

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?

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

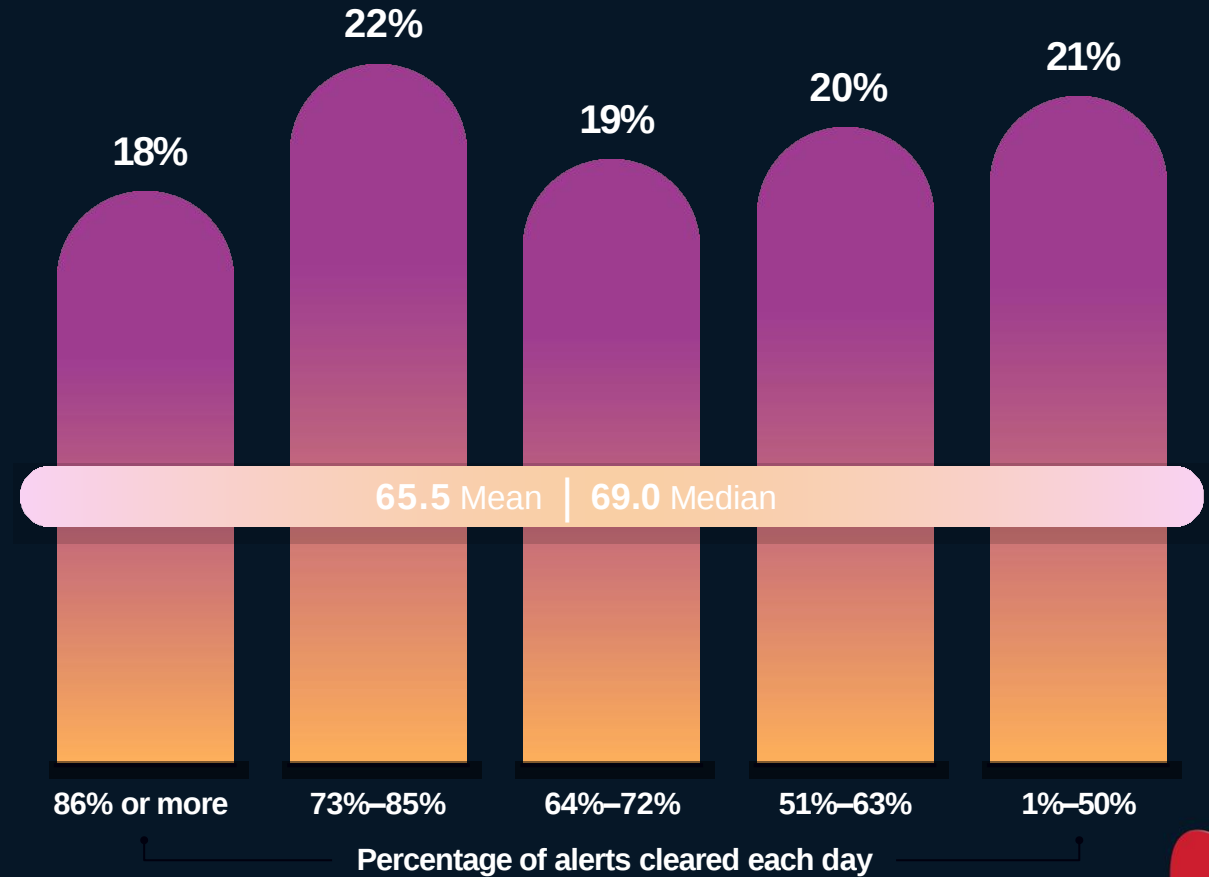
GO **BEYOND**
Cisco Engage GBA

On a daily average,
organizations with a SIEM



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

GO **BEYOND**
Cisco Engage GBA



What are the challenges in the TDIR lifecycle ?

TDIR Are Still Challenging, According to Users and Managers

GO **BEYOND**
Cisco Engage GBA

Top Challenges to Using the Full Capabilities of TDIR Platforms



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



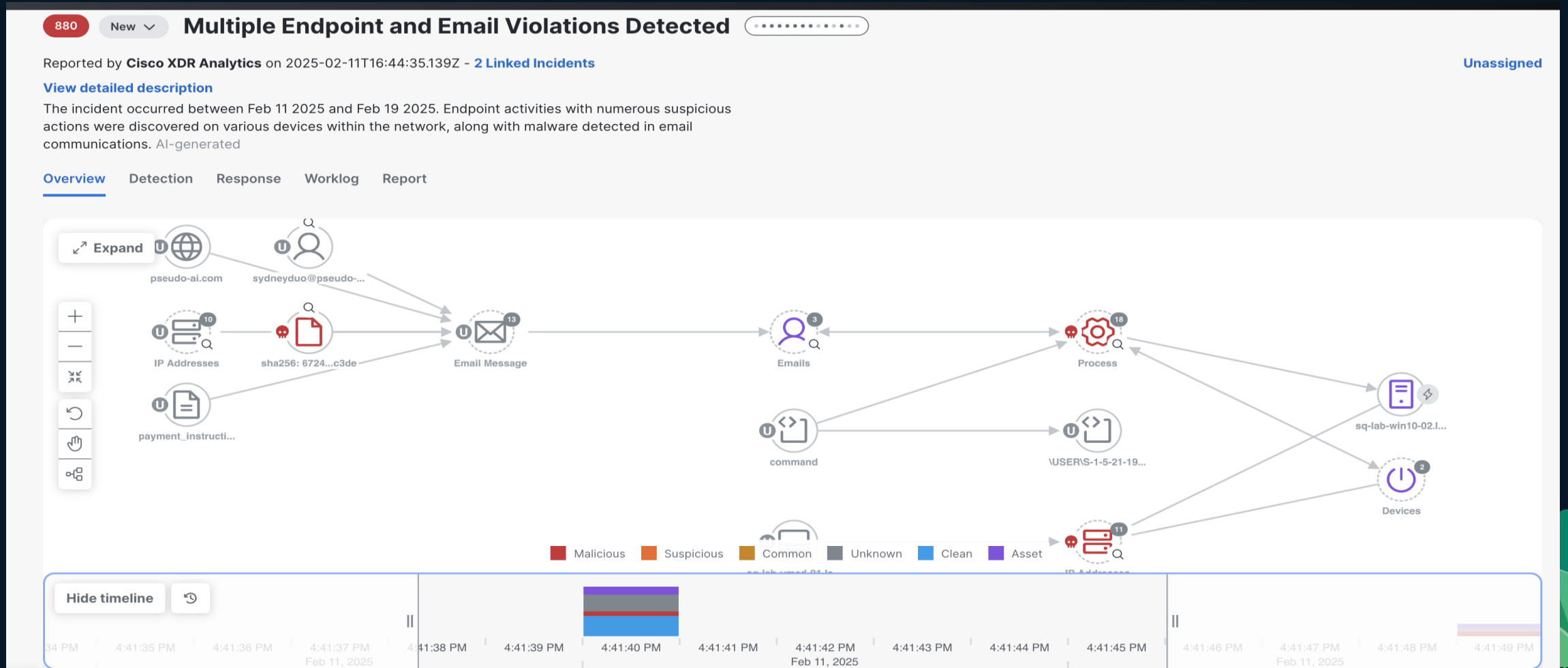
CISCO *Engage*

How can AI assist with TDIR?

AI Assistant for Security

GO BEYOND
Cisco Engage GBA

Attack Graph Enhancement



AI Assistant for Security

GO BEYOND
Cisco Engage GBA

Incident Report

Cisco Advisor

Generate note for incident review.

You 8:54 AM
Generate note for incident review.

Cisco Advisor 8:54 AM
The note has been generated. The next step would be to generate an incident report.

Generate incident report.

You 9:00 AM
Generate incident report.

Cisco Advisor 9:00 AM
The incident report has been generated. What do you want to do next?

Format and save the report as a PDF.

Share report with supervisor.

Close incident.

Write a message to Cisco Advisor

Incident List

New Malicious Email Sent to Multiple Users

Created via Umbrella 2m ago - Linked Incidents

CloudTrail Watchlist Hit for Cisco - Lawrenceville Lab (Earth) View long description

Overview Detection Response Working

Incident Report

Report for 'Malicious Email Sent to Multiple Users' incident.

Executive Summary

The execution of a PowerShell script executing Meterpreter payloads on thirteen systems was identified. Meterpreter is a component of Metasploit, an exploit framework for penetration testing often used by malicious actors. Analysis conducted by CTR indicated this remote activity occurred from an internal host "HOST1". The account used to make this connection was an identified compromised service account SERVICE_ACCOUNT. This host was confirmed to be infected with Trickbot, a credential harvesting malware, previously identified within the ClientName environment. Sixteen successful internal Remote Desktop Protocol (RDP) connections using this compromised account were observed. It is highly likely the Trickbot malware provided the adversary with remote access to the ClientName network, which in turn enabled the adversary to elevate privileges and move laterally within ClientName's environment. Once in the environment, the adversary would then have the ability to manually deploy Ryuk via Meterpreter.

Investigation Summary

The primary concern was to contain and remediate the Ryuk ransomware infection. Containment and recovery efforts, which at the time of this report were either complete or in the process of implementation included the following:

1. Password protect AMP for Endpoints connector installations to mitigate AMP uninstalls.
2. Create "Quarantine" and "Clean/Production" VLANs, to reduce the risk of contamination of new

Close Create PDF

Back Close Incident Generate Report

Security Advisory

Cisco Advisor

this malicious file?

Who are the owners associated with these endpoints?

You 8:30 AM
What endpoints were affected by this malicious file?

Cisco Advisor 8:30 AM
The following endpoints are associated with 4 user accounts that this malicious file was emailed to, and all contain multiple events.

Endpoint
E2E-DataLake-Internet1

Endpoint
DESKTOP-2ER967Q

Endpoint
E2E-Win10-x64-G

Endpoint
Desktop-Win53

How do you want to address this incident?

Quarantine the compromised systems.

Write a message to Cisco Advisor

Incidents

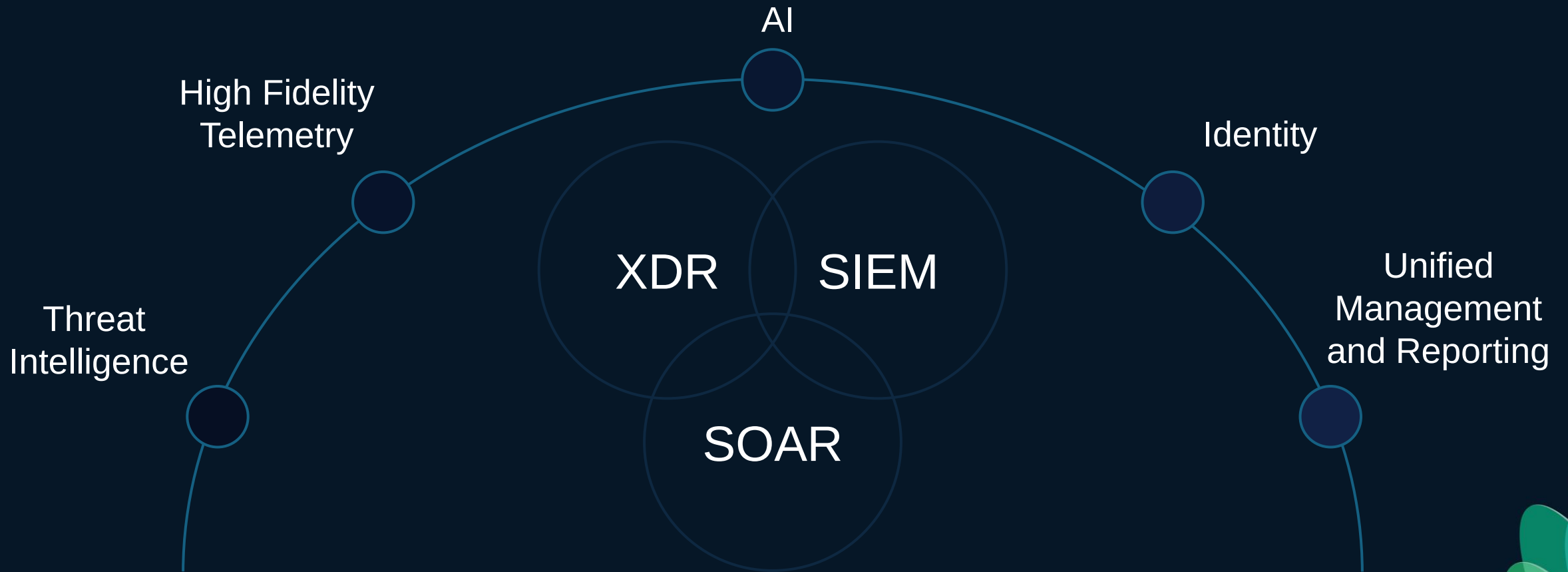
30 Unassigned Incidents 2 Incidents Assigned to Me 4 New Incidents

Search Last 30 days Assignment Status 123 matching results Reset all

Priority	Name	Source
990	Malicious Email Sent to Multiple Users	Endpoint
988	Threat_Audit in group Protect @ 20220124 19:08:04	Umbrella
885	Threat_Audit in group Protect @ 20220124 17:08:04	Endpoint
881	Win.Malware.Razy-9896045-0	Endpoint
793	Emotet-Botnet-Report	Endpoint
780	Mustang Panda deploys a new wave of malware targeting Europe	Talos
777	Qakbot_3 in group Triage @ 20220123 21:09:00	Endpoint
652	WannaCry_Ransomware in group Protect @ 20220123 17:04:49	Endpoint
627	Cryptominers and RATs	Talos
611	Cryptominers and RATs	Talos
230	Manjusaka: A Chinese sibling of Silver and Cobalt Strike	Talos
228	Manjusaka: A Chinese sibling of Silver and Cobalt Strike	Talos
204	Manjusaka: A Chinese sibling of Silver and Cobalt Strike	Talos
0	Plugx in group Protect @ 20220124 17:07:41	Endpoint

Cisco : Delivering SOCs' TDIR Elements

GO **BEYOND**
Cisco Engage GBA



Thank You!