

Security Operations Center Findings Report from RSAC™ 2025 Conference

Published by Cisco and Endace



Contents

Disclaimer3

The Network4

Technology used in the SOC at RSAC 20254

The Statistics13

Security Incident and Event Management.....18

XDR Integration and Threat Hunting22

Secure Access30

Intrusion Detection with Cisco Secure Firewall37

Tales of Insecurity50

Protecting the SOC Infrastructure54

ThousandEyes57

Conclusion61

Acknowledgments.....62

Disclaimer

It is important to understand the role of the Security Operations Center (“SOC”) at RSAC™ 2025 Conference (“RSAC 2025”).

Note: Cisco® Systems Inc. (“Cisco”) and Endace Limited (“Endace”) used data from the Moscone Center Wireless Network (the “Network”) to provide SOC services.

Note: By connecting to the Network during RSAC 2025, all RSAC 2025 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. ENDACE AND CISCO SYSTEMS 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.).”

Note: Additionally, RSA Conference LLC (“RSAC”) advised attendees of the SOC services in printed materials and onsite signage.

Note: The infrastructure at the event is managed by the Moscone Center, which deploys Cisco Secure Access DNS. The SOC has a SPAN of the network traffic from the Network (named .RSACONFERENCE).

Note: The SOC goal is to protect the conference attendees on the Network and educate RSAC 2025 attendees about what happens on a typical open, unsecured wireless network. The education comes in the form of SOC tours, an RSAC 2025 session, and the publication of the findings in this report (“Findings Report”), issued by sponsors Endace and Cisco.

Note: “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 2025 is an open network offered by the Moscone Center.

Note: 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.

Note: Data collected by the SOC Team at RSAC 2025 remained the property of RSAC and has been destroyed. A certificate of destruction is held by RSAC.

Note: 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.

Note: This Findings Report was prepared as a summary of the SOC services at RSAC 2025, is not to be used as a basis for commercial assessment and is provided “as is.” Endace, Cisco, RSAC nor any of their employees or subcontractors, makes any warranty of any kind, including but not limited to, express or 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. Endace, Cisco, 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. While care has been taken in compiling this Findings Report, it may contain estimates and draft information and may not be current, accurate, or complete.

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

The Network

The Network is a flat network with no host isolation, divided into Moscone South and North Expo Halls and the Moscone West Briefings and 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 attaching 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.

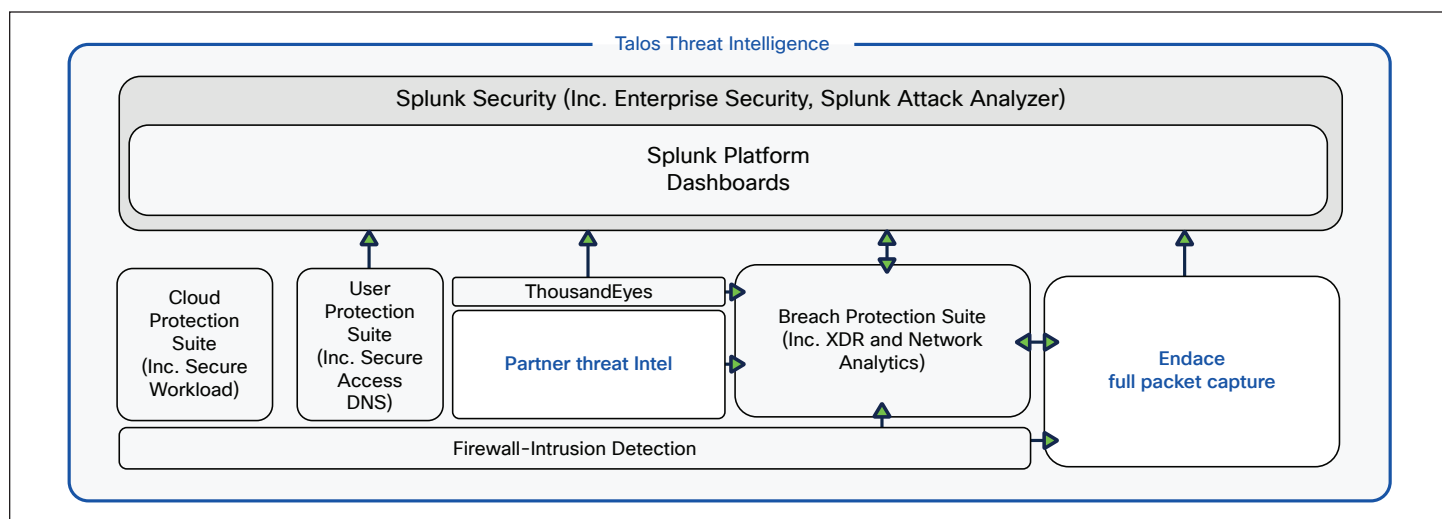
Technology used in the SOC at RSAC 2025

The SOC Team at RSA Conference (RSAC) 2025 deployed the [EndaceProbe™](#) packet capture platform, integrated with the suite of Cisco® tools. Also, Security Operations Center (SOC) engineers used [Cisco Security Cloud](#) in the SOC, comprised of [Cisco Breach Protection Suite](#) and Cisco [User Protection Suite](#), with the foundation of Cisco [Secure Firewall](#).

The Cisco [Cloud Protection Suite](#) was deployed to secure the SOC cloud infrastructure, along with [Cisco Identity Intelligence](#) and Cisco [AI Defense](#).

Incidents were investigated with threat intelligence, provided by [Cisco Talos®](#), and licenses were donated by [alphaMountain](#) and [Pulsedive](#), as well as coming from community sources.

[Endace](#) always-on packet capture was provisioned to record all Network traffic, enabling full investigation of any anomalous behavior. Endace also generated Metadata (including Zeek logs) and NetFlow data into Cisco Secure Network Analytics (SNA) and the Splunk Platform. File content was reconstructed on the fly by Endace, filtered, and streamed to the Splunk Attack Analyzer and Cisco Secure Malware Analytics for sandboxing and analysis.



Workflow integrations to Endace from within [Splunk Enterprise Security](#), Cisco Extended Detection and Response (XDR), Cisco Secure Network Analytics (SNA), and Cisco Secure Firewall, streamlined the work of the SOC team when investigating potential incidents. Endace packet data was used to understand activity before, during, and after any alerts, identify lateral movement, potential command and control (C2), search for Indicators of Compromise (IOCs), and investigate any serious threats that raised the team members' suspicions. No decryption was performed on any network data or connections.



SOC in a Box

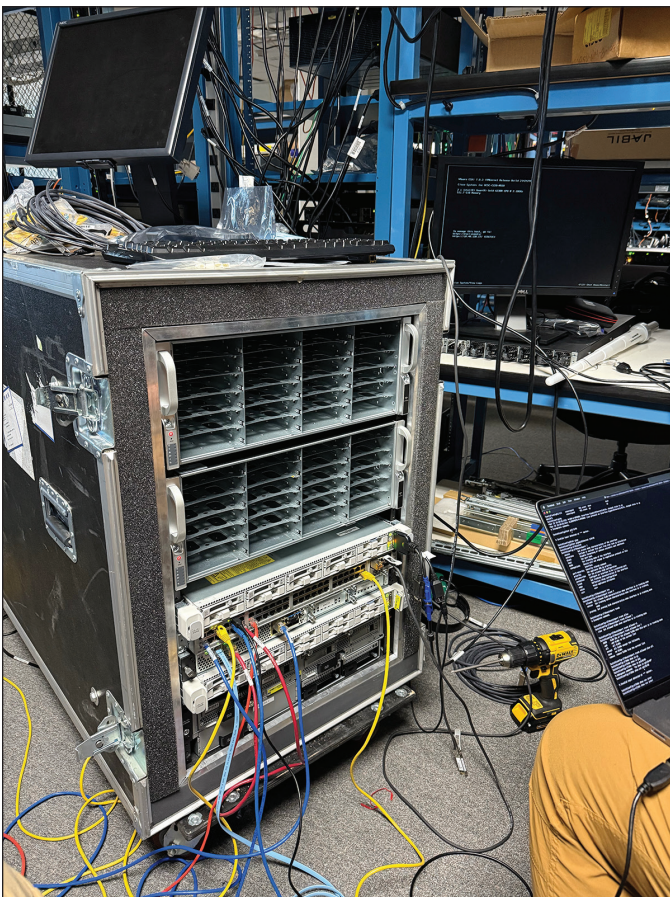
The SOC Team at RSAC 2025 had two-and one-half days to set up the SOC, which meant preparation was imperative. The key to the speed of deployment is what we call a “SOC in a Box,” which is essentially a roadshow case, racked with the required hardware for a full-fledged SOC, that can be closed and shipped to any location. At RSAC 2025, we racked the Endace appliances in the “SOC in a Box.”

This SOC in a Box can be recreated for rapid deployment at other events, natural disaster situations, or even small/ medium businesses who need to upgrade their SOC in a hurry.

Components include:

- 2 x EndaceProbe EP-92C8-G4, each with 432TB Storage
- Switch: Catalyst® 9300 with 10G SFP+ (48 port)
- Firewall: Secure Firewall 4115
- Server: Cisco UCS C220 M5

Below are a couple pictures to show the journey from ideation to the SOC at RSAC 2025, starting with preparation in the Cisco lab and setup in the server section of the SOC.



SOC in a Box was shipped to Moscone Center. Two 10G Small form-Factor Pluggable (SFP) Fiber drops were provided to us for visibility into Network traffic.



The SOC in a Box connected with the Moscone Center Network Operations Center (NOC) and Endace Platform. The SOC was fully operational by Sunday night, April 27.

EndaceProbe Platform

The SOC team at RSAC 2025 utilized EndaceProbe to continuously capture a full and complete record of all traffic transiting the Network gateway, including all north-south and a significant proportion of east-west traffic. A 10G SPAN captured all traffic from Moscone North and South halls, while a second 10G SPAN captured all traffic from Moscone West.

Every single packet that enters or leaves the Network is recorded by EndaceProbe for the full duration of RSAC 2025. This included all DNS traffic to Cisco Secure Access. This historical Network data provided detailed evidence for the SOC team to go back and deeply investigate any event flagged by the other tools in the SOC. EndaceProbe inspects and indexes all the packets and flows to provide rapid search of the Network traffic, through the Endace GUI or via API. Searches were conducted at various layers from L3-L7.



To ensure efficient workflow, we leveraged API integrations between various Cisco security tools and the EndaceProbe packet search to speed up the time to do a deep packet level investigation. Built-in analytics tools within the Endace GUI allowed the SOC team to quickly gain a deep understanding of the traffic and content flowing across the Network including:

- Real-time views of the Network traffic charted real time up to L7.
- Historical, filtered views of traffic, displaying insights such as application breakdowns, top talkers, traffic patterns, conversation views, Chord diagram, etc.
- Fast packet search using intuitive L2-7 filters helped the analysts get to the packets of interest quickly and easily.
- Built-in decodes, using Wireshark hosted within EndaceProbe, for deep analysis of the Network packets.
- File and log reconstruction for content sent across the Network using the built-in Endace file extraction capability. This was useful when investigating suspicious content flowing across the Network.

The SOC team utilized the built-in Hypervisor within the EndaceProbe platform to host other tools. Hosted on EndaceProbe were the following tools:

- A virtual Cisco Secure Network Analytics (SNA) Sensor analyzing all Network traffic and feeding metadata to SNA.
- Zeek opensource sensor analyzing traffic in real time and continuously feeding logs to a custom Splunk dashboard, providing real-time charts and searchable metadata.

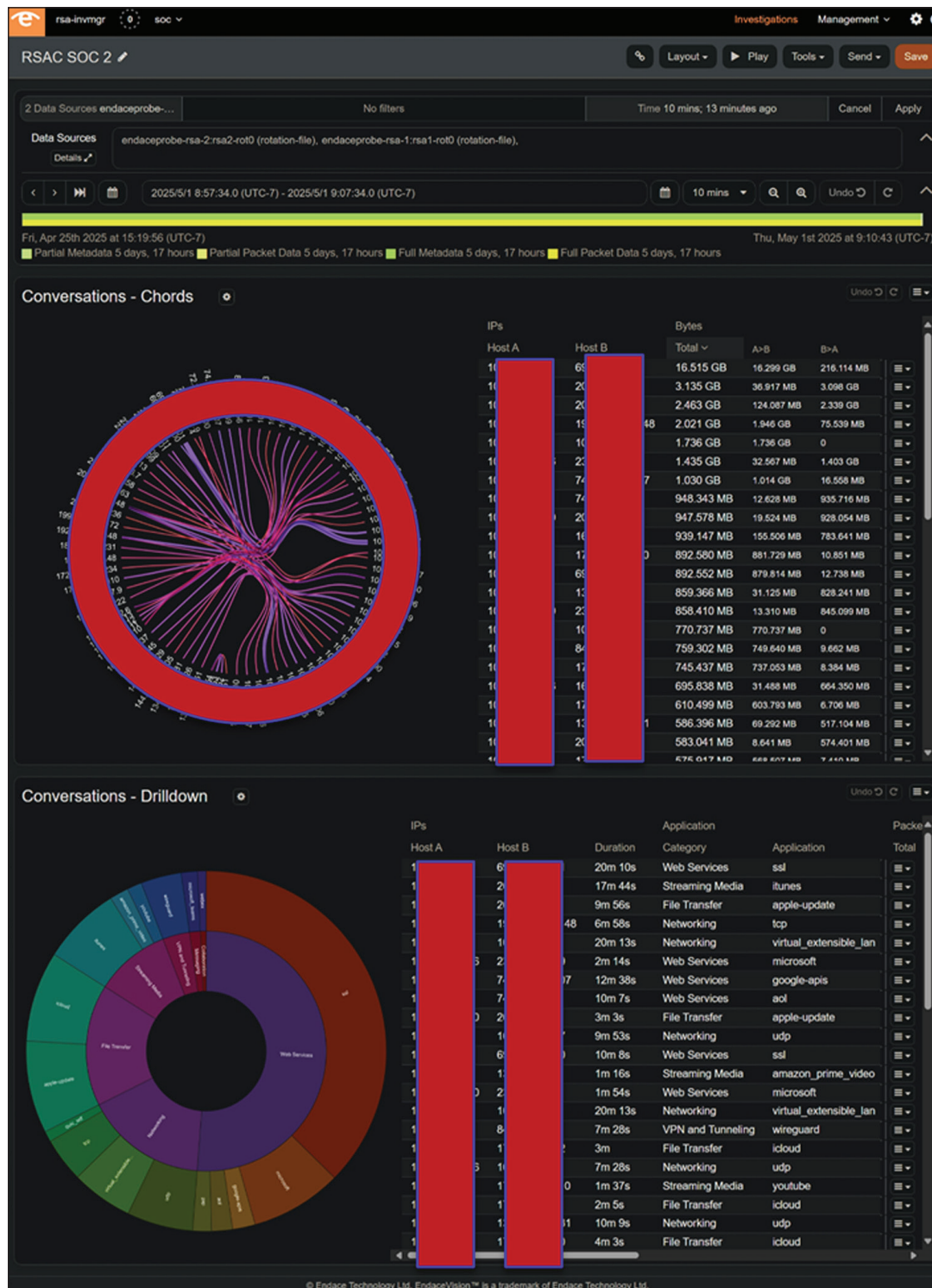
- Real-time file reconstruction, extracting thousands of files from packet streams. Files were submitted to Splunk Attack Analyzer and Cisco Secure Malware Analytics for analysis.
- A variety of other open source and commercial tools used on demand.

The SOC Team at RSAC 2025 utilizes all the capabilities above to create a comprehensive “story” about what is happening on the Network.

A continuously updating Endace dashboard provided a top-level view of all traffic over the entire duration of RSAC 2025.



A more detailed view of the last 10 minutes provided a summary of top Network talkers via a Conversations chords chart that provided a visual representation of who was talking with whom. A Conversations drilldown provided a view of the top applications and protocol stacks seen on the Network. These views were updated continuously during the duration of the conference.



When analysts needed to investigate down to the packet level, they used Wireshark, which is hosted within the EndaceProbe platform. Wireshark allowed analysts to do things like view transactions including logins that should have been encrypted; understand port scanning, beaconing, and potential C2 communications; observe Common Vulnerabilities and Exposures (CVEs) being exploited; and reconstruct voice or video media streams from captured packets.

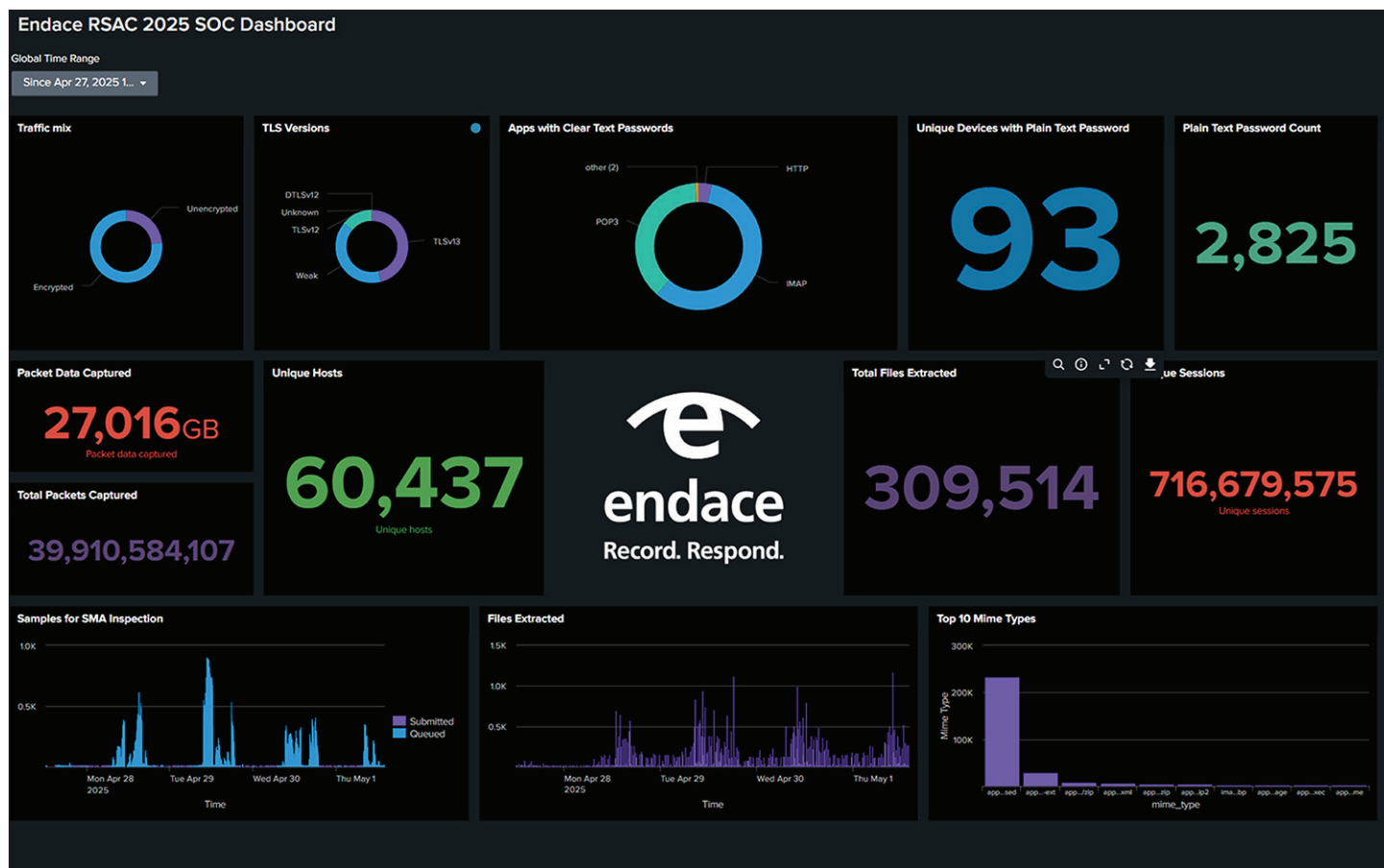
The screenshot displays the Wireshark interface for a packet capture named "wireshark_RSAC-SOC-2_aa50a133-c135-4986-a67d-eea72c9e5c5c.pcap". The main pane shows a list of 49 packets. The selected packet (No. 1) is expanded, showing the following details:

- Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface
- Extensible Record Format
- Ethernet II, Src: IETF-VRRP-VRID_01 (00:00:5e:00:01:01), Dst: 82:c9:c9:5a:03:00
- Internet Protocol Version 4, Src: [redacted], Dst: 82:c9:c9:5a:03:00
- Transmission Control Protocol, Src Port: 443, Dst Port: 62487, Seq: 1, Ack: 1

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000 82 c9 c9 5a 03 0a 00 00 5e 00 01 01 08 00 45 00  ...Z....~....E-
0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  4b @ / - go og - ?
0020 fe 00 00 00 00 00 00 00 00 00 00 00 00 00 00  h P f #
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  . . . . . q . l . 72
0040 ab 22 11 61 83 49  ...* a I
```


New for RSAC 2025 was an Endace Splunk dashboard, created to aggregate important information derived from the traffic, including encryption strength and insecure sessions, which clarified the overall security of the users of the Network. With this dashboard, we were able to see how information was flowing through our SOC security stack and have a summary of how secure or insecure our user base was.



The Statistics

Statistics are always a popular part of the SOC Tours and this Findings Report. Below are the stats from this year and the post-pandemic conferences.

Year over Year

| Year | 2025 (Endace) | 2024 (NetWitness) | 2023 (NetWitness) | 2022 (NetWitness) |
|---|---|-------------------|-------------------|-------------------|
| Attendees (RSAC) | 43,500+ | 41,700+ | ~39,000 | ~19,000 |
| Total packets captured (Endace) | 45.3 billion | 19 billion | 18.5 billion | 11.8 billion |
| Total logs captured (Splunk) | 930 million (Zeek logs added) | 39.9 million* | 214.7million | 108 million |
| Total unique devices (Cisco) | 22,701 | 17,034 | ~40k | 13,253 |
| Total packets written to disk (Endace) | 36.6 terabytes | 17.24 terabytes | 16.26 terabytes | 7.39 terabytes |
| Total logs written to cloud (Splunk) | 193 gigabytes | 79 gigabytes | 774 gigabytes | 50.8 gigabytes |
| Peak bandwidth utilization (Endace) | 3.3 Gbps | 2.2 Gbps | 1.8 Gbps | 1.35 Gbps |
| DNS Requests (Cisco) | ~64.8 million | ~56.3 million | ~53.4 million | ~46 million |
| Total clear text username/passwords (Endace) | 2,825 | 20,916 | 36,910 | 55,525 |
| Unique devices/accounts with clear text usernames/passwords (Endace) | 93 | 99 | 424 | 2,210 |
| Files sent for malware analysis (Endace) | 309,514 file objects reconstructed by Endace. 27,000 sent to SAA*** 7,500 sent to SMA | ~50** | 7,500+ | 570+ |

* In past years at RSAC Conference the SOC team stands up the entire SOC in 1-1/2 days. During RSAC 2024, the logs from the Cisco Firewall Intrusion Detection System were not integrated into the NetWitness Security Information and Event Management (SIEM); 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.

The Data, by Endace

The SOC Team at RSAC 2025 started analyzing all wireless traffic on Monday, April 28, and collected traffic through Thursday, May 1, 2025, at 3 p.m.

We observed a doubling of the amount of network traffic collected from RSAC 2024, 36.6TB vs 17TB in 2024, reflecting an increase in the traffic per device connected to the Network and an increase in the number of devices on the Network. There were 716 million Layer 4 sessions during this period, almost double what was seen in 2023 when we measured 383 million Layer 4 sessions.

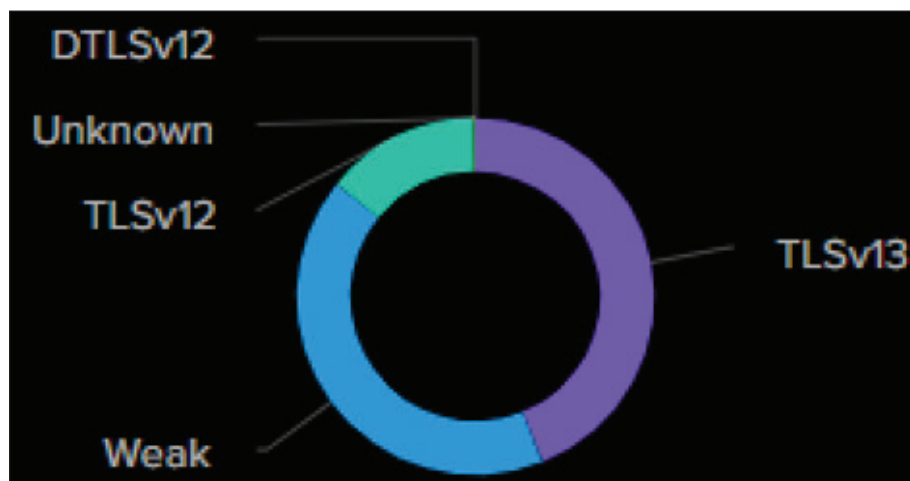
Encrypted vs. Unencrypted

Encryption of traffic is relevant because of the amount of non-public information that is revealed by RSAC Conference attendees. Unencrypted traffic presents several threats to both individuals and organizations. A company or person does not need the Endace platform, Cisco Secure Firewall, or Cisco Malware Analytics to view unencrypted traffic, because any attendee, with the help of a quick internet search, can collect a subset of this data on a personal device. Endace and Cisco technologies enable the SOC Team at RSAC 2025 to collect all the data and easily analyze the top threat categories, as well as understand if any of those threats are visible to other attendees.

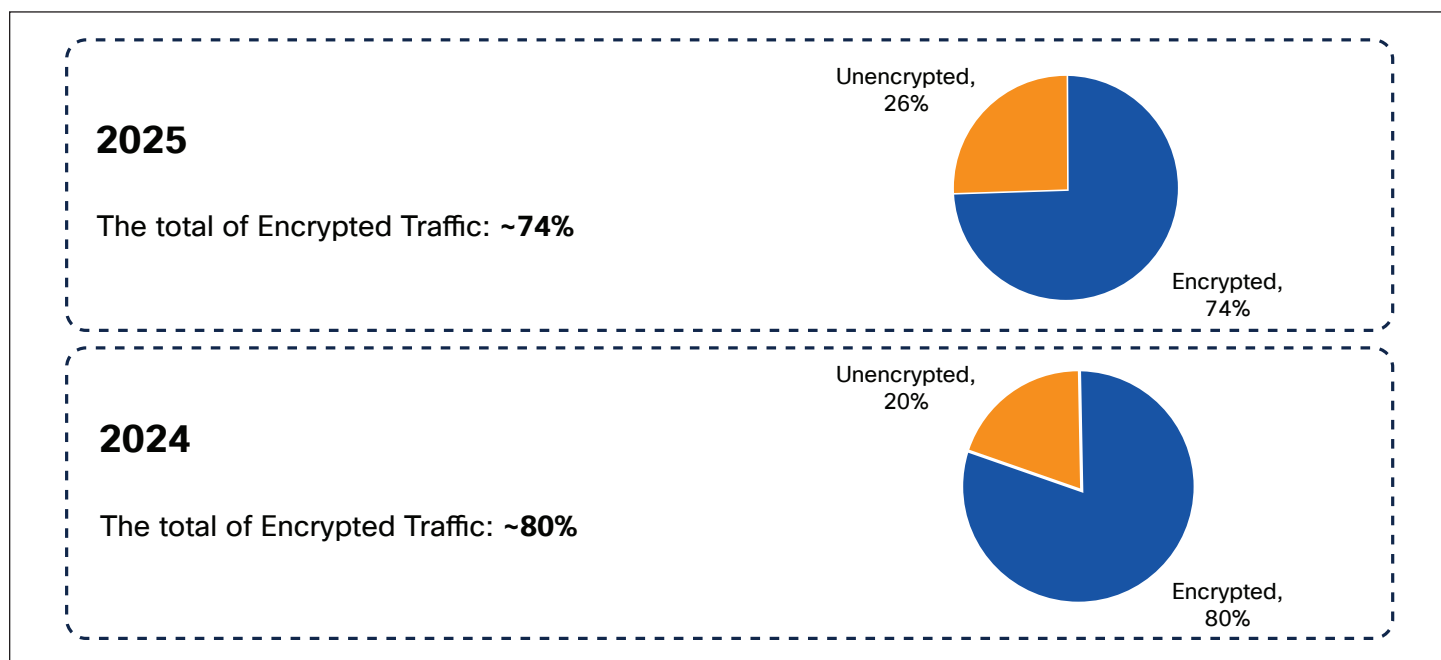
The SOC Team at RSAC Conference **does not** decrypt/terminate or man-in-the-middle encrypted traffic. The primary goal of the SOC is to educate attendees on how to better secure their data through encryption.

Think of this as north-south and east-west. Encrypting traffic does not necessarily make one more secure, but it does stop individuals from giving away their credentials, and organizations from giving away corporate asset information in the clear.

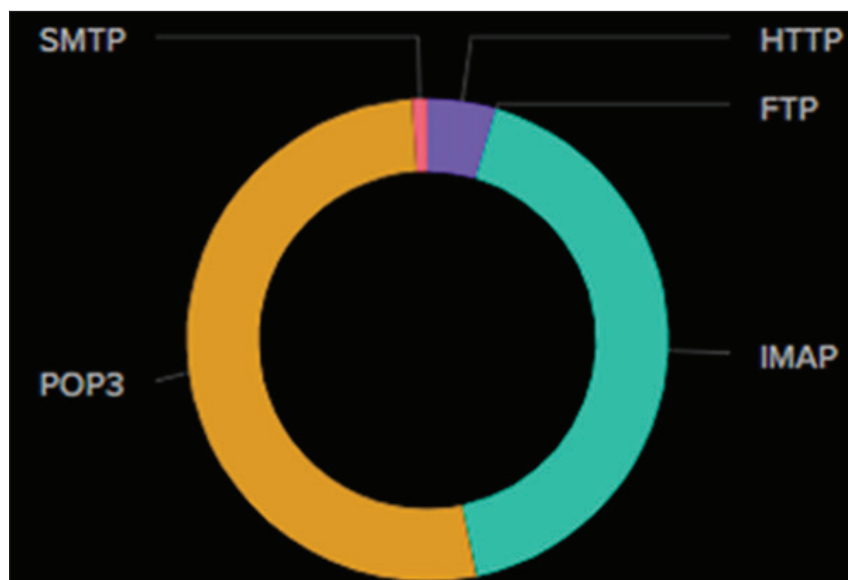
This year was the first time we reported the strength of encryption used across the Network. Surprisingly, we found the percentage of weak encryption increased to 40% this year, when we would expect weak encryption to decline in popularity. Weak is classified as Transport Layer Security (TLS) 1.1 or TLS 1.0 encryption, which are both prone to brute force decryption where compute resources are used to systematically attempt to decrypt sensitive information. By now all systems should have deprecated weak TLS encryption in favor of TLS 1.2 or 1.3.



Even more concerning, we saw an increase in the amount of un-encrypted traffic, with an increase to 26% by the end of the day April 30, up from 20% during RSAC 2024. Surprisingly we saw the encrypted traffic increase back up Thursday, potentially indicating that some insecure services were remediated.



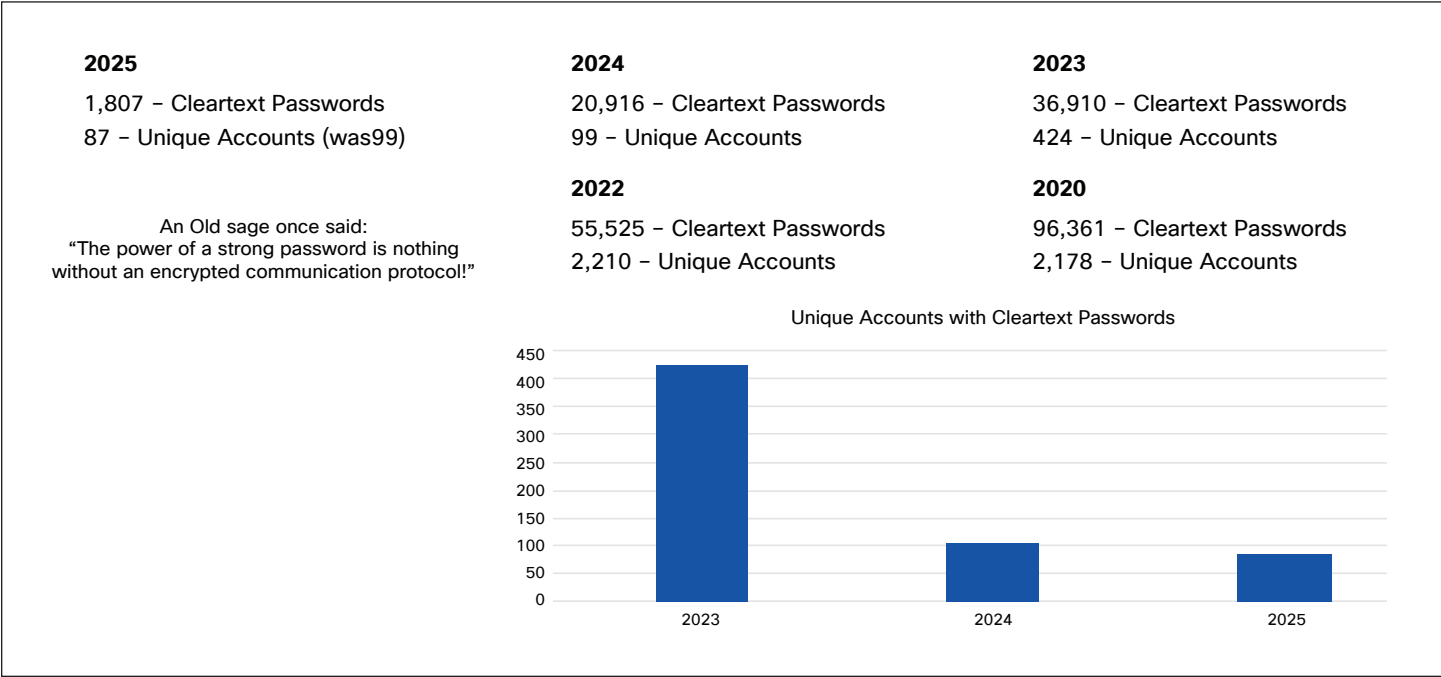
Analyzing un-encrypted traffic showed us that the majority was unsecured email using Post Office Protocol version 3 (POP3), Internet Message Access Protocol (IMAP), and Simple Mail Transfer Protocol (SMTP). In some cases, these email sessions carried sensitive information such as product plans; in other 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.



Unsecured HTTP was also evident in the unencrypted traffic stream, including login pages. Where possible, the SOC team at RSAC 2025 tracked down users of these websites to help better secure their environments and applications.

Cleartext Usernames and Passwords

Cleartext usernames and passwords continued to be observed on the Network. The number of clear text credentials has declined year over year, and we will work to educate users, working to zero.



See the **Tales of Insecurity** later in this report, for some examples of investigations and remediation/attendee education.

Cisco XDR formed a central hub for prioritizing, understanding, and investigating incidents. This year we could make extensive use of tight integration with EndaceProbe for investigations, including alerting the SOC Team when passwords were observed in the clear on the Network.

The screenshot displays the Cisco XDR Incidents dashboard. The top navigation bar includes the Cisco XDR logo, user profile (Jessica Bair Oppen...), and notification icons. The left sidebar contains navigation links: Control Center, Incidents (selected), Investigate, Intelligence, Automate, Assets, Client Management, and Administration. The main content area shows a summary of incidents: 261 total, 101 new, 30 open, and 120 unassigned. Below this is a search bar with filters for 'Endace', 'Last 30 days', 'Hide closed incidents', and 'Filters'. A table lists incidents with columns: Priority, Name, Sources, Created, Assigned, and Status. The table shows several incidents related to 'Password found' detections involving various assets and users.

| Priority | Name | Sources | Created | Assigned | Status |
|----------|--|---------|--------------------------|------------|---------------------|
| 540 | Incident initiated by a "Password found for user admin" detection involving the Asset 10.63.1.1 | Endace | 2025-05-01T18:40:20.160Z | Unassigned | New |
| 540 | Incident initiated by a "Password found for user" detection involving the Asset 10.63.1.1 | Endace | 2025-05-01T18:20:23.078Z | Unassigned | New |
| 540 | Incident initiated by a "Password found for user 10.63.1.1" detection involving the Asset 10.63.1.1 | Endace | 2025-05-01T17:05:23.332Z | Unassigned | New |
| 540 | Incident initiated by a "Password found" - 10.63.1.1 | Endace | 2025-04-30T22:10:24.733Z | IB | Open: Investigating |
| 540 | Incident initiated by a "Password found for user" - RMA system | Endace | 2025-04-30T22:00:32.630Z | IB | Open: Reported |
| 540 | Incident initiated by a "Password found for user" - Company | Endace | 2025-04-30T20:25:21.551Z | IB | Open: Investigating |
| 540 | Incident initiated by a "Password found for user" - detection involving the Asset 10.63.1.1 - Developer API portal | Endace | 2025-04-30T17:40:20.423Z | IB | Open: Investigating |
| 540 | Incident initiated by a "Password found" detection involving the Asset 10.65.1.1 (security) | Endace | 2025-04-29T21:30:24.148Z | IB | Open: Investigating |
| 540 | Incident initiated by a "Password found for user" - detection involving the Asset 10.65.1.1 (account) | Endace | 2025-04-29T20:10:19.555Z | IB | Open: Investigating |
| 540 | Incident initiated by a "Password found" detection involving the Asset 10.63.1.1 | Endace | 2025-04-29T16:50:15.797Z | IB | Open: Investigating |
| 540 | Incident initiated by a "Password found" detection involving the Asset 10.63.1.1 | Endace | 2025-04-29T16:05:13.119Z | IB | Open: Reported |
| 540 | Incident initiated by a "Password found" detection involving the Asset 10.63.1.1 (Private Company) | Endace | 2025-04-29T16:04:54.693Z | IB | Open: Investigating |

Within Cisco XDR analysts could open an Incident, and right-click on the IP to pivot into Endace to investigate further, generating an incident response report as appropriate. Learn more about the integration with Splunk in the next section.

The screenshot displays the Cisco XDR Incidents dashboard with a detailed view of an incident. The top navigation bar includes the Cisco XDR logo, user profile (Jessica Bair Oppen...), and notification icons. The left sidebar contains navigation links: Control Center, Incidents (selected), Investigate, Intelligence, Automate, Assets, Client Management, and Administration. The main content area shows a summary of incidents: 261 total, 101 new, 30 open, and 120 unassigned. Below this is a search bar with filters for 'Endace', 'Last 30 days', 'Hide closed incidents', and 'Filters'. A table lists incidents with columns: Priority, Name, Sources, Created, Assigned, and Status. The table shows several incidents related to 'Password found' detections involving various assets and users.

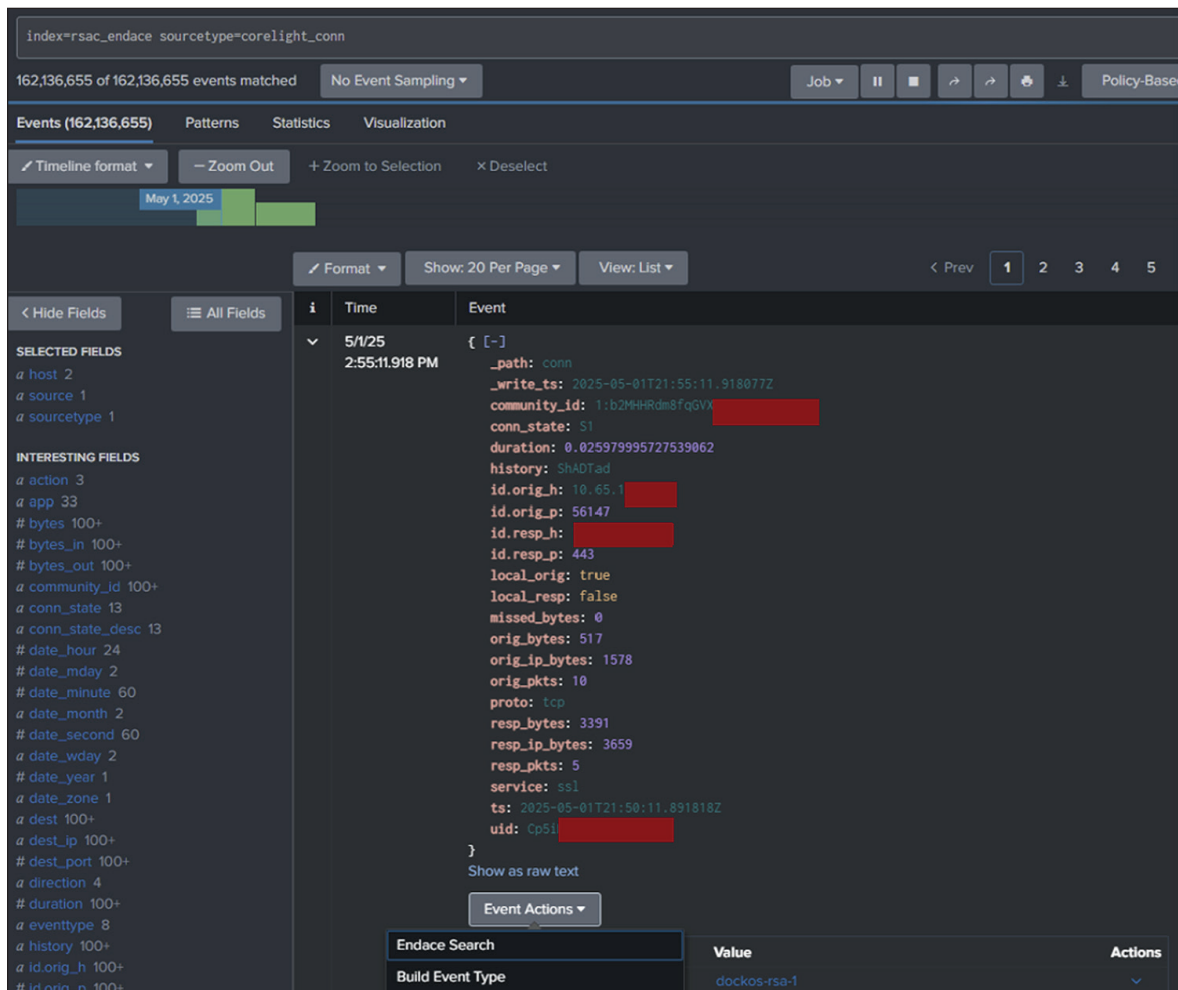
| Priority | Name | Sources | Created | Assigned | Status |
|----------|--|---------|--------------------------|------------|---------------------|
| 540 | Incident initiated by a "Password found for user admin" detection involving the Asset 10.63.1.1 | Endace | 2025-05-01T18:40:20.160Z | Unassigned | New |
| 540 | Incident initiated by a "Password found for user" detection involving the Asset 10.63.1.1 | Endace | 2025-05-01T18:20:23.078Z | Unassigned | New |
| 540 | Incident initiated by a "Password found for user 10.63.1.1" detection involving the Asset 10.63.1.1 | Endace | 2025-05-01T17:05:23.332Z | Unassigned | New |
| 540 | Incident initiated by a "Password found" - 10.63.1.1 | Endace | 2025-04-30T22:10:24.733Z | IB | Open: Investigating |
| 540 | Incident initiated by a "Password found for user" - RMA system | Endace | 2025-04-30T22:00:32.630Z | IB | Open: Reported |
| 540 | Incident initiated by a "Password found for user" - Company | Endace | 2025-04-30T20:25:21.551Z | IB | Open: Investigating |
| 540 | Incident initiated by a "Password found for user" - detection involving the Asset 10.63.1.1 - Developer API portal | Endace | 2025-04-30T17:40:20.423Z | IB | Open: Investigating |
| 540 | Incident initiated by a "Password found" detection involving the Asset 10.65.1.1 (security) | Endace | 2025-04-29T21:30:24.148Z | IB | Open: Investigating |
| 540 | Incident initiated by a "Password found for user" - detection involving the Asset 10.65.1.1 (account) | Endace | 2025-04-29T20:10:19.555Z | IB | Open: Investigating |
| 540 | Incident initiated by a "Password found" detection involving the Asset 10.63.1.1 | Endace | 2025-04-29T16:50:15.797Z | IB | Open: Investigating |
| 540 | Incident initiated by a "Password found" detection involving the Asset 10.63.1.1 | Endace | 2025-04-29T16:05:13.119Z | IB | Open: Reported |
| 540 | Incident initiated by a "Password found" detection involving the Asset 10.63.1.1 (Private Company) | Endace | 2025-04-29T16:04:54.693Z | IB | Open: Investigating |

Security Incident and Event Management

To make our threat hunters' lives richer with more context from Cisco and Endace tools, we brought in Splunk Enterprise Security at the SOC to ingest detections from Endace Probe, Cisco XDR, Secure Malware Analytics, Umbrella, and Secure Firewall and to visualize them into functional dashboards for executive reporting.

Endace and Splunk

This year we had the opportunity to deploy the Endace Splunk App integration, providing a powerful search integration, which we used extensively to validate our findings with the Firewall.



The screenshot displays the Splunk Enterprise Security interface. At the top, the search bar contains the query `index=rsac_endace sourcetype=corelight_conn`. Below the search bar, a status bar indicates "162,136,655 of 162,136,655 events matched" and "No Event Sampling" is selected. The interface shows a timeline view for May 1, 2025, with a zoomed-in view of a specific event.

The event details are as follows:

| Time | Event |
|--------------------------|--|
| 5/1/25 2:55:11.918 PM | <pre>{ [-] _path: conn _write_ts: 2025-05-01T21:55:11.918077Z community_id: 1:b2HHRdm8fqGVX conn_state: S1 duration: 0.025979995727539062 history: ShADTad id.orig_h: 10.65.1 id.orig_p: 56147 id.resp_h: id.resp_p: 443 local_orig: true local_resp: false missed_bytes: 0 orig_bytes: 517 orig_ip_bytes: 1578 orig_pkts: 10 proto: tcp resp_bytes: 3391 resp_ip_bytes: 3659 resp_pkts: 5 service: ssl ts: 2025-05-01T21:50:11.891818Z uid: Cp5i }</pre> |

Below the event details, there is a section for "Event Actions" and a table for "Endace Search" and "Build Event Type".

| Endace Search | Value | Actions |
|------------------|--------------|---------|
| Build Event Type | dockos-rsa-1 | |

Using Splunk's summary search feature, 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.

This powerful aggregation provided us with immediate, actionable insights into Network activity and security threats that were observed in the Network. In a production environment, the attacks would have been blocked and/or investigated.

Splunk Enterprise Security and Cisco Security

The Splunk Cloud instance was configured with the following integrations:

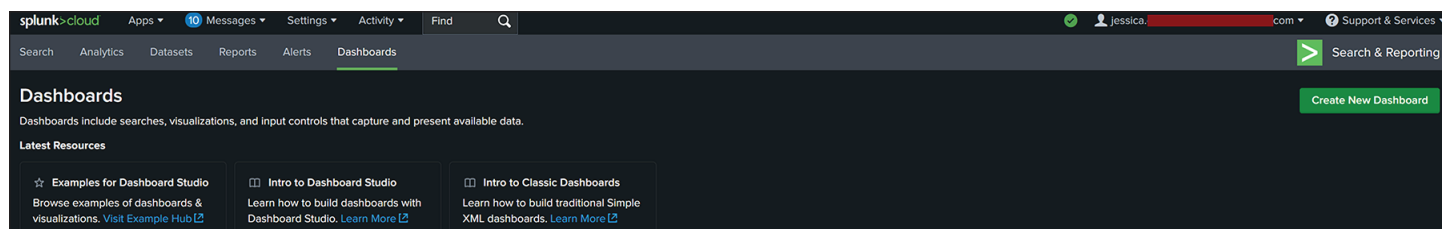
1. [Cisco Security Cloud](#) app
 - Cisco XDR
 - Cisco Secure Firewall
 - Cisco Secure Network Analytics
 - Cisco Secure Malware Analytics
 - Cisco Multicloud Defense
2. Cisco Umbrella®, using the [Cisco Cloud Security App for Splunk](#)
3. Cisco ThousandEyes, using the Splunk HTTP Event Collector (HEC)
4. Cisco Talos Intelligence for Enterprise Security
5. Zeek logs from Endace probes via Splunk Universal Forwarder
6. Syslog logs from appliances via Splunk Heavy Forwarder



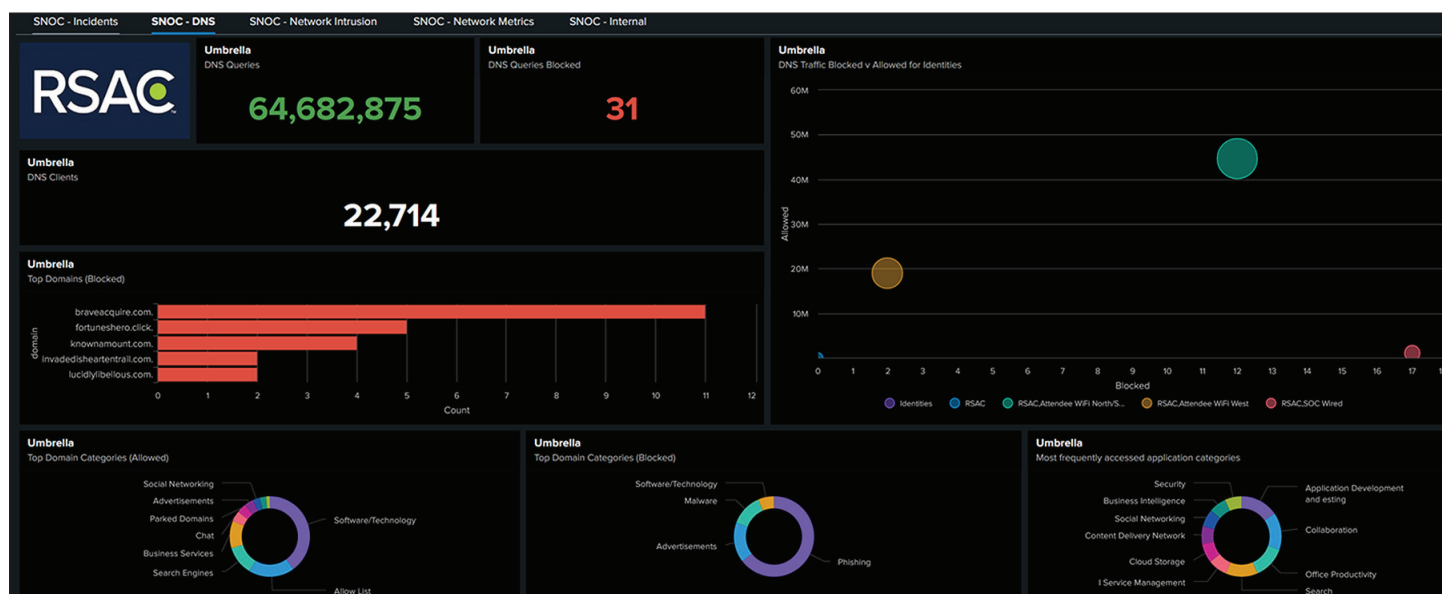
| Name | Actions | Token Value | Source Type | Index | Status |
|--------------------|-------------------------------|-------------|---------------------------|--------------------------|---------|
| CCI_HEC | Edit Disable Delete Copy Show | ***** | | cisco_cii | Enabled |
| CII | Edit Disable Delete Copy Show | ***** | cisco:cii | cisco_cii | Enabled |
| MCD | Edit Disable Delete Copy Show | ***** | cisco:multicloud:defense | cisco_multicloud_defense | Enabled |
| rsac_cisco_sna | Edit Disable Delete Copy Show | ***** | | rsac_cisco_sna | Enabled |
| ThousandEyes | Edit Disable Delete Copy Show | ***** | | thousandeyes_metrics | Enabled |
| xdr_full_incidents | Edit Disable Delete Copy Show | ***** | cisco_xdr_custom | rsac_xdr_full | Enabled |
| xdr_incident_stats | Edit Disable Delete Copy Show | ***** | cisco_xdr_incidents_stats | rsac_cisco_xdr_stats | Enabled |

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](#) to ensure efficient and secure transport of the data. That made data searches for our threat hunters cleaner. Searching for data is where Splunk shines! You begin by simply navigating to **Apps > Search and Reporting** and typing your search query. You do need to know the [Splunk Search Processing Language \(SPL\)](#) to build your queries, but that is just a [quick tutorial](#) away.

The **Visualization** tab allows a user to quickly convert this data into a visual format for previewing. Those search queries were then aggregated and visualized into an executive view using Splunk Dashboard Studio.



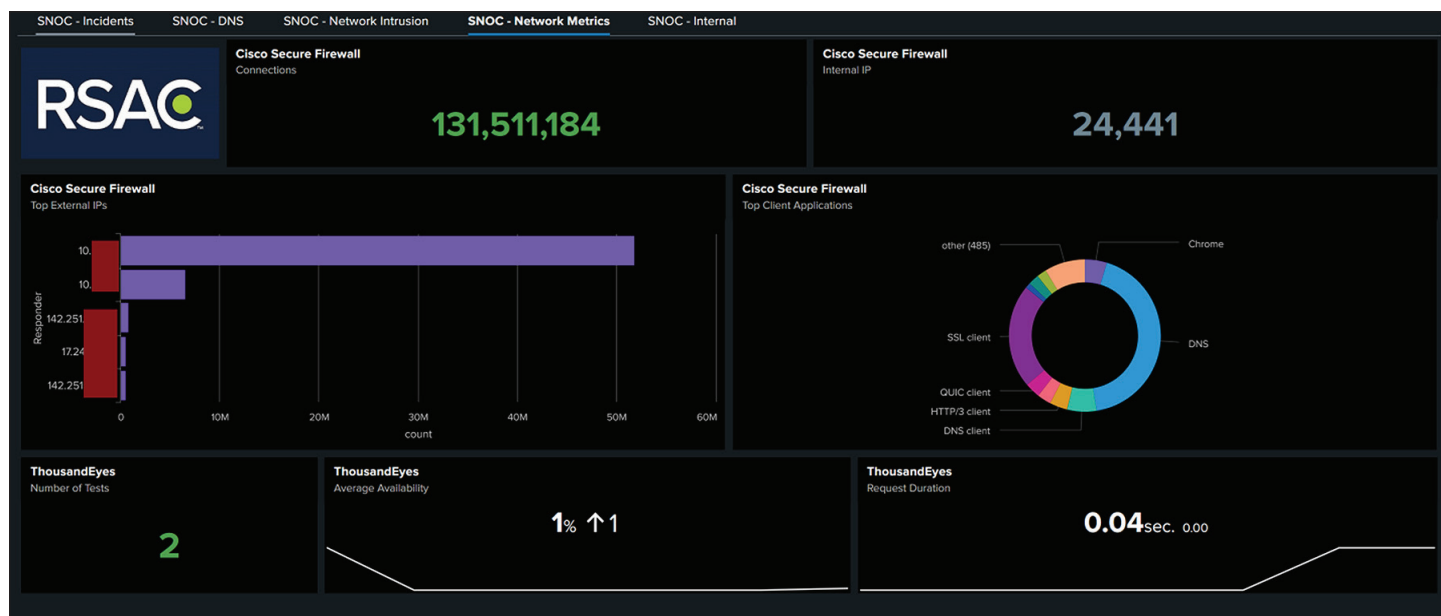
The following two screenshots show two of the five SNOC (Security and Network) dashboards, including DNS, with the total number of connected devices requesting Domain Name Service and number of queries.



Also, a dashboard for “Network Metrics,” with the number of unique IP addresses, connections and ThousandEyes metrics.

We also had dashboards rotating for XDR Incidents (including submitted samples to Secure Malware Analytics), Network Intrusion (Secure Firewall and Endace Zeek) and Internal (users and Cisco Identity Intelligence with Duo).

Since XDR was where the queue was being fielded from, Enterprise Security served as the hub where in-depth investigation occurred. Single-click integrations detailed throughout this report ensured that analysts and threat hunters working on any case had easy pivots between all tooling to focus on the threat at hand instead of navigating the tooling.



The SOC witnessed suspicious behaviors within the Network and wanted to be alerted for the behavior occurring again. We used [scheduled Splunk Alerts](#) to automatically send alerts to email, Webex®, and other locations. This was very useful for attempting to further action potentially compromised devices that were on the Network, for example, if a suspicious device reconnected to the Network, or a suspicious potential exploitation attempt was witnessed again. Some of these alerts went directly to conference leadership for swift action.

XDR Integration and Threat Hunting

With the ever-evolving technological landscape in the SOC at RSAC 2025, automation stands as a cornerstone in achieving XDR outcomes. Cisco XDR Automation embodies a user-friendly, no-to-low code platform with a drag-and-drop workflow editor. This innovative feature empowered the SOC to speed up its investigative and response capabilities.

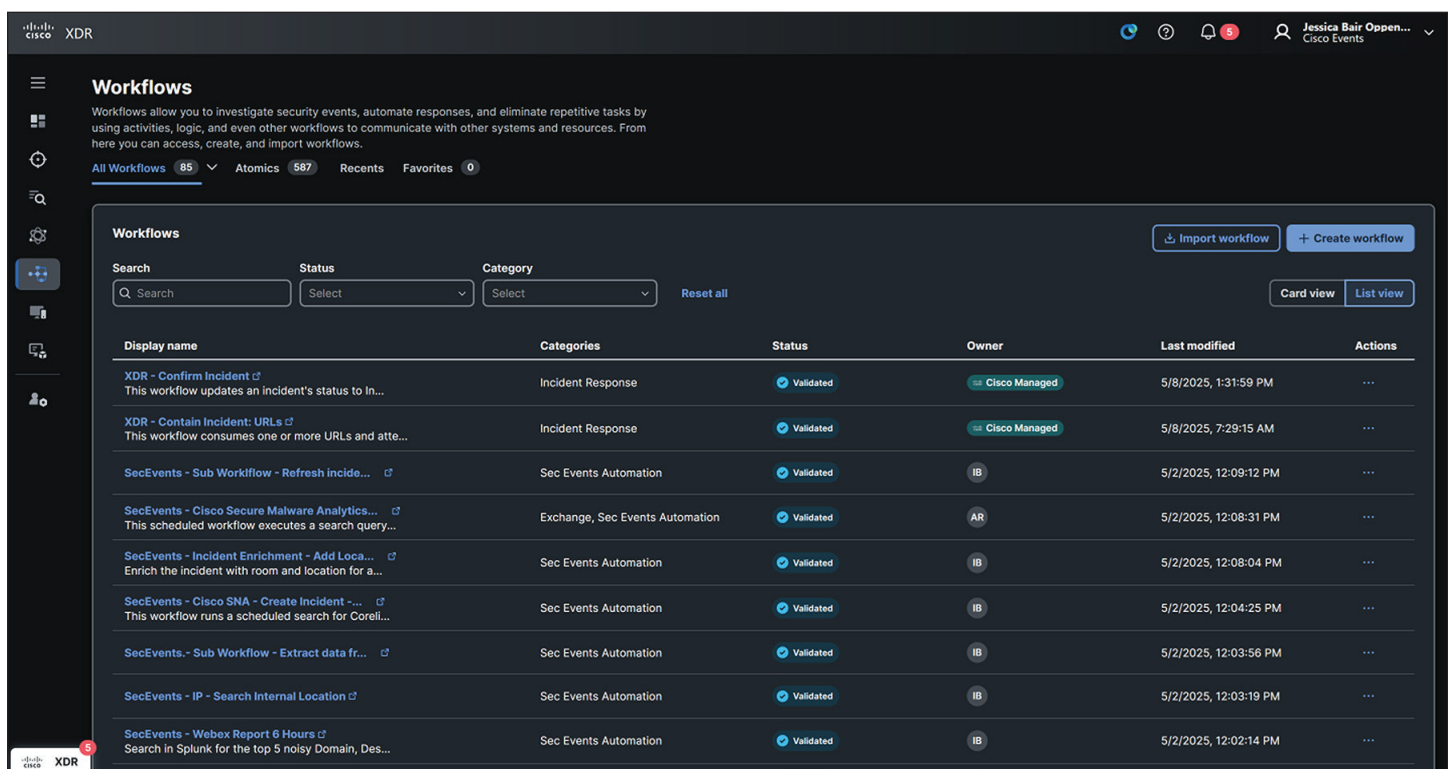
The following automation workflows are examples of those deployed at RSAC 2025:

Create or update XDR incident.

- Via Splunk Search API - XDR incident from Endace Zeek logs
- Via Splunk Search API - XDR incident from Cisco Secure Firewall Intrusion logs
- Via Splunk Search API - XDR Incident from ThousandEyes Alert
- Via Umbrella Reporting API - XDR Incident from Umbrella Security Events
- Via Secure Malware Analytics API - XDR Incident on samples submitted and convicted as malicious

Notify/Collaborate/Reporting

- Webex Notification on new Incident
- Last 6 hours reports to Webex
- Last 24 hours reports to Webex



The screenshot shows the Cisco XDR Workflows management interface. The top navigation bar includes the Cisco XDR logo, user profile (Jessica Bair Oppen...), and notification icons. The main section is titled "Workflows" and includes a description: "Workflows allow you to investigate security events, automate responses, and eliminate repetitive tasks by using activities, logic, and even other workflows to communicate with other systems and resources. From here you can access, create, and import workflows." Below this, there are filters for "All Workflows" (85), "Atoms" (587), "Recents", and "Favorites" (0). The "Workflows" table lists various workflows with columns for Display name, Categories, Status, Owner, Last modified, and Actions. The workflows listed include "XDR - Confirm Incident", "XDR - Contain Incident: URLs", "SecEvents - Sub Workflow - Refresh Incide...", "SecEvents - Cisco Secure Malware Analytics...", "SecEvents - Incident Enrichment - Add Loca...", "SecEvents - Cisco SNA - Create Incident -...", "SecEvents - Sub Workflow - Extract data fr...", "SecEvents - IP - Search Internal Location", and "SecEvents - Webex Report 6 Hours". Each workflow has a "Validated" status and a "Cisco Managed" or "IB" owner.

| Display name | Categories | Status | Owner | Last modified | Actions |
|--|---------------------------------|-----------|---------------|-----------------------|---------|
| XDR - Confirm Incident This workflow updates an incident's status to In... | Incident Response | Validated | Cisco Managed | 5/8/2025, 1:31:59 PM | ... |
| XDR - Contain Incident: URLs This workflow consumes one or more URLs and atte... | Incident Response | Validated | Cisco Managed | 5/8/2025, 7:29:15 AM | ... |
| SecEvents - Sub Workflow - Refresh Incide... | Sec Events Automation | Validated | IB | 5/2/2025, 12:09:12 PM | ... |
| SecEvents - Cisco Secure Malware Analytics... This scheduled workflow executes a search query... | Exchange, Sec Events Automation | Validated | AR | 5/2/2025, 12:08:31 PM | ... |
| SecEvents - Incident Enrichment - Add Loca... Enrich the incident with room and location for a... | Sec Events Automation | Validated | IB | 5/2/2025, 12:08:04 PM | ... |
| SecEvents - Cisco SNA - Create Incident -... This workflow runs a scheduled search for Corel... | Sec Events Automation | Validated | IB | 5/2/2025, 12:04:25 PM | ... |
| SecEvents - Sub Workflow - Extract data fr... | Sec Events Automation | Validated | IB | 5/2/2025, 12:03:56 PM | ... |
| SecEvents - IP - Search Internal Location | Sec Events Automation | Validated | IB | 5/2/2025, 12:03:19 PM | ... |
| SecEvents - Webex Report 6 Hours Search in Splunk for the top 5 noisy Domain, Des... | Sec Events Automation | Validated | IB | 5/2/2025, 12:02:14 PM | ... |

Investigate

- Via Splunk Search API and Global Variables (Table) - Identify Room and Location (incident rules on status new)
- Identify Location (incident playbook)
- Identify Location (Pivot Menu on IP)
- Webex Interactive Bot: Deliberate Observable
- Webex Interactive Bot: Search in Splunk
- Webex Interactive Bot: Location

Report

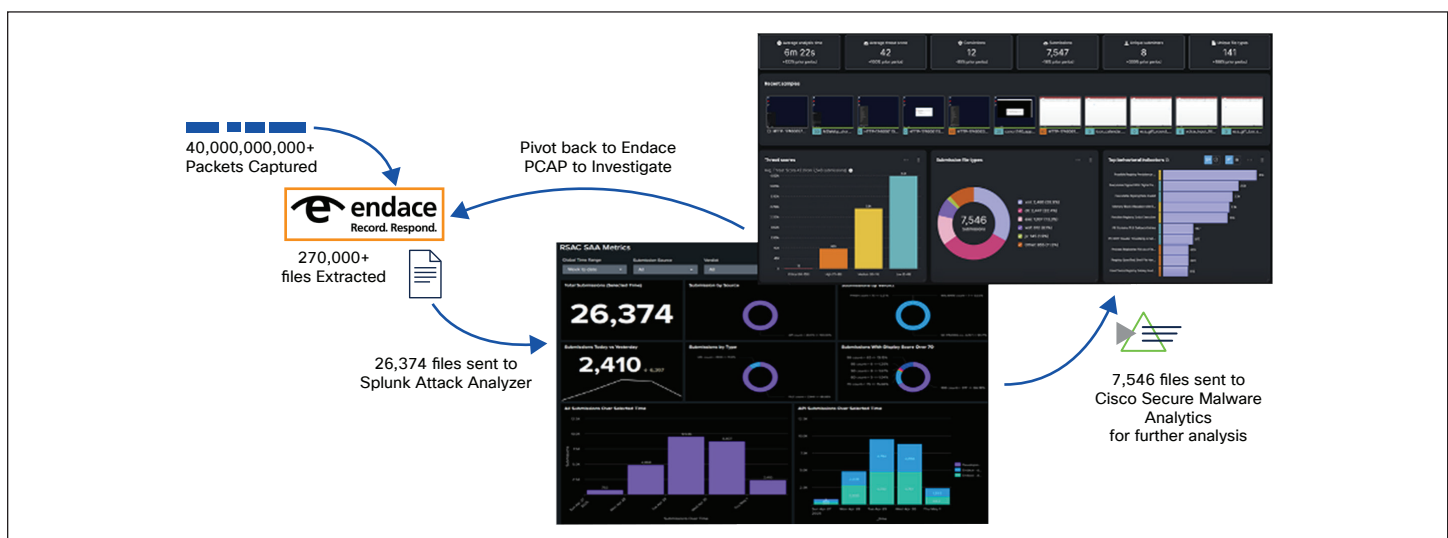
- XDR Incident statistics to Splunk

Malware Analysis

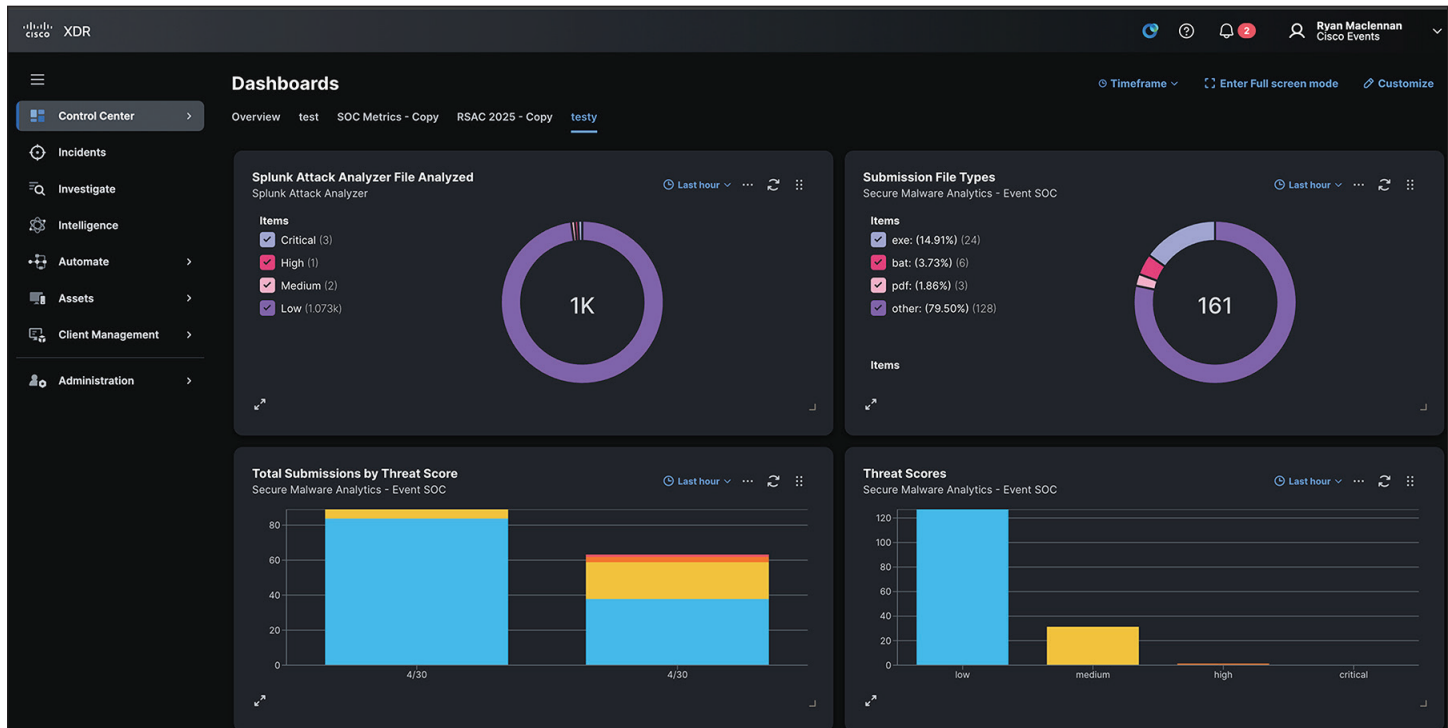
The SOC Team at RSAC 2025 sent thousands of potentially malicious files to Breach Protection - Malware Analytics via the Endace platform integration with Splunk Attack Analyzer, for automated behavioral analysis, and manual submissions to aid threat hunting.

Malware Analytics combines advanced sandboxing with threat intelligence in one unified solution to protect organizations from malware. It analyzed the behavior of a file against millions of samples and billions of malware artifacts. With the Malware Analytics capability, the SOC Team at RSAC 2025 had a global and historical view of the malware, its activity, and how large a threat it posed to the Network.

The Analysis workflow was automated as diagrammed below, Endace analyzed all incoming traffic to reconstruct any file content, file types were filtered to send only relevant Multipurpose Internet Mail Extensions (MIME) types to Splunk Attack Analyzer, further analysis of suspicious content was done by Cisco Secure Malware Analytics, and finally a full investigation of convictions was conducted on Endace using recorded Network packet data. This highly effective workflow allowed skilled analysts to focus on the most serious events.



Using Splunk Attack Analyzer as part of our Malware Analysis stack made it so we could analyze many more files than we previously could. Splunk Attack Analyzer is an engine of engines, meaning it will take the files sent to it and then determine if a certain file analysis engine should be run on that file. In our use case, we sent as many files as was reasonable, and then it would send supported files to Secure Malware Analytics. This workflow gave us a greater width of analysis and helped us protect the attendees from files that we may not have originally caught.



Adding to this design, we wanted to show a cohesive story between the products. We know that Endace would send the file to Splunk Attack Analyzer and then to Secure Malware Analytics. But we also needed to show some data in Cisco XDR. To make this grand vision a reality, we created a new Cisco XDR Relay Module and made an integration between Splunk Attack Analyzer and Cisco XDR in a single day. Below you can see that proof of concept that was made at RSAC 2025.

Documents in the Clear

Most of the samples submitted by API were documents or updates to applications. The analysts also had the ability to submit samples manually, which is especially useful to investigate suspicious websites without infecting your machine. You can choose the operating system you desire or use the best option.

To simulate user activity automatically during sample analysis, Malware Analytics provides emulation through playbooks, which are pre-defined steps that simulate user activity. A system with a user present appears vastly different from an automated analysis system (i.e., a sandbox). For example, an automated system may execute a submitted sample, but never change windows or move the mouse. On the other hand, a system with a real user present will have mouse movement and window changes as the user proceeds with a task or attempts to determine why the file that they just opened did nothing.

Submit Sample ⓘ

Local Data - United States

Submission Type

Upload file

Submit URL

File*

Choose or drag and drop a file

OPTIONS

Tags

zeus, spy-eye, etc...

Access

☐ Mark private

Virtual Machine

Use Best Option

ⓘ

Playbook

None

ⓘ

Network Simulation

None

Use Best Option

Close Active Window

Conduct Active Window Change

Open Embedded Object in Word Document

Random Cursor Movement with Image Recognition

Visit Website Using Internet Explorer

✓

ⓘ

ⓘ

ⓘ

ⓘ

ⓘ

ⓘ

Network Exit

ⓘ

Runtime

ⓘ

Password

ⓘ

Playbooks automatically simulate user activity during sample analysis, which allows Malware Analytics to behave as if a user were present and operating the keyboard and mouse during analysis.

You can also select from the drop-down list under “Network Exit” to investigate malware that behaves differently by region.

Network Simulation

None

As Needed

All Simulated

ⓘ

No network traffic will be simulated.

Network Exit

US - Pennsylvania - Philadelphia (default)

ⓘ

Runtime

US - Pennsylvania - Philadelphia (default)

✓

Password

AU - New South Wales - Sydney

BR - Paraíba/Sao Paulo - Joao Pessoa/Sao Paulo

CA - Alberta - Calgary

DE - Hesse - Frankfurt

GB - England - London

IT - Tuscany/Bergamo - Arezzo/Ponte San Pietro

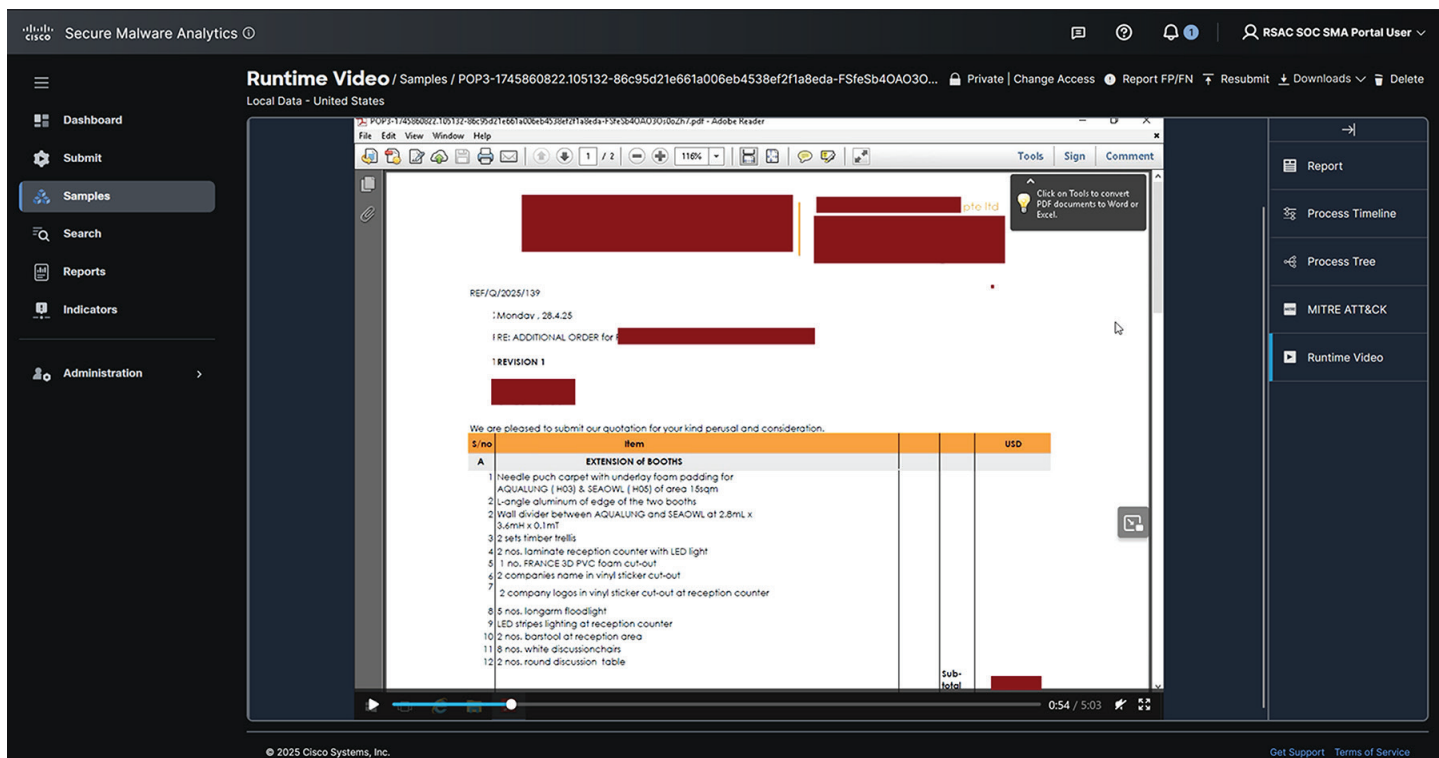
JP - Kanto - Tokyo

KR - Gyeonggi-do/Seoul - Anyang/Seoul

MX - Ciudad de Mexico - Mexico City

US - New York - Latham/NYC

ⓘ



The screenshot shows the Cisco Secure Malware Analytics interface. The main window displays a 'Runtime Video' of a PDF document. The PDF content includes a header with redacted information, a reference number 'REF/Q/2025/139', a date 'Monday, 28.4.25', and a subject line 'RE: ADDITIONAL ORDER for [redacted]'. Below this is a table titled 'EXTENSION of BOOTHS' with columns 'S/no', 'Item', and 'USD'. The table lists 12 items for booth extension, including carpet, aluminum, wall dividers, timber trellis, laminate reception counter, PVC foam cut-out, vinyl stickers, and various lighting and furniture items. The total value is listed as 'Sub-total' with a redacted amount.

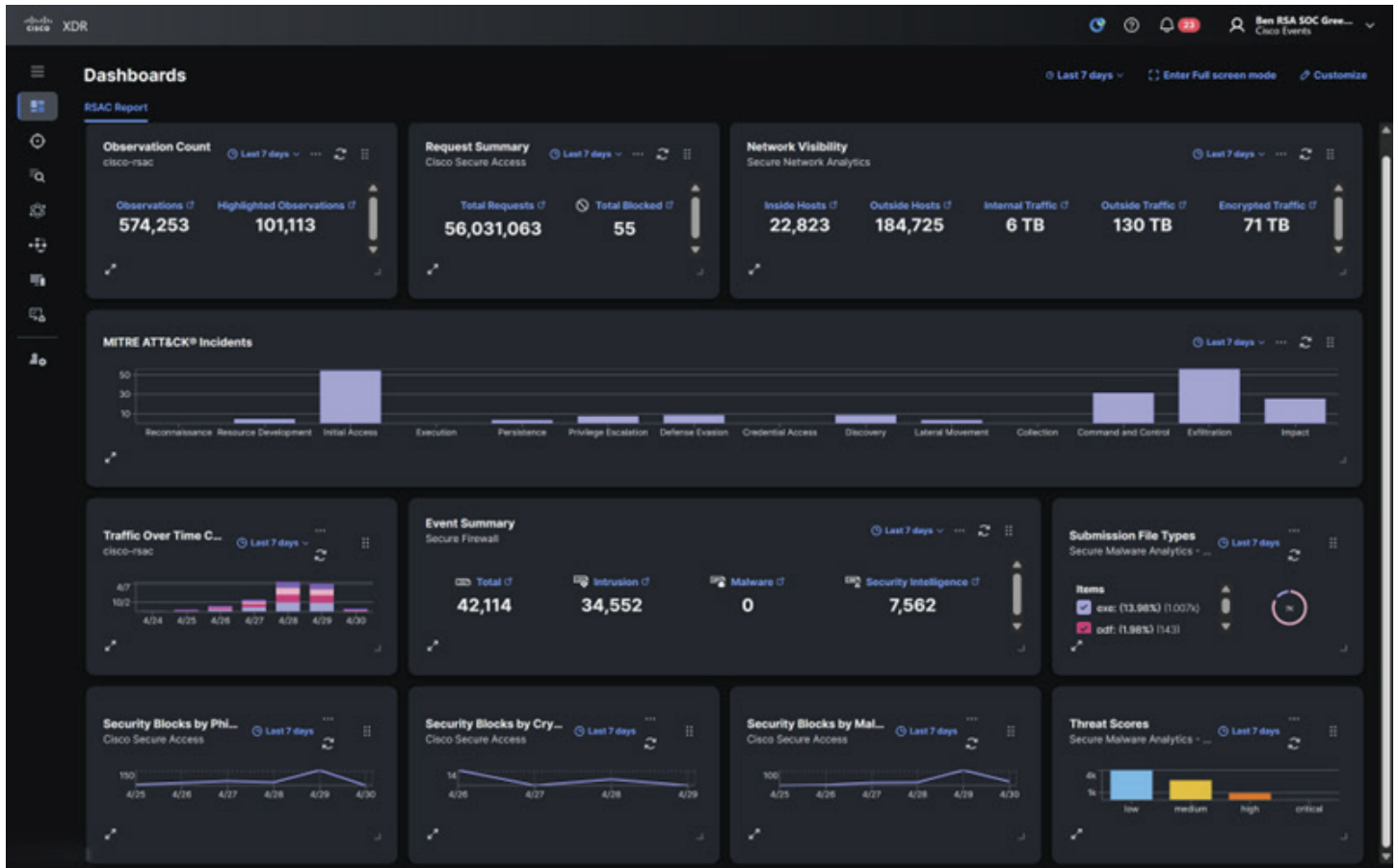
| S/no | Item | USD |
|------|---|------------|
| 1 | Needle punch carpet with underlay foam padding for AQUALUNG (H03) & SEAOWL (H05) of area 1.5sqm | |
| 2 | L-angle aluminum of edge of the two booths | |
| 3 | Wall divider between AQUALUNG and SEAOWL at 2.8mL x 3.6mH x 0.1mT | |
| 3 | 2 sets timber trellis | |
| 4 | 2 nos. laminate reception counter with LED light | |
| 5 | 1 nos. FRANGE 3D PVC foam cut-out | |
| 6 | 2 companies name in vinyl sticker cut-out | |
| 7 | 2 company logos in vinyl sticker cut-out at reception counter | |
| 8 | 5 nos. longarm floodlight | |
| 9 | LED stripes lighting at reception counter | |
| 10 | 2 nos. barstool at reception area | |
| 11 | 8 nos. white discussion chairs | |
| 12 | 2 nos. round discussion table | |
| | Sub-total | [redacted] |

The Endace and Splunk Attack Analyzer found and analyzed many documents that were in the clear. Any attendee at RSAC 2025, who had the right tools and knowledge, would have been able to view the attachments.

Documents sent in this manner provide personal information that would enable an attacker to craft a spear phishing email or text, to trick a person into clicking on a link such as in this example a purchase order that had the names and email addresses of the purchaser of the office furniture.

We contacted the sender of this email and advised them of insecure email protocols. See the **Tales of Insecurity** later in this report for more stories.

We were able to monitor the sample submissions in the Cisco XDR Control Center during the operations.



Remote Access Trojan Command and Control (RAT C2)

One of the SOC Threat Hunters conducted a systematic review of alerts in Cisco XDR. The hunter noticed a device on the Network was observed by Cisco Secure Firewall connecting to a known malicious IP address, alerted by Cisco XDR.

[illegible]

Upon further investigation leveraging available threat intelligence integrations, such as alphaMountain, the IP was identified as a Remco RAT C2 address.

With the new Endace integration, the hunter was able to pivot to the Endace platform from the XDR interface. Packet Capture (PCAP) investigation revealed that the device was beaconing to the C2 of the RAT once per second.

The screenshot displays the Cisco XDR 'Investigate' interface. The main section is titled 'Pivot with VT intel' and shows a diagram of malicious processes connected to a central IP address. The diagram includes nodes for 'sha256: 3d78...cald Malicious Process', 'sha256: b6d0...ae3d Malicious Process', '185.196 Malicious IP Address', and 'sha256: 0919...4d73 Malicious Process'. Arrows indicate connections between these nodes. On the right, a sidebar shows details for the IP address 185.196, including 'Verdict Source', '4 Verdicts', and a list of 'Observables' such as 'IP Address', 'Domain', 'URL', and 'URL'. A red box highlights the 'EndProbe' section, which contains a 'Pivot-to-Vision' button and a 'Generate a Pivot-to-Vision URL from this IP address' button.

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|-----------------------------|--------|-------------|----------|--------|---|
| 7285 | 2025-04-29 11:16:03.7814661 | 10.63 | 185.1 | TCP | 64 | 53274 → 3912 [ACK] Seq=167 Ack=129 Win=131328 Len=0 |
| 7286 | 2025-04-29 11:16:03.7814661 | 10.63 | 185.1 | 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 | 10.63 | TCP | 64 | 3912 → 53274 [RST, ACK] Seq=129 Ack=167 Win=2096896 Len=0 |
| 7288 | 2025-04-29 11:16:04.9479789 | 10.63 | 185.1 | 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 | 10.63 | 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 | 185.1 | TCP | 64 | 53276 → 3912 [ACK] Seq=1 Ack=1 Win=131584 Len=0 |
| 7291 | 2025-04-29 11:16:05.1144963 | 10.63 | 185.1 | TLSv1.3 | 224 | Client Hello |
| 7292 | 2025-04-29 11:16:05.1436238 | 10.63 | 185.1 | 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 | 10.63 | TLSv1.3 | 186 | Server Hello |
| 7294 | 2025-04-29 11:16:05.3031093 | 185.1 | 10.63 | 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 | 185.1 | TCP | 64 | 53329 → 3912 [ACK] Seq=1 Ack=1 Win=131584 Len=0 |
| 7296 | 2025-04-29 11:16:05.3058350 | 10.63 | 185.1 | TLSv1.3 | 224 | Client Hello |
| 7297 | 2025-04-29 11:16:05.3312273 | 10.63 | 185.1 | TCP | 64 | 53276 → 3912 [ACK] Seq=167 Ack=129 Win=131328 Len=0 |
| 7298 | 2025-04-29 11:16:05.4675386 | 185.1 | 10.63 | TLSv1.3 | 186 | Server Hello |
| 7299 | 2025-04-29 11:16:05.4889965 | 185.1 | 10.63 | TCP | 64 | 3912 → 53276 [RST, ACK] Seq=129 Ack=167 Win=2096896 Len=0 |
| 7300 | 2025-04-29 11:16:05.5224879 | 10.63 | 185.1 | TCP | 64 | 53329 → 3912 [ACK] Seq=167 Ack=129 Win=131328 Len=0 |
| 7301 | 2025-04-29 11:16:05.6801091 | 185.1 | 10.63 | TCP | 64 | 3912 → 53329 [RST, ACK] Seq=129 Ack=167 Win=2096896 Len=0 |
| 7302 | 2025-04-29 11:16:09.9238367 | 10.63 | 185.1 | TCP | 70 | 53334 → 3912 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 7303 | 2025-04-29 11:16:10.0085892 | 185.1 | 10.63 | 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 | 185.1 | TCP | 64 | 53334 → 3912 [ACK] Seq=1 Ack=1 Win=131584 Len=0 |
| 7305 | 2025-04-29 11:16:10.0905054 | 10.63 | 185.1 | TLSv1.3 | 224 | Client Hello |
| 7306 | 2025-04-29 11:16:10.2523160 | 185.1 | 10.63 | TLSv1.3 | 186 | Server Hello |
| 7307 | 2025-04-29 11:16:10.3124168 | 10.63 | 185.1 | TCP | 64 | 53334 → 3912 [ACK] Seq=167 Ack=129 Win=131328 Len=0 |
| 7308 | 2025-04-29 11:16:10.4700303 | 185.1 | 10.63 | TCP | 64 | 3912 → 53334 [RST, ACK] Seq=129 Ack=167 Win=2096896 Len=0 |
| 7309 | 2025-04-29 11:16:11.1196384 | 10.63 | 185.1 | TCP | 70 | 53283 → 3912 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 7310 | 2025-04-29 11:16:11.2773142 | 185.1 | 10.63 | 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 interface 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, Dst: 185.194.100.1

Transmission Control Protocol, Src Port: 53337, Dst Port: 3912, Seq: 167, Ack: 129, Len: 0

0000 00 00 5e 00 01 9c ed d5 ffE
0010 00 28 fb 8e 40 fa 95 0a 3f760
0020 09 fb d0 59 0f eb a9 09 dfY.N.4 P
0030 02 01 d0 0c 00 00 00 00h

The identified host was the only host communicating with the C2 IP address. The Splunk Enterprise Security team wrote a search and alert to notify the Threat Hunters when the device returned to the Network and started the beaconing again, to help them remediate the infection.

Secure Access

The SOC had complete Domain Name Service (DNS) visibility, thanks to the support of the Moscone Center with installing Secure Access Virtual Appliances (VAs) in the Network Operation Center.

Over 22,000 devices used the Network to connect to the internet, and the SOC saw over 65 million DNS requests over the week, of which over 2,800 would have been blocked for security policy violations in a production environment.

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 was 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 to RSAC 2025 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 2025 security team and law enforcement, as appropriate, in coordination with the Moscone NOC.

| Requests | | | | |
|-------------------|------------|---------|------------|------------|
| Name | Allowed | Blocked | Total | % of Total |
| ⊕ Security | 2,882 | 60 | 2,942 | 0.0045% |
| Categories | - | 0 | 0 | 0.00% |
| Destination Lists | 0 | 0 | 0 | 0.00% |
| Permitted | 65,242,684 | - | 65,242,684 | 100.00% |
| Total | 65,245,566 | 60 | 65,245,626 | 100% |

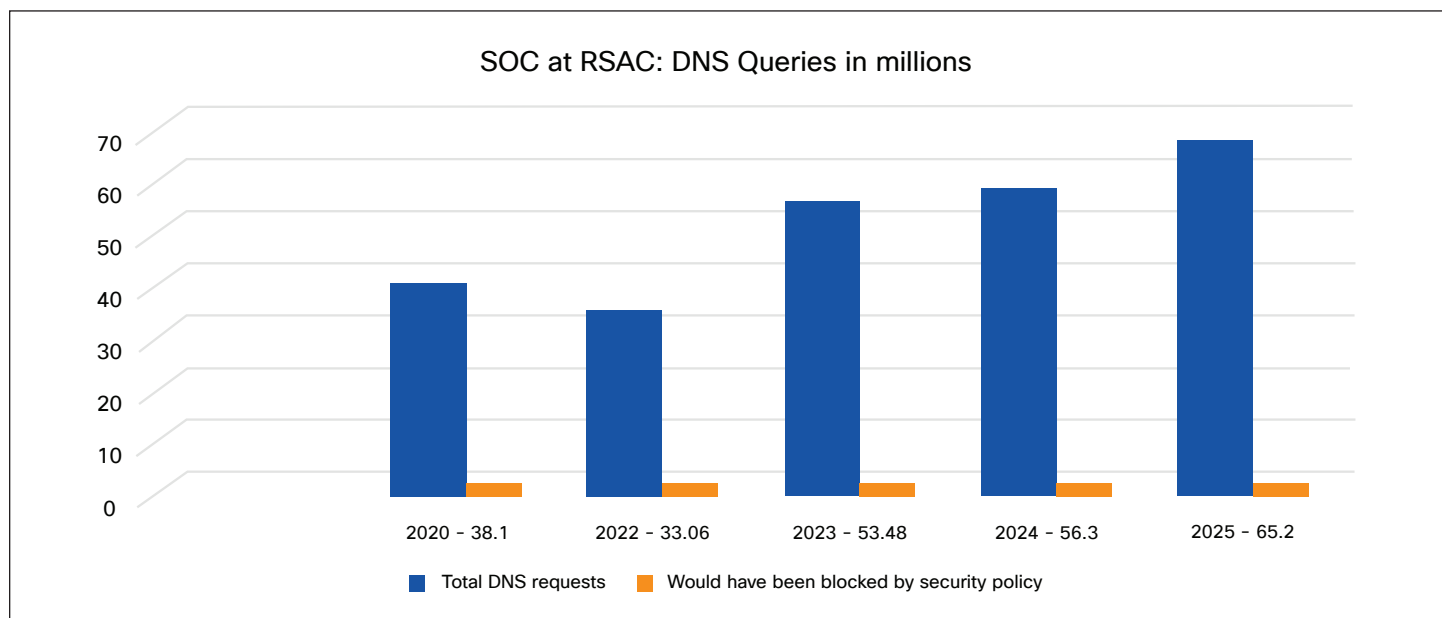
Many production environments block Encrypted DNS queries, as they can be a security vulnerability. At the RSAC Conference, we encourage encryption, and encrypted queries were allowed, over 1 million in 2025.

| Name | Allowed | Blocked | Total | % of Total |
|-----------------------|---------|---------|-------|------------|
| ⊖ Security | 2,869 | 60 | 2,929 | 0.0046% |
| ⊖ — Prevent | 2,506 | 26 | 2,532 | 0.0039% |
| — Malware | 221 | 4 | 225 | 0.0004% |
| — Dynamic DNS | 1,564 | 0 | 1,564 | 0.0024% |
| — Newly Seen Domains | 682 | 0 | 682 | 0.0011% |
| — Potentially Harmful | 0 | 0 | 0 | 0.00% |
| — DNS Tunneling | 0 | 22 | 22 | 0.0000% |
| — Cryptomining | 39 | 0 | 39 | 0.0001% |
| ⊖ — Contain | 363 | 34 | 397 | 0.0006% |
| — Command & Control | 16 | 0 | 16 | 0.0000% |
| — Phishing | 347 | 34 | 381 | 0.0006% |

As mentioned, in the NOC, Secure Access VAs were deployed as internal, recursive DNS resolvers. The benefit of those VAs is twofold:

- To enable outbound encryption of DNS queries, and
- To enrich the queries with the original internal IP address of the client

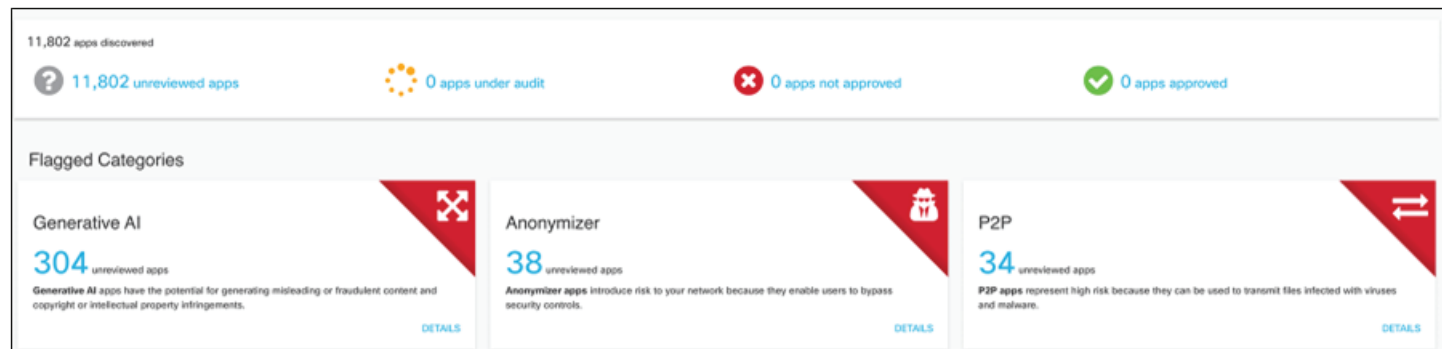
Without the latter benefit, the Secure Access dashboard reporting would be much less useful in threat hunting since without internal IP addresses, correlation with other network activity is difficult. We assign the VAs to the attendee wireless clients via Dynamic Host Configuration Protocol (DHCP), and 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

11,802 applications were identified by DNS queries at RSAC 2025. This is an increase from past conferences.

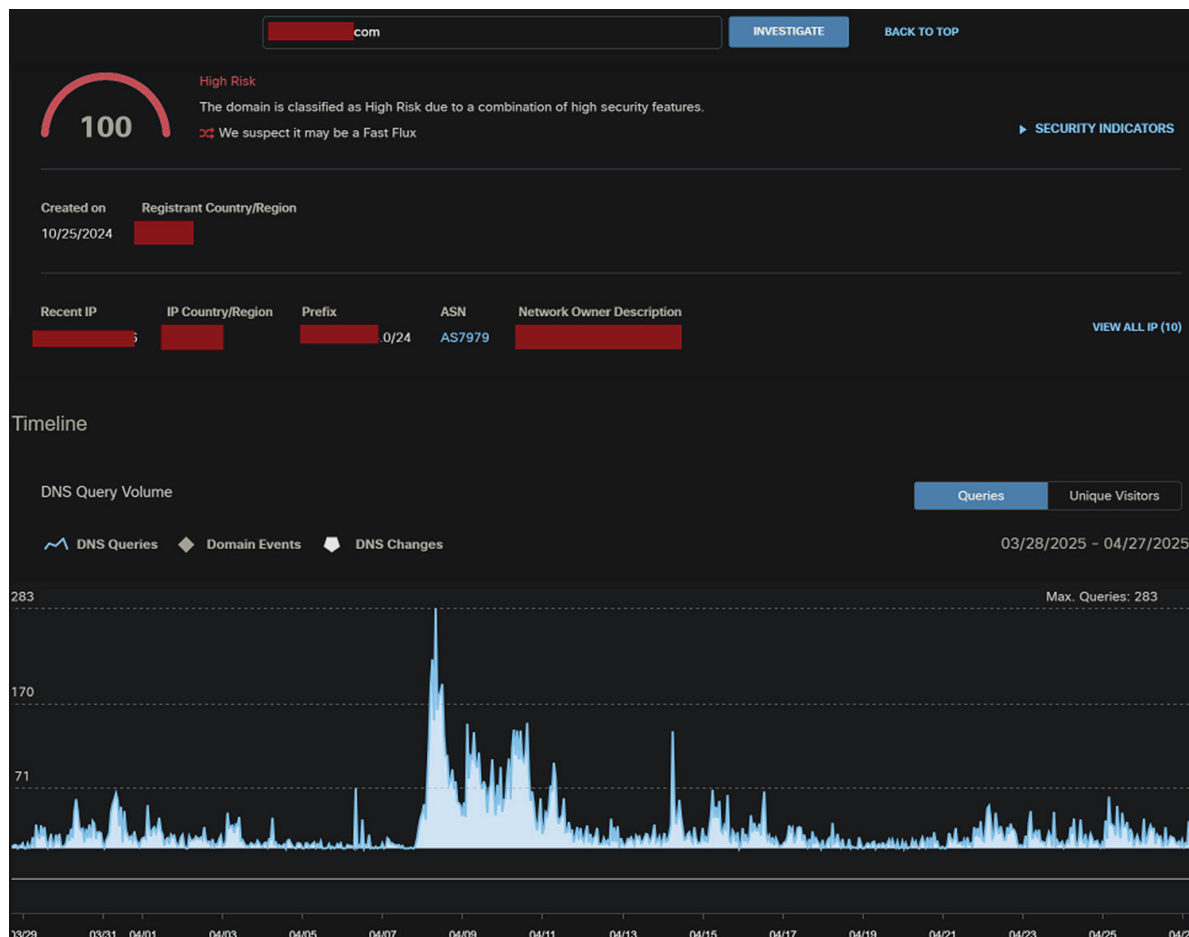
- 2024: 10,167 apps
- 2023: 8,750 apps
- 2022: 7,200+ apps
- 2020: ~4,000 apps



The apps were categorized by risk to an organization in a production environment. A rogue or unauthorized app could have been blocked from RSAC 2025, in the event of a major incident—again, one of the ways the SOC can be used for protection in an emergency.

[illegible]

This campaign relies on malicious advertising pop-ups on legitimate and less-than-legitimate websites to generate revenue, while eventually attempting to install additional software in the form of browser extensions and other adware or PUPs.

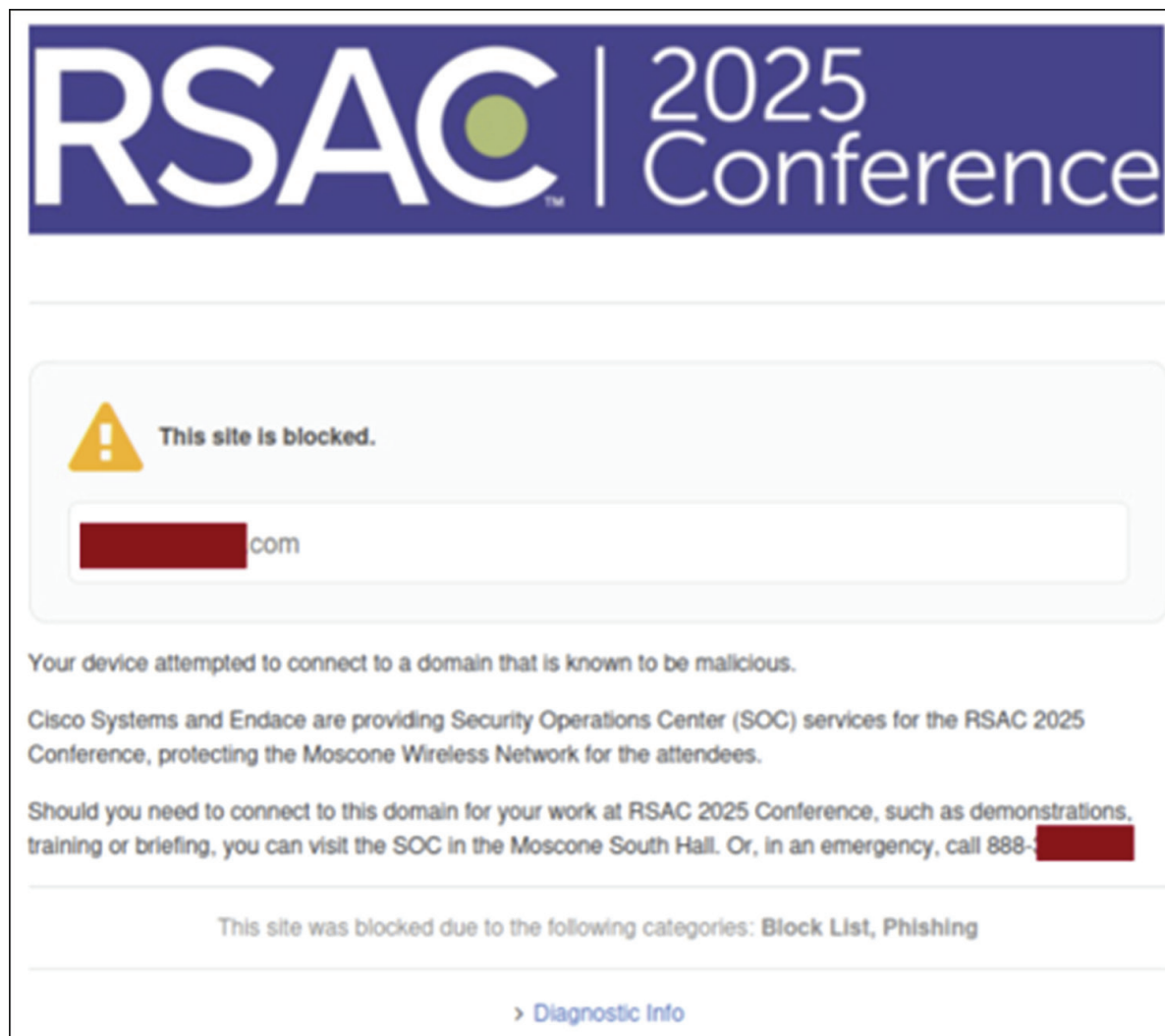


By employing techniques like wildcard DNS abuse, and dynamically generated domain names, attackers are continuously adding new domain names to this campaign, but the back-end infrastructure is the same each time.

We blocked the infrastructure found behind the domain names as listed below:

| | | |
|--------------------------|------------------------------|---------------------------|
| surpXXXXXXXXXXrry[.]com | natXXXXXXXXXXr edent[.]com | invXXXXXXXXXXrrail[.]com |
| coliXXXXXXXXXXself[.]com | mesXXXXXXXXXXosity[.]com | midXXXXXXXXast[.]com |
| frocXXXXXXXXXrbal[.]com | geniXXXXXXXXXset[.]com | instiXXXXXXXXXgnate[.]com |
| bravXXXXXXXXXuire[.]com | knoXXXXXXXXount[.]com | instXXXXXXXXXelp[.]com |
| huXXXXXXXXor.co[.]in | foXXXXXXXXXero[.]click | difXXXXXXXXXld[.]com |
| fundXXXXXXXXXming[.]com | sequenXXXXXXXXybXids[.]com | proXXXXXXXXXecpm[.]com |
| | telegXXXXXXXXXXrightly[.]com | |

A pop-up message appeared for protected RSAC 2025 attendees, including information on how to contact the SOC, should they need to access the domains for their work at the event.

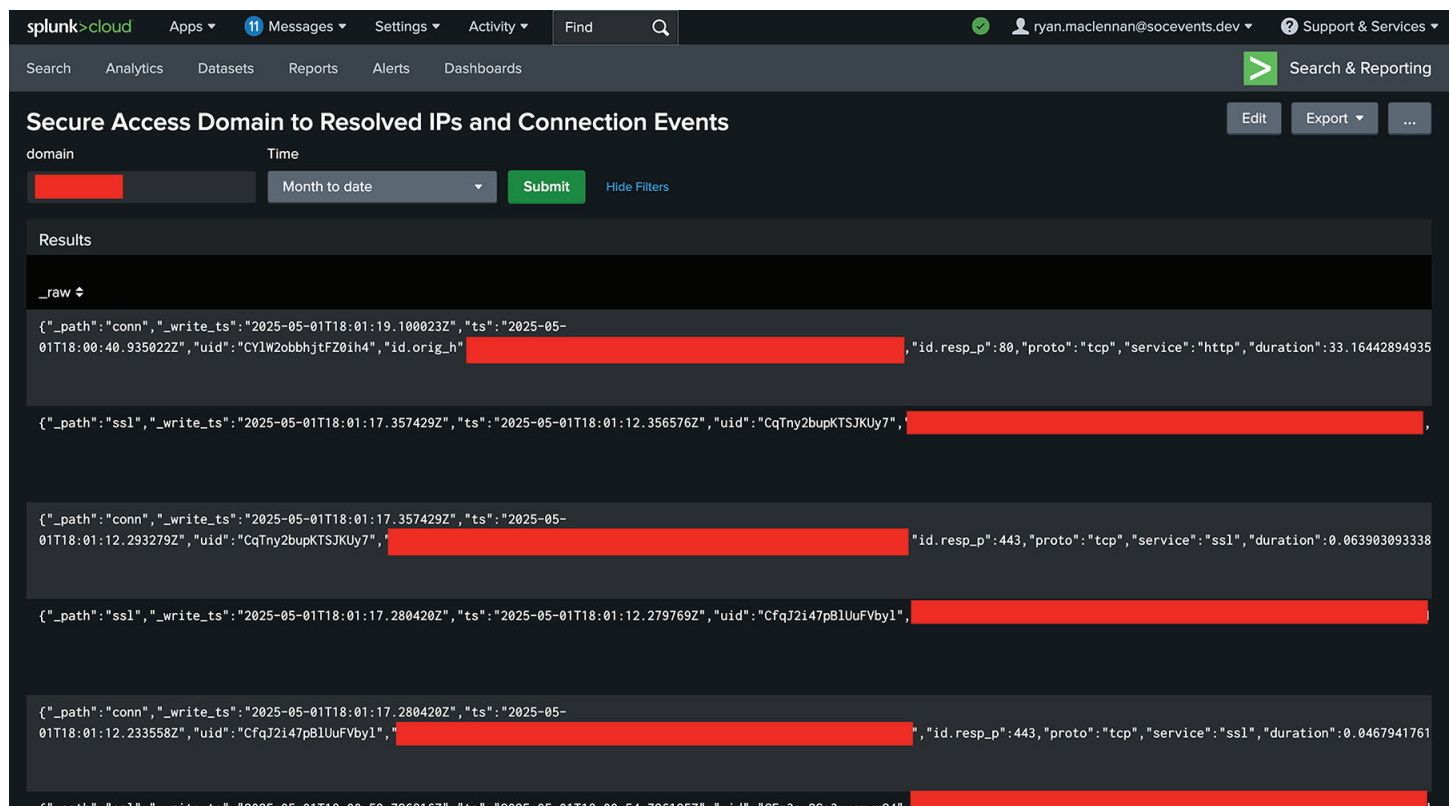


The SOC Team continues to engage with the RSAC on how to best protect the Network, while having the most access possible.

Splunk Query Turned Dashboard

To assist in finding traffic related to a certain domain and the resolved IPs of that domain, we made a Splunk query that would search Secure Access for the domain, pass the found fields we want to an Endace search to resolve the IP addresses associated with the domain, and then do another Endace search to get all the connection logs of the destination IPs resolved from that domain.

The query made the job of manually needing to do a lookup ourselves obsolete and validated that there was traffic going to and from the searched domain. Here is an example of the dashboard we created to facilitate this.



The screenshot shows a Splunk dashboard with the title "Secure Access Domain to Resolved IPs and Connection Events". The interface includes a search bar at the top with the text "splunk>cloud" and navigation tabs for Apps, Messages, Settings, Activity, Find, and Search & Reporting. Below the search bar, there are filters for "domain" (with a redacted input) and "Time" (set to "Month to date"). A "Submit" button and a "Hide Filters" link are also present. The "Results" section displays a list of network events in JSON format, with some fields redacted. The events include details such as "_path", "_write_ts", "ts", "uid", "id.orig_h", "id.resp_p", "proto", "service", and "duration".

Here is the query we used to create this dashboard if you would like to use it yourselves:

index="endace" AND NOT path="dns"

```
[ search index="endace"
  [ search index="umbrella_log" domain=$domain$
    | fields src , domain
    | eval domain = substr(domain, 1, len(domain)-1)
    | rename domain AS query ]
  | fields answer, src
  | stats values(answer) as dest
]
```

XDR AI Assistant

The XDR AI assistant was very helpful in generating Incident Summarization reports in the SOC at RSAC 2025. The AI-generated reports reduced the time required to prepare the SOC Incident Response Reports for RSAC and the NOC team, when an escalation was required.

Incident Summary

The incident involved **endpoint 10[.]65[.]** being accessed by **domain invadedisheartentrail[.]com** at 2025-04-22 03:34:08.000 UTC. Other endpoints were also involved in similar activities. The user accounts and exact number of assets involved in the incident are currently unknown.

- The adversary used **[T1566] Phishing** technique and **[TA0001] Initial Access** tactic.

Remediation actions were taken as follows:

- The incident was promoted on 2025-04-26 20:41:51.557 UTC by Cisco Events
- Analysis was completed on 2025-04-26 20:41:54.000 UTC by Cisco Events
- The incident was modified on 2025-04-26 20:41:54.052 UTC by Cisco Events

The products used for analysis were **Secure Malware Analytics**, **Cisco Secure Access Reporting API**, and **Cisco Secure Access**.

Intrusion Detection with Cisco Secure Firewall

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 2025. We deployed a Secure Firewall 4115 appliance running Cisco Secure Firewall Threat Defense (FTD) software as our IDS. We leveraged the IDS for multiple integrations:

- Events to Security Cloud Control (SCC)
- Events to Cisco XDR for incident correlation
- Events to Splunk
- Files were submitted to Secure Malware Analytics for sandbox analysis
- Integration with Endace for event cross-launch and full session access

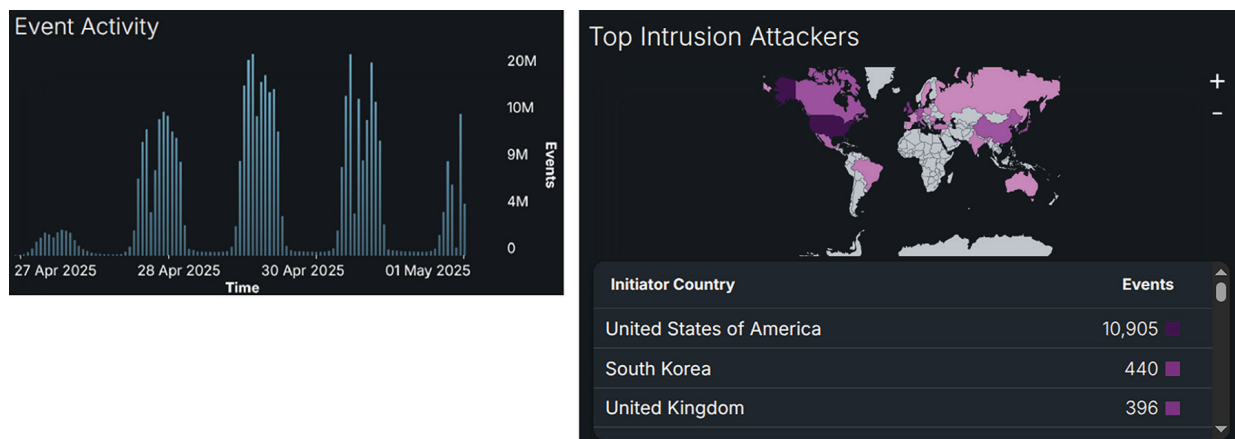
The IDS inspected all wireless guest traffic from event attendees. Cisco Secure Firewall offers breach detection, threat discovery, malware detection and sandbox integration, and security automation. Rich contextual information (such as applications, operating systems, vulnerabilities, intrusions, and transferred files) served by the SOC to help uncover threats lurking in the environment.

While Cisco Secure Firewall offers a wide variety of native threat visibility, this year we found ourselves increasingly leveraging our integrations with Cisco XDR and Splunk to push our investigations to the next level.

Lastly, as the share of encrypted traffic continues to increase, we find ourselves relying on Encrypted Visibility Engine (EVE) more than ever to give us threat visibility for encrypted traffic.

Security Cloud Control and Unified Events

This year was the first time we integrated with Security Cloud Control (SCC), Cisco's new cloud management platform that offers centralized management for Secure Firewall, Multicloud Defense, Hypershield, Secure Access, and other platforms.



SCC brought us both easy remote access to events and a new slate of dashboards, including some custom work from the SCC development team.



The cloud-delivered Cisco Firewall Management Center (FMC) component of SCC offers extensive configuration parity with the on-prem FMC, including the Unified Event viewer. Unified Events for EVE detections was our most fruitful investigative workflow at RSAC 2025.

Cloud-delivered Firewall Management Center

Analysis / Unified Events

[Return Home](#)
[Deploy](#)

Home

Monitor

Analysis

Manage

Policies

Devices

Objects

Integration

EVE Threat Confidence Sco... >75

EVE Process Name !generic dmz process

14

8

0

0

22 events

2025-04-30 18:29:13 EDT

2025-05-01 18:29:13 EDT 1d

| Time | Event Type | EVE Fingerprint | EVE Process Confidence Score | EVE Process Name | EVE Threat Confidence | EVE Threat Confidence Score |
|-----------------------|----------------------|-----------------------|------------------------------|------------------|-----------------------|-----------------------------|
| > 2025-05-01 13:12:06 | Connection | tls/1/(0301)(c00ac009 | 8% | malware-upatre | High | 92% |
| > 2025-05-01 12:48:22 | Connection | tls/1/(0303)(c02cc02b | 15% | malware-upatre | High | 97% |
| > 2025-05-01 12:46:55 | Connection | tls/1/(0303)(c02cc02b | 30% | malware-upatre | High | 95% |
| > 2025-05-01 12:45:25 | Connection | tls/1/(0303)(c02cc02b | 15% | malware-upatre | High | 97% |
| > 2025-05-01 12:45:12 | Connection | tls/1/(0303)(c02cc02b | 15% | malware-upatre | High | 97% |
| > 2025-05-01 12:45:12 | Connection | tls/1/(0303)(c02cc02b | 14% | malware-upatre | High | 90% |
| > 2025-05-01 12:45:12 | Connection | tls/1/(0303)(c02cc02b | 15% | malware-upatre | High | 97% |
| > 2025-05-01 12:35:33 | Connection | http/(474554)(485454 | 18% | malware-stration | High | 84% |
| > 2025-05-01 12:34:10 | Connection | http/(474554)(485454 | 78% | malware-upatre | High | 98% |
| > 2025-05-01 11:00:01 | Security-Related Con | http/(474554)(485454 | 43% | malware-viking | High | 88% |
| > 2025-05-01 10:58:08 | Security-Related Con | tls/1/(0303)(13031302 | 100% | malware-upatre | Very High | 100% |
| > 2025-05-01 09:50:51 | Connection | http/(474554)(485454 | 50% | malware-adware | High | 77% |
| > 2025-05-01 00:18:05 | Connection | http/(474554)(485454 | 18% | malware-stration | High | 84% |
| > 2025-04-30 23:47:31 | Connection | http/(474554)(485454 | 18% | malware-stration | High | 84% |
| > 2025-04-30 21:11:27 | Security-Related Con | tls/1/(0303)(c02cc02b | 91% | malware-upatre | Very High | 91% |
| > 2025-04-30 20:22:37 | Security-Related Con | http/(474554)(485454 | 18% | malware-stration | Very High | 84% |

We can click the ellipses next to an EVE fingerprint to pivot to additional information about the threat.

Cloud-delivered Firewall Management Center

Analysis / Unified Events

Search

Return Home

Deploy

@cisco.c

Home

EVE Threat Confidence Sco... >75

EVE Process Name !generic dmz process

14

8

0

0

22 events

2025-04-30 18:29:13 EDT

2025-05-01 18:29:13 EDT

1d

Monitor

Analysis

Manage

Policies

Devices

Objects

Integration

| Time | Event Type | EVE Fingerprint | EVE Process Confidence Score | EVE Process Name | EVE Threat Confidence | EVE Threat Con Score |
|-----------------------|------------|------------------------|--|------------------|-----------------------|----------------------|
| > 2025-05-01 13:12:06 | Connection | tls/1/(0301)(c00ac008) | 8% | malware-upatre | High | 92% |
| > 2025-05-01 12:48:22 | Connection | tls/1/ | <div> <div>Add inclusion to filter</div> <div>Add exclusion to filter</div> <div>Copy to clipboard</div> <div>View EVE Process Analysis</div> </div> | malware-upatre | High | 97% |
| > 2025-05-01 12:46:55 | Connection | tls/1/ | | malware-upatre | High | 95% |
| > 2025-05-01 12:45:25 | Connection | tls/1/ | | malware-upatre | High | 97% |
| > 2025-05-01 12:45:12 | Connection | tls/1/ | | malware-upatre | High | 97% |
| > 2025-05-01 12:45:12 | Connection | tls/1/ | | malware-upatre | High | 90% |
| > 2025-05-01 12:45:12 | Connection | tls/1/ | | malware-upatre | High | 97% |
| > 2025-05-01 12:35:33 | Connection | http/ | | malware-stration | High | 84% |
| > 2025-05-01 12:34:10 | Connection | http/(474554)(485454) | 78% | malware-upatre | High | 98% |

The process analysis shows some of the logic that goes into EVE determinations. For example, process names associated with the fingerprinted connection are shown. For this fingerprint, most but not all of them are malware.

Secure Firewall Application Detectors

Encrypted Visibility Engine Process Analysis

Customer Contact

Customer Email

Customer Name

Encrypted Visibility Details ⓘ

Fingerprint

VDB Version

Server Name

Application Debug Log(Optional) ⓘ

IP Address

Port

View Request

To provide feedback about any of the processes from the list below, select the applicable entries and submit your request. If there are no results you can still submit your request.

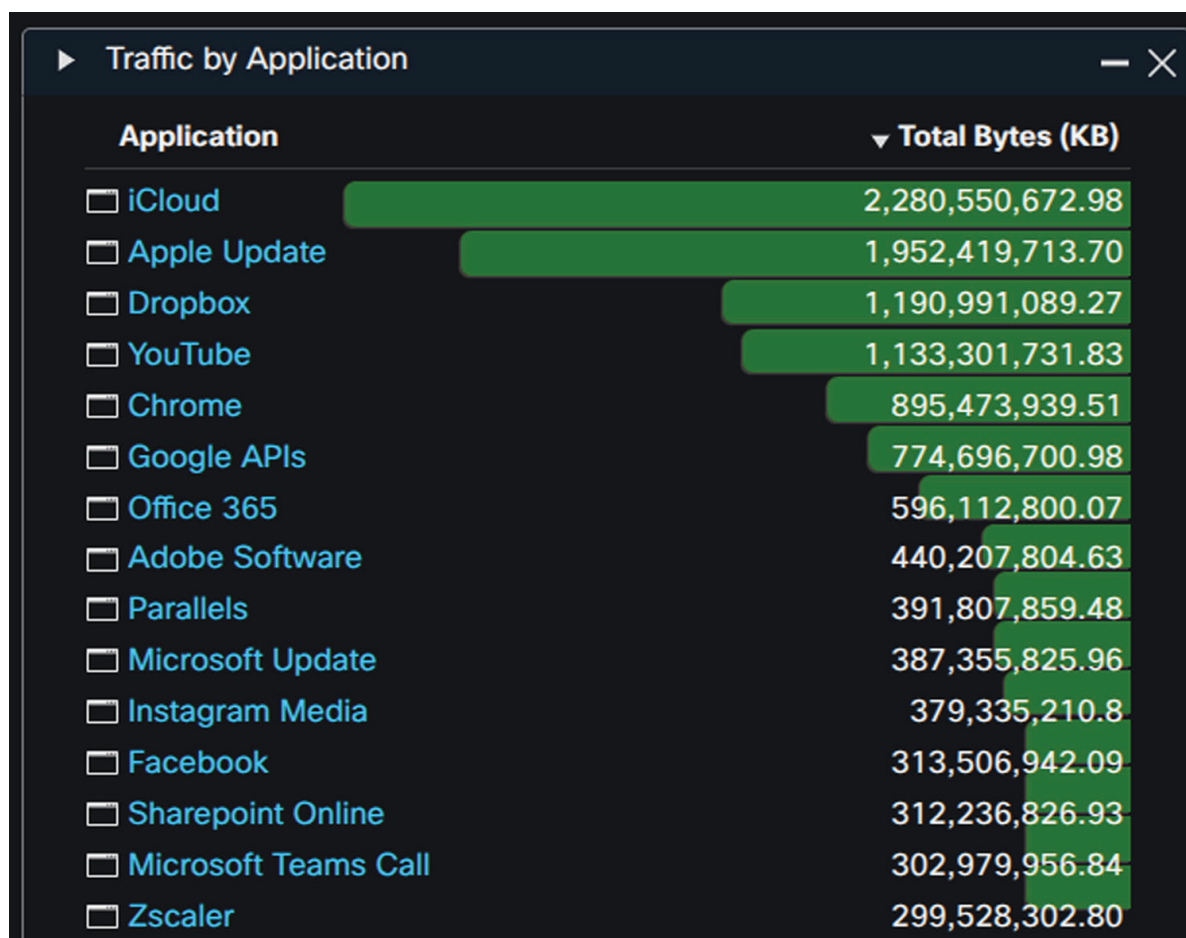
| Process Name ↑↓ | Prevalence ↑↓ | Server Name ↑↓ | IP Address ↑↓ | Port ↑↓ |
|---|---------------|----------------|---------------|---------|
| <input type="checkbox"/> generic dmz process | 0.3969 | 0.0000 | 0.0000 | 0.3297 |
| <input type="checkbox"/> malware-upatre | 0.3580 | 0.0000 | 0.0000 | 0.3979 |
| <input type="checkbox"/> malware-coinminer | 0.0659 | 0.0000 | 0.0000 | 0.0733 |
| <input type="checkbox"/> malware-trojan-njrat | 0.0583 | 0.0000 | 0.0000 | 0.0648 |
| <input type="checkbox"/> malware-shiz | 0.0357 | 0.0000 | 0.0000 | 0.0397 |
| <input type="checkbox"/> malware-karagany | 0.0259 | 0.0000 | 0.0000 | 0.0288 |
| <input type="checkbox"/> malware-cve-2017-11882 | 0.0093 | 0.0000 | 0.0000 | 0.0103 |

Other indicators like server name, IP address, and port are also evaluated as part of the fingerprinting process. We walk through a full investigation of an EVE event in a later section.

Discovered Applications

Cisco Secure Firewall detected over 2,000 different applications during RSAC 2025, with the number of unique applications concurrently seen on the Network spiking during conference hours each day.

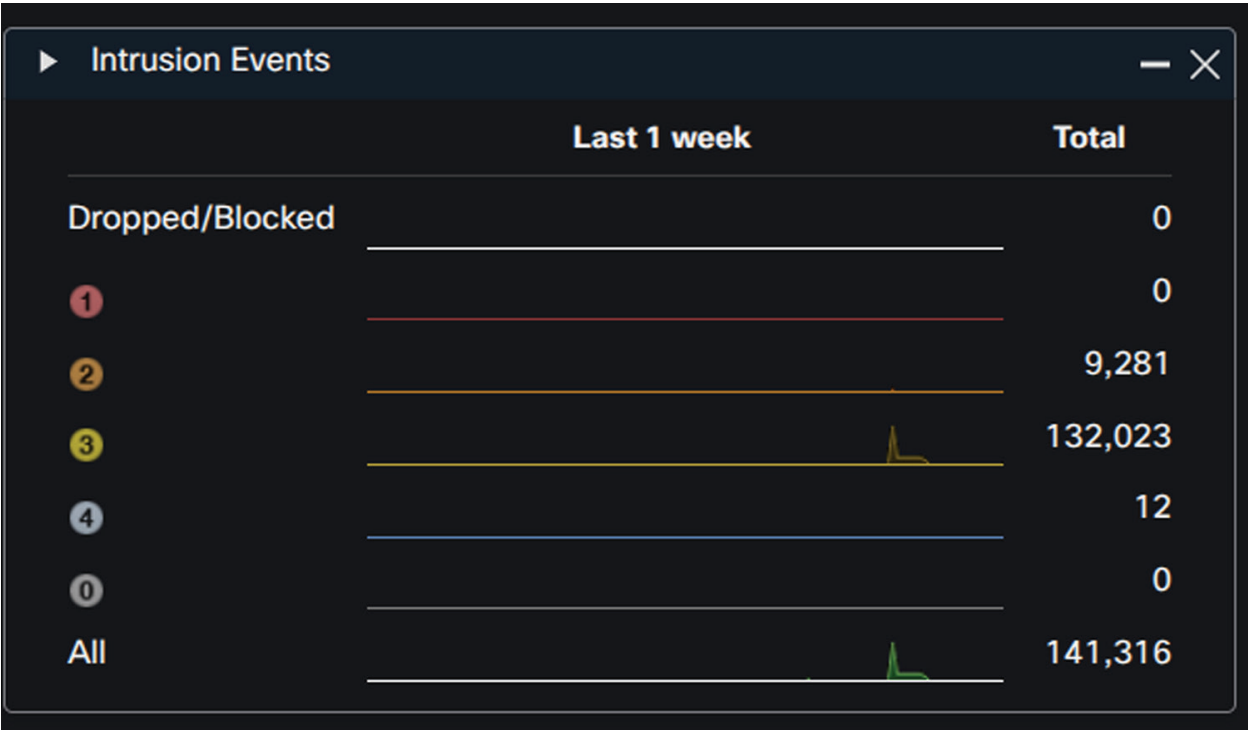
Top client and web applications by traffic were similar to those seen in 2024, with Apple again taking the top spot. Dropbox and YouTube also managed to exceed a terabyte of Network traffic over the course of the conference.



These statistics are for the Network used at RSAC 2025 only and exclude any users who opted to use mobile data instead. Even so, iCloud and Apple Update each managed to rack up around two terabytes of data each over the Network.

Threat Detection

Cisco Secure Firewall detected many (attempted) intrusion events during the conference. These included a significant number of hits for SnortML, which delivers a machine learning approach to detecting attack types like SQL injection without relying on string matches like traditional Intrusion Detection System (IDS) rules. Freeing IDS from string match criteria enables detection of a broader scope of different attack permutations that wouldn't be possible at scale with traditional rules.



All Intrusion Events

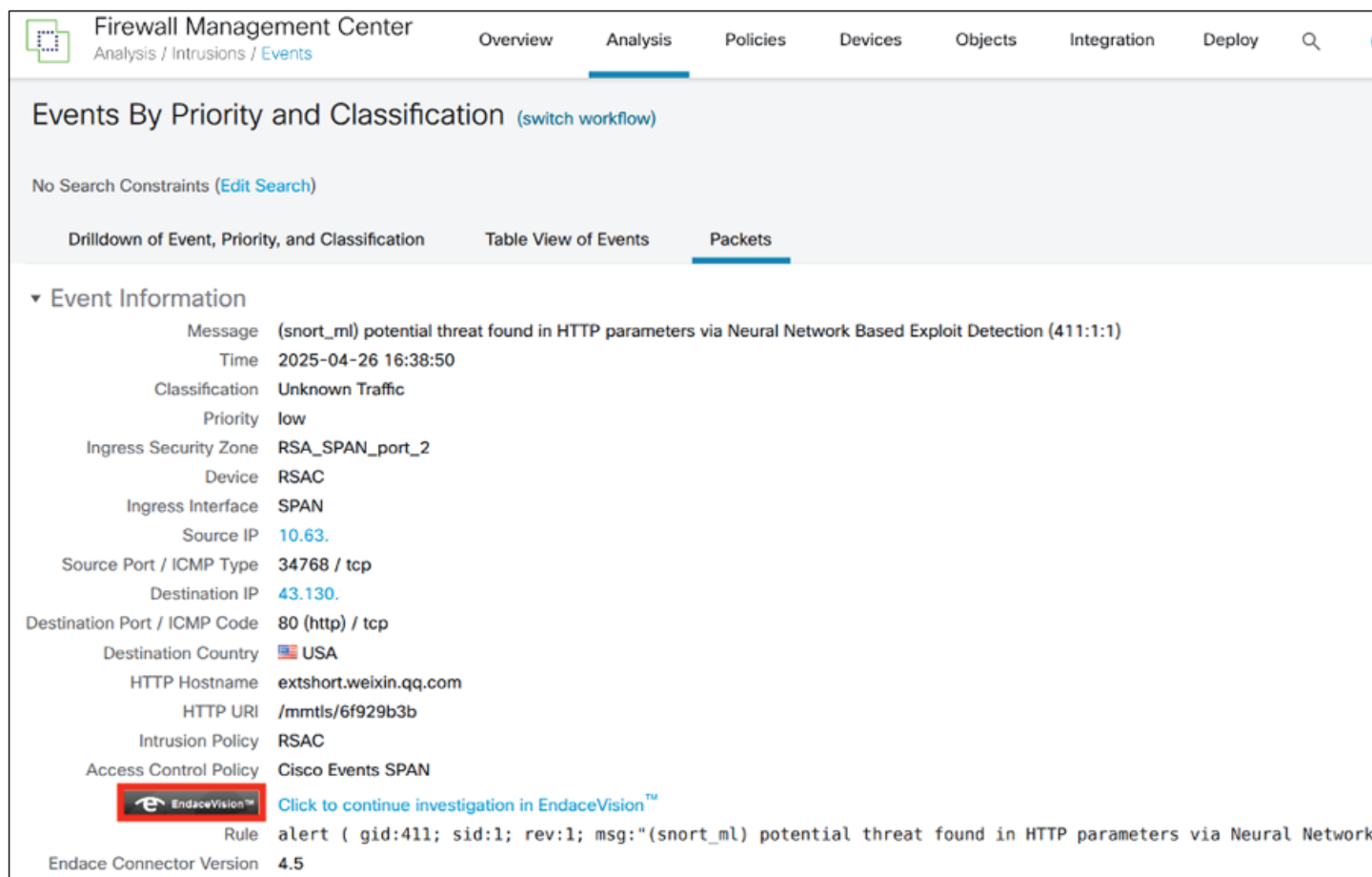
| Message | Count |
|---|-------|
| SERVER-WEBAPP generic server HTTP Auth Header buffer over (snort_ml) potential threat found in HTTP parameters via Neural | 6,322 |
| INDICATOR-COMPROMISE suspicious .null dns query (1:48666: | 589 |
| PROTOCOL-IMAP fetch overflow attempt (1:3070:13) | 440 |
| SMTP_COMMAND_OVERFLOW (124:1:2) | 251 |
| | 151 |

Cisco Secure Firewall can also automate correlation between intrusion and host data, assigning an impact score for individual intrusion events.

For example, if an intrusion event is detected that targets Linux web application servers, and we’ve identified devices with that host profile based on their network traffic, then the impact level will be raised for the intrusion event. This gives SOC analysts an early indicator of the likelihood that an attack may have been successful.

Cisco Secure Firewall and Endace Integration

RSAC 2025 brought a new partnership with Endace for full session packet analysis. Endace has an integration with Cisco Secure Firewall that allows end users to cross-launch from an intrusion event directly into Endace for additional traffic data. While Cisco Secure Firewall always captures the reassembled packet that matched an intrusion rule, sometimes looking at the full session can provide valuable context.



Firewall Management Center
Analysis / Intrusions / Events

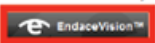
Overview Analysis Policies Devices Objects Integration Deploy

Events By Priority and Classification (switch workflow)

No 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 (411:1:1)
- Time 2025-04-26 16:38:50
- Classification Unknown Traffic
- Priority low
- Ingress Security Zone RSA_SPAN_port_2
- Device RSAC
- Ingress Interface SPAN
- Source IP 10.63.
- Source Port / ICMP Type 34768 / tcp
- Destination IP 43.130.
- Destination Port / ICMP Code 80 (http) / tcp
- Destination Country USA
- HTTP Hostname extshort.weixin.qq.com
- HTTP URI /mmtls/6f929b3b
- Intrusion Policy RSAC
- Access Control Policy Cisco Events SPAN
-  EndaceVision™ Click to continue investigation in EndaceVision™
- Rule alert (gid:411; sid:1; rev:1; msg:"(snort_ml) potential threat found in HTTP parameters via Neural Network
- Endace Connector Version 4.5

However, the existing Endace integration was for firewall version 7.4, and we deployed version 7.6 for RSAC 2025. Our first task was to confirm whether the existing integration worked.

While installing the Endace Connector integration on the Firewall Management Center, we quickly realized the Endace Connector was incompatible with our version. A quick glance through the installation script revealed a simple patch being applied to the packet view script on the FMC. The purpose of this patch is to insert the code responsible for the cross-launch to EndaceVision into the FMC packet view code. Although the installation reported success, we soon found the packet view on the FMC was no longer functional. Luckily, running a quick syntax check on the patched script revealed the error.

```
foreach my $column (grep { $_->{'display'} } @{$sevent->{'columns'}})

#Endace_Integration_Patch begins
if ( $endace_integration_enable )
{
    mkRequest($sevent);
    foreach my $vlink ( @vizlinks )
    {
```

The patch, meant for an earlier version of FMC, had inserted the Endace Connector code between a loop initialization line and its following loop body. A simple moving-around of the inserted code allowed the packet view page on the FMC to function properly once again, now with the EndaceVision cross-launch control.

```
foreach my $column (grep { $_->{'display'} } @{$sevent->{'columns'}})
{
    $retString .= "<tr><th align=left>$column->{'display_name'}</th><td>$column->{'display_data'}</td></tr>";
}

#Endace_Integration_Patch begins
if ( $endace_integration_enable )
{
    mkRequest($sevent);
    foreach my $vlink ( @vizlinks )
    {
```

By now, we had a perfectly working cross-launch from the FMC packet view to EndaceVision, but we wanted to push it further. Can we quickly add custom integration to Unified Events? Here's an example of the URL generated by the Endace Connector on the packet view:

```
https://<redacted>/vision2/pivotintovision/?datasources=tag%3Arotation-
file&title=(snort_ml)%20potential%20threat%20found%20in%20HTTP%20parameters%20
via%20Neural%20Network%20Based%20Exploit%20Detection:411:1:1%20from%20RSAC&start=1745-
709521000&end=1745711621000&tools=conversations_by_ipaddress%20trafficOverTime_by_
app&ip_conv=<redacted>%26<redacted>
```

This URL can be templated and contains variable data about the intrusion event. Fortunately, creating custom cross-launches based on URL templates is an existing feature in Unified Events on the FMC, but with limited available parameters. Parameters such as the source and destination IP addresses are already available while creating Contextual Cross-launches. To support the EndaceVision URL, we needed parameters for the intrusion message, referred to as “title” in the generated URL, as well as start and end times. We were able to slightly modify the FMC to support these required parameters, creating a new Contextual Cross-launch from Unified Events to EndaceVision live at the SOC at RSAC 2025.

| Firewall Management Center | | | | | |
|---|------------|---|-----------|----------------|--|
| Analysis / Unified Events | | | | | |
| OverviewAnalysisPoliciesDevicesObjectsIntegration | | | | | |
| EventsTroubleshooting | | | | | |
| Event TypeIntrusion | | | | | |
| 603 events | | | | | |
| Time | Event Type | Intrusion Message | Source IP | Destination IP | |
| 2025-04-26 19:44:11 | Intrusion | INDICATOR-COMPROMISE suspicious... | 10.63. | 10.8. | |
| 2025-04-26 19:39:45 | Intrusion | (snort_ml) potential threat found in H... | 10.63. | 43.175. | |
| 2025-04-26 19:28:33 | Intrusion | INDICATOR-COMPROMIS | | 10.8. | |
| 2025-04-26 19:28:33 | Intrusion | INDICATOR-COMPROMIS | | 10.8. | |
| 2025-04-26 19:25:36 | Intrusion | SMTP_COMMAND_OVER | | 173.194. | |
| 2025-04-26 19:23:41 | Intrusion | (snort_ml) potential threat | | 43.130. | |
| 2025-04-26 19:18:37 | Intrusion | (snort_ml) potential threat | | 142.251. | |
| 2025-04-26 19:12:53 | Intrusion | (snort_ml) potential threat | | 43.130. | |
| 2025-04-26 19:10:25 | Intrusion | SMTP_RESPONSE_OVERFLOW (124:... | 209.68. | 10.65. | |

Malware Detection with the Encrypted Visibility Engine

RSAC 2025 is a challenging conference for firewall monitoring because over 70% of traffic is encrypted, and we don't perform any TLS decryption. While this is good for guest wireless users (you wouldn't want someone decrypting your traffic), it makes detection very difficult for traditional capabilities like Intrusion Detection Systems (IDS/IPS).

Fortunately, Cisco Secure Firewall has a capability called the Encrypted Visibility Engine (EVE) that provides powerful detection capabilities for traffic where TLS decryption isn't possible. With EVE, we can assign fingerprints to encrypted sessions and reach a confidence score regarding whether or not the communicating process is malicious, all without decryption. One of the fingerprints we tracked at the RSA Conference is for the vtflooder trojan. Vtflooder derives its name from a characteristic of spamming file uploads to Virus Total, and variants can also establish remote access and deliver additional malicious payloads. Two EVE events for vtflooder are shown below. Both events have the same source and destination IPs, but the top event is for an HTTP (port 80) connection, and the bottom event is for an HTTPS (port 443) connection.

| Time | Reason | Source IP | Destination IP | Source Port / ICMP Type | Destination Port / ICMP Code | Encrypted Visibility Fingerprint | Encrypted Visibility Process Name | Encrypted Visibility Threat Confidence Score |
|---------------------|--------------------------|-----------|----------------|-------------------------|------------------------------|----------------------------------|-----------------------------------|--|
| 2025-04-30 09:39:21 | Encrypted Visibility IoC | 10.63 | 195.181 | 53114 / tcp | 80 (http) / tcp | ts/1/(0303)[c030c02c | malware-trojan-vtflooder | 100% |
| 2025-04-30 09:39:21 | Encrypted Visibility IoC | 10.63 | 195.181 | 53113 / tcp | 443 (https) / tcp | ts/1/(0303)[c030c02c | malware-trojan-vtflooder | 100% |

For these connections, EVE assigned a fingerprint to the session associated with the vtflooder trojan, alongside a 100% confidence score that the underlying session was malicious. Case closed!

Well, a big part of SOC work is determining the why and the how, and separating true positives from false positives, so let's dig a little deeper. If we expand one of these events, we can see additional details on what EVE detected.

The screenshot displays a network security interface with a dark theme. At the top, 'TLS Client-offered ALPN' is shown with the value 'anydesk/7.1.6/windows' highlighted by a red rectangle. Below this is an 'Application' section containing a table of metadata:

| | |
|-------------------------------|--|
| Application Protocol Category | network protocols/services |
| Application Protocol Tag | SSL protocol, allows remote connect, file sharing/transfer, opens port |
| Client Application | SSL client |
| Client Application Category | web browser |
| Client Application Tag | SSL protocol |

Below the table is a '▼ Enrichments' section. Underneath, the 'MITRE | ATT&CK® Enterprise' framework is displayed with a progress indicator. A red rectangle highlights the following items:

- ▼ TA0011: Command and Control
 - T1573: Encrypted Channel

Above, we can see that EVE detected the use of the AnyDesk remote access program, which can be used for both legitimate and malicious access to Windows operating systems. The vtflooder trojan is Windows-based, so use of AnyDesk fits the host profile. We can also see that the firewall has associated this event with Command and Control > Encrypted Channel in the MITRE ATT&CK framework, which fits with both a remote access trojan and the use of AnyDesk.

Can we confirm EVE's assessment that the communication was generated by AnyDesk? One way to do this would be if we had access to the endpoint, but we don't have endpoint access for the guest wireless users at RSAC 2025. Another potential way is to pull the full session captures we collected with Endace. Let's look at the HTTP port 80 session from one of the EVE events shown above.

| Source | Destination | Protocol | Length | Info |
|--------|-------------|----------|--------|---|
| 10.63. | 195.18 | TCP | 70 | 53114 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 195.18 | 10.63. | TCP | 70 | 80 → 53114 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128 |
| 10.63. | 195.18 | TCP | 64 | 53114 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0 |
| 10.63. | 195.18 | TCP | 331 | 53114 → 80 [PSH, ACK] Seq=1 Ack=1 Win=131328 Len=273 |

| | | | |
|---|------|-----|-----|
| ts), 331 bytes captured (2648 bits) on interface Port A (ERF Host ac1f6b6e3f6 | 0000 | ... | ... |
| 4:13:ea:97:de:b1), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01) | 0010 | ... | ... |
| 0.63. | 0020 | ... | ... |
| Port: 53114, Dst Port: 80, Seq: 1, Ack: 1, Len: 273 | 0030 | ... | ... |
| | 0040 | ... | ... |
| | 0050 | ... | ... |
| | 0060 | ... | ... |
| | 0070 | ... | ... |
| | 0080 | ... | ... |
| | 0090 | ... | ... |
| | 00a0 | ... | ... |
| | 00b0 | ... | ... |
| | 00c0 | ... | ... |
| | 00d0 | ... | ... |
| | 00e0 | ... | ... |
| | 00f0 | ... | ... |
| | 0100 | ... | ... |
| | 0110 | ... | ... |
| | 0120 | ... | ... |
| | 0130 | ... | ... |
| | 0140 | ... | ... |

We can see from the traffic that our internal IP address established a Transmission Control Protocol (TCP) three-way handshake with an external server, then began an AnyDesk connection with the fourth packet. The usage of HTTP would allow us to see all the communication in plain text and determine more information. However, the HTTP session was quickly terminated and an HTTPS session began (the HTTPS session is the second EVE event shown in the initial screenshot). Even though the HTTPS session is encrypted, we can again see the use of AnyDesk via the Client Hello packet.

| Source | Destination | Protocol | Length | Info |
|--------|-------------|----------|--------|--|
| 10.63. | 195.18 | TCP | 70 | 53113 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM |
| 195.18 | 10.63. | TCP | 70 | 443 → 53113 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128 |
| 10.63. | 195.18 | TCP | 64 | 53113 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0 |
| 10.63. | 195.18 | TLShv1 | 331 | Client Hello |

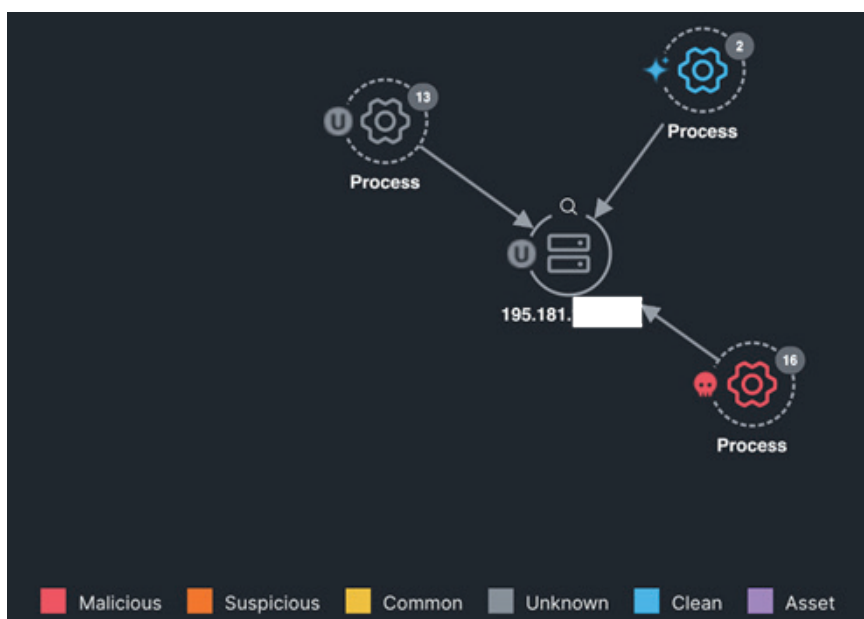
| | | | |
|--|------|-----|-----|
| ts), 331 bytes captured (2648 bits) on interface Port A (ERF Host ac1f6b6e3e | 0000 | ... | ... |
| 4:13:ea:97:de:b1), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01) | 0010 | ... | ... |
| 0.63. | 0020 | ... | ... |
| Port: 53113, Dst Port: 443, Seq: 1, Ack: 1, Len: 273 | 0030 | ... | ... |
| | 0040 | ... | ... |
| | 0050 | ... | ... |
| | 0060 | ... | ... |
| | 0070 | ... | ... |
| | 0080 | ... | ... |
| | 0090 | ... | ... |
| | 00a0 | ... | ... |
| | 00b0 | ... | ... |
| | 00c0 | ... | ... |
| | 00d0 | ... | ... |
| | 00e0 | ... | ... |
| | 00f0 | ... | ... |
| | 0100 | ... | ... |
| | 0110 | ... | ... |
| | 0120 | ... | ... |
| | 0130 | ... | ... |
| | 0140 | ... | ... |

So, we've confirmed the EVE event detail that the session is using AnyDesk. The HTTPS session continued for much longer than the initial HTTP connection, obscuring our visibility. Can we further strengthen our evidence that the use of AnyDesk is malicious? We're once again limited by not having an endpoint client running on the host that made the connection, but one thing we can do is utilize threat intelligence aggregated across the Cisco community to give us additional context on what we're seeing in our own monitored network. Let's pivot to Cisco XDR and search for the server IP address.

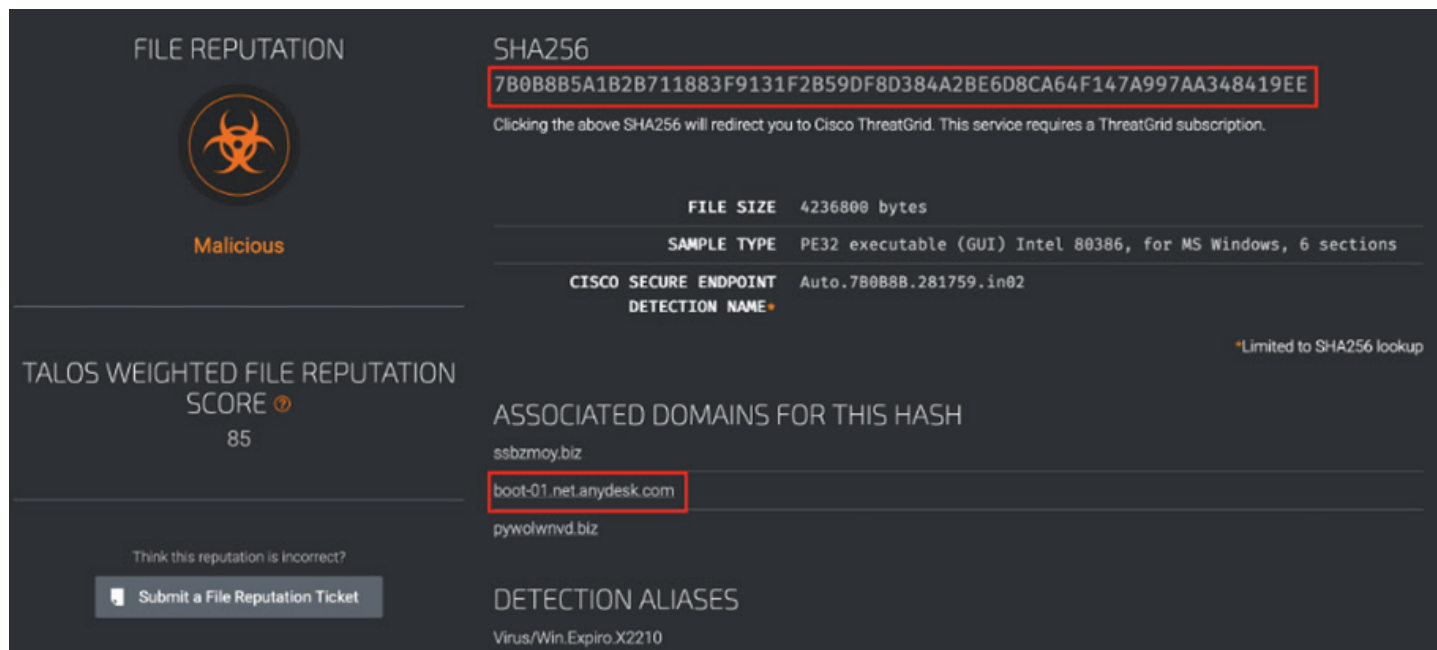
XDR shows that the public IP our device connected to also received connections from 16 different malicious processes. While the lack of an endpoint agent prevents us from confirming what process launched AnyDesk in our investigation, XDR has aggregated valuable threat intelligence for us based on endpoint and sandbox data from hosts that are monitored.

The two things that should jump out to us from the screenshot above are (a) malicious processes are connecting to the same external server we're investigating, and (b) the connections launched by malicious processes account for over half of the connections reported by XDR.


Let's drill down on the malicious processes.



In all 16 cases, XDR has recorded a SHA256 hash for the files that launched malicious connections to the public IP we're investigating. All of these files can offer us context for our investigation, but we'll skip right to the one highlighted in red and check it on [Talos Threat Intelligence](#).



The screenshot displays the Talos Threat Intelligence interface for a file with a reputation of 'Malicious' and a score of 85. The file's SHA256 hash is highlighted in red. The interface also shows associated domains, including 'boot-01.net.anydesk.com' which is also highlighted in red, and detection aliases like 'Virus/Win.Expiro.X2210'.

| FILE REPUTATION | SHA256 |
|---|---|
|  Malicious | 7B0B8B5A1B2B711883F9131F2B59DF8D384A2BE6D8CA64F147A997AA348419EE <small>Clicking the above SHA256 will redirect you to Cisco ThreatGrid. This service requires a ThreatGrid subscription.</small> |

| FILE SIZE | 4236800 bytes |
|--------------------------------------|---|
| SAMPLE TYPE | PE32 executable (GUI) Intel 80386, for MS Windows, 6 sections |
| CISCO SECURE ENDPOINT DETECTION NAME | Auto.7B0B8B.281759.in02 |

TALOS WEIGHTED FILE REPUTATION SCORE 85

ASSOCIATED DOMAINS FOR THIS HASH

- ssbmoy.biz
- boot-01.net.anydesk.com**
- pywolwrvd.biz

DETECTION ALIASES

- Virus/Win.Expiro.X2210

Think this reputation is incorrect?
[Submit a File Reputation Ticket](#)

*Limited to SHA256 lookup

And highlighted above we can see this malicious file also leverages AnyDesk, a direct match to the threat profile we've been building. While we would still need access to the endpoint to fully confirm the malware, these pieces of evidence give us a high degree of confidence that the initial malware assessment from EVE is correct. In a corporate environment, we would immediately move to isolate the host and confirm whether it is infected. At RSAC 2025, we assess the network connectivity of the end user and notify them of the potential compromise of their device if we can identify them via their network traffic.

Tales of Insecurity

During the RSAC Conference, we observe evidence each year that the common cybersecurity best practices are not fully adopted. Often, users trust vendors or engineers to secure their communications and network connections, but they ignore what a system is doing under the hood. They are not fully aware that the best securities are sometimes ignored.

POP3 Will Not Die (Nor will Unsecure IMAP and SMTP)

Each year, we're still stunned to see email being transported via the POP3 protocol. POP3 was designed before anyone was truly concerned about security; the industry's best practice is to turn this protocol off on mail servers. We encourage all email administrators to disable POP3.

Of the many insecure emails sent in the clear on the Network during RSAC 2025, we choose two examples to highlight the seriousness of the issue. In each case, the SOC Team was able to contact the email owner and advise them on best practices to secure their email.

- Non-public car manufacturing documents
 - The SOC Team observed an attendee receiving POP3 email in the clear for two accounts. One of the accounts was a work email for a person who worked at a car dealership in Florida.
 - The SOC Manager called the person in Florida, identified themselves and asked if their spouse was an attendee of the RSAC 2025. Confirming the spouse was an attendee, the person was advised that their work email was observed in the clear, including attachments containing non-public documents from their employer, a major automobile manufacturer in the United States.
 - The spouse in Florida was requested to notify their spouse attending RSAC 2025 and to visit the SOC. The spouse at RSAC 2025 visited the SOC the same day and was advised of the two email accounts sending and receiving email in the clear with POP3. The attendee took remedial action by deleting both email accounts from their mobile device.
- Sponsor demo environment emails
 - The SOC Team observed an attendee receiving unencrypted email pertaining to a sponsoring company of RSAC 2025.
 - The emails were in relation to a cyber challenge environment hosted by the sponsoring company. The emails were sent through a domain setup by an employee to communicate with customers. Email communication and the password were in plain text on the Network.
 - The SOC Team notified representatives of the company and invited them to the SOC. The findings were discussed, and the company took steps to secure the domain and email.

Many other unencrypted emails were observed on the Network and the SOC Team worked diligently to notify the affected attendees.

Unsecure Security Cloud

Each year, the SOC Team observes websites that are accessed via HTTP over port 80 or 8088. Data transmitted in this unencrypted manner can be viewed by anyone on the Network. We observed two web management portals, used by sponsoring companies at RSAC 2025, where the username and password for the cloud-based or cloud-managed security tools were transmitted in the clear, before switching to HTTPS. The user was using the default password of “admin” to connect to and manage firewalls.

| http.request.method==POST | | | | | | |
|---------------------------|-------------|--------|-------------|----------|--------|------------------|
| No. | Time | Source | Destination | Protocol | Length | Info |
| 158 | 65.538188 | 10.63 | 44.200. | HTTP | 782 | POST /login.os H |
| 263 | 66.160773 | 10.63 | 44.200. | HTTP | 640 | POST /menu/sideb |
| 268 | 66.192291 | 10.63 | 44.200. | HTTP | 671 | POST /request/fp |
| 305 | 66.349303 | 10.63 | 44.200. | HTTP | 590 | POST /request/ch |
| 406 | 485.308765 | 10.63 | 44.200. | HTTP | 1479 | POST /approval/a |
| 457 | 523.275528 | 10.63 | 44.200. | HTTP | 626 | POST /menu/sideb |
| 460 | 523.294049 | 10.63 | 44.200. | HTTP | 1479 | POST /approval/a |
| 521 | 544.867178 | 10.63 | 44.200. | HTTP | 626 | POST /menu/sideb |
| 648 | 1984.659056 | 10.63 | 44.200. | HTTP | 626 | POST /menu/sideb |
| 660 | 1984.742191 | 10.63 | 44.200. | HTTP | 1479 | POST /approval/a |
| 761 | 2049.938861 | 10.63 | 44.200. | HTTP | 626 | POST /menu/sideb |
| 777 | 2050.021330 | 10.63 | 44.200. | HTTP | 1479 | POST /approval/a |

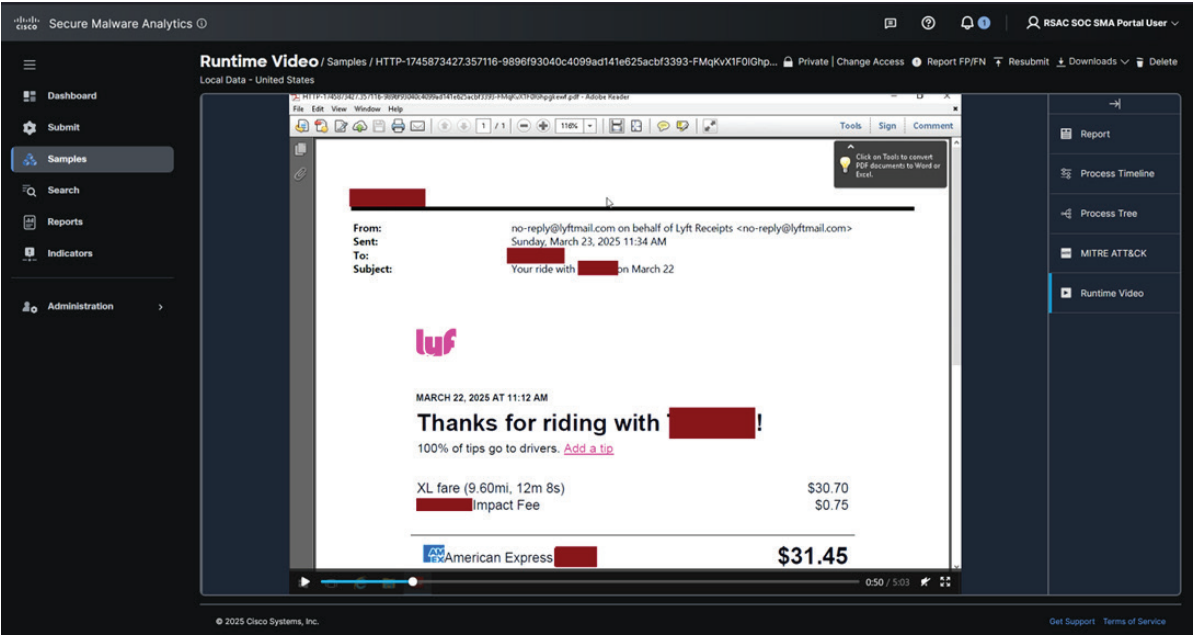
| | | | | | | |
|---|--|--|--|--|--|--|
| Frame 158: 782 bytes on wire (6256 bits), 782 bytes captured (6256 bits) | | | | | | |
| Ethernet II, Src: EFMNetworks, Dst: IE | | | | | | |
| Internet Protocol Version 4, Src: 10.63, Dst: 44.200. | | | | | | |
| Transmission Control Protocol, Src Port: 50059, Dst Port: 8190, Seq: 2037, Ack: 949, Len: 724 | | | | | | |
| Hypertext Transfer Protocol | | | | | | |
| HTML Form URL Encoded: application/x-www | | | | | | |
| Form item: | | | | | | |
| Form item: "password" = "admin" | | | | | | |

A SOC Manager visited one sponsoring company and advised them of the use of HTTP. The person logged in and changed their password, but that was also in the clear, so the SOC Manager returned and advised the company representative that they were still transmitting over HTTP.

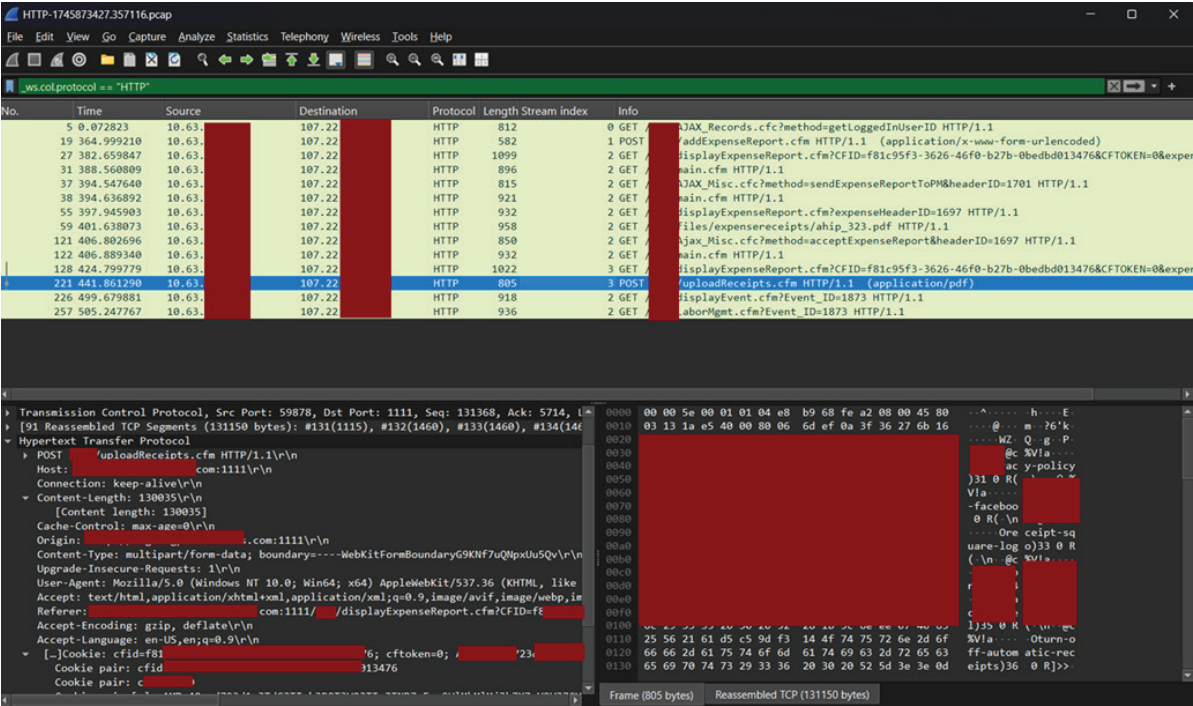
An adjacent sponsoring company was experiencing the same issue: HTTP logon and then switching to HTTPS. The investigation determined both sponsoring companies were using the same web developer. The SOC Team advised them to immediately report the issue to the developer and request a protocol change to HTTPS.

Unsecure Expense Website

At each RSAC Conference, attendees incur expenses for hotel, transportation, dining, and entertainment. Timely reimbursement is essential to keeping business going and the libations flowing.



Expense reporting systems are ubiquitous in the cloud, providing the convenience of uploading receipts and submitting paperless reports.



An event production contractor appeared to be running a non-secured web server for collecting expenses, running on a non-standard port (1111) using HTTP (non-secured).

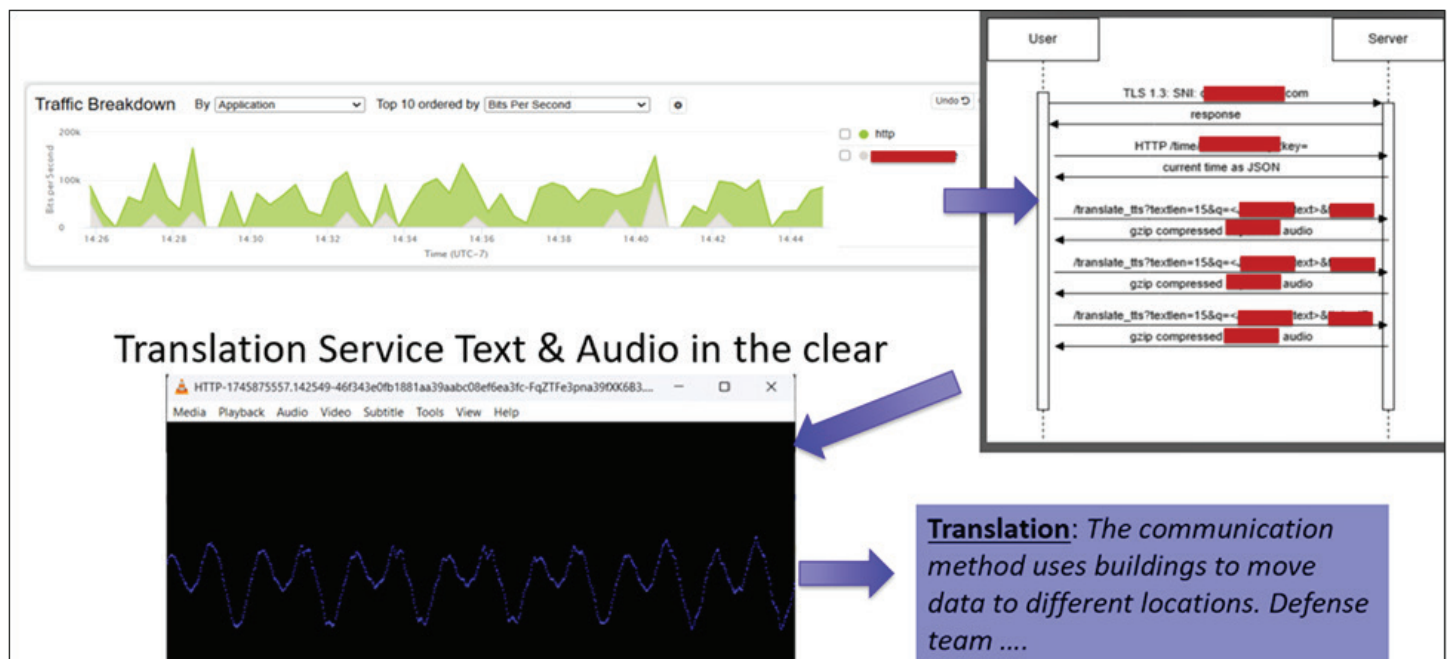
A PCAP file extraction by Endace of a submitted PDF was sent to Splunk Attack Analyzer and Secure Malware Analytics for dynamic analysis. The PDF was of a Lyft receipt for reimbursement. The user was contacted by the SOC Team, who notified them of the unsecure reporting system.

Lost in Translation

The SOC Team was asked by the SOC leaders to look for unencrypted voice transmissions, because in past years we observed Voice over IP conversations in the clear. During their review, the team discovered a 40-minute session that an RSAC 2025 attendee had with a widely used, cloud-based translation service via APIs, which had portions of text and AI generated voice translations in clear text.

We all place a lot of trust in the security of the apps we use. We can imagine a translation app may be used in very sensitive situations where privacy and secrecy are paramount. To learn that information is transmitted in the clear by such an app shakes our confidence and raises serious questions.

In the image below, you can see the HTTP unencrypted traffic in the translation sessions and the APIs communication between text and voice.



Protecting the SOC Infrastructure

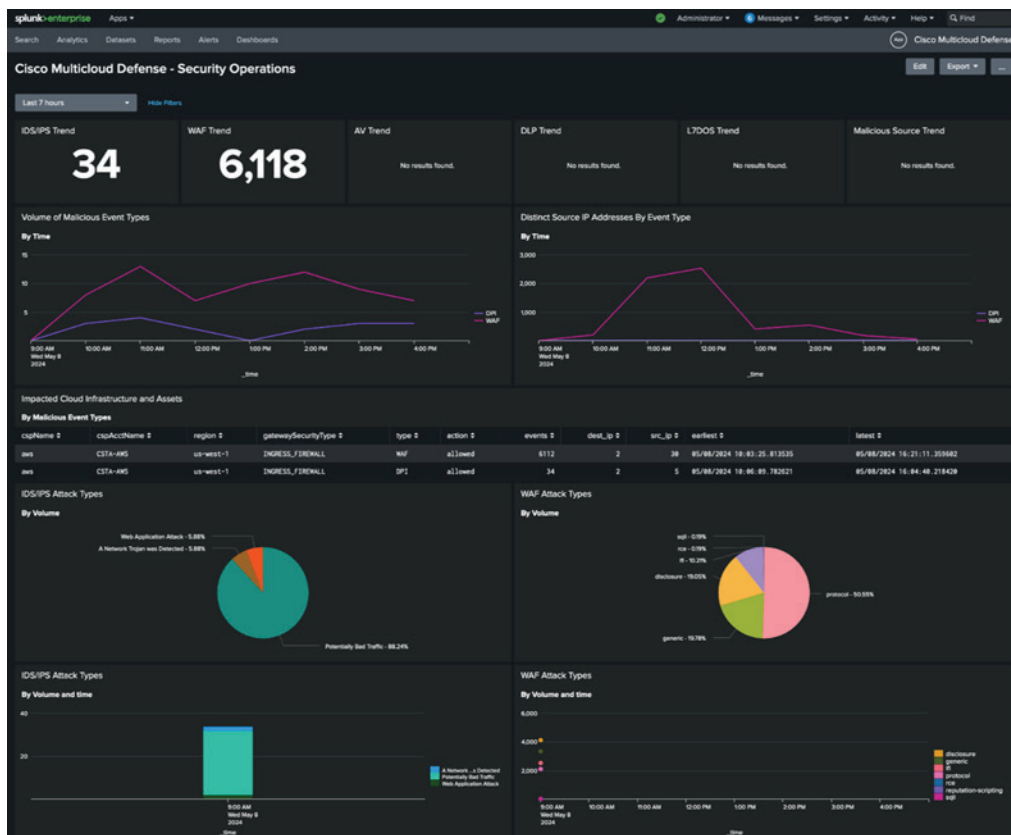
Cloud Protection Events – Malware

After deploying the Multicloud Defense suite, we leveraged Splunk for event visualization and uncovered intriguing findings. Our analysis through the Web Application Firewall (WAF) dashboard revealed malware detection on a cloud asset, with a particular IP address flagged as a potential Trojan. Promptly, we employed XDR and Cisco's Secure Malware Analytics (SMA) to conduct a thorough investigation of the suspicious IP.

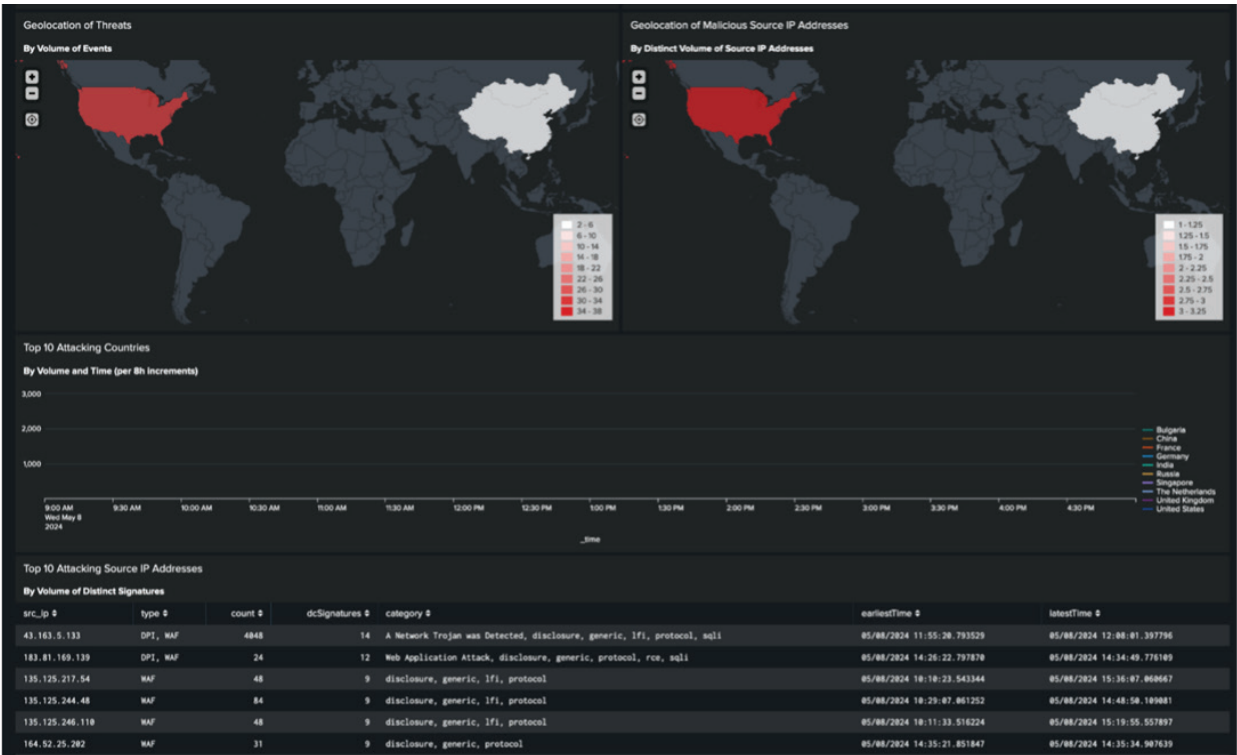
We crafted a controlled experiment within SMA, replicating the suspected Trojan activity within a secure virtual machine environment. The investigation led us to a Chrome browser extension plugin designed for audio control. While SMA's analytical capabilities did not explicitly identify the underlying malware, it did assign a threat score of 75. In conjunction with intelligence from Talos, the threat was categorized as a medium severity level.

Further exploration revealed that the malware was associated with a machine-generated directory that propagated unblockable adware, which aggressively targeted users.

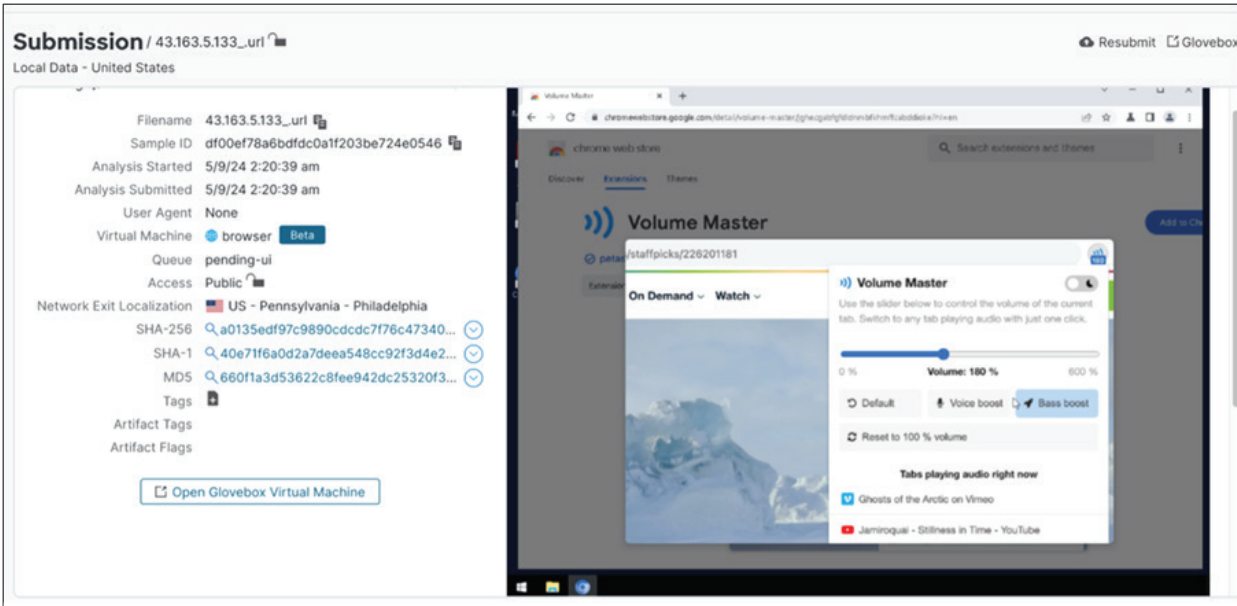
The Splunk Multicloud Defense dashboard presents a comprehensive high-level overview, starting with insights from the Web Application Firewall and supplemented by a suite of complementary log feeds. This integration furnishes a complete and detailed view of the security posture protecting our cloud asset inventory. It meticulously documents all notable events, ensuring that we have a clear and complete picture of the events impacting our cloud environment's security.



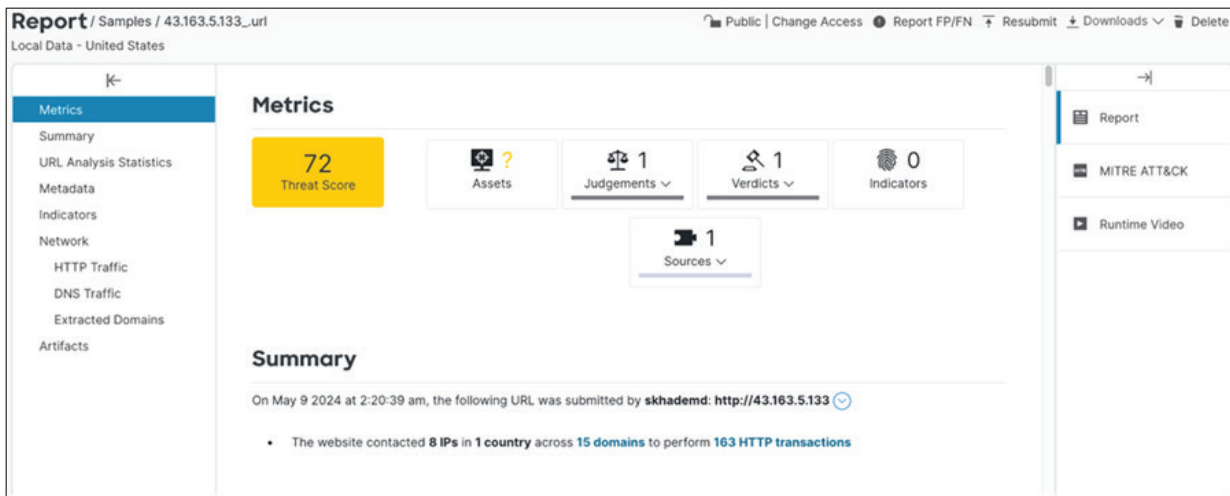
Zeroing in on the specific IDS and File Malware events targeting our cloud assets.



Replaying the malware in Secure Malware Analytics through an XDR investigation.



The report returned the threat score and behavior.



Multicloud Defense

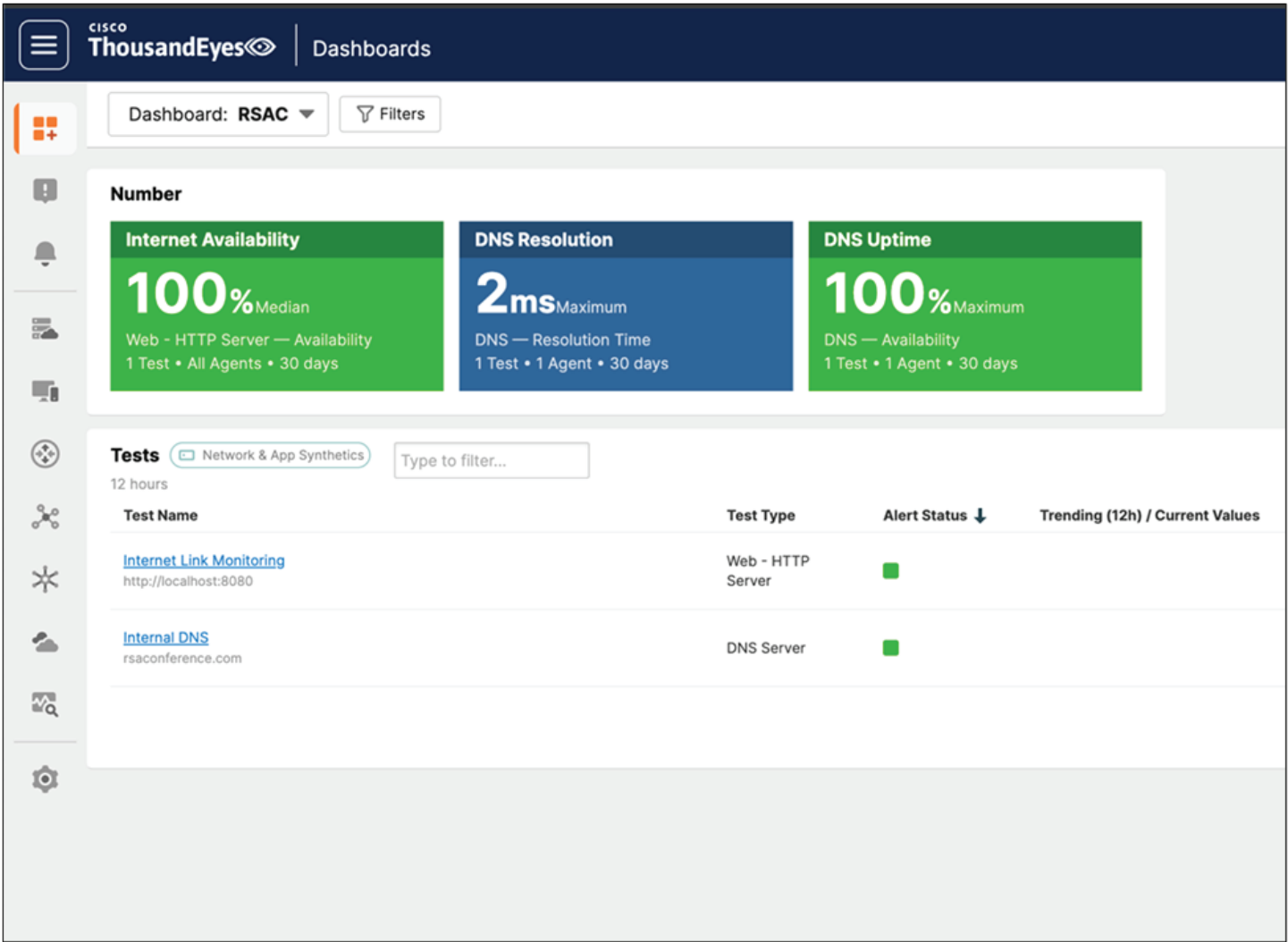
Multicloud Defense is Cisco's cloud native firewall offering. It makes deploying a firewall into the cloud and keeping it highly available easy. It also has similar features to what you would see with our FTD product. Leveraging the ease of deployment and the feature set Multicloud Defense provides, we protected cloud assets from Malicious IPs, injection attacks, and generally monitored the threat levels going to the Amazon Web Services (AWS) deployment.

ThousandEyes

Go ahead, blame the Network

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 has some quick info for us to look at over the last hour.

We can see response time, DNS resolution time, and link speed of our assets and resources in this dashboard. It is useful because we can quickly see what could be an issue and proactively work to figure out what is causing high latency or an outage, in coordination with the NOC.



Workload Security

Cisco Secure Workload (formerly Tetration) is designed to comprehensively address several datacenter operational and security challenges using rich traffic telemetry collected from servers, Layers 4 through 7 service elements, and endpoint devices (such as laptops, desktops, and smartphones). The platform performs advanced analytics using an algorithmic approach to offer a holistic workload protection platform. This algorithmic approach includes unsupervised machine learning techniques and behavioral analysis. The platform provides a ready-to-use solution supporting the following use cases:

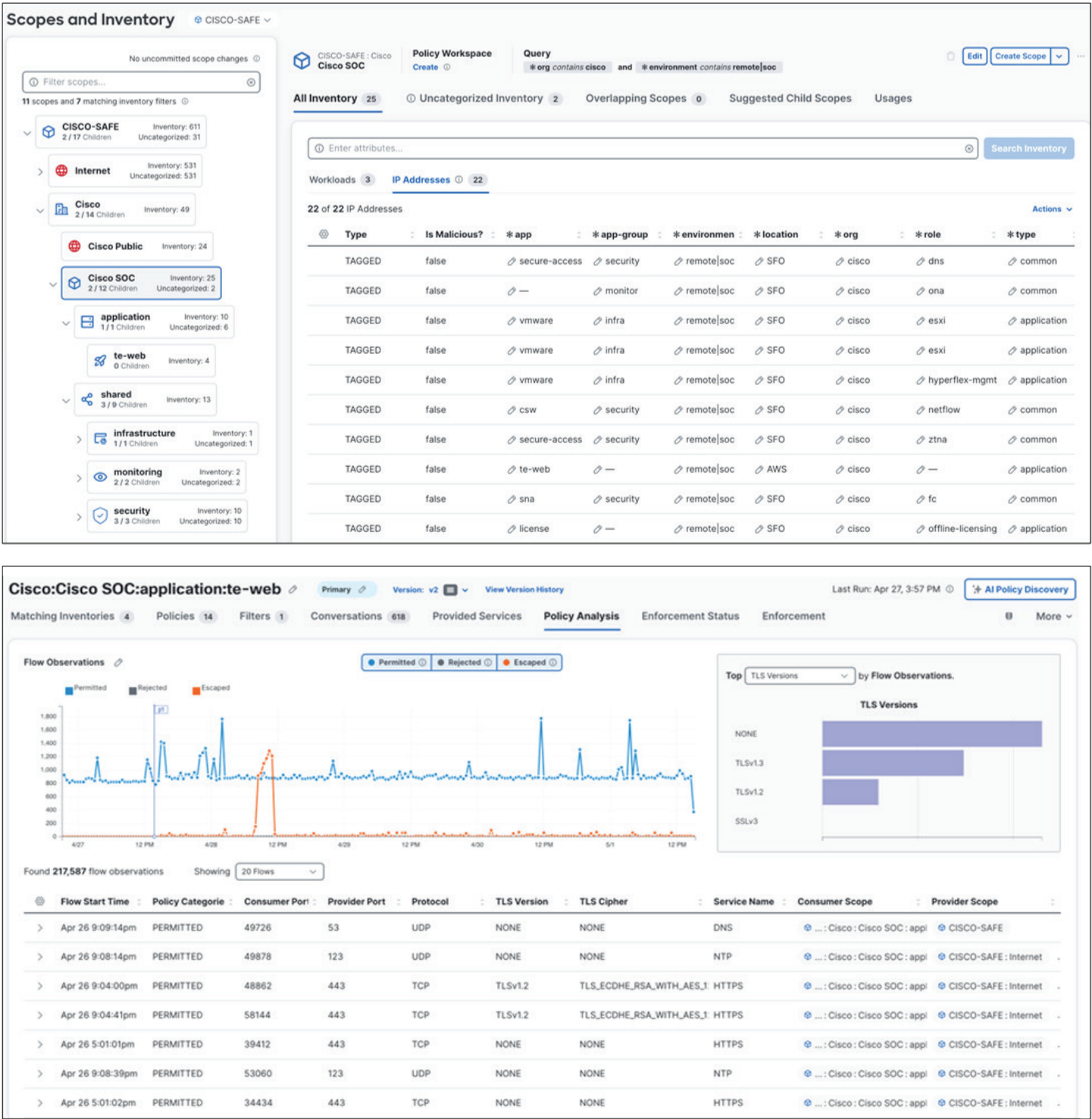
- Provide behavior-based application insight to automate allow-list policy generation.
- Provide application segmentation to enable efficient and secure zero-trust implementation.
- Provide consistent policy enforcement across on-premise data centers, and private and public clouds.
- Identify process behaviors, deviations, software vulnerabilities, and exposure to reduce attack surface.
- Identify application behaviors changes and policy compliance deviations in near-real time.
- Support comprehensive telemetry processing in a heterogeneous environment to provide actionable insight within minutes.
- Enable long-term data retention for deep forensics, analysis, and troubleshooting.

To support the analysis and various use cases within the Cisco Secure Workload platform, consistent telemetry is required from across the data center infrastructure. Rich Cisco Secure Workload telemetry is collected using agents. There are different types of agents available to support both brown-field and green-field data center infrastructures. For the SOC deployment, the following agent types will be considered:

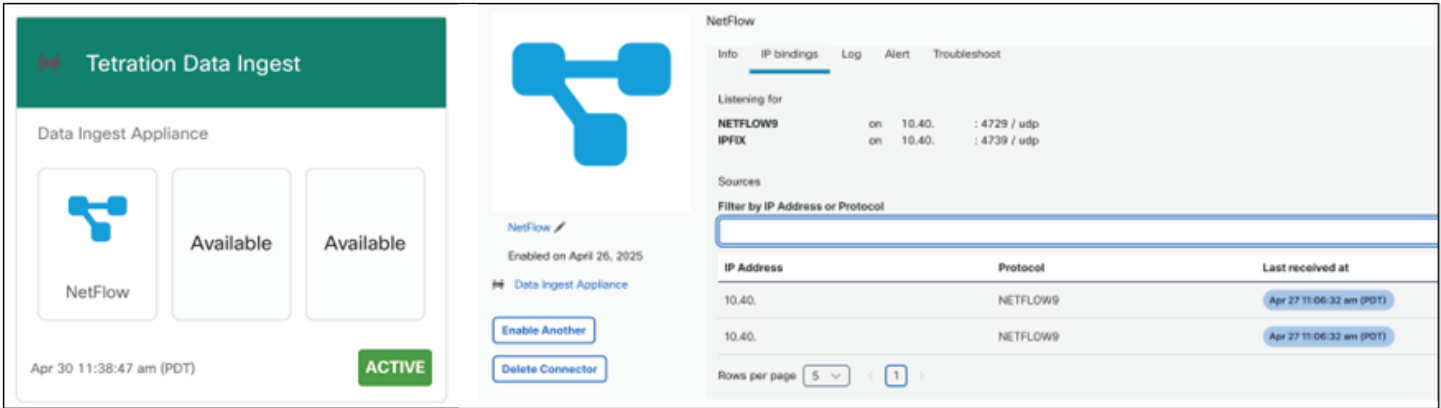
- Software agents installed on virtual machines, bare metal, or container hosts.
- Encapsulated Remote Switched Port Analyzer (ERSPAN) agents that can generate Cisco Secure Workload telemetry from copied packets.
- NetFlow agents that can generate Cisco Secure Workload telemetry based on NetFlow v9 or IPFIX records.

The technical goals and objectives of implementing Secure Workload into the SOC deployment:

- Baseline workload behavior and understanding application dependencies.
- Enable policy development through Application Dependency Mapping (ADM).
- Provide SOC segmentation through workload enforced security policies.
- Retain detailed workload information for troubleshooting, policy, and forensics uses.



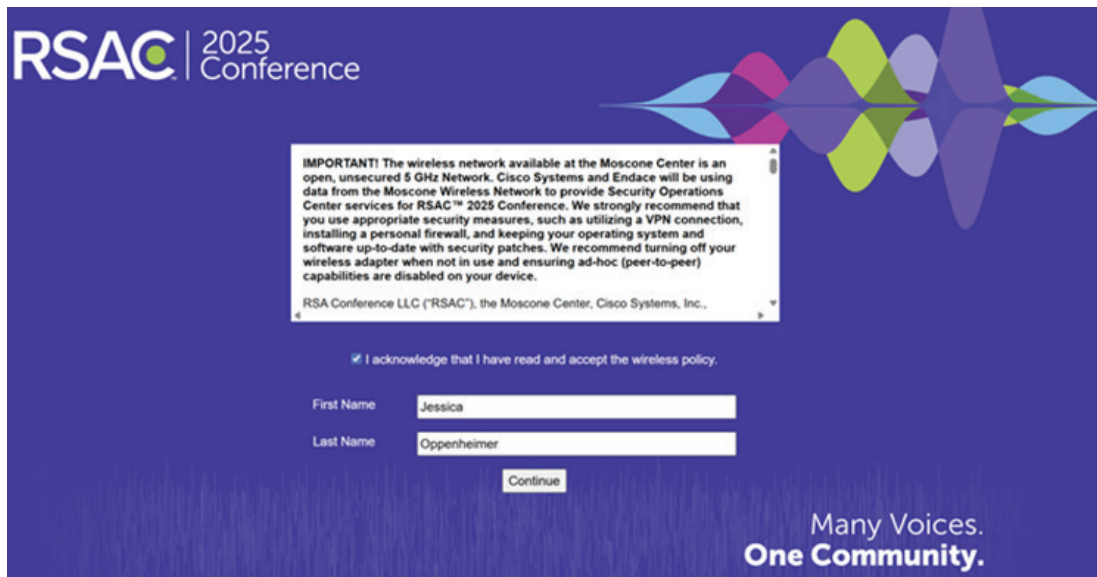
An “Ingest” virtual appliance was deployed within the SOC to allow for the ingestion of Netflow/Network Security Event Logging (NSEL) from Endace and future integrations.



The additional slots available on the Ingest appliance include the ability to accept Network Visibility Module (NVM) telemetry, Internet Protocol Flow Information Export (IPFIX) from Citrix, or F5 BigIP load balancers for flow stitching, and more. With the Cisco Secure Workload (CSW) Agent having process- and package- level information included with connections, the ability to see compliance risk via the dashboard is presented in a clean format for reporting needs.



Conclusion



In the eight RSAC Conferences since 2017, where we've deployed the SOC, we observed some incremental progress in the adoption of encryption and secure protocols. However, both RSAC 2025 and RSAC 2024 had significant declines in encrypted traffic percentages, compared to RSAC 2023 and RSAC 2022.

Our analysis of the data transmitted on the Network reveals a concerning trend: we 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 the unnecessary exposure of critical information that can jeopardize our security.

This year's percentage of encrypted traffic dropped by 6% percent to 74 percent. Also, weak encryption increased to 40% of all encrypted traffic. We need to push this back in the right direction. Encrypt, encrypt ... never trust, and always verify!

As threat actors evolve, we as an industry need to stay ahead of them, which requires ongoing learning and collaboration among 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 2026 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 March 2026!

Acknowledgments

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



Moscone Center Network Operations Center: Jeff Hardy

nthDegree: Sean Shanks

Cisco Staff and Report Contributors

- Jessica (Bair) Oppenheimer – Director, Security Operations and Co-SOC Leader
- Ryan MacLennan, Ivan Berlinson – Innovation – Integrations
- Aditya Sankar and Ben Greenbaum, Ahmadrza Edalat – Breach Protection Suite
- Christian Clasen and Justin Murphy – User Protection Suite
- Adam Kilgore, Brian Shea, and Patrick Whyte – Cisco Secure Firewall, Cloud Protection Suite
- Tony Iacobelli and Richard Marsh – Splunk Cloud Platform, Enterprise Security

Endace Staff and Report Contributors

- Steve Fink – Co-SOC Leader
- Cary Wright – VP Product and Co-SOC Leader
- Barry “Baz” Shaw – Integrations Lead and Engineering Manager
- Stephen Donnelly – CTO
- Caleb Millar and Marshall Patty – Endace Software Engineering
- Tom Leahy – Endace Senior SE
- Michael Morris – Partner Lead, Business Development

Coalfire Threat Hunters

- Neil “Grifter” Wyler, Bart Stump, and Mike Spicer

Authors

Edited by Jessica Oppenheimer, Steve Fink and Cary Wright