cisco Engage

GO BEYOND
Cisco Engage GBA

Shaping the Future of Security Operations (SecOps) with AI

Nelson So, Senior Solutions Engineer
Ricky Mok, Solution Engineer, APJC TDIR Incubation

Is my SOC's TDIR lifecycle: Threat Detection, Investigation and Response cost-efficient?

IDC

InfoBrief, sponsored by Splunk | November 2024

The SIEM of Tomorrow

How SIEMs Are Evolving to Power the Modern SOC

Michelle Abraham
Research Director,
Security and Trust, IDC

Michelle Abraham is the research director in IDC's Security and Trust Group responsible for the Security Information and Event Management (SIEM) & Vulnerability Management practice. Michelle's core research coverage includes SIEM platforms, attack surface management, breach and attack simulation, cybersecurity asset management, and device and application vulnerability management alongside related topics.

Source: Get the IDC InfoBrief: The SIEM of Tomorrow

SOCs Are Dealing with a Lack of Visibility and Too Many Alerts

GO **BEYOND**
Cisco Engage GBA

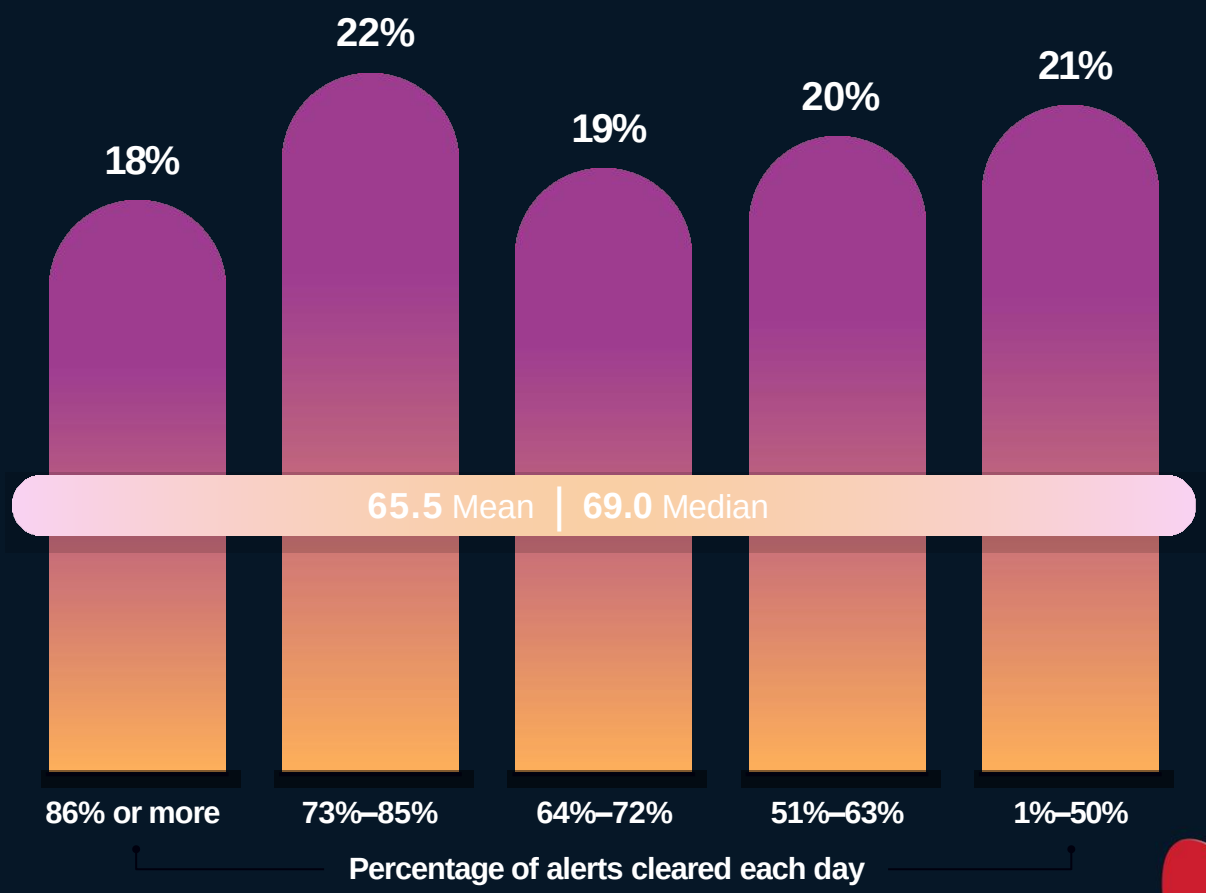
On a daily average,
organizations with a SIEM

clear only **65%** of alerts,

leaving **35%** uninvestigated.

SOC teams find it
impossible to get to all alerts
with the resources they have today.

Percentage of Organizations Clearing Alerts Each Day

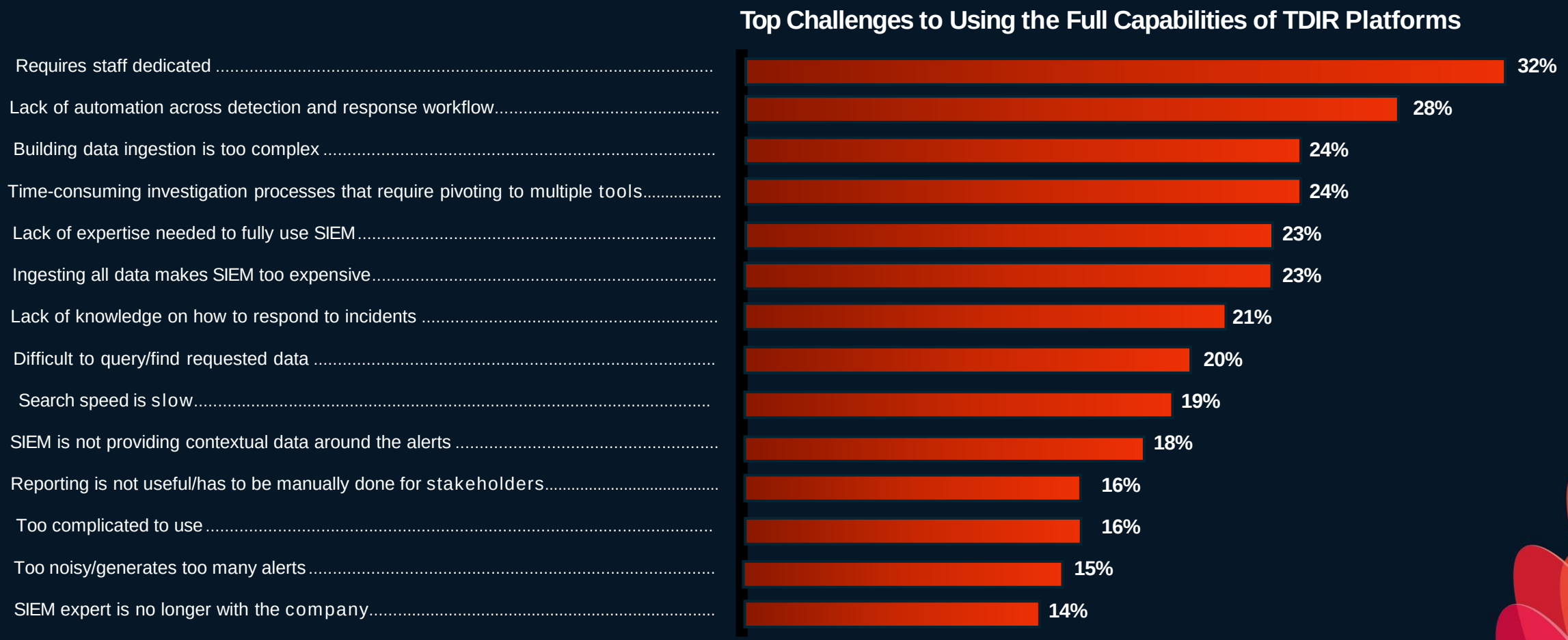


Security Posture for Executives

What are the challenges in the TDIR lifecycle ?

TDIR Are Still Challenging, According to Users and Managers

GO BEYOND
Cisco Engage GBA



What features are required for TDIR?

Today's SOC Teams Prefer These Features

GO **BEYOND**
Cisco Engage GBA

A detection engine that can keep up with the pace of today's threats

Connection to all the data sources
the organization wants to use from the vendor

Deployment flexibility

User and entity behavioral analytics
to find stealthy threats that trend over time

Automation built into the platform,
eliminating the need to swivel into something else

What are the best TDIR options for my SOC?

Cisco's Delivering the SOC of the Future

GO **BEYOND**
Cisco Engage GBA

SIEM

Great at answering complex questions

"Show me all failed login attempts for this 12-hour period, 45 days ago from our U.K. subsidiary"

XDR

Great at notifying you of an incident

"PowerShell created an internal network connection never seen before. This might be ransomware!!!"

SOAR

Great at automating workflows & response actions

"Initiate a password reset for all U.K. employees."

"Quarantine the affected endpoint and take a snapshot of all our data center servers."

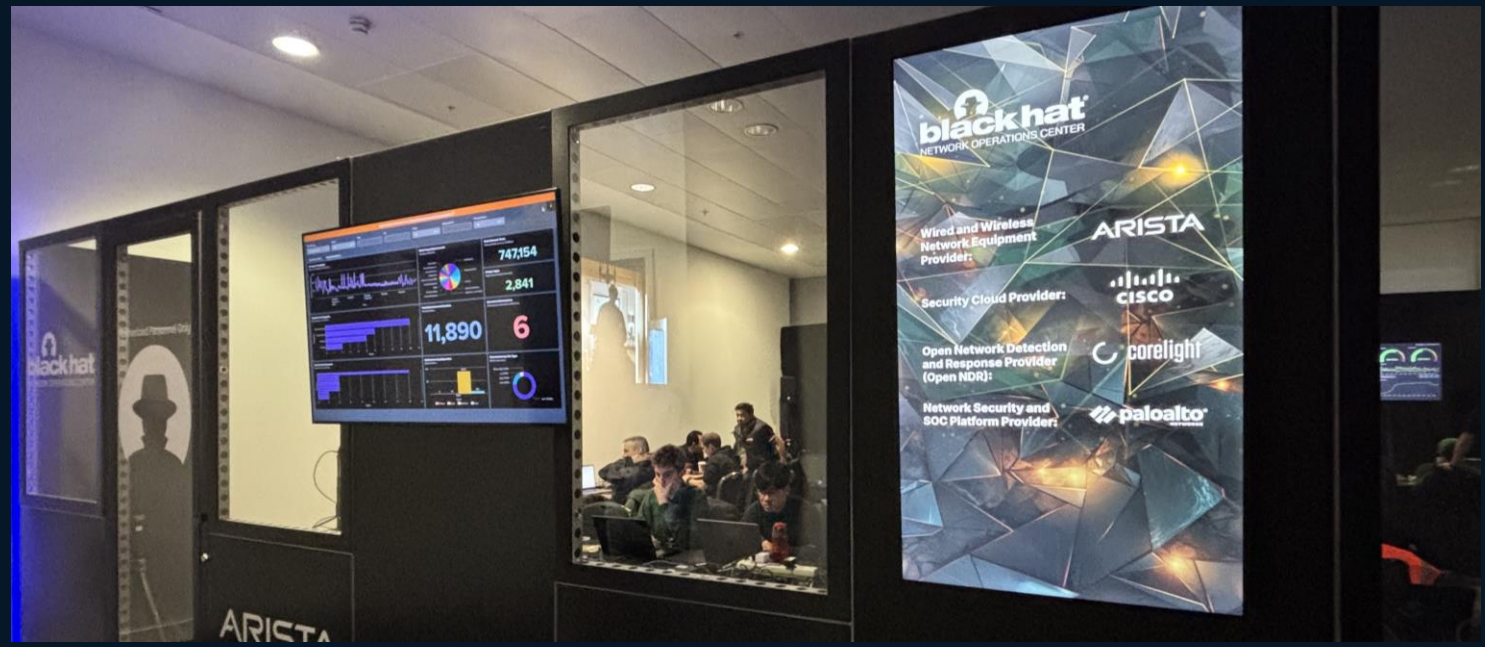
- Identity
- High Fidelity Telemetry
- AI
- Unified Management and Reporting

Is there a showcase to address all the requirements?

Cisco Future SOC Showcases

GO **BEYOND**
Cisco Engage GBA

PARIS 2024



RSAConference2025
San Francisco
Moscone Center | Apr. 28 - May 1, 2025

cisco Live!

NFL

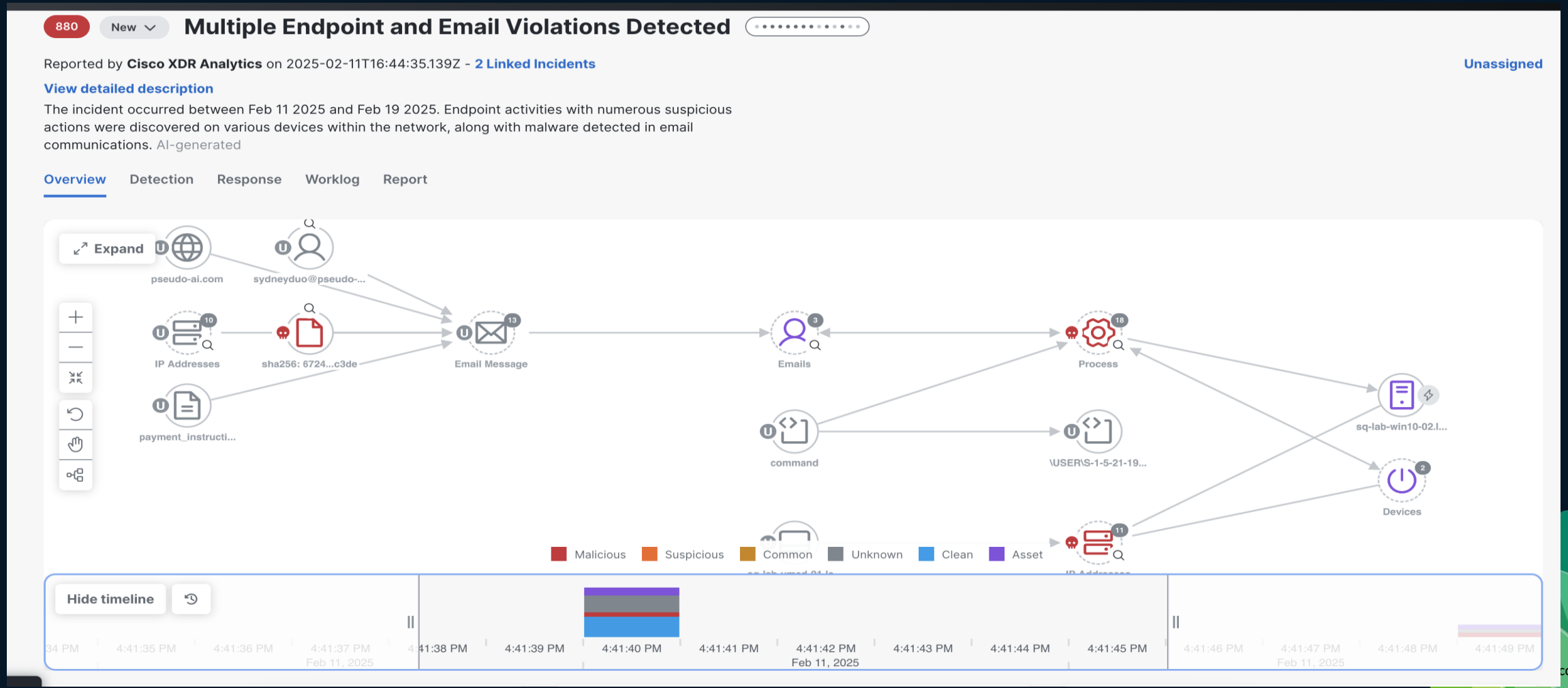
black hat

How can AI assist with TDIR?

AI Assistant for Security

Attack Graph Enhancement

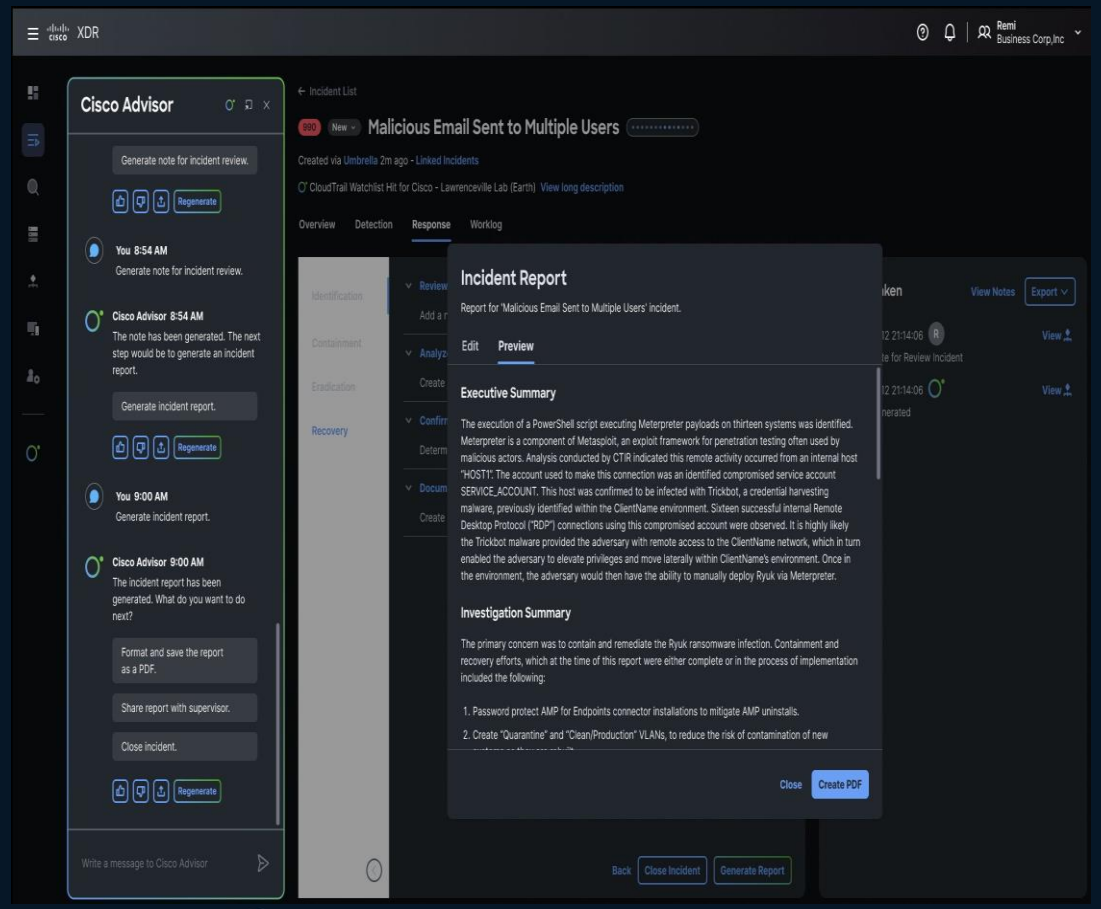
GO **BEYOND**
Cisco Engage GBA



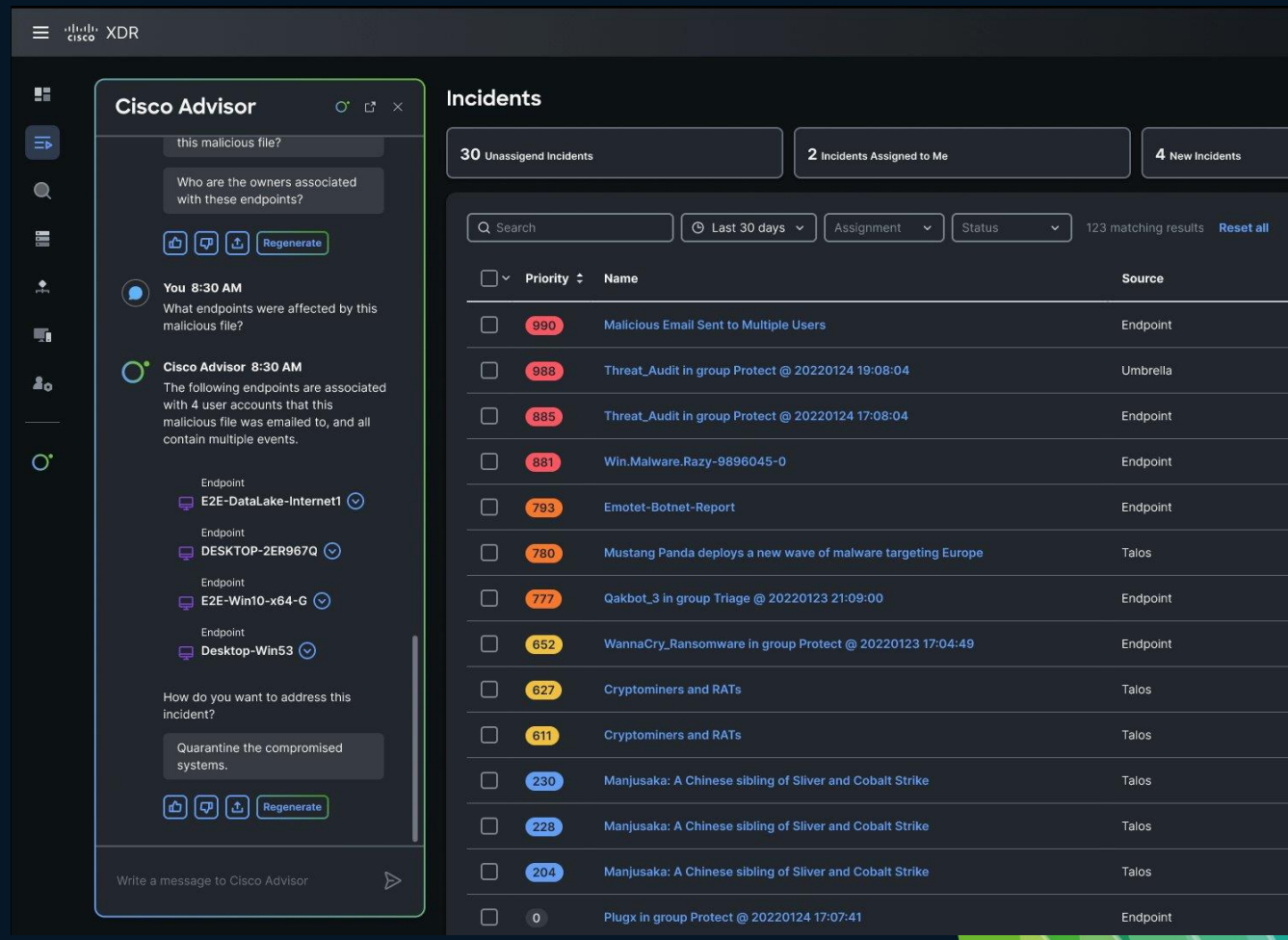
AI Assistant for Security

GO **BEYOND**
Cisco Engage GBA

Incident Report



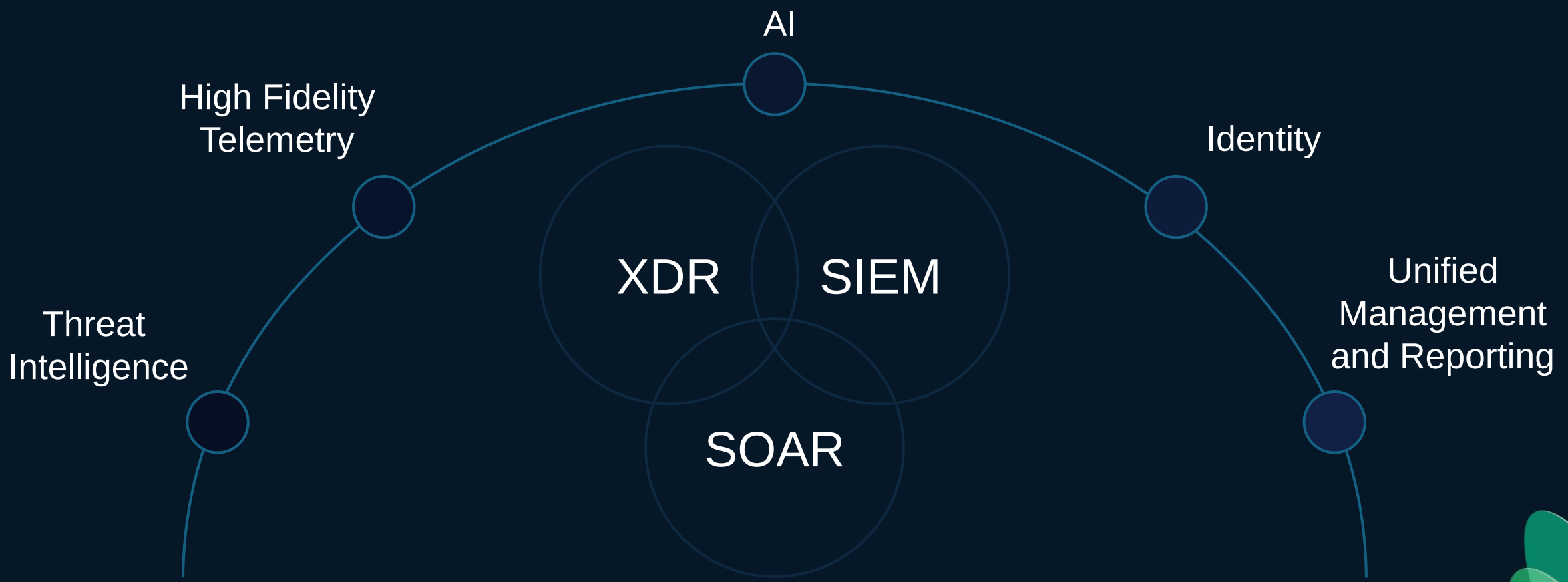
Security Advisory



cisco Engage

Cisco : Delivering SOCs' TDIR Elements

GO BEYOND
Cisco Engage GBA



cisco Engage

GO BEYOND
Cisco Engage GBA

Thank You!