Cisco Event SOCs

A Reference Architecture and Operations Guide

Lessons learned while building the Security Operations Centers (SOCs) that secure the largest cybersecurity conferences around the globe.

Table of Contents

Executive summary

This “Cisco Event SOCs: A Reference Architecture and Operations Guide” outlines a proven, repeatable framework for building and operating Security Operations Centers (SOCs) specifically designed for short-lived, large-scale events such as major cybersecurity conferences. We drew lessons from deployments at RSAC™ Conference, Cisco Live, Black Hat, Paris 2024 Olympics, NFL Super Bowl & Draft, Mobile World Congress and GovWare.

This guide addresses the unique and demanding constraints of these environments, including high background noise, limited endpoint visibility, transient identities, and a need for highly agile, yet selective, response capabilities.

Figure 1: The event SOC team supports the largest cybersecurity & sporting entertainment events.

45.3B
packets captured for investigation

36.6TB
full packet capture written to disk

193GB
logs streamed to the cloud

22,701
unique devices observed on the network

~64.8M
DNS requests inspected

309,514
files reconstructed, 27,000 detonated

Figure 2: Example of the scale we defend (Cisco Live Americas 2025).

Mission

The core mission of these event SOCs is to:

- **Protect** event networks and data,
- **Educate** stakeholders through transparent operations and knowledge sharing,
- and **Innovate** continuously to stay ahead of evolving threats.

The architectural vision is built upon an integrated, cloud-centric ecosystem leveraging the Cisco Security Cloud and Splunk Cloud Platform. Key components include a portable “SOC in a Box” hardware foundation for rapid deployment, Cisco Secure Firewall for inline enforcement, Cisco Secure Access for DNS security, Endace Continuous Packet Capture for deep investigations, and advanced analytics from Cisco Secure Network Analytics.

Operationally, the SOC model employs a “two-plane” approach: Cisco XDR serves as the central hub for Tier 1 and Tier 2 analysts, providing incident-centric workflows, while Splunk Enterprise Security offers advanced correlation and threat hunting capabilities for Tier 3. This is complemented by repeatable workflows, AI-assisted analysis, and strategic automation to ensure consistent triage, rapid investigation, and selective, risk-aware response.

The guide emphasizes continuous innovation, treating each event as an opportunity to refine integrations, workflows, and detections. This approach ensures rapid deployment, consistent high-confidence triage, deep investigative capabilities, and reduced analyst fatigue, ultimately leading to a portable, scalable operating model that strengthens and improves with every deployment.

Our event SOC capability did not start as a mature platform. It began with a small, pragmatic stack of only a few tools of a security operations team inside a Network Operations Center, focused on immediate visibility and basic detection. Over successive events, it evolved the same way most organizations mature their security operations. We added telemetry sources, refined workflows, introduced automation and enrichment, improved identity and access for analysts, and expanded investigation depth through packet capture and advanced analytics. Each event served as a forcing function to harden what worked, remove what did not, and operationalize lessons into standard patterns that can be reused on day one of the next deployment.

Beyond creating a reliable SOC for each conference, this program exists to drive continuous innovation. Real-world operations expose gaps in integration, usability, and workflow efficiency that are difficult to find in lab environments. By capturing those requirements and translating them into improved designs, integrations, and operating procedures we make each new event deployment faster and more effective. We also create a feedback loop that contributes to product improvements and better outcomes for customers who face similar SOC maturity challenges.

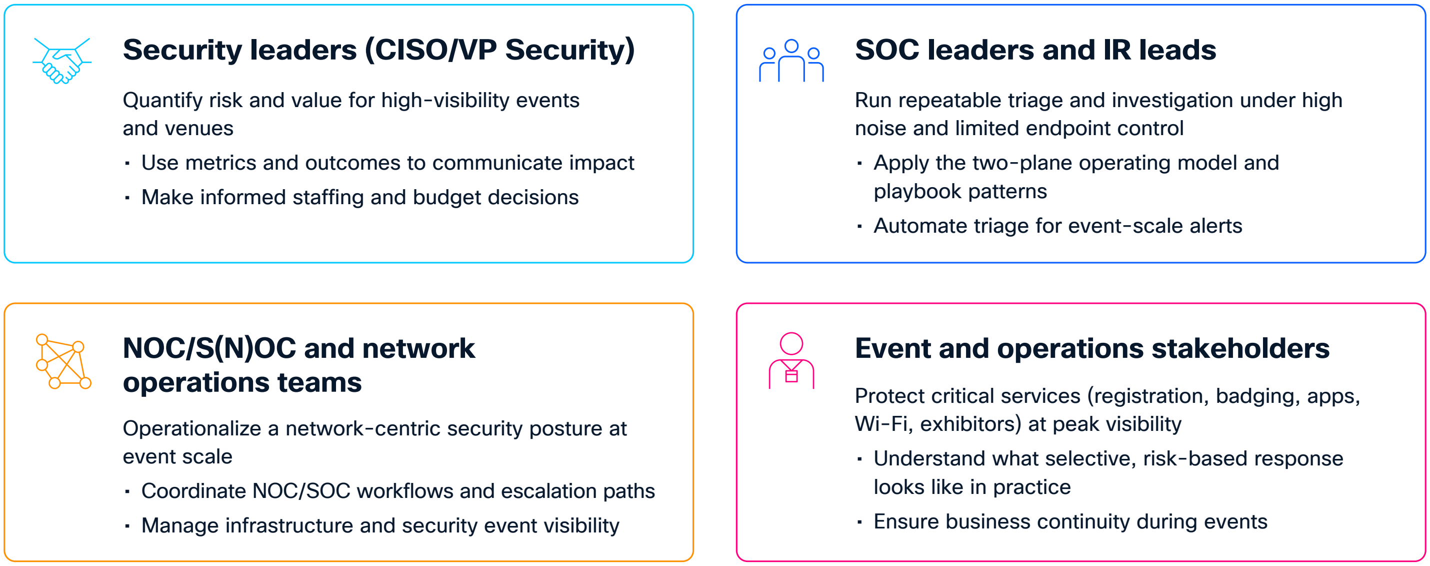
Purpose

- An operational guide to aid new SOCs starting out (likely from within a NOC)
- A reference for maturing SOCs who want to add capability, but are not sure where to start
- Experiences to inspire mature SOCs who want to innovate
- Show how Cisco operationalizes our own tools and third-party integrations in a S(N)OC environment

This “Cisco Event SOCs: A Reference Architecture and Operations Guide,” is based upon the collective experiences and innovations from the Security Operations Centers (SOCs) deployed at RSAC™ 2025 Conference, Cisco Live San Diego & Melbourne 2025, Black Hat USA & Europe 2025, and GovWare 2025.

1. Introduction

The modern threat landscape demands a SOC that is agile, intelligent, and highly integrated. This Reference Architecture & Operations Guide outlines an architectural and operational framework for SOCs built upon the proven successes and innovations demonstrated at major industry events like RSAC™ Conference, Cisco Live, Black Hat, and GovWare. This design emphasizes a cloud-centric approach, deep integration between Cisco Security and Splunk platforms, and an open ecosystem for extensibility, empowering SOC analysts across all tiers to protect, educate, and innovate against evolving cyber threats.



Security leaders (CISO/VP Security)

Quantify risk and value for high-visibility events and venues

- Use metrics and outcomes to communicate impact
- Make informed staffing and budget decisions

SOC leaders and IR leads

Run repeatable triage and investigation under high noise and limited endpoint control

- Apply the two-plane operating model and playbook patterns
- Automate triage for event-scale alerts

NOC/S(N)OC and network operations teams

Operationalize a network-centric security posture at event scale

- Coordinate NOC/SOC workflows and escalation paths
- Manage infrastructure and security event visibility

Event and operations stakeholders

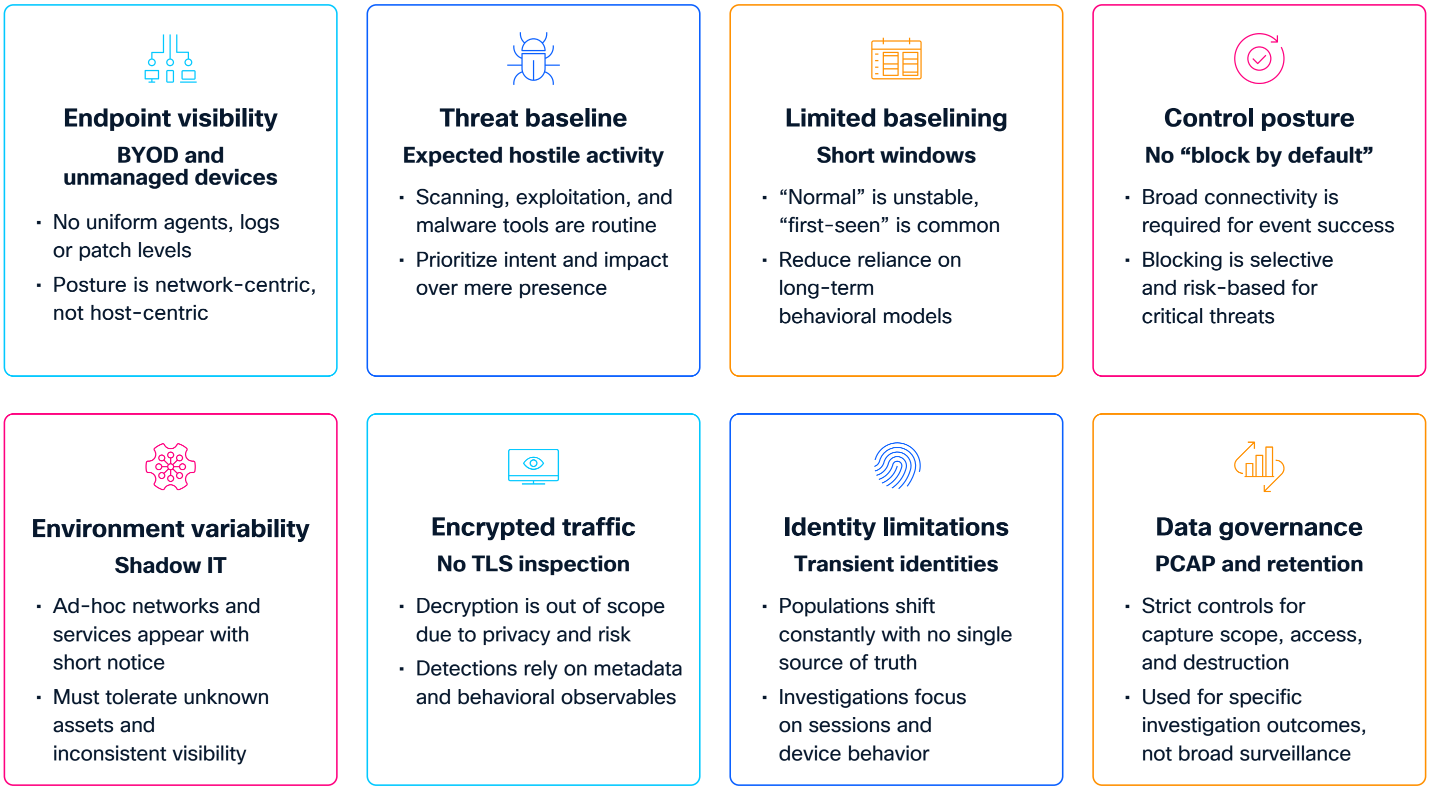
Protect critical services (registration, badging, apps, Wi-Fi, exhibitors) at peak visibility

- Understand what selective, risk-based response looks like in practice
- Ensure business continuity during events

Figure 3: Intended audience.

2. Constraints

Short-lived security operations centers, built for large-scale events, operate under constraints that differ from a steady-state enterprise SOC. Those constraints shape what telemetry you can depend on, how you tune detections, and what “effective response” looks like. The design described in this document assumes a highly dynamic environment with limited administrative authority over endpoints and identities, where operational continuity and attendee privacy must be balanced against detection depth and investigative fidelity.



Endpoint visibility

BYOD and unmanaged devices

- No uniform agents, logs or patch levels
- Posture is network-centric, not host-centric

Threat baseline

Expected hostile activity

- Scanning, exploitation, and malware tools are routine
- Prioritize intent and impact over mere presence

Limited baselining

Short windows

- “Normal” is unstable, “first-seen” is common
- Reduce reliance on long-term behavioral models

Control posture

No “block by default”

- Broad connectivity is required for event success
- Blocking is selective and risk-based for critical threats

Environment variability

Shadow IT

- Ad-hoc networks and services appear with short notice
- Must tolerate unknown assets and inconsistent visibility

Encrypted traffic

No TLS inspection

- Decryption is out of scope due to privacy and risk
- Detections rely on metadata and behavioral observables

Identity limitations

Transient identities

- Populations shift constantly with no single source of truth
- Investigations focus on sessions and device behavior

Data governance

PCAP and retention

- Strict controls for capture scope, access, and destruction
- Used for specific investigation outcomes, not broad surveillance

Figure 4: Cisco Events SOC (operational constraints).

Endpoint visibility: BYOD and unmanaged devices

Bring Your Own Device (BYOD) and unmanaged endpoints significantly constrain visibility. The SOC cannot assume uniform endpoint telemetry such as Endpoint Detection and Response (EDR) agents, consistent local logging, patch levels, or accurate asset inventories for attendee devices. As a result, the SOC posture is primarily network-centric, augmented by infrastructure sources such as wireless controllers, DHCP/DNS, firewalls, authentication systems (when applicable), and audit logs from the SOC's own SaaS platforms. This shifts coverage away from process-level or host-level artifacts and toward behavior-based detection and correlation across network and infrastructure signals.

Threat baseline: "Hostile-looking" activity is expected

The environment assumes that malicious or hostile-looking activity is expected. Security conferences and similar events are a nexus for research, training labs, demos, and ethical hacking. Activity that would be immediately alarming on a corporate network such as scanning, enumeration, exploitation attempts, credential testing, or malware-like tooling can be routine and even legitimate depending on context. This does not mean the SOC ignores it; instead, detections and response must prioritize intent and impact, focusing on behaviors that threaten event infrastructure, indicate propagation, target privileged services, or establish command-and-control patterns. This constraint directly drives alert tuning, suppression logic, and prioritization so analysts are not overwhelmed by endemic "expected noise."

Limited baselining: Short deployment windows and reduced "normal" context

Because conference SOCs are deployed under tight timelines, baselining network activity is inherently limited. In corporate environments, "normal" is established using weeks or months of historical telemetry across stable identities, assets, and business cycles; at conferences, the population of devices and services changes continuously and traffic patterns shift rapidly based on the event schedule. This means "first-seen" behavior is common, and benign activity can appear anomalous simply because there is little historical context.

This constraint can reduce the effectiveness of entity modeling and AI-assisted analytics that rely on learned baselines (e.g., UEBA-style scoring, behavioral profiling, and correlation). Early in the event, models may over-trigger, produce lower-confidence outcomes, or generate correlations that do not remain valid as the environment evolves. Operationally, the SOC should treat AI outputs as decision support and prioritize high-fidelity detections that do not require long history (known-bad infrastructure, protocol/behavior heuristics).

Control posture: No "block by default"

The network posture is typically permissive and not "block by default." Large-scale events require broad connectivity for attendee experience, training labs, vendor demos, and operational services, and aggressive prevention controls can cause unacceptable disruption. The SOC therefore treats blocking and containment as selective, risk-based actions reserved for high-confidence threats to critical services, clear malicious campaigns, or behavior that degrades network stability. This constraint has direct workflow implications: the response model prioritizes rapid triage, scoped containment, and protection of high-value infrastructure while preserving availability for legitimate activity.

Environment variability: Shadow IT and fragmented segments

Shadow IT is an operational reality. Exhibitor booths, training rooms, pop-up demo networks, and ad-hoc services often appear with short notice, may be managed by third parties, and may use local or cloud infrastructure that is only partially observable to the central SOC. Visibility into these segments can be inconsistent, and ingress/egress paths may not always traverse the same enforcement points. The SOC design therefore must tolerate unknown assets rather than relying exclusively on static asset inventories and predetermined correlation logic.

Encrypted traffic: No decryption/TLS inspection

Traffic decryption is out of scope. Implementing TLS/SSL inspection at an event commonly requires installing a trusted certificate on endpoints or operating an interception posture that introduces significant privacy, legal, and reputational risk especially where attendees bring personal devices and have not accepted an enterprise-managed trust model. Registration VLAN visibility is an example of when decryption for network inspection is implemented, to protect critical event infrastructure.

The SOC assumes limited visibility into encrypted payloads and designs detections around metadata and side-channel observables such as:

- Flow characteristics
- Timing and volume anomalies
- DNS and resolution patterns
- SNI and certificate metadata (where available)
- Destination reputation
- Behavioral indicators like beaconing or unusual egress

Where full packet capture is used, it remains valuable for reconstruction and for extracting unencrypted artifacts, but most network traffic will remain encrypted, which is expected. We publish metrics on the amount of unencrypted traffic after each managed event, as part of the Education mission, to encourage robust encryption.

Identity limitations: Transient, non-governed identities

Identities in event environments are transient and often not centrally governed. Unlike corporate environments with an HR-driven identity lifecycle and an authoritative directory, event populations shift constantly, and accounts may be provisioned and deprovisioned frequently without a single source of truth. As a result, identity-based correlation (for example, tying activity to a persistent person or role) is inherently weaker, and investigations tend to rely more heavily on network sessions, device behavior, infrastructure logs, time-bounded context, and open-sourced intelligence instead of specific “who did it” attribution. In practice, the most reliable identities are typically limited to SOC staff and administrators accessing tooling and core infrastructure, not the broader population generating most of the traffic.

Data governance: Full PCAP value vs. retention and destruction requirements

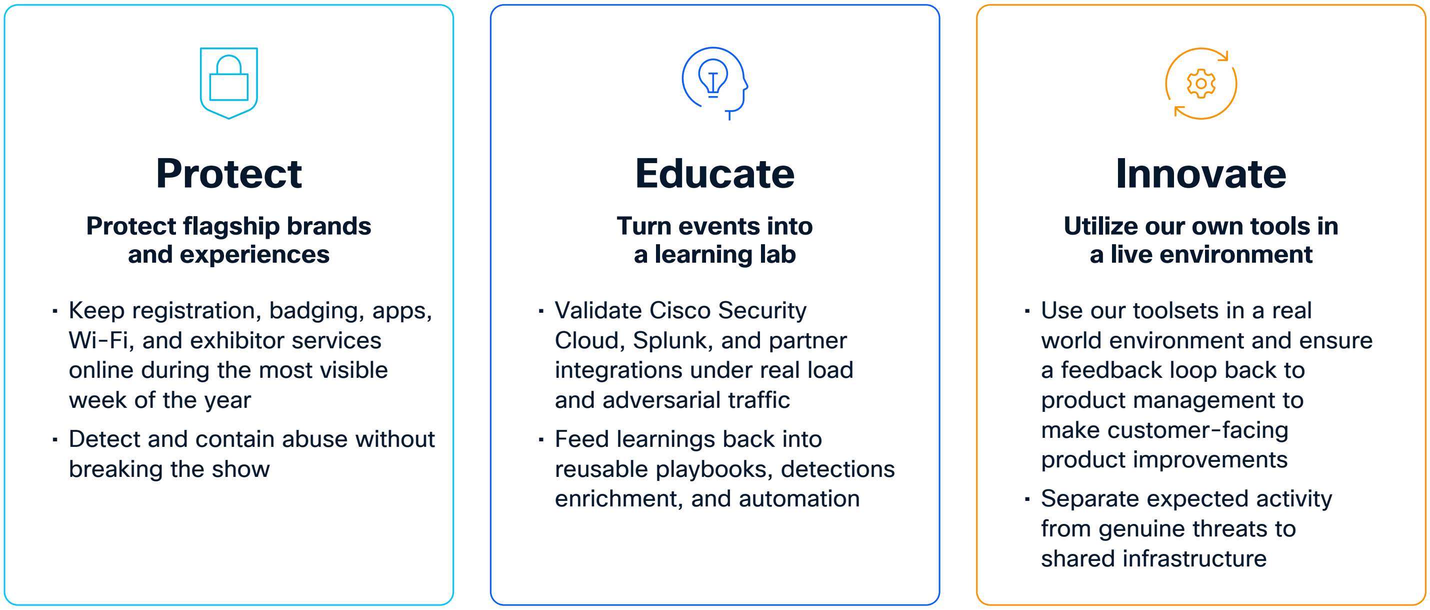
Data capture and destruction require explicit governance, particularly when full packet capture (PCAP) is included in the design. Full PCAP can be decisive for deep investigations and retrospective hunting when endpoint data is limited, but it also increases the sensitivity of collected information. The SOC must operate with clear policies and controls for scope of capture, least-privilege access, audited usage, defensible retention periods, and verified destruction procedures. Practically, this means implementing technical and procedural guardrails that ensure PCAP, and other high-fidelity data are used for investigation outcomes, not broad surveillance, and that retention aligns with compliance and privacy expectations as well as contractual obligations with the conference.

Summary: Operating envelope for this SOC

Taken together, these constraints define the operating envelope for the SOC: detection and investigation are built around network and infrastructure signals, identity attribution is limited, encrypted payload visibility is intentionally constrained, expected adversarial behavior creates a high-noise baseline, and response must balance security outcomes with the availability and openness required by the event.

3. Core principles

The foundation of this SOC design is rooted in three primary missions:



Protect

Protect flagship brands and experiences

- Keep registration, badging, apps, Wi-Fi, and exhibitor services online during the most visible week of the year
- Detect and contain abuse without breaking the show

Educate

Turn events into a learning lab

- Validate Cisco Security Cloud, Splunk, and partner integrations under real load and adversarial traffic
- Feed learnings back into reusable playbooks, detections enrichment, and automation

Innovate

Utilize our own tools in a live environment

- Use our toolsets in a real world environment and ensure a feedback loop back to product management to make customer-facing product improvements
- Separate expected activity from genuine threats to shared infrastructure

Figure 5: Core principles.

- **Protect:** Ensure the security of networks and data by defending against all forms of threats and attacks, both internal and external. Ensuring coverage at different vectors to build a multi-layered robust defense. Full stack coverage requires a multitude of technologies. Delivers unified visibility and control across identity, cloud, network, and endpoints, enabling rapid detection of behavioral anomalies
- **Educate:** Enhance understanding and awareness through transparent operations, insights, and knowledge sharing, including blogs and SOC tours. This could mean informing end users of a compromised machine, sharing cyber hygiene practices, and publishing our findings. Educate defines clear escalation paths to asset owners and, when required, law enforcement, ensuring stakeholders understand their roles and responsibilities during security incidents
- **Innovate:** Continuously advance security capabilities by developing and implementing new integrations, refining processes, optimizing workflows, and deploying automations, particularly leveraging Artificial Intelligence (AI) and other emerging technologies to stay ahead of an evolving threat landscape. You can access our GitHub here.

3.1. SOC tours

As part of these three missions, the SOC team provides tours of the event SOCs, led by the SOC Leader, Co-Leaders, and/or shift leaders, with time allocated to new SOC members to share their first-hand experience and for experienced analysts to discuss threats found. The image below shows the events supported by Cisco.

The purpose of the SOC tour is to demonstrate how Cisco and Splunk engineers collaborate to secure the events by actively monitoring the network for real-time security threats. Attendees gain a behind-the-scenes look at the Cisco Security and Splunk Security clouds in action, witnessing the integration of the Breach Protection Suite, User Protection Suite, Secure Firewall, and Splunk Enterprise Security.

During the tours, participants receive a security briefing and learn about the new innovations we are working on at the event. Attendees have the unique opportunity to engage in Q&A sessions with Cisco and Splunk engineers and the tour experience is designed to inspire thought and innovation, in the same manner as this document.

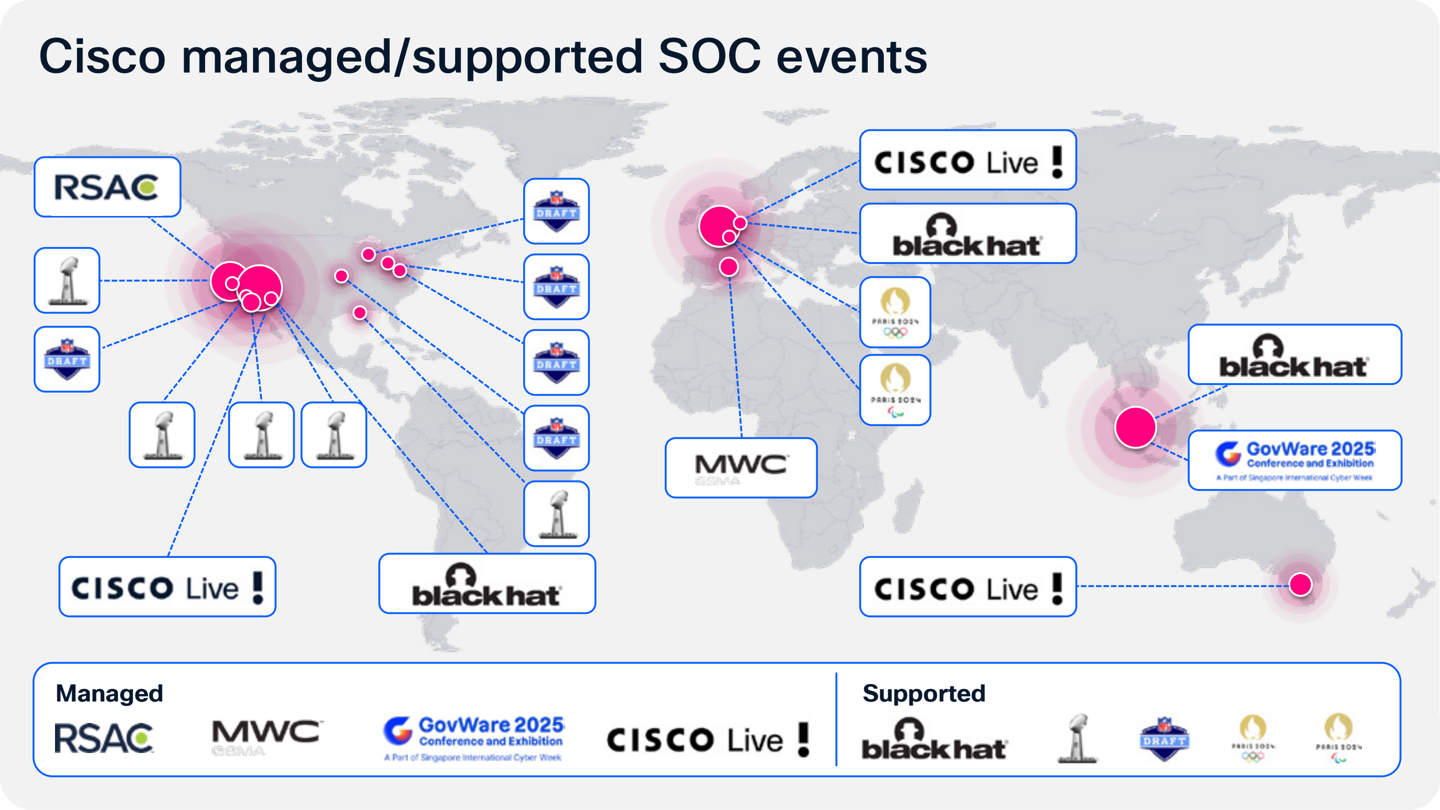

Cisco managed/supported SOC events
RSAC
DRAFT
CISCO Live
black hat
MWC GSMA
PARIS 2024
GovWare 2025 Conference and Exhibition
A Part of Singapore International Cyber Week
Managed
Supported

Figure 6: Global impact.

4. Architectural vision

4.1. Integrated Cisco Security Cloud and Splunk Cloud

This design envisions a seamlessly integrated security ecosystem where Cisco Security Cloud and Splunk Cloud Platform work in concert to provide comprehensive visibility, accelerated detection, and orchestrated response.

Cisco XDR serves as the central hub for Tier 1 and Tier 2 analysts, offering rich context and automation, while Splunk Enterprise Security provides advanced correlation, analytics, and threat hunting capabilities for Tier 3 analysts and incident responders.

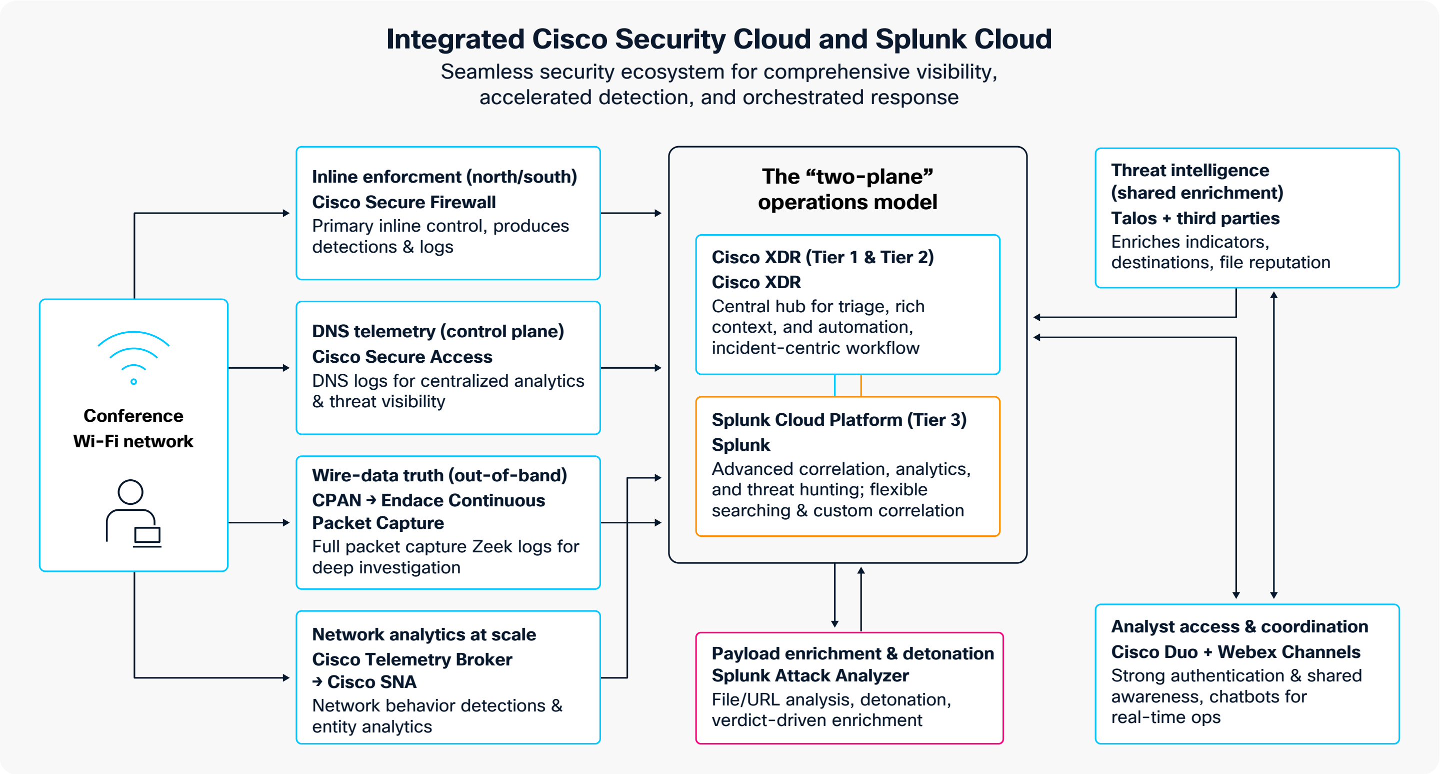

Integrated Cisco Security Cloud and Splunk Cloud
Seamless security ecosystem for comprehensive visibility, accelerated detection, and orchestrated response
Conference Wi-Fi network
Inline enforcment (north/south)
Cisco Secure Firewall
Primary inline control, produces detections & logs
DNS telemetry (control plane)
Cisco Secure Access
DNS logs for centralized analytics & threat visibility
Wire-data truth (out-of-band)
CPAN → Endace Continuous Packet Capture
Full packet capture Zeek logs for deep investigation
Network analytics at scale
Cisco Telemetry Broker → Cisco SNA
Network behavior detections & entity analytics
The "two-plane" operations model
Cisco XDR (Tier 1 & Tier 2)
Cisco XDR
Central hub for triage, rich context, and automation, incident-centric workflow
Splunk Cloud Platform (Tier 3)
Splunk
Advanced correlation, analytics, and threat hunting; flexible searching & custom correlation
Payload enrichment & detonation
Splunk Attack Analyzer
File/URL analysis, detonation, verdict-driven enrichment
Threat intelligence (shared enrichment)
Talos + third parties
Enriches indicators, destinations, file reputation
Analyst access & coordination
Cisco Duo + Webex Channels
Strong authentication & shared awareness, chatbots for real-time ops

Figure 7: Network as a sensor.

The architecture in Figure 8 shows how telemetry and outcomes flow from the conference network through controls, into investigation platforms, and back into analyst workflows.

At many events there are managed endpoints that have Cisco Secure Endpoint or a third-party EDR product installed for protection. Such as laptops to run Cisco Live and the iOS devices at Black Hat, and the organization-owned devices at major sporting events. In those cases, the EDR logs and detections are also used to protect the owned assets connected to the network.

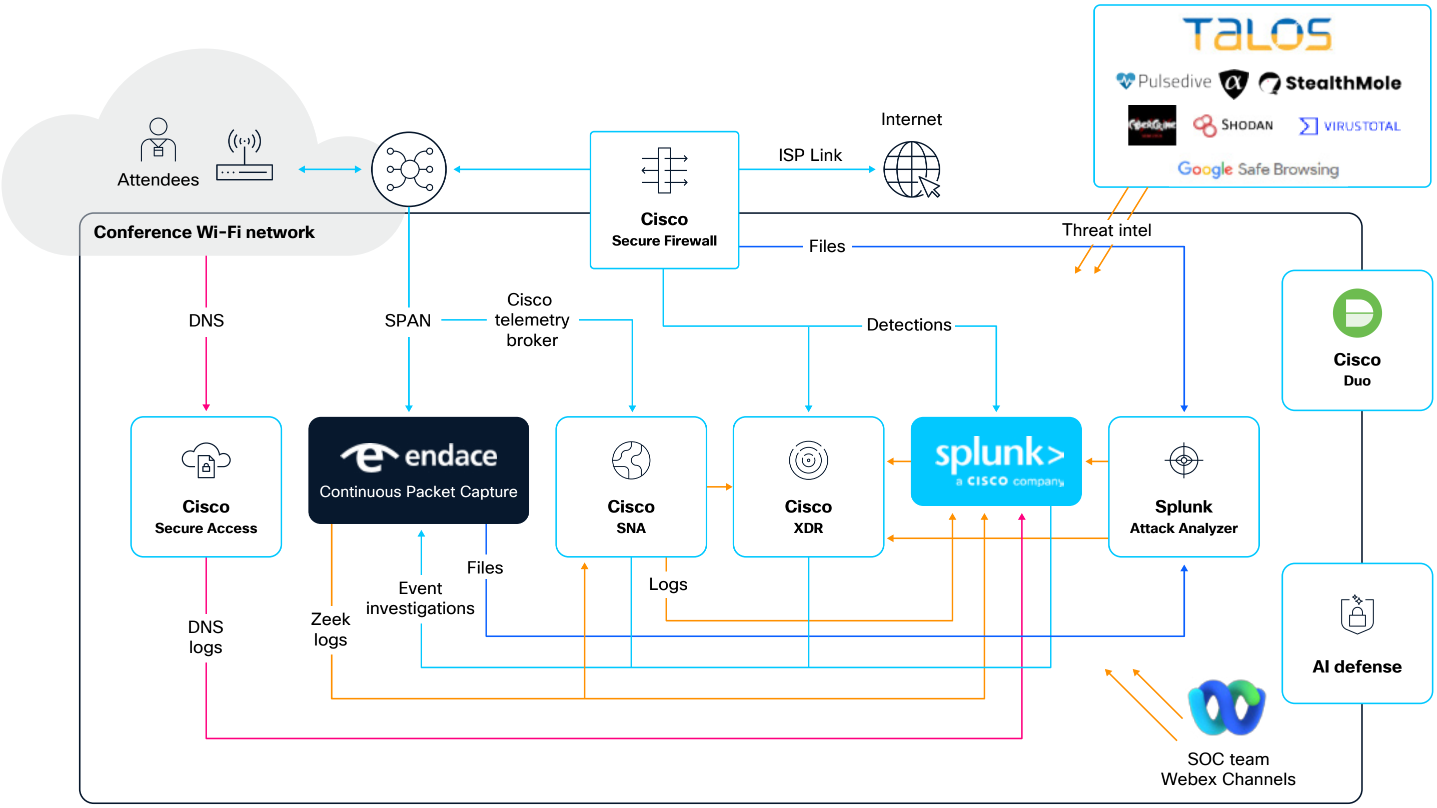


Figure 8: Combined SOC and NOC architecture at GovWare 2025.

4.2. Where the data starts

Conference Wi-Fi network

Attendee devices connect to the **conference (or event) Wi-Fi network,** which is the source of the telemetry pipeline. From here, the architecture intentionally captures three complementary views of activity:

1. Inline enforcement and logging
2. DNS security telemetry
3. Out-of-band packet/flow visibility for investigation

4.3. Inline enforcement and primary north/south telemetry

Cisco Secure Firewall

All attendee traffic egresses through the **Cisco Secure Firewall** before traversing the **ISP link** to the Internet. This makes Secure Firewall the primary inline control and one of the highest-value telemetry sources for the SOC. The firewall produces **detections** and security telemetry that feed downstream analytics and triage systems so that both incident-centric workflows (XDR) and SIEM correlation (Splunk) have access to the same authoritative network edge signals.

At most events, the perimeter firewall is deployed in the NOC and the logs are sent to the Splunk cloud tenant for correlation and detections for the SOC team. The SOC team also often deploys Intrusion Detection (IDS) on the SPAN of the traffic for refined detections and testing, such as Snort ML beta testing during the 2025 season.

4.4. DNS telemetry and control plane visibility

Cisco Secure Access

DNS is treated as a first-class signal. The diagram shows DNS traffic flowing to **Cisco Secure Access,** which generates **DNS logs** that are forwarded to Splunk for centralized analytics. This provides consistent visibility into high-signal indicators such as newly seen domains, suspicious resolution patterns, and DNS-driven command-and-control behaviors. This is especially important in an environment where payload decryption and endpoint telemetry are limited.

4.5. Authoritative packet evidence

SPAN → Endace Continuous Packet Capture

To enable high-confidence validation and retrospective analysis, the architecture mirrors traffic using **SPAN** into **Endace Continuous Packet Capture.** Endace provides the ground truth record of what occurred on the wire, enabling analysts to confirm hypotheses, reconstruct sessions where feasible, and build timelines. In the figure, Endace contributes **Zeek logs** for scalable analytics, and supports deeper investigations when packet-level evidence or analysis is required.

4.6. Network analytics at scale

Cisco Telemetry Broker → Cisco SNA

In parallel to packet capture, telemetry is routed via **Cisco Telemetry Broker** into **Cisco Secure Network Analytics (SNA).** This path exists to produce network-behavior detections and entity/network analytics at scale. SNA outputs **logs/detections** downstream so that the SOC can use SNA-derived signals both for rapid triage and for SIEM-level correlation and hunting.

4.7. The "two-plane" operations model

Cisco XDR for Tier 1 and Tier 2, Splunk for Tier 3 depth

The center of Figure 8 shows the operating model:

- **Cisco XDR (Tier 1 and Tier 2 home):** XDR consumes detections and telemetry from the security controls (e.g., Secure Firewall and SNA) and presents them in an incident-centric workflow with enrichment and automation. The event SOC team also built the first production XDR + Splunk integration in 2024, which became widely used to bring Splunk data to junior analysts for visualization and investigation. The goal is fast and consistent triage. This includes understanding scope, confidence, and executing guided actions and responses without needing to open additional consoles.
- **Splunk (Tier 3 hunting and correlation plane):** Splunk aggregates the broader set of logs (Zeek metadata, DHCP, detections) to enable flexible searching, custom correlation, and hypothesis-driven hunting. Tier 3 analysts use Splunk ES to build/refine detections, tune noise, and run deeper analytics that may not be feasible in Cisco XDR alone.

Importantly, the arrows in the figure are bidirectional in places because this is not a one-way "log sink." XDR and Splunk reinforce each other: Tier 1 and Tier 2 can pivot into Splunk when deeper querying is needed, and Tier 3 outputs can be operationalized back into XDR through improved context, detections, and automation.

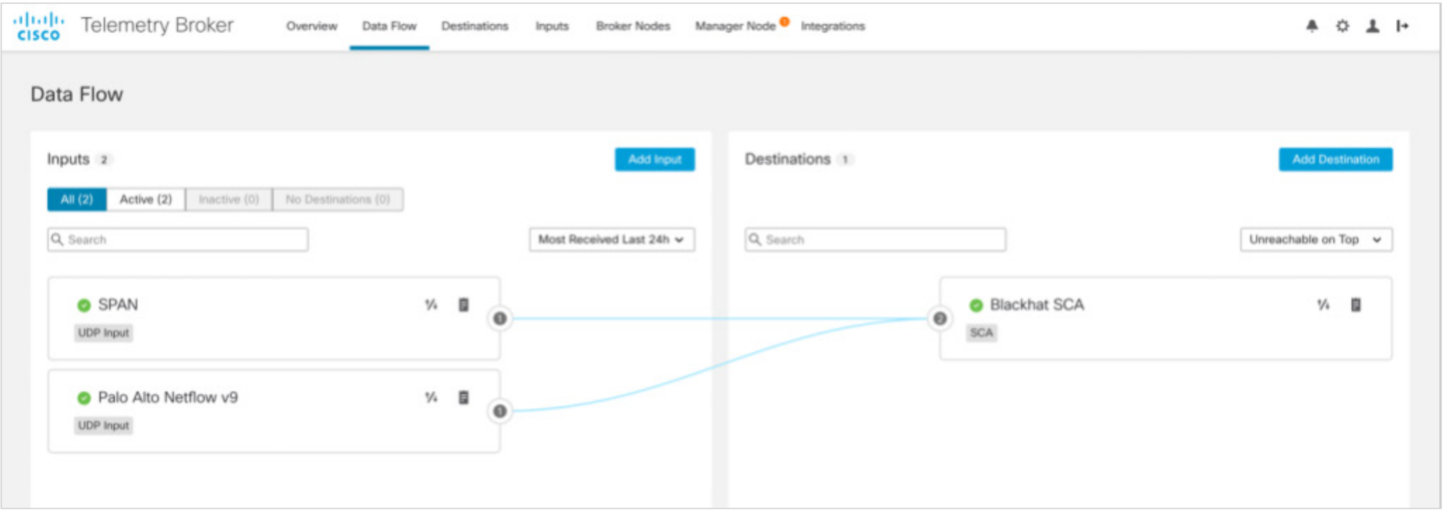


Figure 9: Cisco telemetry broker data flow.

4.8. Payload-centric enrichment and detonation

Splunk Attack Analyzer

When investigations require file or URL analysis, Figure 8 shows files flowing into **Splunk Attack Analyzer.** This enables detonation, static/dynamic analysis, and verdict-driven enrichment that can be referenced during triage and hunting. This is particularly useful for event networks where endpoint agents may not exist, but files can still be extracted or observed via network/security controls and then analyzed safely within a sandbox.

Splunk Attack Analyzer is an ‘engine-of-engines’, and sends supported file types to **Secure Malware Analytics** (Threat Grid), for detonation and investigation of behavioral indicators. A past tagline of Threat Grid was “detonate your malware on our network instead of yours.” The glovebox feature of SMA allows analysts to investigate a URL or file sample in a safe virtual environment, without infecting themselves, while a report and investigation video is automatically generated.

4.9. Threat intelligence as a shared enrichment layer

Talos + third parties

The top-right of Figure 8 explicitly calls out **Threat Intelligence** (e.g., **Cisco Talos** plus complementary sources like VirusTotal and partners shown). This intelligence layer enriches indicators, destinations, and file reputation across the stack so analysts can confidently validate maliciousness and prioritize accordingly. This eliminates the need to rely on manual, one-off lookups during high-tempo operations.

4.10. Analyst access and coordination

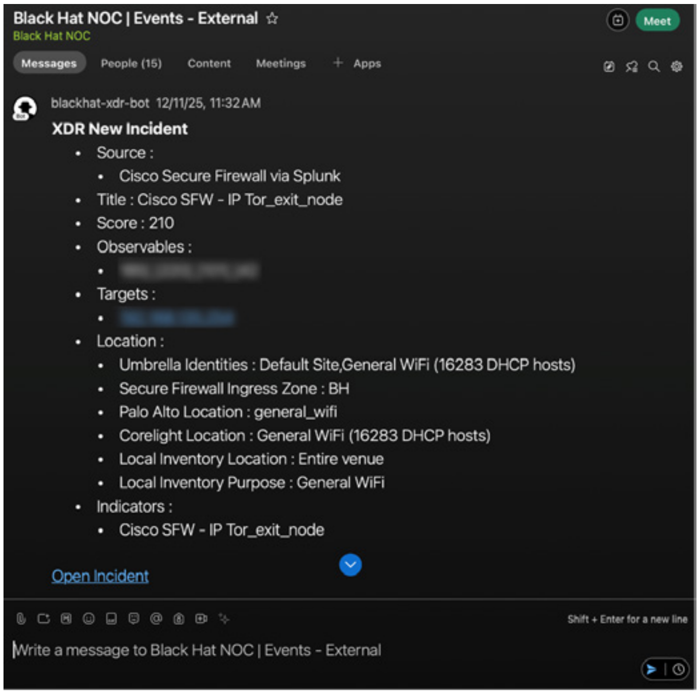
Cisco Duo + Webex Channels

Operationally, the SOC is only as effective as its access controls and collaboration loops. **Cisco Duo** provides strong authentication for the SOC toolchain, while the diagram shows outputs and updates flowing into **SOC Team Cisco Webex Channels** to support shared awareness, handoffs, and coordinated response across the SOC/NOC boundary.

To make collaboration actionable, not just informational, we integrate **chat bots** directly into these Webex channels. These bots are connected to key security tools via **APIs,** allowing them to:

1. Push scheduled and on-demand reports
2. Post incident notifications and enrichment as detections occur
3. Perform real-time lookups (e.g., an IP/domain/URL) to return additional context from the underlying platforms

By embedding these capabilities where the team is already communicating, investigation pivots and enrichment outputs are shared in real time, enabling analysts to provide input, validate hypotheses, and coordinate next steps collaboratively without requiring everyone to pivot into separate consoles.


Black Hat NOC | Events - External ☆
Black Hat NOC
Meet
Messages
People (15)
Content
Meetings
+ Apps
Shift + Enter for a new line
Write a message to Black Hat NOC | Events - External

blackhat-xdr-bot 12/11/25, 11:32 AM

XDR New Incident

- Source :
  - Cisco Secure Firewall via Splunk
- Title : Cisco SFW - IP Tor_exit_node
- Score : 210
- Observables :
  - [redacted]
- Targets :
  - [redacted]
- Location :
  - Umbrella Identities : Default Site,General WiFi (16283 DHCP hosts)
  - Secure Firewall Ingress Zone : BH
  - Palo Alto Location : general_wifi
  - Corelight Location : General WiFi (16283 DHCP hosts)
  - Local Inventory Location : Entire venue
  - Local Inventory Purpose : General WiFi
- Indicators :
  - Cisco SFW - IP Tor_exit_node

Open Incident

Figure 10: Incident notification from Webex chatbot

5. Key architectural components

5.1. Hardware foundation

Our event SOC is built on a portable, pre-configured “SOC in a Box” hardware stack designed to be rolled into a venue, cabled to the Network Operations Center (NOC), and begin producing actionable telemetry immediately. The primary design goal is speed-to-visibility under conference deployment timelines. The SOC is generally deployed in two days, with rapid setup explicitly enabled by the SOC in a Box approach and its pre-integrated connectivity to Splunk Enterprise Security and Cisco Security Cloud.

Figure 11 illustrates the physical implementation: a half-rack road case on wheels containing the core network/security controls, packet capture, and compute needed to operate both SOC and NOC-adjacent workflows. In practice, the “clean” rack layout (left) is how we build and validate the system prior to shipping; the “in-field” photo (right) reflects a realistic event state where we had two hours to wire up the ‘SOC in a Box’, with uplinks, SPAN/TAP feeds, patching, and cabling connected.

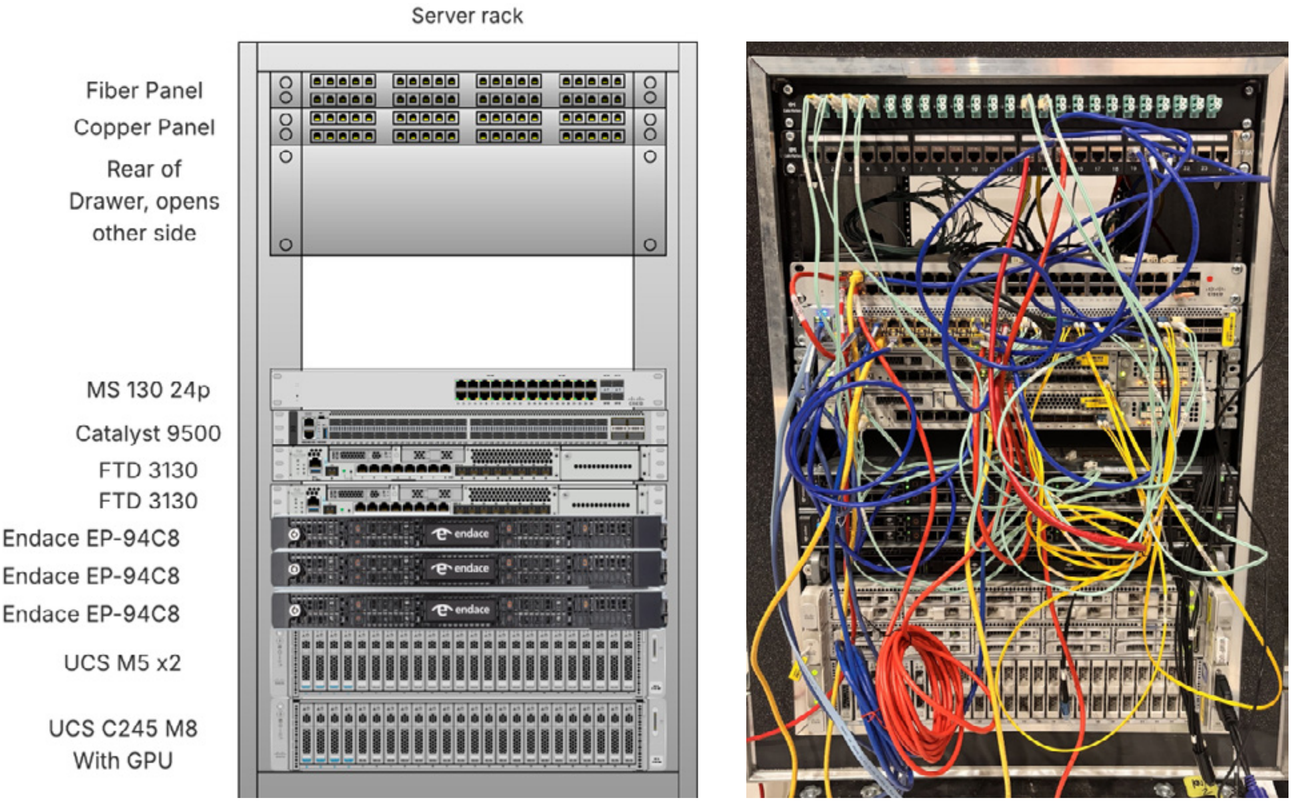


Figure 11: SOC in a Box design and real world deployment in two hours time.

Design pattern: portable rack + standardized ports + pre-validated data paths

The hardware foundation is engineered around repeatable, known-good data flows that match the SOC architecture. These include inline edge visibility/control, continuous full packet capture, and high-throughput telemetry forwarding to cloud analytics platforms. At these events the SOC team needs to collaborate and integrate with the NOC. This means connecting a SPAN feed to our SOC in a Box, deploying Secure Access DNS security, inspecting traffic with Secure Firewall. Endace then generates metadata (including Zeek logs) for Splunk ES, and streams reconstructed file content to Splunk Attack Analyzer for detonation/analysis.

Core rack components

Below is the standard bill-of-materials as represented in the rack rendering, with each component's role in the overall system:

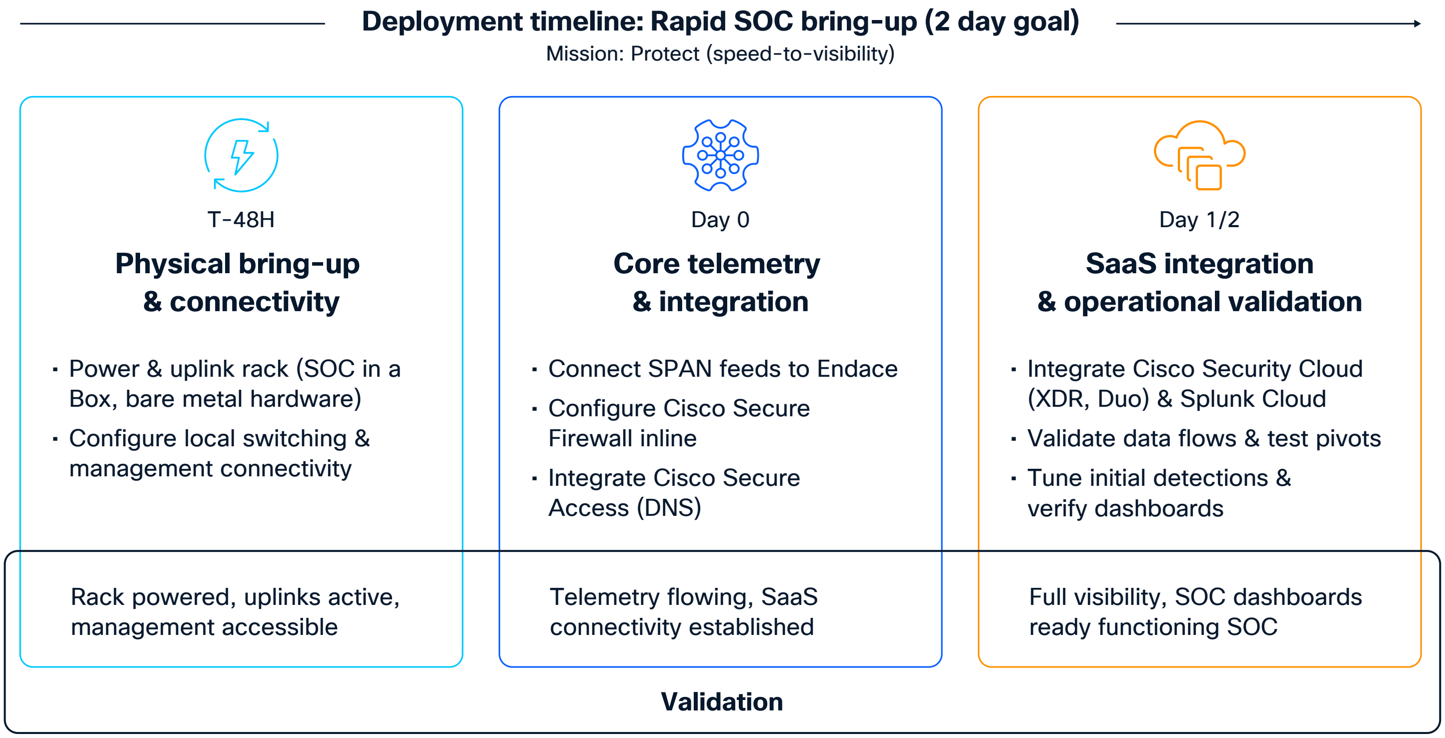
- **Rack/road case (half rack on wheels):** Portable enclosure for shipping, rapid onsite placement, and safe operation in constrained venue spaces.
- **Drawer:** Spare optics, patch cables, console cables, labeling supplies, and small tools required for rapid cutovers and troubleshooting.
- **PDU:** Centralized power distribution for all devices in the rack, simplifying venue power integration and recovery procedures.
- **Meraki MS130 (24-port access switching):** Local access switching for SOC infrastructure, staging, and management connectivity (and/or local AP connectivity depending on event needs).
- **Catalyst 9500 (core/aggregation switch):** High throughput switching for uplinks, SPAN aggregation, and interconnect between firewall, capture, and compute.
- **Copper patch panel:** Standardized RJ45 presentation for 1G copper endpoints, management ports, and venue handoffs where fiber is not available.
- **Cisco Secure Firewall Threat Defense 3130 (x2):** Inline enforcement and north/south telemetry at the conference edge; deployed in high availability mode to avoid a single point of failure and support event uptime requirements.
- **Fiber patch panel:** Standardized presentation for optical uplinks (10/25G) to venue infrastructure, taps, and SPAN handoffs.
- **Endace appliances (Endace 1/Endace 2):** Always-on full packet capture and investigation-grade wire data, plus Zeek metadata generation and support for file reconstruction workflows to sandbox tooling. Endace is the embodiment of the phrase "PCAP or it didn't happen", meaning show me the network evidence (not just the logs, or I cannot confirm the event happened in the manner hypothesized. Endace continuously records traffic so analysts can reconstruct timelines, validate detections, and answer questions that flow logs alone cannot reliably resolve. Endace functions as an investigation pivot point across the SOC toolchain. Analysts can quickly pivot directly from Cisco XDR, Splunk, SNA, and Cisco Secure Firewall into packet capture to confirm or refute hypotheses immediately at the packet level
- **UCS C245 M8 with GPU (compute):** Local compute for event services and virtualization needs (e.g., telemetry broker components, management utilities, and supporting infrastructure services where required). Added to support AI-driven and compute-heavy workloads aligned to modern SOC operations.
- **UCS C220 M5 x2 (compute):** Spare compute for additional virtual machines such as vCenter, automation remote, secure access resource connector, and others. Typically used for non-critical infrastructure.

Optics, cabling, and spares kit (what makes it deployable)

To ensure the rack can interconnect with diverse venue environments without last-minute procurement, the SOC in a Box is shipped with a standardized connectivity kit, including:

- Single-mode 10G SFPs, multi-mode 10G SFPs, multi-mode 25G SFPs, and 1G copper transceivers (GLC-T) to adapt to common venue uplink standards.
- Cat5e and Cat6A copper, plus single-mode and multi-mode fiber patch cables sized for typical NOC handoffs, SPAN/TAP drops, and rack-internal patching.

This hardware foundation is intentionally “boring” in the best way: it is repeatable, labeled, and designed to minimize onsite configuration while maximizing the probability that core SOC telemetry (edge logs, DNS logs, packet capture, metadata, and derived detections) is online quickly and consistently across events.



Deployment timeline: Rapid SOC bring-up (2 day goal)

Mission: Protect (speed-to-visibility)

T-48H

Physical bring-up & connectivity

- Power & uplink rack (SOC in a Box, bare metal hardware)
- Configure local switching & management connectivity

Rack powered, uplinks active, management accessible

Day 0

Core telemetry & integration

- Connect SPAN feeds to Endace
- Configure Cisco Secure Firewall inline
- Integrate Cisco Secure Access (DNS)

Telemetry flowing, SaaS connectivity established

Day 1/2

SaaS integration & operational validation

- Integrate Cisco Security Cloud (XDR, Duo) & Splunk Cloud
- Validate data flows & test pivots
- Tune initial detections & verify dashboards

Full visibility, SOC dashboards ready functioning SOC

Validation

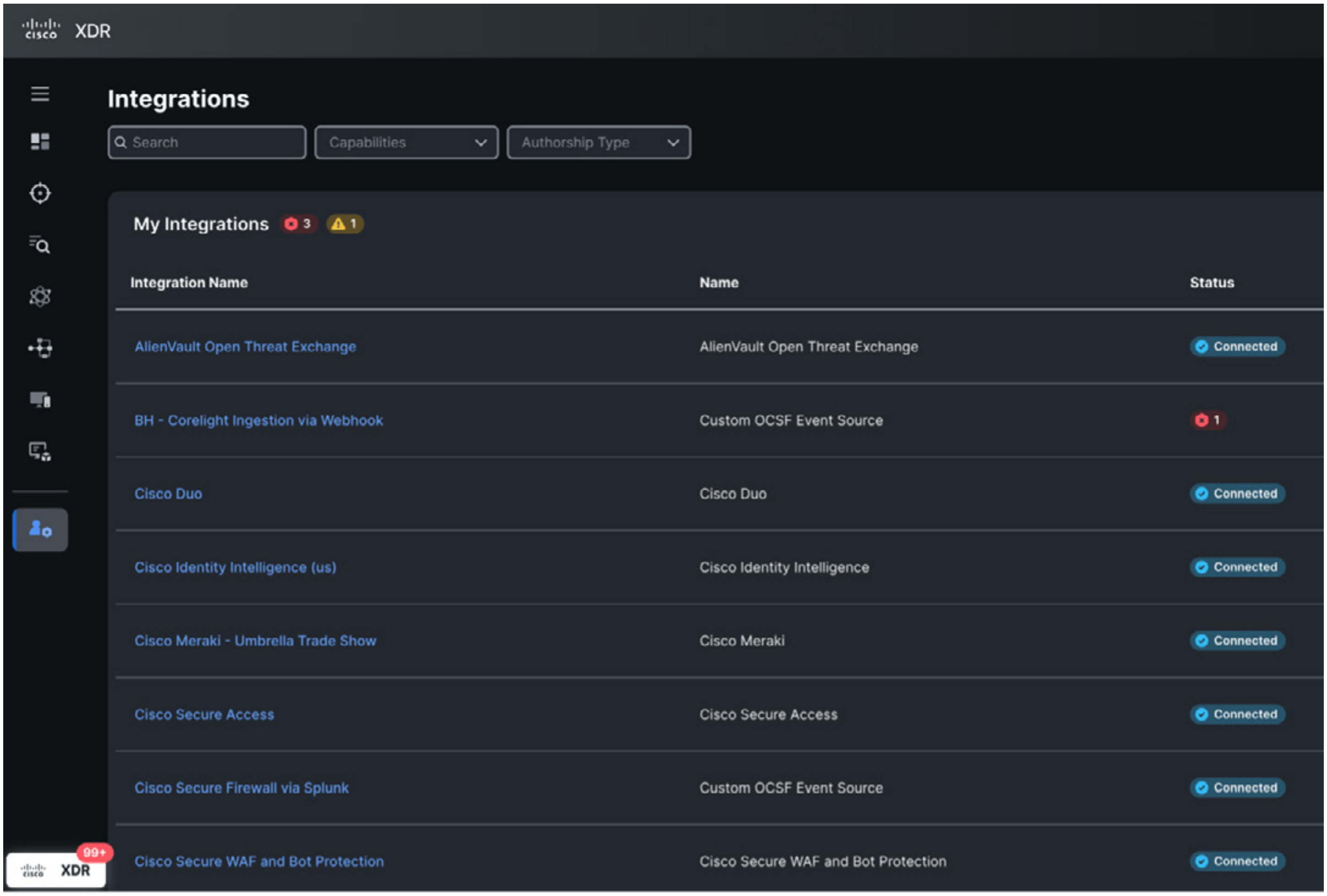
Figure 12: Rapid SOC deployment.

5.2. Cisco Security Cloud software

The Cisco Security Cloud forms the backbone of threat prevention, detection, and user protection for our event SOC deployments. Because conference environments contain large volumes of unmanaged endpoints, Cisco Security Cloud capabilities are intentionally anchored in network-centric visibility (edge, DNS, flow/behavior, packet evidence) and cloud-delivered analytics and response, allowing the SOC to detect and investigate threats even when endpoint coverage is limited.

Cisco XDR (Extended Detection and Response)

- **Role:** Primary interface for Tier 1 and Tier 2 SOC analysts for incident investigation, rapid triage, and orchestrated response. Serves as the central hub that consolidates security outcomes across the SOC toolchain into an incident-centric workflow.
- **Capabilities:**
  - Aggregates telemetry and detections from integrated security controls (e.g., Cisco Secure Firewall, Cisco SNA, DNS/security telemetry, and other sources), enriches incidents with threat intelligence, and provides investigative timelines and entity context.
  - Correlated detections from multiple security controls into incidents. Enables automation via workflows to reduce analyst toil (enrichment, pivots, notifications, and repeatable response actions).



My Integrations 3 ⚠ 1

Integration Name	Name	Status
AlienVault Open Threat Exchange	AlienVault Open Threat Exchange	✓ Connected
BH - Corelight Ingestion via Webhook	Custom OCSF Event Source	1
Cisco Duo	Cisco Duo	✓ Connected
Cisco Identity Intelligence (us)	Cisco Identity Intelligence	✓ Connected
Cisco Meraki - Umbrella Trade Show	Cisco Meraki	✓ Connected
Cisco Secure Access	Cisco Secure Access	✓ Connected
Cisco Secure Firewall via Splunk	Custom OCSF Event Source	✓ Connected
Cisco Secure WAF and Bot Protection	Cisco Secure WAF and Bot Protection	✓ Connected

Figure 13: XDR integrations.

  - Supports API-based integrations with third-party tools (e.g., non-Cisco firewalls) and provides direct pivots into supporting evidence sources such as packet capture and SIEM investigations.
  - Additionally, Cisco XDR offers a post exploit DFIR capability called XDR Forensics, which could be leveraged for devices owned by the event organizers.
- **Integration configuration:**
  - Cisco XDR is integrated with a multitude of technologies. These integrations are called Integration modules and each integration module offers different capabilities.
  - Some integrations offer dashboard tiles and on-demand enrichment queries while others offer data ingest and response actions.
  - Integration modules for other Cisco technologies are generally very simple to configure, requiring only a few clicks to enable and authorize the integrations.
  - Modules for third party technologies generally require copy and pasting an API into XDR to add the integration.
  - Custom integration modules that are created by our SOC team are typically hosted in AWS and added via a custom module type manually added to Cisco XDR. Any custom code created for our own integrations is stored on GitHub to ensure it can be reused and improved upon by others.

Cisco Secure Access

- **Role:** Cloud-delivered Zero Trust Network Access (ZTNA) and DNS security for event networks. Provides high-signal DNS visibility and enforcement in environments where endpoint controls and decryption are limited.
- **Capabilities:**
  - Delivers DNS security enforcement by blocking access to malicious destinations (malware, phishing, C2) and generates DNS logs for centralized analytics and threat hunting.
  - Supports client attribution for DNS requests and control of DNS forwarding to preserve visibility and consistency.
  - Provides application discovery insights to help the SOC understand usage trends and identify anomalous application behavior.
  - Where required, can restrict encrypted DNS techniques to improve DNS observability and reduce blind spots.
- **Integration configuration:**
  - To ensure all DNS requests are routed through Secure Access we deploy two virtual appliances. These are deployed in ESXi in a pair, one for the primary DNS server and one for secondary. The IP addresses of our two virtual appliances are handed out in the DHCP scope for the attendee and management networks.
  - DNS is a critical piece of an operational network so the public Secure Access resolver IP is used as a tertiary DNS server in case something happens to the on-prem virtual appliances the public resolved will be used and we will still have DNS visibility.
  - The main benefit of using virtual appliances is that we have internal IP visibility of which client made which DNS requests. This attribution is critical for the XDR analytics correlation engine to stich alerts from different sources together. Secure Access is integrated with Cisco XDR to bring DNS log data into the data analytics pipeline using a simple copy and paste of API keys.

Cisco Duo & identity intelligence

- **Role:** Identity Provider (IdP), Multi-Factor Authentication (MFA), Single Sign-On (SSO), and identity governance for SOC tooling access. Provides the identity plane for SOC analysts and administrators in short-lived event environments.
- **Capabilities:**
  - Secures access to SOC tools (cloud and on-prem) through strong authentication and a curated SSO portal.
  - Simplifies user and application management through Duo Directory and enables granular administrative separation through Administrative Units and Roles.
  - Supports rapid onboarding so analysts can access required tools within minutes of joining the SOC.
  - Figure 14 below illustrates the event SOC model: a centralized application directory used to launch SOC/NOC tools (e.g., Cisco Security Cloud Control, XDR, Endace, Splunk Cloud) under consistent authentication and access controls.
- **Integration configuration:**
  - SAML authentication is configured on various technologies to ensure logging in is seamless.
  - An SSO login link is created using Duo directory with tiles for each console to have a central place to access the full toolset.
  - Duo and Cisco Identity Intelligence are linked to our Security Cloud Control portal then we add the integrations directly into XDR.

The Black Hat NOC/SOC is the first customer of Duo Directory. You can learn more about their journey from proof-of-concept to beta and full deployment here.

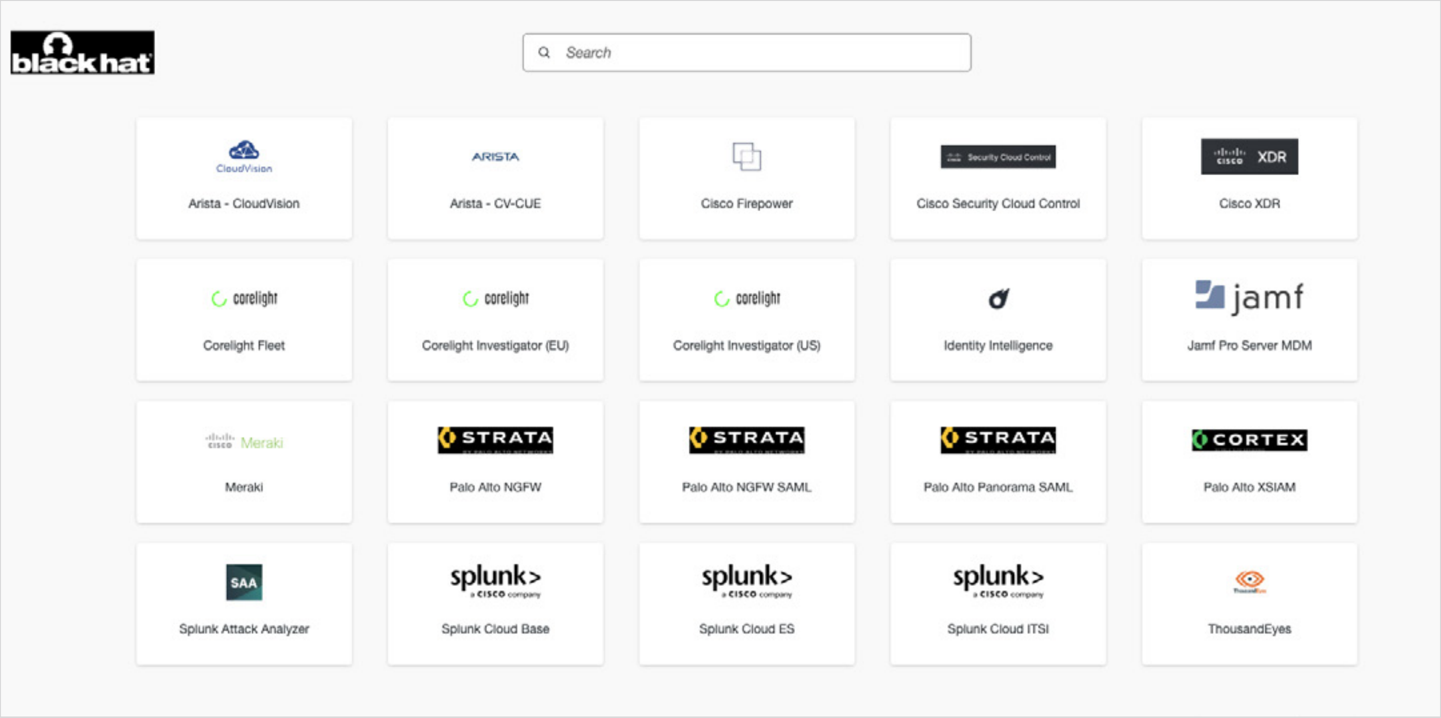
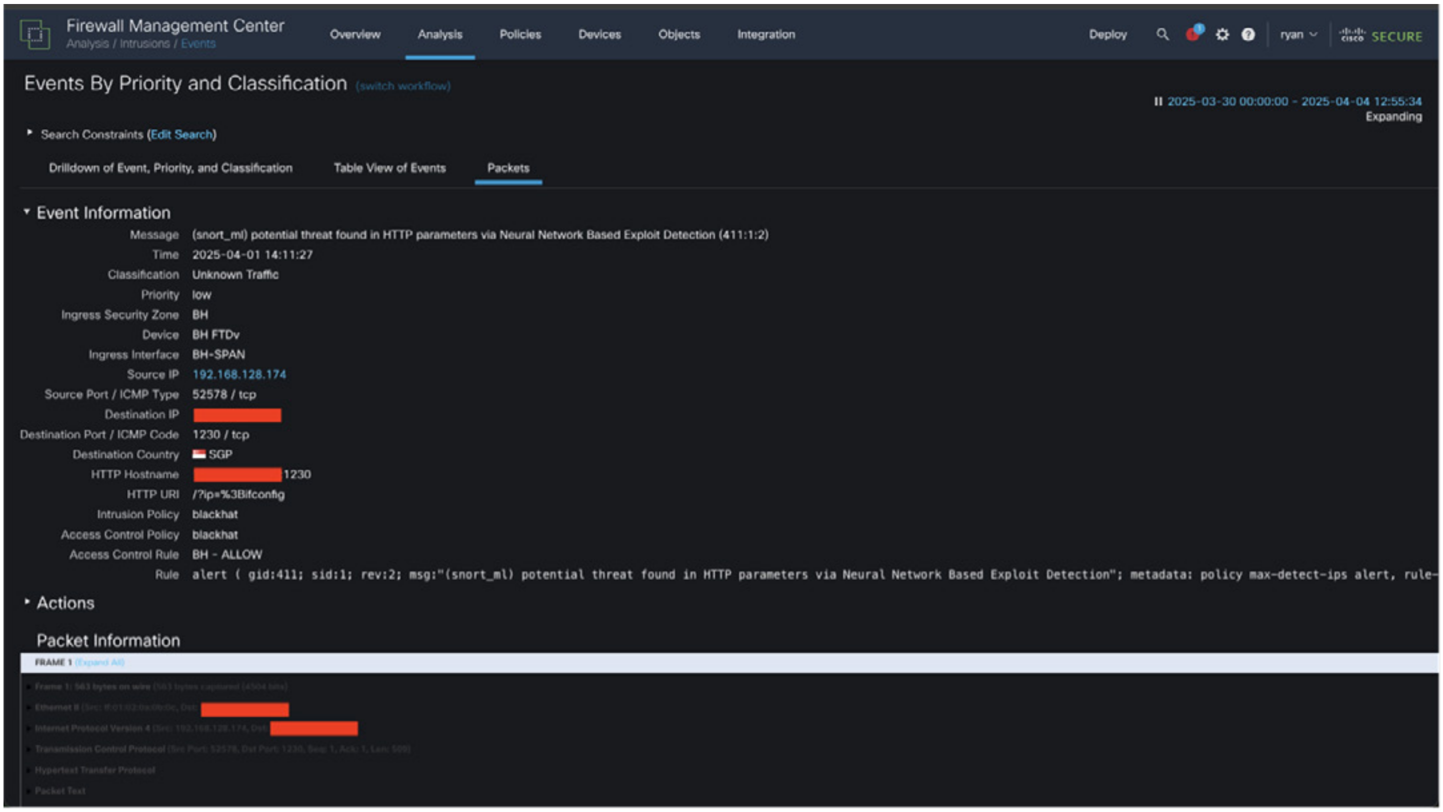


Figure 14: Duo Directory at Black Hat NOC/SOC.

Cisco Secure Firewall/Firepower Threat Defense (FTD)

- **Role:** Primary inline security enforcement and visibility control at the event edge. Provides next-generation firewall capabilities and is a foundational telemetry source for detections and investigations.
- **Capabilities:**
  - Delivers inline protection and produces high-value network security logs for correlation and hunting.
  - Provides IDS/IPS capabilities that remain critical at events for detecting known exploit patterns and reducing exposure to commodity attacks. Encrypted Visibility Engine (EVE) enhances visibility into encrypted traffic without decryption using encrypted traffic analytics (e.g., TLS fingerprinting and application identification).
  - Leverages advanced detection techniques including SnortML (machine learning) to improve fidelity for common attack classes (e.g., injection patterns).
  - Supports investigation pivots into session/log detail and supplies detections to both Cisco XDR and Splunk.
- **Integration configuration:**
  - Our SOC team uses on-prem Firewall Management Center (FMC) to manage our pair of High-Availability (HA) Firewalls.
    - In today's modern world we would typically choose to manage as many technologies as possible using SaaS based solutions. However, in this case cloud-based firewall management does not have the same feature parity as on-prem management. For example, one such capability we rely on with our on-prem management is creating custom snort rules. From a general perspective, our configurations are quite simple.



Events By Priority and Classification (switch workflow)

2025-03-30 00:00:00 - 2025-04-04 12:55:34
Expanding

Search Constraints (Edit Search)

Drilldown of Event, Priority, and Classification | Table View of Events | Packets

Event Information

Message (snort_ml) potential threat found in HTTP parameters via Neural Network Based Exploit Detection (411:1:2)
Time 2025-04-01 14:11:27
Classification Unknown Traffic
Priority low
Ingress Security Zone BH
Device BH FTDv
Ingress Interface BH-SPAN
Source IP 192.168.128.174
Source Port / ICMP Type 52578 / tcp
Destination IP [redacted]
Destination Port / ICMP Code 1230 / tcp
Destination Country SGP
HTTP Hostname [redacted]1230
HTTP URI /?ip=%3Bifconfig
Intrusion Policy blackhat
Access Control Policy blackhat
Access Control Rule BH - ALLOW
Rule `alert ( gid:411; sid:1; rev:2; msg:"(snort_ml) potential threat found in HTTP parameters via Neural Network Based Exploit Detection"; metadata: policy max-detect-ips alert, rule-`

Actions

Packet Information

FRAME 1 (Expand All)

Frame 1: 563 bytes on wire (563 bytes captured (4504 bits)
Ethernet II (Src: ff:01:02:0a:0b:0c, Dst: [redacted]
Internet Protocol Version 4 (Src: 192.168.128.174, Dst: [redacted]
Transmission Control Protocol (Src Port: 52578, Dst Port: 1230, Seq: 1, Ack: 1, Len: 509)
Hypertext Transfer Protocol
Packet Text

Figure 15: Firewall Management Center (FMC) SnortML event.

  - We enable network discovery, security intelligence, file policy, alert only IPS policy, basic access control policy to allow traffic, a simple NAT policy for internet access and enable EVE and SnortML.
  - We may add specific rules or configurations based on different event requirements, but the basic configurations are mostly the same from event to event.
- Security Cloud Control is used to integrate the on-prem firewall to our cloud services to collect logs and provide visibility into Cisco XDR. In addition, we send the Firewall logs to a Splunk heavy forwarder to have them ingested into Splunk Cloud.

Cisco Talos

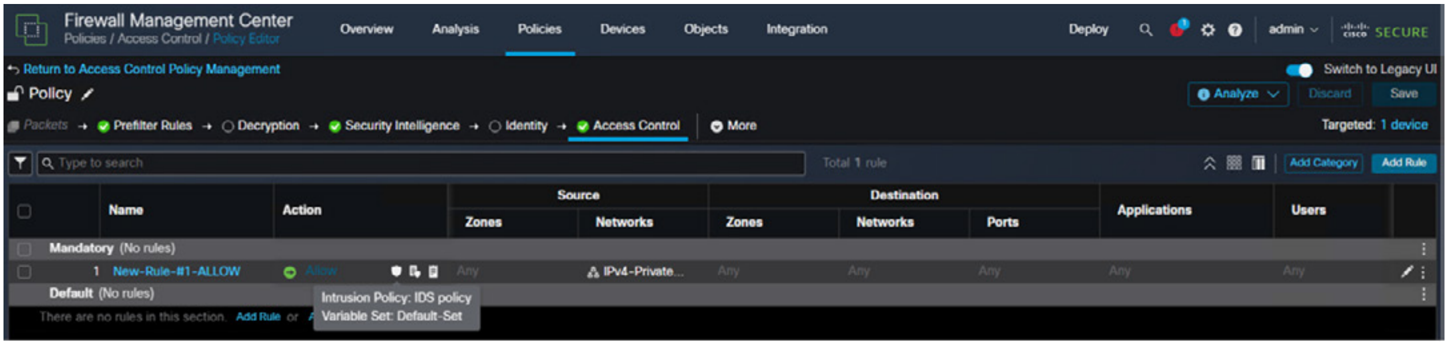
- **Role:** Global threat intelligence organization that supplies shared intelligence used across Cisco Security Cloud and the event SOC stack.
- **Capabilities:** Provides real-time threat intelligence and reputation services to enrich XDR incidents and power detections across Cisco security controls. Enhances confidence scoring across destinations, files, and observed behaviors.
- **Integration configuration:** Talos threat intelligence is ingrained in Cisco XDR and Splunk providing trusted threat intelligence across the ecosystem.

Cisco Secure Malware Analytics (formerly Threat Grid)

- **Role:** Advanced malware sandboxing and verdict enrichment to support file-based investigations.
- **Capabilities:**
  - Performs dynamic analysis of suspicious files identified through network observation and investigation workflows (e.g., content extracted or reconstructed from packet capture and related analysis pipelines).
  - Produces behavior-based verdicts and artifacts that can be used to validate hypotheses, scope potential impact, and enrich incidents and hunts.
  - The glovebox capability allows users to interact with sandbox VMs to analyze payload behaviors in real time.
- **Integration configuration:**
  - Secure Malware analytics is integrated with the Firewalls directly for file submission. In addition, a Secure Malware analytics API key is configured in Splunk Attack Analyzer and Cisco XDR for multiple purposes including sandbox file submissions, investigation enrichment, threat intelligence and one-click URL submissions.

ThousandEyes

- **Role:** Network observability and performance monitoring to ensure attendee experience while


Firewall Management Center
Policies / Access Control / Policy Editor
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
admin
SECURE
Return to Access Control Policy Management
Switch to Legacy UI
Policy
Analyze
Discard
Save
Packets → Prefilter Rules → Decryption → Security Intelligence → Identity → Access Control
More
Targeted: 1 device
Type to search
Total 1 rule
Add Category
Add Rule

	Name	Action	Source		Destination			Applications	Users
			Zones	Networks	Zones	Networks	Ports		
	Mandatory (No rules)								
1	New-Rule-#1-ALLOW	Allow	Any	IPv4-Private...	Any	Any	Any	Any	Any
	Default (No rules)								

There are no rules in this section. Add Rule or A

Intrusion Policy: IDS policy
Variable Set: Default-Set

Figure 16: Firewall access control policy.

detecting network anomalies and upstream issues. ThousandEyes builds dashboards that compare latency/throughput across SaaS targets and internal conference services to quickly highlight where performance is breaking down.

- **Capabilities:**
  - Monitors network connectivity, performance, and availability of internal and external resources.
  - Helps distinguish true security incidents from ISP/SaaS impairments and routing anomalies, and provides independent visibility into critical dependencies.
  - Integrates with Splunk for centralized alerting, metrics, and operational correlation between SOC and NOC functions.
- **Integration configuration:** ThousandEyes integration at Black Hat is typically configured by provisioning Enterprise Agents (e.g., Raspberry Pi/Orange Pi) from the ThousandEyes UI, then registering each agent to the ThousandEyes account by pasting the Access/Account Group token in the agent GUI and setting baseline network items.

AI defense

- **Role:** Security controls for the SOC's AI-related infrastructure and AI-enabled workflows (cloud services and on-prem AI pods where applicable).
- **Capabilities:** Protects AI workloads and supporting infrastructure through secure configuration and monitoring, reduces risk of misuse, and supports safe adoption of AI-assisted SOC workflows as automation and AI analytics become more embedded in event operations.
- **Integration configuration:** Enable Cisco AI Defense in the Event SOC's Security Cloud tenancy, onboard approved AI services plus identity and any AI pods and set policies and export telemetry so AI usage is monitored and controlled.

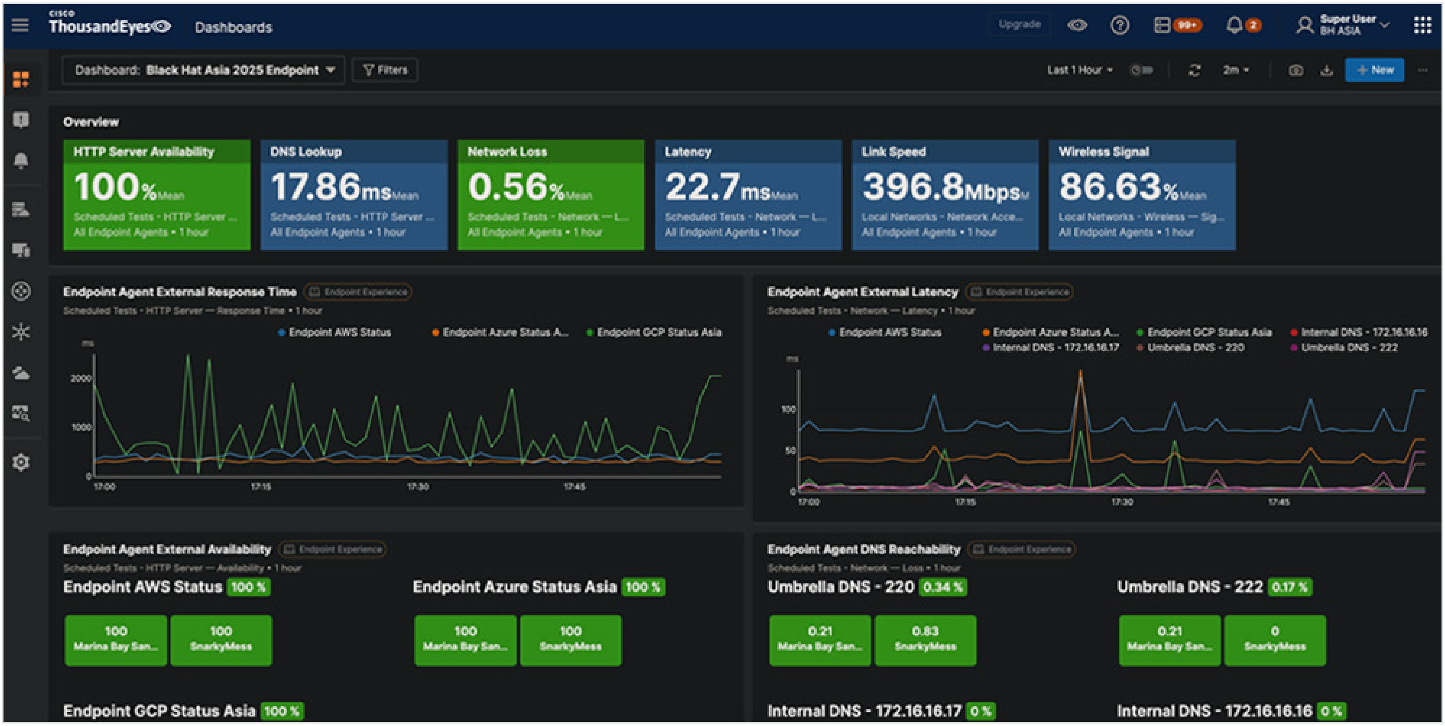

cisco ThousandEyes
Dashboards
Upgrade
99+
2
Super User
BH ASIA
Dashboard: Black Hat Asia 2025 Endpoint
Filters
Last 1 Hour
2m
+ New
Overview
HTTP Server Availability
100%Mean
Scheduled Tests · HTTP Server ...
All Endpoint Agents • 1 hour
DNS Lookup
17.86msMean
Scheduled Tests · HTTP Server ...
All Endpoint Agents • 1 hour
Network Loss
0.56%Mean
Scheduled Tests · Network — L...
All Endpoint Agents • 1 hour
Latency
22.7msMean
Scheduled Tests · Network — L...
All Endpoint Agents • 1 hour
Link Speed
396.8MbpsM
Local Networks · Network Acce...
All Endpoint Agents • 1 hour
Wireless Signal
86.63%Mean
Local Networks · Wireless — Sig...
All Endpoint Agents • 1 hour
Endpoint Agent External Response Time
Endpoint Experience
Scheduled Tests · HTTP Server — Response Time • 1 hour
Endpoint AWS Status
Endpoint Azure Status A...
Endpoint GCP Status Asia
ms
2000
1000
0
17:00
17:15
17:30
17:45
Endpoint Agent External Latency
Endpoint Experience
Scheduled Tests · Network — Latency • 1 hour
Endpoint AWS Status
Endpoint Azure Status A...
Endpoint GCP Status Asia
Internal DNS - 172.16.16.16
Internal DNS - 172.16.16.17
Umbrella DNS - 220
Umbrella DNS - 222
ms
100
50
0
17:00
17:15
17:30
17:45
Endpoint Agent External Availability
Endpoint Experience
Scheduled Tests · HTTP Server — Availability • 1 hour
Endpoint AWS Status 100 %
100 Marina Bay San...
100 SnarkyMess
Endpoint Azure Status Asia 100 %
100 Marina Bay San...
100 SnarkyMess
Endpoint GCP Status Asia 100 %
Endpoint Agent DNS Reachability
Endpoint Experience
Scheduled Tests · Network — Loss • 1 hour
Umbrella DNS - 220 0.34 %
0.21 Marina Bay San...
0.83 SnarkyMess
Umbrella DNS - 222 0.17 %
0.21 Marina Bay San...
0 SnarkyMess
Internal DNS - 172.16.16.17 0 %
Internal DNS - 172.16.16.16 0 %

Figure 17: ThousandEyes agent dashboard.

5.3. Splunk Cloud Platform software

The Splunk Cloud Platform serves as a unified threat detection, investigation, response (TDIR) and analytics engine for security operations.

Splunk Cloud Platform

- **Role:** Scalable, cloud-based platform for ingesting, indexing, and analyzing machine data.
- **Capabilities:** A vendor agnostic tool that can aggregate millions of event data from 2000+ product vendors including Cisco products (Secure Firewall, XDR, Secure Access) and third-party sources (Endace, Corelight, Palo Alto, JAMF, DHCP), providing a unified view for security analysts.
- **Integration configuration:**
  - Configure Splunk Cloud data inputs using Splunk Connect for Syslog, HTTP Event Collector, and vendor add-ons, then validate parsing, field extractions, and CIM mapping so detections and dashboards work consistently across sources.
  - Route high-volume telemetry through heavy forwarders, utilize a deployment server for configuration management, and standardize index naming, retention, and sourcetype conventions for repeatable event deployments.

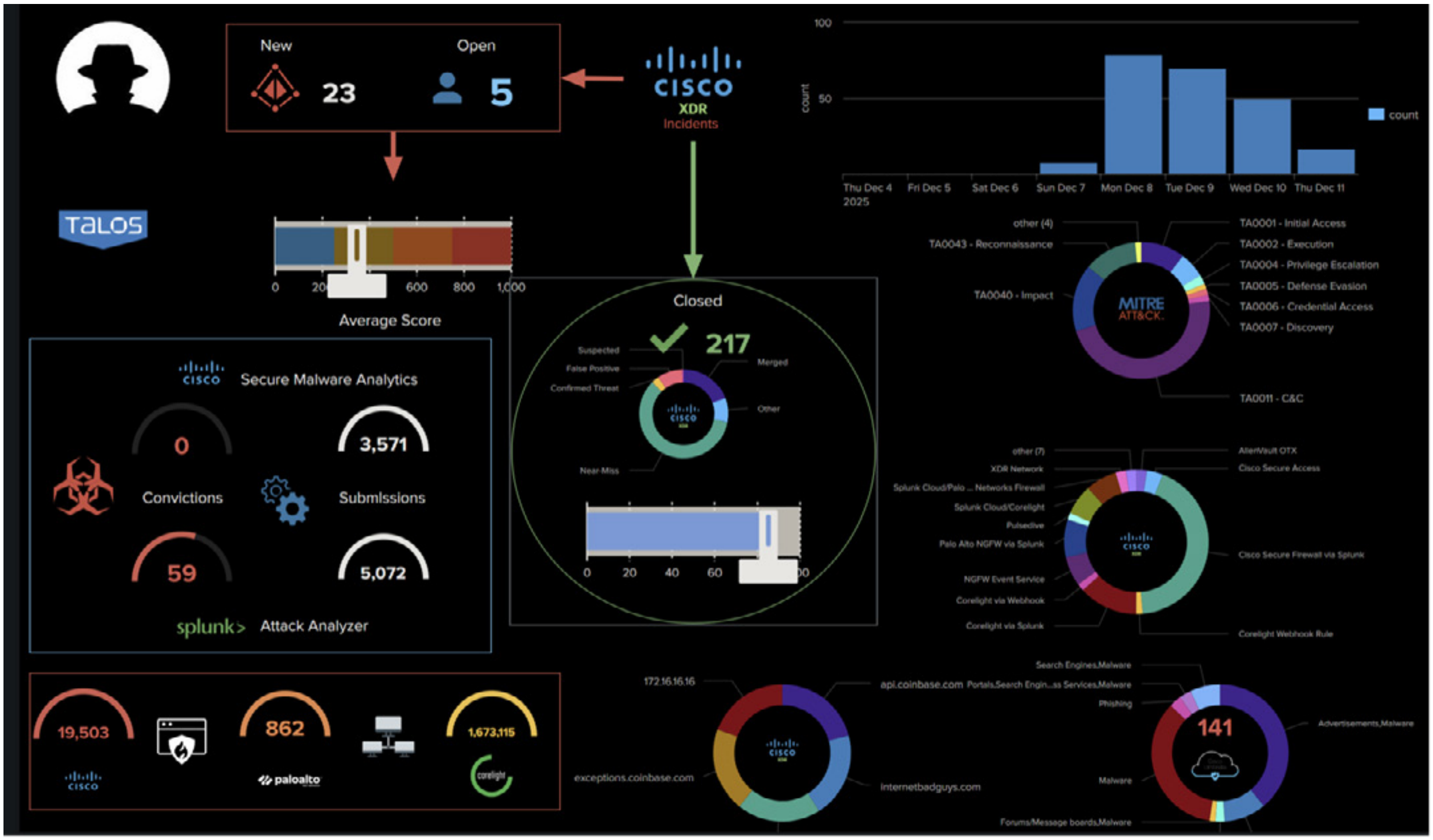


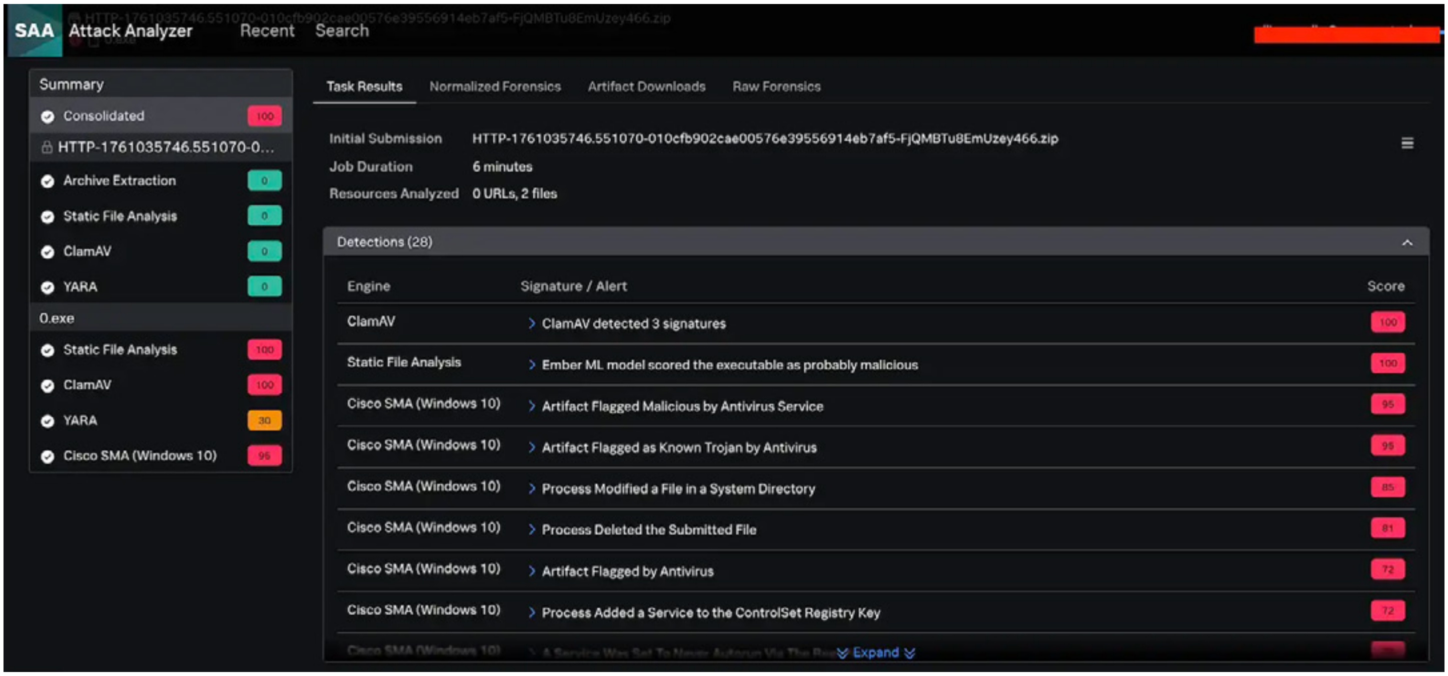
Figure 18: Custom dashboard in Splunk.

Splunk Enterprise Security (ES)

- **Role:** Security Information and Event Management (SIEM) for advanced threat detection and response, available to all SOC analysts and used extensively by threat hunters.
- **Capabilities:** A unified Threat Detection, Investigation, and Response (TDIR) Platform, integrated with Splunk SOAR. ES correlates all events across your organization and provides powerful highly customizable detections and dashboards (e.g., SOC Triage Center, Packet Peeker's Prize Board), supporting complex queries, and integrates with Endace for packet data.
- **Integration configuration:** Enable Splunk ES on top of your Splunk Cloud data by confirming CIM mapping and data model coverage for your key sources like network, endpoint, identity, DNS, and cloud.

Splunk Attack Analyzer

- **Role:** Holistic static and dynamic file analysis, engine of engines.
- **Capabilities:** Analyzes phishing domains, files, and performs malware sandbox detonation, streaming events in real-time, human emulation for website crawling. Paired with Secure Malware Analytics to so that supported file types that are submitted to Splunk Attack Analyzer are also analyzed in Secure Malware Analytics for additional validation.
- **Integration configuration:** Enable analysts, automation workflows and Endace to submit files directly to Splunk Attack Analyzer.



HTTP-1761035746.551070-010cfb902cae00576e39556914eb7af5-FjQMBTu8EmUzey466.zip

[redacted]

Summary	
Consolidated	100
HTTP-1761035746.551070-0...	
Archive Extraction	0
Static File Analysis	0
ClamAV	0
YARA	0
0.exe	
Static File Analysis	100
ClamAV	100
YARA	30
Cisco SMA (Windows 10)	95

Initial Submission HTTP-1761035746.551070-010cfb902cae00576e39556914eb7af5-FjQMBTu8EmUzey466.zip
Job Duration 6 minutes
Resources Analyzed 0 URLs, 2 files

Detections (28)

Engine	Signature / Alert	Score
ClamAV	ClamAV detected 3 signatures	100
Static File Analysis	Ember ML model scored the executable as probably malicious	100
Cisco SMA (Windows 10)	Artifact Flagged Malicious by Antivirus Service	95
Cisco SMA (Windows 10)	Artifact Flagged as Known Trojan by Antivirus	95
Cisco SMA (Windows 10)	Process Modified a File in a System Directory	85
Cisco SMA (Windows 10)	Process Deleted the Submitted File	81
Cisco SMA (Windows 10)	Artifact Flagged by Antivirus	72
Cisco SMA (Windows 10)	Process Added a Service to the ControlSet Registry Key	72
Cisco SMA (Windows 10)	A Service Was Set To Never Autorun Via The Re	[illegible]

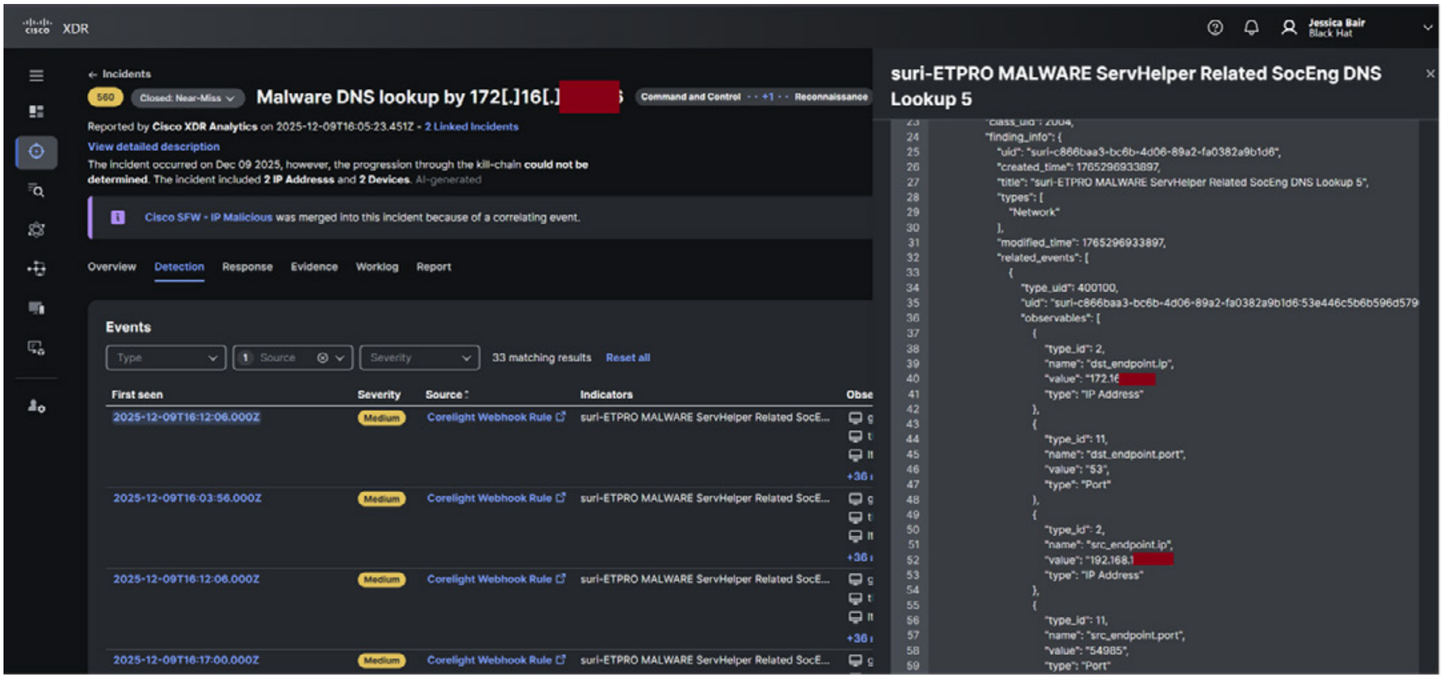
Figure 19: Splunk Attack Analyzer.

Splunk Security Orchestration, Automation, and Response (SOAR)

- **Role:** Automates security workflows and playbooks.
- **Capabilities:**
  - Highly customizable and heavily integrated with Splunk Enterprise Security 8.x to give your SOC analyst a seamless ‘Insight to Action’ experience.
  - Integrated with over 300 security tools, putting over 2800 actions for your security analysts to enable “zero-touch” responses (e.g., for cleartext password detection), automate user notifications.
- **Integration configuration:** Connect ES to Splunk SOAR for automated case handling and to Endace for packet pivots, then tune correlation searches and standardize dashboards and notable event routing so Tier 3 workflows stay consistent across events.

5.4. Packet capture evidence

- **Role:** Save Full Packet Capture of event data for analysis and compliance. Send rebuilt files to file analysis tools.
- **Capabilities:**
  - Full packet capture storage of the event and network detections using Zeek. Endace provides enrichment of investigations for analysts to be able to pivot from XDR to Endace for a deep dive into the packets of a specific incident or investigation.
  - Endace uses Zeek to rebuild files and send them to Splunk Attack Analyzer and Secure Malware Analytics for analysis. Zeek metadata can be used within Splunk to detect passwords in clear text. This is an example of an NDR detection we use across many events where critical passwords may be passed in HTTP, POP3, FTP, SMB or other communication protocols.



Malware DNS lookup by 172[.]16[.][redacted]

Reported by Cisco XDR Analytics on 2025-12-09T16:05:23.451Z - 2 Linked Incidents

The incident occurred on Dec 09 2025, however, the progression through the kill-chain could not be determined. The incident included 2 IP Addresss and 2 Devices. AI-generated

Cisco SFW - IP Malicious was merged into this incident because of a correlating event.

Events

33 matching results

First seen	Severity	Source	Indicators	Obse
2025-12-09T16:12:06.000Z	Medium	Corelight Webhook Rule	suri-ETPRO MALWARE ServHelper Related SocE...	+36
2025-12-09T16:03:56.000Z	Medium	Corelight Webhook Rule	suri-ETPRO MALWARE ServHelper Related SocE...	+36
2025-12-09T16:12:06.000Z	Medium	Corelight Webhook Rule	suri-ETPRO MALWARE ServHelper Related SocE...	+36
2025-12-09T16:17:00.000Z	Medium	Corelight Webhook Rule	suri-ETPRO MALWARE ServHelper Related SocE...	

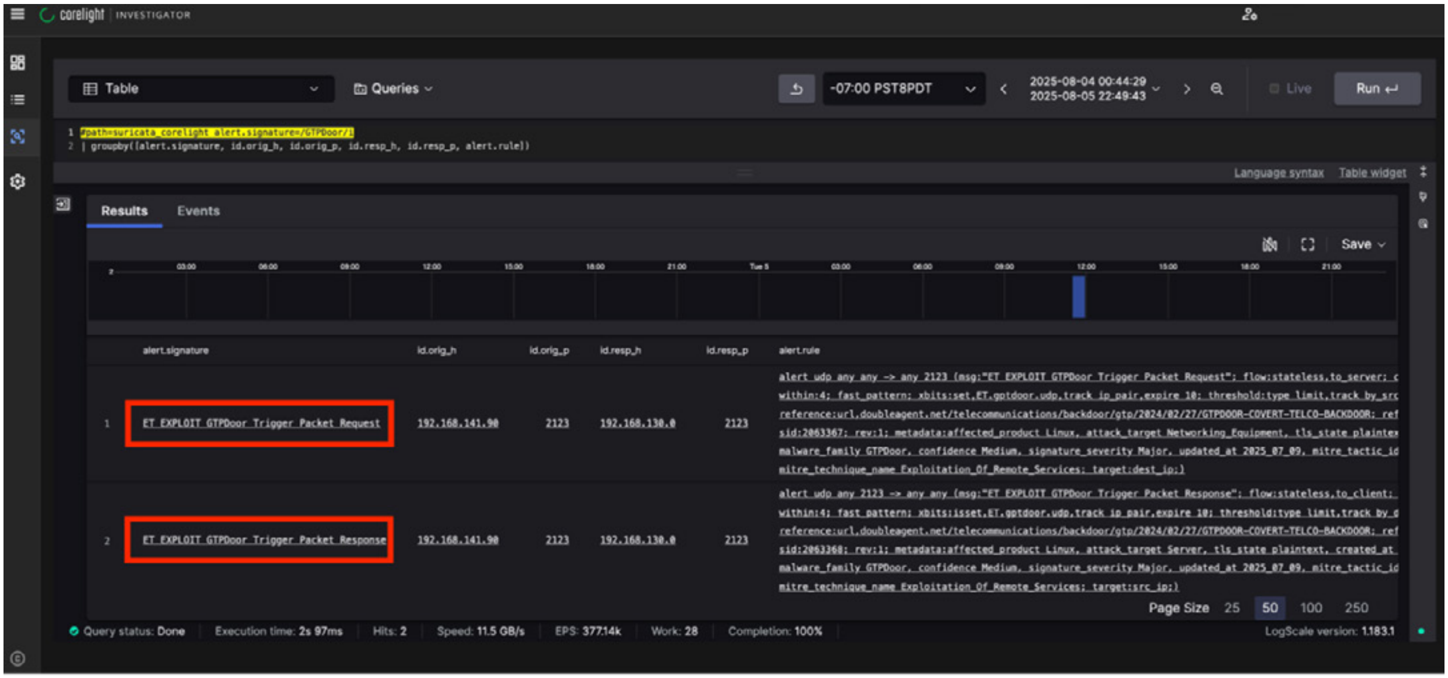
suri-ETPRO MALWARE ServHelper Related SocEng DNS Lookup 5

```
      "class_uid": 2004,
      "finding_info": {
        "uid": "suri-c866baa3-bc6b-4d06-89a2-fa0382a9b1d6",
        "created_time": 1765296933897,
        "title": "suri-ETPRO MALWARE ServHelper Related SocEng DNS Lookup 5",
        "types": [
          "Network"
        ],
        "modified_time": 1765296933897,
        "related_events": [
          {
            "type_uid": 400100,
            "uid": "suri-c866baa3-bc6b-4d06-89a2-fa0382a9b1d6:53e446c5b6b596d579
            "observables": [
              {
                "type_id": 2,
                "name": "dst_endpoint.ip",
                "value": "172.16[redacted]
                "type": "IP Address"
              },
              {
                "type_id": 11,
                "name": "dst_endpoint.port",
                "value": "53",
                "type": "Port"
              },
              {
                "type_id": 2,
                "name": "src_endpoint.ip",
                "value": "192.168.1[redacted]
                "type": "IP Address"
              },
              {
                "type_id": 11,
                "name": "src_endpoint.port",
                "value": "54985",
                "type": "Port"
```

Figure 20: Corelight detections surfaced in Cisco XDR.

- When we find users using extremely long complex passwords sent across the network in clear text, it is an opportunity to educate them. In these cases, we automate sending emails to notify end users that their passwords can be seen in clear text and educate them on the importance of password hygiene and encrypted protocols.

- **Integration configuration:**
  - Deploy Endace probes with SPAN connection from Catalyst 9500 for packets to be searched in the EndaceVision UI.
  - Ensure Zeek metadata and detections flow into Splunk with consistent sourcetypes and fields.



```
#path=suricata_corelight alert.signature=/GTPDoor/i
| groupby([alert.signature, id.orig_h, id.orig_p, id.resp_h, id.resp_p, alert.rule])
```

	alert.signature	id.orig_h	id.orig_p	id.resp_h	id.resp_p	alert.rule
1	ET EXPLOIT GTPDoor Trigger Packet Request	192.168.141.90	2123	192.168.130.0	2123	alert udp any any -> any 2123 (msg:"ET EXPLOIT GTPDoor Trigger Packet Request"; flow:stateless,to_server; c within:4; fast_pattern; xbits:set,ET.gptdoor.udp,track ip_pair,expire 10; threshold:type limit,track by_src reference:url,doubleagent.net/telecommunications/backdoor/gtp/2024/02/27/GTPDOOR-COVERT-TELCO-BACKDOOR; ref sid:2063367; rev:1; metadata:affected_product Linux, attack_target Networking_Equipment, tls_state plaintex malware_family GTPDoor, confidence Medium, signature_severity Major, updated_at 2025_07_09, mitre_tactic_id mitre_technique_name Exploitation_Of_Remote_Services; target:dest_ip;)
2	ET EXPLOIT GTPDoor Trigger Packet Response	192.168.141.90	2123	192.168.130.0	2123	alert udp any 2123 -> any any (msg:"ET EXPLOIT GTPDoor Trigger Packet Response"; flow:stateless,to_client; within:4; fast_pattern; xbits:isset,ET.gptdoor.udp,track ip_pair,expire 10; threshold:type limit,track by_d reference:url,doubleagent.net/telecommunications/backdoor/gtp/2024/02/27/GTPDOOR-COVERT-TELCO-BACKDOOR; ref sid:2063368; rev:1; metadata:affected_product Linux, attack_target Server, tls_state plaintext, created_at malware_family GTPDoor, confidence Medium, signature_severity Major, updated_at 2025_07_09, mitre_tactic_id mitre_technique_name Exploitation_Of_Remote_Services; target:src_ip;)

Query status: Done | Execution time: 2s 97ms | Hits: 2 | Speed: 11.5 GB/s | EPS: 377.14k | Work: 28 | Completion: 100% | LogScale version: 1.183.1

Figure 21: Corelight NDR–Zeek logs.

5.5. Threat intel

Threat intelligence in this design is a shared enrichment layer that improves decision quality in a short-lived, high-noise conference network. It is applied across Cisco Secure Firewall, Cisco Secure Access (DNS), Cisco XDR, and Splunk ES to increase confidence, prioritize what matters, and support selective enforcement and response. In practice, it helps analysts quickly determine whether an observable is risky, whether it is touching something critical, and whether it is expected for the segment where it appears.

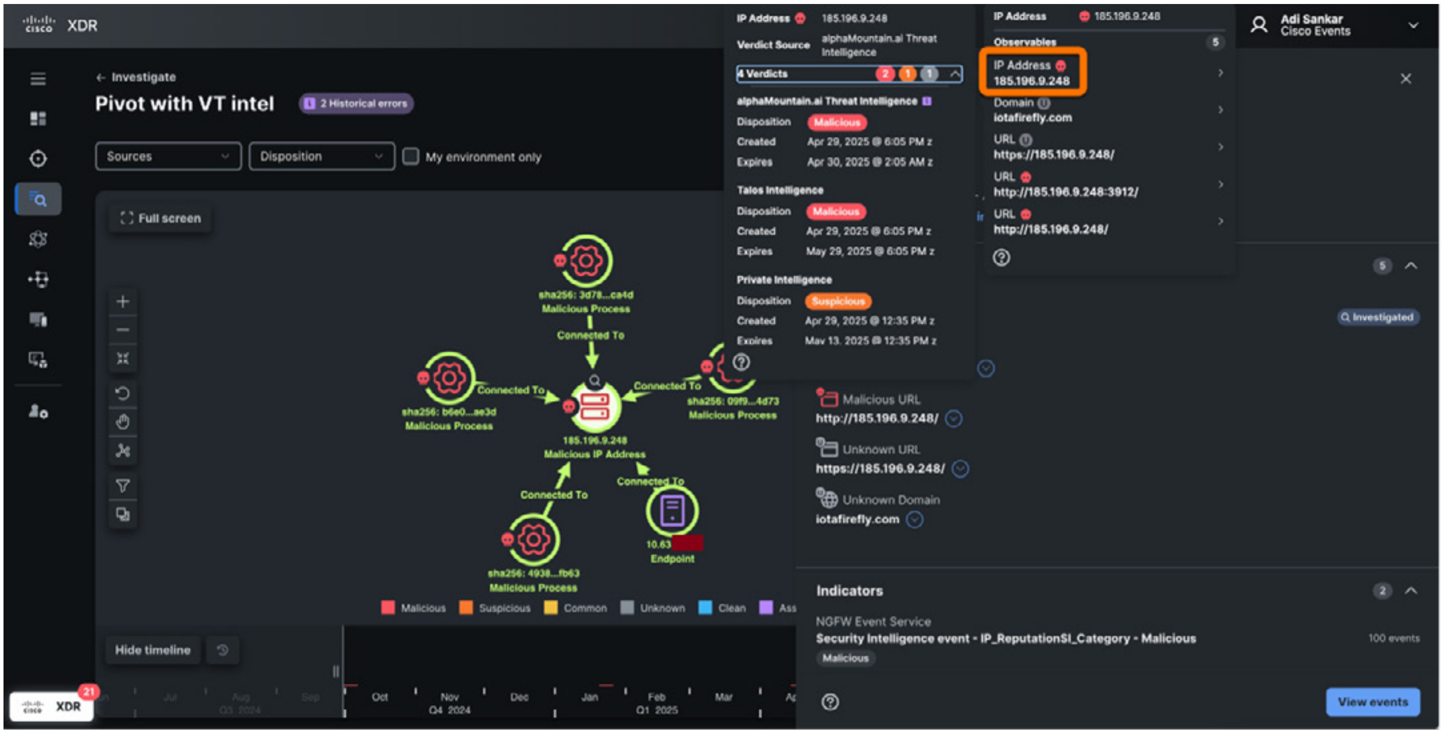
What we use threat intel for

- **Triage confidence:** “Is this IP/domain/hash known-bad?”
- **Scope and priority:** “Is it touching a critical segment (registration/NOC/SOC mgmt.) or an expected-noisy segment (labs/CTF)?”
- **Selective action:** “Should we block/sinkhole/contain this observable for the remainder of the event without disrupting legitimate activity?”

Sources and how they are used

We appreciate alphaMountain, Pulsedive, and StealthMole donating threat intelligence licenses for use in the Cisco Managed Event SOCs.

Global shared intelligence provides the baseline reputation tier, anchored by Cisco Talos and augmented by selected partner and OSINT sources. This layer classifies IPs, domains, URLs, and file hashes so analysts do not spend time on repetitive lookups during high-tempo operations. Secure Firewall uses this intelligence to annotate events and, when confidence is high and operational impact is acceptable, to apply targeted blocks against known-bad infrastructure. Secure Access applies domain reputation to DNS activity and blocks or sinkholes malware, phishing, and command-and-control destinations where policy allows. Cisco XDR and Splunk ES consume the same judgments so observables in incidents and correlation results carry consistent classification and confidence.



IP Address 185.196.9.248
Verdict Source alphaMountain.ai Threat Intelligence
4 Verdicts 2 1 1

alphaMountain.ai Threat Intelligence
Disposition Malicious
Created Apr 29, 2025 @ 6:05 PM z
Expires Apr 30, 2025 @ 2:05 AM z

Talos Intelligence
Disposition Malicious
Created Apr 29, 2025 @ 6:05 PM z
Expires May 29, 2025 @ 6:05 PM z

Private Intelligence
Disposition Suspicious
Created Apr 29, 2025 @ 12:35 PM z
Expires May 13, 2025 @ 12:35 PM z

IP Address 185.196.9.248
Observables 5
IP Address 185.196.9.248
Domain iotafirefly.com
URL https://185.196.9.248/
URL http://185.196.9.248:3912/
URL http://185.196.9.248/

5
Investigated

Malicious URL http://185.196.9.248/
Unknown URL https://185.196.9.248/
Unknown Domain iotafirefly.com

Indicators 2
NGFW Event Service
Security Intelligence event - IP_ReputationSI_Category - Malicious 100 events
Malicious

View events

Figure 22: XDR Investigate querying threat intelligence sources.

Private event intelligence is the environmental context that makes threat intel actionable at a conference. The SOC and NOC maintain a canonical map of subnets, VLANs, and SSIDs and tie them to segment roles, criticality, and expected behavior. This mapping is treated as an internal intelligence source and is operationalized as lookups and asset metadata in Splunk ES, and as enrichment on entities in Cisco XDR. During the event, this is supplemented with short-lived watchlists and suppressions that reflect the reality of conference operations.

Examples include allowed lab ranges, known noisy demo infrastructure, and local indicators such as rogue SSIDs, brand-abuse domains, or repeated scanners crossing boundaries. The goal is to reduce noise while preserving visibility and highlighting activity that violates segment expectations.

Closed intelligence (trusted partner and law enforcement coordination) We also leverage closed intelligence from trusted partners and, when appropriate, law enforcement agencies. This provides time-sensitive context on specific threats such as hacktivism, targeted DDoS, politically motivated activity, threats directed at the conference or its stakeholders, and other credible chatter. When actionable, the SOC converts this into watchlists and targeted monitoring in XDR and Splunk. We may also increase vigilance with respect to these specific threats and apply selective defensive actions through Secure Firewall and Secure Access when necessary.

Derived intelligence closes the loop by turning investigations into reusable detection inputs. When a detection involves a suspicious file or URL, Splunk Attack Analyzer and Secure Malware Analytics provide verdicts and extract additional indicators. Those indicators are promoted into Splunk ES intel collections so similar IOCs can be detected and triaged faster during the same event. When analysts need packet-level proof, Endace and associated Zeek metadata provide validation and scoping. Analysts can confirm behaviors, reconstruct timelines where feasible, and extract additional infrastructure such as C2 endpoints or tunneling gateways. Once validated, these discoveries are added back into event-scoped intel sets to drive continued hunting and targeted response.

Proactive external monitoring is included because event-relevant threats often form off-network. For dark web monitoring, we use the Cisco XDR and StealthMole integration to surface relevant leaks, chatter, and actor infrastructure tied to the event, sponsors, or high-value stakeholders. Findings that are credible and actionable are converted into watchlists or investigation pivots, and they are used to prioritize monitoring of critical assets during the event window.

Optional Threat Intelligence Platform

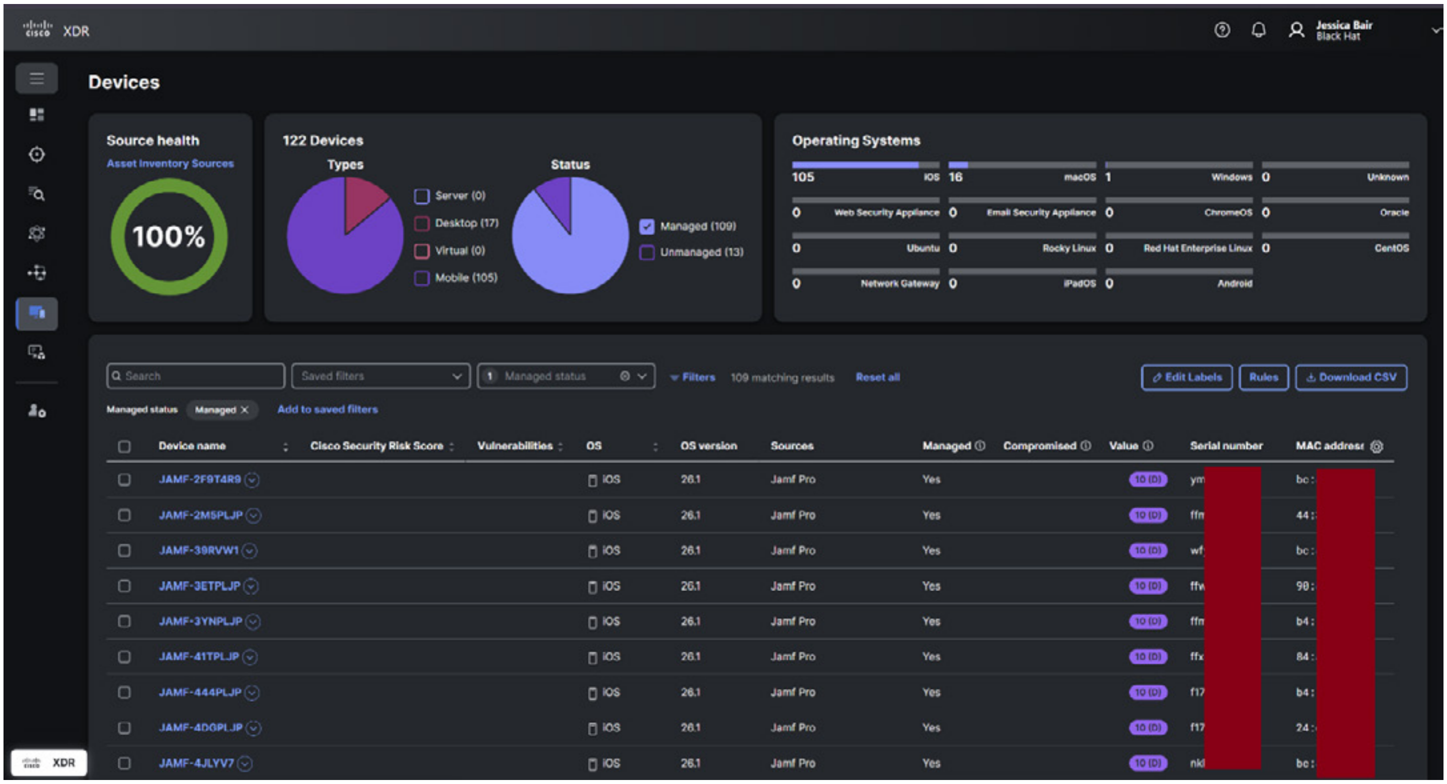
A dedicated Threat Intelligence Platform (TIP) such as the open source MISP project is optional in this architecture. The event SOC operates effectively with Cisco XDR and Splunk ES managing intelligence directly, especially when intelligence needs to be event-scoped and time-bounded. A TIP becomes most useful when an organization already has a mature CTI program. It allows for a centralized place to deduplicate indicators, apply consistent TTL and tagging, and publish curated collections back into the SOC toolchain.

The intelligence workflow is designed as a tight feedback loop. Telemetry is analyzed to produce detections, and those detections are enriched with global and event intelligence context. Confirmed malicious indicators are then pushed down via threat intelligence feeds to individual security controls, so coverage improves over the course of the event, without requiring long historical baselines.

5.6. Mobile device management

A critical operational dependency at large conferences is the managed iOS device fleet that supports attendee-facing workflows. At Black Hat, we use Jamf Pro to manage the iPad registration kiosks used for attendee check-in, as well as the iPhone lead-retrieval devices used across the vendor booth show floor including to scan attendees before a SOC tour. The scale is non-trivial, with roughly three iPhones or iPads per booth in addition to devices supporting Registration, Training, and Briefings operations. These endpoints directly impact the attendee experience and conference business operations, so maintaining availability, integrity, and a consistent security posture is a priority.

From a security operations standpoint, managed iOS fleets are one of the few places where we do have strong endpoint governance in an otherwise BYOD-heavy environment.

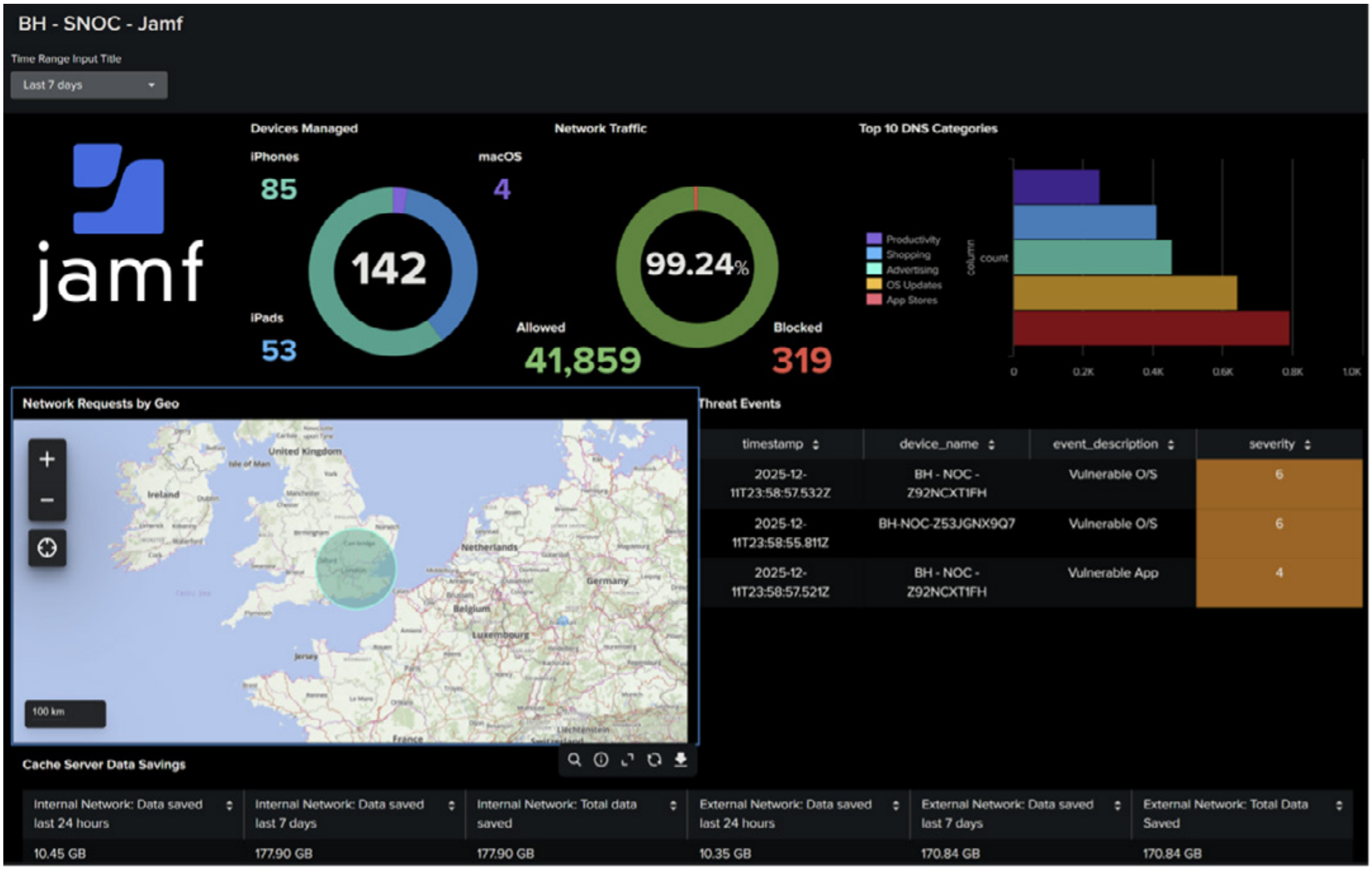


☐	Device name	Cisco Security Risk Score	Vulnerabilities	OS	OS version	Sources	Managed	Compromised	Value	Serial number	MAC address
☐	JAMF-2F9T4R9			iOS	26.1	Jamf Pro	Yes		10 (D)	[redacted]	[redacted]
☐	JAMF-2M5PLJP			iOS	26.1	Jamf Pro	Yes		10 (D)	[redacted]	[redacted]
☐	JAMF-39RVW1			iOS	26.1	Jamf Pro	Yes		10 (D)	[redacted]	[redacted]
☐	JAMF-3ETPLJP			iOS	26.1	Jamf Pro	Yes		10 (D)	[redacted]	[redacted]
☐	JAMF-3YNPLJP			iOS	26.1	Jamf Pro	Yes		10 (D)	[redacted]	[redacted]
☐	JAMF-41TPLJP			iOS	26.1	Jamf Pro	Yes		10 (D)	[redacted]	[redacted]
☐	JAMF-444PLJP			iOS	26.1	Jamf Pro	Yes		10 (D)	[redacted]	[redacted]
☐	JAMF-4DGPLJP			iOS	26.1	Jamf Pro	Yes		10 (D)	[redacted]	[redacted]
☐	JAMF-4JLYV7			iOS	26.1	Jamf Pro	Yes		10 (D)	[redacted]	[redacted]

Figure 23: JAMF MDM and XDR assets—devices.

Jamf Pro enables centralized configuration, policy enforcement, and rapid remediation for thousands of devices, and it provides posture and inventory visibility that is valuable during investigations. Jamf integrates with Cisco XDR to enrich asset context and support incident workflows.

Jamf telemetry can also be operationalized in Splunk for search, correlation, and reporting. This combination helps the SOC quickly distinguish device misconfiguration or operational issues from malicious activity, prioritize protection of high-value conference systems, and coordinate effectively with the registration team when action is required.



Threat Events

timestamp	device_name	event_description	severity
2025-12-11T23:58:57.532Z	BH - NOC - Z92NCXT1FH	Vulnerable O/S	6
2025-12-11T23:58:55.811Z	BH-NOC-Z53JGNX9Q7	Vulnerable O/S	6
2025-12-11T23:58:57.521Z	BH - NOC - Z92NCXT1FH	Vulnerable App	4

Cache Server Data Savings

Internal Network: Data saved last 24 hours	Internal Network: Data saved last 7 days	Internal Network: Total data saved	External Network: Data saved last 24 hours	External Network: Data saved last 7 days	External Network: Total Data Saved
10.45 GB	177.90 GB	177.90 GB	10.35 GB	170.84 GB	170.84 GB

Figure 24: JAMF MDM data visualized in Splunk.

6. Operational workflows

Operational success depends less on bespoke analyst actions and more on repeatable workflows that produce consistent outcomes. For Tier 1 and Tier 2 operations, the Cisco XDR incident is the canonical record. Tier 3 analysis may occur in Splunk Enterprise Security or other advanced tooling, but conclusions, scope, and recommendations are always summarized back into the canonical incident. This preserves a single operational narrative, supports auditability, and enables consistent handoffs across tiers and shifts.

6.1. Threat detection & triage (Tier 1 and Tier 2 analysts)

- **Initial alerting:** Tier 1 and Tier 2 analysts work primarily in Cisco XDR, which serves as the front-door for detections and alert intake. Alerts are generated from core event telemetry sources such as Cisco Secure Firewall (IDS/IPS and encrypted traffic visibility signals), DNS security, and network metadata sources that are forwarded through Splunk. The objective is to get to a triage decision quickly, without excessive tool switching.
- **Contextual enrichment:** For each alert, analysts identify the key observables, which commonly include IPs, domains, URLs, file hashes, hostnames, MAC addresses, etc. XDR automatically enriches these observables with threat intelligence, prior sightings, and related incident context. Analysts also apply event context by checking network segment mapping, which helps distinguish expected conference noise from suspicious activity.
- **Rapid investigation:** Analysts use XDR's Investigate tool to scope impact and answer practical questions including:

1. Is the behavior isolated or widespread?
2. Is it touching a critical segment?
3. Does it show patterns consistent with command-and-control, scanning, or data movement?

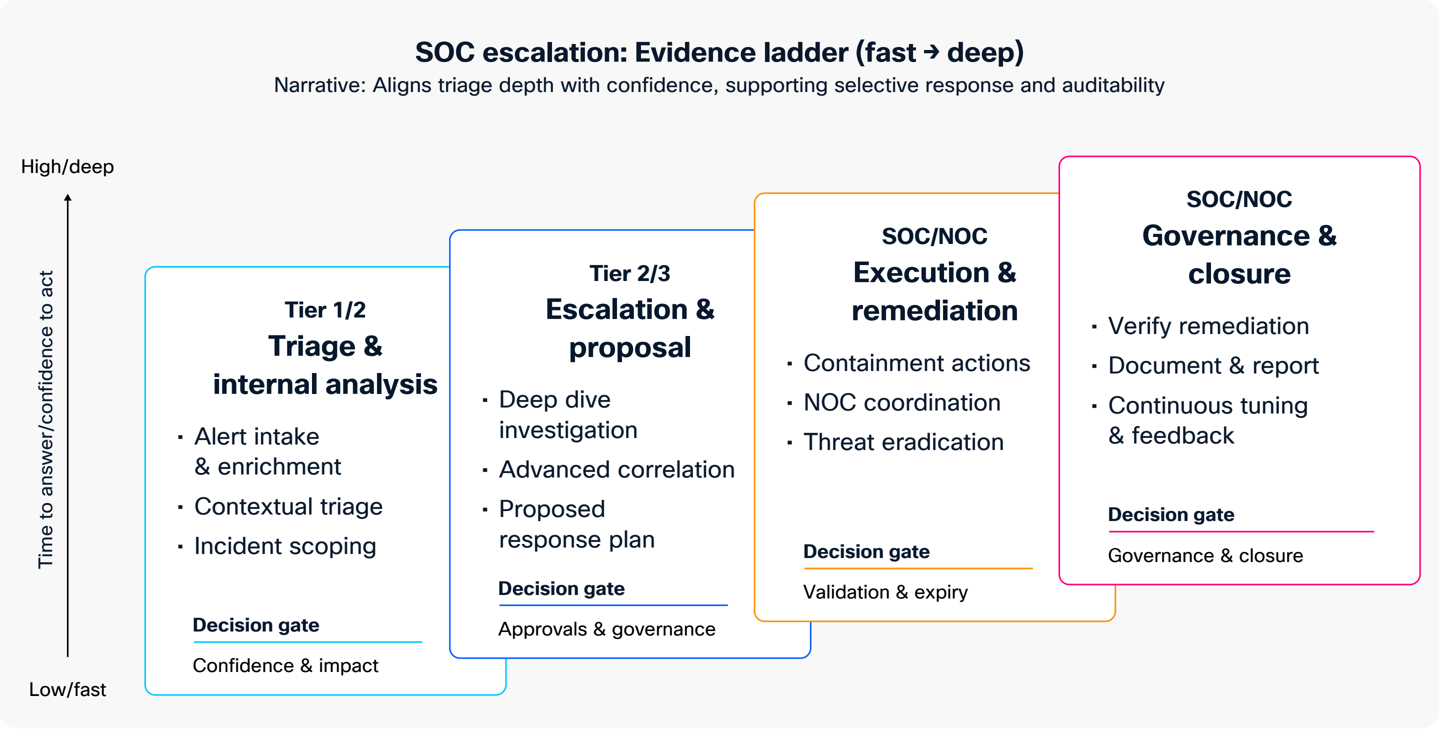


Figure 25: SOC escalation path.

When packet level details are needed, they pivot to Endace for time-bounded PCAP validation using a prebuilt pivot link added to the incident by XDR automation.

- **AI-assisted analysis:** AI is used to reduce alert fatigue and accelerate decision-making, while analysts still validate conclusions using underlying evidence and telemetry. Within XDR, LLM-based capabilities summarize incidents, supporting logs, and observed attack flows into clear, human-readable narratives that analysts can review quickly during triage. AI is also used to recommend guided response actions which helps new analysts.

6.2. Deeper investigation & threat hunting (Tier 3 analysts/threat hunters)

Advanced correlation

Tier 3 analysts operate primarily in Splunk Enterprise Security, where high-volume telemetry from integrated platforms is aggregated for complex correlation. The core mechanism is risk-based alerting and enrichment, which allows analysts to join multiple weak signals into higher-confidence detections and identify more sophisticated patterns that may not surface as a single alert. Analysts start with a working theory and a defined time window, then test it across relevant data sources to confirm scope, intent, and impact. This approach stays effective even when baselining is limited.

Forensic analysis

EndaceProbes provide always-on packet capture and serve as the definitive validation layer for all SOC analysts. Analysts pivot from Splunk and XDR into packet evidence to reconstruct sessions, validate what occurred, and support root cause analysis. In an environment with heavy encryption and limited endpoint control, packet capture is still valuable for full-fidelity network coverage. It provides timing, sequence, and corroboration, and when reconstruction or artifact extraction is feasible it strengthens conclusions and produces evidentiary findings.

Proactive hunting

Threat hunters use Splunk ES to search for unknown threats and low-signal behaviors that do not reliably trigger alerts. With Tier 1 triage and Tier 2 investigation handling most alerted incidents, Tier 3 has the bandwidth to focus on deeper searches across non-alerting data and surface hidden risks. Hunts are time-bound and outcome-driven. Hunters prioritize behaviors that matter in event environments, such as credential exposure, anomalous remote access, and targeting critical infrastructure. A hunt is considered complete when it tests a hypothesis thoroughly. A successful threat hunt produces an operational output such as a tuned detection, improved correlation logic, an updated intelligence set, a scoped suppression, or a clear response recommendation.

Malware and artifact analysis

When suspicious files or URLs are identified, artifacts are submitted automatically or manually from Endace and Splunk Attack Analyzer into Cisco Secure Malware Analytics for deeper sandboxing. Experienced analysts use both automated and manual methods, including static and dynamic analysis, to confirm maliciousness and extract indicators. Derived indicators and verdicts are fed back into Splunk ES and Cisco XDR, as event-scoped intelligence, so detection and triage improve during the event window.

6.3. Automated response & remediation

Response philosophy

Response in event SOCs is deliberately selective, scoped, and reversible. The architecture does not assume universal enforcement authority, and it avoids a block-by-default posture. Instead, response follows a practical ladder. It starts with visibility and education, then progresses to targeted controls when confidence and impact justify action. This preserves availability for conference operations while still protecting critical services.

XDR automation

Cisco XDR automation is designed to improve consistency and readiness, not to operate autonomously. Common patterns include automated enrichment, standardized worklogs, and evidence links that support quick analyst review. Worklogs routinely include pivots to supporting sources such as Splunk investigations and packet evidence references when applicable. Cisco XDR also drives shared awareness by posting incident notifications and updates to collaboration channels so Tier 1 and Tier 2 can coordinate triage and escalation efficiently, while Tier 3 can quickly pick up deeper investigation when required.

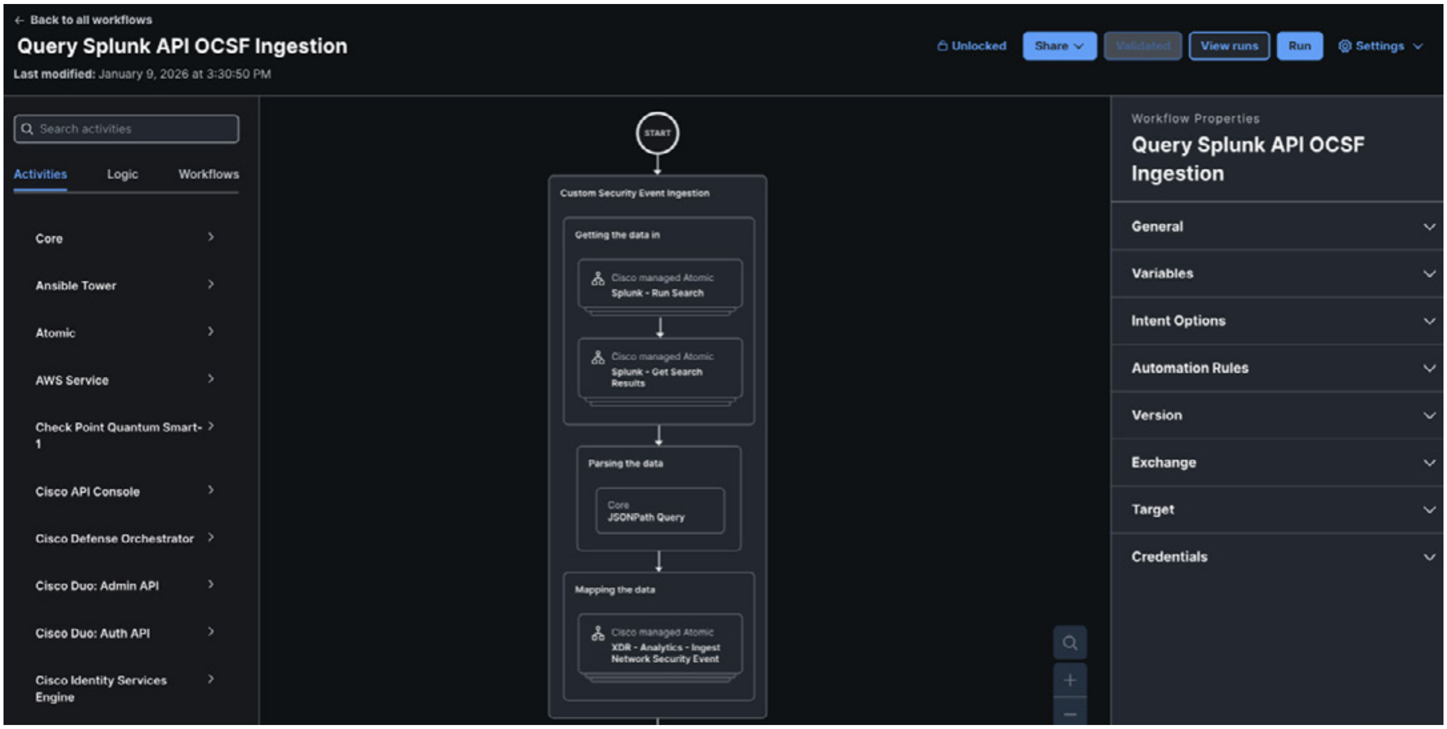


Figure 26: XDR automation workflow canvas.

Splunk SOAR playbooks

Splunk SOAR playbooks provide a library of repeatable actions that can be adopted based on authority and SOC maturity. The most portable actions include enrichment tasks, case updates, time-bounded list management, and user notifications that align to the Educate principle. For example, notifications may be triggered for behaviors such as cleartext credential exposure or policy-violating tooling. Where enforcement actions are automated, playbooks should include explicit scoping, approvals, and expiration semantics so controls remain reversible and do not outlive the event context.

Containment requests and coordination with the NOC

When response requires network changes, the SOC issues a structured containment request to the NOC. The request includes indicators, affected scope, segment context, confidence level, evidence reviewed, and a proposed duration. This supports different operating models, including SOC-executed changes or NOC-executed changes, while ensuring decisions are defensible and easy to roll back.

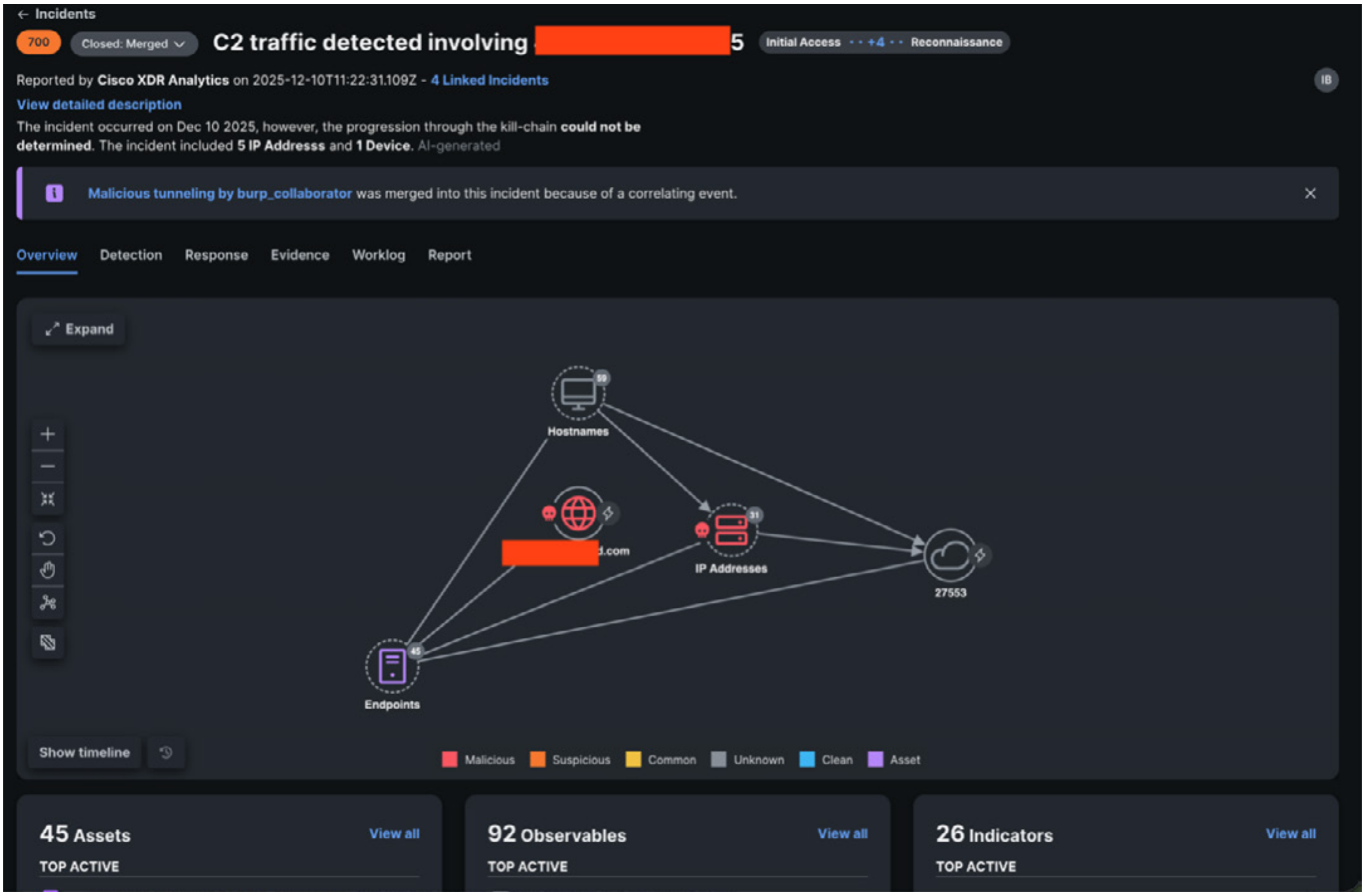
Governance and closure

Remediation concludes with validation and feedback. Analysts confirm whether the behavior stopped or changed, document outcomes, and feed lessons into tuning and playbook refinement.

6.4. Investigation process

When we decide to perform an investigation, usually we are prompted by an initial incident surfacing in Cisco XDR. Initially, when the incident rolls into the XDR console, it is triaged by Tier 1 & 2 analysts where MITRE TTP's such as reconnaissance, C2, etc., are shown. Cisco XDR helps an analyst out by automatically enriching data, such as whether a domain name is malicious, an IP address is associated with C2 traffic, etc.

The incident in Figure 27 has the Attack Graph open showing 46 internal hosts from the public Wi-Fi connecting to 60 domains with 1 being of specific interest to us. These domains are associated with 31 external IP addresses. Cisco XDR classifies the alert as Initial Access, and a few other TTPs. Using the Cisco XDR investigate tool to dig into the external IPs we can see that about half are malicious.



← Incidents

700 Closed: Merged **C2 traffic detected involving [redacted]5** Initial Access • • +4 • • Reconnaissance

Reported by **Cisco XDR Analytics** on 2025-12-10T11:22:31.109Z - 4 Linked Incidents

View detailed description

The incident occurred on Dec 10 2025, however, the progression through the kill-chain **could not be determined**. The incident included **5 IP Addresss** and **1 Device**. AI-generated

Malicious tunneling by burp_collaborator was merged into this incident because of a correlating event.

45 Assets View all
TOP ACTIVE

92 Observables View all
TOP ACTIVE

26 Indicators View all
TOP ACTIVE

Figure 27: Cisco XDR incident overview.

This would lead us to believe that those unknown IPs are malicious as well but have not been categorized yet. We also see that there are many domains related to these IPs.

Looking at the one main domain in Figure 28, we can use the Pivot menu to check for more information about the malicious verdict provided.

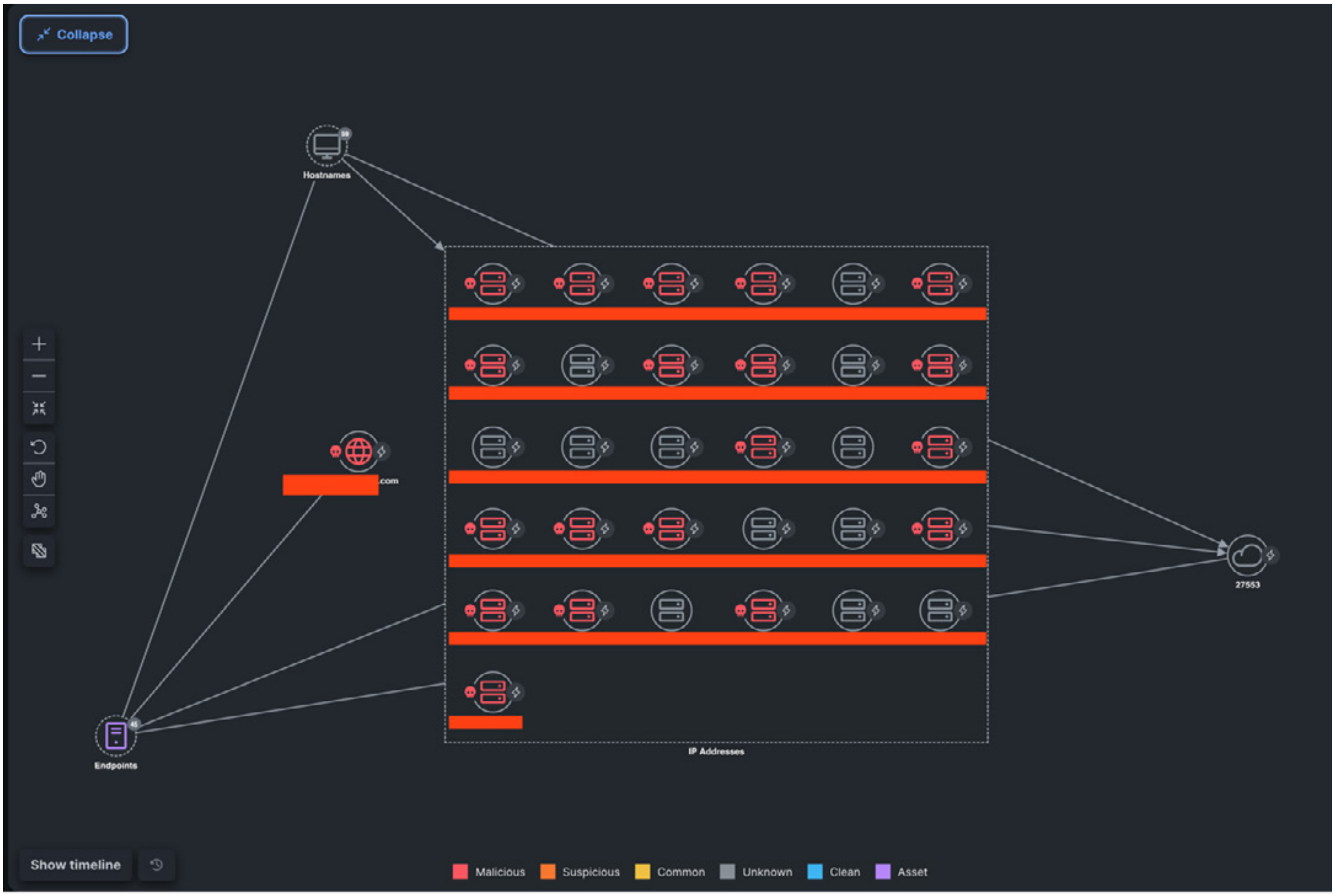


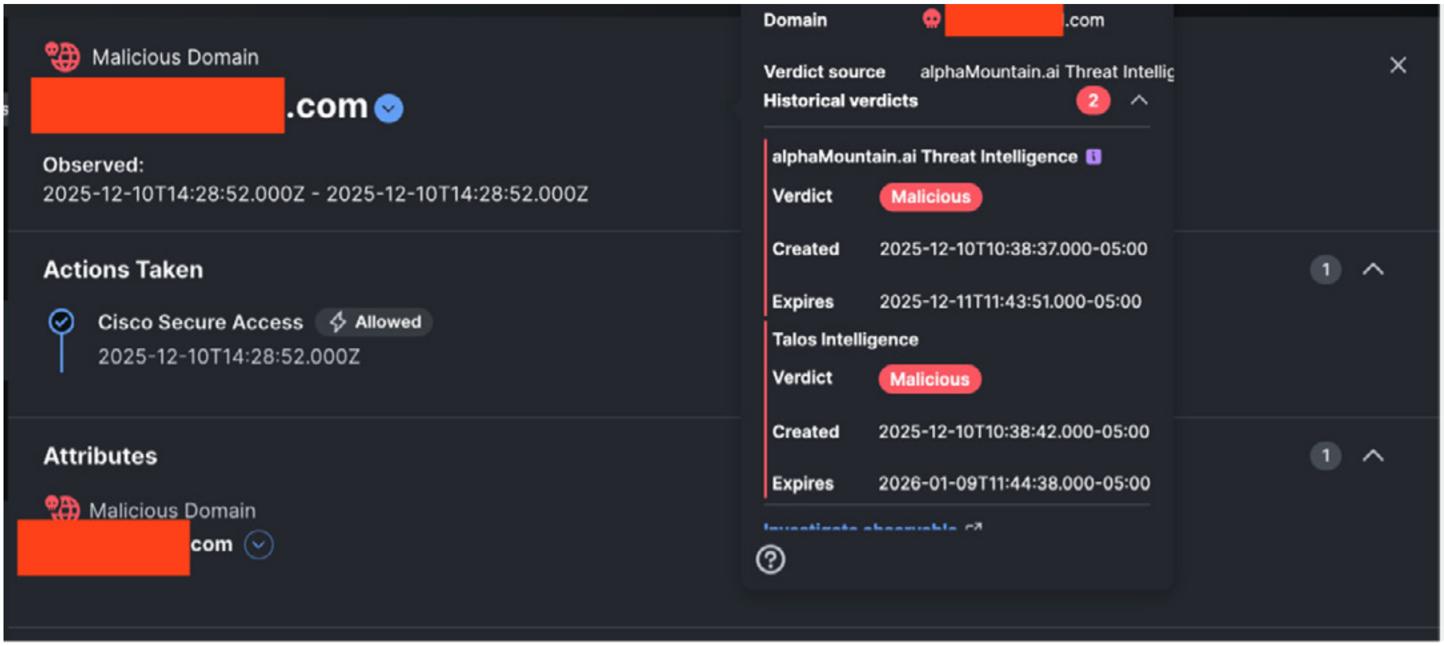
Figure 28: Cisco XDR's investigate feature.

In figure 29 we can see that Secure Access allowed it and that alphaMountain and Cisco Talos have both marked it as malicious.

Many of the other domains look like legitimate services but are not the right format for those services. They are just slightly off and most likely haven not been investigated yet. This is where we could do additional investigations on those domains and submit verdicts on them, but we will not, as we are on a time crunch. From here, a Tier 1 or Tier 2 analyst could escalate this issue to a lead for review providing evidence that there is malicious activity and that it is not intentional by the user. Most of the malicious activity we expect should be on dedicated wireless networks, while this occurred on the public attendee network.

The above process is all automated and enriched by Cisco XDR. Generally, we would have to follow the below process if it was not automated (note this is one example of an investigative flow):

1. See malicious domain come in via Secure Access.
2. Check Secure Access logs for the IP address that made the request.
3. Check the Firewall to get the resolved IP of the domain.
4. Use Talos Intelligence, Alpha Mountain, and Virus Total to check the domain and IP reputation.
5. Check if there are other requests to that domain or IP address from other attendees.
6. After deciding if this is legitimate traffic or not, close or escalate for review providing findings. The review could be to double check the work or to ask for action on the traffic.



Malicious Domain

[redacted].com

Observed:
2025-12-10T14:28:52.000Z - 2025-12-10T14:28:52.000Z

Actions Taken

Cisco Secure Access Allowed
2025-12-10T14:28:52.000Z

Attributes

Malicious Domain
[redacted]com

Domain [redacted].com

Verdict source alphaMountain.ai Threat Intellig

Historical verdicts 2

alphaMountain.ai Threat Intelligence

Verdict Malicious

Created 2025-12-10T10:38:37.000-05:00

Expires 2025-12-11T11:43:51.000-05:00

Talos Intelligence

Verdict Malicious

Created 2025-12-10T10:38:42.000-05:00

Expires 2026-01-09T11:44:38.000-05:00

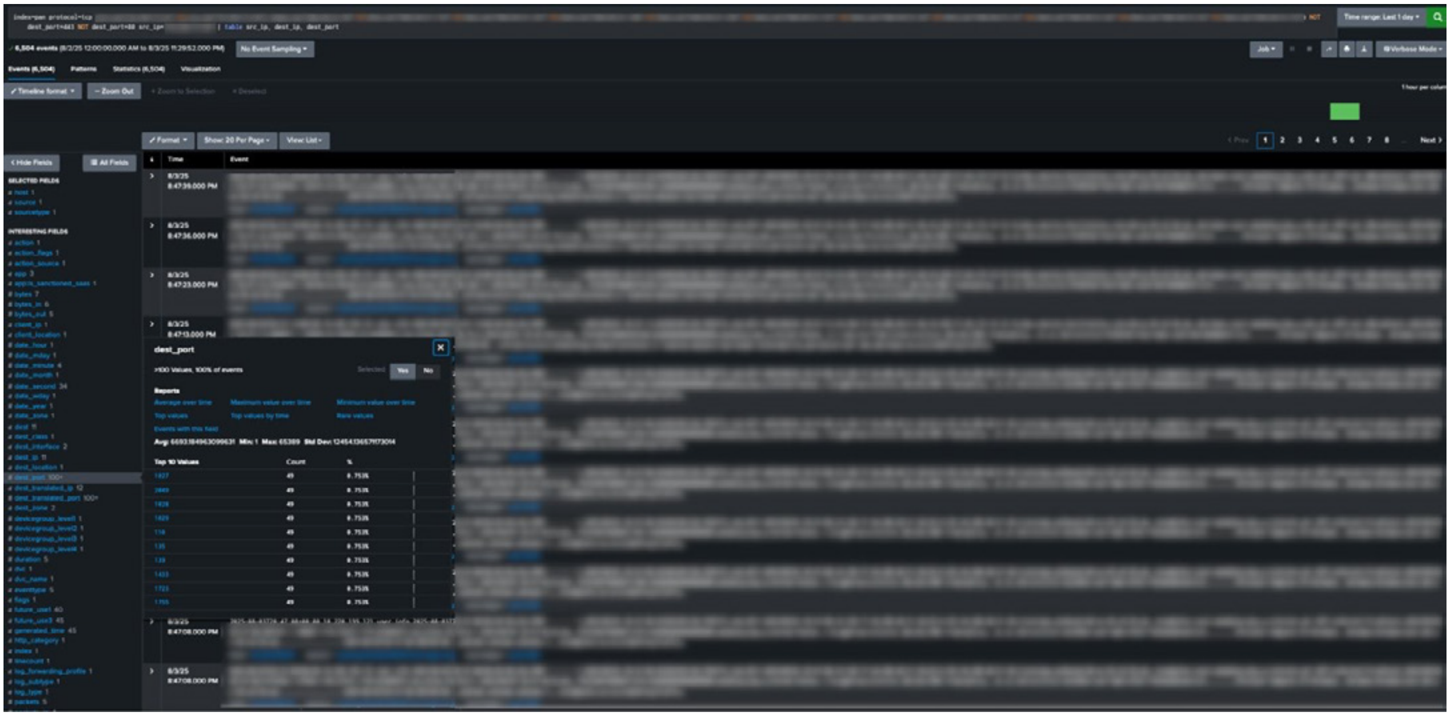
Investigate observable

Figure 29: Cisco XDR Threat Intelligence Context.

These steps could take 10's of minutes to an hour depending on the scope of the incident we are looking at, but XDR has reduced this down a few minutes by automatically enriching this data for us and providing findings in a central UI.

This saves our Tier 1 and Tier 2 analysts valuable time and reduces our Mean Time to Triage (MTT) an incident. After the incident is sent for review, the reviewer may decide that it needs a more in-depth investigation and escalate it to the Tier 3 analysts.

Now that the Tier 3 analyst is involved, they may query Splunk to do advanced correlations, check traffic trends, and do a root cause analysis. This could call for packet analysis as part of the investigation. Connection patterns observed were consistent with scanning and C2 activity.



```
index=pan protocol=tcp [redacted]
    dest_port!=443 NOT dest_port=80 src_ip=[redacted] | table src_ip, dest_ip, dest_port
```

✓ 6,504 events (8/2/25 12:00:00.000 AM to 8/3/25 11:29:52.000 PM)

dest_port

>100 Values, 100% of events

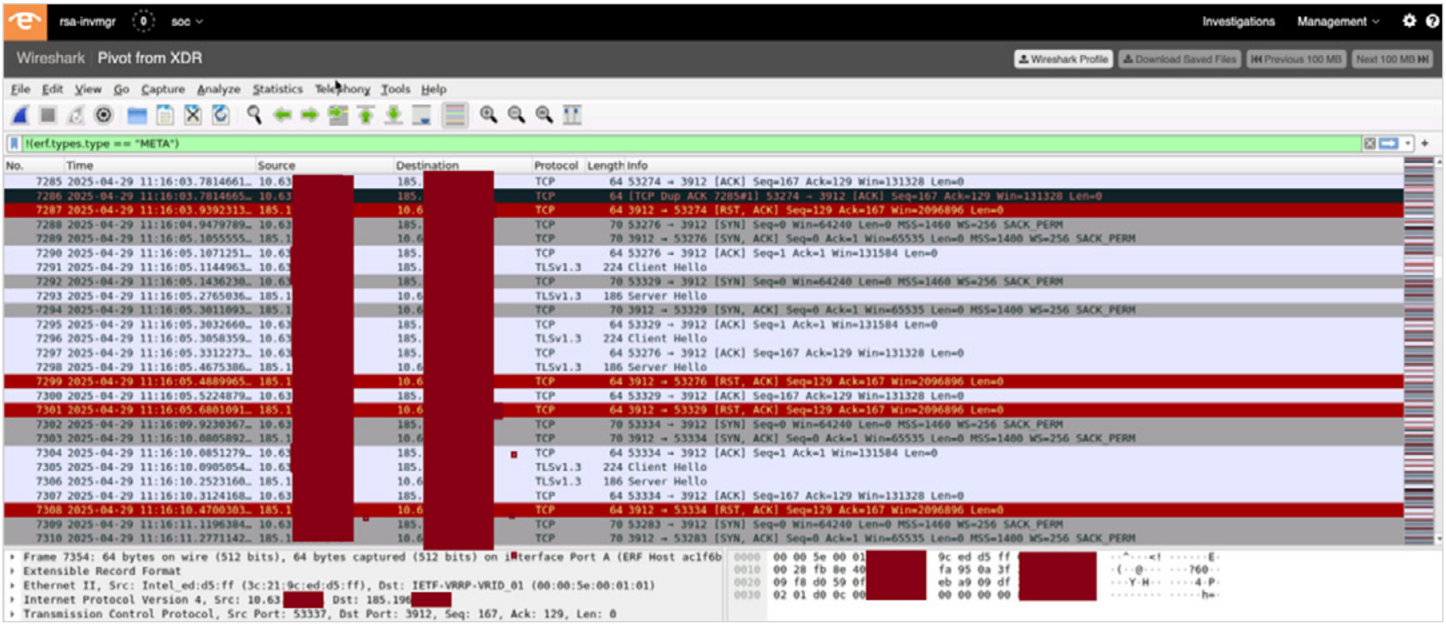
Avg: 6693.184963099631 Min: 1 Max: 65389 Std Dev: 12454.13665791173014

Top 10 Values	Count	%
1827	49	0.753%
2869	49	0.753%
1828	49	0.753%
1829	49	0.753%
118	49	0.753%
135	49	0.753%
139	49	0.753%
1433	49	0.753%
1723	49	0.753%
1755	49	0.753%

[redacted]

Figure 30: Advanced searching in Splunk.

The analysts can pivot directly to the network packets via Endace integration.



```
!(erf.types.type == "META")
```

```
No.   Time                            Source            Destination       Protocol Length Info
 7285 2025-04-29 11:16:03.7814661…   10.63[redacted]   185.[redacted]    TCP        64 53274 → 3912 [ACK] Seq=167 Ack=129 Win=131328 Len=0
 7286 2025-04-29 11:16:03.7814665…   10.63[redacted]   185.[redacted]    TCP        64 [TCP Dup ACK 7285#1] 53274 → 3912 [ACK] Seq=167 Ack=129 Win=131328 Len=0
 7287 2025-04-29 11:16:03.9392313…   185.1[redacted]   10.6[redacted]    TCP        64 3912 → 53274 [RST, ACK] Seq=129 Ack=167 Win=2096896 Len=0
 7288 2025-04-29 11:16:04.9479789…   10.63[redacted]   185.[redacted]    TCP        70 53276 → 3912 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 7289 2025-04-29 11:16:05.1055555…   185.1[redacted]   10.6[redacted]    TCP        70 3912 → 53276 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM
 7290 2025-04-29 11:16:05.1071251…   10.63[redacted]   185.[redacted]    TCP        64 53276 → 3912 [ACK] Seq=1 Ack=1 Win=131584 Len=0
 7291 2025-04-29 11:16:05.1144963…   10.63[redacted]   185.[redacted]    TLSv1.3   224 Client Hello
 7292 2025-04-29 11:16:05.1436230…   10.63[redacted]   185.[redacted]    TCP        70 53329 → 3912 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 7293 2025-04-29 11:16:05.2765036…   185.1[redacted]   10.6[redacted]    TLSv1.3   186 Server Hello
 7294 2025-04-29 11:16:05.3011093…   185.1[redacted]   10.6[redacted]    TCP        70 3912 → 53329 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM
 7295 2025-04-29 11:16:05.3032660…   10.63[redacted]   185.[redacted]    TCP        64 53329 → 3912 [ACK] Seq=1 Ack=1 Win=131584 Len=0
 7296 2025-04-29 11:16:05.3058359…   10.63[redacted]   185.[redacted]    TLSv1.3   224 Client Hello
 7297 2025-04-29 11:16:05.3312273…   10.63[redacted]   185.[redacted]    TCP        64 53276 → 3912 [ACK] Seq=167 Ack=129 Win=131328 Len=0
 7298 2025-04-29 11:16:05.4675386…   185.1[redacted]   10.6[redacted]    TLSv1.3   186 Server Hello
 7299 2025-04-29 11:16:05.4889965…   185.1[redacted]   10.6[redacted]    TCP        64 3912 → 53276 [RST, ACK] Seq=129 Ack=167 Win=2096896 Len=0
 7300 2025-04-29 11:16:05.5224879…   10.63[redacted]   185.[redacted]    TCP        64 53329 → 3912 [ACK] Seq=167 Ack=129 Win=131328 Len=0
 7301 2025-04-29 11:16:05.6801091…   185.1[redacted]   10.6[redacted]    TCP        64 3912 → 53329 [RST, ACK] Seq=129 Ack=167 Win=2096896 Len=0
 7302 2025-04-29 11:16:09.9230367…   10.63[redacted]   185.[redacted]    TCP        70 53334 → 3912 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 7303 2025-04-29 11:16:10.0805892…   185.1[redacted]   10.6[redacted]    TCP        70 3912 → 53334 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM
 7304 2025-04-29 11:16:10.0851279…   10.63[redacted]   185.[redacted]    TCP        64 53334 → 3912 [ACK] Seq=1 Ack=1 Win=131584 Len=0
 7305 2025-04-29 11:16:10.0905054…   10.63[redacted]   185.[redacted]    TLSv1.3   224 Client Hello
 7306 2025-04-29 11:16:10.2523160…   185.1[redacted]   10.6[redacted]    TLSv1.3   186 Server Hello
 7307 2025-04-29 11:16:10.3124168…   10.63[redacted]   185.[redacted]    TCP        64 53334 → 3912 [ACK] Seq=167 Ack=129 Win=131328 Len=0
 7308 2025-04-29 11:16:10.4700303…   185.1[redacted]   10.6[redacted]    TCP        64 3912 → 53334 [RST, ACK] Seq=129 Ack=167 Win=2096896 Len=0
 7309 2025-04-29 11:16:11.1196384…   10.63[redacted]   185.[redacted]    TCP        70 53283 → 3912 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
 7310 2025-04-29 11:16:11.2771142…   185.1[redacted]   10.6[redacted]    TCP        70 3912 → 53283 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400 WS=256 SACK_PERM
```

```
› Frame 7354: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on i[redacted]terface Port A (ERF Host ac1f6b
› Extensible Record Format
› Ethernet II, Src: Intel_ed:d5:ff (3c:21:9c:ed:d5:ff), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
› Internet Protocol Version 4, Src: 10.63[redacted] Dst: 185.196[redacted]
› Transmission Control Protocol, Src Port: 53337, Dst Port: 3912, Seq: 167, Ack: 129, Len: 0
```

```
0000  00 00 5e 00 01[redacted]  9c ed d5 ff [redacted]  ··^···<!  ······E·
0010  00 28 fb 8e 40[redacted]  fa 95 0a 3f [redacted]  ·(··@···  ···?60··
0020  09 f8 d0 59 0f[redacted]  eb a9 09 df [redacted]  ···Y·H··  ····4·P·
0030  02 01 d0 0c 00[redacted]  00 00 00 00 [redacted]  ········  ·····h=·
```

Figure 31: PCAP viewed in Wireshark (EndaceProbe).

7. Extensibility and open ecosystem

This Cisco Event SOCs reference architecture is built around an open, API-driven operating model because event environments are dynamic and the toolchain must adapt quickly without breaking day-to-day operations. During setup for a live conference, new telemetry sources appear from new vendors joining the team, and detection patterns shift as the threat landscape changes. An open ecosystem lets the SOC onboard new event sources, add enrichment, and automate repeatable actions while keeping workflows consistent.

7.1. Why extensibility matters in an event SOC

Extensibility is not about integrating “everything.” It is about shortening time-to-decision when the environment changes. In practice, this means being able to add a new log source, enrichment feed, or investigation pivots. Cisco XDR benefits when new context lands inside the incident record and produces predictable pivots to evidence. Splunk benefits when new data can be normalized quickly for correlation and hunting. Open ecosystem capabilities also support SOC maturity. A less mature team can start with a small set of high-value integrations and repeatable workflows that deliver consistent triage from day one. A more mature team can expand into deeper correlation, automation, and enrichment.

7.2. Integration should enable capability, not just ingest data

We evaluate integrations by what they allow analysts to do, not by how much data they produce. A high-value integration typically enables one or more of the following outcomes:

- Better detection fidelity through richer fields, enhanced context, or higher-confidence detections
- Faster investigations through predictable pivots to evidence such as PCAP, DNS history, or correlated SIEM events
- Stronger situational awareness through dashboards and shared reporting
- Improved asset and entity context so analysts can quickly understand “what is this device or segment”
- Safer response through scoped, AI assisted response processes

Connectivity

- **Seamless communication:** Enables effortless information flow
- **Interoperability:** Systems and devices work together
- **Global reach:** Connects people and markets worldwide

Flexibility

- **Adaptable:** Quickly responds to change
- **Scalable:** Expands or contracts easily
- **Customizable:** Tailors solutions to specific needs

Community

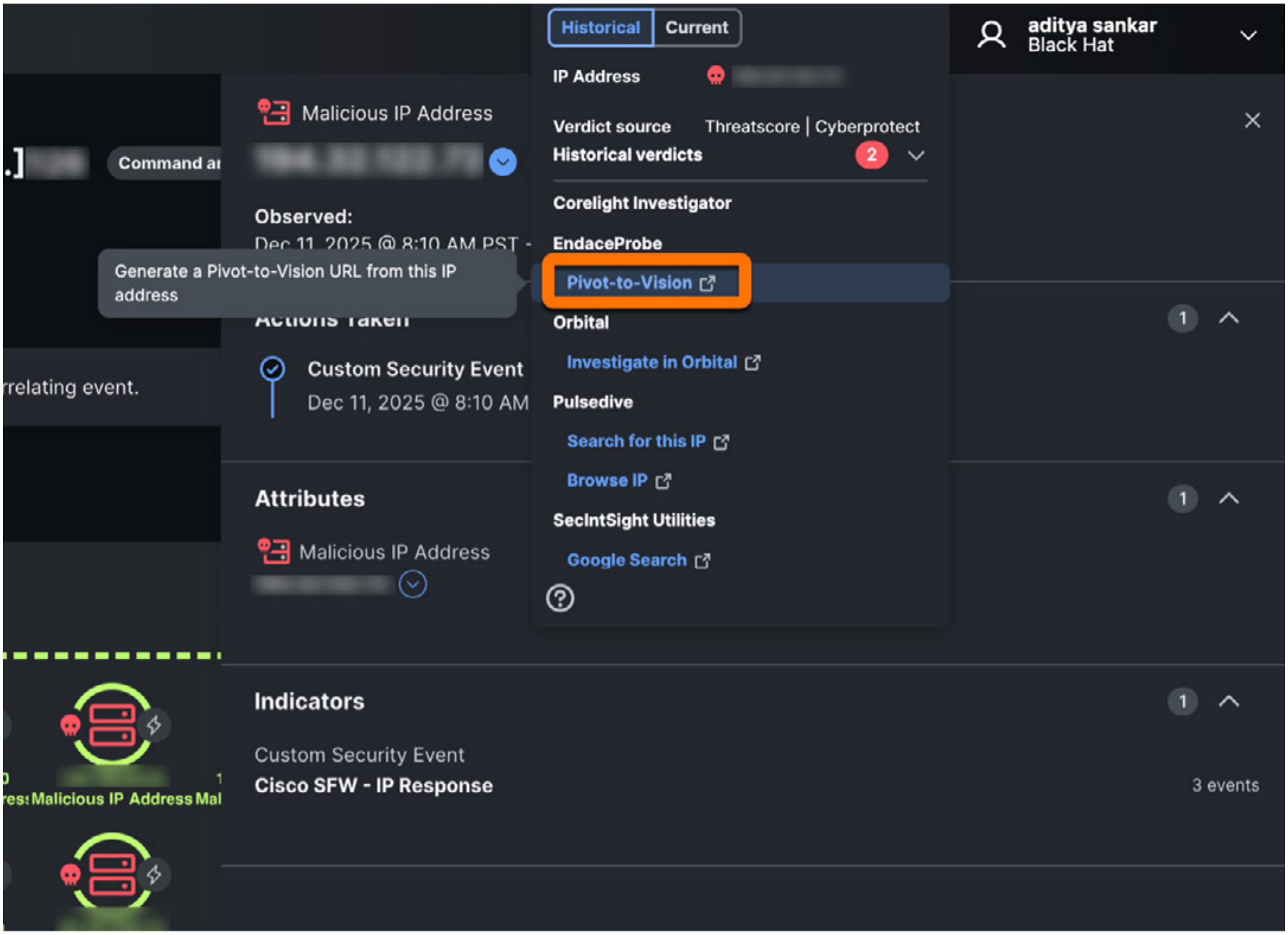
- **Collaboration:** Shared knowledge and resources
- **Support:** Peer-to-peer assistance
- **Innovation:** Collective problem-solving

Figure 32: Importance of Open ecosystem.

This capability-focused approach avoids the most common failure mode of open ecosystems, which is adding telemetry faster than the SOC can operationalize it. When integrations are selected for the analyst outcomes they enable, new data improves detection fidelity, speeds up investigations through reliable pivots, and supports safer response actions instead of inflating alert volume. It also gives the SOC flexibility to adopt best-of-breed tools without redesigning workflows each time. The result is an ecosystem that can evolve during live operations while staying usable, defensible, and consistent for the team.

7.3. Cisco XDR extensibility

Cisco XDR is the workflow hub for Tier 1 and Tier 2. Extensibility matters most when it reduces analyst friction. The best integrations pull high-value context into the incident record, standardize enrichment, and provide direct pivots to authoritative sources like packet evidence and SIEM logs. This keeps frontline workflows fast and consistent, and it improves escalation quality when a senior analyst needs to take over.



Historical | Current

IP Address [redacted]

Verdict source: Threatscore | Cyberprotect

Historical verdicts 2

Corelight Investigator

EndaceProbe

Pivot-to-Vision

Orbital

Investigate in Orbital

Pulsedive

Search for this IP

Browse IP

SecIntSight Utilities

Google Search

Generate a Pivot-to-Vision URL from this IP address

aditya sankar
Black Hat

Malicious IP Address

[redacted]

Command ar

Observed:
Dec 11, 2025 @ 8:10 AM PST -

Actions Taken

Custom Security Event
Dec 11, 2025 @ 8:10 AM

rrelating event.

Attributes

Malicious IP Address [redacted]

Indicators

Custom Security Event
Cisco SFW - IP Response 3 events

Malicious IP Address Mal

Figure 33: XDR pivot to EndaceProbe.

Cisco XDR supports rapid discovery and deployment of integration content. This is important for event SOCs because automation must be a day-one capability, not a post-event improvement. Priority integrations include those that standardize enrichment, evidence links, collaboration notifications, and automations for OCSF (Open Cybersecurity Schema Framework) ingestion from a SIEM such as Splunk.

Cisco XDR also supports event-driven ingress patterns such as webhooks. This allows external systems, partner tools, Splunk detections, and custom analytics to trigger the same standardized incident workflows. A detection can originate anywhere, but it can still be correlated into a decision-ready incident record with consistent context and documentation. Cisco XDR is API first by design, meaning custom integrations can be created for any technology that has a REST API.

7.4. Splunk openness

Splunk Cloud and Splunk Enterprise Security provide a vendor-agnostic ingestion and analytics plane that can onboard diverse telemetry quickly. This is crucial at events because it is unrealistic to assume every signal will arrive through a single vendor pipeline. Splunk allows the SOC to normalize and correlate across sources, build event-specific detections, and run hypothesis-driven investigations.

Openness increases the importance of data quality. Parsing, normalization, time synchronization, and retention policy directly determines how effective hunting will be. In an event SOC, baselining windows are short, and analyst time is limited. Poor fields or inconsistent timestamps slow investigations and weaken conclusions.

7.5. Third-party integrations

Third-party integrations are essential because the best telemetry often comes from specialized tools. The architecture is designed so these sources contribute to the same playbook-driven operating model rather than creating separate silos. Integrations are prioritized by the operational capability they add, such as richer entity context, stronger evidence fidelity, improved coverage for a known gap, or safer response options. Sources that increase alert volume without improving decision quality are deprioritized.

Common third-party integrations used in event SOC deployments include Endace for packet evidence and pivots, Palo Alto Networks telemetry into Splunk and XDR, Corelight NDR into Splunk and XDR, threat intelligence sources such as alphaMountain, Pulsedive, and StealthMole enrichment in XDR, Jamf Pro for MDM and asset context, and Slack and Cisco Webex integrations for incident notifications and bot-driven workflows via API.

Together, these open ecosystem capabilities make the SOC adaptable without becoming chaotic. They allow the team to integrate new signal quickly, preserve consistent workflows, and continuously improve outcomes across repeated events.

8. Security of the SOC infrastructure

The SOC does not just monitor the event; it must also defend its own critical infrastructure. The “SOC in a Box” and its associated cloud assets are high-value targets. To ensure operational integrity, we deploy a dedicated security stack to protect the SOC’s compute, cloud assets, and connectivity. This “SOC protecting the SOC” model leverages AI Defense, cloud-native firewalls, workload protection, and deep observability.

8.1. AI defense: Protecting the AI-enabled cloud

Securing the AI model interaction: The SOC leverages Large Language Models (LLMs) to summarize incidents and generate response scripts. AI Defense sits between the analyst’s prompt and the model, acting as a security gateway.

Prompt injection protection: It inspects inputs to prevent “jailbreaking” or prompt injection attacks where malicious actors might try to manipulate the AI into revealing sensitive configuration data or bypassing safety guardrails.

Data privacy & redaction: Before data is sent to an inference model, AI Defense ensures that sensitive PII (Personally Identifiable Information) or specific event-sensitive data is redacted or tokenized, ensuring that customer or attendee data does not inadvertently train public models.

Protecting the AI runtime environment: The cloud infrastructure hosting these AI services (within Cisco Security Cloud and Splunk Cloud) is secured using the same principles as our critical workloads, but with specific tuning for AI behaviors:

- **Model integrity:** We monitor for anomalies in model behavior that might indicate “model poisoning” or unauthorized drift.
- **Resource exhaustion defense:** AI workloads are computationally intensive. We monitor for Denial of Wallet (DoW) or Denial of Service (DoS) attacks targeting the AI inference APIs to ensure these expensive resources remain available for legitimate SOC operations.
- **Visibility into Shadow AI:** Just as we monitor for Shadow IT, the SOC uses AI Defense capabilities to detect “Shadow AI” usage. This ensures that analysts or other event staff are not pasting sensitive event telemetry into unapproved, public generative AI tools. By enforcing policy at the browser and network level (via Cisco Secure Access), we ensure that all AI interaction happens solely through the sanctioned, secured channels of the Cisco and Splunk platforms.

8.2. Cloud asset protection: Multicloud defense

We utilize **Cisco Multicloud Defense,** a cloud-native firewall offering, to protect the SOC’s cloud assets (e.g., AWS deployments) from malicious IPs, injection attacks, and general threat traffic. Its ease of deployment and high availability features allow us to secure cloud environments rapidly.

Operational workflow example: During RSAC™ 2025 Conference, Multicloud Defense successfully identified a potential Remote Access Trojan on a cloud asset via its Web Application Firewall (WAF) dashboard. The workflow proceeded as follows:

1. **Detection:** The WAF flagged a specific IP address as a potential Trojan.
2. **Visualization:** Splunk Multicloud Defense dashboards provided a high-level overview of the IDS and File Malware events, offering a complete picture of the security posture.

3. **Investigation:** Analysts pivoted to **Cisco XDR** and **Cisco Secure Malware Analytics (SMA)** to investigate the suspicious IP.
4. **Detonation & analysis:** A controlled experiment was crafted within SMA to replicate the activity. The investigation identified a Chrome browser extension plugin designed for audio control. While not explicitly malware, SMA assigned a threat score of 75, and Talos intelligence categorized it as medium severity.

Conclusion: The malware was confirmed to be a machine-generated directory propagating aggressive, unblockable adware.

This integration demonstrates how the SOC uses its own toolchain including Multicloud Defense, Splunk, XDR, and SMA to detect, analyze, and neutralize threats targeting SOC infrastructure.

8.3. Workload Zero Trust & segmentation: Cisco Secure workload

To secure the compute layer, we deploy Cisco Secure Workload (formerly Tetration). This platform uses software agents, ERSPAN, and NetFlow to collect rich telemetry from servers, virtual machines, and endpoints. It applies unsupervised machine learning to baseline behavior and enforce a Zero Trust model within the SOC's own data center.

Key technical objectives:

- **Baseline behavior:** Understanding application dependencies and normal traffic patterns (e.g., baselining the 'te-web' application).
- **Policy enforcement:** Providing segmentation through workload-enforced security policies to reduce the attack surface.
- **Vulnerability management:** Identifying process behaviors, software vulnerabilities, and compliance deviations (e.g., TLS version usage) in near-real time.
- **Forensics:** Retaining detailed workload information for deep troubleshooting and analysis.

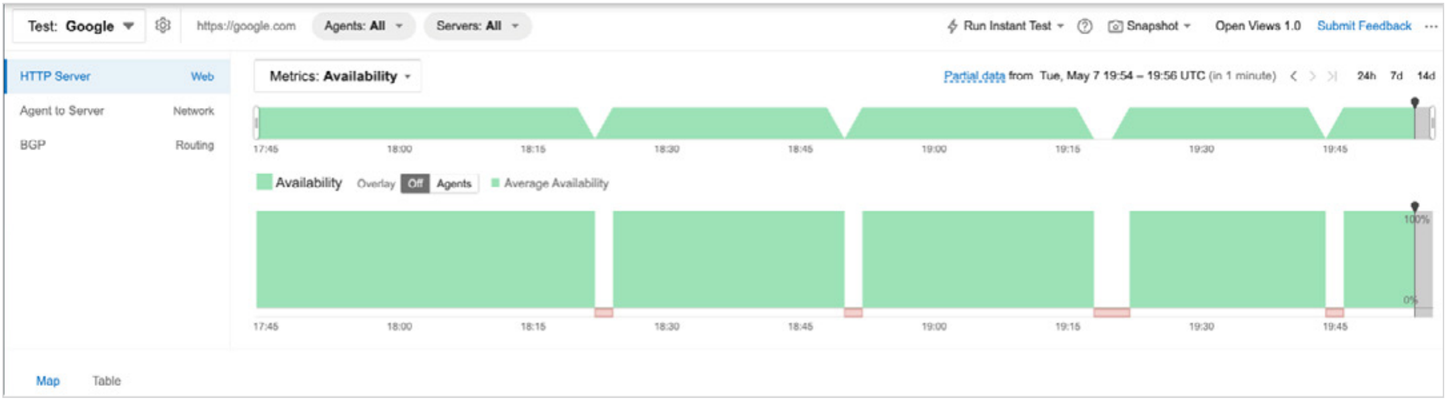
For the event SOC, we specifically deployed an 'Ingest' virtual appliance to accept NetFlow/NSEL from Endace and other sources. This allows us to stitch flows together and view compliance risk via a unified dashboard, ensuring that even if a node is replaced or behavior changes, the SOC maintains visibility into "escaped" traffic and policy adherence.

8.4. Infrastructure observability: ThousandEyes

To distinguish between a security incident and a network outage, we deploy **ThousandEyes.** It provides network availability observation from the perspective of the SOC and its connection to management tools.

Why it matters: The dashboard provides real-time metrics on response time, DNS resolution time, and link speed for SOC assets. This allows the team to:

1. Quickly identify the root cause of high latency or outages.
2. Proactively coordinate with the NOC to resolve connectivity issues.
3. Avoid “blaming the network” without proof, ensuring that security analysts focus on true threats rather than infrastructure troubleshooting.



Test: Google
https://google.com
Agents: All
Servers: All
Metrics: Availability
Partial data from Tue, May 7 19:54 – 19:56 UTC (in 1 minute)
Overlay Off Agents

Figure 34: ThousandEyes helping to identify the root case of a network outage.

9. Staffing

SOC Leader and Co-Leader

Provide overall direction and decision authority for SOC operations. Sets severity posture, owns escalation and approval paths for high-impact actions. This role sets the governance tone by defining what actions are allowed, what evidence is required before enforcement, and how decisions are documented and communicated to stakeholders.

SOC Deployment Lead (Architecture and Build Owner)

Owns end-to-end build, readiness, and teardown of the event SOC deployment. This role has deep familiarity with the SOC in a Box technology stack and is responsible for bringing the SOC online from a zero baseline, so operational workflows can begin.

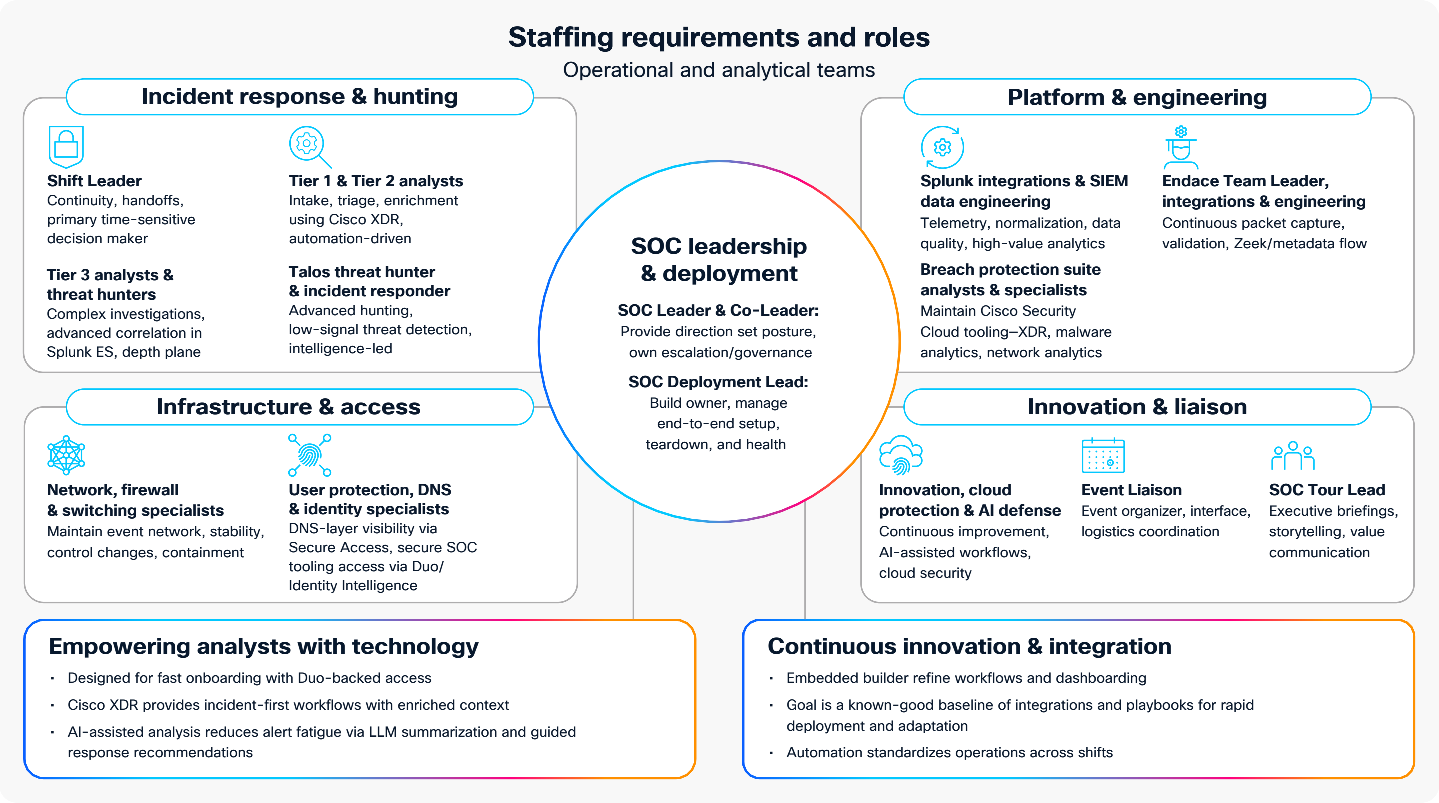
The Deployment Lead coordinates partners and specialists during set up. They communicate dependencies between tools, and ensures the overall design vision is implemented correctly. During the event, they oversee the health of the deployment, drive resolution of platform-level issues that impact visibility or workflows and own the post-event teardown and readiness reset for the next deployment.

Splunk integrations and SIEM data engineering

Maintains telemetry onboarding, parsing, normalization, and data quality across sources feeding Splunk Cloud and Splunk ES. Ensures the analytics plane is reliable and supports high-value dashboards, correlation content, and investigation patterns.

Shift Leader (staffed when operating 24 hours)

Ensures continuity within a shift and owns the quality of handoffs. Maintains discipline around playbook execution, incident documentation, and escalation pathways. Acts as the primary decision-maker for time-sensitive issues when SOC leadership is not immediately available.



Staffing requirements and roles

Operational and analytical teams

Incident response & hunting

Shift Leader
Continuity, handoffs, primary time-sensitive decision maker

Tier 1 & Tier 2 analysts
Intake, triage, enrichment using Cisco XDR, automation-driven

Tier 3 analysts & threat hunters
Complex investigations, advanced correlation in Splunk ES, depth plane

Talos threat hunter & incident responder
Advanced hunting, low-signal threat detection, intelligence-led

Infrastructure & access

Network, firewall & switching specialists
Maintain event network, stability, control changes, containment

User protection, DNS & identity specialists
DNS-layer visibility via Secure Access, secure SOC tooling access via Duo/ Identity Intelligence

SOC leadership & deployment

SOC Leader & Co-Leader:
Provide direction set posture, own escalation/governance

SOC Deployment Lead:
Build owner, manage end-to-end setup, teardown, and health

Platform & engineering

Splunk integrations & SIEM data engineering
Telemetry, normalization, data quality, high-value analytics

Endace Team Leader, integrations & engineering
Continuous packet capture, validation, Zeek/metadata flow

Breach protection suite analysts & specialists
Maintain Cisco Security Cloud tooling–XDR, malware analytics, network analytics

Innovation & liaison

Innovation, cloud protection & AI defense
Continuous improvement, AI-assisted workflows, cloud security

Event Liaison
Event organizer, interface, logistics coordination

SOC Tour Lead
Executive briefings, storytelling, value communication

Empowering analysts with technology

- Designed for fast onboarding with Duo-backed access
- Cisco XDR provides incident-first workflows with enriched context
- AI-assisted analysis reduces alert fatigue via LLM summarization and guided response recommendations

Continuous innovation & integration

- Embedded builder refine workflows and dashboarding
- Goal is a known-good baseline of integrations and playbooks for rapid deployment and adaptation
- Automation standardizes operations across shifts

Figure 35: Staffing roles.

Tier 1 and Tier 2 analysts (incident-centric operations)

Execute alert intake, triage, enrichment, initial scoping, and escalation using Cisco XDR as the primary console. These roles are most effective when playbooks define clear decision gates for escalation, containment requests, and closure. The junior analysts handle the majority of incidents when enrichment, evidence pivots, and response ladders are well operationalized.

Tier 3 analysts and threat hunters (depth plane)

Conduct complex investigations, advanced correlation, and hypothesis-driven hunting primarily in Splunk Enterprise Security and supporting evidence platforms. The senior analyst also owns converting discoveries into tuned detections, improved enrichment, scoped suppressions, and response recommendations.

Network, firewall, and switching specialists

Maintain stability and availability of the event network and implement approved control changes. This role is critical to selective response because it ensures containment actions are scoped, reversible, and coordinated with operational availability requirements. It owns or supports execution of enforcement changes when the SOC requests containment.

Endace team leader, integrations, and engineering

Operate the continuous packet capture platform, packet validation for investigations and closure. Ensures EndaceProbes remain reliable, that Zeek and related metadata flows into Splunk and Cisco Secure Network Analytics. They also ensure that analysts have predictable pivots for packet-level evidence when needed.

User protection, DNS, and identity specialists

Maintain DNS-layer visibility and controls and secure access to SOC tooling. Operate Cisco Secure Access for DNS security and application visibility, Cisco Duo and Cisco Identity Intelligence for MFA, SSO, and rapid onboarding. The primary object for this role is to ensure all DNS traffic flows through Secure Access for visibility and security.

Breach Protection Suite analysts and specialists

Support Tier 1 and Tier 2 operations by maintaining the Cisco Security Cloud tooling that powers incident workflows, enrichment, and automation. This includes Cisco XDR, Cisco Secure Malware Analytics for sandbox detonation, and Cisco Secure Network Analytics for network behavior visibility and anomaly context. These specialists keep the platform tuned and operational, so frontline workflows remain fast and consistent.

Talos threat hunter and incident responder

Provide advanced threat hunting and incident response depth, leveraging Talos intelligence and tradecraft to surface sophisticated or low-signal threats. This role supports high-confidence outcomes when additional expertise is needed to interpret emerging patterns and validate risk. Starting with a strong hypothesis, these threat hunters sift through telemetry data to potentially uncover threats that have not been alerted on.

Innovation, cloud protection, and AI defense

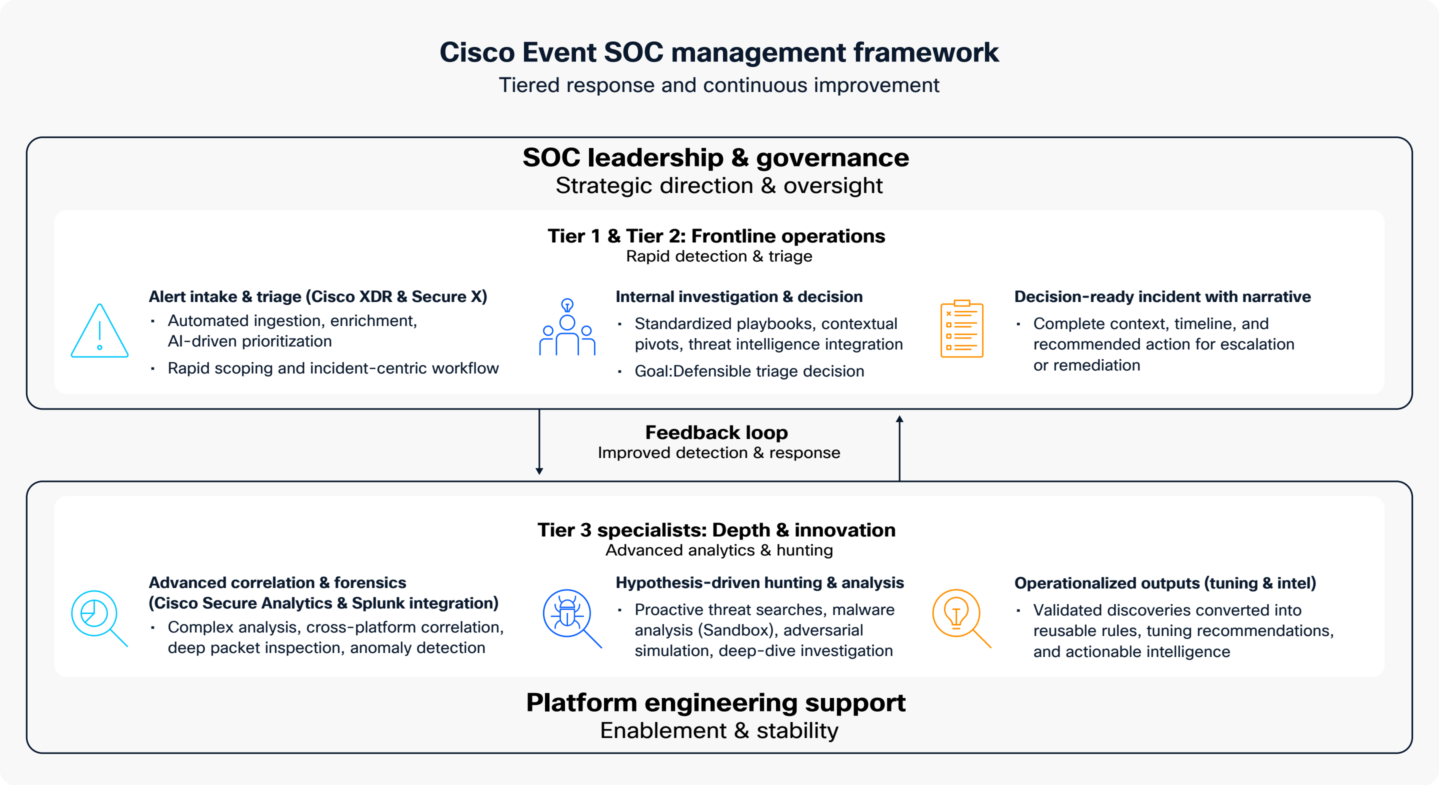
Drive continuous improvement during and between events. Develops new integrations, refines workflows, and operationalizes automation, particularly where AI-assisted capabilities can reduce toil. Secures the SOC’s cloud infrastructure and supports safe adoption of AI-enabled workflows and custom models where applicable.

Event Liaison (Event operations point of contact)

Serves as the primary interface between the SOC and event organizers. Owns coordination for event requirements, SOC location and access logistics, power and network readiness checks, special requests, and tour scheduling. This role protects engineering and analyst time by resolving operational coordination issues quickly and proactively.

SOC Tour Lead (executive briefing and storytelling)

Leads SOC tours and briefings for groups that often include attendees, analysts, executives, and CISOs. Translates SOC operations into an understandable narrative and communicates value using metrics, examples, and tool demonstrations appropriate to the audience. Brings seniority and credibility to explain why the SOC exists, how the toolchain works together, and what innovations are driving improved outcomes.



Cisco Event SOC management framework

Tiered response and continuous improvement

SOC leadership & governance

Strategic direction & oversight

Tier 1 & Tier 2: Frontline operations

Rapid detection & triage

Alert intake & triage (Cisco XDR & Secure X)

- Automated ingestion, enrichment, AI-driven prioritization
- Rapid scoping and incident-centric workflow

Internal investigation & decision

- Standardized playbooks, contextual pivots, threat intelligence integration
- Goal:Defensible triage decision

Decision-ready incident with narrative

- Complete context, timeline, and recommended action for escalation or remediation

Feedback loop

Improved detection & response

Tier 3 specialists: Depth & innovation

Advanced analytics & hunting

Advanced correlation & forensics (Cisco Secure Analytics & Splunk integration)

- Complex analysis, cross-platform correlation, deep packet inspection, anomaly detection

Hypothesis-driven hunting & analysis

- Proactive threat searches, malware analysis (Sandbox), adversarial simulation, deep-dive investigation

Operationalized outputs (tuning & intel)

- Validated discoveries converted into reusable rules, tuning recommendations, and actionable intelligence

Platform engineering support

Enablement & stability

Figure 36: Staffing requirements and roles.

Empowering Tier 1 and Tier 2 analysts with technology

The staffing model depends on Tier 1 and Tier 2 being productive quickly and consistently, even when they are not experts in every tool on day one. We designed for fast onboarding and low friction access so analysts can get into the toolchain quickly, then rely on a consistent incident workflow to guide decisions. At recent event SOCs, new analysts were onboarded in minutes using Duo Directory-backed access, then worked primarily out of Cisco XDR where incidents already arrived with context and intelligence. This reduces the ramp up time from “new to the SOC” to “able to triage and escalate with confidence.”

The design goal is incident readiness. Incidents should arrive enriched with the key context, threat intelligence, and predictable pivots. Endace provides a direct pivot to packet-level validation when needed. Standardized documentation patterns and clear escalation paths keep outcomes consistent across shifts and reduce variability between analysts.

AI-assisted analysis is treated as decision support that reduces alert fatigue and speeds triage. LLM-based summarization turns incidents, related logs, and attack flows into a human-readable narrative. Guided response recommendations and MITRE ATT&CK mappings help analysts prioritize and choose the next best action. Analysts still validate conclusions against telemetry, and approval gates remain in place for actions that could affect availability or attendee experience.

Integration engineers and continuous innovation

Repeatable event SOC success requires integration specialists embedded in operations. These may be dedicated integration engineers or analysts who can translate operational friction into improvements quickly. They refine dashboards, strengthen pivots, expand integrations, and operationalize playbooks.

For organizations without dedicated integration specialists, this capability can be built incrementally. Standardize integration patterns, document workflows, and treat automation content as managed assets. Over time, the goal is a known-good baseline of integrations, dashboards, and playbooks that can be deployed quickly and adapted safely for constraints.

10. Why we made these choices

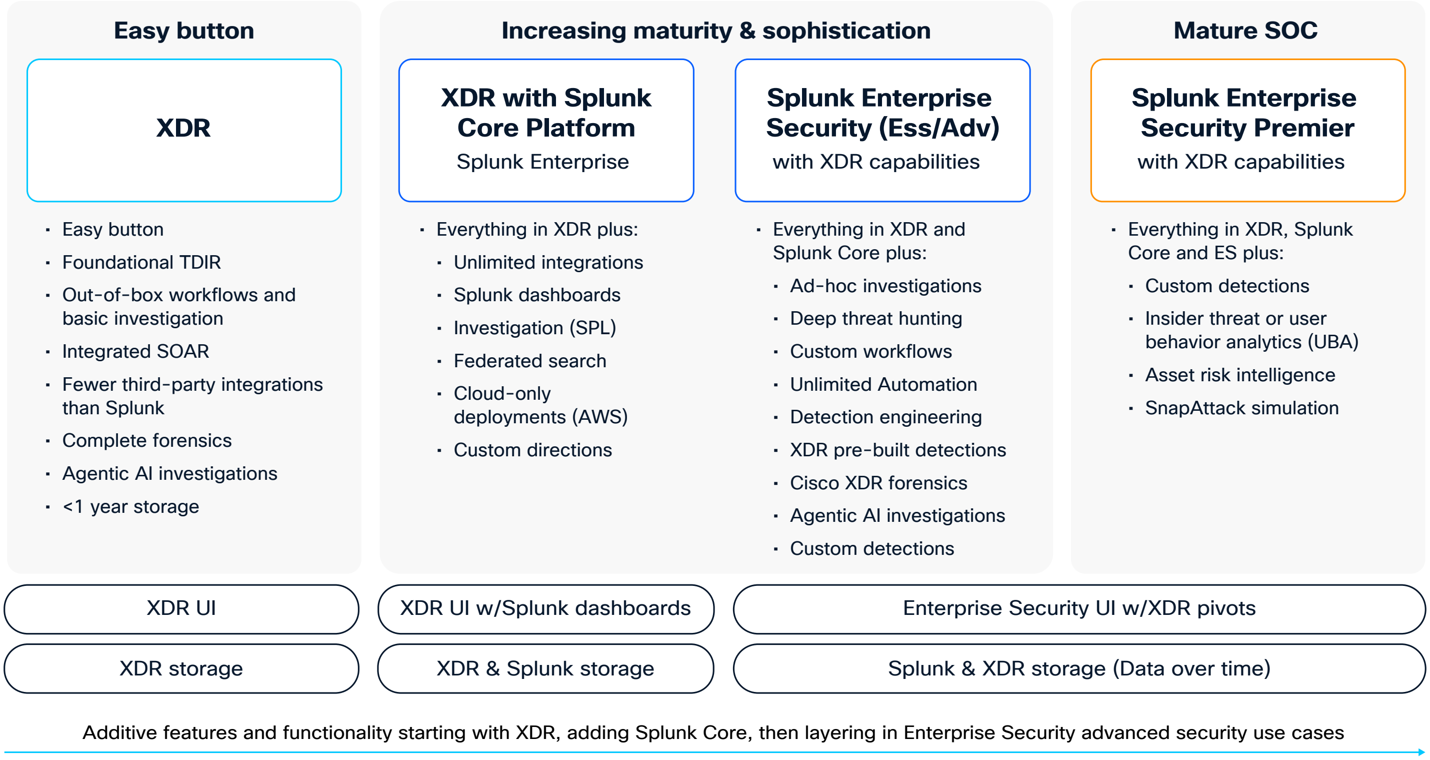
The architectural and operational choices in this document are grounded in real deployment constraints seen at large, high-noise cybersecurity conferences. These environments combine high background scanning, limited endpoint authority, constrained baselining windows, heavy encryption, and a requirement to preserve availability while protecting critical services. Our choices align to the mission to Protect, Educate, and Innovate, and they are optimized for repeatability: deploy quickly, operate consistently under pressure, and improve measurably over successive deployments.

Cloud-centric architecture: Cisco Security Cloud and Splunk Cloud

We chose a cloud-centric approach to accelerate deployment and standardize operations across venues. Cloud delivery centralizes configuration and analytics, supports elastic scaling, and enables reuse of dashboards, detections, and workflows with minimal rework between events. The event SOC team is in the middle of its maturity journey.

Deep integration and an open ecosystem

Event environments often include partner tooling and venue-specific constraints. We chose deep integration and an open ecosystem because event SOCs must connect many security controls and evidence sources quickly. Cisco XDR provides the primary incident queue for analysts, while Splunk provides broad correlation and hunting across the full dataset. The value of open APIs is practical. It lets us add third-party telemetry, enrichments, and response actions without redesigning workflows each time. It also enables consistent pivots from an alert to the right evidence source such as DNS history, firewall events, or packet capture. This approach keeps operations flexible and prevents the SOC from becoming dependent on any single tool's data model or integration roadmap.



Easy button

XDR

- Easy button
- Foundational TDIR
- Out-of-box workflows and basic investigation
- Integrated SOAR
- Fewer third-party integrations than Splunk
- Complete forensics
- Agentic AI investigations
- <1 year storage

Increasing maturity & sophistication

XDR with Splunk Core Platform
Splunk Enterprise

- Everything in XDR plus:
  - Unlimited integrations
  - Splunk dashboards
  - Investigation (SPL)
  - Federated search
  - Cloud-only deployments (AWS)
  - Custom directions

Splunk Enterprise Security (Ess/Adv)
with XDR capabilities

- Everything in XDR and Splunk Core plus:
  - Ad-hoc investigations
  - Deep threat hunting
  - Custom workflows
  - Unlimited Automation
  - Detection engineering
  - XDR pre-built detections
  - Cisco XDR forensics
  - Agentic AI investigations
  - Custom detections

Mature SOC

Splunk Enterprise Security Premier
with XDR capabilities

- Everything in XDR, Splunk Core and ES plus:
  - Custom detections
  - Insider threat or user behavior analytics (UBA)
  - Asset risk intelligence
  - SnapAttack simulation

XDR UI | XDR UI w/Splunk dashboards | Enterprise Security UI w/XDR pivots

XDR storage | XDR & Splunk storage | Splunk & XDR storage (Data over time)

Additive features and functionality starting with XDR, adding Splunk Core, then layering in Enterprise Security advanced security use cases

Figure 37: Increasing SOC maturity.

SOC in a Box hardware foundation

Rapid deployment and portability are core requirements for event SOCs. A standardized portable foundation reduces onsite engineering risk, accelerates time-to-visibility, and makes repeated deployments predictable. It also enforces known-good data paths and trust boundaries, including where telemetry originates, where evidence is captured, and how data is forwarded to cloud analytics. Standardization improves resiliency because troubleshooting and recovery procedures can be reused across deployments.

Dedicated full packet capture: EndaceProbes

Definitive evidence matters when endpoint coverage is limited and much traffic is encrypted. Full packet capture enables deeper investigations when flow logs alone are insufficient. There are rigorous packet capture data destruction requirements due to the sensitivity of the data.

Cisco XDR as the central hub for Tier 1 and Tier 2

Frontline throughput determines whether the SOC remains effective. Cisco XDR provides the incident-centric queue that consolidates detections, enrichment, and automation into repeatable workflows. It improves consistency by standardizing enrichment, guiding investigation pivots, and structuring documentation so the incident record stays consistent across shifts. This design prioritizes operational clarity by maintaining a single record that can be escalated, audited, and closed consistently.

Splunk Enterprise Security for Tier 3 investigation and hunting

Tier 3 requires correlation depth, flexible searching, and content engineering to address complex or low-signal threats. Splunk Enterprise Security facilitates advanced correlation, hunting, and detection lifecycle management. This preserves frontline efficiency while enabling deep investigations when needed, including longer-horizon analysis where appropriate.

Repeatable workflows, automation, and AI

Lean teams scale through repeatability. Automation reduces manual effort, standardizes enrichment and documentation, and makes workflows consistent across shifts. AI accelerates time-to-understanding by summarizing incidents and attack flows, suggesting investigation pivots, and supporting prioritization through guided actions and MITRE ATT&CK mappings.

Selective, risk-aware response

Event response must protect critical services while preserving availability and attendee experience. Response actions are scoped, reversible, and auditable, with structured containment requests and playbook-defined decision gates. This supports different operating models, including SOC-executed or NOC-executed changes, while maintaining a stable and predictable response posture.

Strategic staffing and empowerment

This model is designed so Tier 1 and Tier 2 handle most incident volume consistently, while Tier 3 focuses on deeper investigations and continuous improvement. Specialists in network operations, identity and access management, packet evidence, and data engineering keep the deployment safe and resilient while every analyst still maintains a generalist skillset. Clear handoffs, analyst empowerment, and auditable decision-making support both operational effectiveness and sustainability.

Together, these choices create a SOC model that can be deployed quickly, operated consistently, and improved iteratively. Each event contributes lessons that are translated into reusable integrations, workflows, and detections that strengthen the baseline for the next deployment.

11. Continuous innovation

This document is intended to serve as a living prototype that evolves with every event. Each deployment runs in a real environment with real constraints such as high noise, compressed baselining, limited endpoint governance, and a response posture that must preserve availability. These conditions expose friction quickly, including missing context, noisy detections, brittle pivots, and ambiguous escalation paths. Continuous innovation is treated as an operational loop: **observe** what slowed triage or reduced confidence, implement improvements as repeatable workflows with guardrails, and reuse those improvements as part of the baseline for the next deployment. The intent is measurable progress over time, including faster triage, fewer unnecessary escalations, higher-confidence decisions, and safer controls that remain reversible.

11.1. Observe-Orient-Decide-Act

Within Cyber Security we typically refer to this as Observe-Orient-Decide-Act (OODA) and we have to progress through this loop faster.

- We **observe** through telemetry and detections,
- **orient** through enrichment and segment context,
- **decide** using playbook-driven decision gates and
- **act** through scoped response actions and validated outcomes.

The goal is to tighten the loop, so analysts spend less time assembling context and more time making defensible decisions.

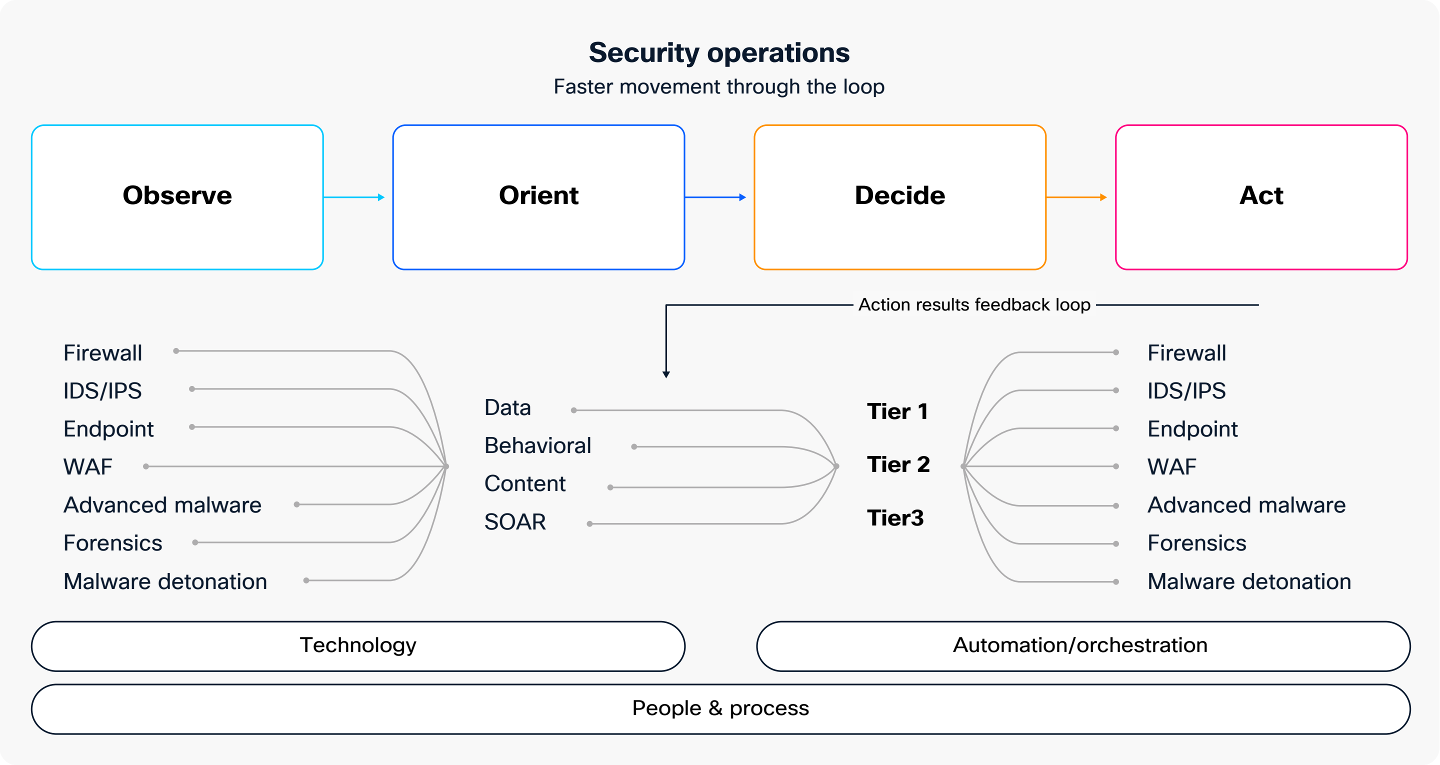


Figure 38: SecOps OODA loop.

11.2. Splunk Security Maturity Methodology

As we look toward upcoming deployments at **Cisco Live EMEA 2026 and beyond,** our focus shifts to reducing the operational separation between analyst tiers. The only way to do this is by adopting a maturity model, like the Splunk Security Maturity Methodology **(S2M2).** This methodology will help us identify where our gaps are in people, process and technology while enabling us to prioritize risk and eliminate noise. These events aren't just about deploying technology but being able to navigate the correct blend of People, Process and Technology (just like in an actual corporate environment). A SOC, as defined by SANS, is "A **combination** of people, processes and technology protecting information systems of an organization through proactive design and configuration, ongoing monitoring of system state, detection of unintended actions or undesirable state and minimizing damage from unwanted effects."

S2M2 is the methodology that helps our customers to fully adopt our products to help scale their security operations, no matter the team size. Technology is a multiplier, not a force replacement, this methodology helps us identify the gaps in our tooling to see where things like Artificial Intelligence, Machine Learning, Security Orchestration and Automation for response, Extended Detection and Response can best augment ours and your operations.

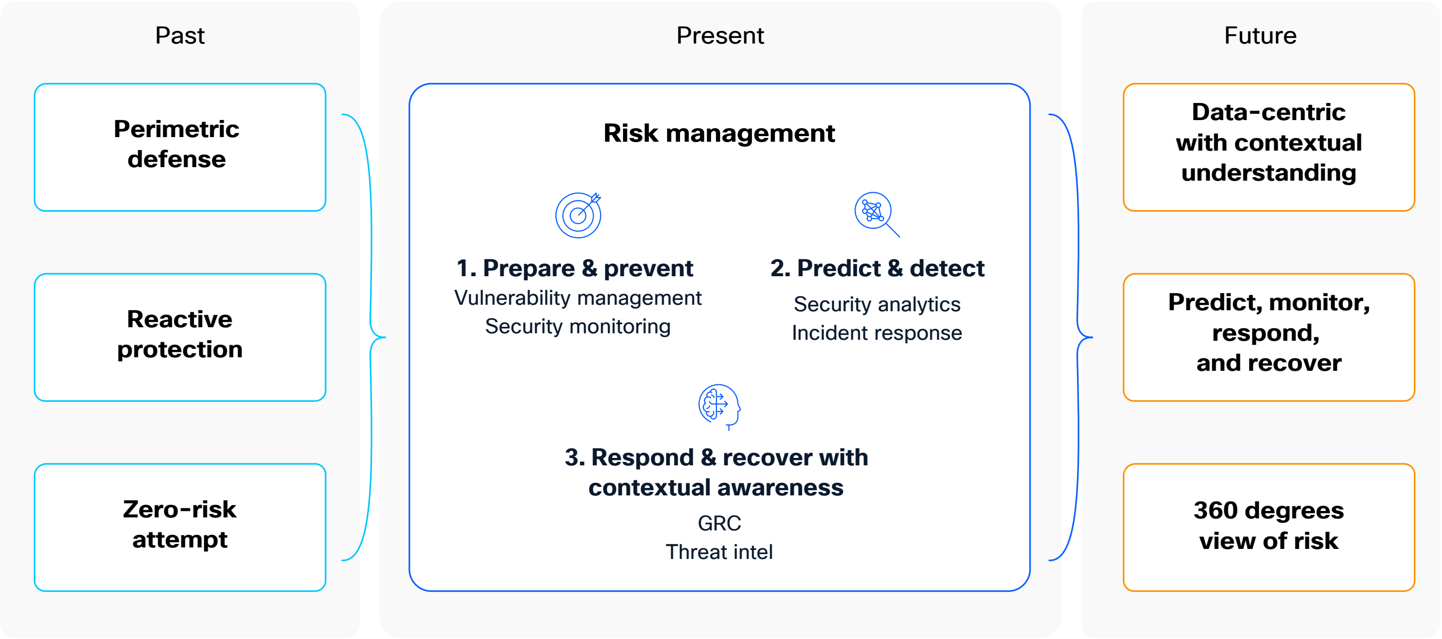


Figure 39: 360 degree view of risk.

We identified five primary outcomes that we would like to see in the coming events:

- **Accelerate time to value:** Rapidly deploying a fully functional, integrated SOC
- **Reduce noise:** Utilizing Risk-Based Alerting (RBA) in Splunk ES to filter millions of event logs into actionable intelligence while utilizing XDR analytics for quicker verdicts
- **Holistic maturity:** Operationalizing high-fidelity data streams from Cisco XDR alongside disparate third-party sources within a SIEM
- **A reference and inspiration** to maturing SOC's who want to add capability but are afraid of breaking things
- **A demonstration** of how Cisco utilizes our own tools along with partner tools and integrations in a live SOC

This is less about forcing everything into one interface and more about reducing friction through consistent enrichment at intake, predictable pivots to authoritative evidence, and standardized documentation and handoffs.

We will continue to modernize the SOC by aligning the toolchain to the emerging AI data fabric, where AI capabilities are integrated into the same workflows analysts already use. AI is applied to accelerate understanding and consistency by summarizing incidents, narrating timelines, highlighting likely pivots, and reducing repetitive interpretation of long log trails. The objective is faster, more consistent decisions, not automated decision-making without accountability. As these capabilities mature, we also expect to expand how we operationalize **MCP and agentic AI** so assistants can execute well-scoped tasks inside governed workflows while analysts retain validation and decision authority.

11.3. Democratizing advanced analytics

To advance the maturity of the entire team, our evolving architecture implements a "Democratization of Analytics" strategy.

- **Current state:** Analysts tend to silo themselves into one tool.
- **Future state:**
  - Both Splunk ES and Cisco XDR must enrich the analyst experience through advanced curated analytics and the ability to deep dive into the who, what, where, when in the data to determine root cause.
  - Additionally, by pulling deep-packet insights directly into your SIEM, analysts can perform advanced investigations without ever leaving the Splunk interface. This effectively extends Splunk's correlation power with a dedicated network analysis layer.

By curating specific content and simplified search workflows within Splunk, we aim to:

- **Reduce escalation latency** by allowing Threat Hunters and Analysts alike the ability to validate common hypotheses directly.
- **Enhance context** by providing a broader view across time and across related signals, beyond the immediate incident window
- **Upskill the workforce** by quickly moving analysts from alert consumption to evidence-driven investigation in a live environment

The future of the integrated analyst

Ultimately, this innovation supports our broader staffing strategy. By blurring the practical separation between triage and hunting workflows, Tier 2 analysts can handle higher complexity incidents with more confidence, which reduces dependency on Tier 3 for common scoping tasks. Tier 3 retains focus on the most sophisticated and low-signal threats. This includes converting discoveries into tuned detections, improved enrichment, scoped suppressions, and response recommendations.

A key part of this maturity path is formalizing response and learning using industry standard response frameworks like Prepartion, Identification, Containment, Eradication, Recovery and Lessons Learned (PICERL). Cisco XDR Response is aligned to the PICERL framework and it provides a consistent structure for progressing from identification through containment, eradication, and recovery. We routinely convert what worked in live incidents into reusable automation workflows that are published to the Cisco XDR Automation Exchange and new detections in Splunk. These become building blocks for custom playbooks at future events.

As the program matures, automation increasingly executes the repetitive portions of playbooks. Progress is measured using operational metrics that reflect decision quality and efficiency, like decreasing Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) which are key SOC metrics. We'll also start looking at signal to noise ratio (false positives vs. true false positives) as well as number of incidents created and closed. These measurements keep the innovation loop focused on operator benefit and repeatable improvement across deployments.

11.4. Knowledge management and carrying forward lessons learned

Event SOCs are short-lived, but the knowledge created during each deployment must compound over time while still meeting strict teardown and privacy requirements. We preserve reusable operational outcomes by maintaining a private knowledge catalogue as the system of record in the form of a GitHub repository. The repository retains only sanitized artifacts, repeatable analyst pivots, validated tuning decisions, and reusable automation workflows.

We explicitly exclude raw event telemetry such as PCAP, packet payloads, and raw logs, as well as any attendee identifiers, PII, or sensitive venue/conference operational details. Knowledge capture is continuous during live operations (shift handoffs, daily ops summaries, and a tuning change log). It is consolidated immediately post-event into an After-Action Report (AAR) that documents what worked, what did not, and the highest-confidence carry-forward updates. Validated improvements are then promoted into the reusable baseline for the next deployment including updated playbooks, searches, dashboards, enrichment updates, and automation workflows.

Reuse is anchored in the internal archive, with select outputs eligible for external publication only after sanitization and review, such as Cisco blogs.

Teardown and decommissioning guardrails ensure raw event data is wiped, retained artifacts are verified as sanitized, and event-specific collaboration surfaces (e.g., Webex Spaces, Slack channels) are decommissioned.

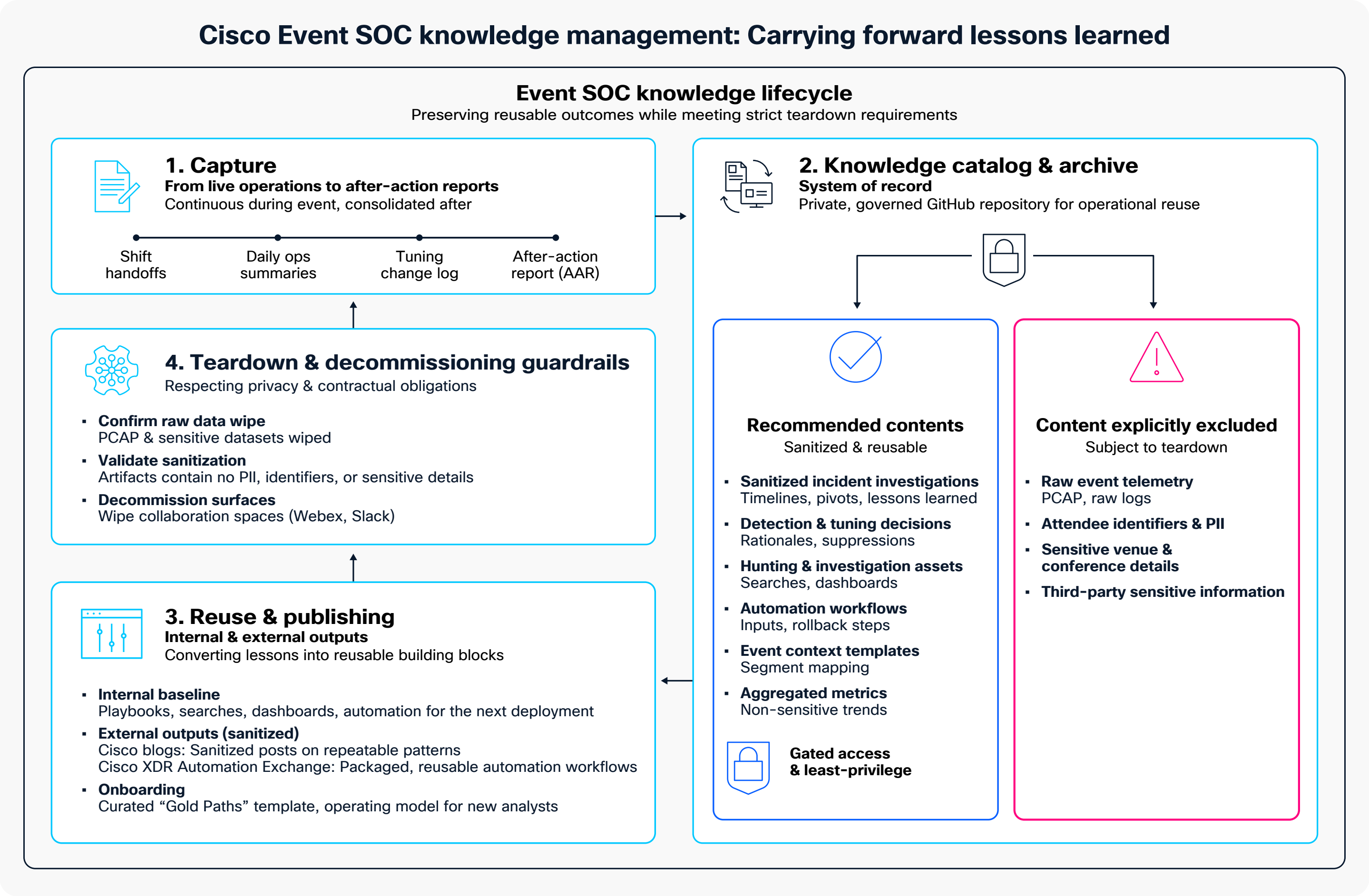

Cisco Event SOC knowledge management: Carrying forward lessons learned
Event SOC knowledge lifecycle
Preserving reusable outcomes while meeting strict teardown requirements
1. Capture
From live operations to after-action reports
Continuous during event, consolidated after
Shift handoffs
Daily ops summaries
Tuning change log
After-action report (AAR)
2. Knowledge catalog & archive
System of record
Private, governed GitHub repository for operational reuse
Recommended contents
Sanitized & reusable
Sanitized incident investigations
Timelines, pivots, lessons learned
Detection & tuning decisions
Rationales, suppressions
Hunting & investigation assets
Searches, dashboards
Automation workflows
Inputs, rollback steps
Event context templates
Segment mapping
Aggregated metrics
Non-sensitive trends
Gated access & least-privilege
Content explicitly excluded
Subject to teardown
Raw event telemetry
PCAP, raw logs
Attendee identifiers & PII
Sensitive venue & conference details
Third-party sensitive information
4. Teardown & decommissioning guardrails
Respecting privacy & contractual obligations
Confirm raw data wipe
PCAP & sensitive datasets wiped
Validate sanitization
Artifacts contain no PII, identifiers, or sensitive details
Decommission surfaces
Wipe collaboration spaces (Webex, Slack)
3. Reuse & publishing
Internal & external outputs
Converting lessons into reusable building blocks
Internal baseline
Playbooks, searches, dashboards, automation for the next deployment
External outputs (sanitized)
Cisco blogs: Sanitized posts on repeatable patterns
Cisco XDR Automation Exchange: Packaged, reusable automation workflows
Onboarding
Curated “Gold Paths” template, operating model for new analysts

Figure 40: SOC knowledge management.

12. Conclusion

The Cisco Event SOCs: A Reference Architecture and Operations Guide describes a repeatable way to stand up and operate short-lived SOCs at large events. These environments are materially different from steady-state enterprise networks. They are high-noise, identity signals are constrained, endpoint governance is limited, and much of the traffic is encrypted. Response authority can also vary by venue and stakeholder. The intent of this guide is not to prescribe one implementation. The intent is to provide a blueprint that produces consistent outcomes across deployments.

What this guide is designed to achieve

This reference architecture is optimized for the operating envelope defined in the Constraints section. It is built to deliver rapid visibility, consistent triage, and reliable escalation when the environment is dynamic and time is limited. It also emphasizes repeatability. Each event should be easier to deploy and easier to operate than the last.

Why the model is repeatable

Repeatability comes from treating SOC setup as a baseline, not an ad hoc engineering effort. Our customized SOC in a Box deployment is a key enabler. It provides a portable, known-good hardware foundation with pre-defined data paths, trust boundaries, and connectivity patterns. Cloud delivery in Cisco Security Cloud and Splunk Cloud complements this approach. It centralizes configuration, dashboards, detections, and workflows so the team can reuse what works with minimal rework. Repeatability also depends on carrying forward validated improvements through a knowledge catalogue, so lessons learned become part of the baseline, not tribal memory.

How operations stay consistent under high noise

This model uses an incident-centric workflow for Tier 1 and Tier 2, with deeper analytics and hunting for Tier 3. The separation is practical rather than rigid. It keeps default workflows efficient while still enabling deeper investigation when needed. Over the course of the event, Tier 3 improvements feed back into frontline operations. This includes tuning, enrichment updates, scoped suppressions, and curated searches that reduce noise and improve disposition quality.

Continuous improvement through OODA and PICERL

Continuous innovation is treated as an operational loop. It aligns closely with **OODA.** The SOC **observes** through telemetry and detections, **orients** through enrichment and segment context, **decides** using playbook-driven decision gates, and **acts** through scoped response steps. The goal is to tighten this loop so time-to-decision improves even when the environment changes event by event.

The incident response workflow is also grounded in SANS PICERL framework, which is reflected in the Cisco XDR Response experience. PICERL provides a common structure for preparation through recovery, and it reinforces the importance of lessons learned. Lessons learned are not just notes at the end of an event. They are converted into reusable content for the next deployment. This includes updated playbooks, refined enrichment, and automation workflows.

What success looks like in practice

- **Rapid deployment** using SOC in a Box and cloud-hosted platforms, so time-to-visibility is measured in days, not weeks
- **High-confidence triage at scale** through consistent enrichment, predictable pivots, and a clear operating model for Tier 1 and Tier 2
- **Depth when it matters** through Splunk ES correlation and hunting, plus PCAP and artifact tooling that supports closure and validation
- **Lower analyst fatigue** through repeatable workflows, automation that standardizes the first steps, and AI LLM summaries that improve time-to-triage.
- **Protected operations** through a "SOC protecting the SOC" approach that secures SOC cloud assets, workloads, and critical dependencies to preserve integrity and availability.
- **Measurable improvement over successive events** as tuning, workflows, integrations and sanitized lessons learned are carried forward as part of the baseline.

Final takeaway

This guide exists to methodize what we have learned from repeated event deployments. It shows how to build a SOC capability that can deploy quickly, operate consistently in high-noise conditions, and improve after every event. The end state is not a perfect SOC for a single venue. The end state is a portable, scalable operating model that becomes stronger with every deployment.

This guide captures that journey, showing how we evolved from a small two-product setup into a repeatable, integrated SOC capability that improves with every deployment and helps others mature along the same path.

13. Acknowledgments

The event SOC is a team effort and our deep appreciation to the engineers, analysts and event coordination teams who made the 2025 SOC season the most successful, capping ten years of work.

More is yet to come in 2026 and beyond, as we look to continue maturation, integrations and empowerment of a ‘SOC of the Future”.

Special thanks to Steve Nowell, Customer Experience (professional services) leader with the Super Bowl and Draft SOCs.

13.1. Black Hat Asia 2025

- Cisco Security: Christian Clasen, Shaun Coulter, Aditya Raghavan, Justin Murphy, Ivan Berlinson, and Ryan Maclennan
- Meraki Systems Manager: Paul Fidler, with Connor Loughlin supporting
- ThousandEyes: Shimei Cridlig and Patrick Yong
- Additional support and expertise: Tony Iacobelli and Adi Sankar

Also, to our NOC partners Palo Alto Networks (especially James Holland and Jason Reverri), Corelight (especially Mark Overholser and Eldon Koyle), Arista Networks (especially Jonathan Smith), MyRepublic, Lumen and the entire Black Hat/Informa Tech staff (especially Grifter ‘Neil Wyler’, Bart Stump, Steve Fink, James Pope, Michael Spicer, Jess Jung and Steve Oldenbourg).

About Black Hat

Black Hat is the cybersecurity industry’s most established and in-depth security event series. Founded in 1997, these annual, multi-day events provide attendees with the latest in cybersecurity research, development, and trends. Driven by the needs of the community, Black Hat events showcase content directly from the community through Briefings presentations, Training courses, Summits, and more. As the event series where all career levels and academic disciplines convene to collaborate, network, and discuss the cybersecurity topics that matter most to them, attendees can find Black Hat events in the United States, Canada, Europe, Middle East and Africa, and Asia. For more information, please visit www.BlackHat.com.

13.2. RSAC™ 2026 Conference

- Moscone Center Network Operations Center: Jeff Hardy
- nthDegree: Sean Shanks and John Kodis

Cisco staff and report contributors:

- Innovation—Integrations: Ryan Maclennan, Ivan Berlinson
- Breach Protection Suite: Aditya Sankar and Ben Greenbaum, Ahmadreza Edalat
- User Protection Suite: Christian Clasen and Justin Murphy
- Cisco Secure Firewall, Cloud Protection Suite: Adam Kilgore, Brian Shea and Patrick Whyte
- Splunk Cloud Platform, Enterprise Security: Tony Iacobelli and Richard Marsh

Endace Staff and Report Contributors: Steve Fink, Cary Wright, Barry “Baz” Shaw, Stephen Donnelly, Caleb Millar, Marshall Patty, Tom Leahy and Michael Morris

Coalfire Threat Hunters: Neil ‘Grifter’ Wyler, Bart Stump and Mike Spicer

And, special thanks to our partners at RSAC™ 2025 Conference: Amy Hitchcock, Amy Keltner, Petros Efstathopoulos, Ben Waring, Ryan Jamieson and Dianah Brown.

About RSAC

As the cybersecurity industry's convening authority, RSAC brings together diverse minds to exchange perspectives, knowledge, and ideas. RSAC provides the world's leading platform for uniting and advancing the cybersecurity community to create a safer society. RSAC is at the cutting edge of cybersecurity innovation and education. The company's flagship event, RSAC™ Conference, is the largest and most influential global gathering in cybersecurity. RSAC gives cybersecurity professionals a platform to connect and grow. To learn more, visit www.OneRSAC.com.

About RSAC™ Conference

RSAC™ Conference is the largest and most influential Conference in the cybersecurity industry. Today, under the expanded RSAC brand, the Conference is central to a larger mission that unites the cybersecurity community to create a safer society. To learn more, visit www.rsaconference.com/usa.

13.3. Cisco Live Americas 2025

Network Operations Center Liaisons: Freddy Bello, Andy Phillips, Scott Neuman

Cisco Security and Splunk SOC Team:

- Innovation/Cloud Protection Suite: Ryan Maclennan
- Integrations: Ivan Berlinson
- Splunk: Tony Iacobelli and Austin Pham
- Breach Protection Suite: Aditya Sankar, Ahmadreza Edalat, Mindy Schlueter, Dave Bush, Darryl Hicks, and Kevin Mast
- User Protection Suite: Christian Clasen and Justin Murphy
- Firewall and Security Cloud Control: Adam Kilgore and Patrick Whyte
- Remote Support: Aditya Raghavan, Ben Greenbaum, and Shaun Coulter

Endace SOC Team: Michael Morris, Steve Fink, Barry 'Baz' Shaw, Anantha Srinivasan, Tom Leahy, Philip Kennedy

13.4. Black Hat USA 2025

- Security Cloud Innovation: Ryan Maclennan
- Integrations: Ivan Berlinson
- Breach Protection: Steve Nowell, Aditya Sankar, Matt Vander Horst and Bilal Qamar
- User Protection: David Keller and Adam Kilgore, with Justin Murphy
- Meraki Systems Manager: Paul Fidler
- ThousandEyes: Mauro Caballero and Daniel Gaona Campos
- Splunk: Tony Iacobelli

13.5. GovWare 2025

Marina Bay Sands Network Operations Center Liaison: John Lee Kuo Yang

GovWare/Image Engine Liaison: Goh Choon Hua, Ivan Lim and Zoe Chin

Cisco Singapore: Sharon Koo, Peter Lye, Juan Huat Koo, David Ong and Ian Lim

Cisco Security and Splunk SOC Team:

- Innovation, AI Defense, Cloud Protection Suite: Ryan MacLennan
- Splunk Incident Response: Allison Gallo and Sumit Juyal
- Splunk Enterprise Security Integrations: Kenneth Bouchard
- Talos IR Threat Hunter: Yuri Kramarz
- XDR Integrations: Ivan Berlinson
- Breach Protection Suite, Agentic AI: Aditya Sankar, Ahmadreza Edalat and Robin Wei

- User Protection Suite: Claire Fulk
- Firewall and Security Cloud Control: Adam Kilgore and Carol Trincia Dsouza
- Splunk Remote Support: Josh Wilson

Endace SOC Team: Steve Fink, Cary Wright, Barry ‘Baz’ Shaw and Sundarram Paravata

About GovWare

GovWare Conference and Exhibition is the region’s premier cyber information and connectivity platform, offering multi-channel touchpoints to drive community intel sharing, training, and strategic collaborations.

A trusted nexus for over three decades, GovWare unites policymakers, tech innovators, and end-users across Asia and beyond, driving pertinent dialogues on the latest trends and critical information flow. It empowers growth and innovation through collective insights and partnerships.

Its success lies in the trust and support from the cybersecurity and broader cyber community that it has had the privilege to serve over the years, as well as organizational partners who share the same values and mission to enrich the cyber ecosystem.

13.6. Cisco Live APJC 2025

Network Operations Center Liaisons: Freddy Bello, Andy Phillips, Chris Augulewicz and Scott Neuman

Cisco Security and Splunk SOC Team

- Co-SOC Leader: Shaun Coulter
- Innovation/Cloud Protection Suite: Ryan Maclennan
- Cisco Security Integrations: Ivan Berlinson
- Splunk Integrations: Duane Waddle
- Splunk Incident Responder: Brendan Kuang
- Breach Protection Suite: Robin Wei, Cam Dunn, Hanna Jabbour and Pradnya Padaki
- User Protection Suite: Justin Murphy and Jaki Hasan
- Firewall and Security Cloud Control: Adam Kilgore and Apaar Sanghi
- Remote support: Ben Greenbaum and Josh Wilson

Endace SOC Team: Steve Fink, Cary Wright, Caleb Millar, Daniel Lawson and Peter Watt

13.7. Black Hat Europe 2025

- Security Cloud Innovation: Ryan Maclennan
- Integrations: Ivan Berlinson
- Breach Protection: Rene Straube and Piotr Jarzynka
- User Protection: Rob DeCooman
- ThousandEyes: Roberto D’Amato and Susheela Francis
- Splunk Incident Response Manager: Tony Iacobelli
- MDM Expert: Paul Fidler
- Remote Team: Adi Sankar

14. Glossary of acronyms/terms

AI (Artificial Intelligence): Simulation of human intelligence processes by computer systems, used in this architecture for summarizing incidents, suggesting responses, and reducing analyst toil.

APJC: Asia Pacific, Japan, and China (geographic region).

BYOD (Bring Your Own Device): A policy allowing attendees to use their personal devices on the event network, which limits the SOC's ability to enforce endpoint security controls.

C2 (Command and Control): A technique used by attackers to maintain communication with compromised systems within a target network.

CTI (Cyber Threat Intelligence): Evidence-based knowledge about existing or emerging menaces to assets, used to inform decisions regarding the subject's response.

DDoS (Distributed Denial of Service): A malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic.

DHCP (Dynamic Host Configuration Protocol): A network management protocol used on IP networks for automatically assigning IP addresses and other communication parameters.

DNS (Domain Name System): The phonebook of the Internet, translating domain names to IP addresses. In this architecture, it is a critical control and visibility point via Cisco Secure Access.

EDR (Endpoint Detection and Response): A technology that monitors and gathers data from endpoints (computers, phones) to detect and analyze suspicious behavior. (Note: Often limited in event environments due to BYOD by the attendees).

EMEA: Europe, Middle East, and Africa (geographic region).

ES (Enterprise Security): Refers to Splunk Enterprise Security, a SIEM solution used for advanced threat detection, investigation, and response.

FTD (Firepower Threat Defense): The software image that runs on Cisco Secure Firewall appliances, providing next-generation firewall capabilities.

IDS/IPS (Intrusion Detection System/Intrusion Prevention System): Network security technologies that monitor network traffic for suspicious activity and known threats, either alerting (IDS) or blocking (IPS) them.

IOC (Indicator of Compromise): A piece of digital forensics data, such as a file hash or IP address, that indicates a system has been compromised.

ISP (Internet Service Provider): The company providing internet access to the event venue.

LLM (Large Language Model): A type of AI algorithm that uses deep learning techniques to understand, summarize, and generate new content.

MDM (Mobile Device Management): Software used to monitor, manage, and secure mobile devices.

MFA (Multi-Factor Authentication): A security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity.

MITRE ATT&CK: A globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

NOC (Network Operations Center): The location or team responsible for monitoring and managing the network infrastructure. The SOC works closely with the NOC.

OCSF (Open Cybersecurity Schema Framework): An open-source project delivering an extensible framework for developing schemas to standardize security data.

OODA (Observe, Orient, Decide, Act): A decision-making loop used as a strategic framework for the SOC's continuous improvement process.

OSINT (Open Source Intelligence): Intelligence collected from publicly available sources.

PCAP (Packet Capture): The process of intercepting and recording data packets crossing a specific point in a data network. Used for deep forensic investigation.

PDU (Power Distribution Unit): A device fitted with multiple outputs designed to distribute electric power, especially to racks of computers and networking equipment.

PICERL: The incident response lifecycle framework defined by SANS: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.

SIEM (Security Information and Event Management): A solution that provides real-time analysis of security alerts generated by applications and network hardware (e.g., Splunk ES).

SNA (Secure Network Analytics): Cisco's network traffic analysis solution (formerly Stealthwatch) that detects threats in encrypted traffic and anomalous behavior.

SNI (Server Name Indication): An extension to the TLS protocol that indicates which hostname is being contacted by the browser at the beginning of the 'handshake' process.

SOAR (Security Orchestration, Automation, and Response): Technologies that enable organizations to collect inputs monitored by the security operations team and define standardized analysis and response procedures.

SOC (Security Operations Center): A centralized facility where information security issues are monitored, assessed, and defended.

SPAN (Switched Port Analyzer): A method of mirroring network traffic on a switch to a destination port for analysis (e.g., sending traffic to Endace).

SSID (Service Set Identifier): The primary name associated with an 802.11 wireless local area network (WLAN).

SSO (Single Sign-On): An authentication scheme that allows a user to log in with a single ID and password to any of several related, yet independent, software systems.

TDIR (Threat Detection, Investigation, and Response): A framework or category of tools focused on the lifecycle of a threat.

TIP (Threat Intelligence Platform): A system used to aggregate, correlate, and analyze threat data from multiple sources.

TLS (Transport Layer Security): A cryptographic protocol designed to provide communications security over a computer network.

UEBA (User and Entity Behavior Analytics): A cybersecurity process that uses algorithms to detect anomalies in the behavior of users and entities (routers, servers, endpoints) connected to a network.

VLAN (Virtual Local Area Network): A subnetwork which can group together collections of devices on separate physical local area networks (LANs).

XDR (Extended Detection and Response): A security tool that consolidates data from multiple security products (endpoints, network, cloud) to detect and respond to threats.

Contributors

Adi Sankar, Sr. Technical Leader

Ivan Berlinson, SOC Domain Specialist

Bilal Qamar, Technical Marketing Engineer

Ryan Maclennan, SOC Integrations Engineer

Tony Iacobelli, Sr. Manager, Splunk Advanced Response

Kenneth Bouchard, Splunk Engineering Product Manager

Paul Pelletier, Director, Splunk Security Products Labs

Jessica Oppenheimer, Director, SOC Integrations