CISCO Connect

Building the Modern SOC:

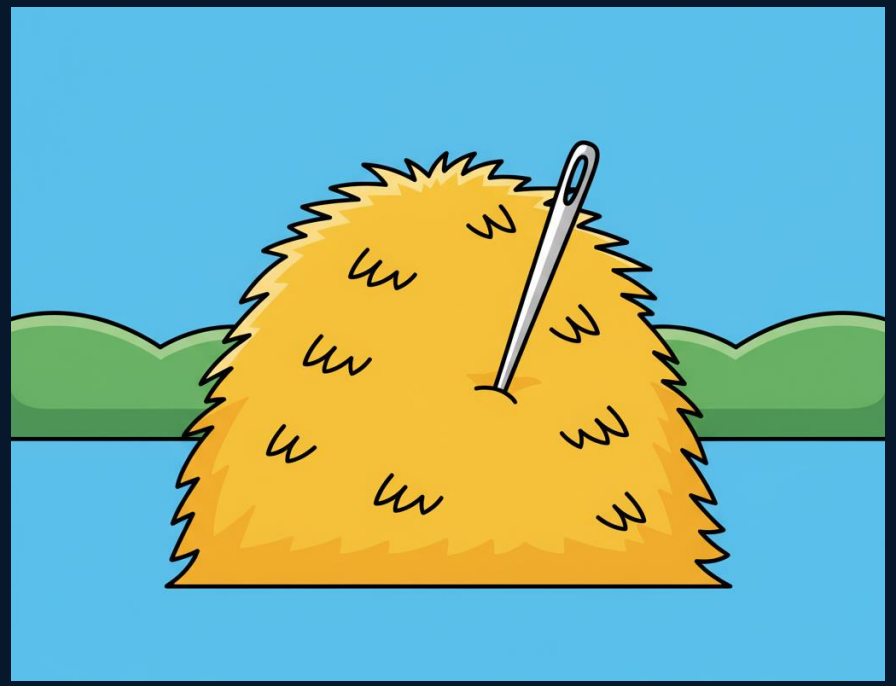
The Future of Threat Detection and Response

Matt Robertson
Distinguished Engineer, Threat Detection and Response

November 19, 2025

Security Operations

Continuously monitoring, detecting, and responding to cybersecurity threats



Finding the needle in the haystack

Security Operations

Continuously monitoring, detecting, and responding to cybersecurity threats

Finding the mouse in the beer bottle

Agenda

01 Introduction

02 The Security Operations Centre

03 Cisco Security Events SOC

04 **Network Behaviour and Anomaly Detection**

05 Summary

About Me

Matt Robertson

- Distinguished Technical Marketing Engineer
- Extended Threat Detection and Security Analytics
- Cisco Live Distinguished Speaker
- 17+ years at Cisco: Development, TME, Lancope
- Canadian eh

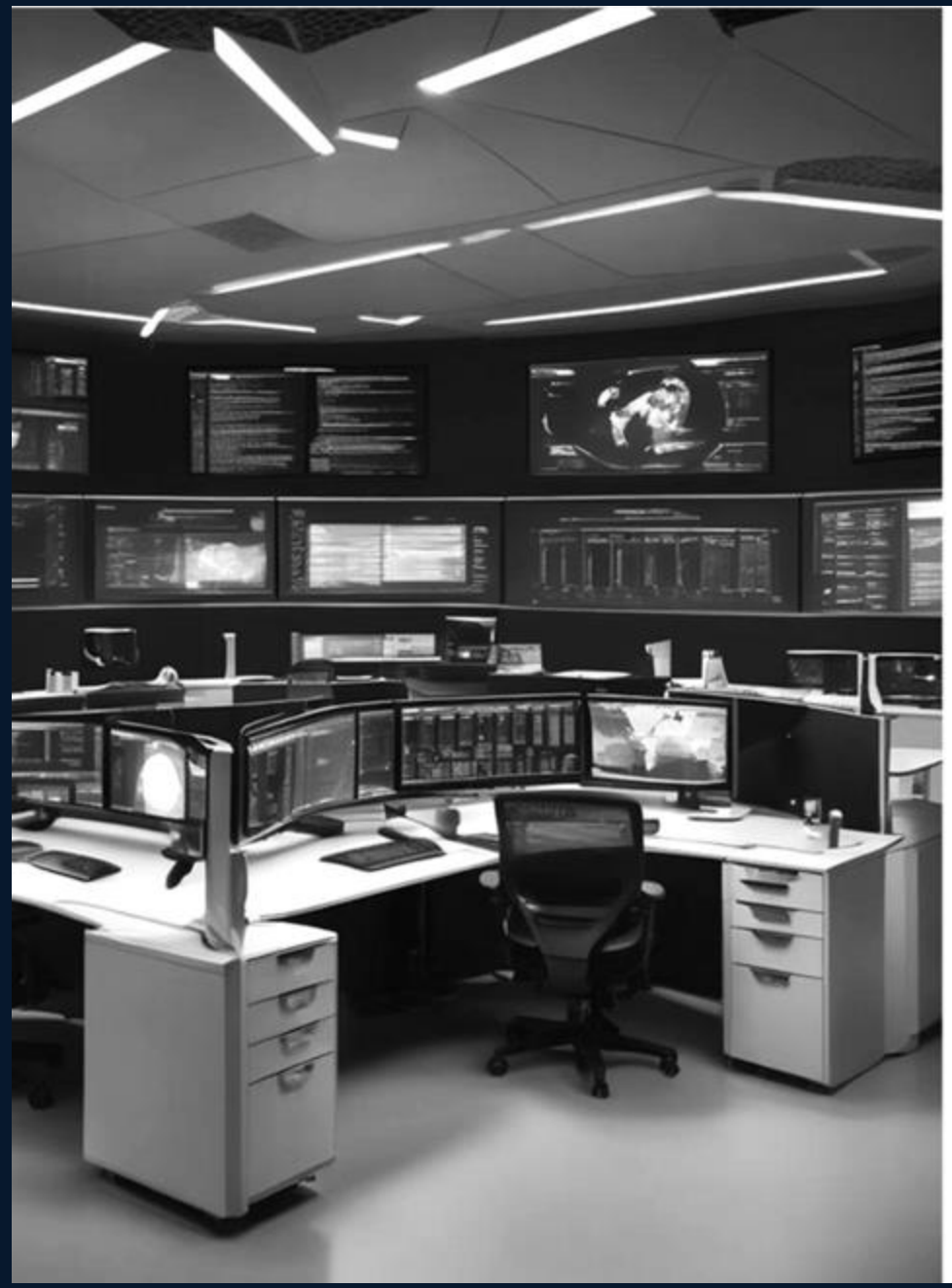
The Security Operations Centre

Security Operations Fundamentals

The primary objective of a Security Operations Center (SOC) is to protect an organization's assets and data by continuously monitoring, detecting, and responding to cybersecurity threats in real-time.

Evolution of Security Operations

	1962-1995	1996-2000	2001-2006	2007-2013	2013-2015	2015-2020	2021- today
	Network Operations Centers	SNOC (NOC + SOC)	Enterprise Operation Center (EOC) (SOC +NOC + Call center)	SOC (EOC split apart)	NexGen SOC	Cyber Defense Center	SOC of the Future
Capabilities	• Network Alerts	• Antivirus • IDS • Firewall	• Vulnerability Management • Dynamic • Packet filtering • Antispam • IPS	• DLP • SIEM • SecOPs • Advanced Threat Protection	• CASB • Cloud Security • UEBA • Sandboxing • CERT • BYOD	• Big Data • CSPM/CWPP • SOAR • Deception • EDR/NDR/XDR • Cloud Native Security Tools • Threat Intel Platforms	• AI Assistant / Generative AI chat bots • Deep/Machine Learning • Natural Language Processing • Predictive monitoring • Anomaly Detections systems
Functions	• Network Device Management • Malicious code analysis	• Virus Alerts • Intrusion detection and Response	• Compliance • Incident Response	• Regulatory compliance • Log Monitoring • Malware Analysis	• Reverse Engineering • AI/ML Models • Threat Intelligence	• Threat Hunting • Automation • Orchestration • Playbooks • Analytics • External Risk Scoring	• Automated Dispositions • Ai Guided workflows
	Availability Monitoring	Reactive Monitoring	Proactive Monitoring	Automated Monitoring & Response		AI assisted	



Designing the SOC

SOCitecture: The Blueprint for Cybersecurity Wizards

1. **Clear Objectives and Scope:** Define the primary objectives of the SOC, including the types of threats it will monitor and the services it will provide (e.g., threat detection, incident response, compliance monitoring).
2. **Compliance and Regulatory Considerations:** Ensure that the SOC operations align with relevant legal, regulatory, and industry compliance requirements.Staffing and Skill Set: Hire and develop a team with the necessary skills in cybersecurity, incident management, threat analysis, and technical support.
3. **Technology and Tools**: Invest in the right technology stack to support SOC operations, including:
   - Security Information and Event Management (SIEM) systems
   - Security Orchestration Automation & Response (SOAR)
   - Detection and Response tools, (E.G. NDR, EDR, XDR)
   - User and Entity Behavior Analytics (UEBA)
   - Threat intelligence platforms (TIP)
   - Malware Analysis tools
   - Etc.
4. **Processes and Procedures:** Establish clear processes for incident detection, monitoring, investigation, response, and reporting. This includes defining workflows and playbooks for different types of incidents.
5. **Metrics and Reporting:** Establish key performance indicators (KPIs) and metrics to measure the effectiveness of the SOC. Regular reporting will help communicate the SOC's performance and areas for improvement.
6. **Training and Development:** Ensure ongoing training for SOC personnel to keep their skills updated with the latest threats, tools, and techniques.

Major Components of the SOC

People:
(Volume of)
Talent and skills

Processes:
Procedures used by people and tools

Technology:
Can the technology support the people and processes to achieve the desired outcome

SOC: Detect and Respond to Threats

Is this a threat?

Is this a threat?

Yes or No?

- Signal:
  - A network connection is made from an internal host to an external host

- Signal:
  - A network connection is made from an internal host to an external host.
  - The network connection lasted 20 minutes and uploaded 1 GB of data.

- Signal:
  - A network connection is made from an internal host in the data centre to an external host that resolves to a known malicious domain
  - The network connection lasted 20 minutes and uploaded 1 GB of data.

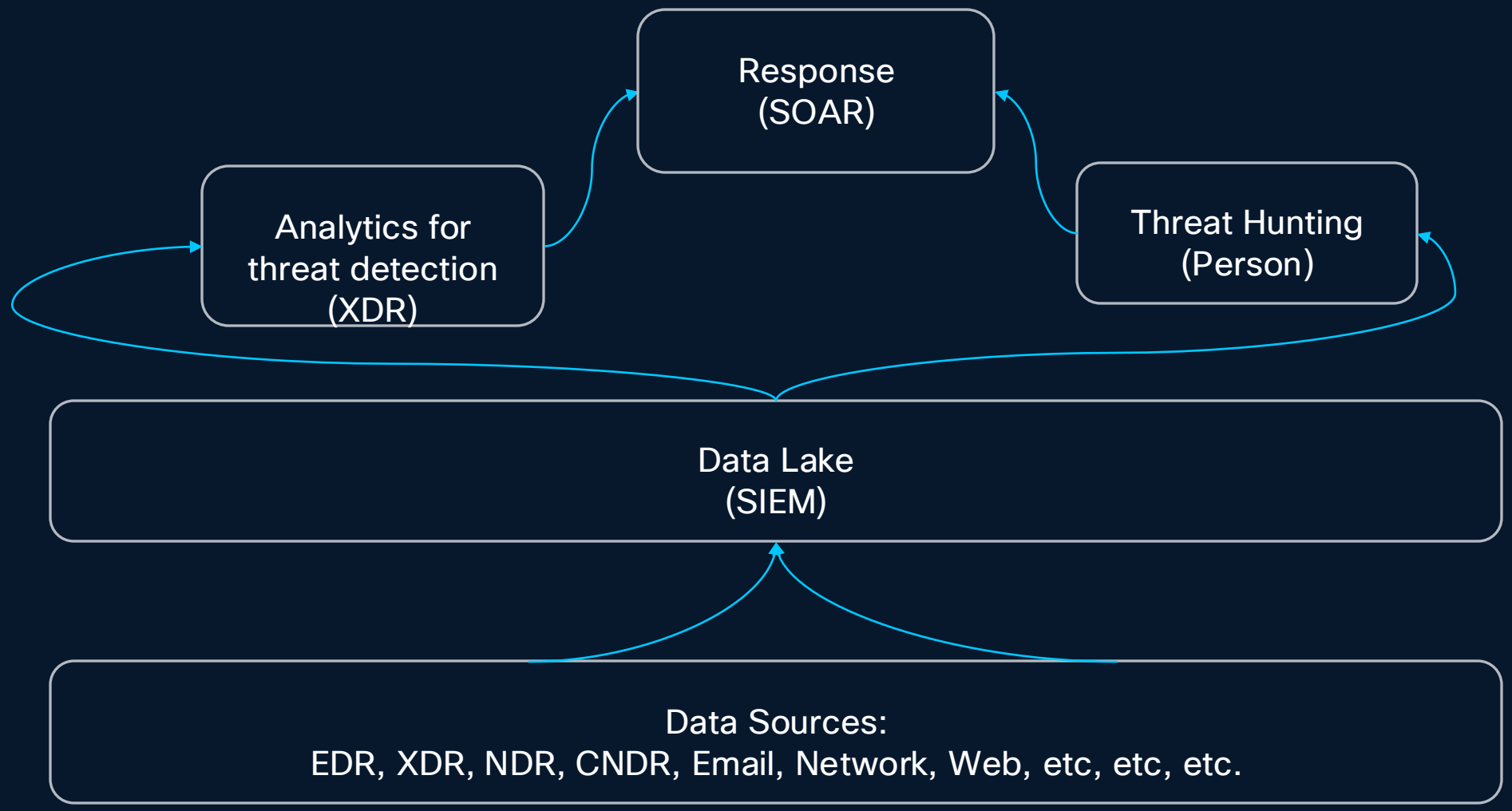
“

Detection Engineering has become a tooling and data science problem

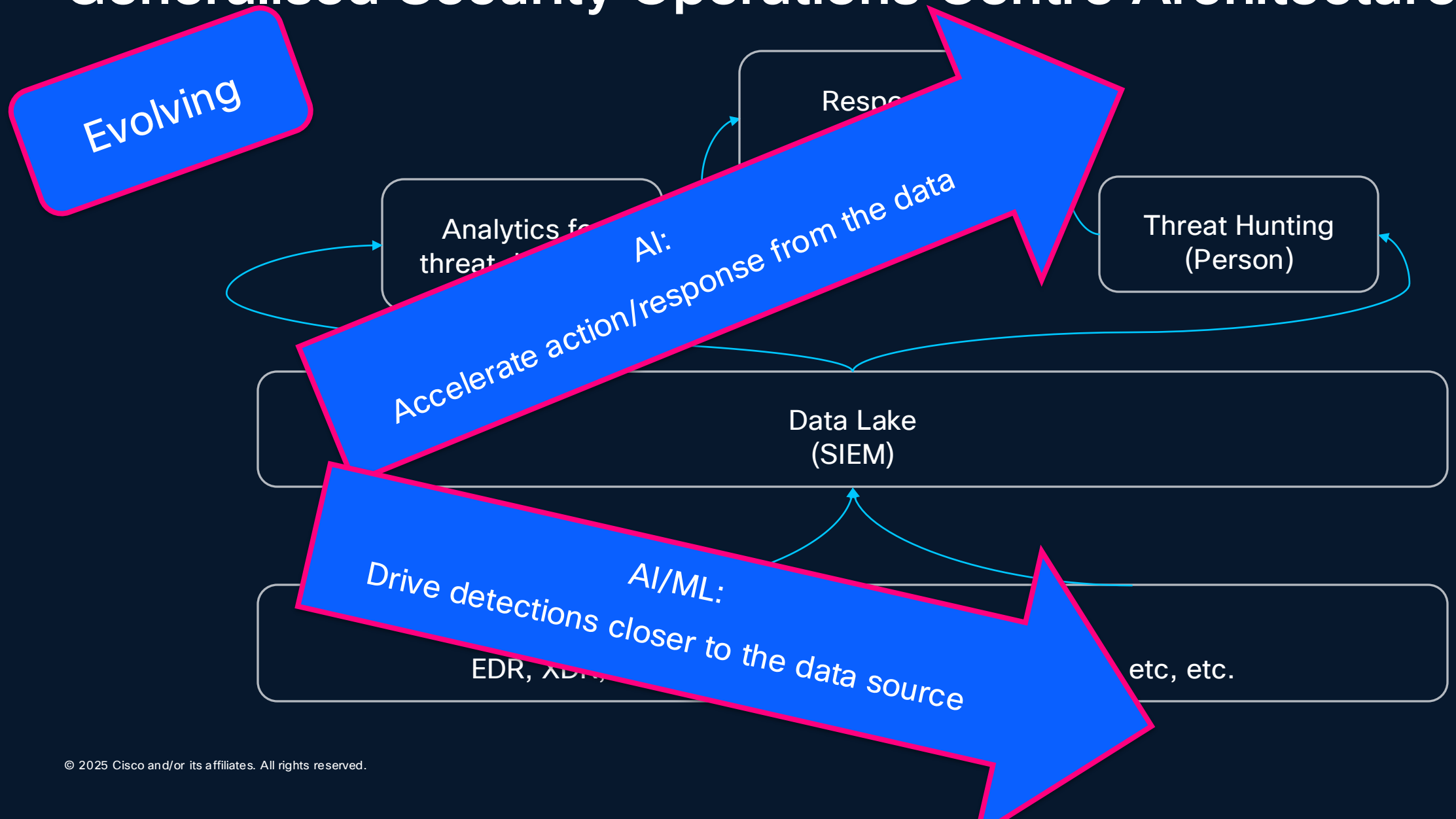
Critical capabilities for the SOC

- AI-Driven Threat Detection & Monitoring
- AI-Augmented Incident Triage & Investigation
- AI-Powered Incident Response & Remediation
- Proactive Threat Hunting with AI Hypotheses
- AI-Enriched Threat Intelligence
- Executive Reporting, Metrics & AI Narratives
- Continuous SOC Improvement through AI Feedback Loops

Generalised Security Operations Centre Architecture

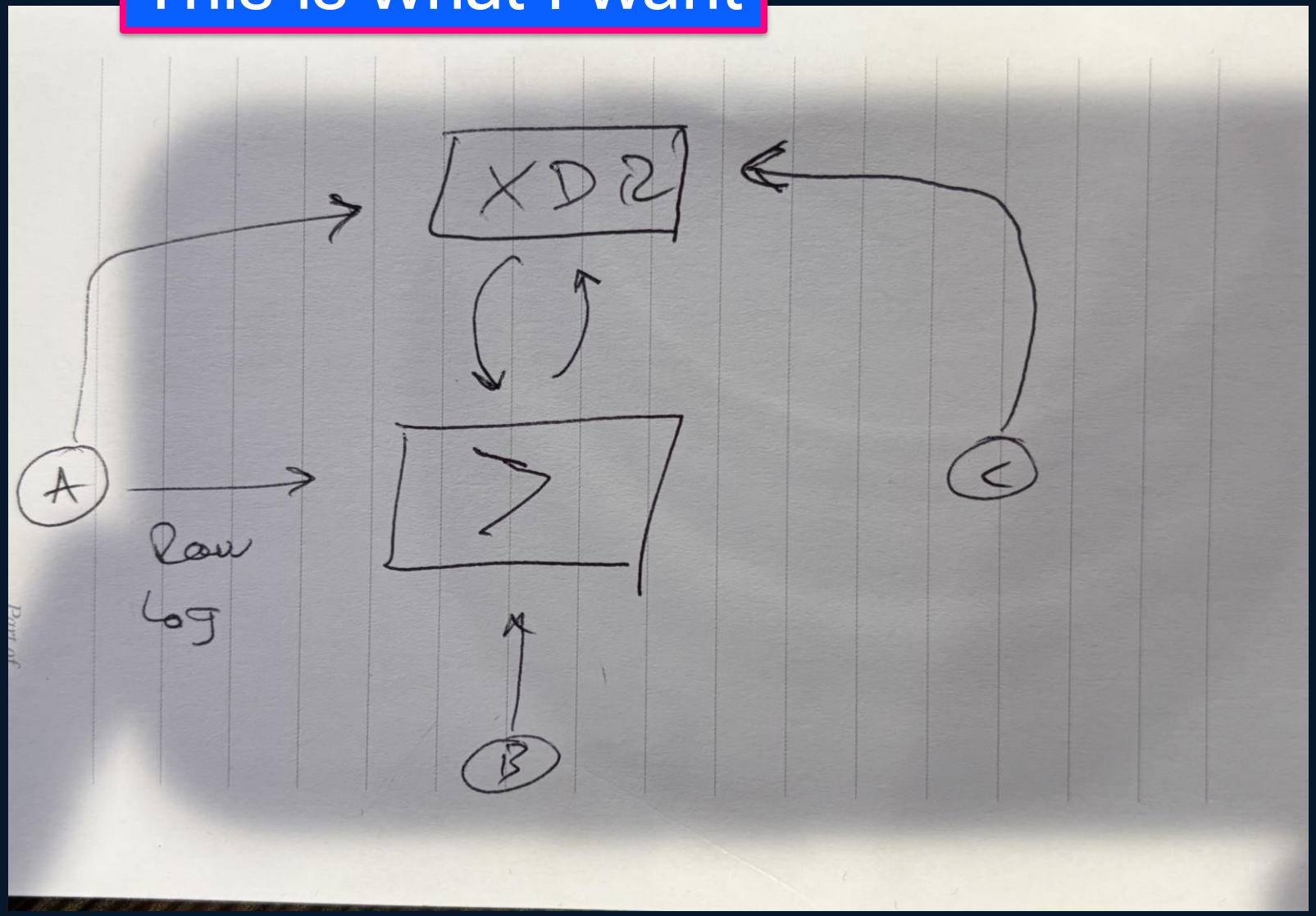


Generalised Security Operations Centre Architecture



CISO Request:

This is what I want



CISO Request: Broken down

XDR:
Analytics

A-Data:

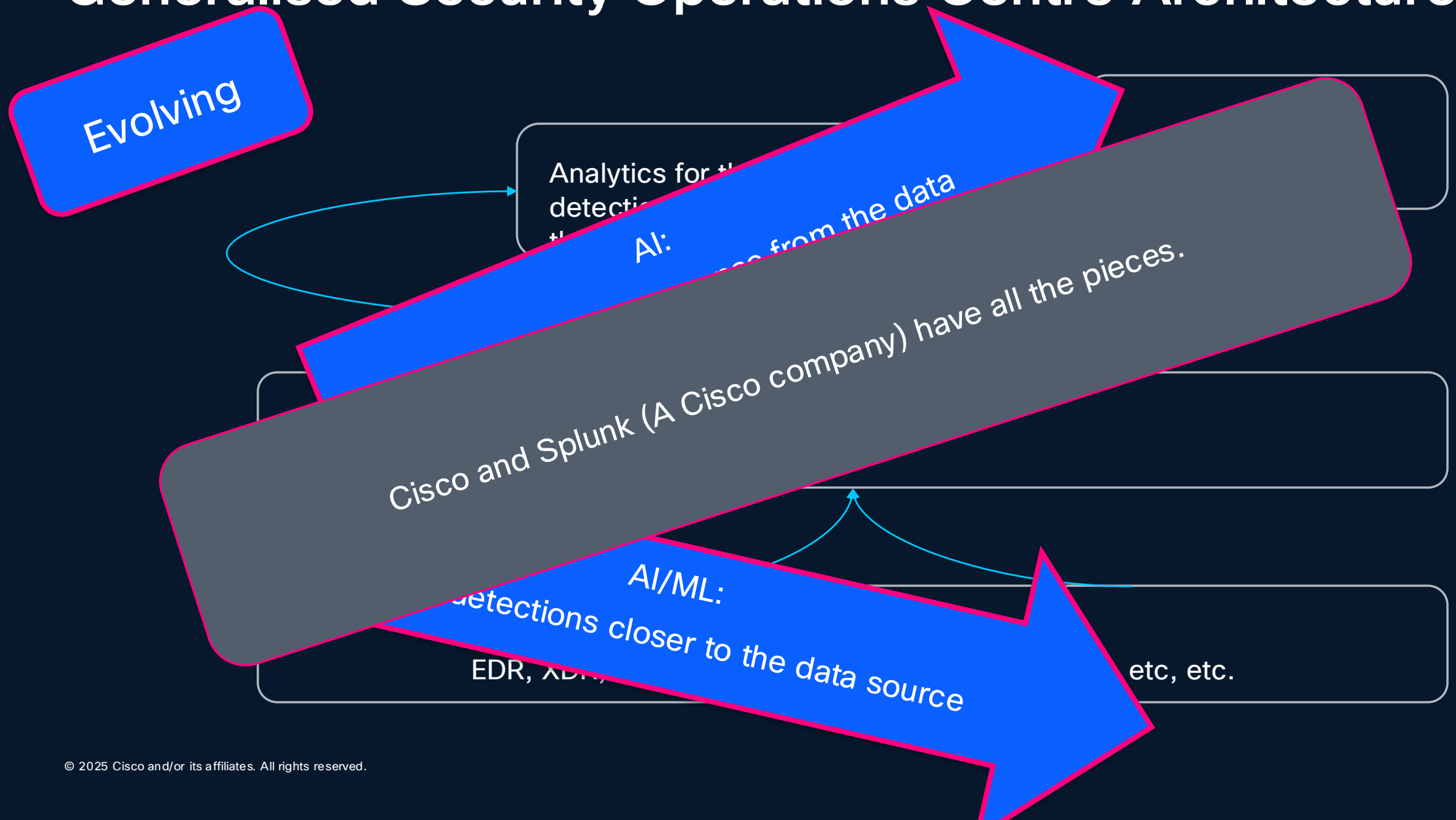
Logs that have inherent value for multiple outcomes/ For example threat analytics and threat hunters.
Ex: EDR logs

C-Data:
Data of little value without analytics first: ex. Network flow logs

Splunk: SIEM and SOC data platform

B-Data:
Compliance requirements
Ex. PCI DSS logging/retention requirements

Generalised Security Operations Centre Architecture



Unified SOC platform

Unified Threat Detection, Investigation, & Response

Federated data management

Advanced threat detections

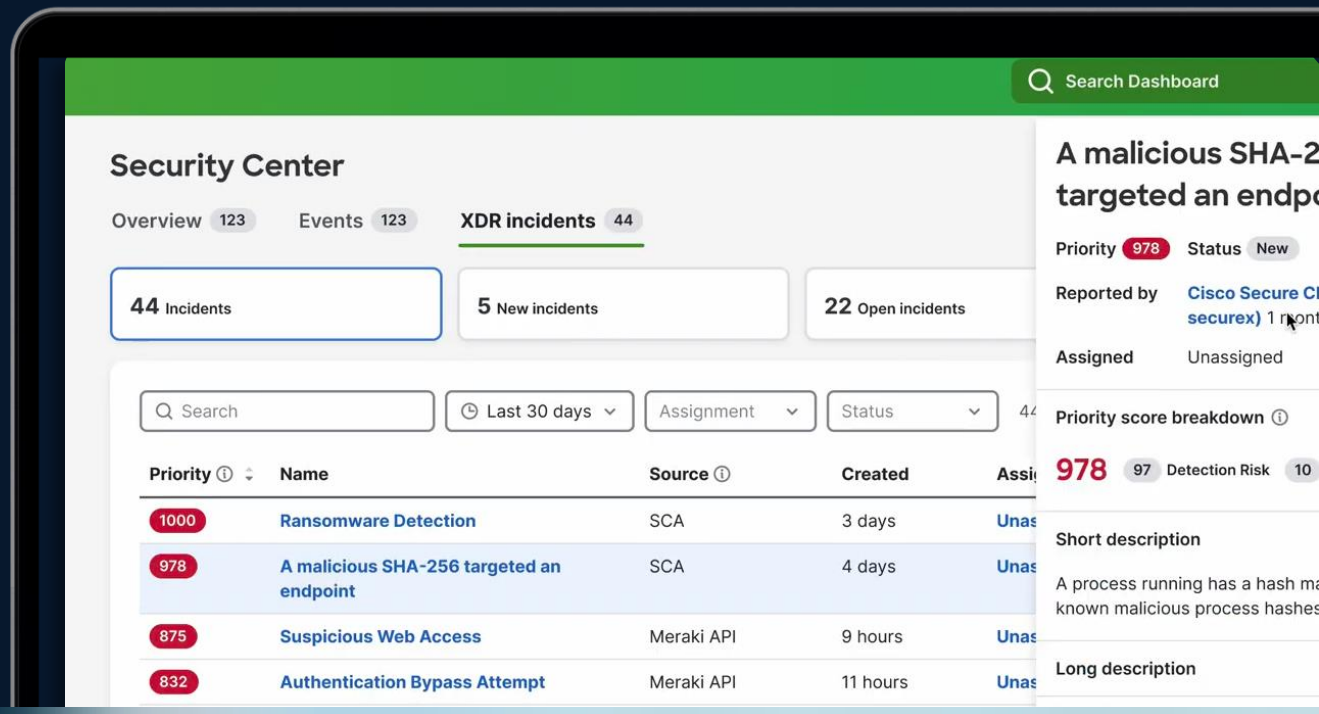
AI-accelerated investigations

Automated response

Unified security analyst experience

Cisco XDR 2.0

Detect and stop attacks at AI speed



Instant attack verification with Agentic AI

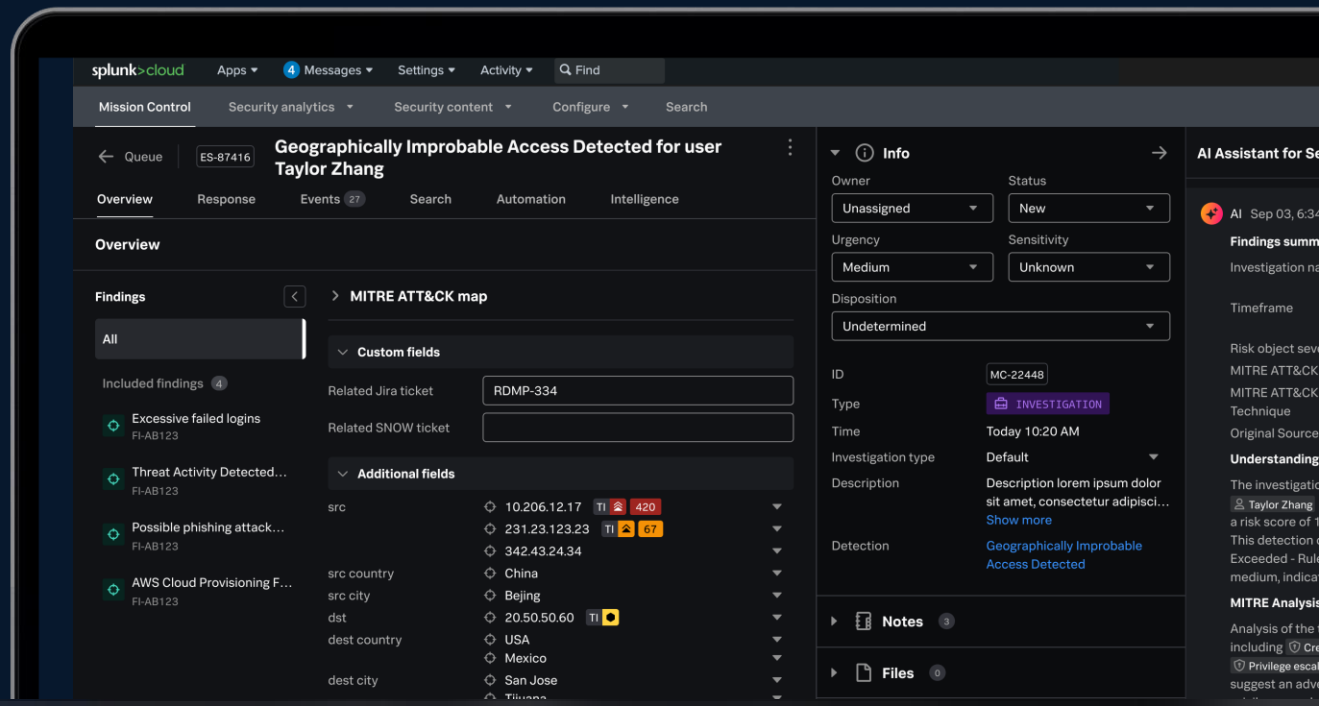
Automated forensics

Attack storyboard

Native Meraki Integration

Splunk Enterprise Security

Market-leading SIEM with AI-powered capabilities



- Natively integrated SOAR
- Enhanced detection
- Alert aggregation & triage
- Cisco Talos integration
- Multi-cloud & on-premises

AI-driven Security Operations

Unified Threat Detection, Investigation & Response (TDIR)

Cisco XDR
Real-time Attack Detection

Splunk Enterprise Security
Security Analytics

Splunk SOAR
Security Automation

EMBEDDED AI

Splunk Platform
Data Management and Federation

CONTENT AND THREAT RESEARCH

Cisco Security Cloud

Identity | Firewall | Talos | SSE | & more

Third-party tools

Clouds

Devices

Data centers

Applications

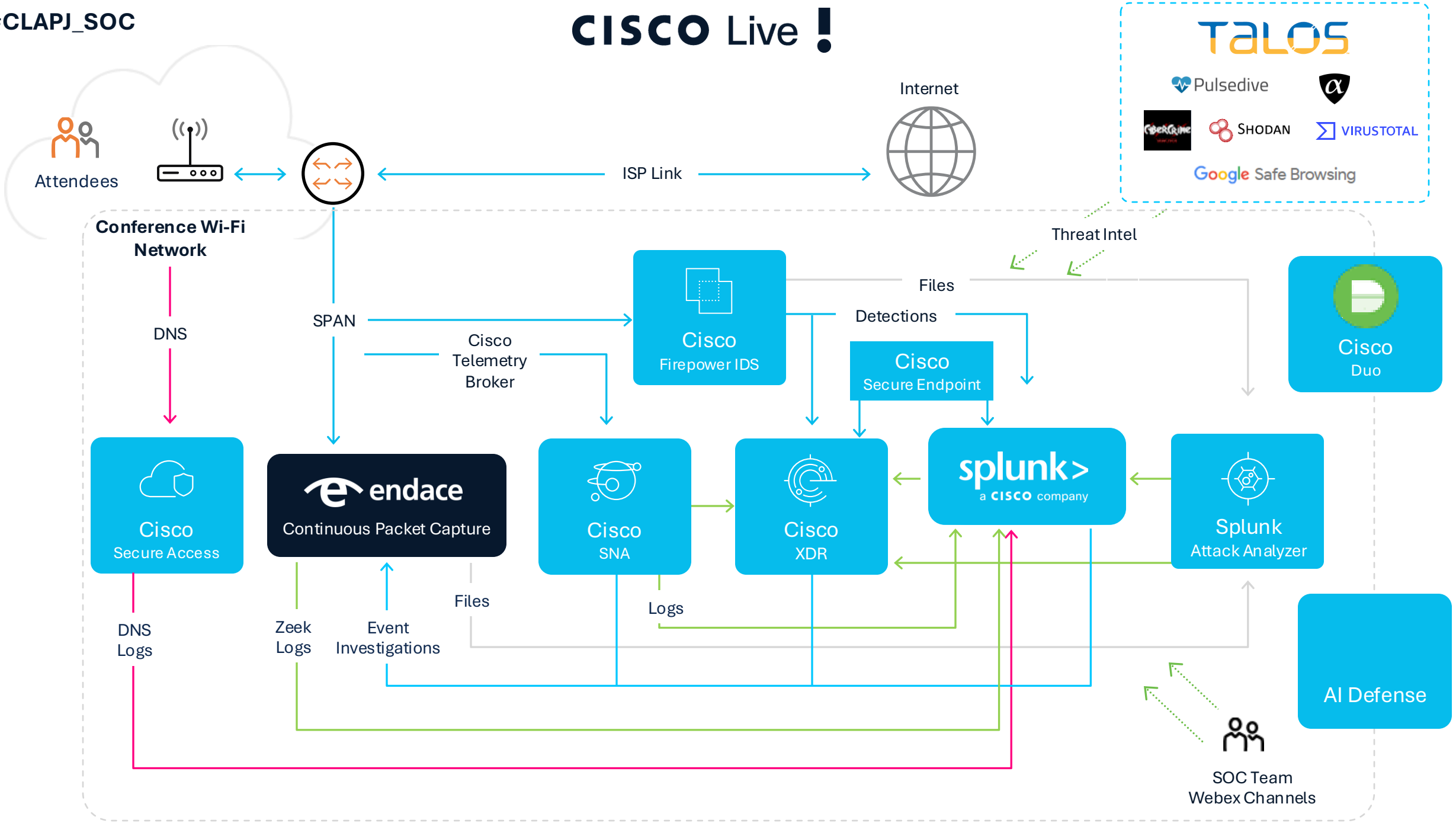
Cisco Security Events SOC

What is the Events SOC?

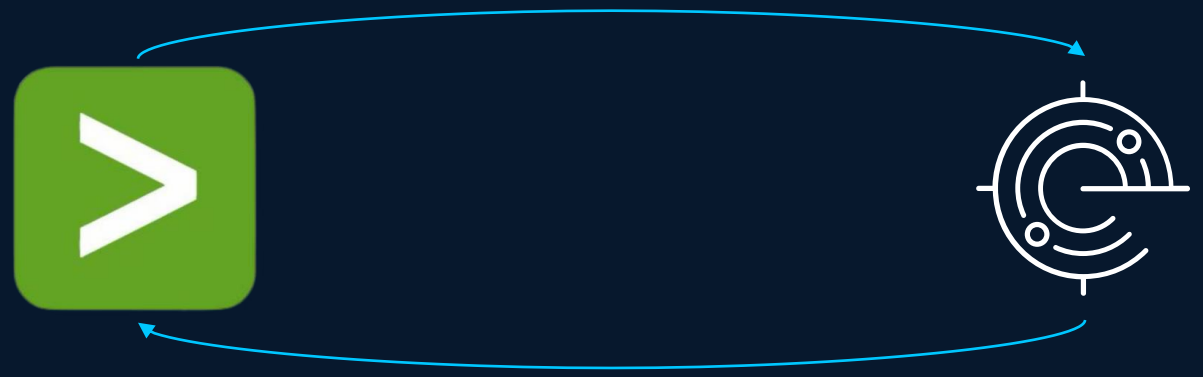
- Black Hat
- RSA
- Cisco Live
- Global Sporting Events
- Mobile World Congress
- Upcoming Olympics

#CLAPJ_SOC

CISCO Live !



Events SOC Architectural Benefits



Splunk:

- Native support for 2800+ data sources
- Custom dashboarding for various job roles
- Robust platform for advanced threat hunting

XDR:

- Extremely rich analyst experience
- Out-of-box detection and incident generation
- Tier 1 incident response

SOC Manager Dashboards in Splunk

Time Range: Last 24 hours

Priority Score: All (1)

SNOC - Incidents | SNOC - DNS | SNOC - Network

Total Incidents
Global
125

Total Incidents - New
Global
123

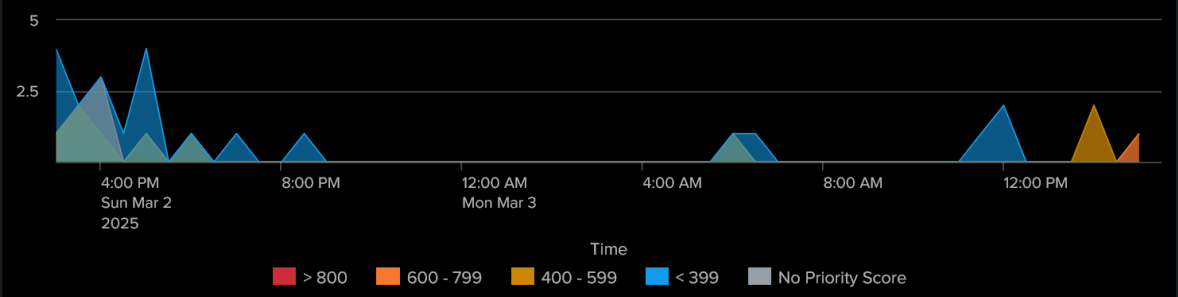
Total Incidents - Open
Global
1

Total Incidents - Hold
Global
0

Total Incidents - Closed
Global
1

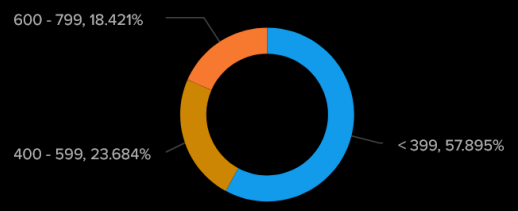
Total Cases
SOC Threat Hunting
0

Cisco XDR - Priority Score Timeline
Trend of Incidents in XDR over the last 24 hrs



Cisco XDR - MITRE Tactics Observed

Cisco XDR - Incident Priority Score
Split by incident priority score

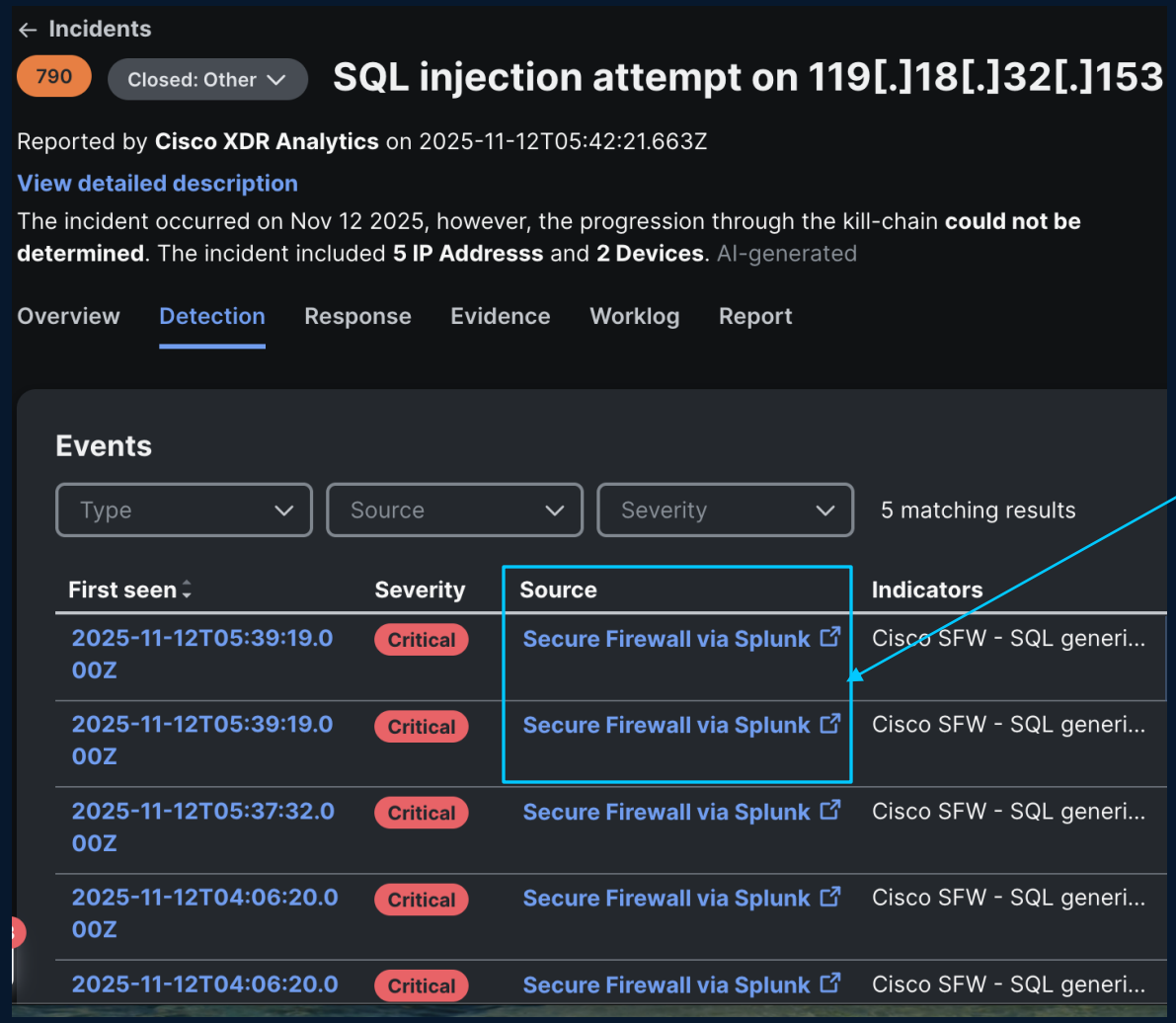


SOC - Cases
Apply filters at the top to reduce dataset

Title	Created	Status	Priority Score	Tactic	Count	Incident URL
DNS or URL Security Hit for Domain img.tnastatic.com - Last Update Mon Mar 3 14:10:42 2025 UTC	2025-03-03 14:10	New	500	TA0002	1	https://xdr.us.security.cisco.com/incidents/incident-6ea9bf4d-

< Prev 1 2 3 4 Next >

XDR with Splunk



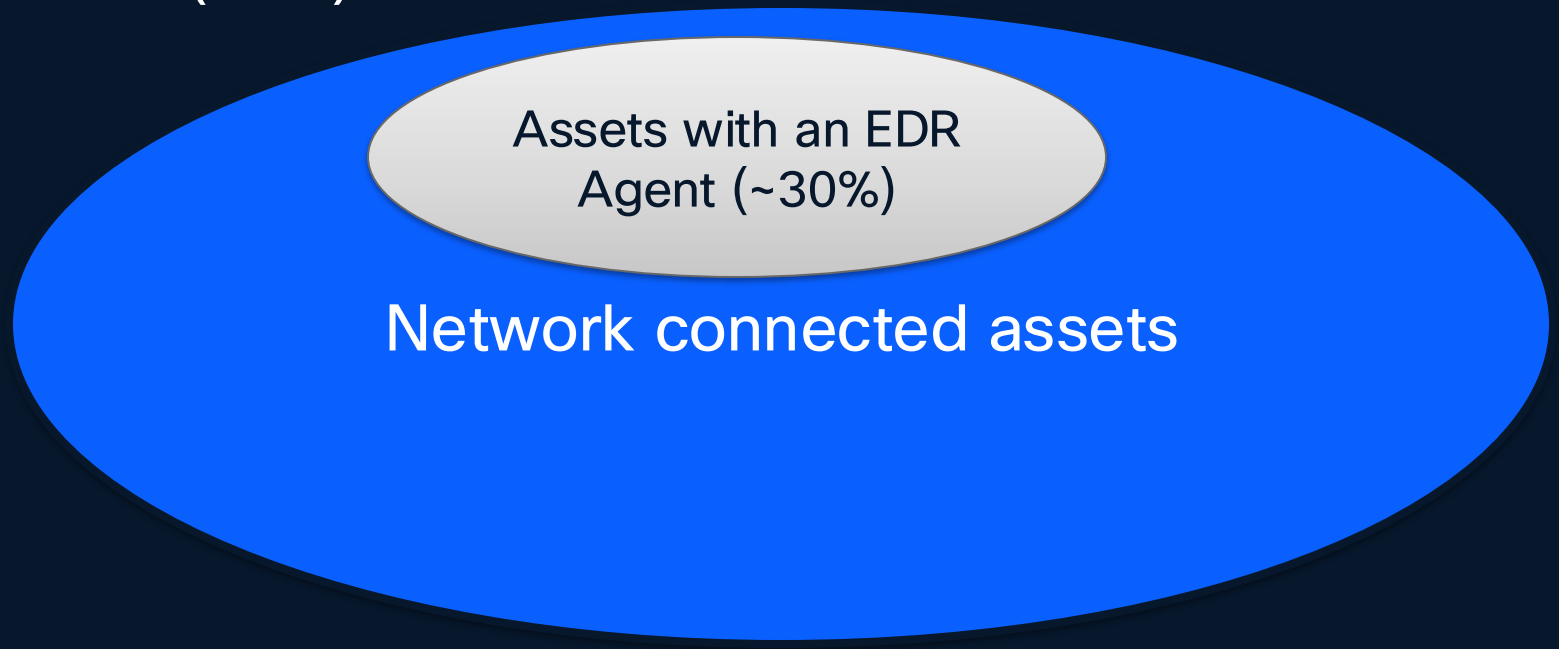
Leveraging Splunk data platform to pull data from multiple sources into XDR analytics and User experience

Network Behaviour and Anomaly Detection

Why does the SOC need network visibility?

Many of the devices connected to the network, wired and wireless, do not run an endpoint security client (EDR).

- IOT (MRI, cameras)
- Smart building
- Card readers
- Infrastructure
- Printers
- Phones
- Scanners
- TVs
- Etc.



Threat actors are increasingly using these “other” network connected assets as their point of presence/operations

Cisco Products that do NBAD

Cisco Secure Network Analytics

Secure Network Analytics is an enterprise grade collector and aggregator of network telemetry for the purposes of security analysis and monitoring

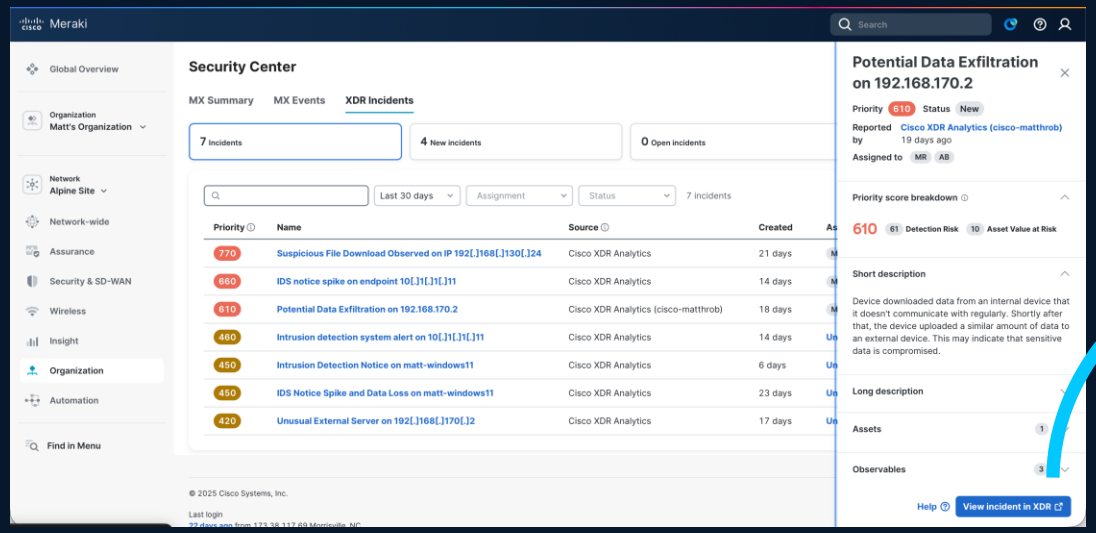
Cisco XDR

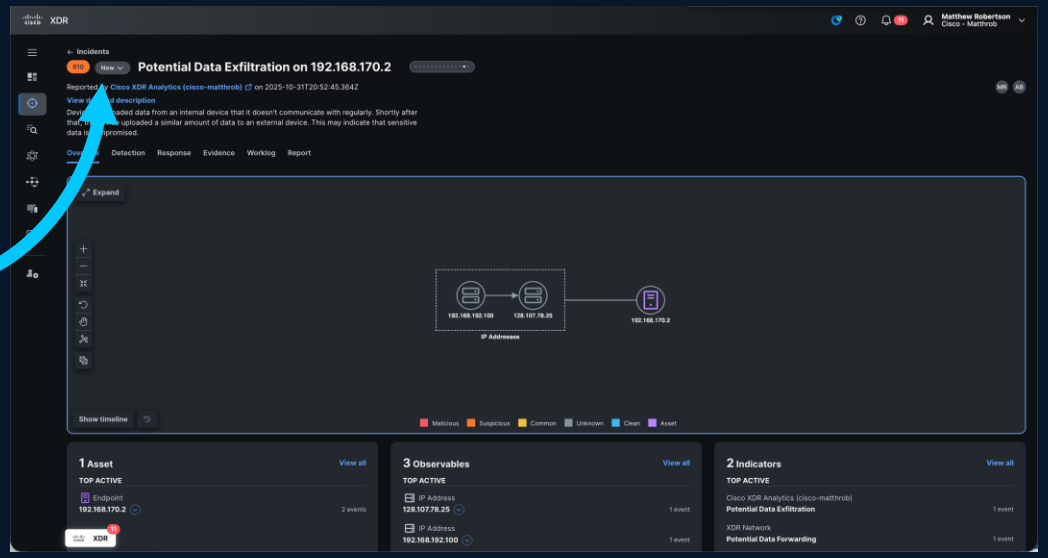
Cisco XDR collects and analyses telemetry from multiple sources to accelerate security operations.

One of those sources is the Network

Cisco XDR and Meraki

World's easiest to deploy NDR





- SSO driven integration between XDR and Meraki Dashboard
- Easy configuration to upload MX flow logs direct to XDR for analysis
- View/Manage incidents in Dashboard, pivot to XDR for investigation and response
- Monitor networks with overlapping IP Space

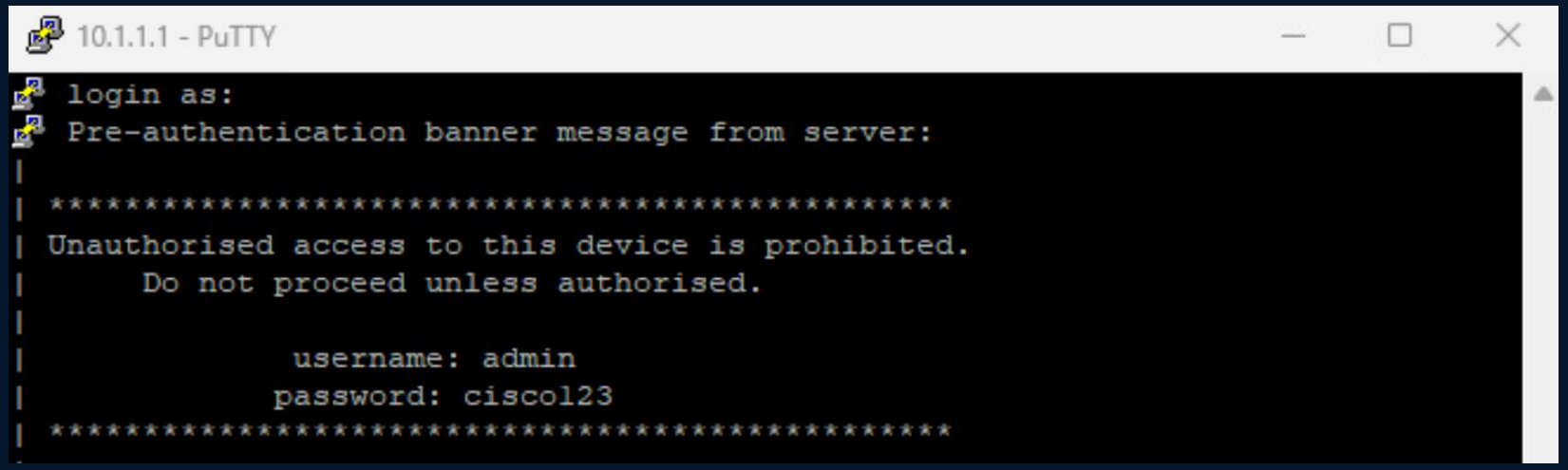
Living off the LAN

Threat Actors are increasing leveraging network infrastructure as their points of presence

https://blog.talosintelligence.com/salt-typhoon-analysis/

Living off the LAN

Evolution of Living of the Land techniques



Attractive target due to high value and many security deficits

Upon initial access, adversaries remain and capitalize on evasion

Threat actors advancing espionage objectives through this target

Increasing need to monitor the management plane of network devices for malicious and/or suspicious activity

Example Threat Actor Scenario

Threat Actor

Accesses environment using stolen credentials

ssh

Switch

Initiates packet capture

Downloads sensitive data from internal assets

Internal servers

Upload files to desktop for storage

Management Desktop

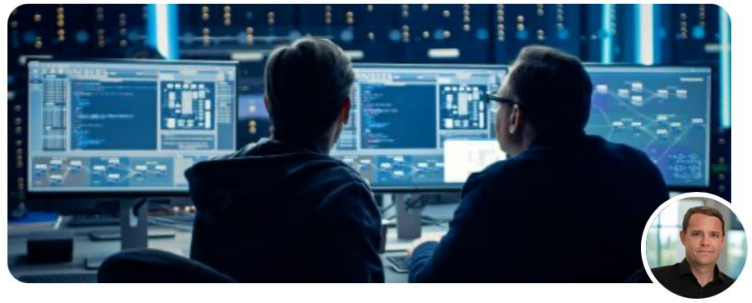
Exfiltrate to public web service

Public Web Service

Comprehensive network visibility with SNA

November 11, 2025

Leave a Comment



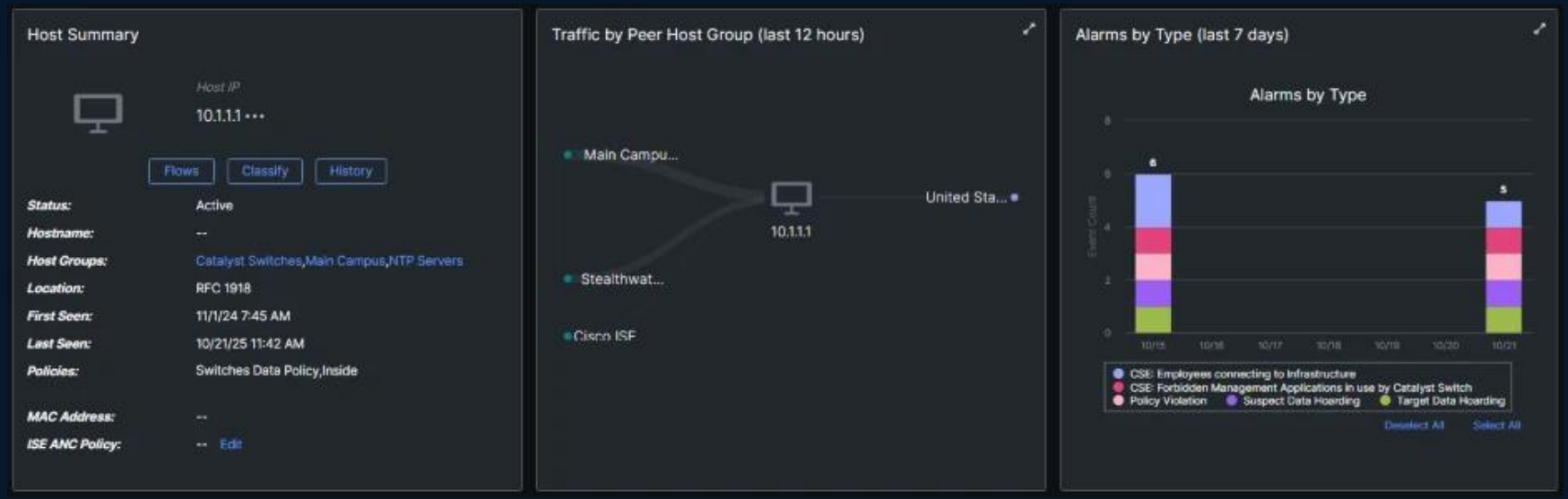
Security

Seeing Inside the Vortex: Detecting Living off the Land Techniques

3 min read

Matthew Robertson

https://blogs.cisco.com/security/seeing-inside-the-vortex-detecting-living-off-the-land-techniques



Key Takeaways

The modern SOC revolves around effective data analysis

Cisco and Splunk can help you build the modern SOC

NBAD is a critical capability of the Modern SOC

Find that mouse!

Visit the Solutions Expo

Thank you

CISCO