Security Operations Center

Findings Report from RSAC™ 2026 Conference

10th Year of the SOC

Published by Cisco and Splunk Security, a Cisco Company

Edited by Jessica Oppenheimer, Tony Iacobelli, Cary Wright and Steve Fink

Table of Contents

1. Introduction and scope

2026 marks the 10th year of the Security Operations Center (SOC) at RSAC™ 2026 Conference. Our appreciation to the team at RSA Conference LLC (“RSAC”), Nth Degree, the Moscone Center Network Operations Center and the dozens of engineers, analysts and incident responders who made the SOC a success since 2017.

The core missions of the SOC are:

- **Protect**

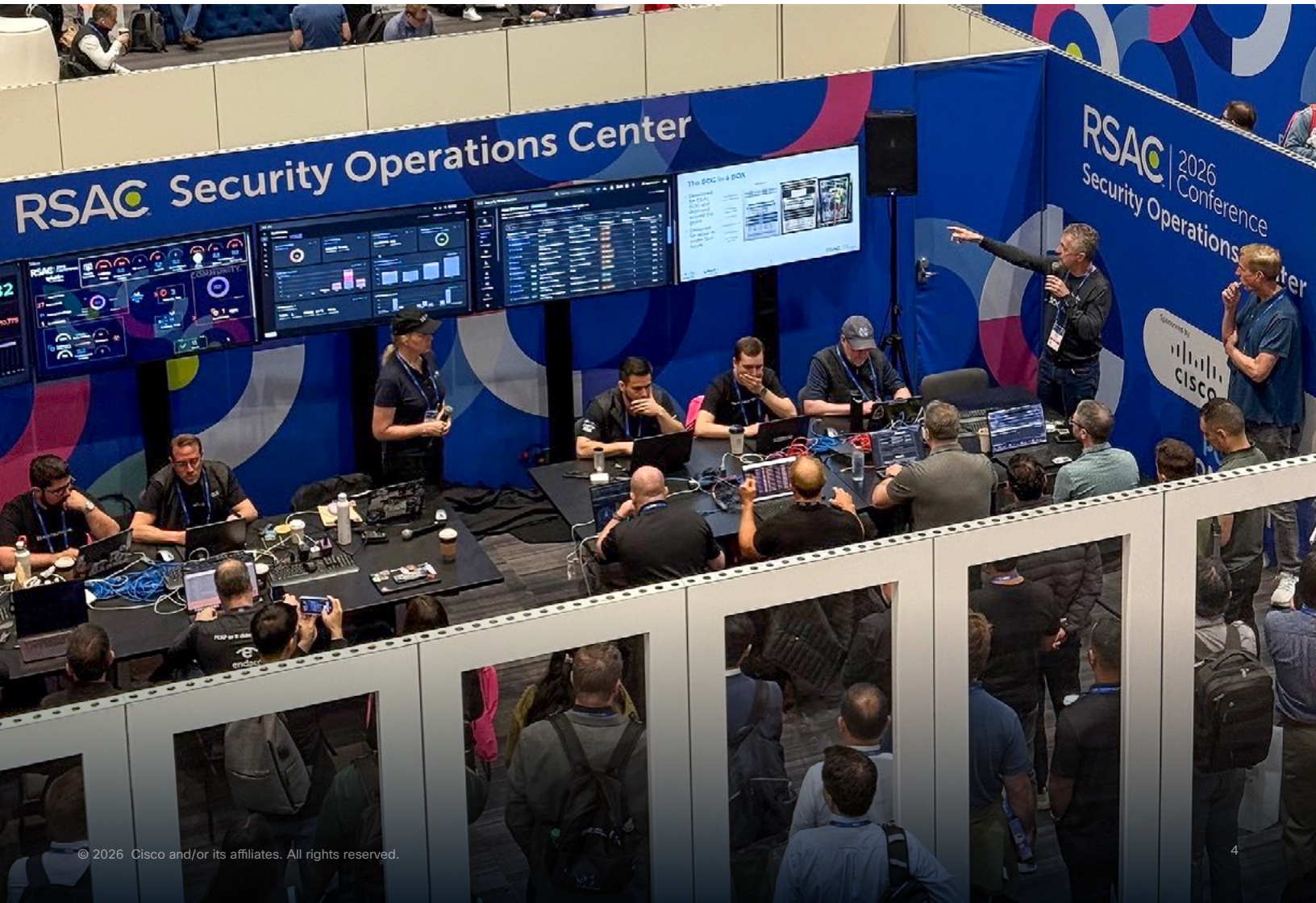
  Safeguard the network from threats and attacks, both internal and external

- **Educate**

  Inform and engage attendees through SOC tours, the SOC Report Session, this Findings Report, and our lessons learned

- **Innovate**

  Develop and implement new integrations, processes, workflows, and automations



1.1 Disclaimer and legal

The role of the Security Operations Center ("SOC") at RSAC™ 2026 Conference ("RSAC 2026") is to provide SOC services.

Cisco Systems Inc. ("Cisco"), Splunk, a Cisco Company ("Splunk") and Endace Limited ("Endace") used data from the Moscone Center Wireless Network (the "Network") to provide SOC services.

By connecting to the Network during RSAC 2026, all RSAC 2026 attendees (including e.g., sponsors, exhibitors, guests, employees) accepted the following terms and conditions: "THE WIRELESS NETWORK AVAILABLE AT THE MOSCONE CENTER IS AN OPEN, UNSECURED 5 GHZ NETWORK. CISCO AND SPLUNK, A CISCO COMPANY, WILL BE USING DATA FROM THE MOSCONE WIRELESS NETWORK TO PROVIDE SOC SERVICES. WE STRONGLY RECOMMEND THAT YOU USE APPROPRIATE SECURITY MEASURES, SUCH AS UTILIZING A VPN CONNECTION, INSTALLING A PERSONAL FIREWALL AND KEEPING YOUR OPERATING SYSTEM UP-TO-DATE WITH SECURITY PATCHES. WE RECOMMEND TURNING OFF YOUR WIRELESS ADAPTER WHEN NOT IN USE AND ENSURING AD-HOC (PEER-TO-PEER) CAPABILITIES ARE DISABLED ON YOUR DEVICE.)."

Additionally, RSAC advised attendees of the SOC services in printed materials and onsite signage.

The infrastructure at the event is managed by the Moscone Center, which deploys Cisco Secure Access DNS, this provides the SOC with visibility into the DNS Logs. The SOC also receives a SPAN feed of the network traffic from the Wi-Fi Network (named .RSACONFERENCE). The SOC correlates the data between these two sources to enable the security tools and the security analysts.

The goal of SOC is to protect RSAC 2026 attendees on the Network and educate RSAC 2026 attendees about what happens on a typical open, unsecured wireless network. The education comes in the form of SOC tours, a presentation by the SOC leaders at an RSAC 2026 session and the publication of the findings in this report ("Findings Report"), issued by sponsors Cisco and Splunk.

"The Network" is a typical network that users connect to for Internet access, similar to networks in hotels, airports or coffee shops. The Network used during RSAC 2026 is an open network offered by the Moscone Center.

This Findings Report and any security issues identified herein solely relate to user activity, not Cisco's products, processes, or offerings, or the Network itself.

Data collected by the SOC Team at RSAC 2026 remained the property of RSAC and has been destroyed. A certificate of destruction is held by RSAC.

The red or white blocks in the diagrams, screenshots, or figures in this Findings Report represent redacted data and information. This is done to protect privacy and/or confidential information.

This Findings Report was prepared as a summary of the SOC services at RSAC 2026, is not to be used as a basis for commercial assessment and is provided "as is". Cisco, Splunk, Endace, RSAC nor any of their employees or subcontractors, makes any warranty of any kind, including but not limited to, implied warranties of accuracy, merchantability, fitness for a particular purpose, and non-infringement of any third party intellectual property rights, or assumes any legal liability or responsibility for the accuracy,

completeness, or any third party's use or the results of such use of any information, product, or process referenced or discussed herein. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement or recommendation. Cisco, Splunk, Endace, and RSAC will not be liable for any misstatements or omissions, including in relation to instructions for the use, operation, or maintenance of any equipment, system components, or software. Whilst care has been taken in compiling this Findings Report, it may contain estimates and draft information and may not be current, accurate, or complete. Only representations made in executed agreements with customers will be binding on the customer and Cisco, Splunk, Endace, or RSAC, as applicable.

This Findings Report is copyrighted material prepared by Cisco and Splunk and may not be reproduced, distributed, or changed without the express written approval of Cisco and Splunk.

1.2 The environment

The Network is a flat network with no host isolation, divided into Moscone South & North Expo Halls and the Moscone West Briefings & Keynotes. The absence of host isolation is an important starting point for understanding wireless networks and the risks associated with connecting to them. A flat network without host isolation means that anyone with an IP address can theoretically communicate with any other devices on the network. Host isolation provides a device with a one-way route out to the Internet, but no routes within the network.

Knowing which type of network you are connecting to can be discovered by identifying your IP address and trying to ping another IP address on that network. If you get a response, you are on a network without host isolation; if you get a "request timed out" response, you are probably isolated.

The Moscone Conference complex has a Network Operations Center (NOC), a centralized location where network administrators and operations staff monitor, manage, and maintain the health and performance of the Wi-Fi network. The NOC provided a SPAN of the Network traffic, along with logs of the perimeter firewalls and DHCP server.

2. SOC architecture and deployment

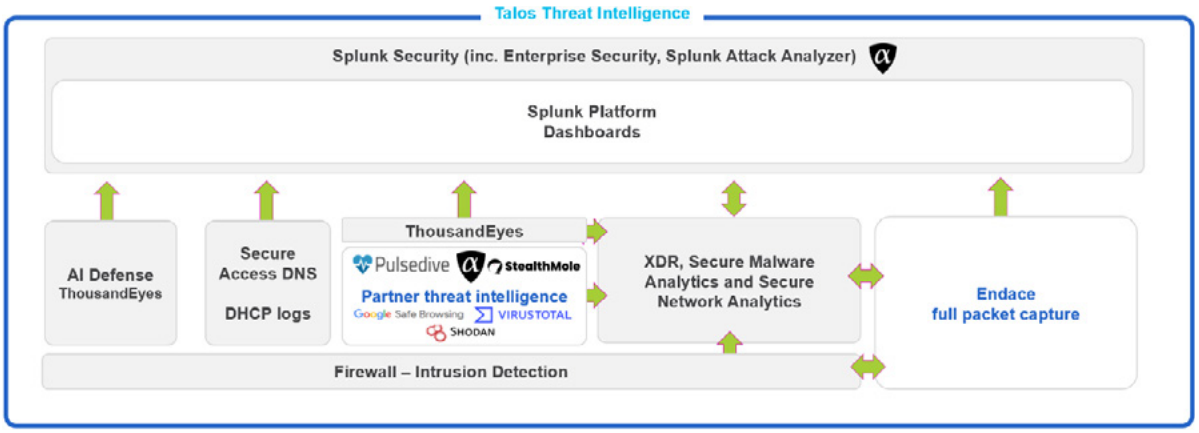
2.1 SOC in a Box

With a limited window of just two and a half days to establish the SOC at RSAC 2026, the team's success relied heavily on streamlined preparation and advanced planning, built around the "SOC in a Box".

The SOC in a Box was built for rapid deployment at major events. The Box can be replicated for natural disaster situations, or even small/medium businesses who need to upgrade their SOC in a hurry.

Components include:

- 3 x EndaceProbes, with total 244TB packet storage, and resources for network monitoring VMs
- Switch: Catalyst 9500 with 10G SFP+ (48 port) & 40G QSFP+(4 port) for SPAN and WAN
- Switch: Meraki 125 (48 port) switch for SOC management
- Firewall: x2 Secure Firewall 3130
- Server: x2 UCS C220 M5
- Server: UCS C245 M8, with three Nvidia GPUs

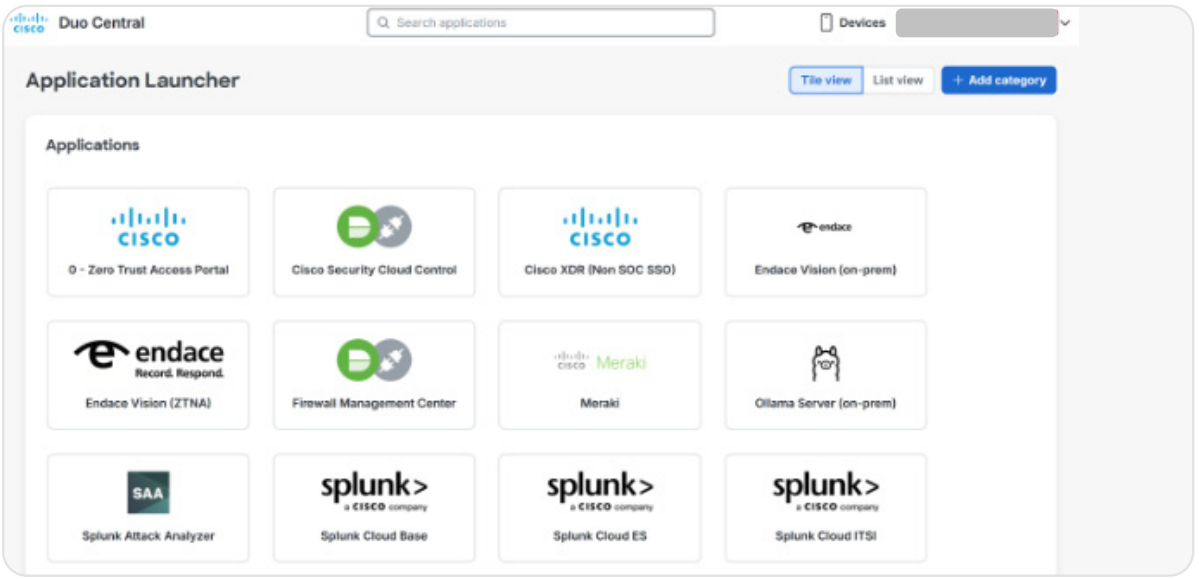


2.2 Technology overview

The SOC Team connected the EndaceProbe packet capture platform to the SPAN of the Network, and Splunk Enterprise Security tooling, with the foundation of Secure Firewall. AI models were protected by Cisco AI Defense, Cisco Security Cloud and Splunk Enterprise Security tooling, with the foundation of Cisco Secure Firewall.

Duo Directory and Cisco Identity Intelligence provided the identity plane, securing role-based access to our tools via Single Sign-On and ensuring our analysts were authenticated and authorized within minutes of joining the SOC for the first time.

Incidents were investigated with threat intelligence, provided by Cisco Talos, and licenses donated by alphaMountain, Pulsedive, and StealthMole, along with community sources.



2.3 Core components

Packet capture

The SOC team used an EndaceProbe to continuously capture a comprehensive record of all traffic traversing the Network gateway via a 10G SPAN, including all north-south and a substantial portion of east-west traffic.

EndaceProbe recorded every packet entering or leaving the Network for the entire duration of RSAC 2026, including all DNS traffic directed to Cisco Secure Access. This historical Network data enabled the SOC team to conduct in-depth investigations of any events flagged by other SOC tools, providing detailed forensic evidence.

The EndaceProbe inspects and indexes all packets and flows, allowing for rapid searches of Network traffic via the Endace GUI or API. Searches were conducted across multiple layers, from L3 to L7, facilitating efficient and granular analysis.

Endace also generated Zeek Metadata into Cisco Secure Network Analytics (SNA) and the Splunk Platform, with customized detections of plain text credentials. File content was reconstructed on the fly by Endace using Zeek, filtered, de-duplicated and streamed to Splunk Attack Analyzer (SAA) and Cisco Secure Malware Analytics for sandboxing and analysis. File filtering and deduplication were introduced this year, to reduce the volume of files submitted to SAA for analysis. Deduplication submitted only unique files for full analysis. Any subsequent sightings of the same file hash were logged to Splunk but not submitted for analysis. This allowed us to keep track of the 'blast radius' of malware to understand who is potentially infected without overloading SAA.

The Cisco XDR – Endace integration included the Endace Vault API, new for RSAC 2026, where incidents of specific severity trigger automation that preserves PCAP and other important evidence in a file vault and places links to that evidence in the XDR worklog for easy access by incident responders.

Security incident and event management platform

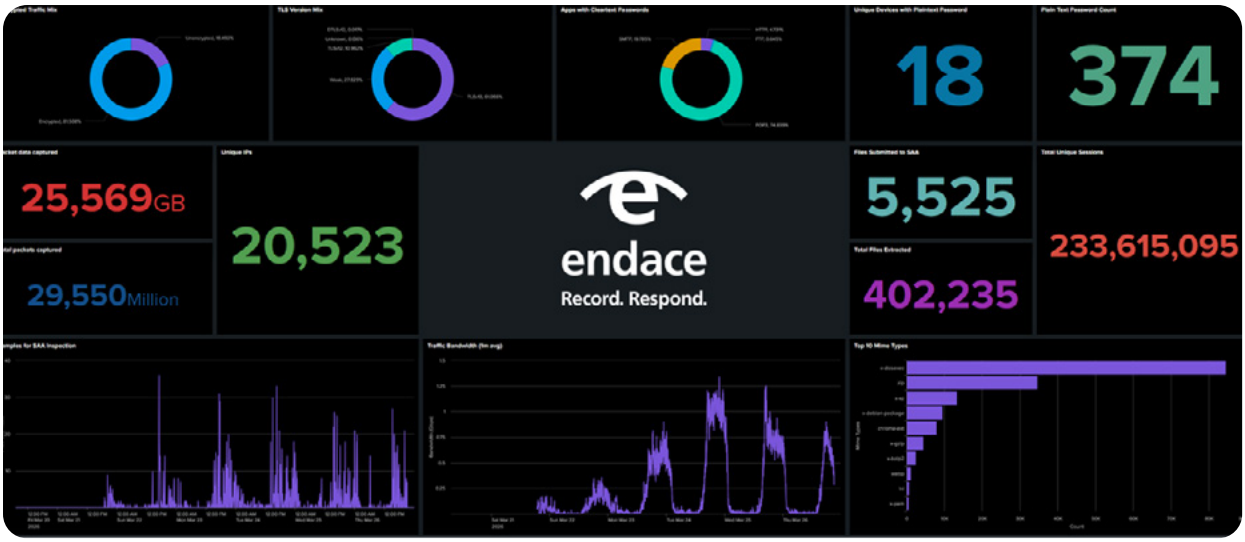
To make our threat hunters' lives richer with more context from Cisco and Endace tools, we connected our Splunk Cloud-based Enterprise Security deployment to the SOC in a Box. This integration allows us to ingest logs and detections from EndaceProbe, Cisco XDR, Secure Malware Analytics, Secure Network Analytics, Secure Access, and Secure Firewall, and visualize them into functional dashboards for executive reporting.

We deployed the Endace Splunk App integration which provides a powerful search integration, which we used extensively to validate our findings with the Firewall.

Leveraging Splunk's summary indexing, we were able to instantly aggregate critical data, showcasing the top categories of network destinations, domains, DNS queries, and attack techniques employed among 50+ other telemetry points normalized by the Endace Splunk integration.

By aggregating Endace metadata into a Splunk dashboard, the SOC team gained actionable insights into encryption strength and insecure sessions.

This centralized view offered visibility into the Network activity, the flow of logs and files into the security stack, and a real-time summary of user security levels.



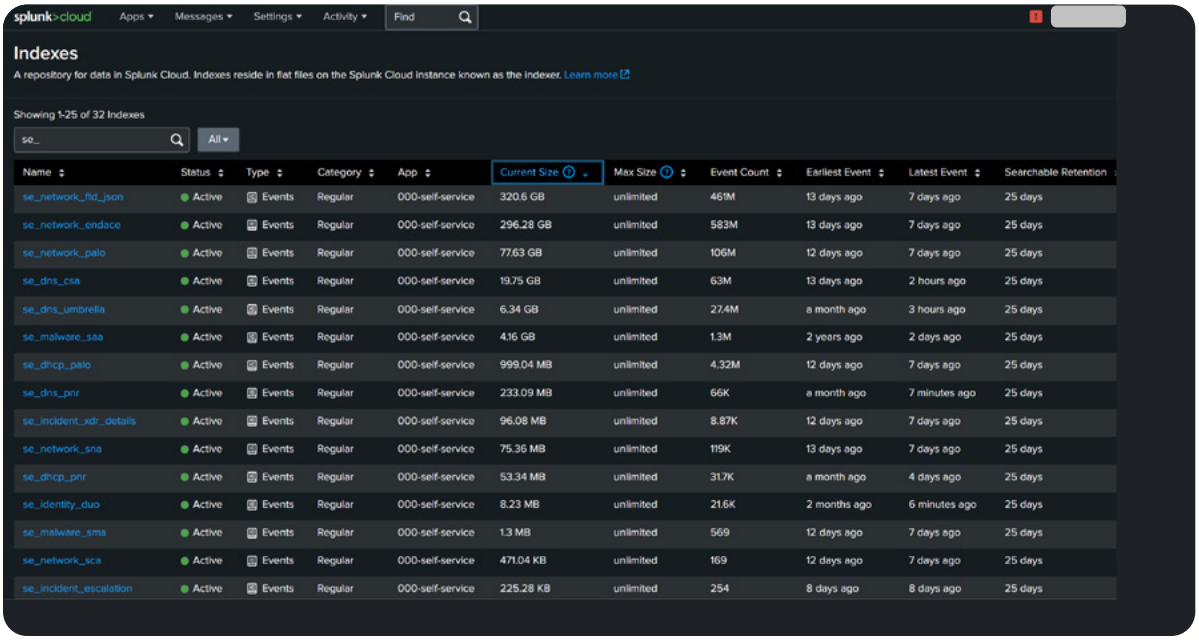
Cisco Security and NOC Telemetry

Splunk Cloud aggregates telemetry and event data from a diverse array of security and network infrastructure sources, including network traffic, DNS and DHCP activity, identity management, malware detection, and incident response workflows.

The specific sources of data, categorized by their security domain, include:

- **Network security and traffic**
  Telemetry and network events sourced from
  - Firepower Threat Defense (se_network_ftd_json)
  - Endace (se_network_endace)
  - Palo Alto Networks (se_network_palo)
  - Secure Network Analytics (se_network_sna)
  - XDR Analytics (se_network_sca)
- **DNS & DHCP services**
  Domain Name System and Dynamic Host Configuration Protocol logs collected from
  - Secure Access (se_dns_csa)
  - Palo Alto Networks (se_dhcp_palo)
- **Identity and access management**
  Authentication and identity verification logs sourced from Cisco Duo (se_identity_duo)
- **Malware analysis**
  Threat detection and malware analysis data from
  - Splunk Attack Analyzer (se_malware_saa)
  - Secure Malware Analytics (se_malware_sma)
- **Incident management**
  Security operations data tracking
  - Extended Detection and Response (XDR) details (se_incident_xdr_details)
  - Incident escalations (se_incident_escalation)

The ingested data for each integrated platform was deposited into their respective indexes. Cloud-based services were ingested directly into our stack, while data sources that were running on hardware in our SOC in a Box leveraged both heavy and universal forwarders efficient and secure transport of the data.



Name	Status	Type	Category	App	Current Size	Max Size	Event Count	Earliest Event	Latest Event	Searchable Retention
se_network_ftd_json	Active	Events	Regular	000-self-service	320.6 GB	unlimited	461M	13 days ago	7 days ago	25 days
se_network_endace	Active	Events	Regular	000-self-service	296.28 GB	unlimited	583M	13 days ago	7 days ago	25 days
se_network_palo	Active	Events	Regular	000-self-service	77.63 GB	unlimited	106M	12 days ago	7 days ago	25 days
se_dns_csa	Active	Events	Regular	000-self-service	19.75 GB	unlimited	63M	13 days ago	2 hours ago	25 days
se_dns_umbrella	Active	Events	Regular	000-self-service	6.34 GB	unlimited	27.4M	a month ago	3 hours ago	25 days
se_malware_saa	Active	Events	Regular	000-self-service	4.16 GB	unlimited	1.3M	2 years ago	2 days ago	25 days
se_dhcp_palo	Active	Events	Regular	000-self-service	999.04 MB	unlimited	4.32M	12 days ago	7 days ago	25 days
se_dns_pnr	Active	Events	Regular	000-self-service	233.09 MB	unlimited	66K	a month ago	7 minutes ago	25 days
se_incident_xdr_details	Active	Events	Regular	000-self-service	96.08 MB	unlimited	8.87K	12 days ago	7 days ago	25 days
se_network_sna	Active	Events	Regular	000-self-service	75.36 MB	unlimited	119K	13 days ago	7 days ago	25 days
se_dhcp_pnr	Active	Events	Regular	000-self-service	53.34 MB	unlimited	31.7K	a month ago	4 days ago	25 days
se_identity_duo	Active	Events	Regular	000-self-service	8.23 MB	unlimited	21.6K	2 months ago	6 minutes ago	25 days
se_malware_sma	Active	Events	Regular	000-self-service	1.3 MB	unlimited	569	12 days ago	7 days ago	25 days
se_network_sca	Active	Events	Regular	000-self-service	471.04 KB	unlimited	169	12 days ago	7 days ago	25 days
se_incident_escalation	Active	Events	Regular	000-self-service	225.28 KB	unlimited	254	8 days ago	8 days ago	25 days

Network security—firewall threat detection

In any SOC, Next Gen Firewalls with intrusion detection systems (IDS) serve as a vital source of data, and the same is true of our SOC at RSAC 2026. We deployed two Secure Firewall 3130 appliances in a High Availability configuration for resiliency. Both Firewalls run Cisco Secure Firewall Threat Defense (FTD) software on version 10. We leveraged the IDS for multiple integrations:

- Events to Cisco XDR for incident correlation
- Traditional and Advanced Logs to Splunk
- Files submitted to Secure Malware Analytics for sandbox analysis
- Integration with Endace for event cross-launch and full session access

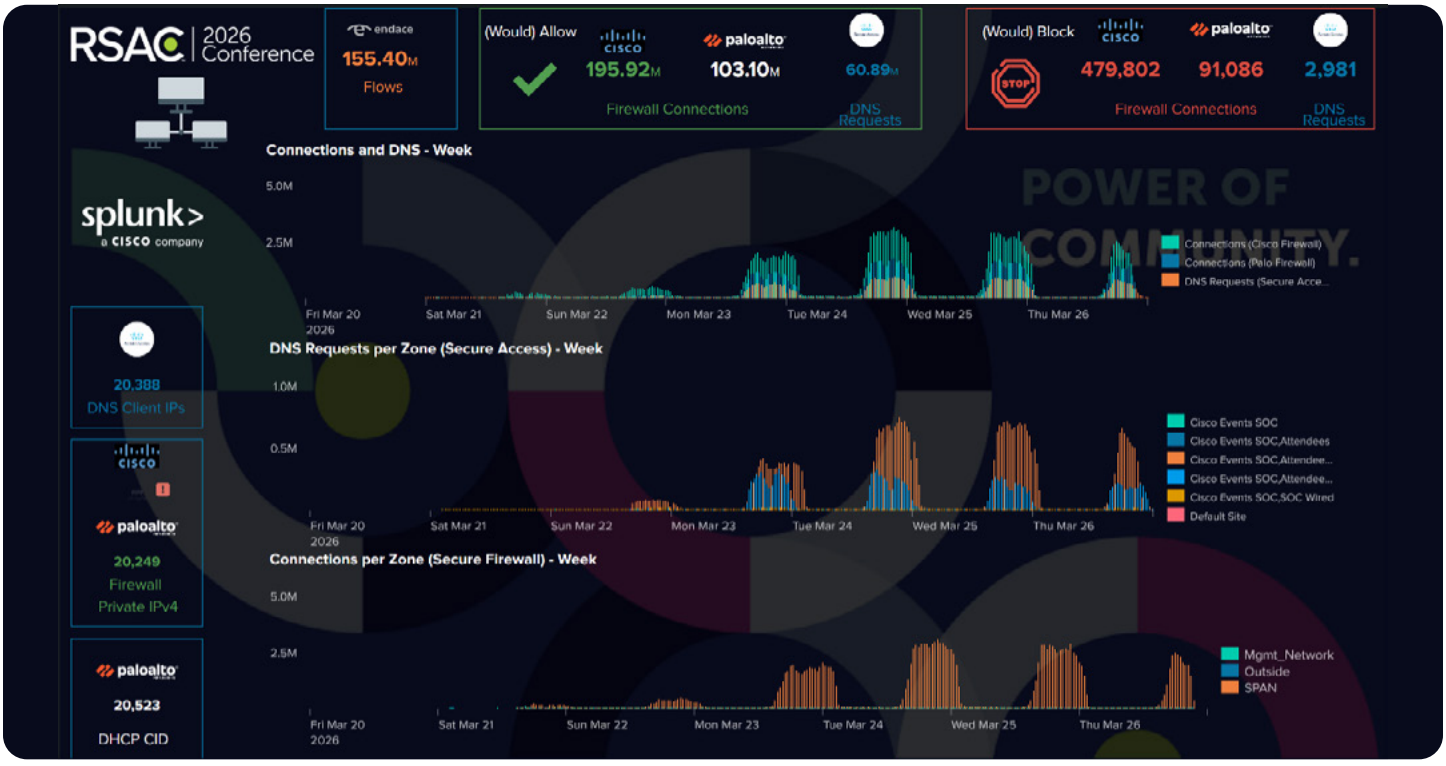
The IDS inspected all wireless guest traffic from event attendees. Cisco Secure Firewall offers breach detection, threat discovery, malware detection, sandbox integration, and security automation.

Rich contextual information (such as applications, operating systems, vulnerabilities, intrusions, and transferred files) empowered the SOC to help uncover threats lurking in the environment.

While Cisco Secure Firewall offers a wide variety of native threat visibility, we closely integrate Cisco XDR and Splunk to push our investigations to the next level. At RSAC 2026, we deployed new firewall to Splunk integrations and log types that gave us much more log granularity with our Splunk log retention.

And as the volume of encrypted traffic continues to increase, the Encrypted Visibility Engine (EVE) continues to be a key component into giving us more threat visibility for encrypted traffic.

Lastly, our new Shadow Traffic dashboard offers improved visibility into traffic that tries to evade detection and analysis. These evasions include VPNs, encrypted DNS, and multi-hop proxies. This new dashboard was our marquee feature for Secure Firewall on the monitor in the SOC.



DNS Security

With the deployment of Cisco Secure Access DNS the SOC had complete Domain Name Service (DNS) visibility, thanks to the support of the Moscone Center for installing Secure Access Virtual Appliances (VAs) in the NOC.

The default security settings for Cisco Secure Access are to block malware, command-and-control callback, and phishing attacks. Most security and content category blocking were turned off for the Network, to allow security training, demos and briefings to operate unimpeded. However, when domains were proven to be a direct threat against RSAC 2026 and/or attendees, we documented the threats in SOC Incident Response Reports for consideration by RSAC for blocking.

Domains also could have been blocked for content, such as pornography, hate/discrimination, or other such categories. It is impossible to turn off blocking for certain criminal queries. Such attempted access is reported to the RSAC 2026 security team and law enforcement, as appropriate, in coordination with the Moscone NOC.

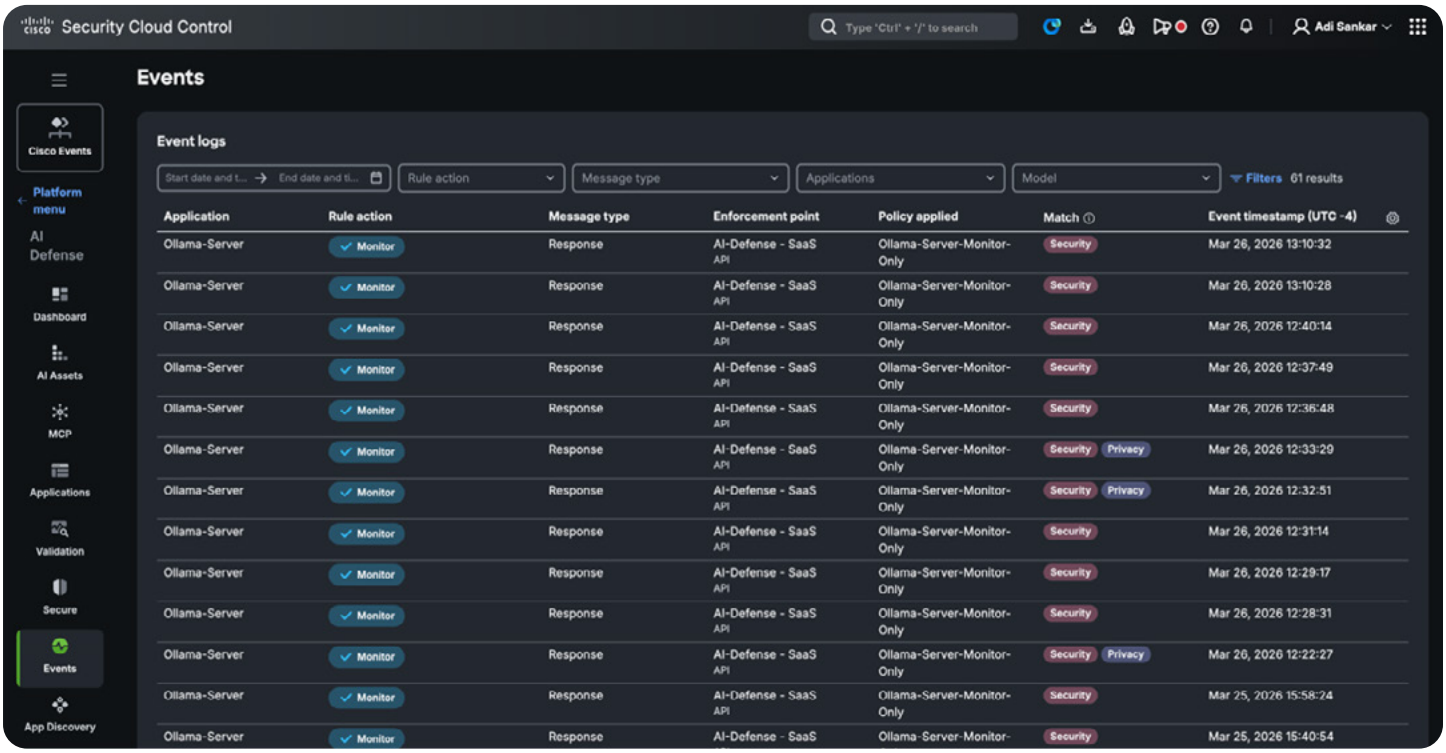
2.4 Protecting the SOC infrastructure

AI Defense

Cisco AI Defense analyzed prompt/response exchanges in real time to identify techniques such as prompt injection, sensitive data exfiltration, and adversarial model abuse, generating structured detections with risk context. Integrating AI Defense with Cisco Secure Access allows us to monitor and analyze the growing use of generative AI applications across the conference network. Based on the DNS activity seen in Secure Access, AI Defense allows us to see what the most popular applications classified as generative AI are and the risk associated with those applications. In addition to Network visibility, we also use AI Defense to protect models running on-premise in our SOC in a Box.

In our SOC in a Box, we have three Nvidia L40 GPUs in the M8 UCS server. This hardware provides GPU acceleration for models running on-premises in Ollama. The frontend of our on-premises Ollama server is built using Open WebUI. The prompts and responses are proxied through the AI Defense inspection API. The policies in AI Defense protect against certain content types, data leakage, code leakage, and prompt injection. For example, XDR automation leveraged Foundation AI by Cisco's Foundation-Sec-8B model, to provide incident summaries and add notes to the incident worklog.

This approach enabled the SOC to not only detect AI-specific attacks, but also to operationalize the team within existing workflows by augmenting analyst visibility and accelerating triage. The SOC demonstrated how agentic AI can be both a target and a defensive capability within modern security operations.



ThousandEyes

We deployed ThousandEyes for Network availability observation from the perspective of the SOC and our connection to our management tools. The dashboard below in ThousandEyes gave us status on the Network health.

This view provides visibility into key performance metrics, including response time, DNS resolution time, HTTP response time, and HTTP availability for our assets. These insights enable us to rapidly identify potential performance bottlenecks and proactively investigate the root causes of latency or outages in collaboration with the (NOC).

ThousandEyes provided visibility into WAN and Internet path performance, allowing us to identify upstream provider issues and external dependencies impacting connectivity. We also configured a synthetic test to download a 50MB file from testfile[.]org, giving us a consistent benchmark for throughput and end-to-end user experience validation across the network.

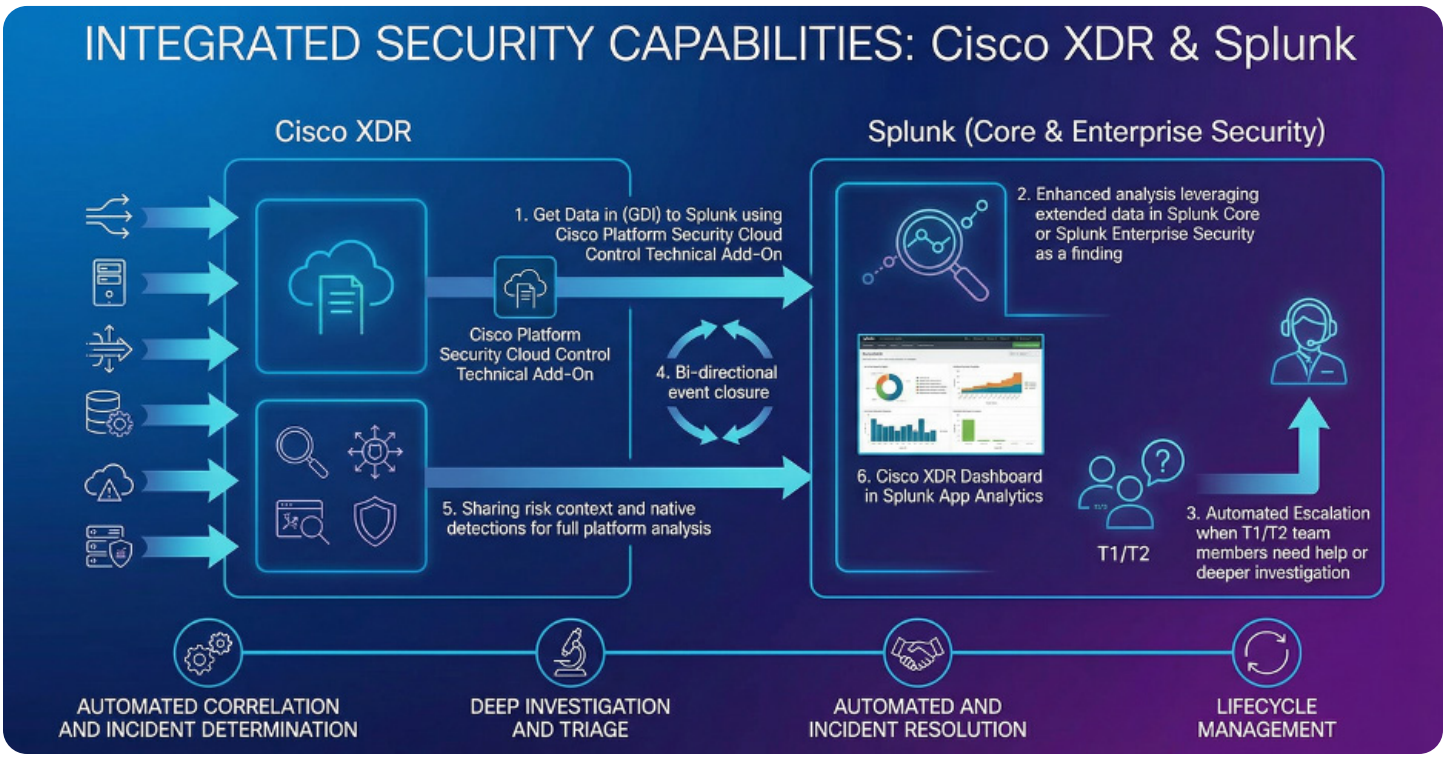
3. Integrated operations

Our main goal in the SOC is to avoid data silos. We require every tool to integrate directly with our platform and communicate with our other systems, ensuring that all our data, process, and tools work together effectively.

3.1 Integrations strategy

The SOC implemented a “System of Systems” approach to security operations. The primary objective was to eliminate the operational friction that typically exists between frontline analysts performing triage in Cisco XDR, and incident responders performing deep hunting in Splunk Enterprise Security. Prior to this integration, the SOC faced a disconnected workflow where investigations were often “thrown over the wall,” resulting in a loss of context, the need for manual data re-entry, and a missed opportunity for upskilling junior analysts. To resolve this, the team implemented three specific technical innovations to create a seamless, closed-loop workflow.

The first innovation focused on an **automated escalation architecture** that streamlines the movement of confirmed threats from the frontline analysts to the incident responders. When a frontline analyst determines that an incident requires deeper forensic analysis, they simply change the XDR Incident Status to “Open: Reported.” This action triggers an automation rule that sends a structured JSON payload containing the incident summary and observables directly to the Splunk HTTP Event Collector (HEC). Splunk then parses this payload, flattening the observables and grouping them by incident ID to map them to Splunk “Threat Objects.”



The integration uses Splunk SOAR (Security Orchestration, Automation, and Response) to pull the XDR Worklog, including analyst notes and AI-generated summaries, and writes them directly into the Splunk Investigation Notes view. This ensures the incident responder understands exactly why the incident was escalated without ever having to switch consoles.

To ensure the operational loop is fully closed, the team developed a **bi-directional closure** mechanism. This allows incident responders to resolve incidents without leaving their primary tool. Once the deep investigation is complete in Splunk Enterprise Security (ES), the analyst updates the status and disposition within Splunk. An on-demand SOAR playbook then triggers a synchronization back to Cisco XDR, automatically updating the original Incident Status to match the Splunk resolution. The system simultaneously sends a Webex message containing links to the specific ES Investigation, ensuring the entire team is aware of the closure and the outcome of the threat.

The SOC implemented a **cross-pollination of detections** to enhance correlation capabilities across both platforms. This involved a bi-directional sharing of raw detection data. Logs from the Splunk Risk Index are ingested into Cisco XDR as sources, allowing XDR to correlate Splunk-generated risk findings with native telemetry from endpoints and NetFlow. Conversely, native detections from Cisco XDR are ingested into Splunk ES, where they act as “Intermediate Findings” within the Splunk Risk Index, contributing to the overall risk score of assets and users.

This fully integrated architecture delivers immediate, measurable benefits to the SOC. Triage occurred efficiently in XDR while deep investigations remained in Splunk, utilizing the specific strengths of both platforms. By eliminating manual data entry and context switching, the team significantly improved efficiency. Furthermore, the integration facilitated education and upskilling; frontline analysts gained visibility into the notes and findings added by incident responders in Splunk, effectively learning from the advanced investigations. Ultimately, this unified approach allowed new analysts to be trained on the XDR interface in less than one hour while contributing to a workflow that reduced the overall Mean Time to Respond (MTTR).

4. Statistical overview

To provide historical context, the following statistics compare this year's findings with data captured during our most recent conferences, a key highlight of the annual Findings Report.

4.1 Year-over-Year comparison

The table comparing 2023–2026 statistics:

Year	2026 (Endace)	2025 (Endace)	2024 (NetWitness)	2023 (NetWitness)
Attendees (RSAC 2026)	43,500+	43,500+	41,700+	~39,000
Total packets captured (Endace)	29.5 billion	45.3 billion	19 billion	18.5 billion
Total logs captured (Splunk)	1,251 million (PANW and DHCP logs added)	930 million (Zeek logs added)	39.9 million*	214.7 million
Total unique devices (Cisco)	20,581	22,701	17,034	~40k
Total packets written to disk (Endace)	25.6 terabytes	36.6 terabytes	17.24 terabytes	16.26 terabytes
Total logs written to cloud (Splunk)	727 gigabytes	193 gigabytes	79 gigabytes	774 gigabytes
Peak bandwidth utilization (Endace)	2.9 Gbps	3.3 Gbps	2.2 Gbps	1.8 Gbps
DNS Requests (Cisco)	~63.8 million	~65.2 million	~56.3 million	~53.4 million
Total clear text username/passwords (Endace)	374	2,825	20,916	36,910
Unique devices/ accounts with clear text usernames / passwords (Endace)	18	93	99	424
Files sent for malware analysis (Endace)	402,235 file objects reconstructed by Endace. 5,525 sent to SAA‡ 934 sent to SMA	309,514 file objects reconstructed by Endace. 27,000 sent to SAA† 7,500 sent to SMA	~50**	7,500

* During RSAC 2024, the logs from the Cisco Firewall Intrusion Detection System were not integrated into the NetWitness SIEM due to technical issues, therefore the statistics of total logs captured showed a major decline simply by losing this single log source. This highlights the importance of capturing all logs across an entire enterprise ecosystem for full visibility.

** In 2024, submitted files from NetWitness to Cisco Secure Malware Analytics were checked first against known files before submission.

† In 2025, Endace submitted all files to Splunk Attack Analyzer, which then submitted potentially malicious files to Secure Malware Analytics. Endace additionally implemented file deduplication that reduced the overall number of submissions to SAA.

‡ In 2026, Endace implemented file deduplication and mime type filtering that reduced the overall number of submissions to SAA.

Traffic analysis

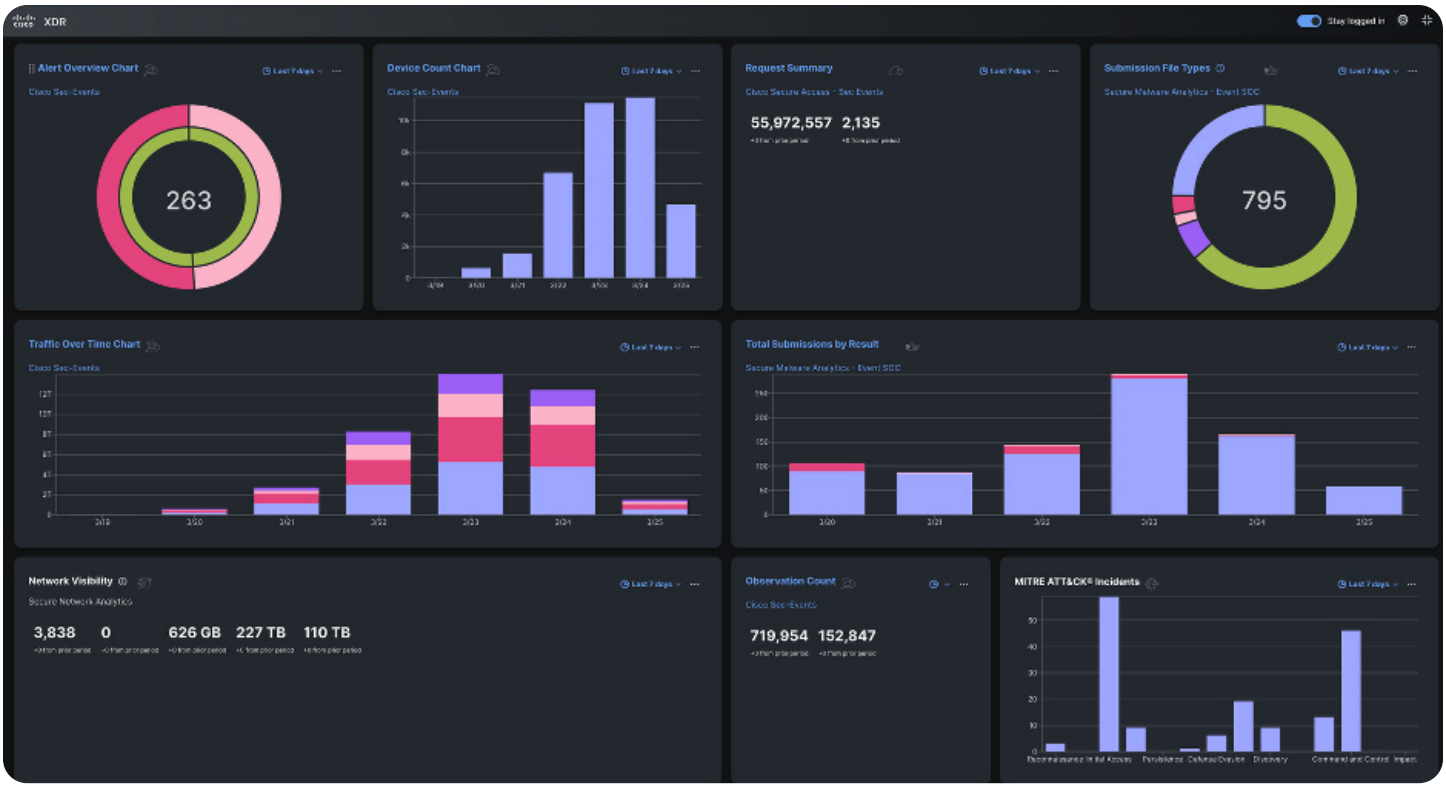
The SOC team analyzed wireless traffic at RSAC 2026 from Sunday, March 22, through Thursday, March 26, 2026, at 3 p.m.

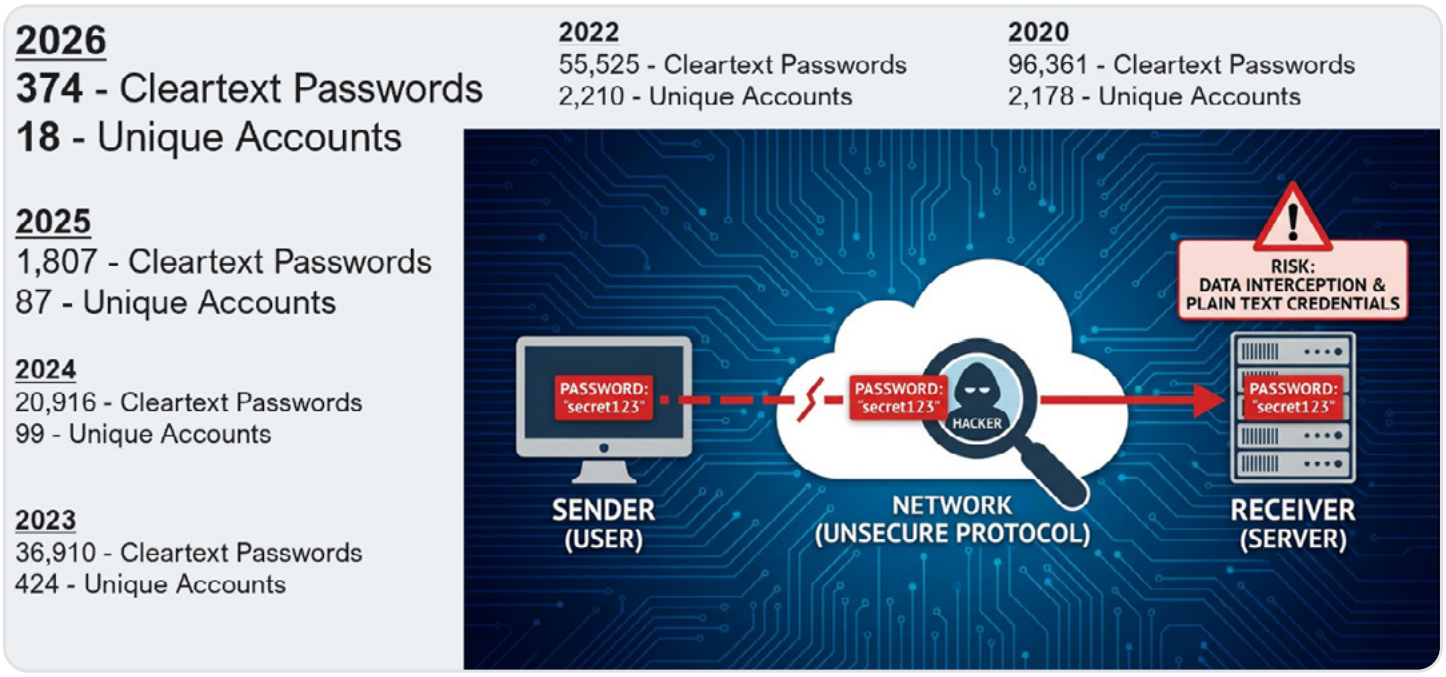
We observed a 30% decrease in traffic compared to last year. This is likely due to changes in how the configured SPAN traffic forwarded traffic in the Moscone network; last year, we may have inadvertently duplicated traffic leveraging multiple SPANs.
Since the total number of devices on the network was only 10% lower than last year, this supports our theory that last year's traffic totals were inflated by duplicate data.

The Control Center dashboard in XDR made it very easy for the SOC managers to view statistics for the last hour, last 24 hours, last seven days, and event last 30 days, with no refresh lag.

Cleartext usernames and passwords

Cleartext usernames and passwords continued to be observed on the Network. The unique number of clear text credentials has declined year-over-year, as we continue to educate users with a goal of not seeing cleartext authentications. Before this automation, each one of these case types would take approximately 30 minutes for an analyst to complete.
By automating this use case, we were able to save over nine hours, which equates to an entire shift plus an additional hour for an analyst.





4.2 Evolution of automated response for cleartext credential transmissions

A recurring vulnerability observed across RSAC 2026 is the transmission of cleartext credentials by attendees using insecure or legacy protocols (e.g., HTTP, unencrypted POP3). As part of the continuous refinement of our SOC architecture, the Team prioritized the rapid identification and remediation of these exposures to protect attendees and reduce manual analyst workload.

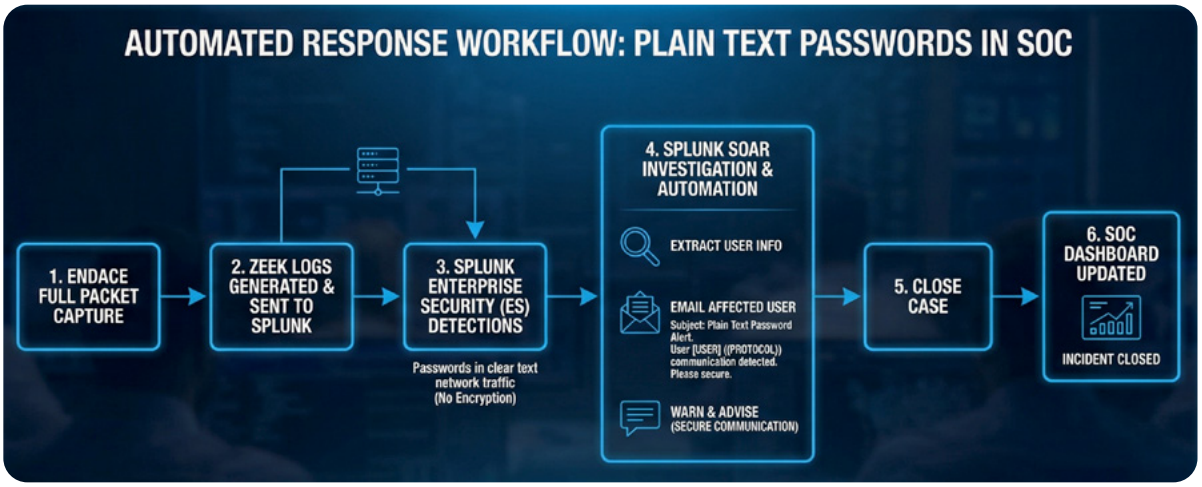
To achieve true end-to-end orchestration, the SOC engineering team transitioned from standalone scripting to a fully integrated SOAR model.

The complex search queries originally used for the dashboard were converted into formal detection findings within Splunk ES. Engineers ensured these detections accurately parsed critical data, specifically isolating the entity/risk_object fields to capture the affected user's email address.

- **Action 1 (automated communication)**
  Utilizing an out-of-the-box internal_smtp action, the playbook automatically extracts the user's email from the finding and dispatches a standardized security warning and remediation instructions.
- **Action 2 (ticket lifecycle management)**
  Utilizing an API, the playbook automatically updates the finding's disposition to "Benign Positive—Suspicious But Expected" and shifts the incident status from "New" to "Closed."

Automation rules

Leveraging a new feature in Splunk ES, an Automation Rule was established to seamlessly link the cleartext password detection rule directly to the newly created SOAR playbook.



Attendee risk notification

Below is the email received by RSAC 2026 attendees with passwords in the clear.

From: [redacted]
Date: Tuesday, March 24, 2026 at 11:48
To [redacted]
Subject: RSAC Security Operations Center- Important Information About Your Account Password

Hello [redacted]

Thank you for attending RSA Conference (RSAC) 2026.

At the Security Operations Center, we protect the network and the attendees.

During the course of the conference, we observed that one of the accounts that you own is sending and receiving emails in plain text either via POP3, HTTP, FTP protocol, which is not secure.

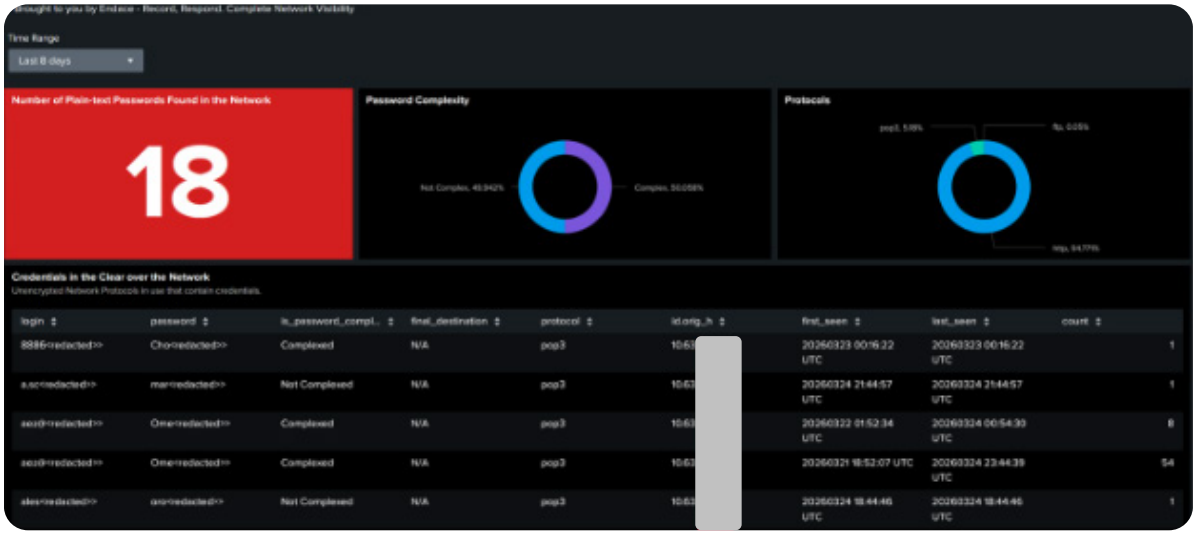
Your password and contents of your email are visible on the conference network.

We are happy to show you the data, so you can connect with your service provider and update your email protocol.

The SOC is open during Expo hours each day through Thursday, March 27th. We are in the South expo hall 3500 at the bottom of the escalators.

Best regards,
[redacted]

The redacted case data was then updated on the SOC dashboard.



4.3 DNS and application visibility

This year at RSAC 2026, 20,581 devices used the Network to connect to the Internet, and the SOC saw over 63 million DNS requests throughout the week, of which over 17,400 would have been blocked for security policy violations in an enterprise environment.

Requests

Name	Allowed	Blocked	Total	% of Total
Security	17,400	65	17,465	0.03%
Categories	-	543	543	0.0009%
Destination Lists	0	0	0	0.00%
Permitted	63,797,651	-	63,797,651	99.97%
Total	63,815,051	608	63,815,659	100%

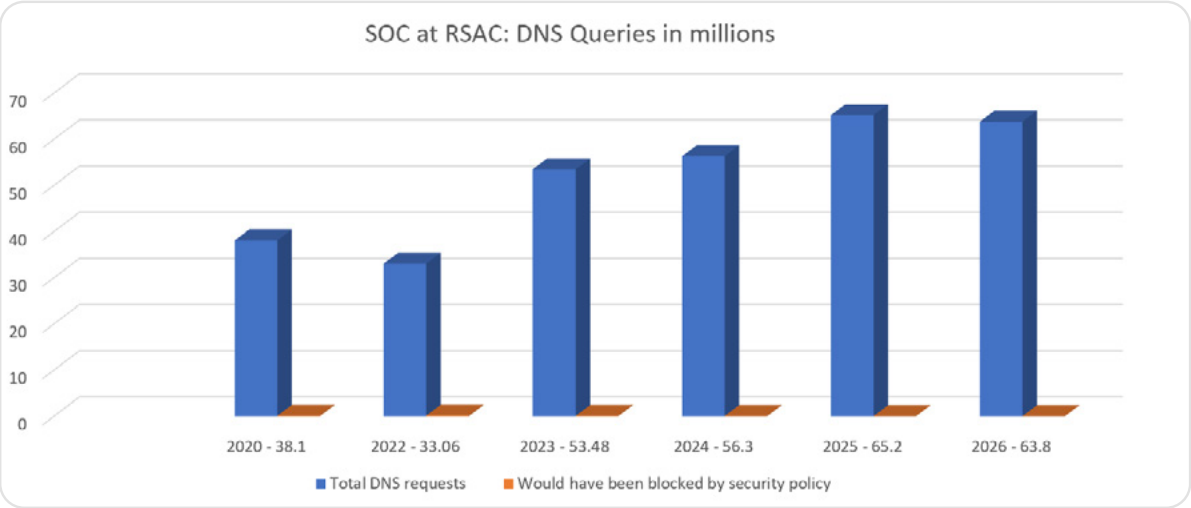
Many enterprise environments block Encrypted DNS queries, as they can be a security vulnerability.
At RSAC 2026 we encourage encryption, and more than 1.1 million encrypted queries were allowed in 2026.

As mentioned earlier in the architecture, Secure Access VAs were deployed in the Moscone NOC as internal, recursive DNS resolvers. The benefit of those VAs is two-fold:

- Outbound encryption of DNS queries
- Visibility into the internal IP address of the client

Name	Allowed	Blocked	Total	% of Total
Security	17,400	65	17,465	0.03%
— Prevent	13,086	37	13,123	0.02%
— Malware	4,786	37	4,823	0.0076%
— Dynamic DNS	7,406	0	7,406	0.01%
— Newly Seen Domains	887	0	887	0.0014%
— Potentially Harmful	0	0	0	0.00%
— DNS Tunneling	0	0	0	0.00%
— Cryptomining	7	0	7	0.0000%
— Contain	4,314	28	4,342	0.0068%
— Command & Control	5	0	5	0.0000%
— Phishing	4,309	28	4,337	0.0068%

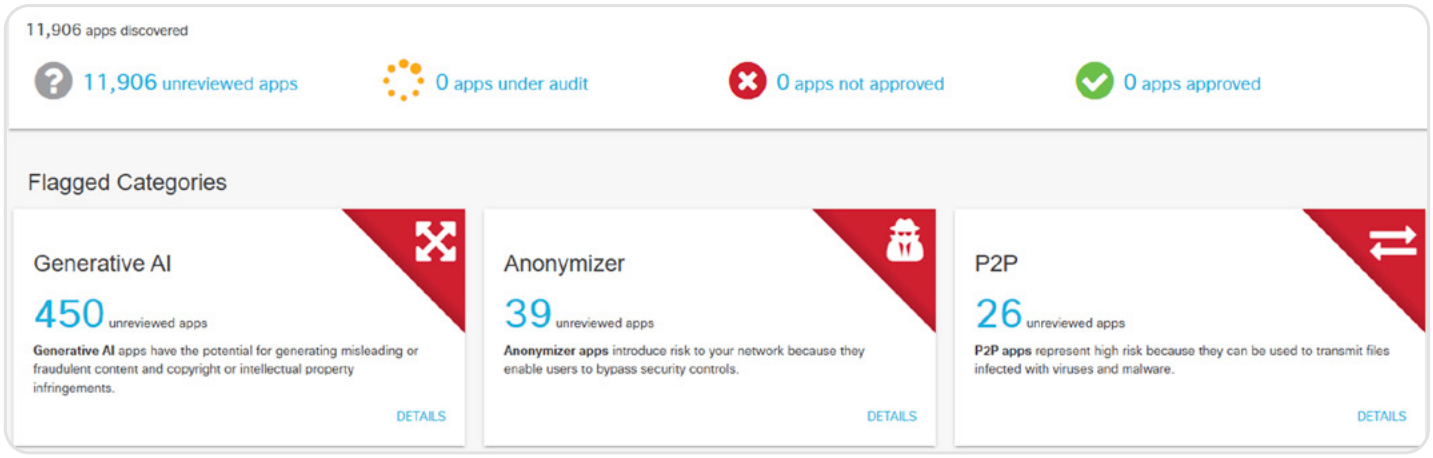
This enabled Secure Access reporting to now contain rich data that enables more efficient threat hunting and correlation with other network activity. The Secure Access VAs provide the DNS resolution and in 2025, the Moscone NOC team used firewall rules to redirect hard coded DNS queries (such as to 8.8.8.8) back to the VAs.



Apps, apps and more apps

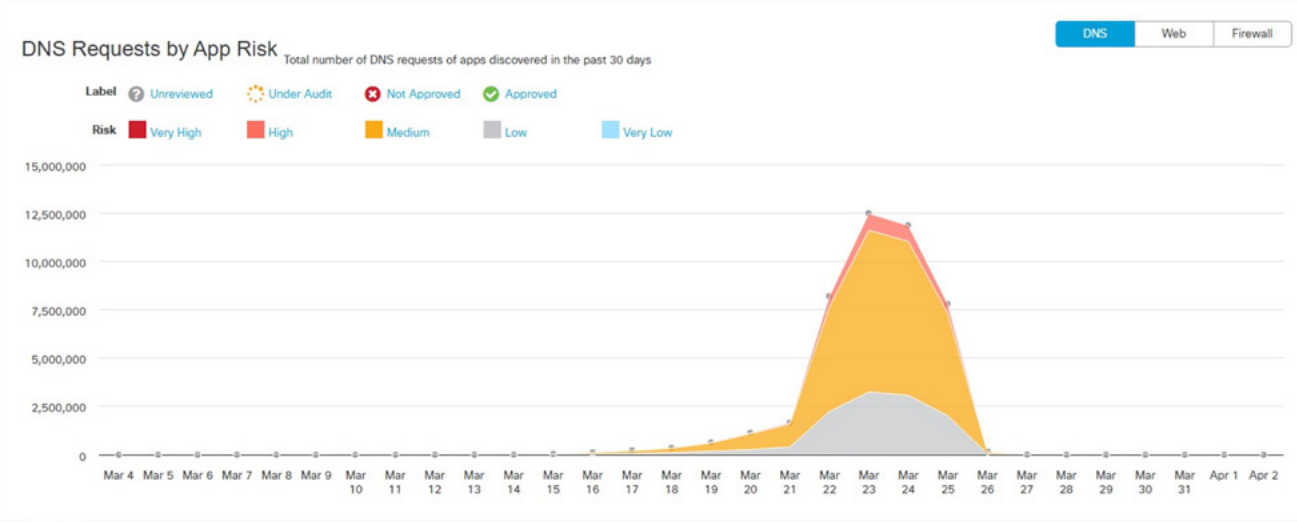
This year at RSAC 2026, 11,906 distinct applications were identified by DNS queries. This is a slight increase from 2025.

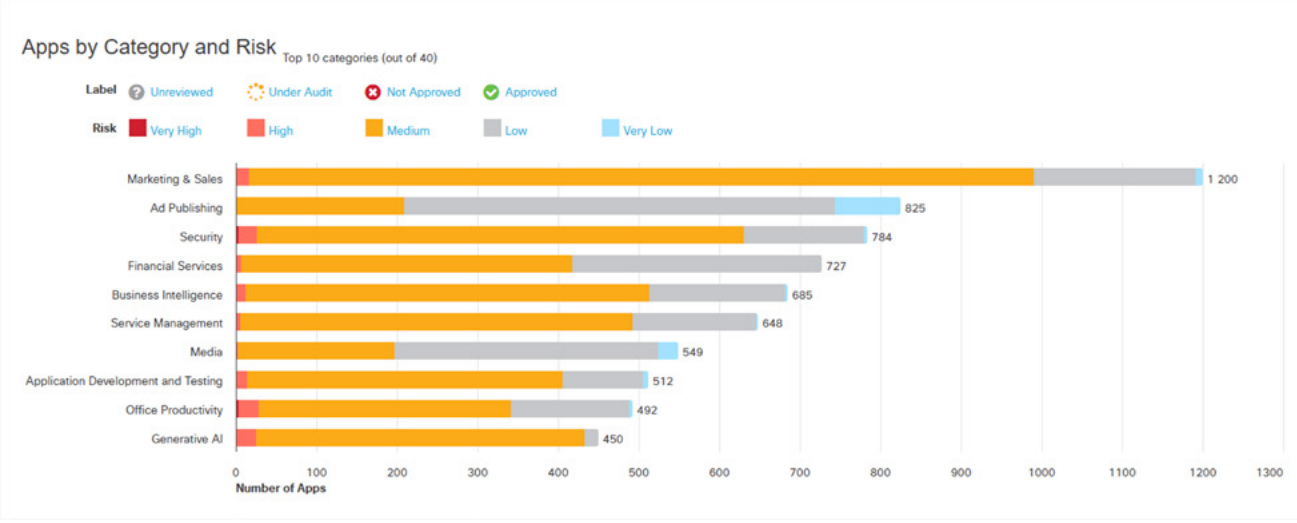
2026 11,906 apps	**2025** 11,802 apps	**2024** 10,167 apps
2023 8,750 apps	**2022** 7,200+ apps	**2020** ~4,000 apps



The apps were categorized by risk to an organization in a typical enterprise environment. In the event that an app was implicated in a major incident or caused a service disruption, the SOC would have leveraged blocking capabilities to mitigate any impact.

For destinations where access was blocked, a popup message was used to inform attendees, including information on how to contact the SOC.





Shadow AI

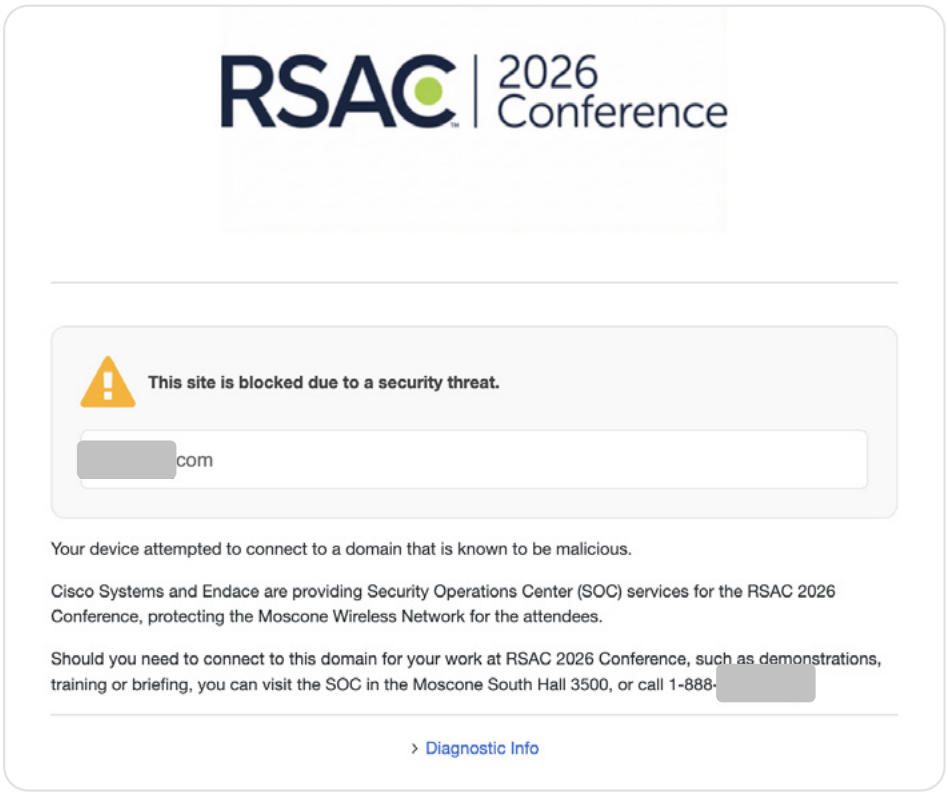
Organizations increasingly face the challenge of "shadow AI," which involves unsanctioned AI use that must be detected, managed, and secured effectively.

The SOC leveraged Cisco AI Defense within Security Cloud Control as an App Discovery function to identify and classify AI models accessed over the network. This allows security teams to identify which AI applications are being used, their associated risk levels, and the volume of traffic (DNS requests) they generate.

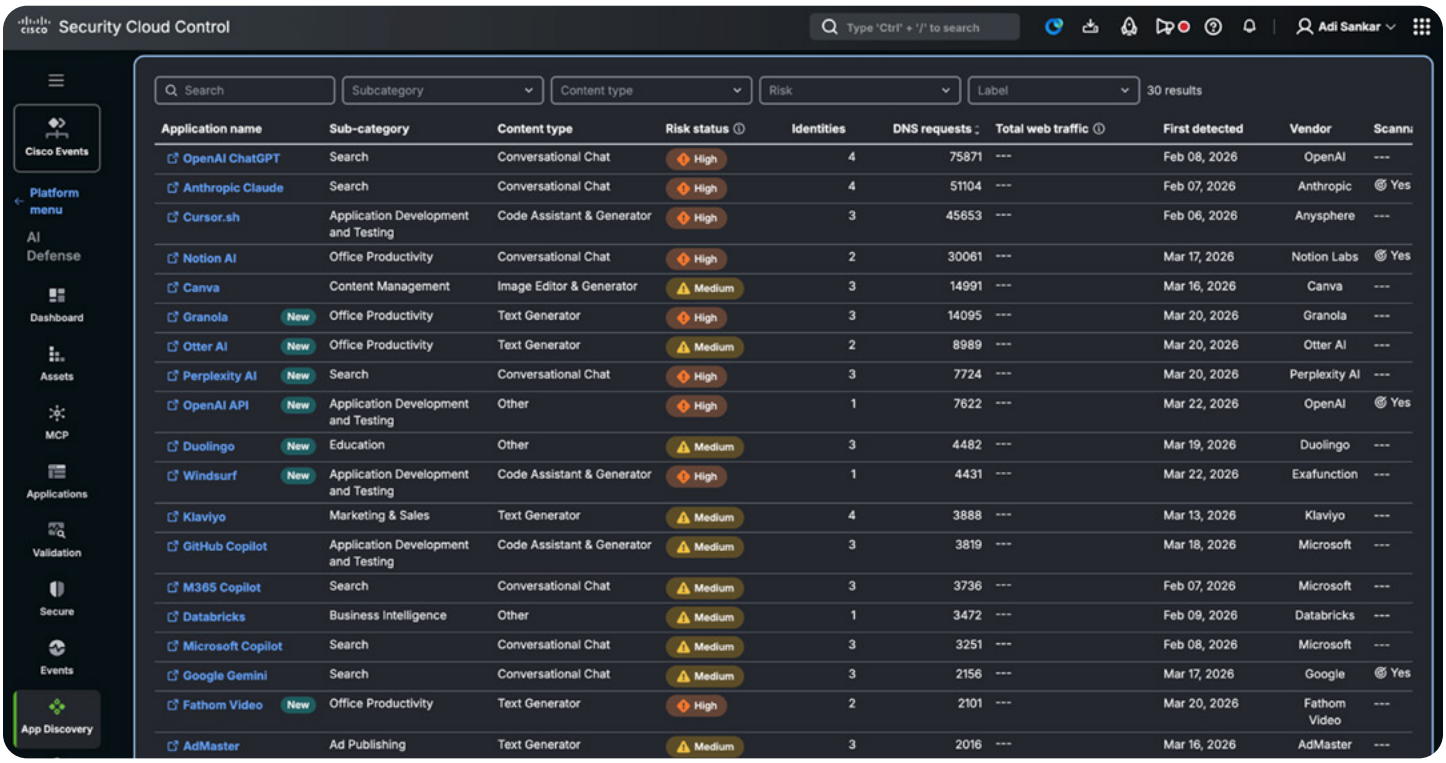
Risk assessment and enforcement

Using AI models without an established legal agreement (such as an enterprise data processing agreement) poses significant risks, as standard consumer terms may not protect sensitive corporate data, potentially leading to data loss or unauthorized training on proprietary information.

Beyond visibility, the platform enables administrators to take action. At RSAC 2026 we took a permissive approach and allowed access to all AI models. In an enterprise environment we would integrate with Secure Access to enforce policies that restrict or block access to specific AI models that fail to meet internal security standards, thereby mitigating the risk of data exposure.



The AI Defense dashboard provided the necessary visibility to audit the landscape of AI models accessed via the Network. The Security Cloud Control dashboard gave us a comprehensive view of high-risk applications in use at RSAC 2026, providing an understanding of exposure to potential for intellectual property leakage or data loss when AI is used in an inappropriate or unsanctioned manner. Should an incident on the Network require the SOC to block or restrict the use of a model, we retained the ability to protect the Network and attendees.



Application name	Sub-category	Content type	Risk status	Identities	DNS requests	Total web traffic	First detected	Vendor	Scanni
OpenAI ChatGPT	Search	Conversational Chat	High	4	75871	---	Feb 08, 2026	OpenAI	---
Anthropic Claude	Search	Conversational Chat	High	4	51104	---	Feb 07, 2026	Anthropic	Yes
Cursor.sh	Application Development and Testing	Code Assistant & Generator	High	3	45653	---	Feb 06, 2026	Anysphere	---
Notion AI	Office Productivity	Conversational Chat	High	2	30061	---	Mar 17, 2026	Notion Labs	Yes
Canva	Content Management	Image Editor & Generator	Medium	3	14991	---	Mar 16, 2026	Canva	---
Granola New	Office Productivity	Text Generator	High	3	14095	---	Mar 20, 2026	Granola	---
Otter AI New	Office Productivity	Text Generator	Medium	2	8989	---	Mar 20, 2026	Otter AI	---
Perplexity AI New	Search	Conversational Chat	High	3	7724	---	Mar 20, 2026	Perplexity AI	---
OpenAI API New	Application Development and Testing	Other	High	1	7622	---	Mar 22, 2026	OpenAI	Yes
Duolingo New	Education	Other	Medium	3	4482	---	Mar 19, 2026	Duolingo	---
Windsurf New	Application Development and Testing	Code Assistant & Generator	High	1	4431	---	Mar 22, 2026	Exafunction	---
Klaviyo	Marketing & Sales	Text Generator	Medium	4	3888	---	Mar 13, 2026	Klaviyo	---
GitHub Copilot	Application Development and Testing	Code Assistant & Generator	Medium	3	3819	---	Mar 18, 2026	Microsoft	---
M365 Copilot	Search	Conversational Chat	Medium	3	3736	---	Feb 07, 2026	Microsoft	---
Databricks	Business Intelligence	Other	Medium	1	3472	---	Feb 09, 2026	Databricks	---
Microsoft Copilot	Search	Conversational Chat	Medium	3	3251	---	Feb 08, 2026	Microsoft	---
Google Gemini	Search	Conversational Chat	Medium	3	2156	---	Mar 17, 2026	Google	Yes
Fathom Video New	Office Productivity	Text Generator	High	2	2101	---	Mar 20, 2026	Fathom Video	---
AdMaster	Ad Publishing	Text Generator	Medium	3	2016	---	Mar 16, 2026	AdMaster	---

5. Threat landscape and findings

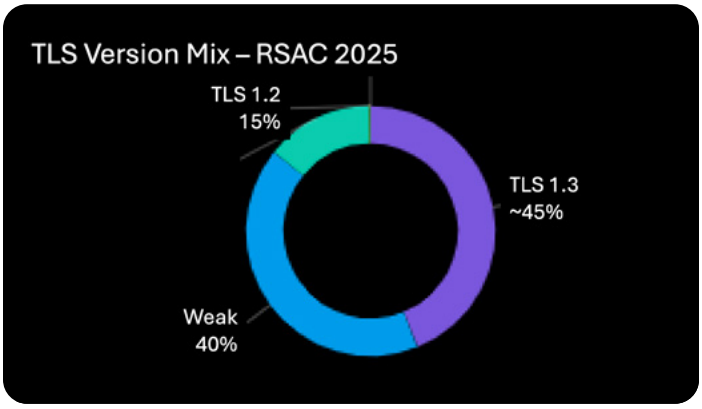
5.1 Encryption analysis

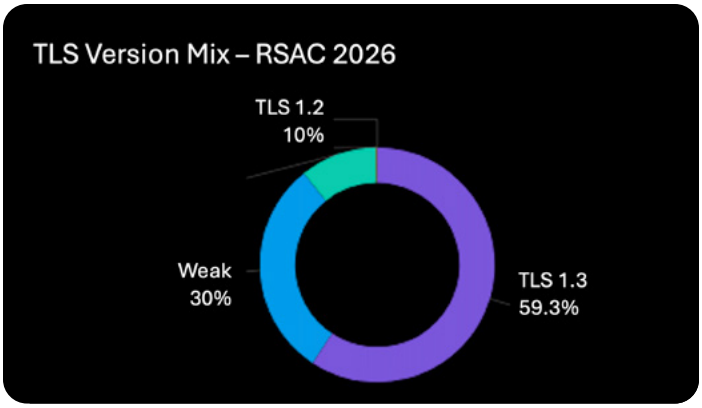
The importance of encryption

Encryption is essential at RSAC Conference, where attendees frequently transmit sensitive, non-public information. Unencrypted traffic represents a major security vulnerability; while the SOC leverages advanced Cisco and Endace technologies to monitor these risks at scale, this same data can be intercepted by anyone using basic, readily available tools. The SOC utilizes its security stack to categorize these threats and evaluate the exposure of attendee data to unauthorized parties.

SOC policy and mission

The SOC Team enforces a strict policy prohibiting the decryption of encrypted traffic. One mission of the SOC is educational: to help attendees learn how to better protect their data. Although encryption alone does not guarantee complete security, it serves as the primary defense against exposing credentials and data across both north-south and east-west traffic flows.

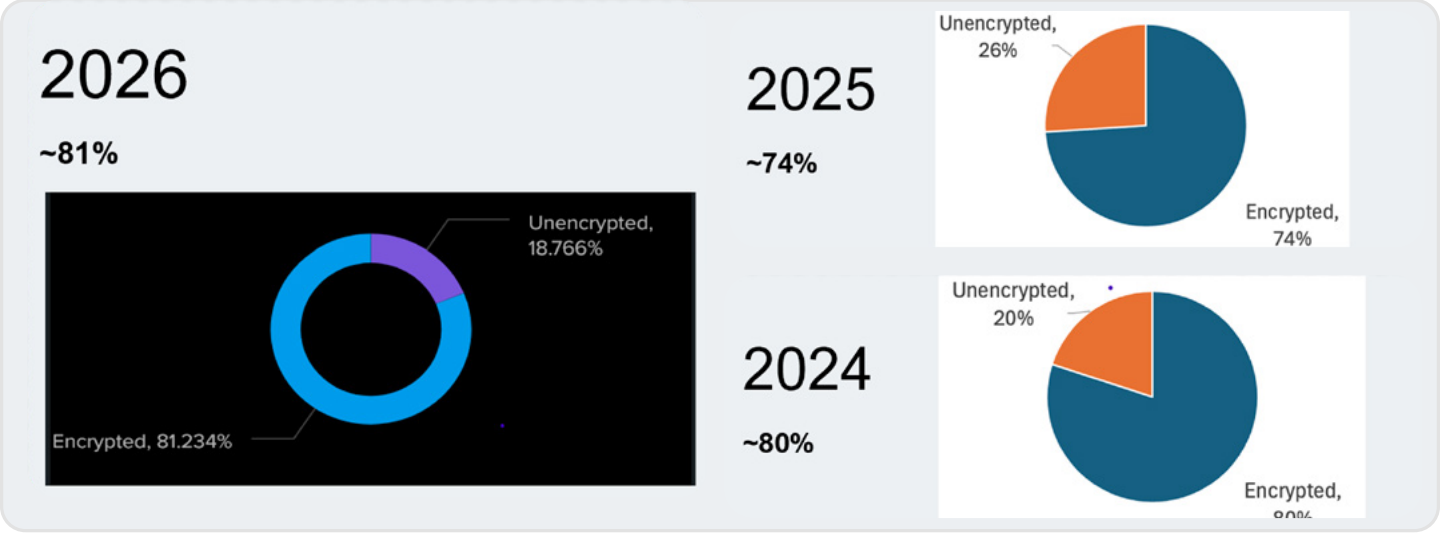




Encryption trends and findings

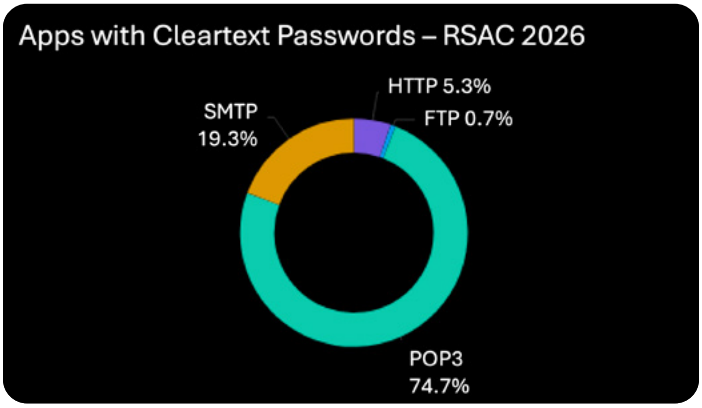
In 2025, we began reporting on the strength of encryption across the Network. The 2026 data shows good progress moving to strong encryption, weak encryption decreased from 40% to 30% of total traffic. “Weak” encryption is defined as TLS 1.0 or 1.1—protocols that are vulnerable to brute-force attacks and should have been deprecated in favor of TLS 1.2 or 1.3. 30% is still a significant portion of traffic leveraging weak encryption.

Another positive trend, we saw a decrease in the amount of un-encrypted traffic, from 26% last year down to 18% this year reverting back to the levels we saw in 2024, where 20% was un-encrypted during RSAC 2024. While these improvements are welcome, significant progress is still needed to ensure only modern protocols are used. 39% of traffic observed at RSAC 2026 was either weakly encrypted or not encrypted at all.



Analyzing un-encrypted traffic showed us that the majority was unsecured email using POP3, IMAP and SMTP. In some cases, these email sessions carried sensitive information such as product plans, in other cases these included exploitable information such as invoices that could be cloned and used to extract payment from the unwitting or credentials that could be abused by an attacker. What makes the volume of unencrypted email traffic notable is that most major email providers (Microsoft, Google, Yahoo/AOL, etc) have phased out unencrypted mail protocols, which implies that most of this insecure infrastructure is either corporate in nature or leveraging lesser known email providers.

Unsecured HTTP was also evident in the unencrypted traffic stream, including login pages. Where possible, the SOC team at RSAC 2026 tracked down users of these websites to help better secure their environments and applications.



5.2 Malware detection with the encrypted visibility engine

RSAC 2026 is a challenging conference for firewall monitoring because over 70% of traffic is encrypted, and TLS is not decrypted. While this is an excellent move to protect attendee privacy, traditional capabilities like Intrusion Detection Systems struggle to detect threats in encrypted traffic.

To address this challenge, Cisco Secure Firewall has a capability called Encrypted Visibility Engine (EVE) mentioned in Section 2.3, that provides powerful detection capabilities for traffic where TLS decryption isn't possible. With EVE, fingerprints are assigned to encrypted sessions along with a confidence score regarding whether or not the communicating process is malicious, all without decryption.

One of the fingerprints the SOC tracked at RSAC 2026 is for the upatre malware. Upatre is an older strain that has been repurposed multiple times by threat actors.

The connections that matched with known fingerprints and their malware associations were to a pair of online services that return the public IP of an internal host.

EVE Process Name	EVE Threat Confidence	EVE Process Confidence Score
malware-upatre	High	86%
malware-upatre	High	86%
malware-generic-infostealer	High	93%
malware-generic-infostealer	High	93%
malware-upatre	High	86%
malware-generic-infostealer	High	93%
malware-generic-infostealer	High	93%
malware-upatre	High	86%
malware-generic-infostealer	High	93%
malware-upatre	High	86%
malware-upatre	High	86%
malware-generic-infostealer	High	91%
malware-upatre	High	86%
malware-generic-infostealer	High	91%

These services have a number of legitimate uses for various tools, but they are also used by malware to identify the public IP of a compromised host.

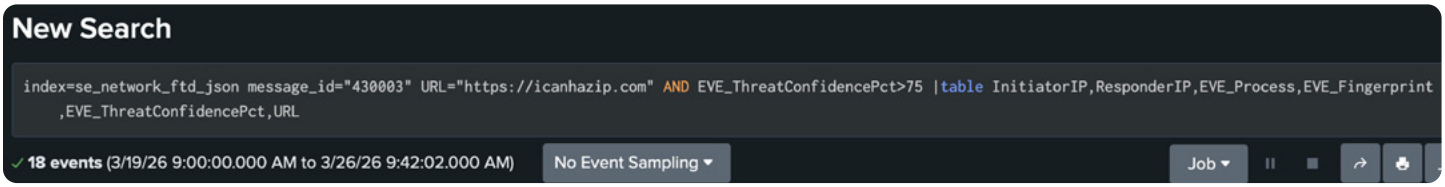
A key capability of EVE is that it uses its granular fingerprinting system to differentiate between legitimate and illegitimate connections to these services.

InitiatorIP	ResponderIP	EVE_Process	EVE_Fingerprint	EVE_ThreatConfidencePct	URL
10.63	104.16	malware-generic-infostealer	tls/1/(0303)(13021301c02cc02bc030c02fc024c023c028c027c00ac009c014c013009d009c003d003c0035002f)[(0000)(000a00080006001d00170018)(000b00020100)(000d001a00180804080508060401050102010403050302030202060106003)(0017)(0023)(002b0009080304030303020301)(002d00020101)(0031)(0033)(ff01)]	93	https://icanhazip.com
10.63	23.158	malware-upatre	tls/1/(0303)(13021301c02cc02bc030c02fc024c023c028c027c00ac009c014c013009d009c003d003c0035002f)[(0000)(000a00080006001d00170018)(000b00020100)(000d001a00180804080508060401050102010403050302030202060106003)(0017)(0023)(002b0009080304030303020301)(002d00020101)(0031)(0033)(ff01)]	88	https://wtfismyip.com
10.63	23.158	malware-upatre	tls/1/(0303)(13021301c02cc02bc030c02fc024c023c028c027c00ac009c014c013009d009c003d003c0035002f)[(0000)(000a00080006001d00170018)(000b00020100)(000d001a00180804080508060401050102010403050302030202060106003)(0017)(0023)(002b0009080304030303020301)(002d00020101)(0031)(0033)(ff01)]	88	https://wtfismyip.com
10.63	104.16	malware-generic-infostealer	tls/1/(0303)(13021301c02cc02bc030c02fc024c023c028c027c00ac009c014c013009d009c003d003c0035002f)[(0000)(000a00080006001d00170018)(000b00020100)(000d001a00180804080508060401050102010403050302030202060106003)(0017)(0023)(002b0009080304030303020301)(002d00020101)(0031)(0033)(ff01)]	93	https://icanhazip.com
10.63	104.16	malware-generic-infostealer	tls/1/(0303)(13021301c02cc02bc030c02fc024c023c028c027c00ac009c014c013009d009c003d003c0035002f)[(0000)(000a00080006001d00170018)(000b00020100)(000d001a00180804080508060401050102010403050302030202060106003)(0017)(0023)(002b0009080304030303020301)(002d00020101)(0031)(0033)(ff01)]	91	https://icanhazip.com
10.63	23.158	malware-upatre	tls/1/(0303)(13021301c02cc02bc030c02fc024c023c028c027c00ac009c014c013009d009c003d003c0035002f)[(0000)(000a00080006001d00170018)(000b00020100)(000d001a00180804080508060401050102010403050302030202060106003)(0017)(0023)(002b0009080304030303020301)(002d00020101)(0031)(0033)(ff01)]	88	https://wtfismyip.com
10.63	104.16	malware-generic-infostealer	tls/1/(0303)(13021301c02cc02bc030c02fc024c023c028c027c00ac009c014c013009d009c003d003c0035002f)[(0000)(000a00080006001d00170018)(000b00020100)(000d001a00180804080508060401050102010403050302030202060106003)(0017)(0023)(002b0009080304030303020301)(002d00020101)(0031)(0033)(ff01)]	91	https://icanhazip.com

InitiatorIP	ResponderIP	EVE_Process	EVE_Fingerprint	EVE_ThreatConfidencePct	URL
10.63	104.16	malware-generic-infostealer	tls/1/(0303)(13021301c02cc02bc030c02fc024c023c028c027c00ac009c014c013009d009c003d003c0035002f)[(0000)(000a00080006001d00170018)(000b00020100)(000d001a00180804080508060401050102010403050302030202060106003)(0017)(0023)(002b0009080304030303020301)(002d00020101)(0031)(0033)(ff01)]	93	https://icanhazip.com
10.63	23.158	malware-upatre	tls/1/(0303)(13021301c02cc02bc030c02fc024c023c028c027c00ac009c014c013009d009c003d003c0035002f)[(0000)(000a00080006001d00170018)(000b00020100)(000d001a00180804080508060401050102010403050302030202060106003)(0017)(0023)(002b0009080304030303020301)(002d00020101)(0031)(0033)(ff01)]	88	https://wtfismyip.com
10.63	23.158	malware-upatre	tls/1/(0303)(13021301c02cc02bc030c02fc024c023c028c027c00ac009c014c013009d009c003d003c0035002f)[(0000)(000a00080006001d00170018)(000b00020100)(000d001a00180804080508060401050102010403050302030202060106003)(0017)(0023)(002b0009080304030303020301)(002d00020101)(0031)(0033)(ff01)]	88	https://wtfismyip.com
10.63	104.16	malware-generic-infostealer	tls/1/(0303)(13021301c02cc02bc030c02fc024c023c028c027c00ac009c014c013009d009c003d003c0035002f)[(0000)(000a00080006001d00170018)(000b00020100)(000d001a00180804080508060401050102010403050302030202060106003)(0017)(0023)(002b0009080304030303020301)(002d00020101)(0031)(0033)(ff01)]	93	https://icanhazip.com
10.63	104.16	malware-generic-infostealer	tls/1/(0303)(13021301c02cc02bc030c02fc024c023c028c027c00ac009c014c013009d009c003d003c0035002f)[(0000)(000a00080006001d00170018)(000b00020100)(000d001a00180804080508060401050102010403050302030202060106003)(0017)(0023)(002b0009080304030303020301)(002d00020101)(0031)(0033)(ff01)]	91	https://icanhazip.com
10.63	23.158	malware-upatre	tls/1/(0303)(13021301c02cc02bc030c02fc024c023c028c027c00ac009c014c013009d009c003d003c0035002f)[(0000)(000a00080006001d00170018)(000b00020100)(000d001a00180804080508060401050102010403050302030202060106003)(0017)(0023)(002b0009080304030303020301)(002d00020101)(0031)(0033)(ff01)]	88	https://wtfismyip.com
10.63	104.16	malware-generic-infostealer	tls/1/(0303)(13021301c02cc02bc030c02fc024c023c028c027c00ac009c014c013009d009c003d003c0035002f)[(0000)(000a00080006001d00170018)(000b00020100)(000d001a00180804080508060401050102010403050302030202060106003)(0017)(0023)(002b0009080304030303020301)(002d00020101)(0031)(0033)(ff01)]	91	https://icanhazip.com

A great demonstration of the precision of EVE fingerprints is when we run a query for just the icanhazip[.]com URL, we get 6,293 hits.

As we said above, this service is used by legitimate tools. Whether the site is launched by a legitimate tool, a user, or malware, the URL will be the same. EVE sorts through this massive dataset to only identify the malicious connections. If we run the same search again for an EVE threat score of 75 or above, we get just 18 events:



Malware identification is very difficult at the SOC because we don't have any visibility into the endpoint. We can't run a virus scan or look for a malicious process, and unless we happen to see a malware file sent in plain text across the Network, we won't know about it. But with the granular detection of EVE, we can gain confidence that a given connection was initiated by malware.

For the event set above, EVE's granularity gave us the confidence to raise a malware detection with RSAC Conference based just on encrypted network traffic. The incident report led to a laptop being seized and taken off the network.

Discovered processes

In addition to the malicious process detections covered earlier in the blog, the Encrypted Visibility Engine can provide visibility into both rare process usage and the most widely used processes as well. Below is a dashboard that shows the most common processes that EVE detected at the conference:

EVE Discovered Processes

EVE Process Name	Total Connections
apple safari/networking	15,359,840
chromium browser	12,141,863
microsoft office	3,577,511
zscaler tunnel	2,036,563
google chromeos vm ...	1,972,237
hangzhou hikvision	1,529,318
cisco secure client	1,179,075
cisco webex	988,978
microsoft teams	837,415
python	650,257
firefox browser	648,874
openai chatgpt	623,996
slack	598,979
ixeau cursor	490,220
microsoft networking	487,280
generic mobile process	447,223
tailscale vpn	405,658
adobe productivity	380,387
apple news	370,613
whatsapp	352,212

EVE also has a dashboard that breaks connections down into broad categories. As shown below, the vast number of connections had a threat score of “Very Low”, while only 15 had a threat score of “Very High”:

EVE Threat Confidence

EVE Threat Confidence	Total Connections
Very Low	52,806,073
Low	601,114
Medium	126,827
High	9,397
Very High	15

Traffic by geolocation

As expected for RSAC 2026, connections to the United States dominated traffic. We also saw moderate traffic to Europe, Asia, and some countries from other continents:

Connections by Destination Country

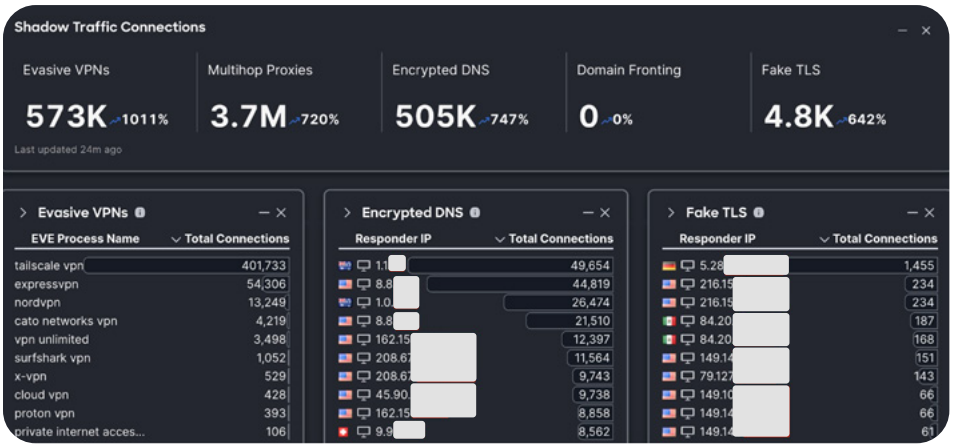
Responder Country	Allowed Connections
USA	76,843,906
DEU	593,255
IRL	539,884
SGP	487,976
NLD	449,962
AUS	428,341
CHN	402,636
GBR	390,425
KOR	271,029
CAN	240,940
JPN	237,312
IND	202,401

Threat detection

Cisco Secure Firewall detected many attempted intrusions during the conference. These attacks included SQL injection, buffer overflow, and connections to malware sinkholes.

Intrusion Events

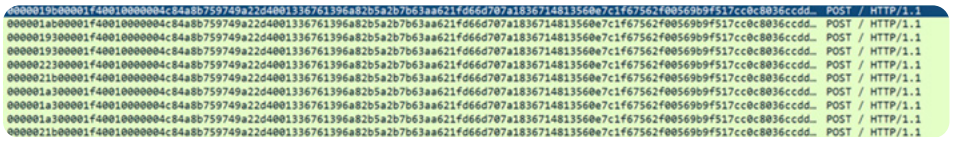
Message	Count
SERVER-WEBAPP generic server H...	869
SQL 1 = 1 - possible sql injection at...	269
INDICATOR-COMPROMISE Suspici...	66
SERVER-OTHER Cisco IOS IKEv2 s...	56
INDICATOR-COMPROMISE suspici...	35
MALWARE-CNC Torpig bot sinkhol...	32



Shadow traffic

A new feature we deployed at RSAC 2026 is the Cisco Secure Firewall Shadow Traffic dashboard.

At the SOC, we actually encourage attendees to use a VPN to better secure their traffic, but for many corporations, evasive encryption services are a threat to visibility and strong network control. The Shadow Traffic Dashboard gave broad visibility into VPN use, Encrypted DNS, and Fake TLS usage.



5.3 Malware investigations

Command and control

Since October 2025, the SOC Team has been investigating a specific suspicious behavior that has made an appearance at multiple events the SOC team has supported in different continents. The telltale signs of this persistent threat were seen emanating from multiple devices at RSAC 2026. We first detected this threat last year as HTTP post traffic to a malicious IP, digging into the packet capture data revealed a User-Agent string from a Windows Instant Messaging app that went defunct in 2008 and masquerading as MPEG video traffic.

This activity matches patterns previously observed at Cisco Live APJC 2025 and GovWare 2025. The traffic was directed to a destination IP known to be associated with Android malware, though traffic inspection indicates the involved devices may include both Apple and Android-derivative systems.

Magic Numbers and Their Meaning

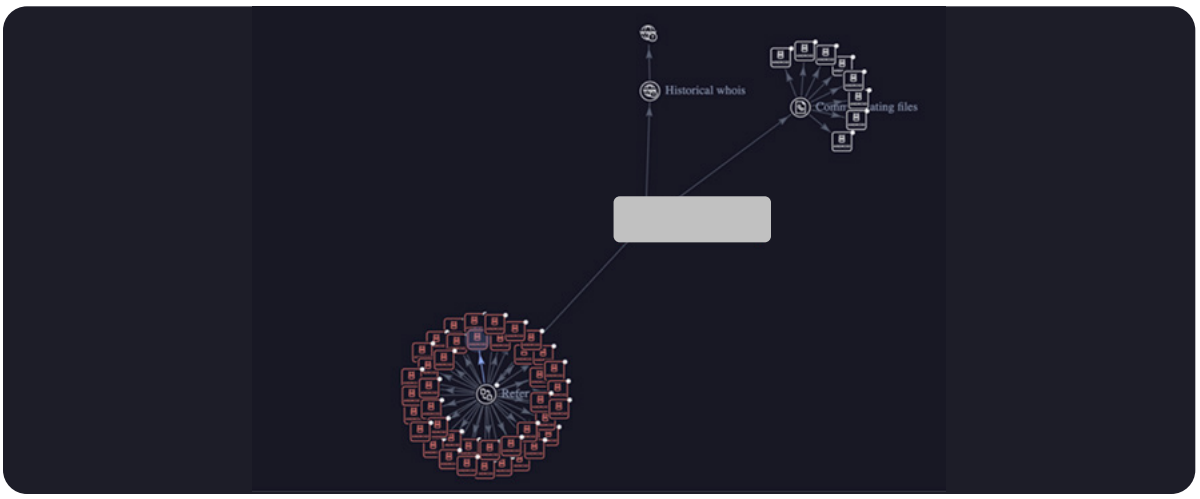
Magic Number (Hex)	Description	File Type
`00 00 01 93`	Private stream 1	MPEG-2 Program Stream (`.mpg`, `.mpeg`, `.vob`)
`00 00 01 9B`	Private stream 2	MPEG-2 Program Stream
`00 00 01 AB`	ECM stream (used in conditional access systems)	MPEG-2 Transport Stream
`00 00 02 23`	Possibly a PES (Packetized Elementary Stream) start code or proprietary extension	MPEG-2 or vendor-specific

Key Indicators of Compromise (IOCs):

- Destination IP: 162[.]14[.]17[.]141
- User-Agent: IM-SIMUHTTP
- Disguised as MPEG stream by Magic Number

The HTTP POST data contained heavily obfuscated payloads. Attempts to decode the data (using Base85, Base64, and UTF-16) resulted in untranslatable Asian scripts that caused notable hallucinations in Google Translate, though secondary AI tools confirmed the text lacked valid linguistic meaning. We are yet to break the coding of these messages, but given the behavior, association with Android malware, we suspect this to be a C2 channel attempting connection.

Analysis of mDNS queries from a 72-hour packet capture revealed significant Personally Identifiable Information (PII) also being revealed from the infected machines. Queries from the affected devices contained specific names, including the CIO/CISO of a company attending RSAC 2026, as well as other shared names. The overlap in queried names strongly indicates that at least two of the infected devices have previously resided on the same corporate network.



Analysis of mDNS queries from a 72-hour packet capture revealed significant Personally Identifiable Information (PII) also being revealed from the infected machines. Queries from the affected devices contained specific names, including the CIO/CISO of a company attending RSAC 2026, as well as other shared names. The overlap in queried names strongly indicates that at least two of the infected devices have previously resided on the same corporate network.

We noted how effectively mDNS broadcast requests were exposing the list of machine names previously connected to by the host. Some of these machine names contained the owners' full name, company name, or company specific strings, this presents an opportunity for intelligence gathering by anyone monitoring public networks. This type of PII provides threat actors with additional intelligence that may be abused to advance an attack against an organization. We recommend using a naming convention that obfuscates any PII, organization, or asset information, in this case we utilized this information to identify affected users. The prevailing theory is that the infected devices belong to conference exhibitors or attendees, who brought the pre-existing infection into the RSAC 2026 environment.

The SOC team's immediate next steps included cross-referencing the extracted PII with RSAC 2026 attendee registration data to identify and isolate the affected users. Additionally, further investigation is required to resolve the discrepancy between the expected Android-based malware profile and the presence of Apple devices generating this traffic. Understanding this persistent threat will be an ongoing research task for the SOC team.

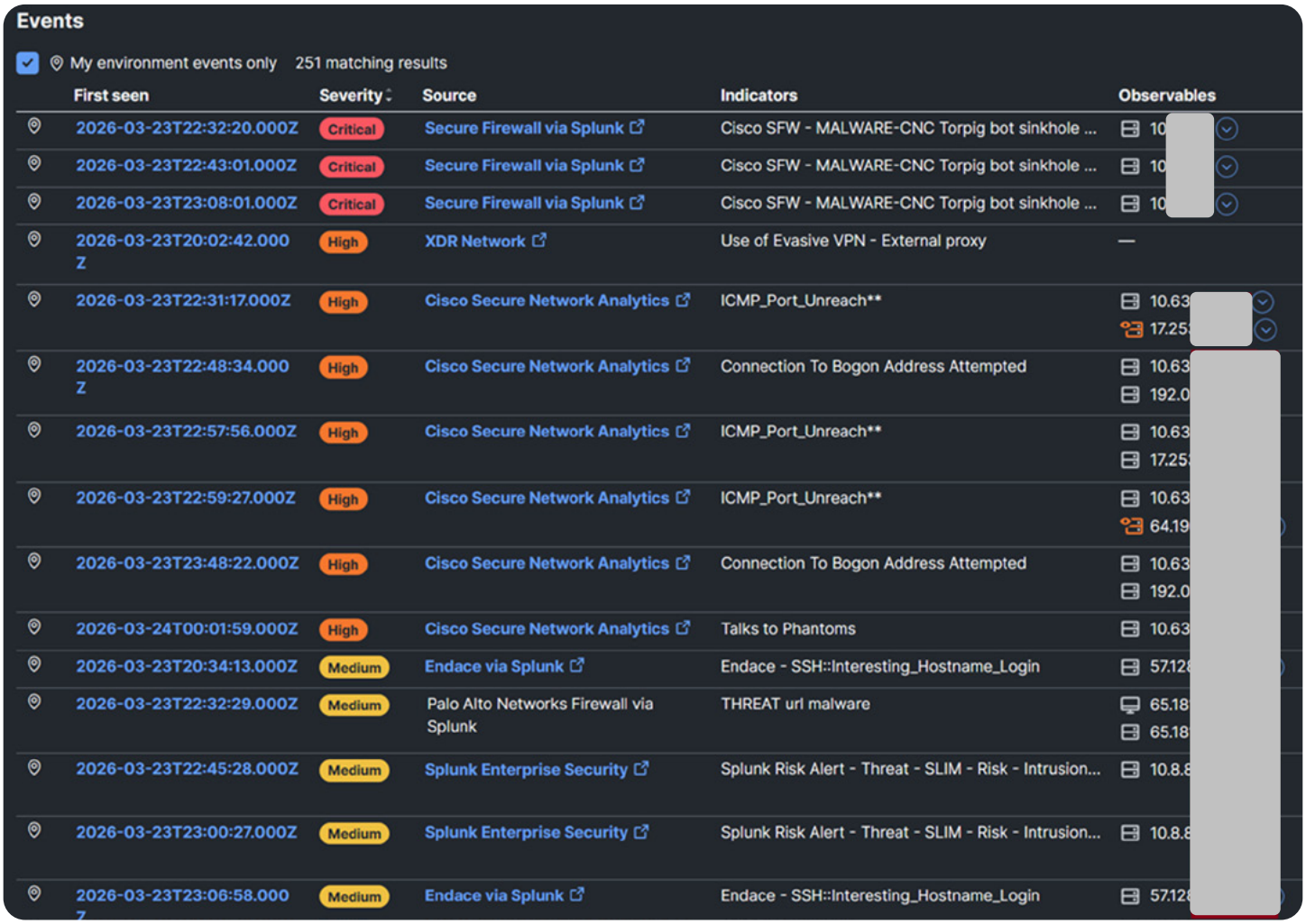
224.0.0.251	MDNS	142 5353	5353	[redacted]	F7M36FPXMJ.…
224.0.0.251	MDNS	142 5353	5353	[redacted]	F7M36FPXMJ.…
224.0.0.251	MDNS	217 5353	5353	[redacted]	mac._compan…
224.0.0.251	MDNS	217 5353	5353	[redacted]	mac._compan…
224.0.0.251	MDNS	217 5353	5353	[redacted]	mac._compan…
224.0.0.251	MDNS	217 5353	5353	[redacted]	mac._compan…
224.0.0.251	MDNS	123 5353	5353	[redacted]	rplay._tcp.…

Trojan compromise

A potentially infected endpoint was identified making repeated connections to malicious domains, strongly suggesting the presence of a Network Trojan. The investigation was initiated following a critical alert from the Firepower Management Center (FMC) indicating malware command-and-control (C2) activity.

Subsequent Cisco XDR and Splunk investigations revealed a pattern of suspicious network behaviors associated with this device.

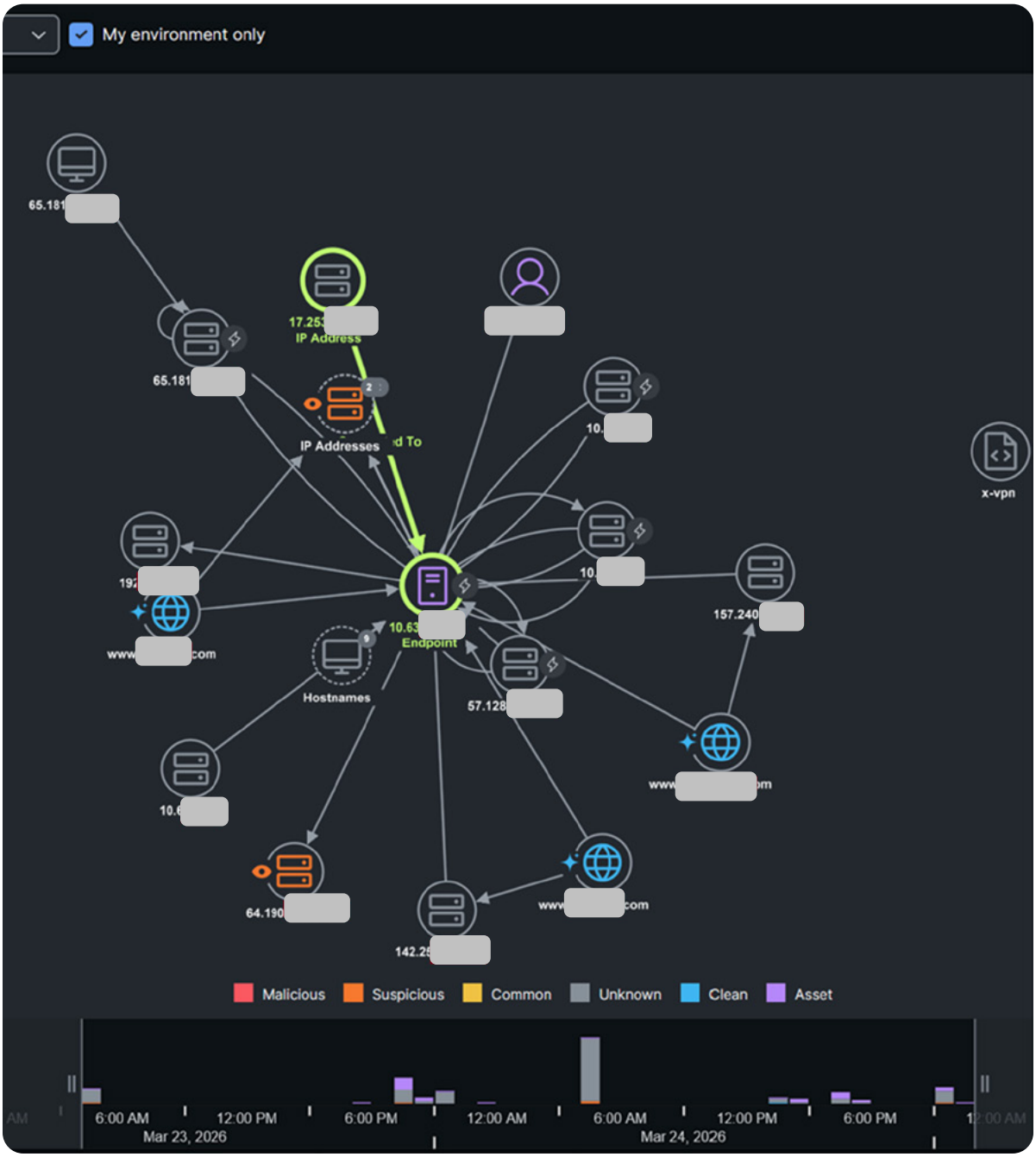
Timestamp (GMT)	Event
2026-03-23T20:02:42.000Z	First notable XDR event: “Use of Evasive VPN - External proxy”
2026-03-23T20:02:42.000Z	Another notable XDR event: “Suspicious Network Activity detected by EVE on 10.63.XX.XX”
2026-03-23T22:32:20.000Z	The event that started my investigation: “Cisco SFW - MALWARE-CNC Torpig bot sinkhole server DNS lookup”
2026-03-23T22:43:01.000Z	A second attempt of the same Critical event: “Cisco SFW - MALWARE-CNC Torpig bot sinkhole server DNS lookup”
2026-03-23T22:48:34.000Z	Another High rated event: “Connection to Bogon Address Attempted”



The repeated C2 DNS lookups and evasive network activity indicate that the machine is likely compromised by the Torpig botnet (or a related variant) and is attempting to phone home to a sinkholed server.

The SOC team worked with the NOC to identify the physical location and/or owner of the device associated with MAC address.

Coordinating with RSAC IT Security, the machine was removed from the Network immediately to prevent potential lateral movement, with the recommendation of a full forensic analysis and remediation/cleaning.

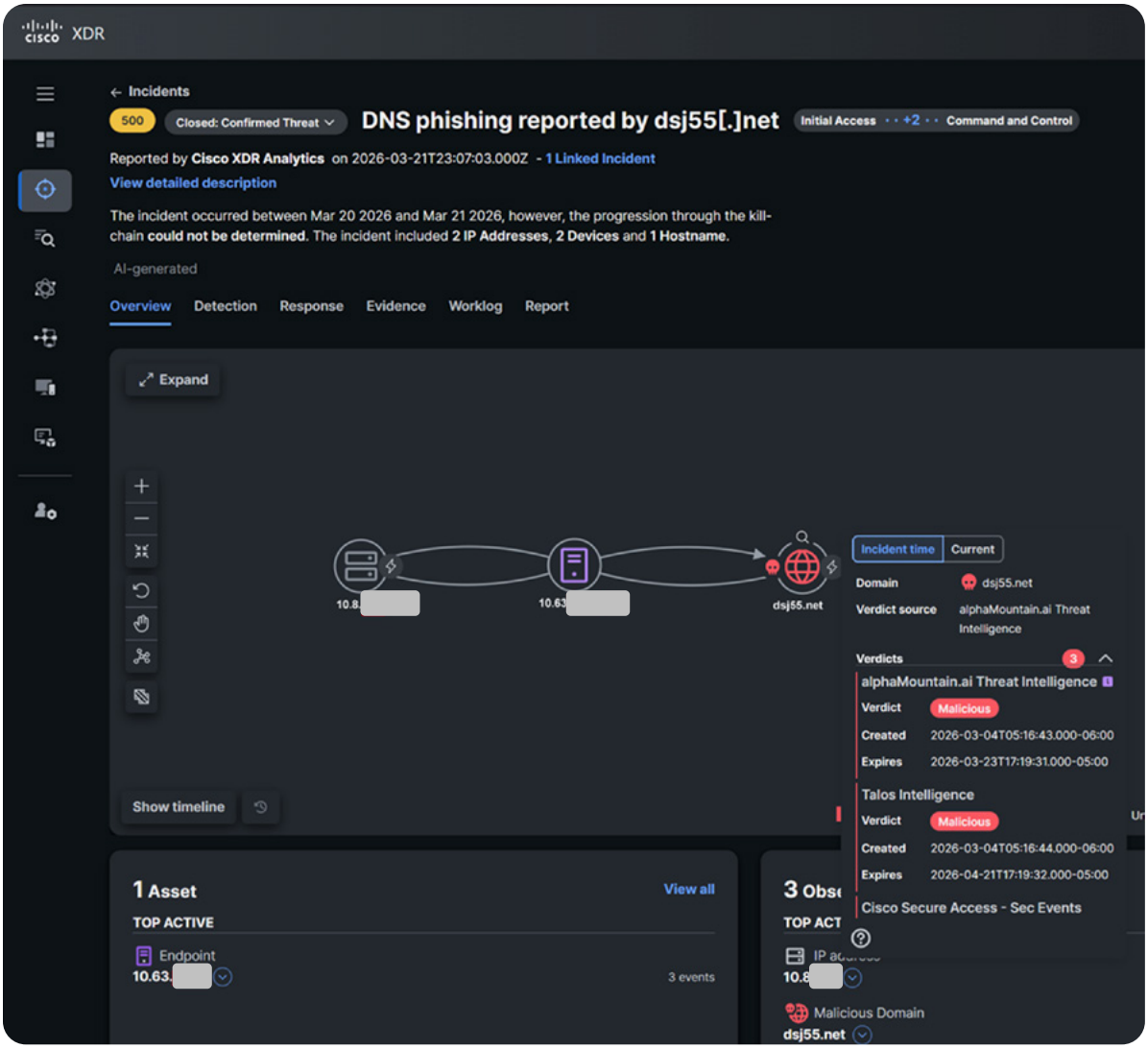


5.4 Phishing and scams

Investment scam domain activity

Between March 20 and March 22, 2026, the SOC team used Cisco Secure Access and Cisco Secure Firewall to detect suspicious DNS queries originating from the Network. Attendee devices were observed attempting to connect to known malicious domains associated with a cryptocurrency investment fraud campaign.

The domains in question are part of a suspected cryptocurrency investment scheme tracked by the Cisco SOC team and flagged by the Alberta Securities Commission (ASC) and the Financial Conduct Authority (FCA). The campaign operates under the name “BG Wealth Sharing” and is linked to a web-based trading platform called “DSJ Exchange (DSJ EX).”



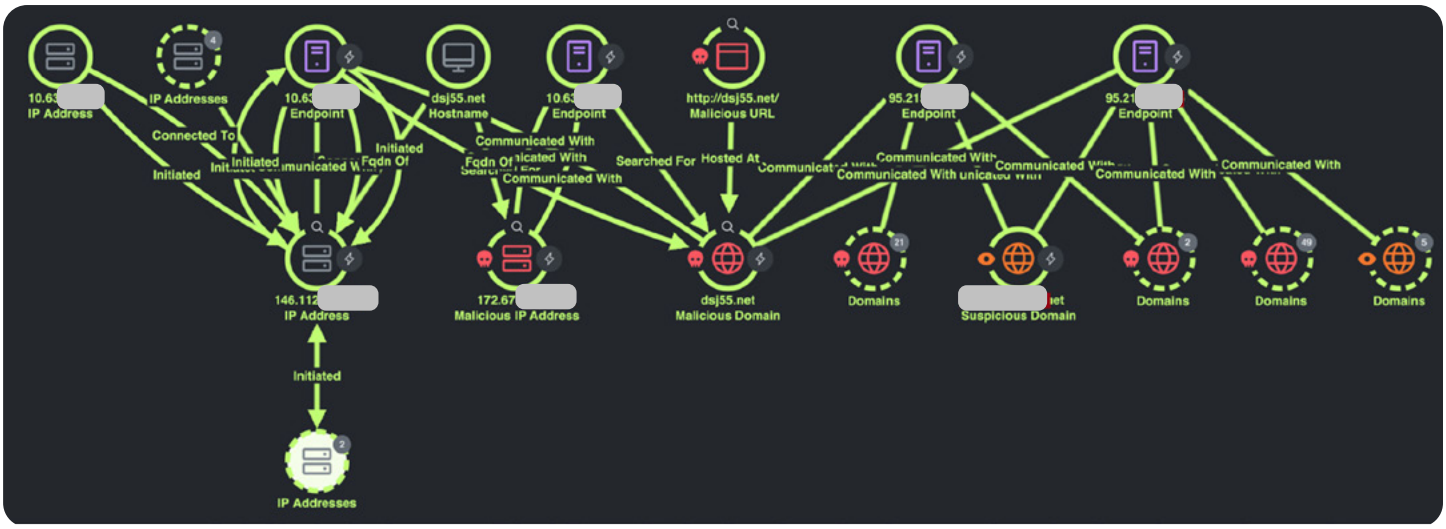
Threat actors promote the scheme via social media and encrypted messaging apps (such as Telegram, WhatsApp, and BonChat). They lure victims by claiming to use AI-generated trading signals that guarantee near-perfect trades and rapid returns. Victims are instructed to deposit cryptocurrency into DSJ EX. When users attempt to withdraw their funds, they are blocked by exorbitant withdrawal fees and artificial, time-consuming management approval processes.

Known domains: dsj55[.]net | dsj35[.]net | dsj33[.]net

Nameservers: ARMFAZH.NS.CLOUDFLARE[.]COM | TORI.NS.CLOUDFLARE[.]COM

Because the endpoints were actively querying these domains, there is a high probability that the end-users behind these devices were exposed to, or had fallen victim to, the investment scam.

The SOC team recommended that RSAC authorize the immediate blocking of all known domains and IP addresses associated with this investment scam infrastructure across the Network to prevent further compromise or financial loss.



Typo squatting and phishing domains

The SOC observed a significant surge in typo squatting over previous events. These domains were identified via threat intelligence, or when a victim device attempted DNS resolution of these domains. Notably, while investigating an unrelated case, analysts identified a lookalike domain targeting Cisco's primary corporate website.

Further monitoring revealed similar typo squatted and phishing domains mimicking the official RSAC website, which were blocked.

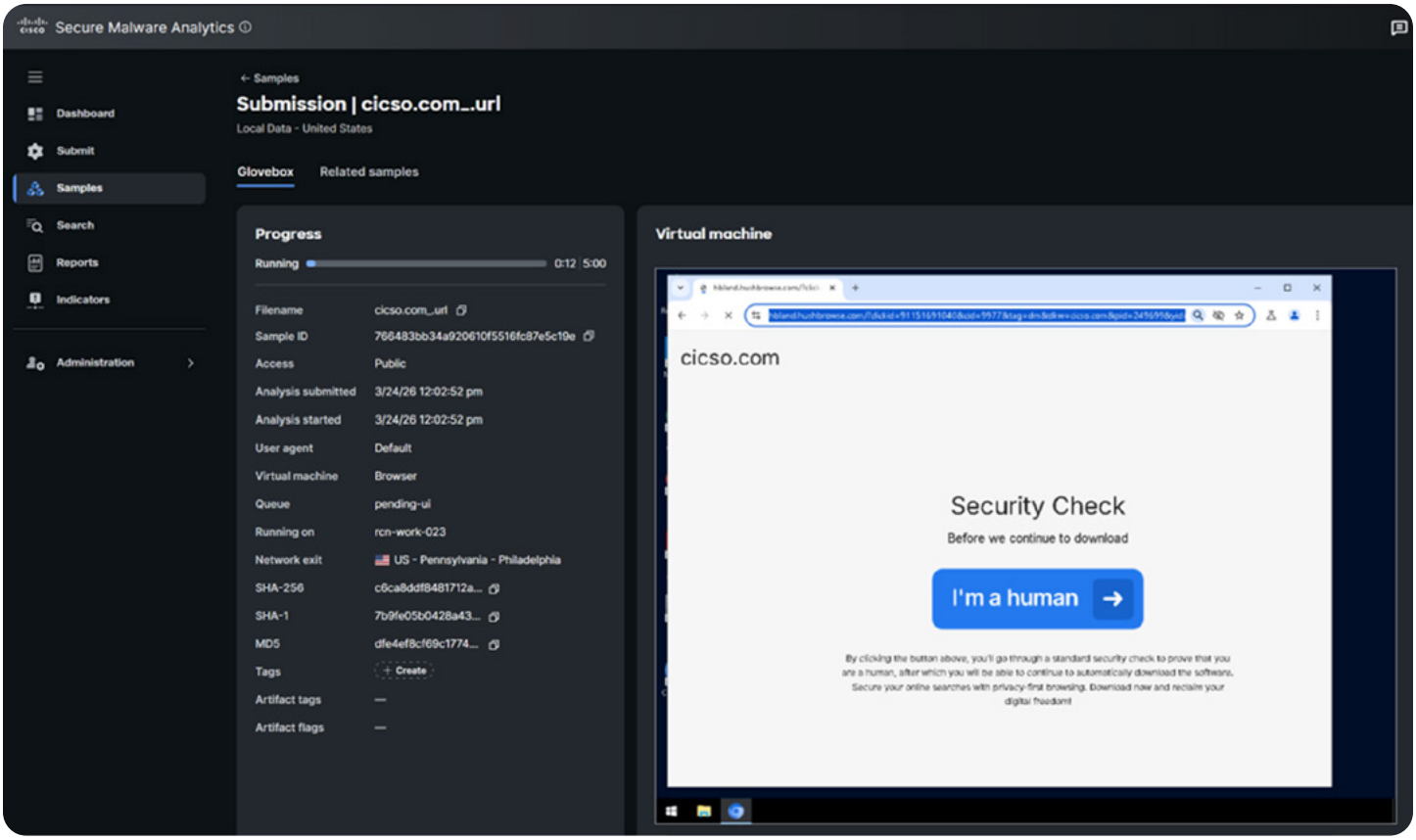
rsac2026[.]net

rsaconference2026[.]co

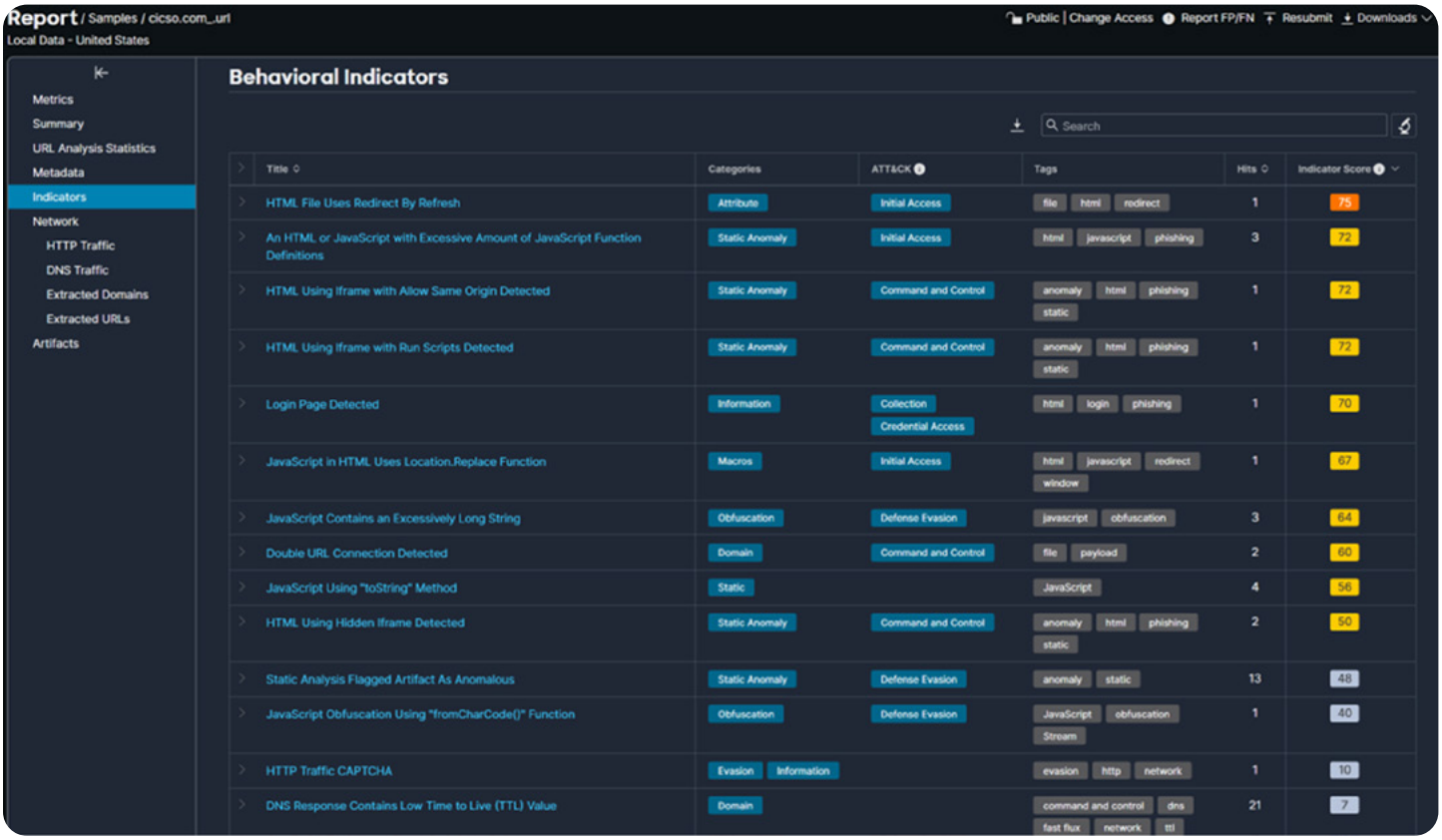
rsac-2026[.]com

rsacthreat-1[.]net

rsacconference[.]com

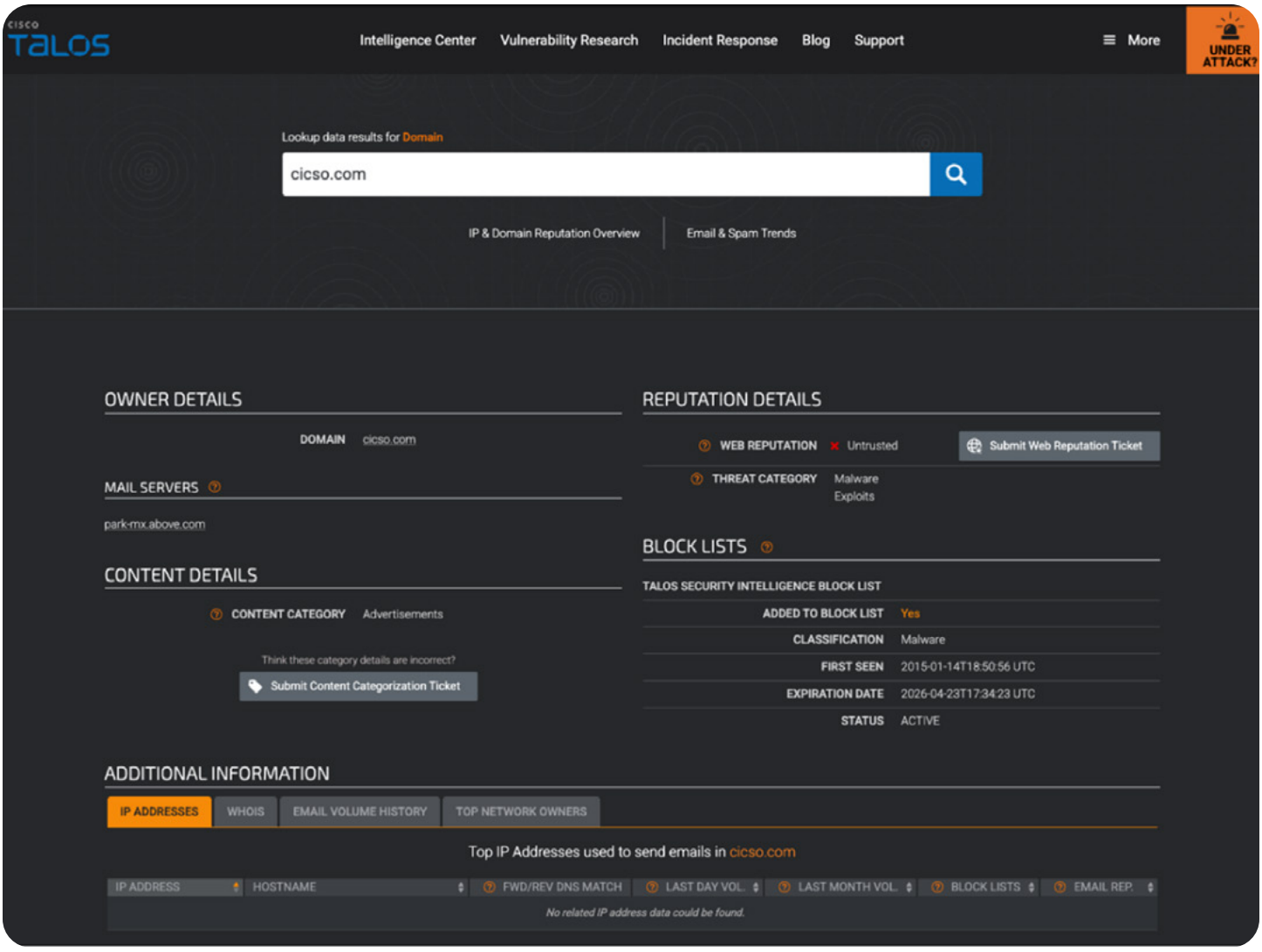


The attack chain involved a series of redirects that ultimately led users to a malicious site offering a deceptive browser plugin.



In response, the SOC collaborated with the Cisco Talos team to facilitate the global denylisting of these malicious domains.

This proactive intervention by the SOC has directly enhanced the security posture of the broader community, providing immediate protection to all organizations globally that leverage Talos Threat Intelligence.



6. Tales of insecurity—case studies

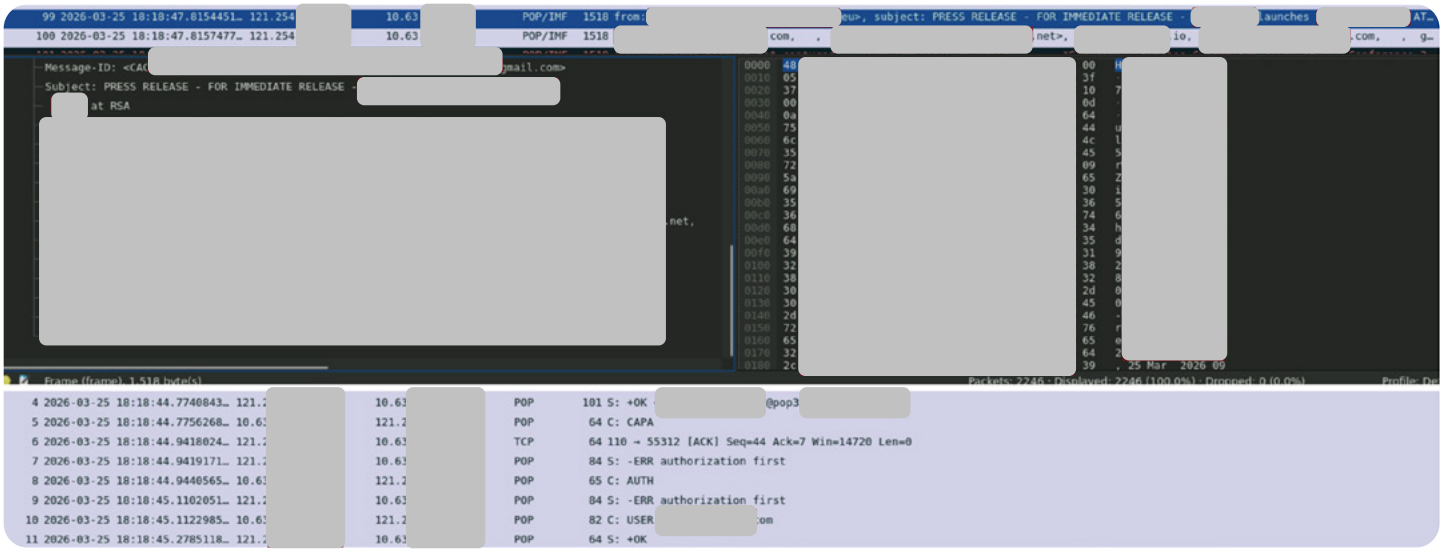
Each of the 10 years the SOC was in operation, we observed instances of accidental data exposure. We investigated these incidents and worked with RSAC to identify and educate the persons/organizations involved.

6.1 Email insecurity

On March 25, 2026, the SOC identified an incident involving the transmission of an unencrypted PDF file via a POP3 mail server. A small security provider distributed marketing materials that were subsequently accessed by a recipient using an insecure email account.

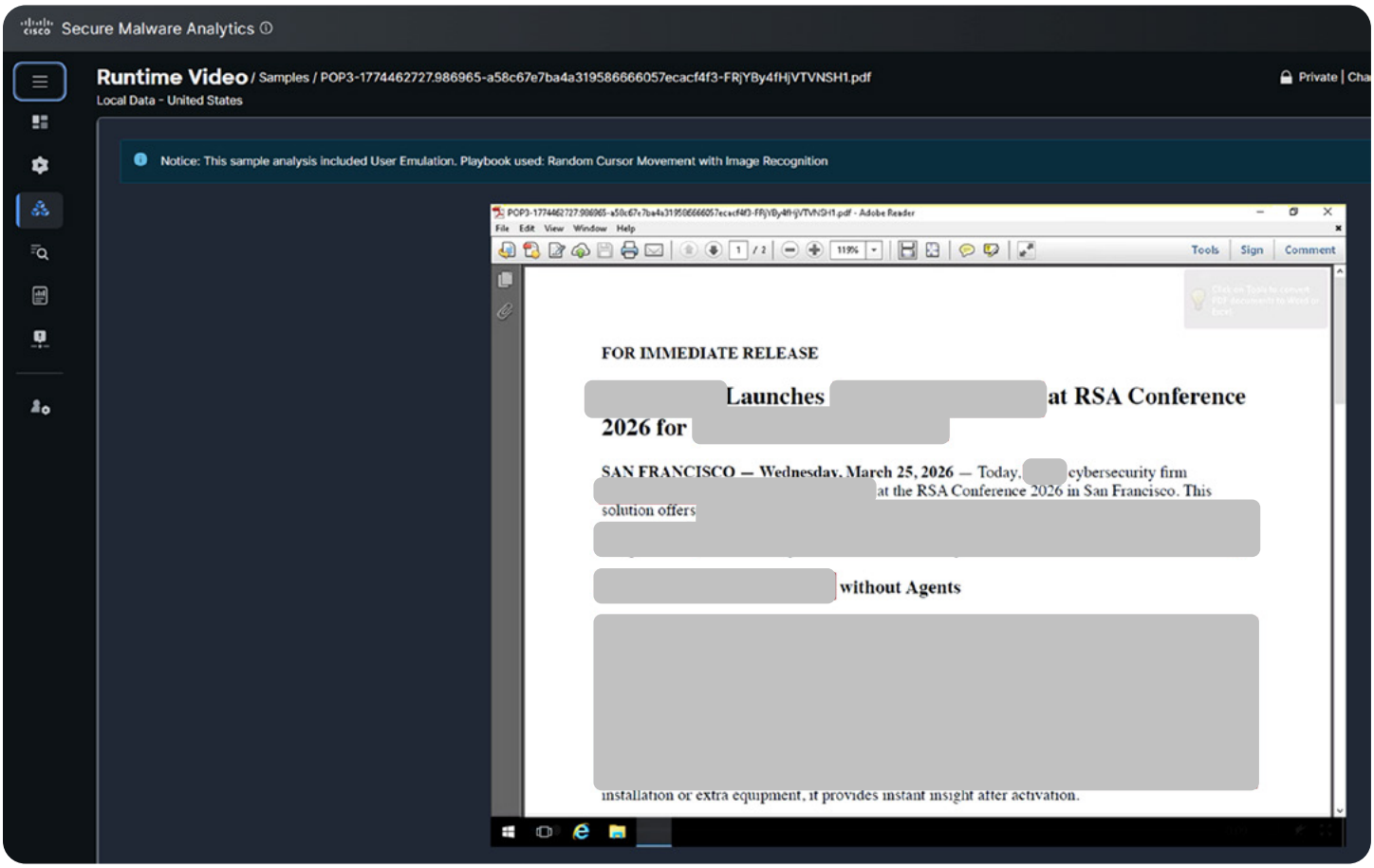
The investigation confirmed that the PDF was downloaded over an unencrypted POP3 session. The SOC team cross-referenced this activity with logs from Splunk, Splunk Attack Analyzer, Secure Malware Analytics and Endace. It was determined that the security provider initiated a public email campaign. Due to the lack of encryption on the recipient's mail server, the content was transmitted in the clear, potentially exposing sensitive information.

The SOC team coordinated with the NOC to locate the security provider and found them on the Expo Hall floor after finding a hashtag that was used for RSAC 2026 about their new product and location also announced on LinkedIn.



The contents of the email distribution were not sent by a blind carbon copy and therefore the other recipients of this Email blast were exposed on the list.

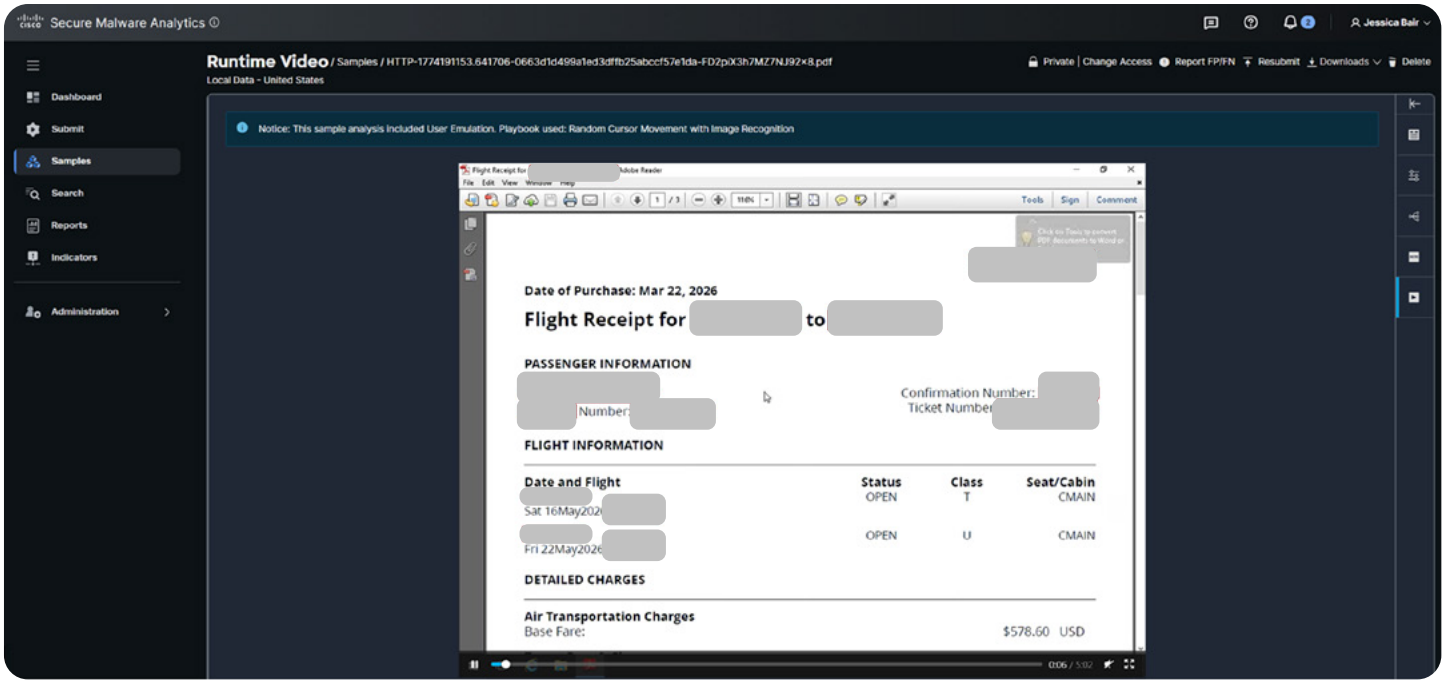
The Senders of this announcement were told to find another way to communicate securely to recipients of this specific domain.



6.2 Web vulnerabilities

On March 21, 2026, a newly onboarded SOC analyst, working their very first day on the job, successfully identified and investigated a data leak involving private expense reports. The seamless integration of ready-to-use SOC capabilities allowed the analyst to immediately jump into the investigation. The incident involved an event production contractor running an unsecured web server to collect employee expenses, which resulted in the exposure of sensitive personal information in cleartext.

Because the HTTP traffic was unencrypted, the SOC team was able to fully reconstruct the files and data sent over the Network, including PDFs, JPGs, names, and company details. If intercepted by malicious actors, this leaked personal and financial information could be weaponized to craft highly convincing spear-phishing lures or to socially engineer access to the victims' travel accounts (such as airline portals).



The incident was escalated through RSAC directly to the CEO of the event production company. Following the escalation, the contractor took immediate action and secured the website that same evening.

The following day, the same new SOC member utilized packet data monitoring to validate the fix, confirming that the unencrypted server is now utilizing SSL encryption for data transport.

[redacted]

Client: [redacted]
Show:
Venue:
Location:
Contact:

Event #(s): [redacted]
Event Dates:

[redacted] Overall Event Labor / Updated Labor Actuals Onsite

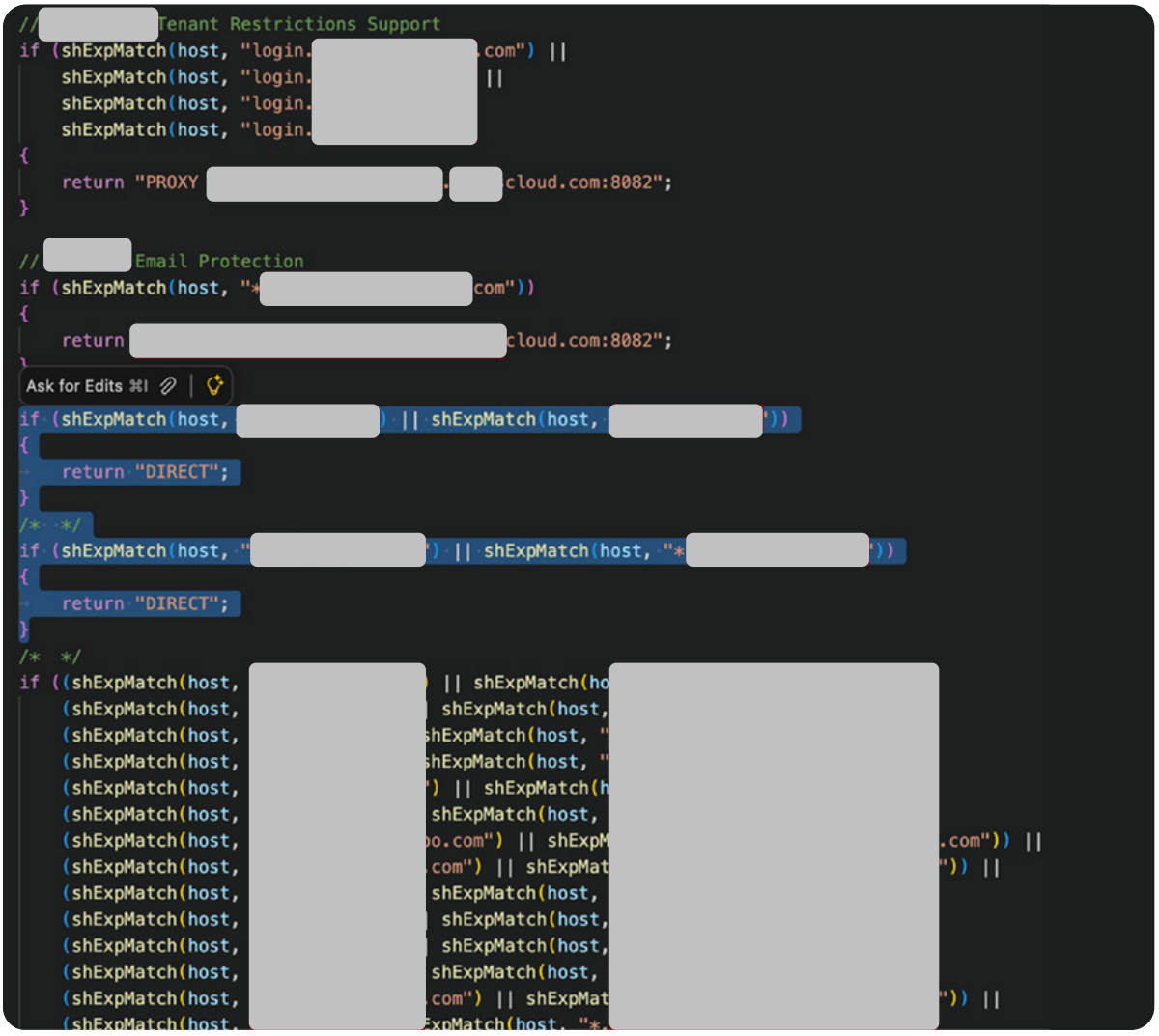
		Price Each	Discount	Discounted Price	Item Total
Event Labor					
Pre-Production Hours					
Digital Signage					
1	Labor	$0.00		$0.00	$0.00
	Account Executive [redacted]				

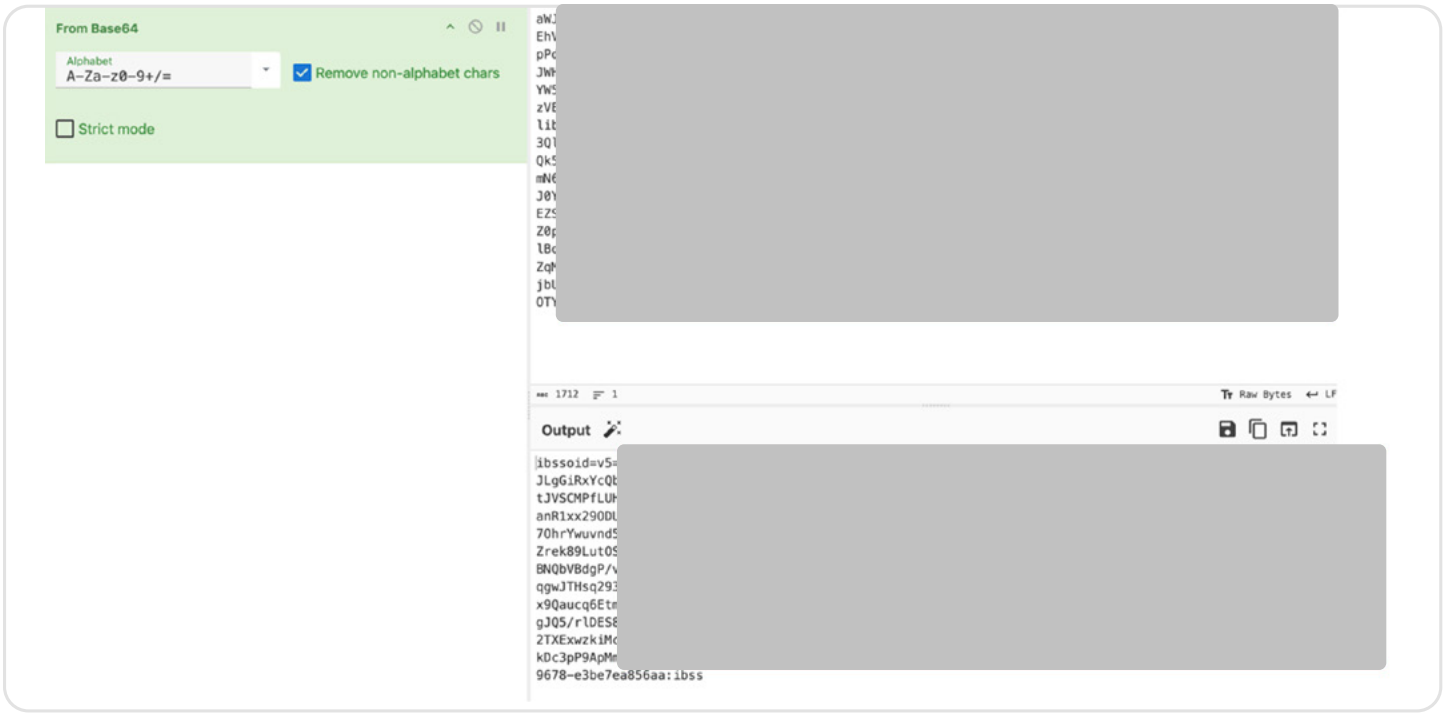
6.3 Zero Trust

To securely connect remote clients, organizations implement cloud SASE/ZTNA. SASE (Secure Access Service Edge) is a cloud-delivered architecture that converges networking and security functions into a single, integrated service. Instead of managing separate tools for connectivity and protection, SASE allows organizations to apply security policies directly at the “edge”—wherever the user or device is located. ZTNA (Zero Trust Network Access) is a security model based on the principle of “never trust, always verify.” Unlike a traditional VPN that often grants broad access to a network once a user is “in,” ZTNA provides granular, application-level access.

The SOC Team observed that an RSAC 2026 attendee’s SASE/ZTNA/Web proxy configuration was configured to permit the transmission of unencrypted traffic. This misconfiguration exposed corporate network data to interception on the Network via insecure HTTP protocols.

Furthermore, the proxy configuration and all internal/external “split tunnel” connections were transmitted in plaintext, which enables unauthorized actors to intercept and potentially compromise sensitive network infrastructure settings in addition to viewing sensitive intellectual property exposed in plaintext over the network connection.





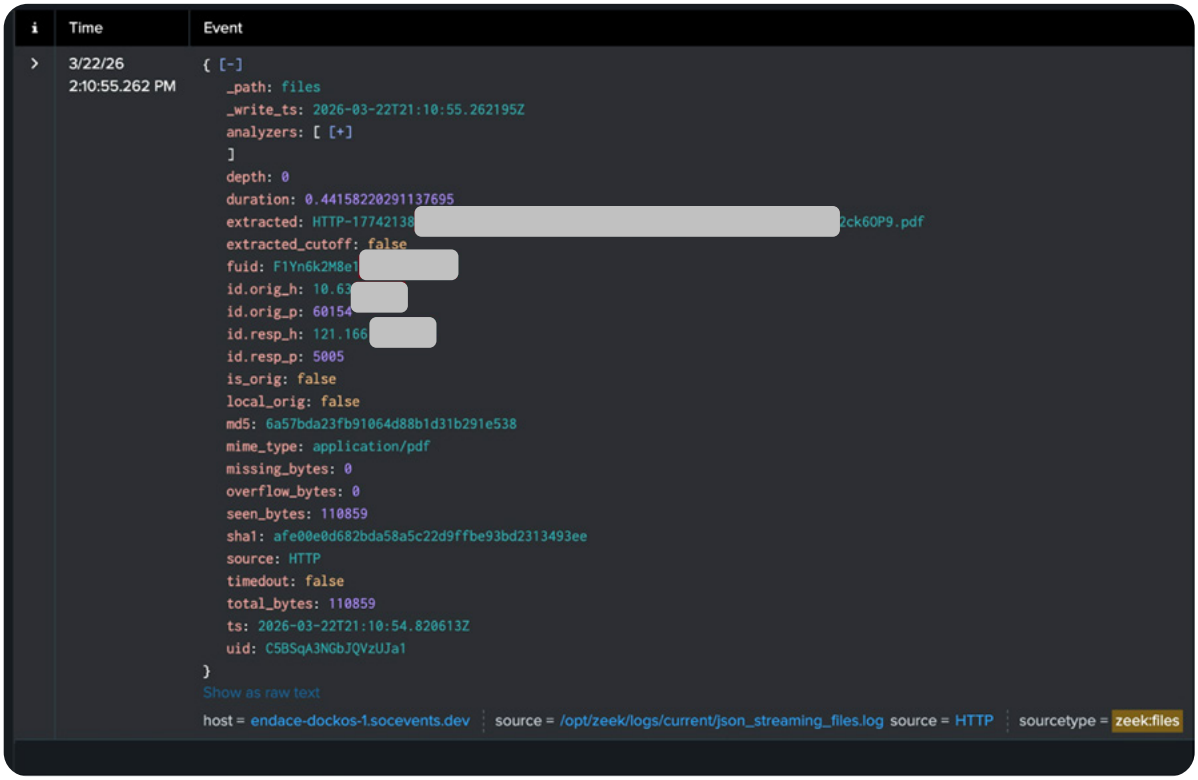
The SOC team confirmed it was not a systemic issue with the proxy provider and provided RSAC with the information to contact the attendee to advise them of this misconfiguration.

6.4 Data leaks

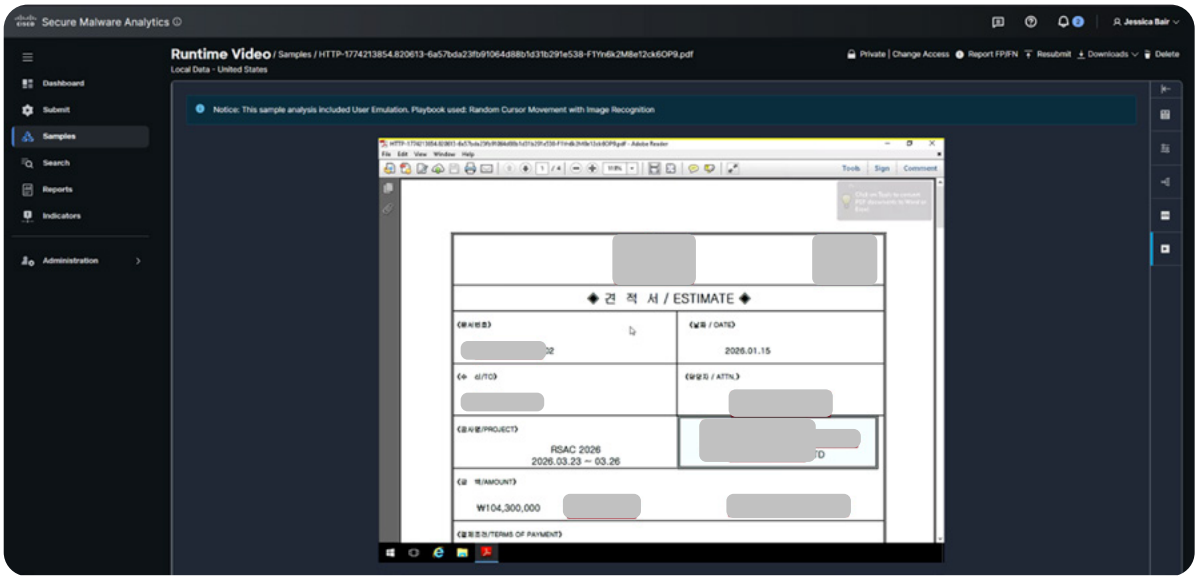
Network Access Storage (NAS) is a convenient method of hosting materials in a file server for access on to go. However, when not configured properly, a NAS can also expose nonpublic business data and put the organization at risk of a bad actor uploading a malicious payload disguised as a legitimate file.

6.5 Contractor billing

The SOC identified sensitive project documentation being transmitted across the network via an insecure protocol. The source was a contractor managed NAS exhibiting significant security deficiencies, specifically regarding the choice of authentication mechanism and a lack of encryption in transport. These vulnerabilities combined allow for the interception of credentials in plaintext during the authentication process. Furthermore, the entire directory, containing three years of business records, was exposed. This configuration also permitted the unauthorized modification or injection of files, posing a risk of device compromise for any users accessing the NAS.

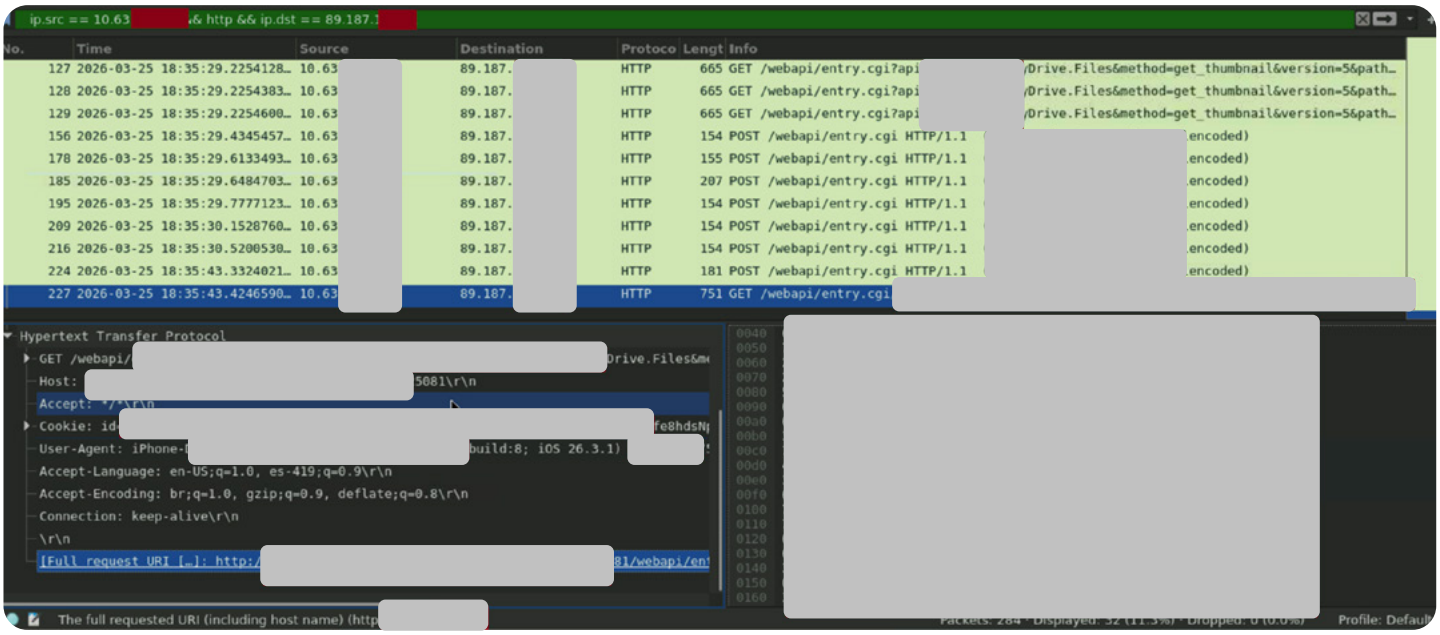


After escalation with RSAC and Moscone NOC, they located the contractor, who was building the booth of a major sponsor. The contractor was advised to secure the NAS, Inspect the NAS for any tampering or attacker activity, and change their password.



Privileged pricing data

The SOC team detected the unencrypted (HTTP) download of a confidential pricing spreadsheet for an RSAC 2026 sponsor by a conference attendee. The file was accessed in the clear from an external NAS URL, exposing sensitive business data to interception.



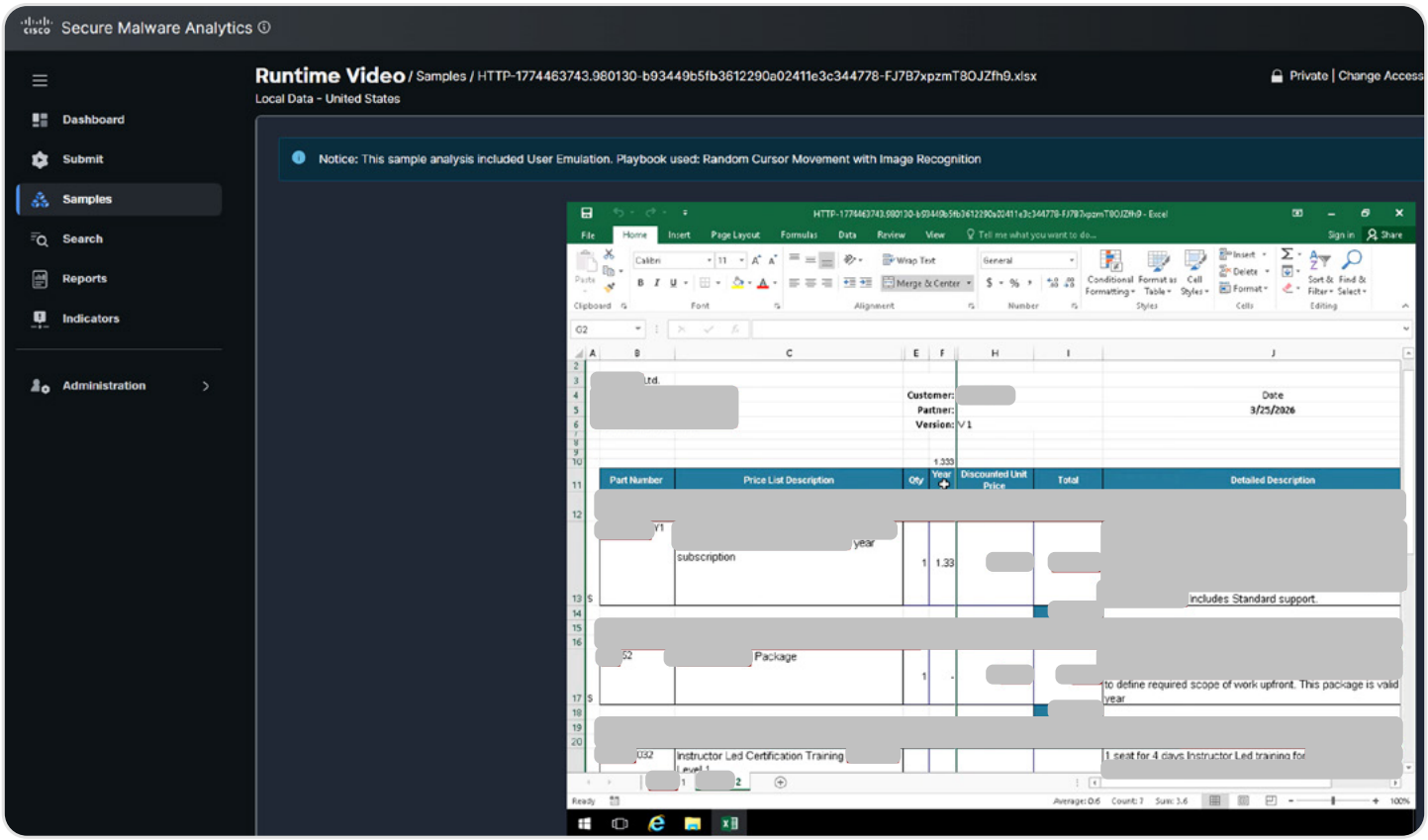
The SOC team utilized Endace/Wireshark, Splunk, and Cisco Secure Malware Analytics to analyze the traffic. Initial analysis confirmed the request originated from an internal endpoint. Files contained the contact information of a security provider of software and services.

The SOC provided RSAC with the information needed to contact the sponsor whose materials were exposed. The RSAC IT Security team met with the sponsor to help them contain the exposure by the services partner.

6.6 AI agent development

During RSAC 2026, the SOC identified an AI Agent demonstration environment utilizing insecure communication protocols. The demo components operated across multiple ports without transport-level encryption, exposing all traffic to potential machine-in-the-middle (MITM) attacks.

The environment leveraged Client Initiated Backend Authentication (CIBA), an OIDC extension; however, the combination of the chosen authentication mechanism and the lack of transport encryption created significant security vulnerabilities. This configuration allowed for potential traffic interception, manipulation, and unauthorized impersonation of the AI agent, enabling an attacker to emulate the agent's permissions.



Furthermore, critical configuration data—including certificate information, IAM details, administrative credentials, and personally identifiable information (PII)—was transmitted in cleartext. This exposure posed a severe risk of unauthorized access and system compromise.

This finding was escalated to the Moscone NOC to ensure the vendor implements appropriate security controls for their demonstration environment.

7. Conclusion

7.1 Summary of security posture

In the 10 years since we deployed the SOC, we observed some incremental progress in the adoption of encryption and secure protocols. However, we saw a small improvement in encrypted network traffic over RSAC 2025, though still stubbornly around 81%.

Our analysis of the data transmitted on the Network reveals a concerning trend: conference attendees are still leaking too much sensitive data. We continue to call for cybersecurity professionals, and those they support, to prioritize robust security measures and prevent unnecessary exposure of critical information that can jeopardize our security.

This year's percentage of encrypted traffic improved by 7 points to 81%. Also, weak encryption declined to 30% of all encrypted traffic. We continue to encourage: Encrypt, encrypt... Never trust, and always verify!

7.2 Recommendations

As threat actors evolve, our industry needs to stay ahead of them, which requires ongoing learning and collaboration amongst teams. The collaboration within the SOC has led to many technical advancements from which attendees can benefit. As AI advances, we can leverage it to analyze large amounts of data and provide a finding and path to remediation, but we always need to ensure that we foster a security mindset in every individual throughout our entire organizations.

Thank you to everyone who attended our session and provided feedback. We appreciate your support. We're looking forward to monitoring the traffic at RSAC 2027 and reporting the results to you. The SOC Team at RSAC Conference is always looking for ways to educate and assist attendees.

- Use a Virtual Private Network
- Use a personal firewall when possible
- Keep your operating system patched
- Check your configuration settings

See you in April 2027!

7.3 Acknowledgments

Thank you to the amazing engineers and analysts who made the SOC possible.

RSAC Conference

Amy Hitchcock, Erik Dierks, Petros Efstathopoulos, Mike DeFronzo and Ryan Jamieson

Moscone Center and Nth Degree

Jeff Hardy, Sean Shanks and John Kodis

SOC Advisor Emeritus: Steve Fink

Cisco staff and report contributors

SOC Leaders: Jessica Oppenheimer and Tony Iacobelli

SOC in a Box hardware: Adi Sankar, with Ryan Maclennan

SOC and XDR Integrations: Ivan Berlinson

Splunk Enterprise Security Integrations: Paul Pelletier and Christian Cloutier, with Nasreddine Bencherchali

Firewall/Security Cloud Control: Adam Kilgore

Incident Response: Richard Marsh and Allison Gallo

Splunk Security/XDR/SMA/SNA: Kevin Wofford, Todd Dow, Jake Ruddy, Erik Dove, Justin Hang and London Eubanks

User Protection Suite/DNS: Steve Vida and Victor Hogarth

Endace staff and report contributors

Endace Management: Cary Wright and Michael Morris

Endace Engineering: Barry Shaw, Erez Birenzwig, Tom Leahy and Kamal Boiri