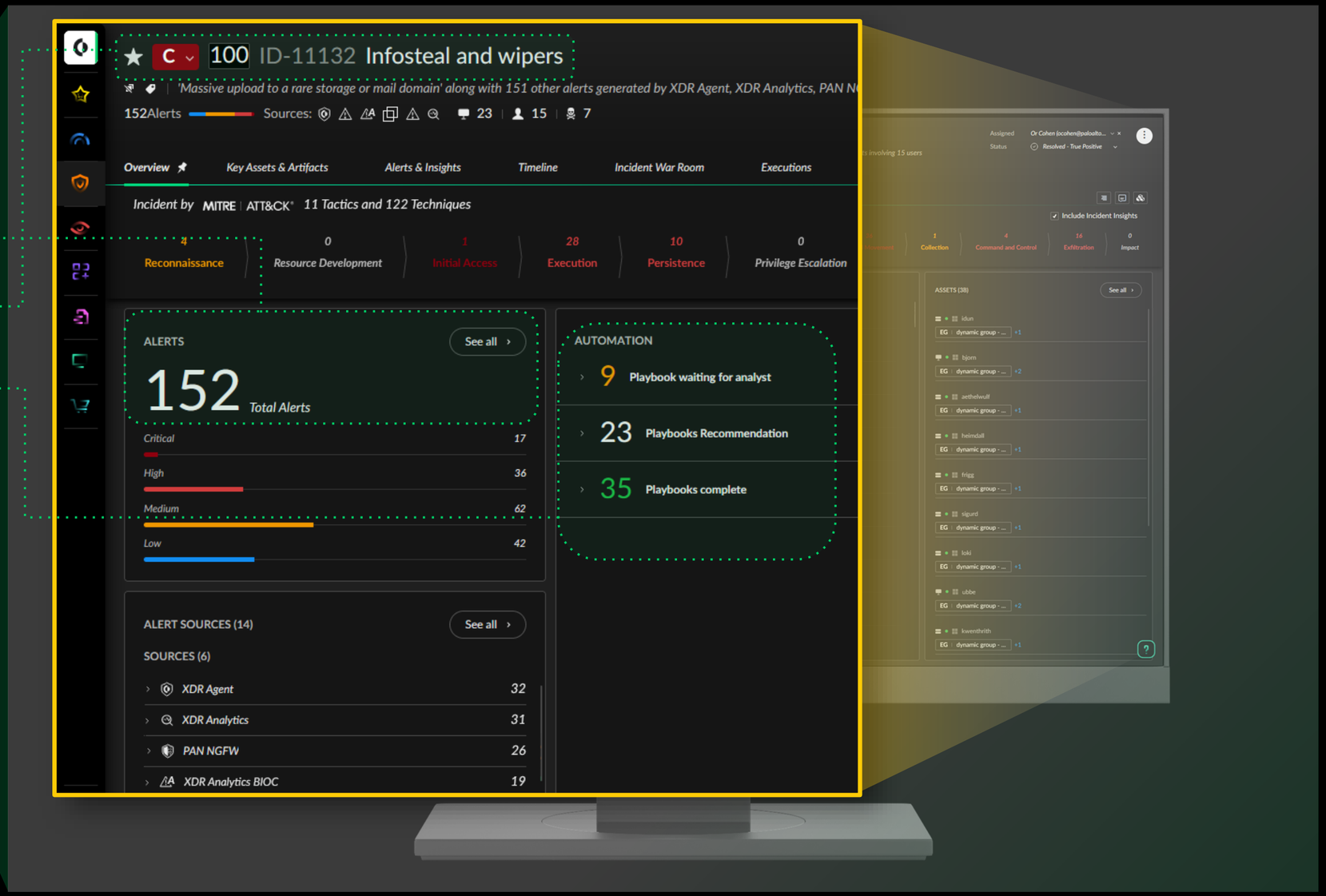
- Runbook automation
- Suggested playbooks
- Marketplace for integrations

Machine + human automation in XSIAM



Simplifying The Complexity of Responding To An Attack

- SmartGrouping elevates 150+ alerts from 14 sources
- Created one critical priority incident
- Automatically:
  - Presented 9 response automations to resolve the incident
  - Recommended 23 playbooks for increased automation in the future
  - Ran 35 actions to prepare for response



Stitching Data from All Major Sources with Dedicated Data Models

ENDPOINT

14+

Cortex XDR · CROWDSTRIKE · Microsoft · SentinelOne · cisco · Carbon Black.

CLOUD

26+

Cortex XDR · Azure · WIZ · Microsoft 365 · Google Cloud · Google Workspace · LACEWORK

NETWORK

23+

paloalto NETWORKS · CHECK POINT · cisco · FORTINET · zscaler · netskope · Trellix

MSSP

IBM · Deloitte. · orange™ · Bell

and more…

IDENTITY

6+

okta · CYBERARK · Microsoft · DUO · onelogin

OTHER

35+

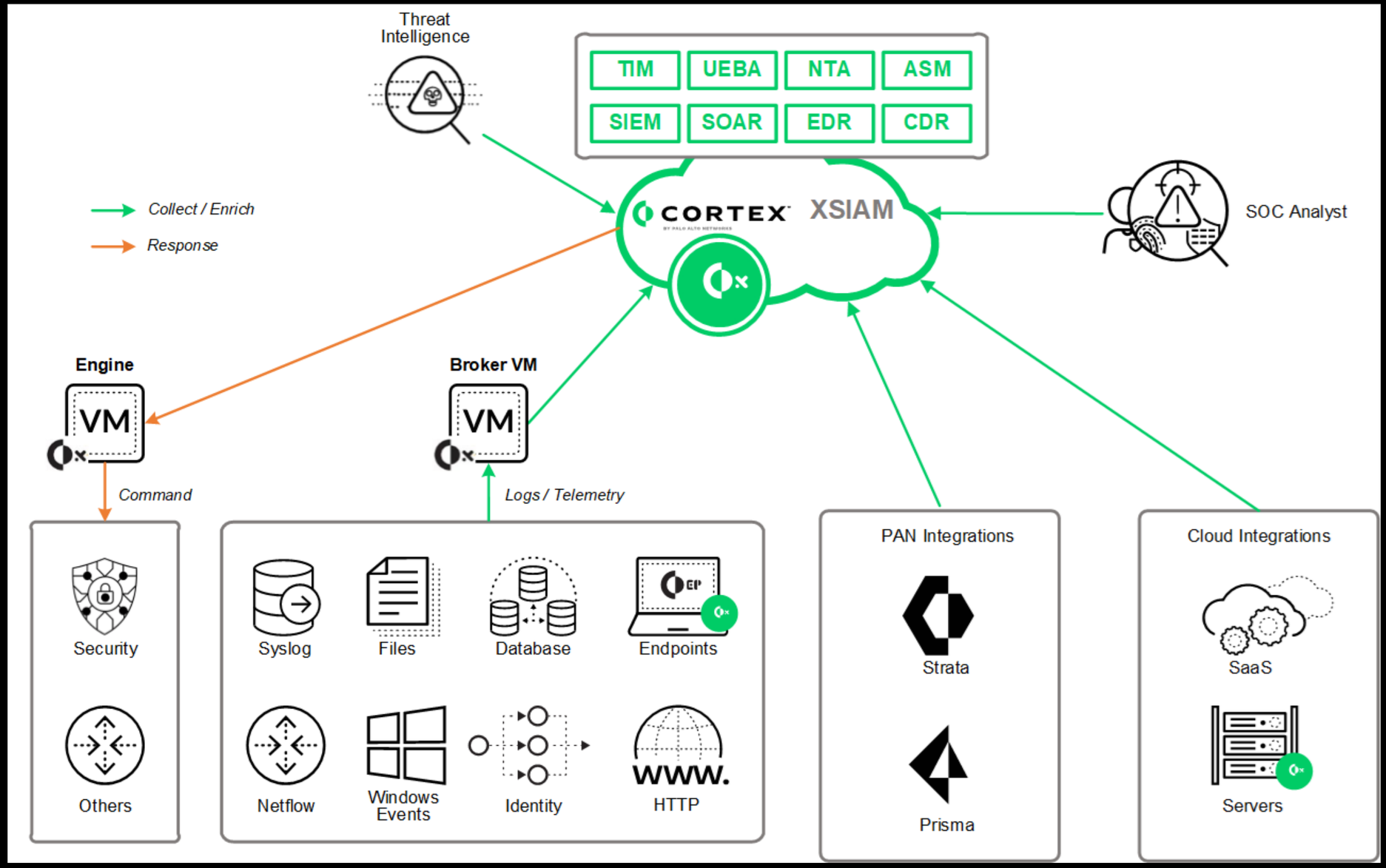
box · Dropbox · Forcepoint · proofpoint · salesforce · workday · servicenow

Syslog Collector · Apache Kafka Collector · CSV Collector · Netflow Collector

Database Collector · FTP Collector · Files and Folders Collector · SNMP Collector

Architecture

Cortex XSIAM High Level Architecture



Demo

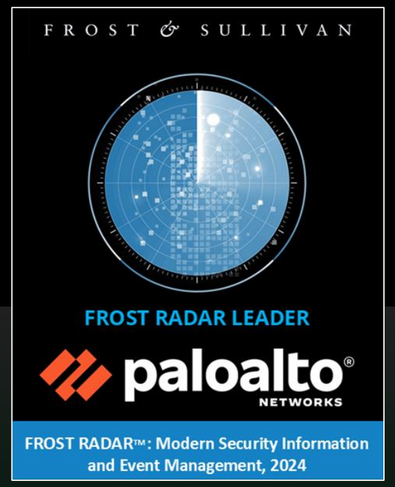
XSIAM Demo

Thank You

paloaltonetworks.com

Recognized As A Leader By Industry Analysts

LEADER: GigaOm Radar for the 2nd year in a row



LEADER: Frost and Sullivan Modern SIEM

LEADER: Omdia Universe: Next-Gen SIEM

100% DETECTION: MITRE ATT&CK Evaluations: Enterprise

4.5 STARS OVERALL for Cortex XSIAM

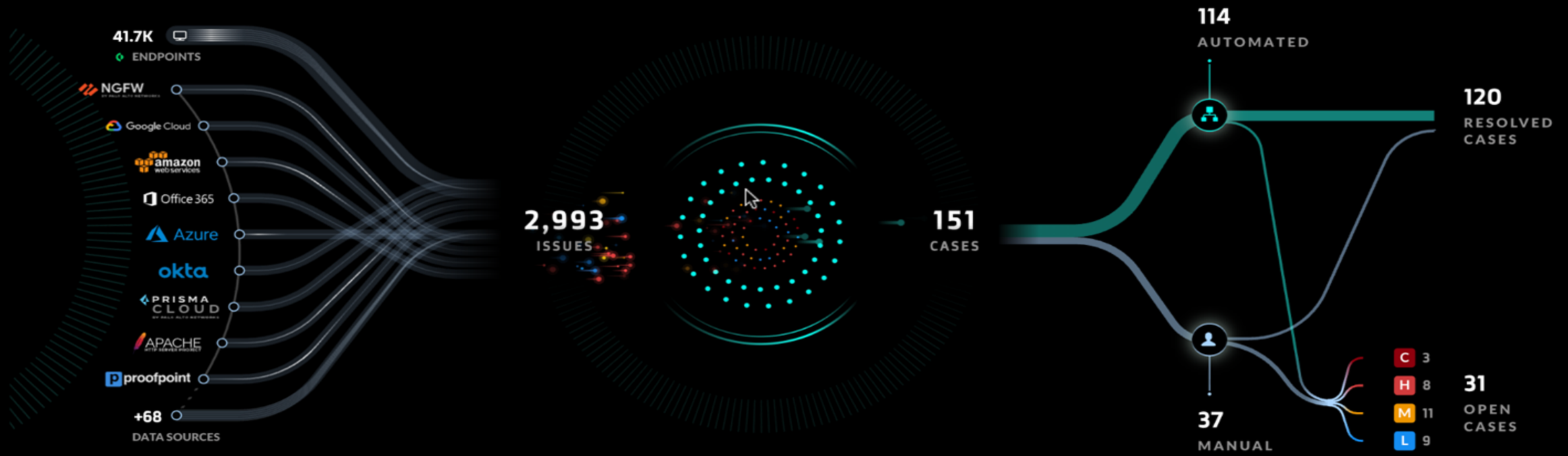
APPENDIX

Managed by Unit42 Managed Services

XSIAM Command Center

Last 24H

Good Morning, Tien



Events Ingestion

43 B/24H

Data Ingestion

65 TB/24H

Total Open Cases

31

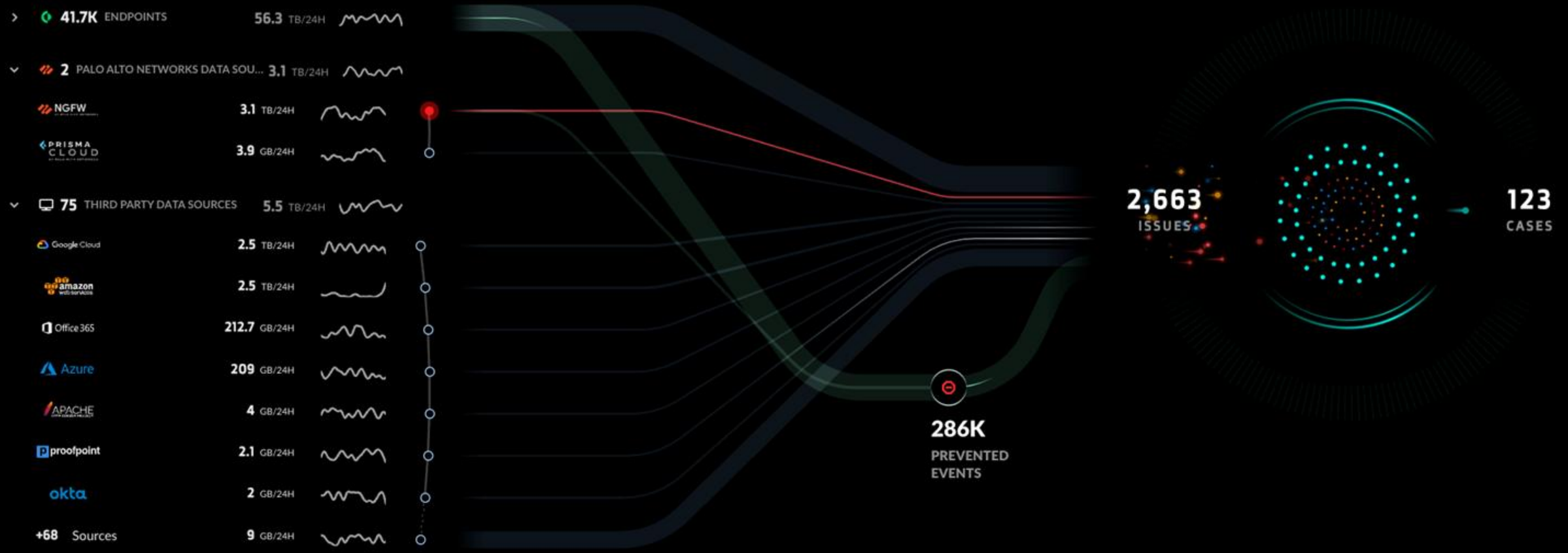
C 3 H 8 M 11 L 9

286.1K

PREVENTED EVENTS

TN

Data Inventory



View Data Ingestion

Events Ingestion

43 B/24H

Data Ingestion

65 TB/24H

1

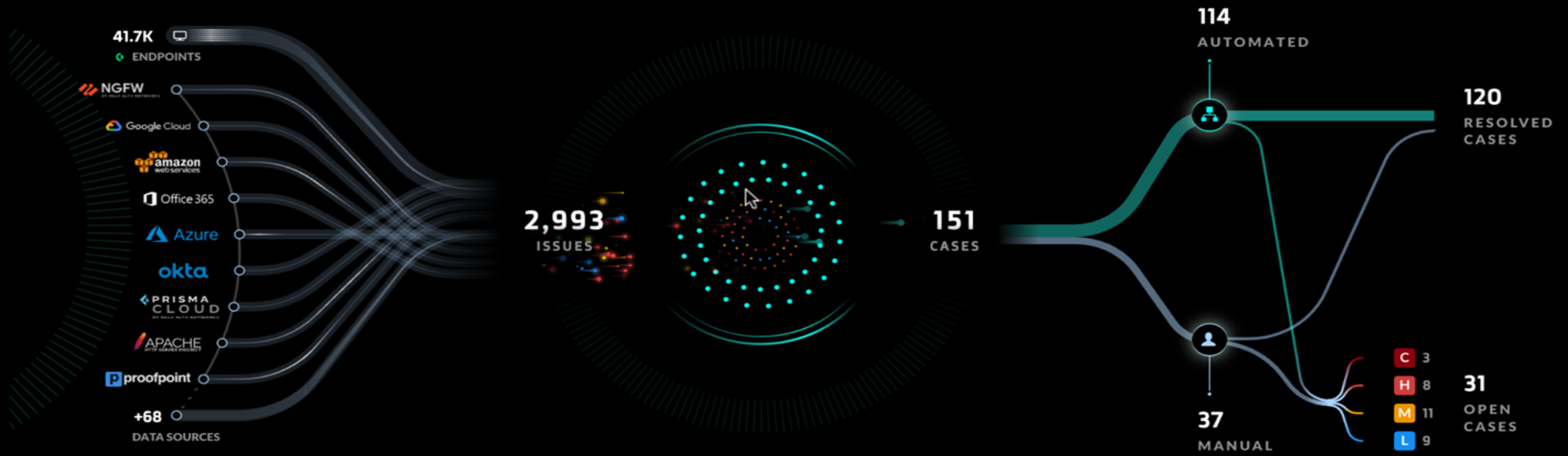
COLLECTION ERROR

Managed by Unit42 Managed Services

XSIAM Command Center

Last 24H

Good Morning, Tien



Events Ingestion

43 B/24H

Data Ingestion

65 TB/24H

Total Open Cases

31

C 3 H 8 M 11 L 9

286.1K

PREVENTED EVENTS

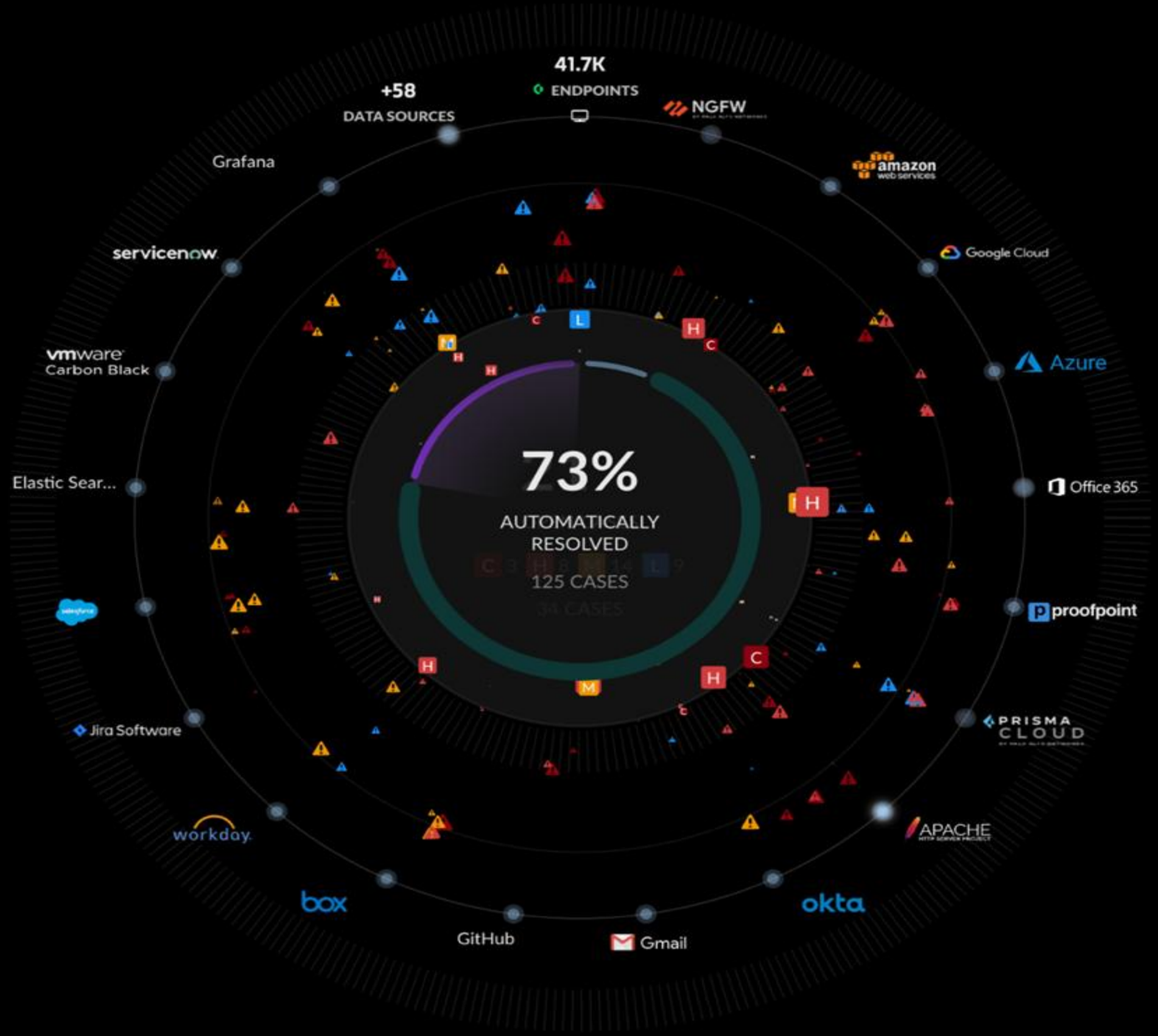
TN

Managed by Unit42 Managed Services

XSIAM Command Center

Last 24H

Dynamic View



Data Ingestion

65 TB/24H

Total Open Cases

34

C 3 H 8 M 14 L 9

LIVE FEED

- New playbook suggestion | ID-...
- L Case created | ID-977
- C Case reopened | ID-981
- C 6 Issues added | to 2 Cases
- L 9 Incidents created
- 12 Playbooks suggestion | for ...
- Case resolved by XSIAM | ID-...
- H Case created | ID-923
- Case resolved by XSIAM | ID-...
- 8 Cases | Resolved by XSIAM
- 8 Cases | Resolved by XSIAM
- Case resolved by Elad C... | ID-...
- H Case reopened | ID-953
- 19 Playbooks suggestion | for ...
- Case resolved by Elad C... | ID-...

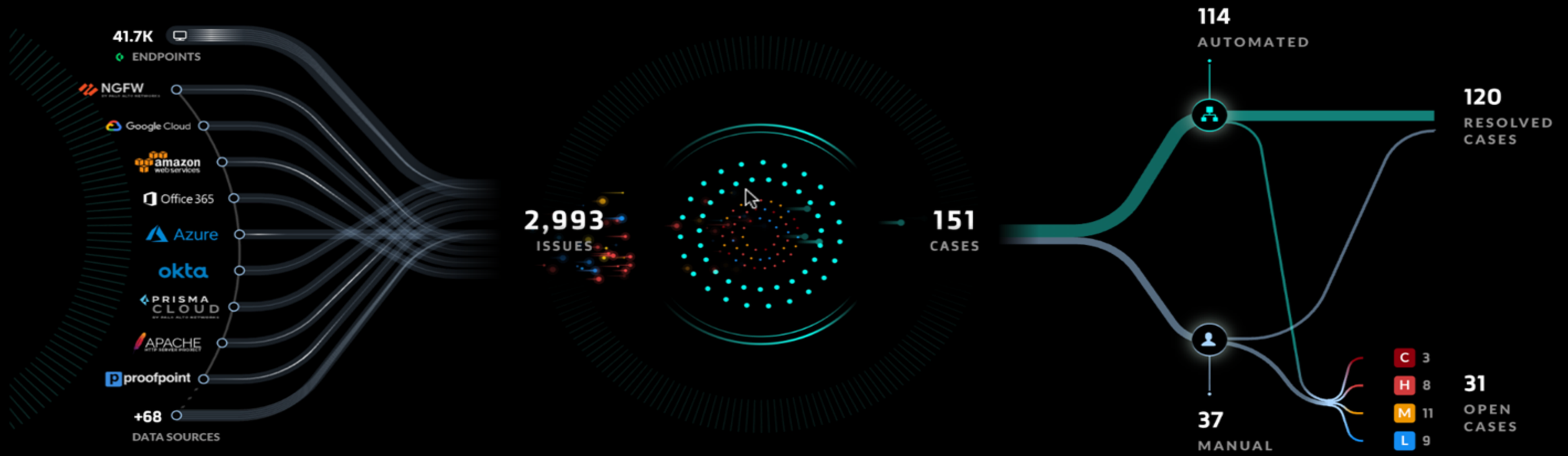
TN

Managed by Unit42 Managed Services

XSIAM Command Center

Last 24H

Good Morning, Tien



Events Ingestion

43 B/24H

Data Ingestion

65 TB/24H

Total Open Cases

31

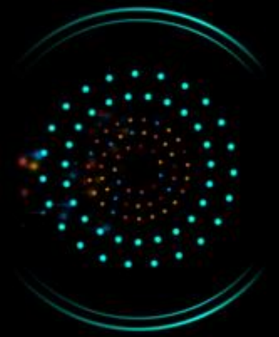
C 3 H 8 M 11 L 9

286.1K

PREVENTED EVENTS

TN

Cases Overview



3,096
ISSUES

182
CASES

139
AUTOMATED

43
MANUAL

30 Can be automated
By 15 recommendations

145
RESOLVED CASES

37
OPEN CASES

- C 3
- H 8
- M 12
- L 14

Resolved Cases by Assignee

Jaydon Bator	26
Lindsey Culhane	21
Makenna Stanton	13

MITRE | ATT&CK®

3	Reconnaissance
1	Resource Development
11	Initial Access
1	Execution
2	Persistence
1	Privilege Escalation
0	Defense Evasion
0	Credential Access
2	Discovery
4	Lateral Movement
2	Collection
2	Command and Control
2	Exfiltration
4	Impact

Data Ingestion

65 TB/24H

Managed by Unit42 Managed Services

H 94 Security ID-9470 Project Sliver - APT Attack Detected

'Local Analysis Malware' along with 18 other issues detected on 6 hosts involving 4 users

19 Issues | Sources: 1

Assigned: Muktadir Wali (mwali@palo...)
Status: New
Open for 2 years

Overview | Key Assets & Artifacts | Issues & Insights | Timeline | Case War Room | Executions

View MDR Thread | Include Case Insights

Case by MITRE | ATT&CK® 7 Tactics and 8 Techniques

0	1	0	2	0	0	2	4	1	0	1	0	2	0
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact

ISSUES

See all

19 Total Issues

High	5
Medium	11
Low	3

ISSUE SOURCES (11)

See all

DETECTION METHODS (5)

Correlation	5
PAN NGFW	4
XDR Agent	4
XDR Analytics BIOC	3
XDR Analytics	3

DATA SOURCES (6)

PANW/XDR Agent	10
PANW/NGFW	7
Okta/Sso	2
msft/O365 Sharepoint Online	1
msft/Azure AD	1
microsoft/mssql_audit_offest	1

AUTOMATION

4 Playbooks complete

- H 56539353 - WildFire Malware
- H 56538850 - Local Analysis Malware
- H 56539393 - Malicious Network Operation - 219029901
- M 56539808 - [AUTH] - Failed login from unusual location

View in Issues & Insights tab

ARTIFACTS (26)

See all

runner.exe (1787...aaea)
WF Malware | VT Unknown

msedge.exe (8cb3...5544)
WF Benign | VT 0/72

OneDrive.exe (a02b...092d)
WF Benign | VT 0/72

msedge.exe (92fa...0bb9)
WF Benign | VT 0/74

rundll32.exe (d64d...8c9e)
WF Benign | VT 0/72

cmd.exe (8258...1bdf)
WF Benign | VT 0/71

deployer.exe (edfa...25ef)
WF Benign | VT 3/72

svchost.exe (dab2...d021)
WF Benign | VT 0/72

WMIC.exe (3640...8458)
WF Benign | VT 0/72

diagnostics.exe (82b2...aa4e)
WF Benign LC | VT Unknown

conhost.exe (b5d9...dbf0)
WF Benign | VT 0/72

ASSETS (9)

See all

client-02
EG | Democloud wind... +1

dc01
EG | windows servers +3

client-01
EG | Democloud wind... +2

dc02
EG | windows servers +2

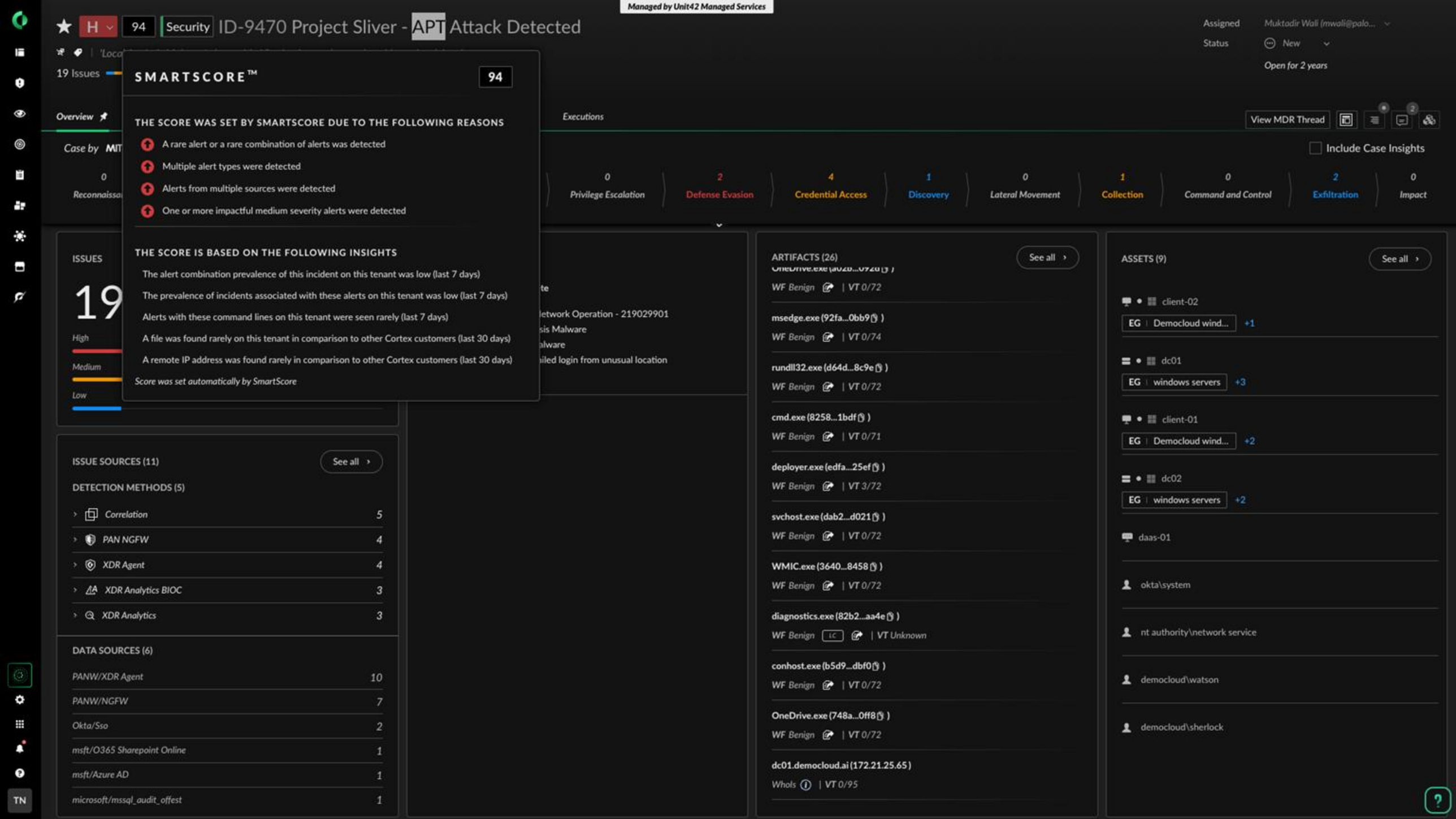
daas-01

okta\system

nt authority\network service

democloud\watson

democloud\sherlock


Managed by Unit42 Managed Services
H
94
Security
ID-9470 Project Sliver - APT Attack Detected
19 Issues
Assigned
Muktadir Wali (mwali@palo...
Status
New
Open for 2 years
SMARTSCORE™
94
THE SCORE WAS SET BY SMARTSCORE DUE TO THE FOLLOWING REASONS
A rare alert or a rare combination of alerts was detected
Multiple alert types were detected
Alerts from multiple sources were detected
One or more impactful medium severity alerts were detected
THE SCORE IS BASED ON THE FOLLOWING INSIGHTS
The alert combination prevalence of this incident on this tenant was low (last 7 days)
The prevalence of incidents associated with these alerts on this tenant was low (last 7 days)
Alerts with these command lines on this tenant were seen rarely (last 7 days)
A file was found rarely on this tenant in comparison to other Cortex customers (last 30 days)
A remote IP address was found rarely in comparison to other Cortex customers (last 30 days)
Score was set automatically by SmartScore
Overview
Executions
View MDR Thread
Include Case Insights
0 Reconnaissa
0 Privilege Escalation
2 Defense Evasion
4 Credential Access
1 Discovery
0 Lateral Movement
1 Collection
0 Command and Control
2 Exfiltration
0 Impact
ISSUES
19
High
Medium
Low
ISSUE SOURCES (11)
See all
DETECTION METHODS (5)
Correlation 5
PAN NGFW 4
XDR Agent 4
XDR Analytics BIOC 3
XDR Analytics 3
DATA SOURCES (6)
PANW/XDR Agent 10
PANW/NGFW 7
Okta/Sso 2
msft/O365 Sharepoint Online 1
msft/Azure AD 1
microsoft/mssql_audit_offest 1
letwork Operation - 219029901
sis Malware
alware
iled login from unusual location
ARTIFACTS (26)
See all
WF Benign | VT 0/72
msedge.exe (92fa...0bb9)
WF Benign | VT 0/74
rundll32.exe (d64d...8c9e)
WF Benign | VT 0/72
cmd.exe (8258...1bdf)
WF Benign | VT 0/71
deployer.exe (edfa...25ef)
WF Benign | VT 3/72
svchost.exe (dab2...d021)
WF Benign | VT 0/72
WMIC.exe (3640...8458)
WF Benign | VT 0/72
diagnostics.exe (82b2...aa4e)
WF Benign LC | VT Unknown
conhost.exe (b5d9...dbf0)
WF Benign | VT 0/72
OneDrive.exe (748a...0ff8)
WF Benign | VT 0/72
dc01.democloud.ai (172.21.25.65)
Whois | VT 0/95
ASSETS (9)
See all
client-02
EG | Democloud wind... +1
dc01
EG | windows servers +3
client-01
EG | Democloud wind... +2
dc02
EG | windows servers +2
daas-01
okta\system
nt authority\network service
democloud\watson
democloud\sherlock
TN

H | #56539393 | Malware | Open for 707 days | XDR Agent

Malicious Network Operation - 219029901

Overview | War Room | Work Plan

Automation: T1059 - Command and Scr...

MITRE | ATT&CK

TA0042 Resource Development

T1059.001 Command and Scripting Interpreter: PowerShell

Affected Assets

democloud\watson

client-02

Linked Cases

94 H Project Sliver - APT Attack Detected

Evidence

Malicious Network Operation - 219029901