

Security Operations Center Findings Report from RSA Conference 2024

Published by Cisco and NetWitness

Edited by Jessica Oppenheimer and Steve Fink,
with Steve Nowell and Alessandro Zatti

Contents

Technology Used in the SOC at RSA Conference	5
SOC in a Box	6
NetWitness Platform	8
Security Cloud	10
The data, by NetWitness	11
Encrypted vs. Unencrypted	11
Cleartext usernames and passwords	12
Stories of insecurity	14
POP3 forever	14
Sit back, relax and enjoy your flight	15
Security by obscurity	16
Home sweet home	17
Unsecure vendor	17
Integration and threat hunting	19
XDR AI Assistant	20
MITRE ATT&CK Heatmap	22
Malware analysis	23
Documents in the clear	24
Security incident and event management	31
NetWitness and Splunk Enterprise Security	31
Splunk and Secure Firewall	32
Recorded future	33
Intrusion detection	37
Port scanning	39
File transfers	41
Malware threats	43
Firepower and NetWitness integration	44
Plaintext playlist	44
Desperately seeking Canon	45
Other firepower statistics	47
Security Cloud	48
Go ahead, blame the network	48
Multicloud Defense	49
Attack Surface Management	50
Conclusion	51
Acknowledgments	52

DISCLAIMER

It is important to clearly understand the role of the security operations center (“SOC”) at RSA Conference (“RSAC”).

- The SOC is an educational exhibit sponsored by NetWitness® (“NetWitness”) and Cisco Systems, Inc. (“Cisco”) that monitors network activity during the course of the RSA Conference event.
- By connecting to Moscone Center public Wi-Fi or using the RSAC mobile application, all RSAC 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. NETWITNESS AND CISCO SYSTEMS WILL BE USING DATA FROM THE MOSCONE WIRELESS NETWORK FOR AN EDUCATIONAL DEMONSTRATION ON A WORKING SOC. WE STRONGLY RECOMMEND THAT YOU USE APPROPRIATE SECURITY MEASURES, SUCH AS UTILIZING A VPN CONNECTION, INSTALLING A PERSONAL FIREWALL AND KEEPING YOUR OPERATING SYSTEM UP-TO-DATE WITH SECURITY PATCHES. WE RECOMMEND TURNING OFF YOUR WIRELESS ADAPTER WHEN NOT IN USE AND ENSURING AD-HOC (PEER-TO-PEER) CAPABILITIES ARE DISABLED ON YOUR DEVICE.).”
- Additionally, RSA Conference advised attendees of the educational SOC in printed materials and onsite signage.
- The SOC is not a true security operations center. The infrastructure at the event is managed by the Moscone Center, which deploys Cisco Umbrella DNS. The SOC has a SPAN of the network traffic from the Moscone Center wireless network (named .RSACONFERENCE). There are limited log files from Cisco Firepower Threat Defense Intrusion Detection System (IDS) because it is not inline; however, the primary data is a real-time mirror of the traffic traversing the wireless network.
- The SOC goal is to use technology to educate RSAC attendees about what happens on a typical open, unsecured wireless network. The education comes in the form of SOC tours, an RSAC session and the publication of this Findings Report, issued by sponsors NetWitness and Cisco.
- The SOC Team at RSA Conference is not part of the RSAC security team. The SOC at RSA Conference acted as an educational exercise and was not intended to protect, mitigate or remediate any issue uncovered during the SOC educational exercise.
- “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 is an open network offered by the Moscone Center.
- The findings of this report and any security issues identified relate to user activity, not the network itself.
- Data collected by the SOC Team at RSA Conference has been wiped and a certificate of completion is held by RSAC.

NOTE: This report was prepared as a summary of the RSA Conference educational SOC exercise. NetWitness Cisco nor any of their employees or subcontractors, makes any warranty, express or implied, 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 disclosed herein, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement or recommendation.

The Network

The RSACONFERENCE wireless network is a flat network with no (as in zero) host isolation. This alone is an important statement and a great 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 to any other devices on the network. Host isolation provides a device 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 RSA Conference

The SOC Team at RSA Conference deployed the [NetWitness platform](#), including NetWitness® Network, NetWitness® Logs and NetWitness® Orchestrator. Also, Engineers used [Cisco Security Cloud](#) in the SOC, comprised of [Cisco Breach Protection Suite](#), [User Protection Suite](#), [Cloud Protection Suite](#), with the foundation of [Secure Firewall](#).

Incidents were investigated with threat intelligence, provided by [Cisco Talos](#), and licenses donated by [Recorded Future](#), [alphaMountain](#), [Pulsedive](#), [IBM X-Force Exchange](#) and community sources.

[Splunk Enterprise Security](#) was utilized as a SIEM in the SOC at RSA Conference for integrations of Cisco Firewall logs, combined with the metadata and intelligence of NetWitness NDR, along with enrichment with Recorded Future, for visibility and investigations with Cisco XDR.

SOC in a Box

The SOC team at RSA Conference only had a day and a half to set up the SOC, which means preparation is 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 we keep the “SOC in a Box” adjacent to the NetWitness physical appliances for ease of integration, and there is room for the NetWitness appliances, should we need to ship them together.

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:

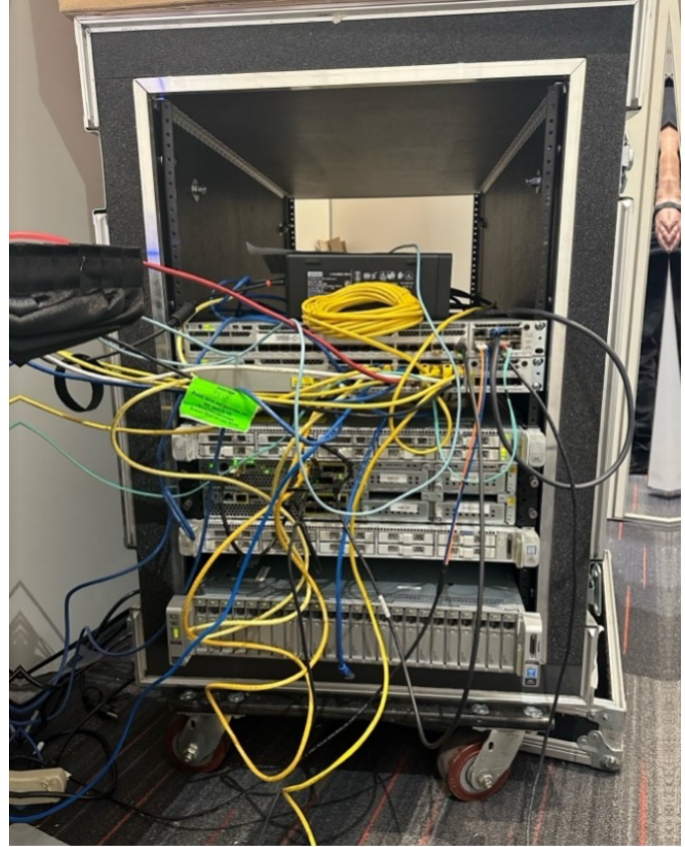
- Switch: Catalyst (24 port)
- Switch: Catalyst 3850 with 10G SFP+ (48 port)
- Firewall: Secure Firewall 4115
- Server: UCS C220 M5
- Server: UCS C240 M4

Here are a few pictures to show the journey from ideation to the SOC at RSA Conference First, preparation in the Cisco lab.





SOC in a Box was shipped to Moscone Center. A 10G SFP Fiber drop was provided to us for visibility into the conference traffic.



The SOC in a Box connected with the Moscone Center NOC and NetWitness Platform. The SOC was fully operational by Monday at 3pm.



Once everything is operational, it is simple enough to get our dashboards up on the big screens!

In the topology shown below, the purple box encompasses the on-premise “SOC in a Box” infrastructure. Starting in the bottom right, the Umbrella Virtual appliances are deployed within the Moscone Network Operations Center. By assigning the virtual appliances as the DNS servers in the DHCP scope all DNS queries on the network are visible to Cisco Umbrella – User Protection Suite.

NetWitness Platform

The SOC Team at RSA Conference utilizes two main components of the NetWitness Platform Network and Logs. NetWitness Platform collects and stores both Network and Log data separately, because the two data types are unique NetWitness generates metadata about the two different data types which becomes a common query language, allowing both Network and Log data to be correlated to find the common thread between them and then stitch them together to create a comprehensive “story” about what’s happening on the network.

NetWitness Logs by itself is a security monitoring and forensics tool that collects, analyzes, reports on and stores log data from a variety of sources to support security. NetWitness Logs parses, enriches and indexes logs at capture time, creating metadata that serves to accelerate alerting and analysis commonly known throughout the industry as SIEM.



NetWitness Network provides real-time visibility into network traffic. It enables detection and threat hunting with streamlined workflows and automated investigation tools used to monitor the timing and movements of threat actors. NetWitness Network utilizes correlation, data science and threat intelligence to detect anomalies and speed up analyst response times. The proprietary capability to reconstruct the full communication sessions permits analysts to perform deep analysis and detection. It allows analysts to have a full picture of the communication and to hunt for threats without ever having to look at the raw packets again. This capability also permits the analyst to extract files as well, even if it’s incapsulated in a non-standard/unknown protocol.

NetWitness collected all the raw network traffic from the Moscone Center network, generated metadata, and visually prioritized threats occurring in real time.

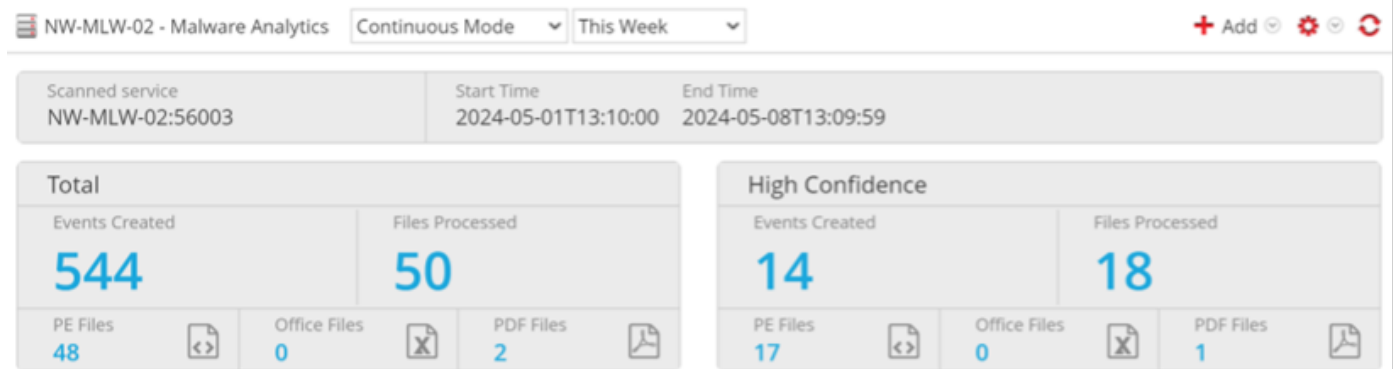
It inspected every network packet session for threat indicators at time of collection and enriched this data with threat intelligence and business context.



To simplify analysts' analysis, a dashboard was created. Starting from dashboards, they can drill from the evidence to the specific events (till the raw packets if needed). Threat intelligence information was also used to implement specific behaviors and trigger real-time alerts to speed up detections.

For suspicious files that might be malicious, NetWitness performed a community anti-virus (AV) lookup, some static analysis, and its own network intelligence. NetWitness Orchestrator, built on ThreatConnect, then sent the files to Cisco Breach Protection Suite - Secure Malware Analytics for dynamic malware analysis.

Summary of Events



Malware Analytics combined 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 RSA Conference had a global and historical view of the malware, its activity, and how large a threat it posed to the RSAC network.

Security Cloud

Cisco Cloud Protection Suite – The Cloud Protection Suite was used to protect an XDR Relay Module used to bring visibility of ThousandEyes agents into XDR. In addition to deploying the Cloud Protection Suite, we added some of the Breach Protection Suite to the cloud deployment to provide additional security.

Using Attack Surface Management, we can see relationships between different assets in the cloud and even on prem. We can use it to see the relationships between firewall rules, VMs, IAM roles, and many more assets. This is useful because we can immediately go into Attack Surface Management and check if there are any firewall rules or roles assigned to VMs that we do or do not want. For example, it is common to use a rule to allow access from anywhere while setting up the environment for the first time. Attack Surface Management notified us the access rule was still there after a few hours and we could see the exact issue in the product. Then we removed the rule since we did not need it anymore.

Secure Application can do something similar but in an interesting way. It maps out these relationships and then shows them as Attack Paths. We can use the attack path to see how an attacker can reach an asset in our cloud account and then work to remediate it proactively instead of after a breach occurs.

Lastly, we have Secure Workload. Secure Workload was used to prevent any unwanted connections from being made to the ThousandEyes relay module and to provide forensics if we detected an issue.

The statistics

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

Year over Year Stats

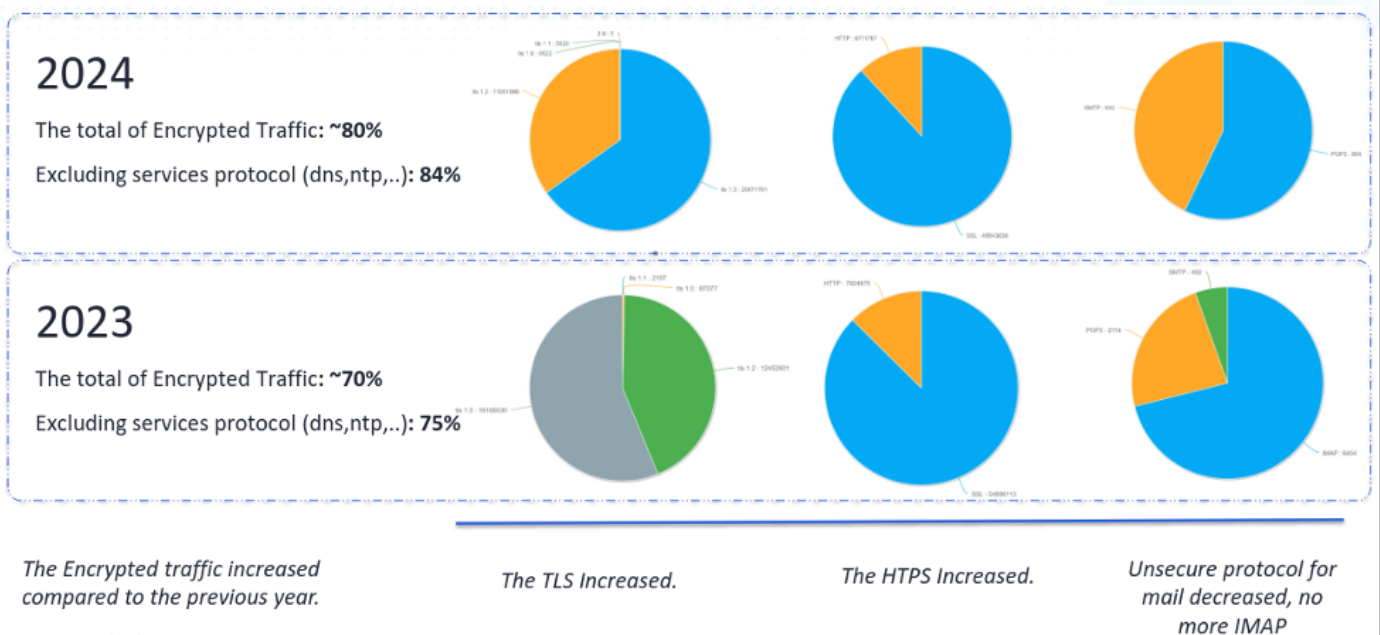
Year	2024	2023	2022
Attendees	~40,000	~39,000	~19,000
Total packets captured	19 billion	18.5 billion	11.8 billion
Total logs captured	39.9 million*	214.7million	108 million
Total sessions	159 million	383 million	187.3 million
Total unique devices	17,034	~40k	13,253
Total packets written to disk	17.24 terabytes	16.26 terabytes	7.39 terabytes
Total logs written to disk	79 gigabytes	774 gigabytes	50.8 gigabytes
Peak bandwidth utilization	2.2 Gbps	1.8 Gbps	1.35 Gbps
DNS Requests	~56.3 million	~53.4 million	~46 million
Total clear text username/passwords	20,916	36,910	55,525
Unique devices / accounts with clear text usernames / passwords	99	424	2,210
Files sent for malware analysis	~50**	7,500+	570+

* Every year at RSAC 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 SIEM, therefore the statistics of total logs captured and total logs stored 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.

** Submitted files from NetWitness to Cisco Secure Malware Analytics are now checked first against known files before submission.

The data, by NetWitness

The SOC Team at RSA Conference started analyzing all wireless traffic on Monday, May 6, and collected traffic through Thursday, May 9, 2024, at 3p.m. There were 159 million sessions during this period. Which was much less than the amount of traffic collected from RSAC 2023, reflecting the drop in the number of devices connected to the network

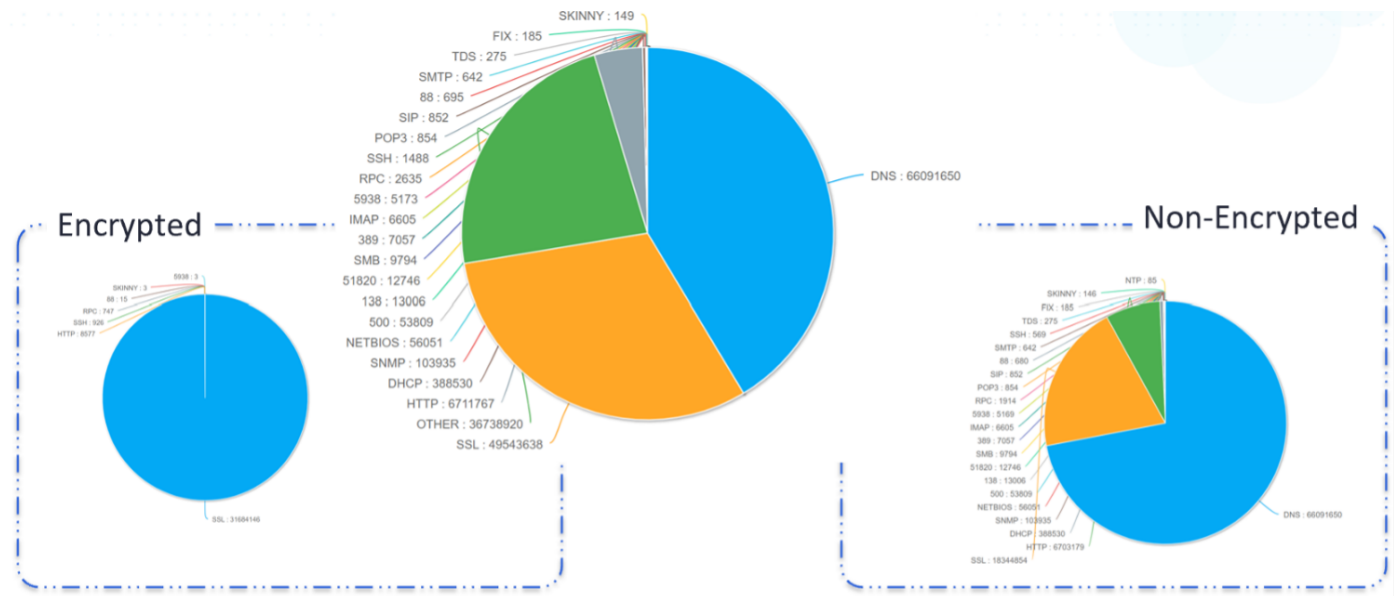


Encrypted vs. Unencrypted

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

The SOC Team at RSA Conference never decrypts/terminates/man-in-the-middle encrypted traffic. The primary goal of the SOC is to educate the attendees in how to better secure their data through encryption.

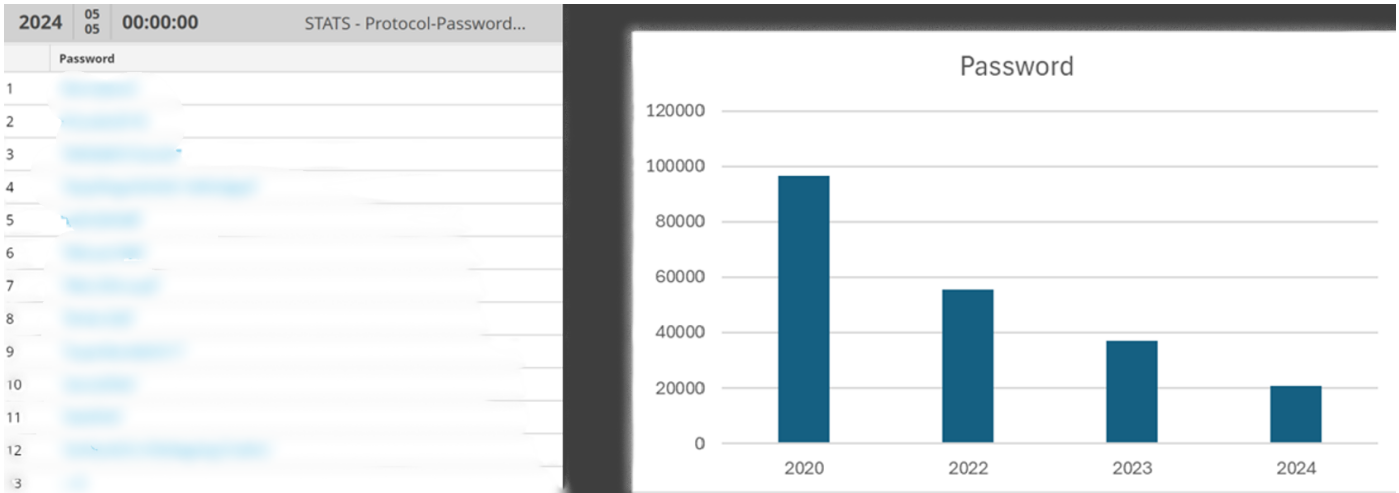
Think of this as north-south and east-west. Encrypting traffic does not necessarily make one more secure, but it does stop individuals from giving away their credentials, and organizations from giving away corporate asset information in the clear.



The role of the RSAC SOC is to help educate RSAC attendees and vendors about the information that is readily available on a public wireless network. In the past, we have spoken to many people on SOC tours about their mobile applications. We have seen mobile applications such as dating and home security video camera applications streaming data in the clear. Authentication to the apps was secure, but once authenticated, the data went back to an insecure transport—and we could see it all. Fortunately, many of these applications, but not all, have been secured and are now using secure protocols post-authentication to secure viewing.

Cleartext usernames and passwords

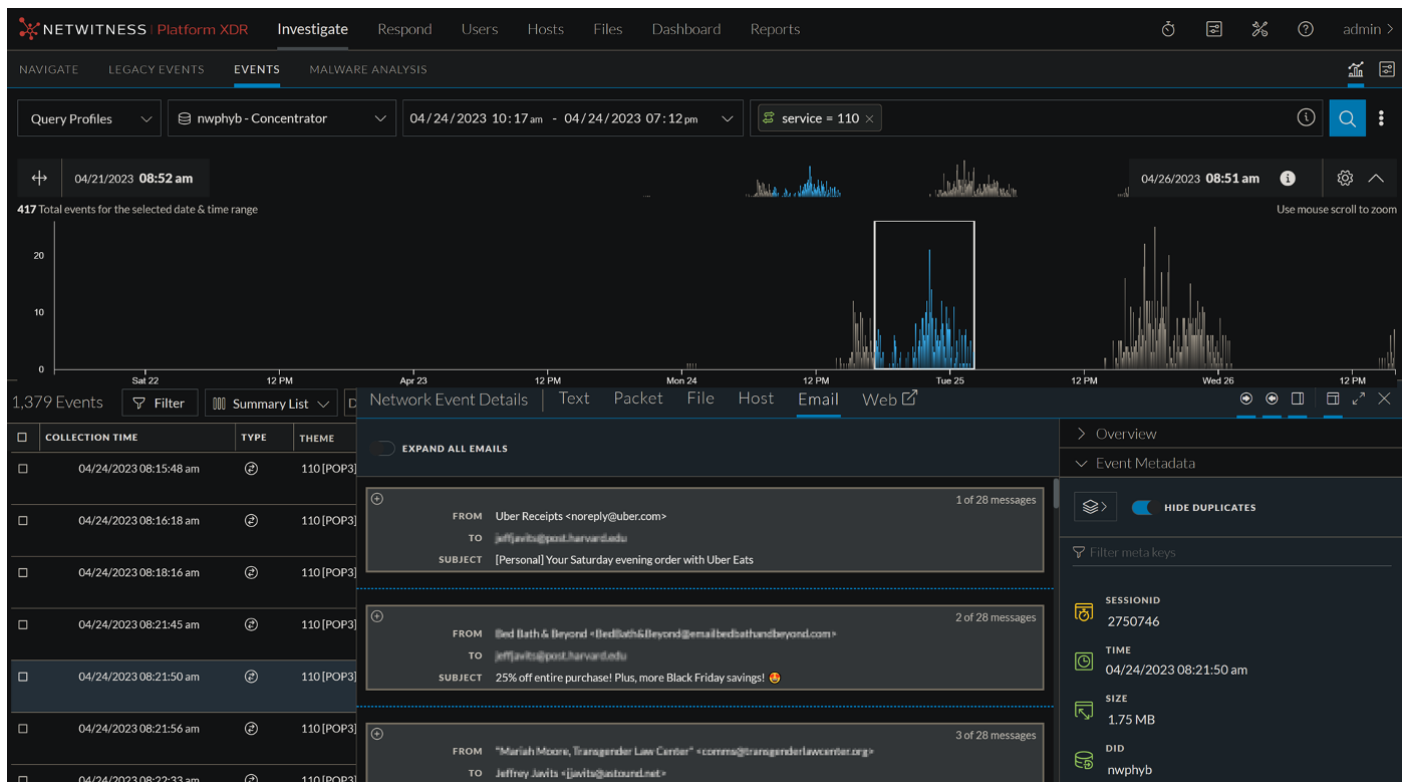
Cleartext usernames and passwords continue to pose a problem. The SOC Team saw 20,916 cleartext passwords (down from 36,910 in 2020) from 99 unique accounts (down from 424 in 2023). Both are an improvement from 2022, with 55,525 clear text passwords.



MITRE mapping



Security events



Stories of insecurity

During RSAC, we observe evidence each year that the common cybersecurity best practices are not fully adopted.

In the actual growing hyperconnected world the number of systems that can be connected to the internet has increased, but the common security best practices are not always implemented. Analyzing the findings of the impression is a missing of the “awareness”, and users are relying on and trusting vendors or engineers, but they ignore what a system is doing under the hood. They are not fully aware that the best securities are ignored. In the following sections we describe evidence of this.

POP3 forever

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

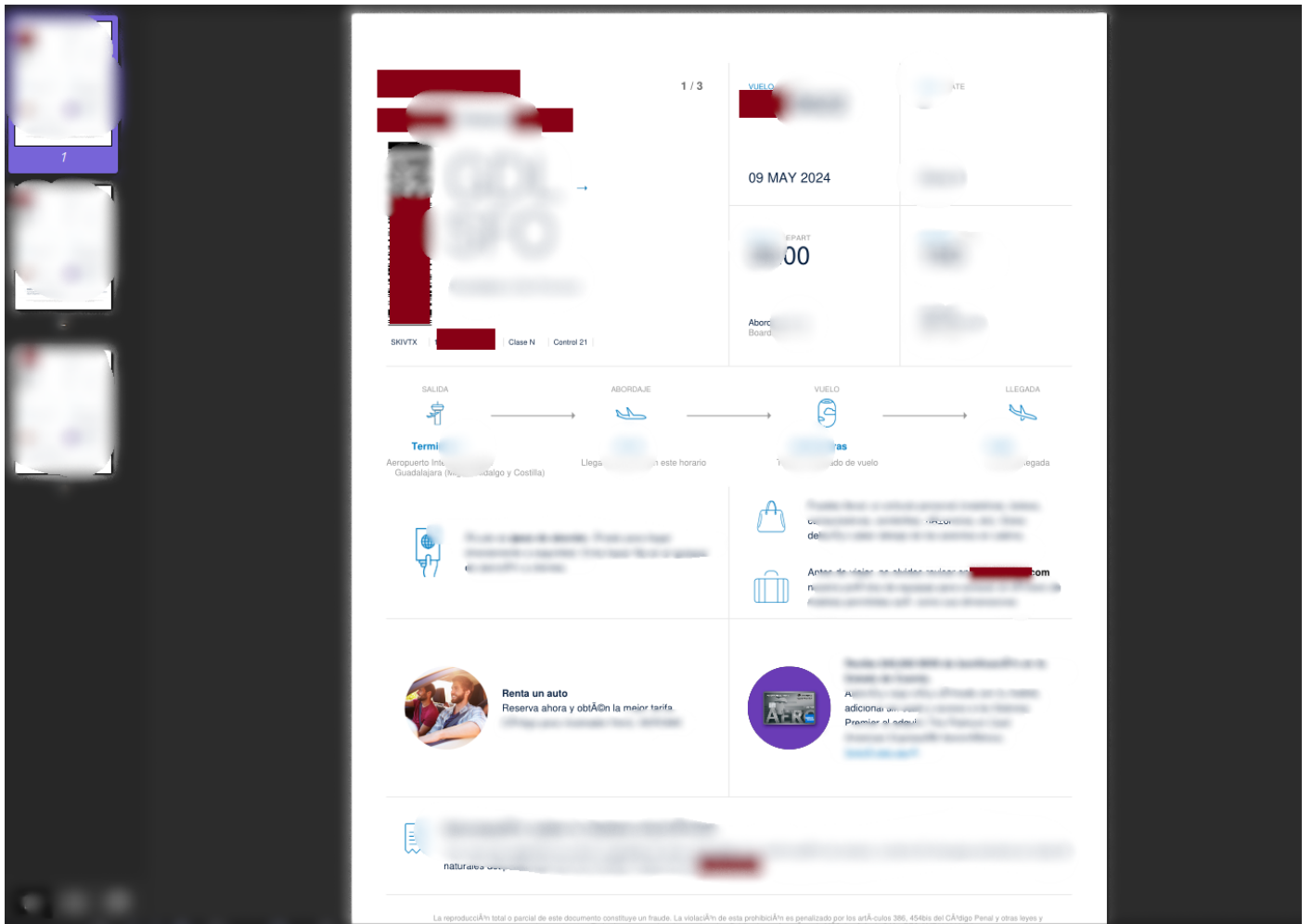
Sit back, relax and enjoy your flight

Using GET methods in web applications has significant security implications. GET requests append data to the URL, making it visible in DNS queries, the browser history, web server logs, and referrer headers, each of these increases the risk of sensitive information exposure. GET requests are also more vulnerable to CSRF (Cross-Site Request Forgery) attacks since they can easily be triggered by loading a URL. Additionally, the ease of manipulating URL parameters in GET requests can be exploited in phishing and social engineering attacks. GET should not be used to transmit sensitive information.

POST requests, on the other hand, include data in the body of the HTTP request, reducing the risk of exposure since the data is not visible in the URL. This makes POST more suitable for actions that change the server state, such as form submissions and financial transactions. However, POST requests can still be vulnerable to CSRF attacks, so implementing additional protection like CSRF tokens is essential. Regardless of the method used, using HTTPS to encrypt data in transit and ensuring proper input validation, session management, and CSRF protection should be part of standard DevSecOps when it comes to web application security.

The screenshot displays the NetWitness Platform interface. At the top, there are navigation tabs for 'Investigate', 'Respond', 'Users', 'Hosts', 'Files', 'Dashboard', and 'Reports'. Below this, there's a search and filter section with 'Saved Queries' and a filter for 'medium = 1 AND ip.all = 23.211'. The main area shows a list of 32 events, with one event selected and its details expanded. The 'Network Event Details' pane shows an HTTP GET request to a host with a redacted IP address. The request headers include 'Connection: keep-alive', 'Cache-Control: max-age=0', 'DNT: 1', 'Upgrade-Insecure-Requests: 1', 'User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36', 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7', 'Accept-Encoding: gzip, deflate', and 'Accept-Language: es-419,es;q=0.9'. The 'Overview' pane on the right shows session ID 159075817, source IP:port 10.65:60217, destination IP:port 23.211:80, and packet statistics.

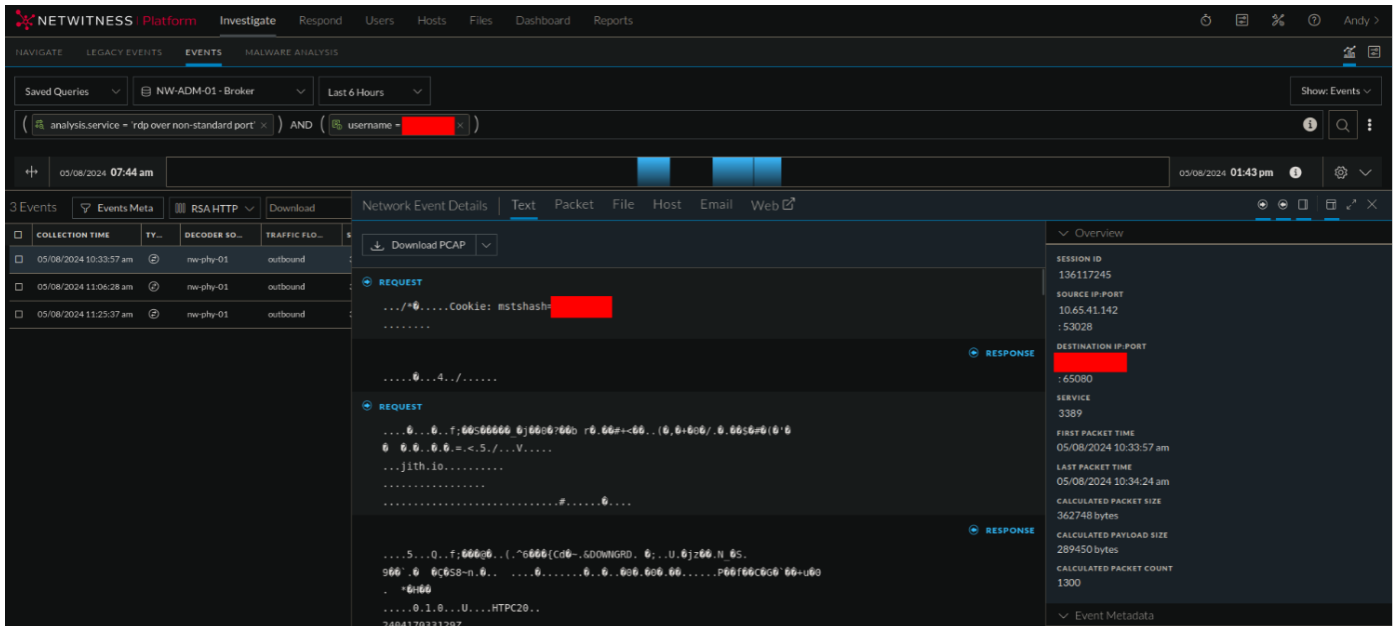
The boarding passes were visible during dynamic analysis (redacted).



Security by obscurity

Changing an insecure application to a non-standard port, often referred to as "security by obscurity," is a misguided attempt to enhance security. This approach relies on the notion that by moving services to uncommon ports, potential attackers will be less likely to find and exploit them. However, this method fails to address the underlying vulnerabilities within the application itself. Skilled attackers can easily discover services running on non-standard ports through port scanning tools and techniques, rendering the strategy ineffective. Security by obscurity provides only a superficial layer of protection and can create a false sense of security, leading organizations to neglect essential security practices like proper configuration, patching, hardening of the application and encrypting the data both in transit and at rest.

True information security requires a comprehensive approach that includes identifying and mitigating vulnerabilities, implementing strong encryption, identity and access management backed up by multi-factor authentication. By focusing on obscuring the application's presence rather than addressing its inherent weaknesses, organizations leave themselves vulnerable to attacks. Effective security measures must be transparent, robust, and based on industry best practices rather than relying on the hope that an attacker will overlook a service running on an unconventional port. Ultimately, security by obscurity is no substitute for a well-architected and executed information security strategy.



Home sweet home

IoT (Internet of Things) are frequently affected by insecure protocols or misconfiguration. Someone's security cameras were sending images in the clear (photos not shared for privacy), something we continue to see year after year.

Lesson Learned: Long story short, the user doesn't always know what an app, a platform or a system is doing behind the user interface. When connecting to any public Wi-Fi always utilize a VPN, not all VPNs are created equal so you need to test your VPN too. You don't have to get sophisticated and have all of the technology we deploy here in at the SOC at RSA Conference, you can purchase an inexpensive network TAP, install Wireshark and start capturing your own network traffic for analysis.

Unsecure vendor

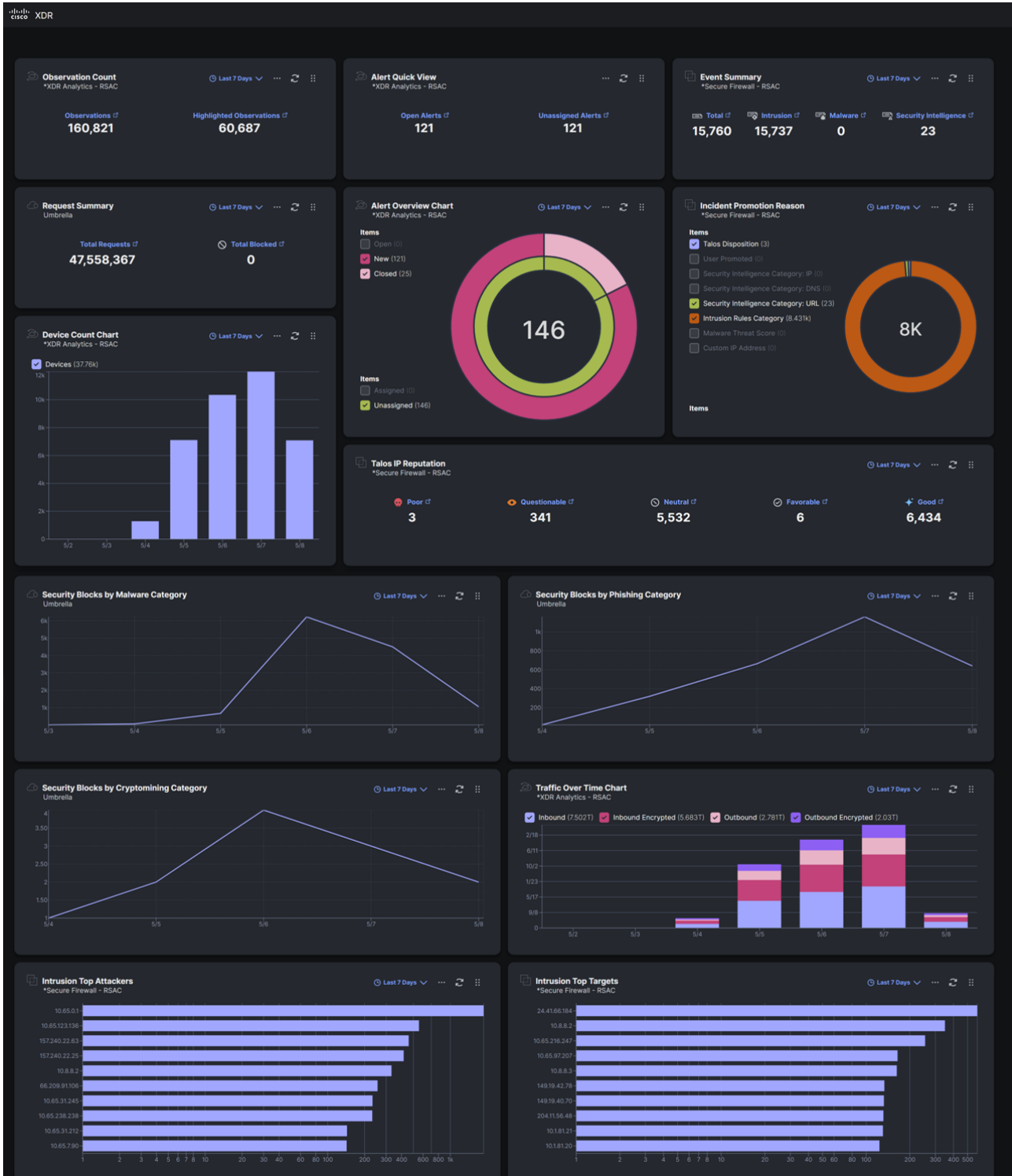
For the second RSAC, the NetWitness team was looking at unencrypted HTTP traffic - and noticed that certain web proxy configuration files are unauthenticated and can be exchanged in clear text. This means anyone (including bad actors) can request them and enumerate the data contained in them. This is production data of clients using the SaaS based web proxy.

The file tells you how to route certain domains through a web proxy. Why is this bad? Well, by seeing a company's web proxy file an attacker can enumerate information of the hosts and or domains they use internally. The attacker can also enumerate the data to determine what security controls and tools the organization is using.

Integration and threat hunting

Cisco brought Splunk Enterprise and the Cisco Security Cloud, composed of three suites: Breach Protection, User Protection and Cloud Protection; to provide visibility and integrate with NetWitness and threat intelligence partners.

The Cisco XDR Control Center widgets for Breach and User Protection provided insights into the network data and any threats. Widgets included XDR analytics, DNS, Malware Analysis, Thousand Eyes and Firewall Intrusion Detection.



To provide better context for our Threat Hunters, we integrated threat intelligence from several sources.

Cisco built a custom integration with NetWitness to visualize sightings, targets and relationships during investigations. This custom integration connects the NetWitness platform hosted at RSA Conference, using Security Services Exchange.

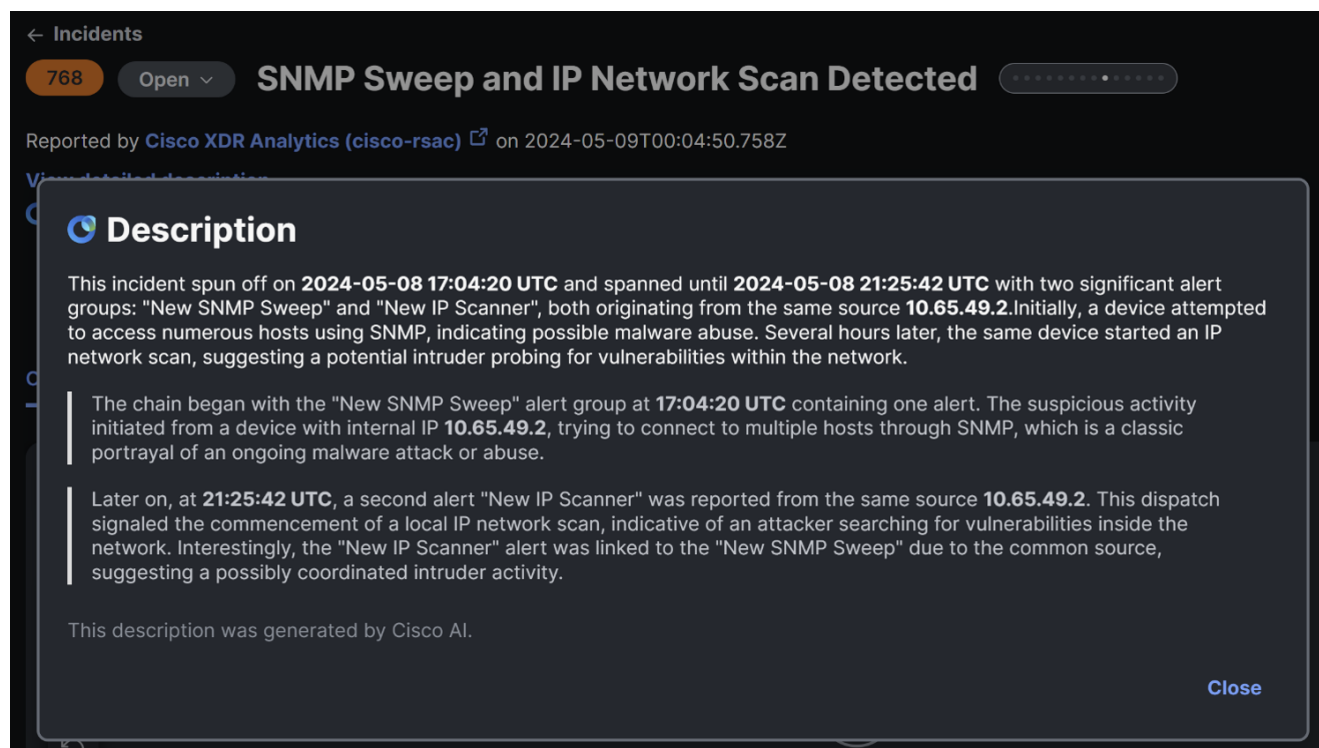
XDR AI Assistant

The XDR AI assistant provided three primary functions in the SOC at RSA Conference.

Incident summarization

Cisco XDR Analytics correlates complex series' of many discrete events into a single pattern of activity. It transforms lengthy and disjointed events from logs, into a common set of organized relevant data that can then be visualized by our graphing tools and understood much more rapidly and thoroughly, especially by less-seasoned analysts. However, even those diagrams can at times be complicated or populous.

AI Assistant can generate "human-readable" summary paragraphs that tell a comprehensive story that describes the attack timeline.



Documentation Chatbot

Cisco XDR publishes updates every two weeks. Everyone, at some point, may have a question. Better than poring over help documents and API specs, one can now ask the AI assistant simple questions from the icon in the upper menu bar.

You

Where can I get my API client credentials to make custom integrations?

AI Assistant

Certainly, to create your API client credentials for enabling custom integration with Cisco XDR, please follow these steps:

1. Navigate to **Administration > API Clients** from the navigation menu in Cisco XDR, then click **Generate API Client**.
2. Next, input a **Client Name** and (optionally) choose a **Client Preset** from the drop-down list. Note that if you select a **Client Preset**, all of the scopes are pre-configured for a particular function.
3. If you didn't select a **Client Preset**, you will need to manually select the check boxes for the scopes you want to grant privileges to the client. Alternatively, you can click **Select All** to grant all scopes to the client.
4. Optionally, input a description in the **Description** field, then click **Add New Client**.

At this point, the **Client Id** and **Client Password** are generated and displayed in the **Add New Client** dialog box.

Please be sure to note down your **Client Password** as it cannot be recovered once you close the window. If you lose or disclose the client password, you have to delete the API client and create a new one.

Remember that the API Client is tied to your user identity. If your user identity loses its privileges, then your API Client will also lose those privileges. All actions taken by the API Client are transected in your name and recorded as your actions. If access to your application is revoked, API Client will also become invalid.

Sources

1. [API Clients](#)



Cisco AI Assistant

You

What is an Indicator in Cisco XDR and what is the specification for it in CTIM?

AI Assistant

In Cisco XDR, an indicator refers to a pattern of behavior or a set of conditions that suggest malicious activity. It helps to pinpoint potentially harmful behavior exhibited by an observable, which helps the incident responder make an informed decision about how to respond.

As described in Cisco XDR, indicators essentially help analysts determine which bad behaviors a particular observable, such as a domain or IP address, is exhibiting. These behaviours could potentially indicate malicious activities, making them an important tool for incident response teams.

Cisco XDR uses the Cisco Threat Intelligence Model (CTIM) which is a specific way of decomposing, storing, and retrieving vast amounts of threat intelligence. This model also aids in curating libraries of advanced threat behavioral indicators. These indicators, alongside traditional research methods, are utilized to discover new kinds of malware as well as new behaviors exhibited by known malware. The intelligence gathered in the process is then fed back into Cisco's ecosystem, allowing for continuous enrichment of threat intelligence resources.

While the specific specifications for creating or distinguishing indicators in the CTIM are detailed and technical, you may refer to the [Modeling Threat Intelligence in CTIM](#) tutorial for further understanding. This tutorial provides detailed descriptions and methods for modeling threat intelligence within the CTIM framework, and includes best practices for client developers.

Sources

1. [Glossary](#)

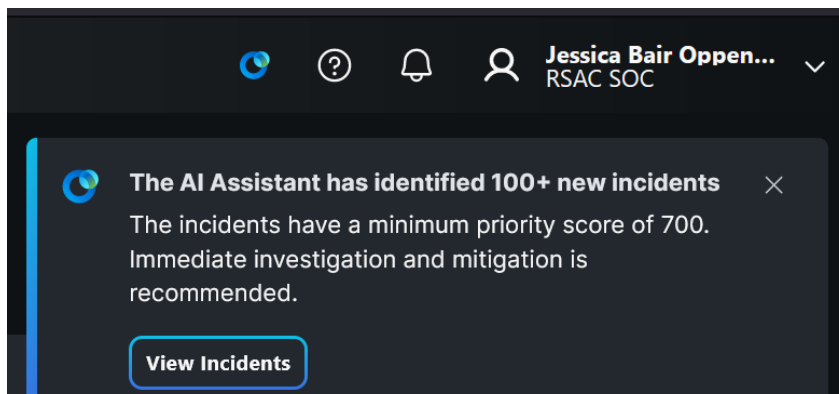


Incident Response Guidance

Cisco XDR AI Assistant will also notify you of new Incidents, the count of new Incidents since you last looked, and the Priority score range of those new Incidents.

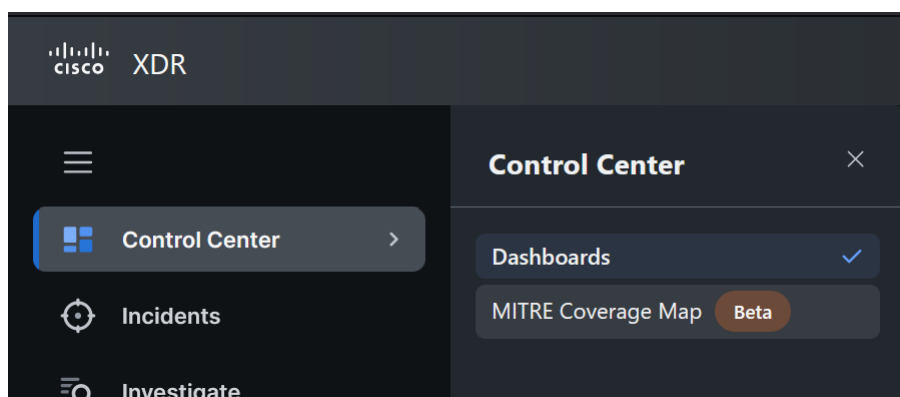
Once you choose and select an incident to work with, the AI assistant can track recent actions taken in the incident and suggest next steps.

The suggested actions are based on industry standard IR processes, and will change as you complete the various steps.



MITRE ATT&CK Heatmap

Another new function in the SOC was [MITRE ATT&CK Coverage Map](#).



The SOC team at RSA Conference could quickly assess the MITRE coverage with the XDR and integrated products.

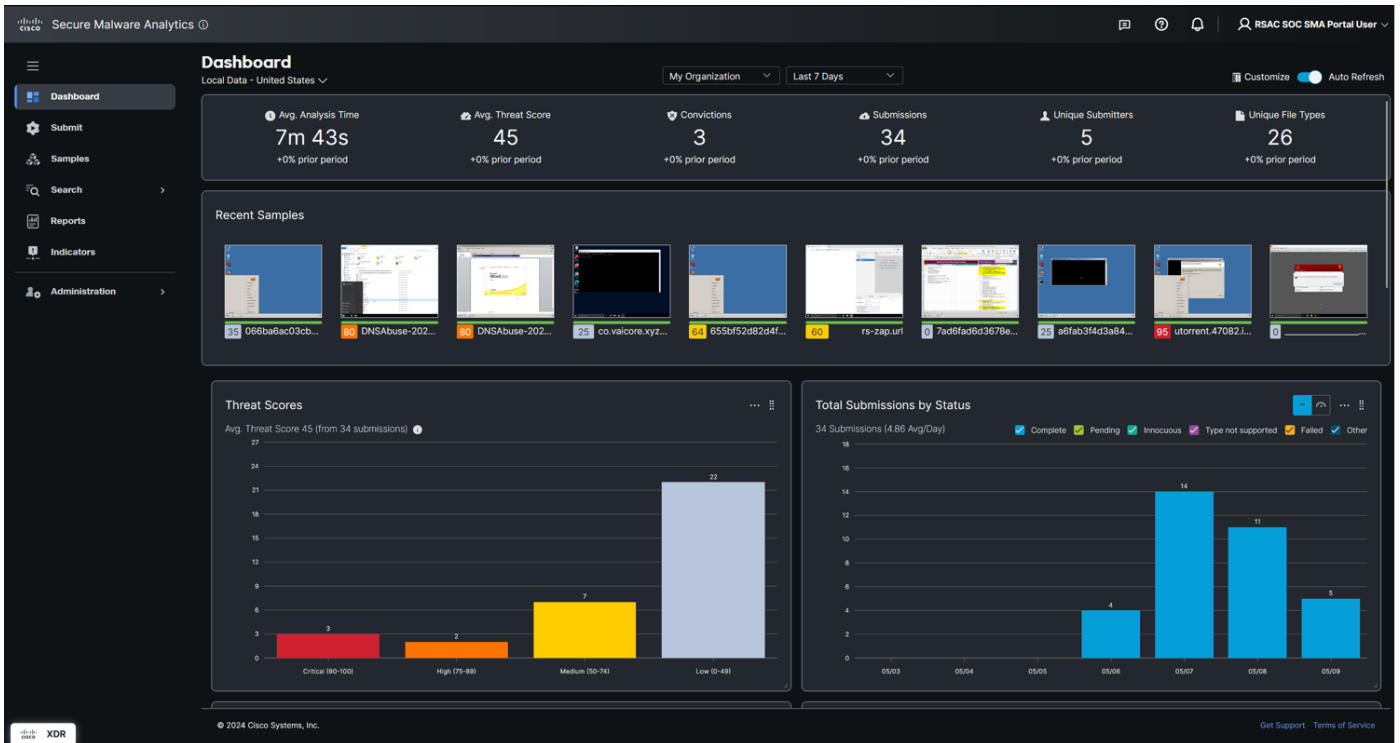
Using this tool, the SOC team could gain quick insights into which tactics could be best detected and mitigated by our security deployment.

In a production SOC, we could have used this data to inform security architecture decisions and deploy interim stopgaps, while a less well-informed team may have still been wondering what their risk exposure was even at this high level.

Exposure mapping is not an exact science – vendor claims vary widely, and attacks don't often fit neatly into the ATT&CK structure. As a broadest-brush first pass to inform strategy and upon which to base further discovery, the MITRE ATT&CK Heatmap greatly decreases the amount of time and effort required to improve an organization's overall security posture.

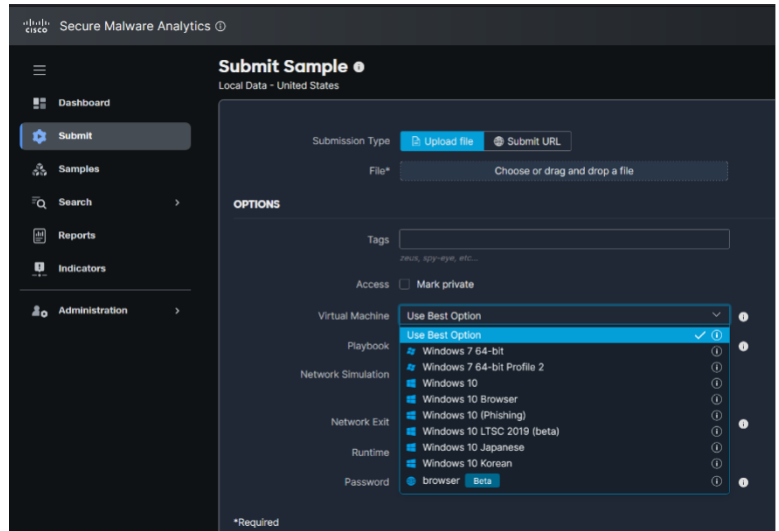
Malware analysis

The SOC Team at RSA Conference sent dozens of potentially malicious files to Breach Protection - Malware Analytics via the NetWitness platform and Secure Firewall, for automated behavioral analysis, and manual submissions to aid threat hunting.

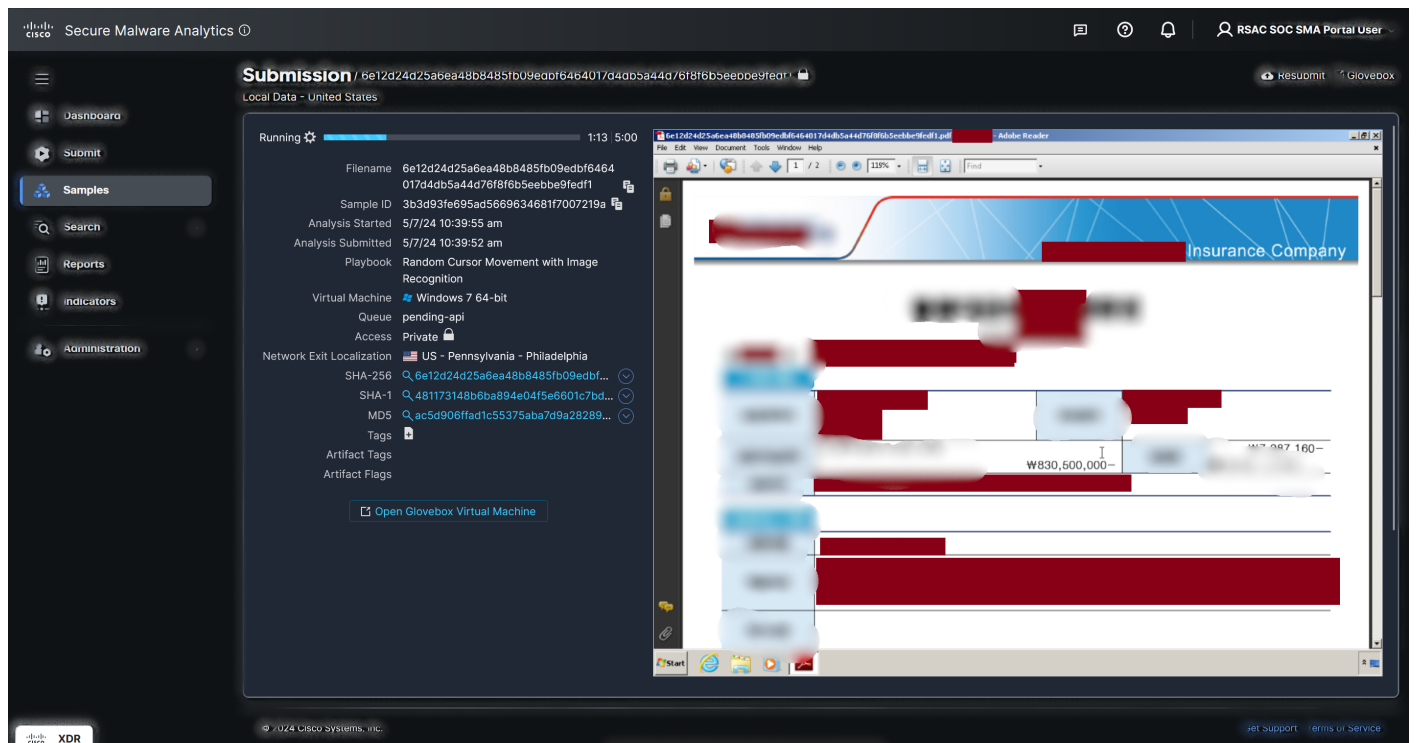


Documents in the clear

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 desired or use the best option.



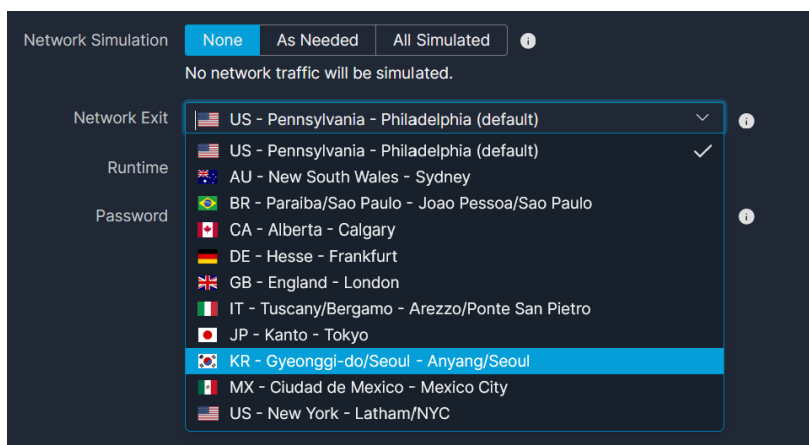
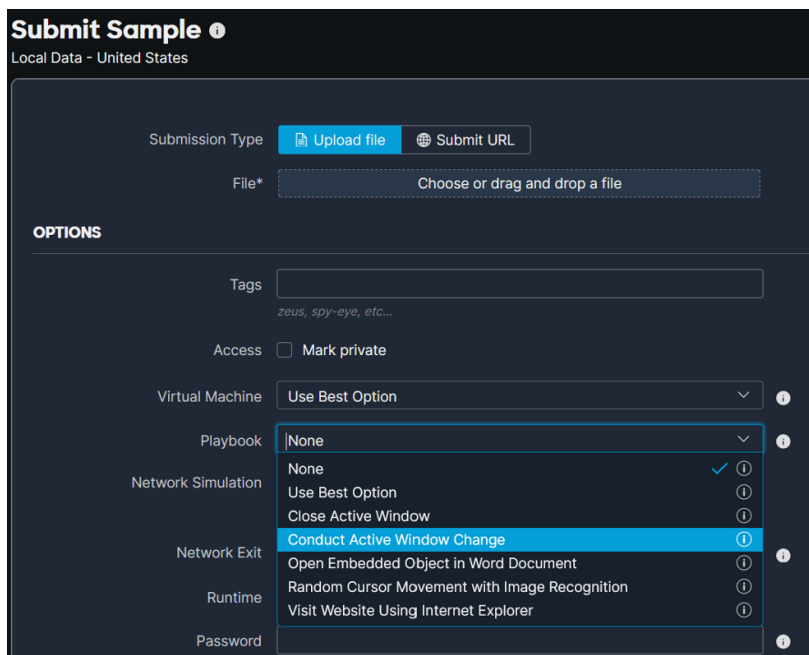
The best option was useful when investigating Korean language documents, that were auto detected. Such as this contract of insurance for a shipment of gold.



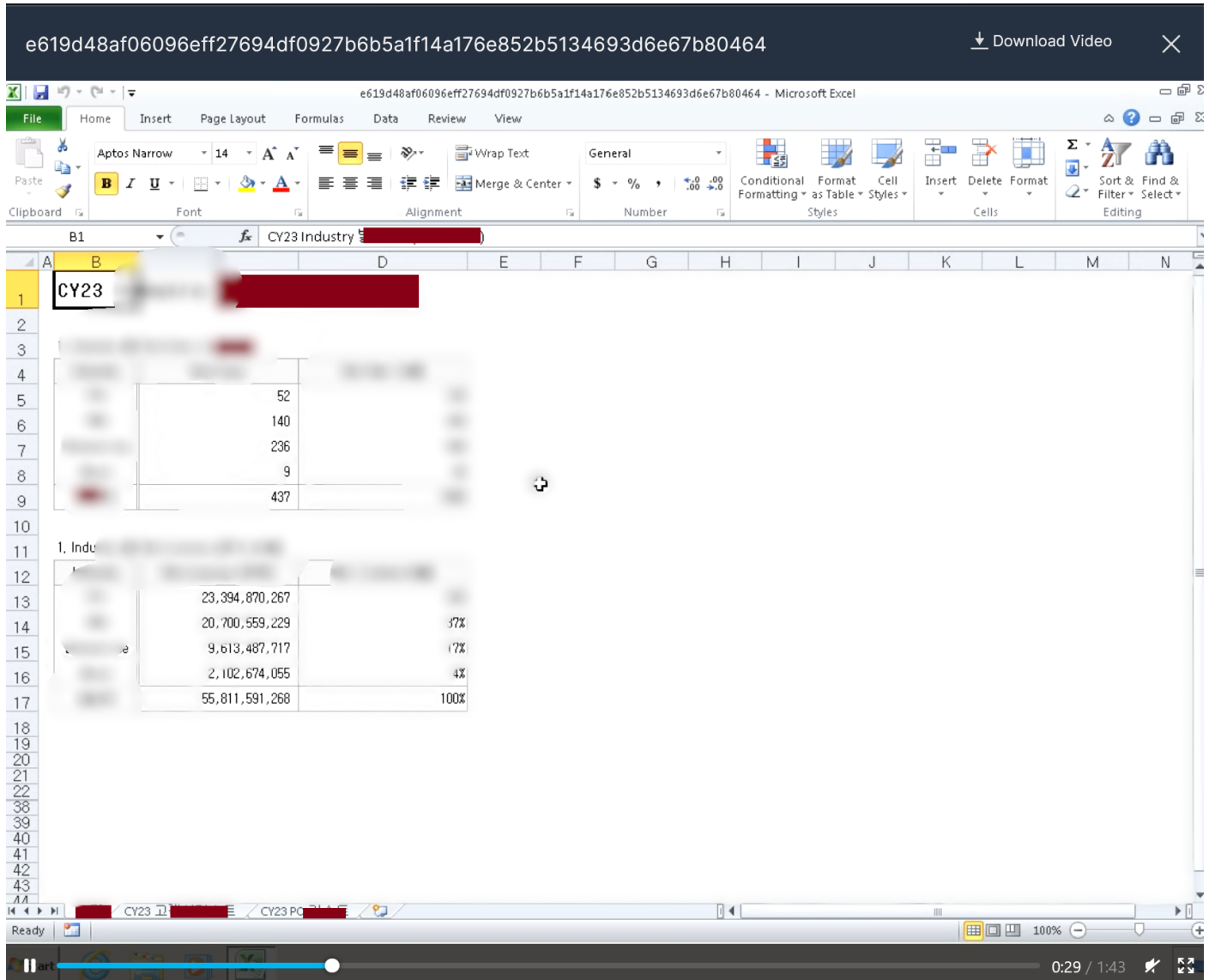
To simulate user automatically during sample analysis, Malware Analytics provides emulation through playbooks, which are pre-defined steps that simulate user activity. A system with a user present appears vastly different from an automated analysis system (i.e., a sandbox). For example, an automated 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 they just opened did nothing.

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 the “Network Exit”, to investigate malware that behaves differently by region.



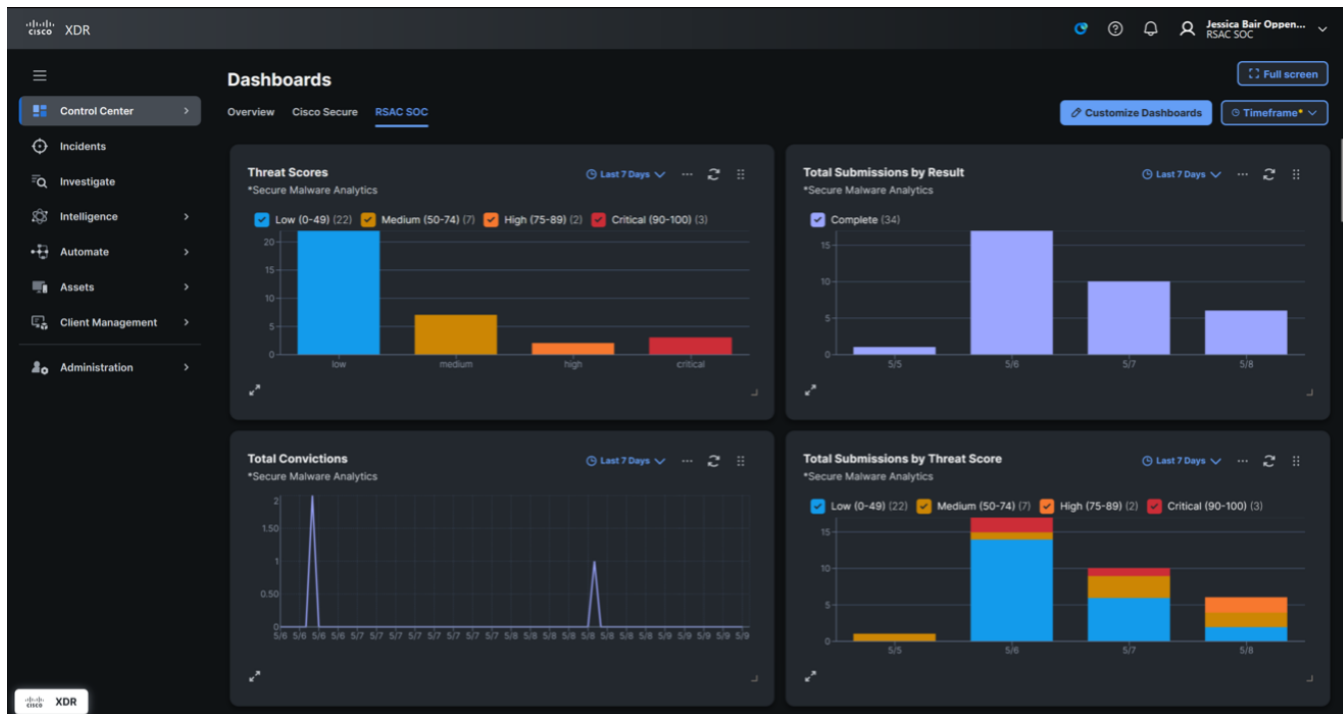
The Firepower Management Center found and analyzed many documents which were in the clear. Any attendee at the conference, who had the right tools and knowledge, would have been able to view the attachments.



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 a purchase order, that had the names and email addresses of the CEO for the security software vender and the customer.

SOC leader Steve Fink, visited the booth of the sponsor listed and showed them the firewall alert, full packet capture metadata and screenshots of the confidential business documents. The company was a reseller of the Security Service Edge technology, but implemented the technology incorrectly. The RSAC sponsor agreed to contact the reseller about the data leakage and misconfiguration to get it corrected. We see this all too often when technology is misconfigured, security teams need to be included early in the deployment cycle and continue to monitor production systems.

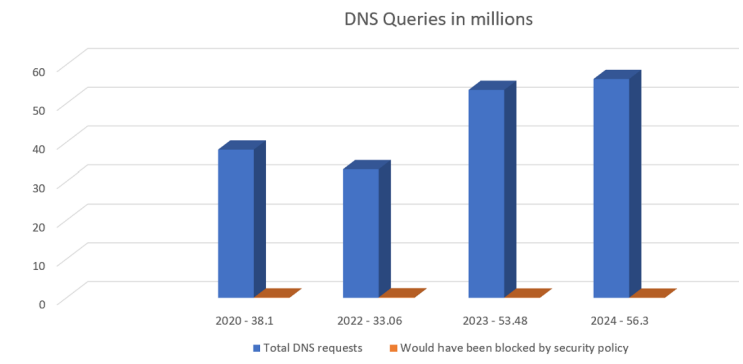
We were able to monitor the sample submissions in the Cisco XDR Control Center during the operations.



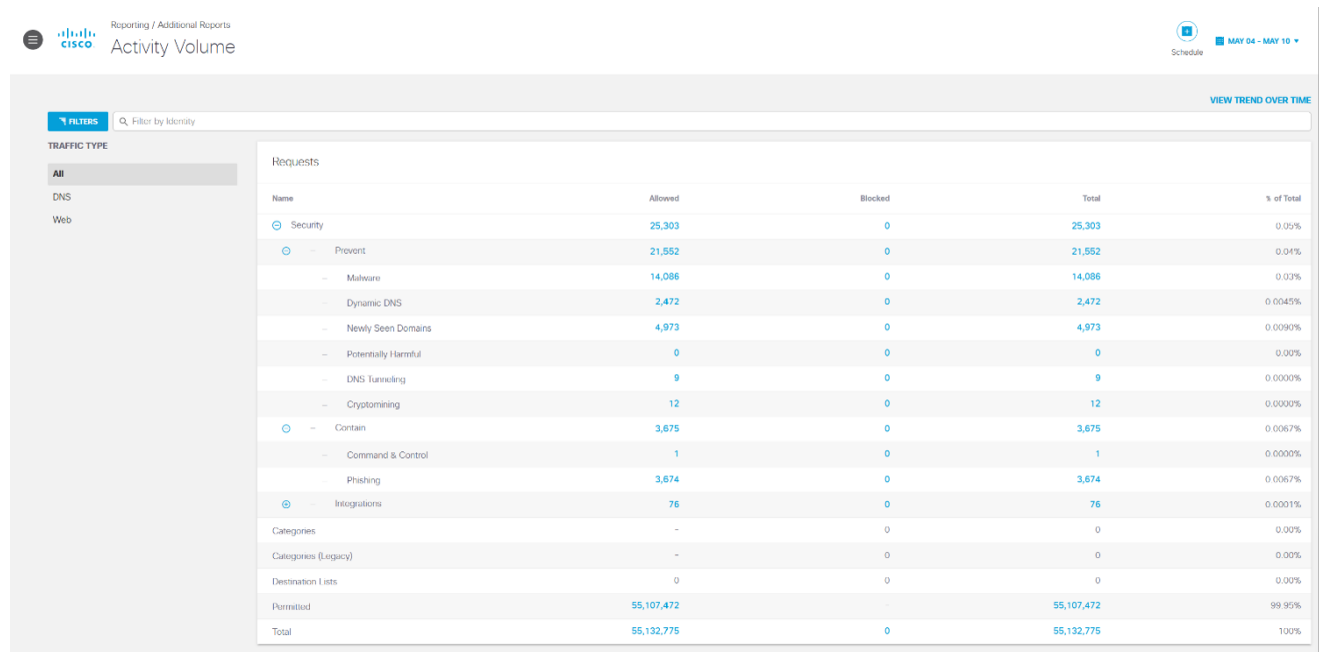
Domain Name Server (DNS)

The SOC had complete DNS visibility, thanks to the support of the Moscone Center with installing Umbrella virtual appliances (VAs) in the Network Operation Center.

The default security settings for Cisco Umbrella are to block malware, command-and-control callback, and phishing attacks. All security and content category blocking was turned off for the conference network, to allow security training, demos and briefings to operate unimpeded.



We saw over 56 million DNS requests over the week, of which over 30,000 would have been blocked for security policy violations.



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 conference security team and law enforcement, as appropriate, in coordination with the Moscone NOC.

As mentioned, in the NOC are deployed Umbrella VAs 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 Umbrella 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 DHCP, but we do not enforce their use.

This presents a problem for SOC analysts who benefit from internal IP information but need a way to glean this information out-of-band of the query itself. To solve this problem, we implemented a work-around to essentially replay the DNS queries with the original client IP intact. These replays were aimed at another VA dedicated to these queries.

This quick bit of DevSecOps provided us some valuable information:

Alerting and reporting in the Umbrella dashboard for non-Umbrella DNS resolutions.

An easy way to differentiate these queries (using the “out-of-band VA” as a Site definition in Umbrella). Metrics on how many queries were destined for custom resolvers versus the VAs are below.

Identity	Requests
RSA VAs	55.2M
OOB-DNS	1.2M

SOC issued awards to the top domains in the SOC session on 9 May 2024.

#1 🐱 24: Apple | 23: Google | 22: Office365
#1 🗨️ 24: Mchat | 23: Mchat | 22: WhatsApp
#1 🪛 24: IBS.Team | 23: Forsts | 22: NiceHash
#1 ❤️ 24: grindr | 23: grindr | 22: grindr

Apps, Apps and more Apps

10,167 applications were identified by the DNS queries at RSAC 2024. This is an increase from past conferences.

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

Reporting / Core Reports
Cisco App Discovery Download PDF

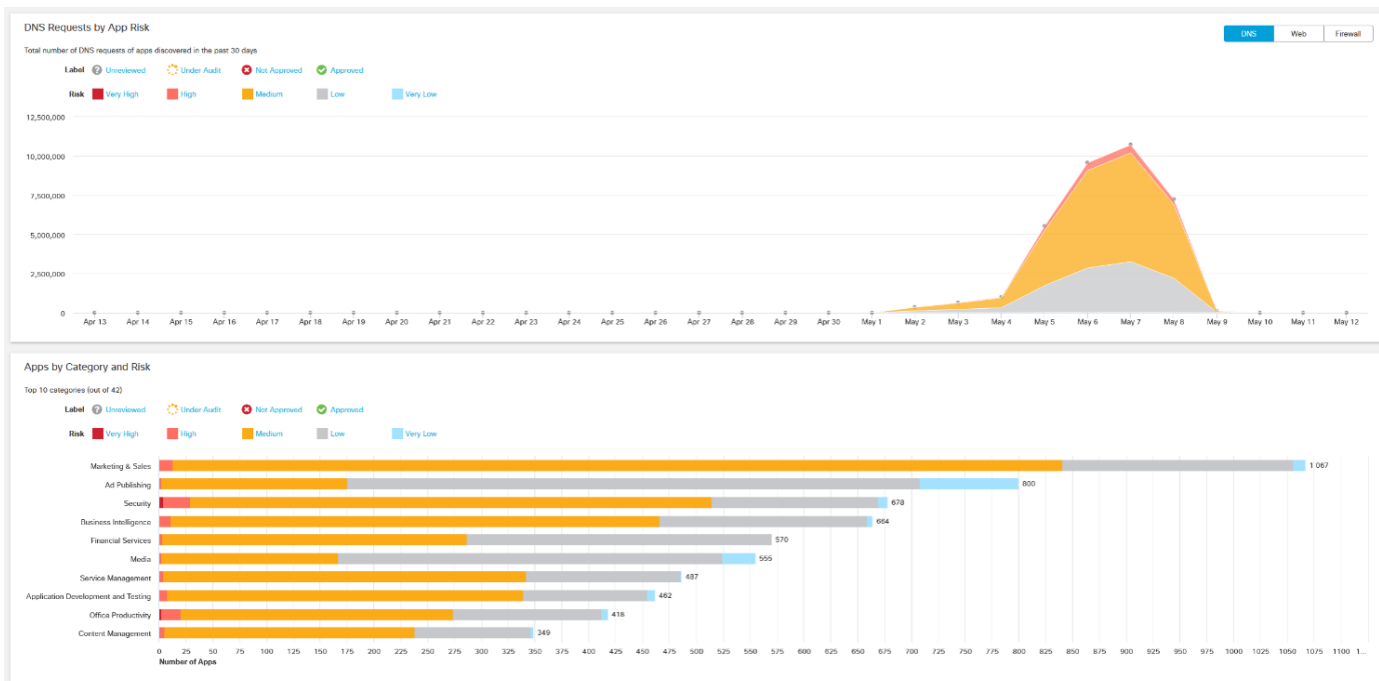
10,167 apps discovered

10,167 unreviewed apps 0 apps under audit 0 apps not approved 0 apps approved

Flagged Categories

- Generative AI**
80 unreviewed apps
Generative AI apps have the potential for generating misleading or fraudulent content and copyright or intellectual property infringements. [DETAILS](#)
- Anonymizer**
35 unreviewed apps
Anonymizer apps introduce risk to your network because they enable users to bypass security controls. [DETAILS](#)
- P2P**
22 unreviewed apps
P2P apps represent high risk because they can be used to transmit files infected with viruses and malware. [DETAILS](#)

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



AI was a big topic at RSAC 2024, and these were the top AI apps in use by attendees.

Application ▾

- Notion AI
Generative AI
- Bing AI
Generative AI
- OpenAI ChatGPT
Generative AI
- GitHub Copilot
Generative AI
- Canva
Generative AI
- Tidio
Generative AI
- Microsoft Copilot
Generative AI
- Perplexity AI
Generative AI
- Anthropic Claude
Generative AI
- Descript
Generative AI
- Writer Platform
Generative AI
- Cursor.sh
Generative AI

Security incident and event management

NetWitness and Splunk Enterprise Security

This year we had the opportunity to deploy the NetWitness Splunk App integration, and while it does not yet offer a dashboard, it provides a powerful search integration, which we used extensively to validate our findings with firewall.

Utilizing 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 NetWitness Splunk integration.

dest_org

>100 Values, 21.082% of events

Selected

Reports

Top values Top values by time Rare values

Events with this field

Top 10 Values	Count	%
Moscone Center Joint Ventures	26,579	45.186%
Microsoft Azure	6,696	11.384%
Google Servers	6,211	10.559%
Amazon.com	2,810	4.777%
Cloudflare	2,168	3.686%
Cisco OpenDNS, LLC	1,686	2.866%
Google	1,633	2.776%
Apple	1,378	2.343%
Google Cloud	1,322	2.247%
Amazon CloudFront	1,199	2.038%

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.

List ▾ Format 20 Per Page ▾

de Fields All Fields

CTED FIELDS

st 1

urce 1

urcetype 1

RESTING FIELDS

alysis_service 64

alysis_session 22

ack_tactic 9

ack_technique 19

ack_tid 19

apture_port 1

mmunity_id 100+

nfig 100+

te_hour 2

te_mday 1

te_minute 29

te_month 1

te_second 60

te_wday 1

te_year 1

te_zone 1

st_country 100+

st_domain 100+

attack_technique

19 Values, 31.592% of events Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Top 10 Values	Count	%
fast flux dns	693,776	49.024%
data transfer size limits	377,949	26.707%
dns	241,360	17.055%
non-application layer protocol	66,398	4.692%
direct network flood	19,092	1.349%
malicious link	15,065	1.064%
web session cookie	993	0.07%
smb/windows admin shares	273	0.019%
encrypted channel	127	0.009%
change default file association	62	0.004%

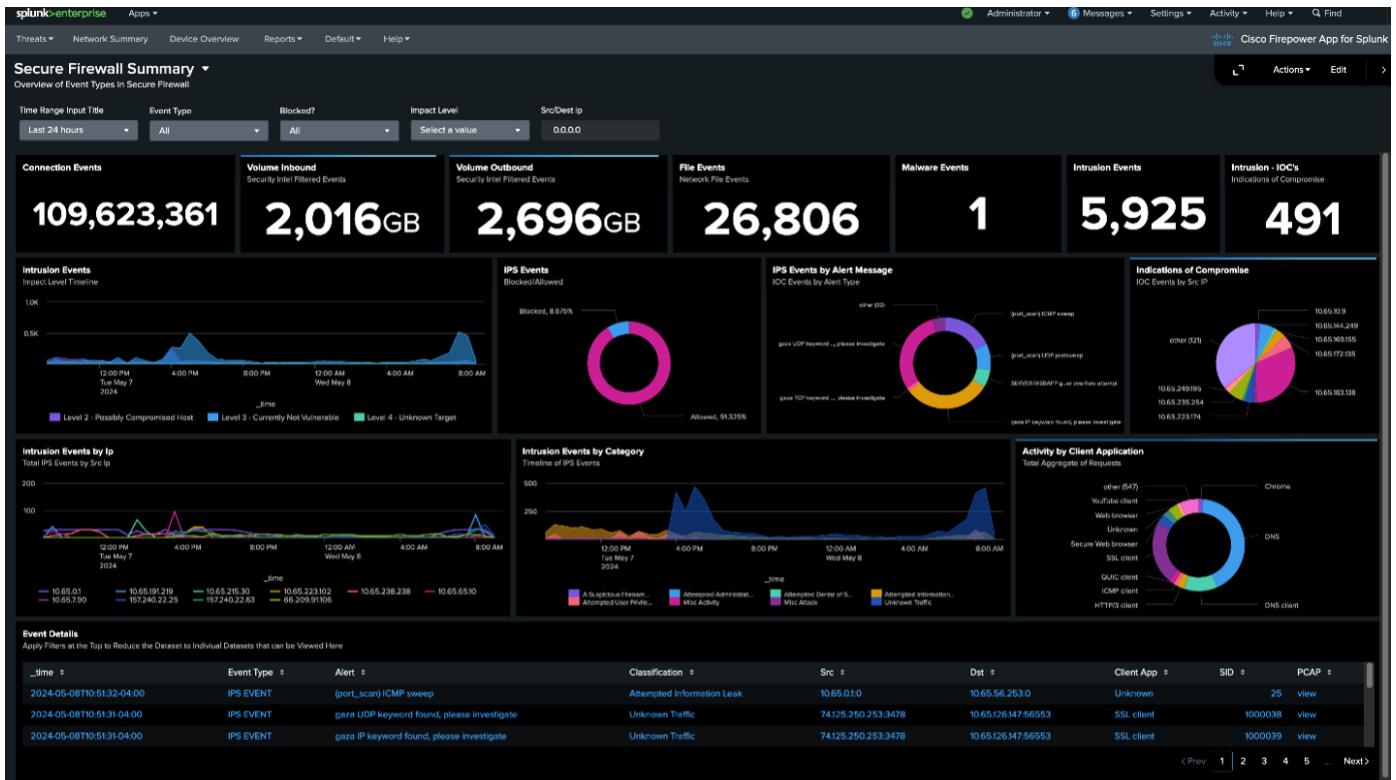
> 5/7/24 _time=1715117013 sessionid=86234960 size=33556920 dvc_host=nw-phy-01 pay
2:23:33.000 PM 216.131.81.39 proto=17 src_port=65245 dest_port=51820 community_id="1:dK

Splunk and Secure Firewall

While data searching may seem like a simple feature at first glance, it is, in fact, a pivotal component of search technology, underpinning its significance in rendering information readily accessible, refining business intelligence, elevating user experience, conserving time, enabling data analysis, securing competitive edges, and driving revenue generation.

Splunk is no stranger to the Cisco Secure Firewall integration, for the past five years, it has consistently ranked as the topmost downloaded Cisco application within [Splunkbase](#).

At this year's RSA Conference, we employed the most recent user experience enhancements. With the integration of advanced CIM mapping and OCSF, our Firewall further showcased the formidable capabilities of Cisco's synergy with the Splunk platform.



The Firewall app dashboard presented above offered a comprehensive snapshot of the network's health, meticulously outlining crucial event types such as connections, intrusions, and malware incidents. This high-level view enables us to swiftly identify potentially infected IP addresses, meticulously track the timing and volume of events, and visually discern the categories of threats posed by malicious actors.

Recorded future

The Recorded Future Splunk App integrates with Splunk to enhance firewall data analysis by enriching it with real-time threat intelligence. This enrichment provides context to the data, helping prioritize threats, generate alerts for potential breaches, and assess risk more accurately. The app offers visualization tools for better reporting and automates the correlation of firewall logs with threat intelligence, improving the efficiency of security operations.

At RSA Conference, we leveraged detailed threat intelligence rules to augment the data from the secure firewall events, yielding deeper insights into potential threats. Harnessing the capabilities of Splunk's Common Information Model (CIM), we crafted correlation rules that seamlessly integrated metadata from both the firewall sensors and Recorded Future's threat intelligence feeds. This synergy enabled real-time alerts for suspect events. The screen displayed below illustrates the alerting rules embedded within the platform, which the RSAC team diligently monitored for potential matches.

splunk-enterprise Apps Administrator Messages Settings Activity Help Find

Alert Center Enrichment Threat Hunts Search Data Configuration Docs Recorded Future Portal Recorded Future

Recorded Future Alerts

524 alerts Alert rule All alerts Filter Any time Any Status Docs

ID	Alert Title	Triggered	Status	Assignee	Note
>	Global Trends, Trending Targets - Rise: Минобороны Британии	5/6/24, 8:41 PM	New	None assigned	
>	Global Trends, Trending Attackers - Rise: LulzsecMuslims	5/6/24, 8:39 PM	New	None assigned	
>	Global Trends, Trending Targets - Rise: Kuwait Civil Aviation	5/6/24, 8:35 PM	New	None assigned	
>	Global Trends, Trending Targets - Rise: Non Fungible Token and @avelina_ve	5/6/24, 8:30 PM	New	None assigned	
>	Global Trends, Trending Targets - Rise: #exgiguy	5/6/24, 8:24 PM	New	None assigned	
>	Global Trends, Trending Attackers - Rise: David McBride	5/6/24, 8:20 PM	New	None assigned	
>	Global Trends, Trending Targets - Rise: @theredbestioy	5/6/24, 8:09 PM	New	None assigned	
>	Global Trends, Trending Targets - Spike: London	5/6/24, 8:03 PM	New	None assigned	
>	Global Trends, Trending Targets - Spike: Greater London	5/6/24, 7:58 PM	New	None assigned	
>	Global Trends, Trending Targets - Spike: Final Fantasy XIV	5/6/24, 7:52 PM	New	None assigned	
>	Global Trends, Trending Attackers - Rise: Charles Hoskinson	5/6/24, 7:48 PM	New	None assigned	
>	Global Trends, Trending Targets - Surge: Netflix	5/6/24, 7:47 PM	New	None assigned	
>	Global Trends, Trending Methods - Rise: Cuckoo	5/6/24, 7:44 PM	New	None assigned	
>	Global Trends, Trending Attackers - Rise: @CTESPNWisconsin	5/6/24, 7:42 PM	New	None assigned	

We utilized Recorded Future's enrichment portal to enhance our analysis of suspect IP addresses, which provided us with a comprehensive threat score and an in-depth summary of the suspected attack types and malevolent activities associated with these IPs. Our findings primarily revealed the presence of spam and adware, which, fortunately, registered as relatively low-level threats on the intelligence scale.

splunk-enterprise Apps Administrator Messages Settings Activity Help Find

Alert Center Enrichment Threat Hunts Search Data Configuration Docs Recorded Future Portal Recorded Future

IP Enrichment

IP lookup CIDR range

Submit

Link To Portal

Severity: Suspicious
Risk Score: 38 of 99
Triggered Risk Rules: 9 of 77

ASN: AS16276
ORG: OVH SAS
GEO: Germany, Europe

First Reference: 2019-04-11
Latest Reference: 2024-05-16
References: 1188

MITRE ATT&K
T1090 (Proxy), T1090.003 (Proxy: Multi-hop Proxy), T1566.001 (Phishing: Spearphishing Attachment), T1566.002 (Phishing: Spearphishing Link), T14001 (Initial Access: TAOUI) (Command and Control)

Docs Risk Score

Infrastructure Detections

Triggered Risk Rules

Criticality	Rule	Evidence for Rule
2	Recent Spam Source	24 sightings on 1 source: External Sensor Spam. 51.75.64.23 was identified as spam in External Sensor data. Reported to Recorded Future on Apr 26, 2024.
2	Recent Tor Node	1 sighting on 1 source: Dan.me: Tor Nodelist.
1	Historical Botnet Traffic	87 sightings on 3 sources: Bot Scout, Botscout - Bot IPs, External Sensor Data Analysis. 51.75.64.23 was historically observed as botnets. No longer observed as of Nov 10, 2021. Most recent link (Mar 8, 2024): https://botscout.com/ipcheck.htm?ip=51.75.64.23
1	Historical Multicategory Blocklist	94 sightings on 1 source: AbuseIP Database. Most recent link (Jan 21, 2021): https://www.abuseipdb.com/check/51.75.64.23?d=2021-01-21T18:34:38.000Z
1	Historical Open Proxies	2 sightings on 1 source: External Sensor Data Analysis. 51.75.64.23 was historically observed as proxy. No longer observed as of Nov 10, 2021.
1	Historical Phishing Host	1 sighting on 1 source: External Sensor Data Analysis. 51.75.64.23 was historically observed as phishing. No longer observed as of Oct 24, 2021.

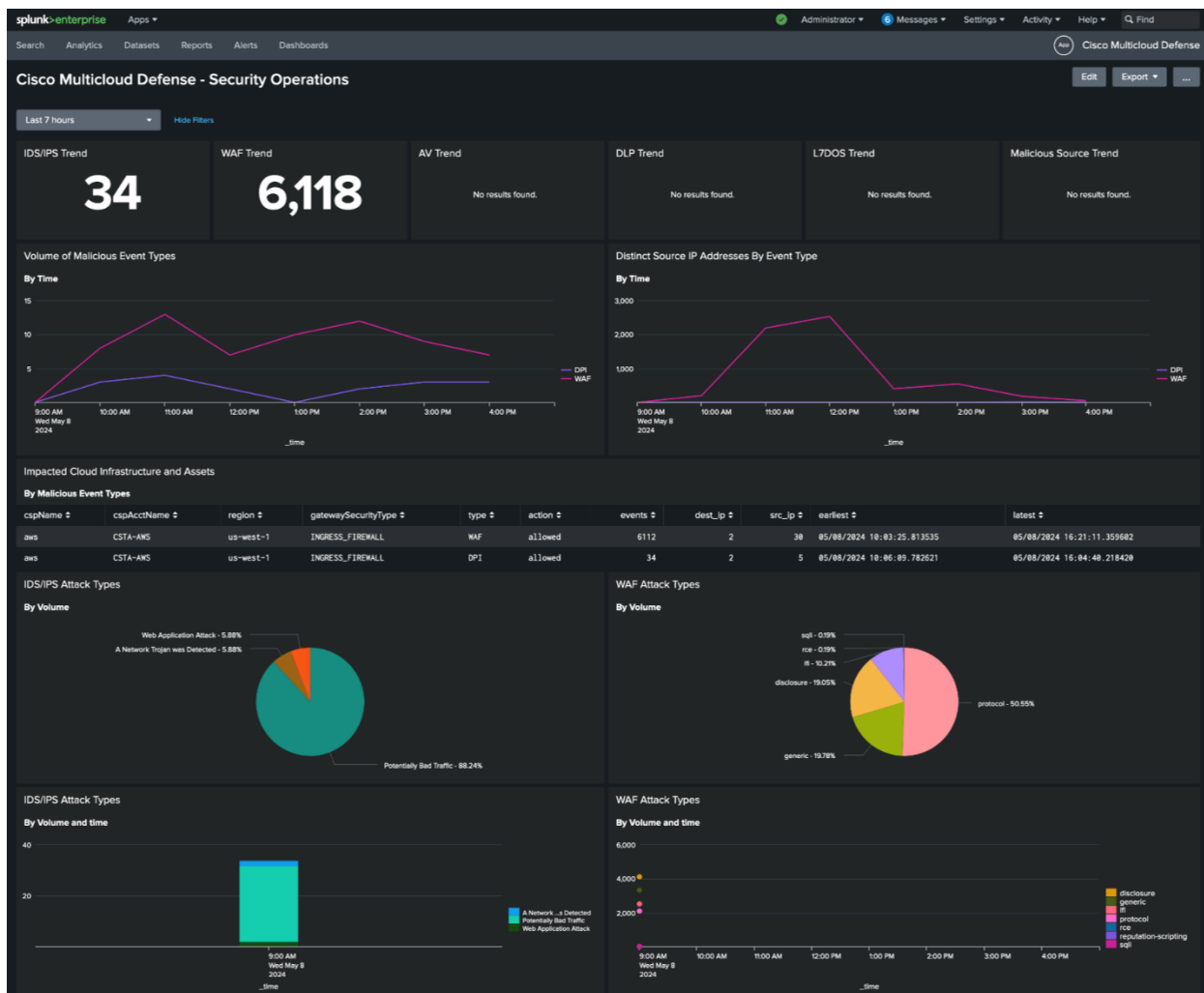
Cloud Protection Events – Malware

After deploying the Multicloud Defense suite, we leveraged Splunk for event visualization and uncovered intriguing findings. Our analysis through the 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.

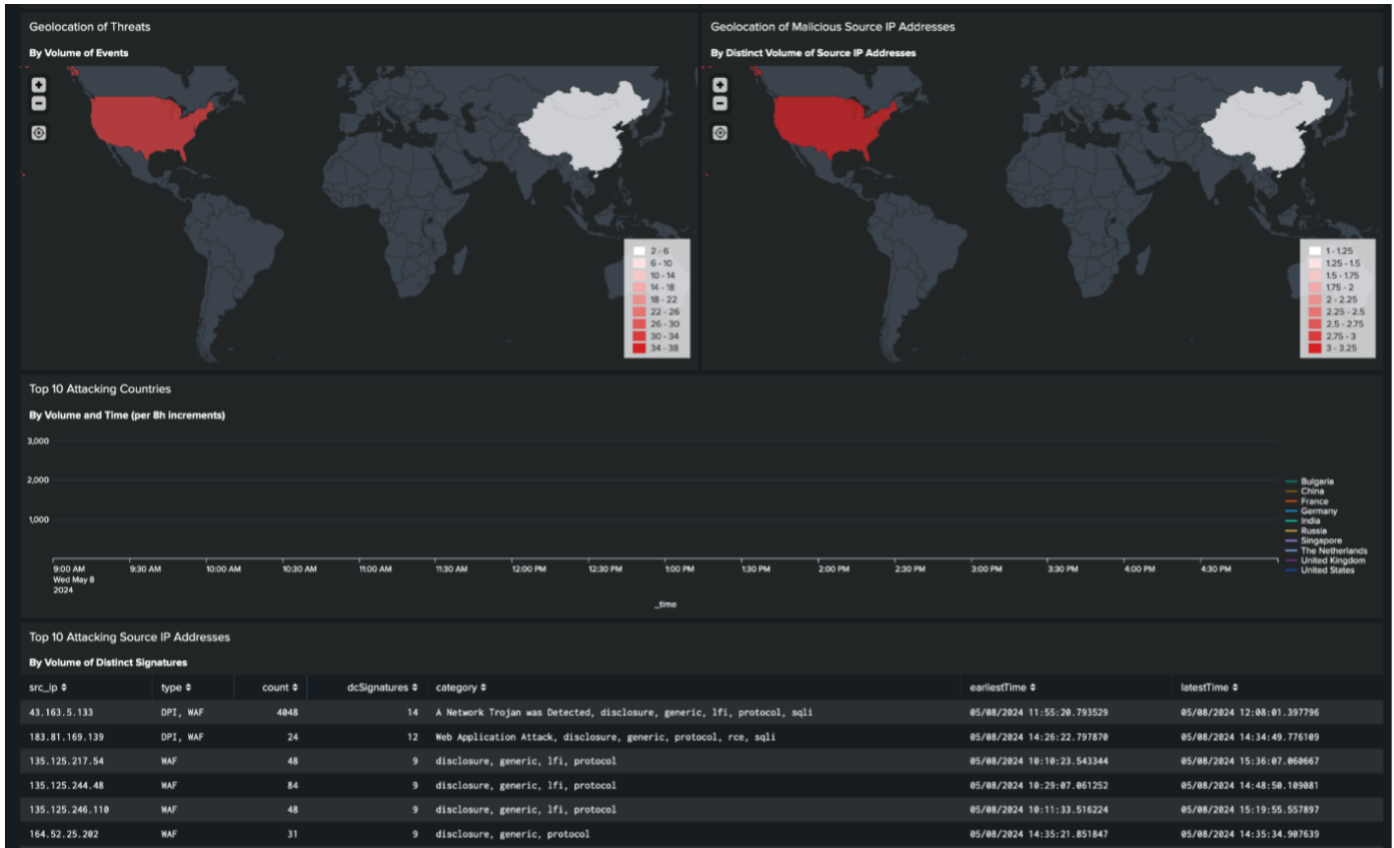
We crafted a controlled experiment within SMA, replicating the suspected Trojan activity within a secure virtual machine environment. The investigation led us to a Chrome browser extension plugin designed for audio control. While SMA's analytical capabilities did not explicitly identify the underlying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

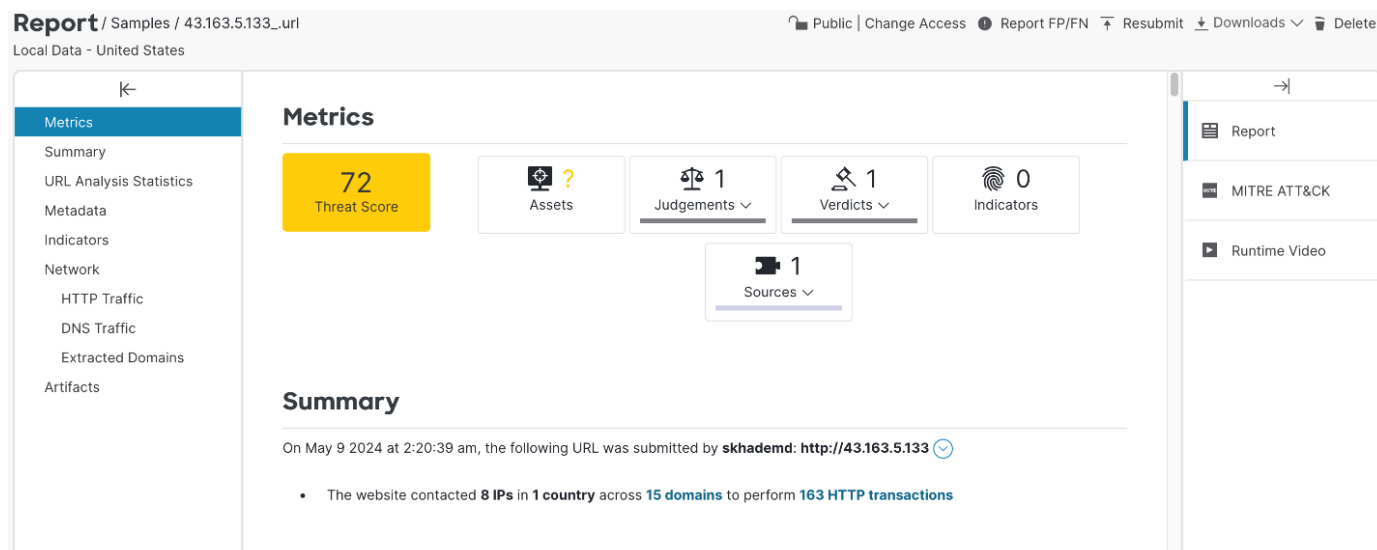


Replaying the malware in Secure Malware Analytics through an XDR investigation.

The screenshot shows a submission page for a file named '43.163.5.133_url'. The page includes metadata such as Sample ID, Analysis Started/Submitted times, User Agent, Virtual Machine type, and Network Exit Localization. It also lists SHA-256, SHA-1, and MD5 hashes, and provides a link to 'Open Glovebox Virtual Machine'.

Overlaid on the submission page is a browser window showing the 'Volume Master' extension interface. The interface includes a volume slider set to 180%, buttons for 'Default', 'Voice boost', and 'Bass boost', and a list of tabs playing audio, including 'Ghosts of the Arctic on Vimeo' and 'Jamiroquai - Stillness in Time - YouTube'.

The report returned the threat score and behavior.



Intrusion detection

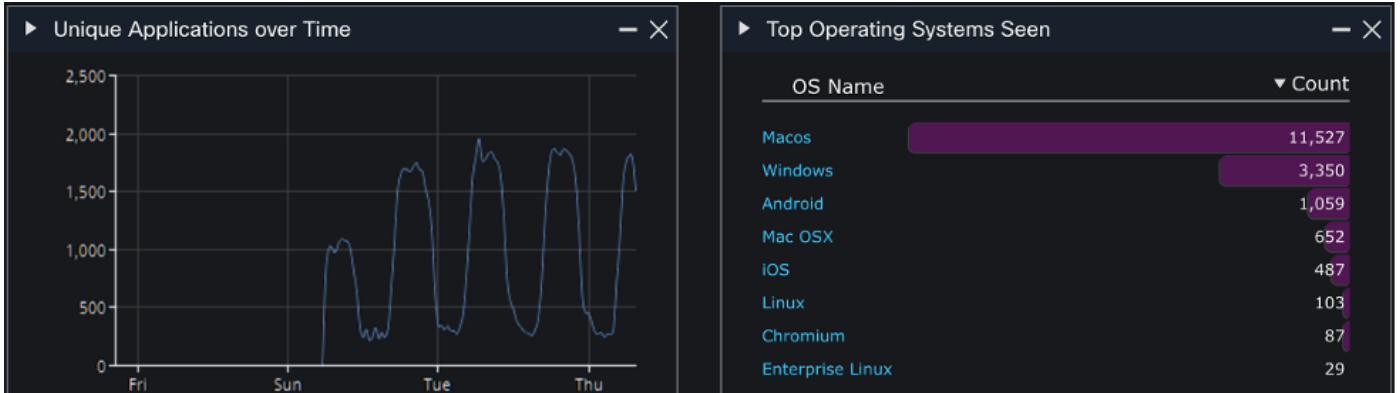
In any SOC, Next Gen Firewalls with intrusion detection (IDS) serve as a vital source of data, and the same is true of our SOC at RSAC. We deployed a Secure Firewall 4115 appliance running Firepower Threat Defense (FTD) software as our IDS. We leveraged the IDS for multiple integrations:

- Syslog was sent to Cisco XDR for further correlation
- Multiple event types were sent to Splunk and NetWitness
- Files were submitted to Secure Malware Analytics for sandbox analysis

The IDS inspected all wireless guest traffic from event attendees. Firepower 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 the SOC to help uncover threats lurking in the environment. Sending this data to Cisco XDR facilitated advanced correlation of event data across the different technologies deployed in the SOC at RSA Conference.

Discovered applications

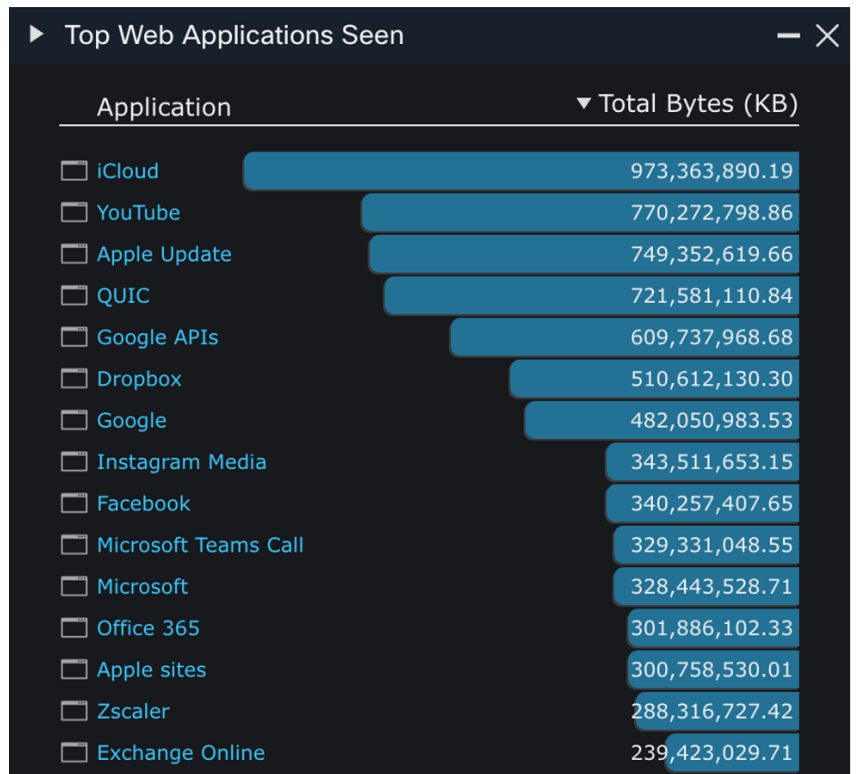
Firepower detected nearly 2,000 different applications during the conference, with the number of unique applications concurrently seen on the network spiking during conference hours each day. The top operating system was once again Apple's Mac OS, with Microsoft Windows taking the #2 spot. In 2024, users showed a clear preference for laptops over mobile devices when connecting to the Moscone Center Public Wi-Fi, as shown by the prevalence of Mac OS and Windows, over Android and iOS.



Daily OS counts also help provide a rough number of how many attended the event for that day.

Web Application traffic had some significant differences from 2023. While Apple again took the top spot with iCloud, YouTube more than doubled its traffic to reach #2. Dropbox and the QUIC protocol also greatly increased their traffic. IPSec failed to make the list this year.

These statistics are for the RSAC public Wi-Fi only and exclude any users who opted to use mobile data instead. Even so, iCloud managed to rack up nearly a terabyte of data over the course of the conference.



Firepower threat detection

Cisco's portscan detector is a threat detection mechanism designed to help detect and prevent portscan activity in all types of traffic to protect networks from eventual attacks. Portscan traffic can be detected efficiently in both allowed and denied traffic. Portscan is a form of network reconnaissance that is often used by attackers as a prelude to an attack. In a portscan, an attacker determines the types of network protocols or services a host supports and sends specially crafted packets to a targeted host. By examining the packets that the host responds with, the attacker can often determine which ports are open on the host and, either directly or by inference, which application protocols are running on these ports.

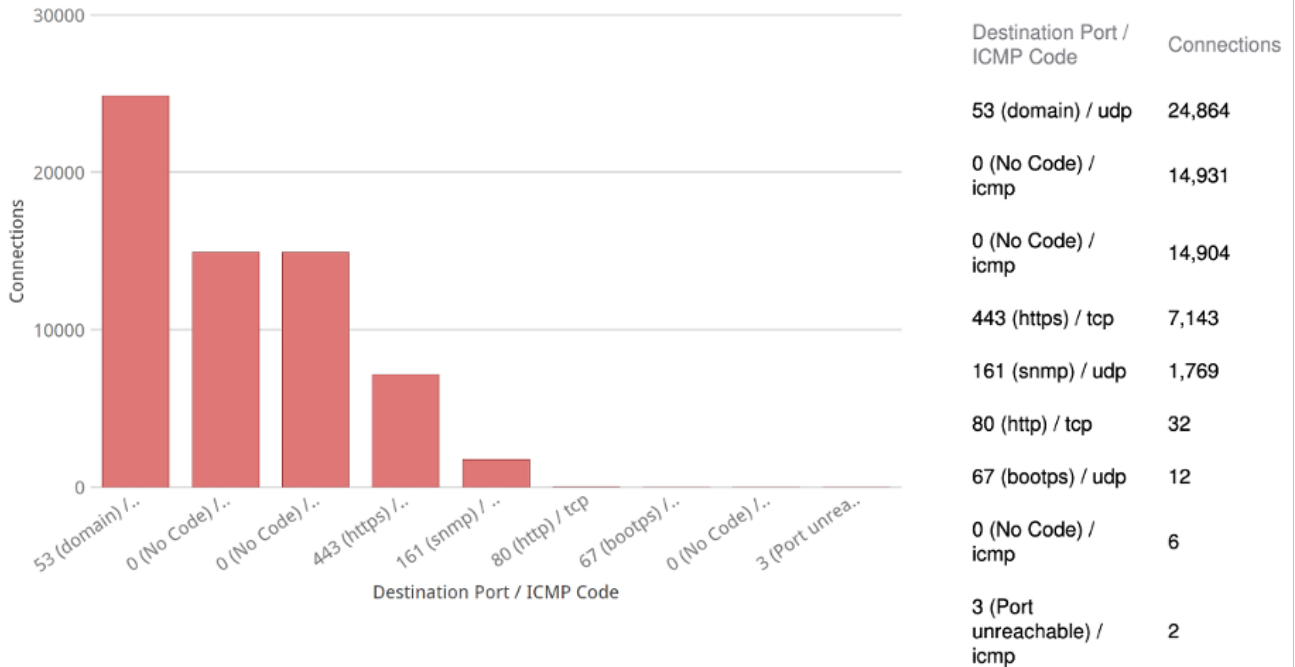
Port scanning

At last year's conference we saw several scans from a handheld scanning tool on the show floor. This year we applied the same monitoring techniques and saw more scans from the same family of scanning devices. In addition to the portscan detection mentioned in the prior section, we also perform large scale analysis of the traffic on the network, identifying and filtering high volume devices like media servers, and focusing on outliers. The chart below shows a traffic profile for one of the handheld scanners.

Table View of Connection Events

Time Window: 2024-05-05 00:00:00 - 2024-05-08 19:45:34

Constraints: Initiator IP =



The scanner iterated through its targets, hitting most of them 13-14 times via ICMP during the observed window.

Table View of Connection Events

Time Window: 2024-05-05 00:00:00 - 2024-05-08 20:04:59

Constraints: Initiator IP = Source Port / ICMP Type = 8 (Echo Request) / icmp



Digging into the packets from the same source IP revealed a user agent (redacted in the screenshot below) associated with the handheld scanning company.

No.	Time	Source	Destination
1	0.000000		
2	0.017008		

> Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624)

▼ Ethernet II, Src: [redacted]_55:08:ad (00:c0:17:55:08:ad), Dst: > Destination: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)

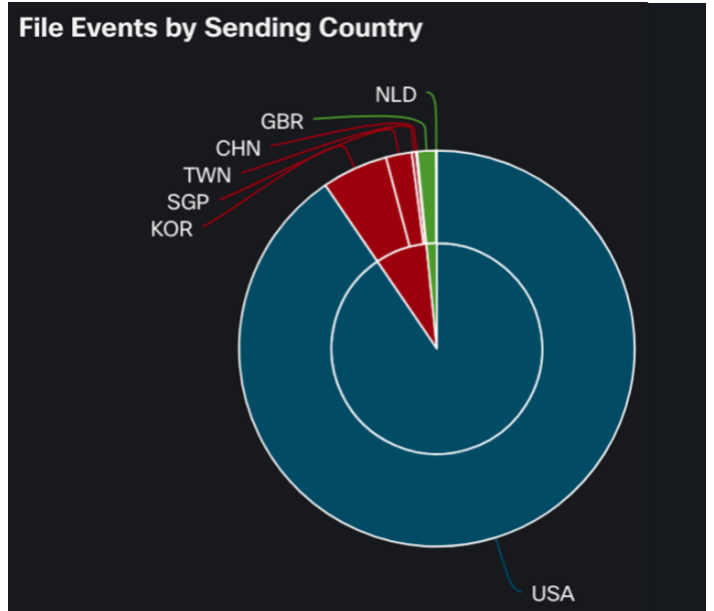
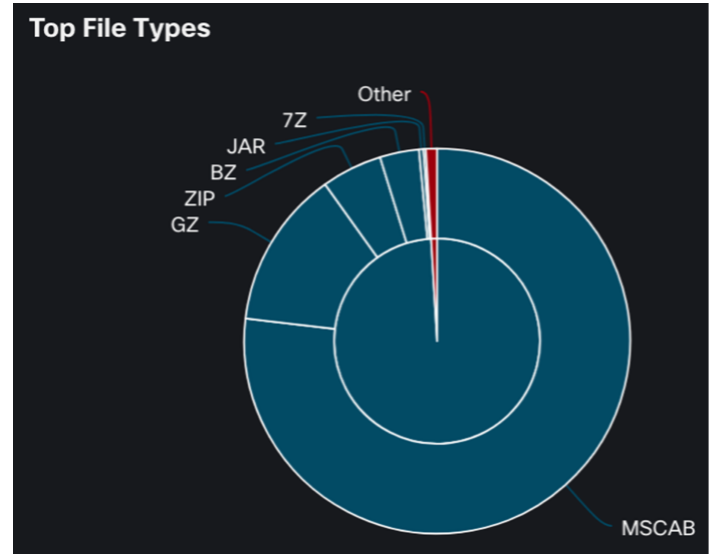
> Source: [redacted]_55:08:ad (00:c0:17:55:08:ad)

File transfers

File monitoring and analysis yields valuable insight into user activity and behavior on the network. While file transfers are often obscured by the growing prevalence of encrypted protocols, we do still see a large number of files at each conference. In 2024, MSCAB files dominated the list.

We also tracked geolocation data for file transfers. The US was unsurprisingly the top destination for file hosts, but we also saw file transfers to and from a number of other countries.

In 2024, most malware is transmitted over HTTPS. With the SOC Team at RSA Conference running in IDS mode on SPAN traffic, TLS decryption isn't possible, greatly limiting visibility. However, we still saw a heavy volume of traffic to malware related domains and caught some malware instances on the wire, as covered in the Malware Threats section.

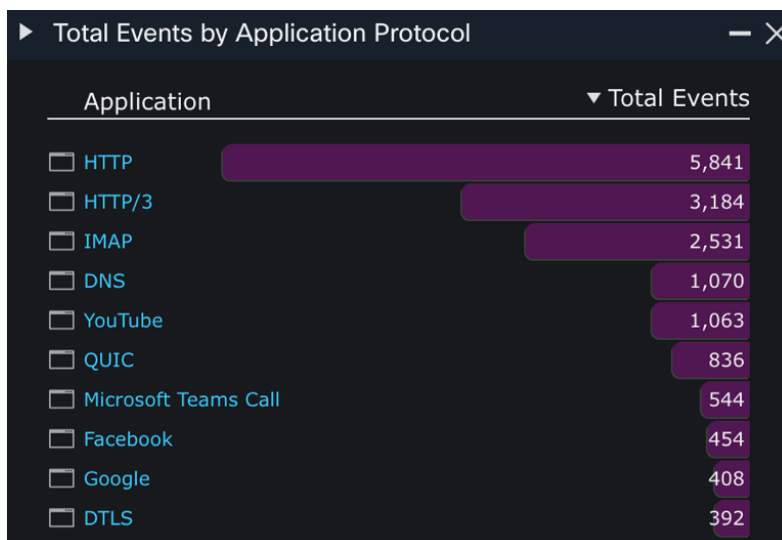
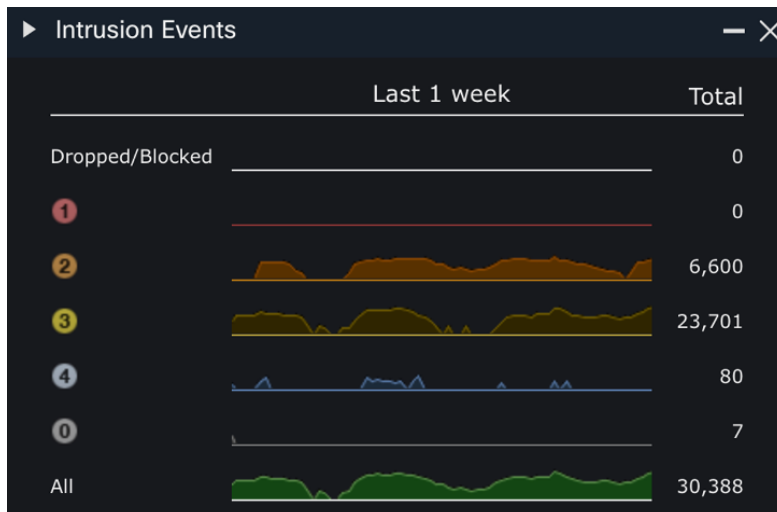


Intrusion information

Firepower detected many (attempted) intrusion events during the conference. Automated event analysis correlated threat events with contextual host profile data do automatically determine threat severity. Whenever a working exploit targeted a vulnerable host on the guest network, an Impact 1 event was raised. Intrusion events with the Impact 1 flag are automatically promoted to XDR incidents and can be investigated directly from the ribbon in FMC. For this conference we didn't witness any Impact 1 events, but we did see a very high volume of Impact 2 and Impact 3 intrusion events.

The application protocol that carried the most events was easily HTTP. This is not surprising given HTTP is both a common threat vector and an unencrypted protocol.

As with general network traffic, intrusion events spiked during the conference days and flat lined overnight. We saw an especially large volume of events on Wednesday.



Malware threats

Malware has always been a rapidly evolving area of security, and is a major focus for the SOC at each RSA Conference. Endpoint security does a lot of heavy lifting with malware detection in any real-world environment, but it obviously isn't an option for us on a guest wireless network like RSAC. Fortunately, Firepower offers us a wide array of capabilities for detecting malware activity and files.

When Firepower detects the start of a file transfer in a network packet, it will compile all the packets into the complete file, perform a file hash, and validate whether the file hash has a designation such as malware or clean. This hash check allows Firepower to check every observed file against a massive list of known malware.

For files with an unknown disposition, Firepower can perform additional analysis, including submitting the file to a sandbox. These layers of protection, from file hash checks, to onbox analysis, to sandboxing, provide multiple chances to catch malware as it transits the network. The below screenshots show a detected trojan from the conference that was masquerading as a uTorrent installer.

The screenshot displays the Firepower interface for a malware detection. The top section, titled "Malware Summary", shows search constraints and navigation options. Below this is a table with columns for Detection Name, File Name, and File SHA256. A single entry is visible with a red malware icon, File Name "utorrent.47082.installer.exe", and File SHA256 "44e91f68...bb21b857".

The bottom section, "Network File Trajectory for 44e91f68...bb21b857", provides detailed file information:

File SHA256	44e91f68...bb21b857	First Seen	2024-05-05 18:35:15 on [redacted]
File Name	utorrent.47082.installer.exe	Last Seen	2024-05-07 20:57:55 on [redacted]
File Size (KB)	3795.8203	Event Count	2
File Type	MSEXE	Seen On	2 hosts
File Category	Executables	Seen On Breakdown	1 sender → 1 receiver
Current Disposition	Malware		
Threat Score	None		
Detection Name	W32.Trojan.27hg.1201		

The trajectory section shows a timeline from May 05 to May 07, with a network diagram illustrating the path of the file between hosts. At the bottom, there are controls for actions like Transfer, Block, Create, Move, Execute, Scan, Retrospective, and Quarantine, along with disposition filters for Unknown, Malware, Clean, Custom, and Unavailable.

The above screenshot shows a feature of Firepower called Network File Trajectory that will trace the path of a malicious file from its origin across the network. In RSAC we only have one detection point so the trajectory is limited to only a host on the wireless network and an external public IP.

Metrics

95 Threat Score

Assets 1 Judgements 1 Verdicts 0 Indicators 1 Sources

Metadata

Sample ID	81880327da53c9999e05f7c223fa589d	Filename	utorrent.47082.installer.exe
Login	rsac_soc	Magic Type	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Name	RSAC SOC SMA Portal User	File Type	exe
Access	Public	First Seen	5/4/24 11:00:18 am
Virtual Machine	Windows 7 64-bit	Last Seen	5/8/24 3:30:15 pm
Started	5/8/24 3:30:21 pm	SHA-256	44e91f68e2440fcc567530b72bbe0d04c8fc...
Ended	5/8/24 3:39:17 pm	SHA-1	804c1a7738d16240c6a3333ee10127a1182679a9
Duration	0:08:56	MD5	d5bda33383b3ace63aa7df579ccef364
Playbook	Random Cursor Movement with Image Recognition	Tags	
Network Exit Localization	US - Pennsylvania - Philadelphia	FP/FN	0 False Positive / 0 False Negative

Behavioral Indicators

Only show Indicators with Orbital queries

Title	Categories	ATT&CK	Tags	Hits	Indicator Score
Artifact Flagged Malicious by Antivirus Service	Anti-Virus		antivirus, file	2	95
Signed Executable DLL Execution	Code Injection	Defense Evasion, Persistence, Privilege Escalation	DLL, DLL Hijacking, file, legitimate	1	85

Firepower and NetWitness integration

The Cisco Event Streamer (also known as eStreamer) enables users to stream Firepower System events to external client applications. You can stream host, discovery, correlation, compliance allow list, intrusion, user activity, file, malware, and connection data from a Management Center.

Plaintext playlist

Security is also awareness of external forces that could impact operations, including both natural and human factors. While conducting monitoring in coordination with the RSAC physical security team, the SOC threat hunters observed a peer-to-peer music sharing service with a very distinctive traffic format

Firewall Management Center
Analysis / Intrusions / Events

Event Information

- Message: palestine TCP keyword found, please investigate (2000:1000025:1)
- Time: 2024-05-07 19:49:30
- Classification: Unknown Traffic
- Priority: Invalid ID
- Device: RSA-SOC-FTD741
- Ingress Interface: SPAN2
- Source IP: [REDACTED]
- Source Port / ICMP Type: 2234 / tcp
- Source Country: GBR
- Destination IP: [REDACTED]
- Destination Port / ICMP Code: 60353 / tcp
- Intrusion Policy: RSA-IPS-Policy
- Access Control Policy: RSA-SOC-Policy
- Access Control Rule: New-Rule-#1-ALLOW
- Rule: alert tcp any any -> any any (msg:"palestine TCP keyword found, please investigate";

The music sharing program transmits user music searches in clear text. The end result is an unusual packet format with a long list of user music queries, sharing the preferences with the listening public

The screenshot shows the Firewall Management Center interface. The top navigation bar includes 'Overview' and 'Analysis'. The main content area displays a hierarchical view of network layers: Ethernet II, 802.1Q Virtual LAN, Internet Protocol Version 4, and Transmission Control Protocol. Below this, a list of 'Protocol' entries is shown, with a vertical white bar obscuring some details. At the bottom, specific event details are listed: Message Length (50), Message Type (Distributed Search (Byte: 3)), Integer (49), Username, Token (334), and Search Text.

Desperately seeking Canon

In addition to monitoring alerts for malicious activity, we also keep an eye on general network traffic to look for patterns of concern. Part of this process involves sorting through the noise. One bit of traffic that generated a lot of noise was the BJNP Discovery protocol, which is used to connect to Canon printers.

Connection Events (switch_workflow)

Search Constraints [Edit Search](#) [Save Search](#)

Connections with Application Details Table View of Connection Events

Jump to...

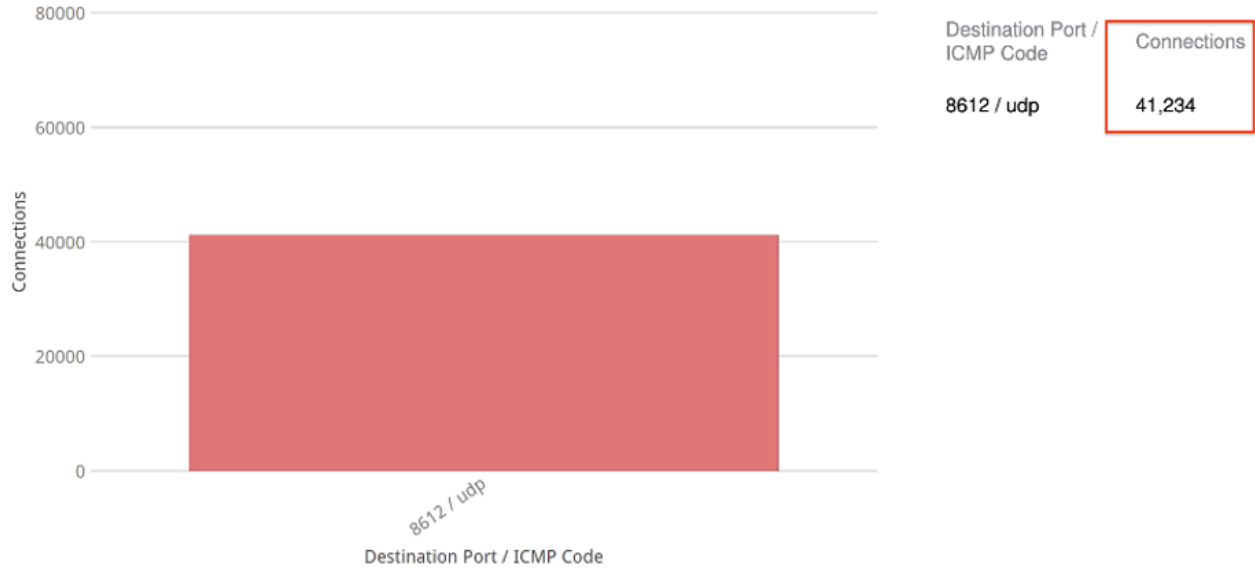
<input type="checkbox"/>	↓ First Packet x	Last Packet x	Action x	Initiator IP x	Responder IP x	Security Intelligence x Category	Source Port / ICMP Type x	Destination Port / ICMP Code x	Application Protocol x
▼ <input type="checkbox"/>	2024-05-08 18:49:06		Allow				49356 / udp	8612 / udp	<input type="checkbox"/> BJNP Discovery
▼ <input type="checkbox"/>	2024-05-08 18:49:02		Allow				54788 / udp	8612 / udp	<input type="checkbox"/> BJNP Discovery
▼ <input type="checkbox"/>	2024-05-08 18:49:02		Allow				54788 / udp	8612 / udp	<input type="checkbox"/> BJNP Discovery
▼ <input type="checkbox"/>	2024-05-08 18:49:02		Allow				54788 / udp	8612 / udp	<input type="checkbox"/> BJNP Discovery
▼ <input type="checkbox"/>	2024-05-08 18:49:02		Allow				54788 / udp	8612 / udp	<input type="checkbox"/> BJNP Discovery
▼ <input type="checkbox"/>	2024-05-08 18:49:01		Allow				54788 / udp	8612 / udp	<input type="checkbox"/> BJNP Discovery

Sifting through the top talkers lead us to just three endpoints that were generating the majority of BJNP traffic, a whopping 41,000 connections from only three hosts over a three-hour period.

Table View of Connection Events

Time Window: 2024-05-08 15:39:29 - 2024-05-08 18:39:29

Constraints: Destination Port / ICMP Code = 8612; Initiator IP =



Aside from putting load on the network infrastructure, could this traffic be malicious? Exploiting printers is a viable attack vector, and it's possible a malicious actor could search the network for an available and vulnerable printer.

One way to determine whether further investigation could be fruitful is to look at the results of those 41,000 attempted connections. FTD allows us to filter on dozens of traffic data points, including fields like responder packets and responder bytes. If a device on the network responded to a BJNP request, it would be worth our time to further review connections to that device and try to determine whether it was under attack or vulnerable. However, in the RSAC network, no device responded to the BJNP requests, as we can see by filtering the 41,000 events for sessions with at least one responder packet.

Attackers have a lot of advantages, from new zero-day vulnerabilities to encrypted traffic protocols that limit the visibility of security tools. However, network-based attacks still follow the basic laws of networking, and even encrypted network traffic leaves behind information that can provide a lot of valuable investigative data to a SOC.

Connection Events (switch_workflow)

▼ Search Constraints (Edit Search Save Search)

Connections with Application Details **Table View of Connection Events**

Destination Port / ICMP Code 8612

Responder Packets >0

Jump to...

<input type="checkbox"/>	↓ First Packet ×	Last Packet ×	Action ×	Initiator IP ×	Responder IP ×	Security Intelligence × Category	Source Port / ICMP Type ×	Destination Port / ICMP × Code	Application Protocol ×
No Records									

Other firepower statistics

Firewall user activity

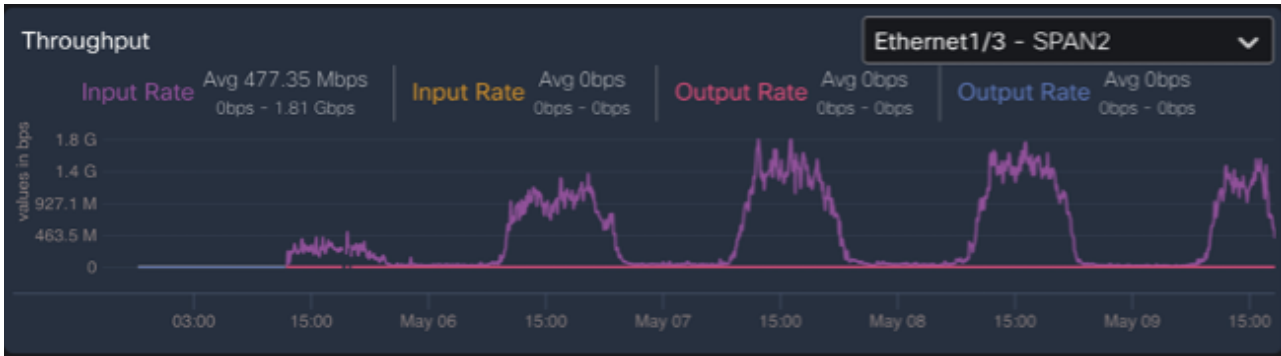
Firewall's deep packet inspection makes it capable of learning about every user's activity and capture details like Usernames/password from applications like FTP, SIP (VoIP), non-encrypted email (IMAP, POP3), API's not using encryption for many apps like an automatic dog feeder.

Time	Username	Event	Realm	Discovery Application	Authentication Type	IP Address	Start Port	End Port
2024-05-08 19:34:36	12484893004@	New User Identity	Discovered Identities	SIP	No Authentication			
2024-05-08 19:34:36	12484893004@	User Login	Discovered Identities	SIP	No Authentication			
2024-05-08 18:53:57	16693066319@	New User Identity	Discovered Identities	SIP	No Authentication			
2024-05-08 18:53:57	16693066319@	User Login	Discovered Identities	SIP	No Authentication			
2024-05-08 16:24:08	18186492183@	New User Identity	Discovered Identities	SIP	No Authentication			
2024-05-09 16:24:08	18186492183@	User Login	Discovered Identities	SIP	No Authentication			
2024-05-09 14:07:14	wpftp	New User Identity	Discovered Identities	FTP	No Authentication			
2024-05-09 14:07:14	wpftp	User Login	Discovered Identities	FTP	No Authentication			
2024-05-07 17:11:33	novalct	User Login	Discovered Identities	FTP	No Authentication			
2024-05-05 16:06:36	novalct	New User Identity	Discovered Identities	FTP	No Authentication			
2024-05-05 16:06:36	novalct	User Login	Discovered Identities	FTP	No Authentication			

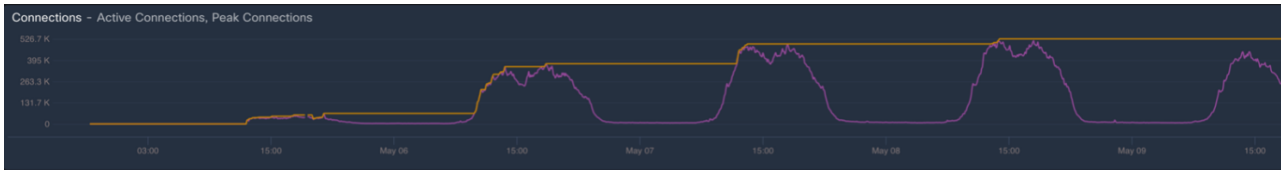
Firewall traffic summary

Following are some of the performance statistics for peak traffic, total number of connections and events/connections per second from firewall.

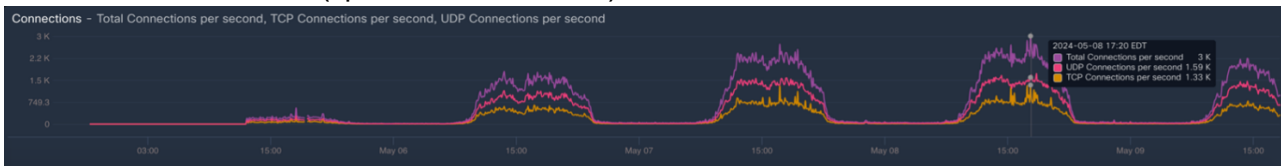
Peak Traffic: 1.83 Gbps (up from 1.52 Gbps in 2023)



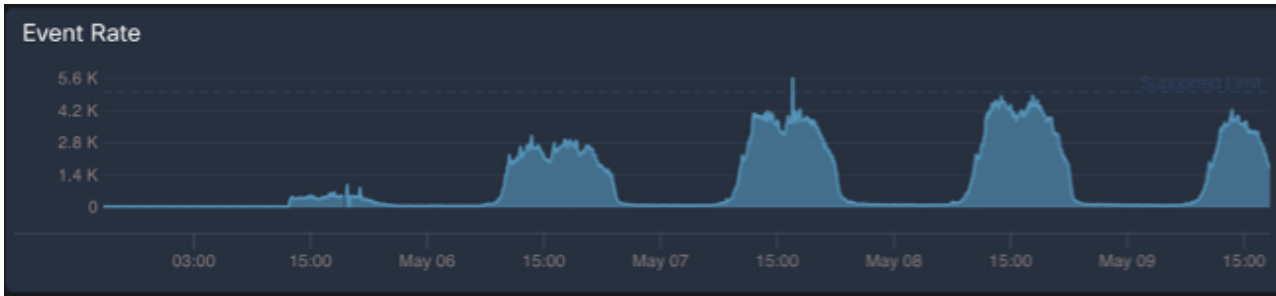
Peak Connections: 495K (up from 255K in 2023)



Connections/sec: 2.83K (up from 2.37K in 2023)



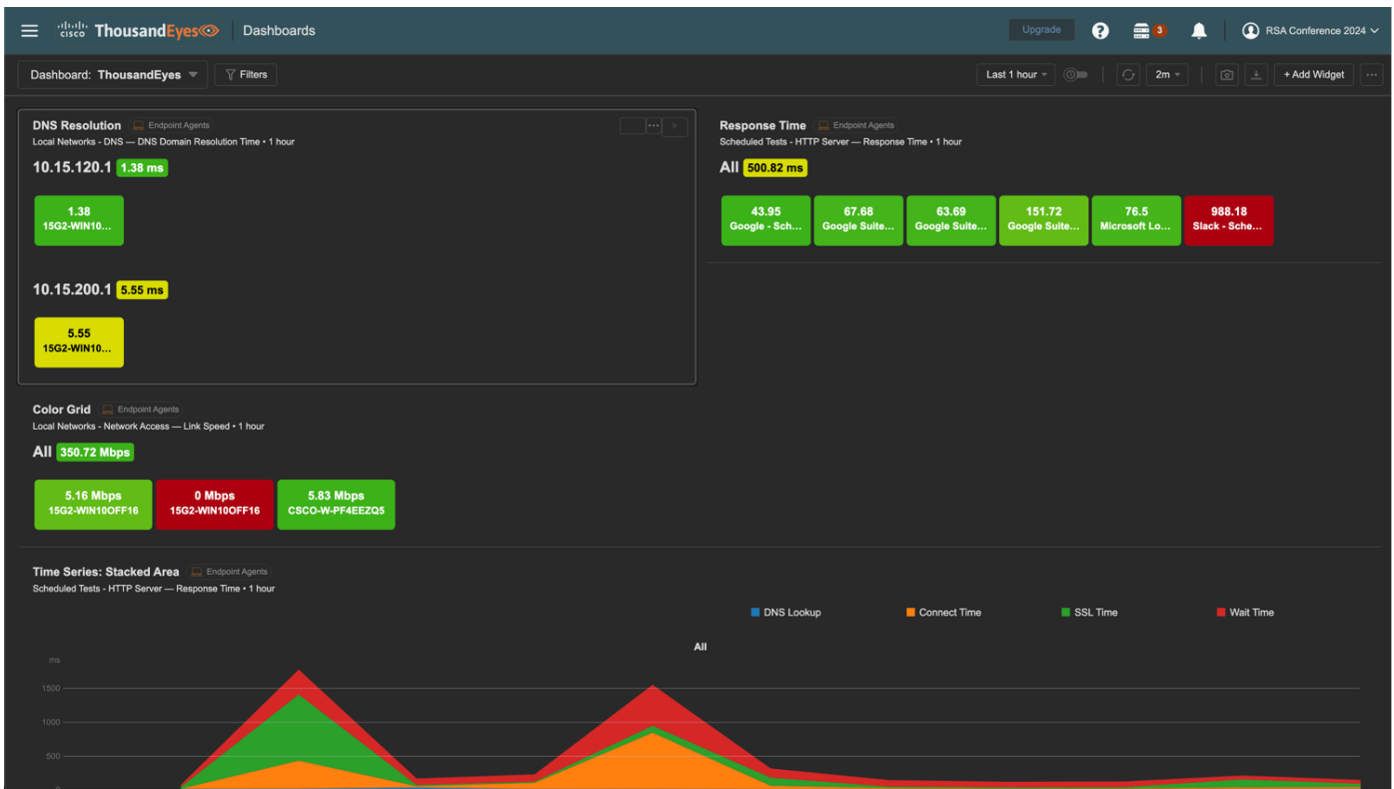
Event Rate: 4.6K/sec (up from 4.4K/sec in 2023)



Security Cloud

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.



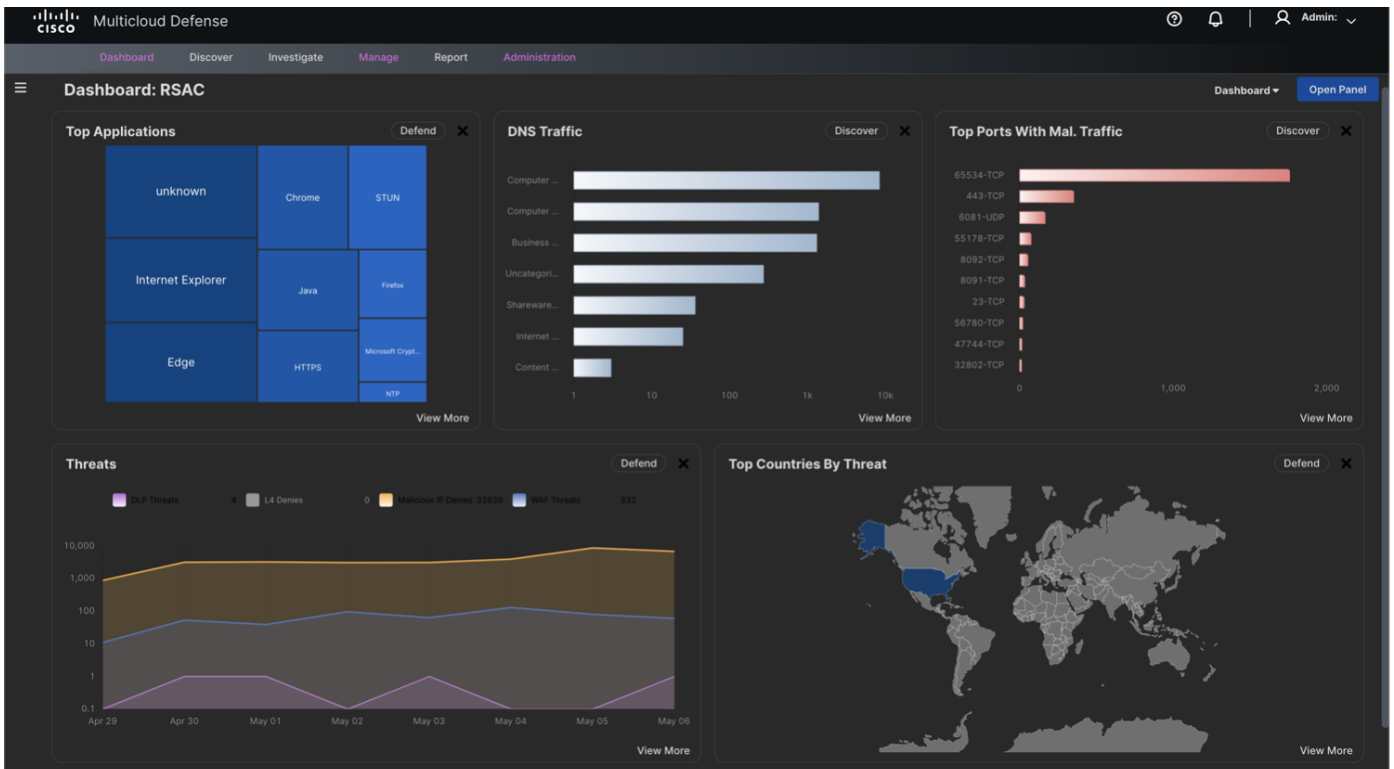
At one point, there was a damaged physical cable and we were able to confirm this with the Network Operations Center, to get a replacement installed. What was interesting, is that in ThousandEyes, we were able to see the exact same outages in ThousandEyes as we were experiencing, as seen below.

This helped us confirm it was a network issue and not a configuration issue, improving the communication with the Moscone Center to fix the cable.



Multicloud Defense

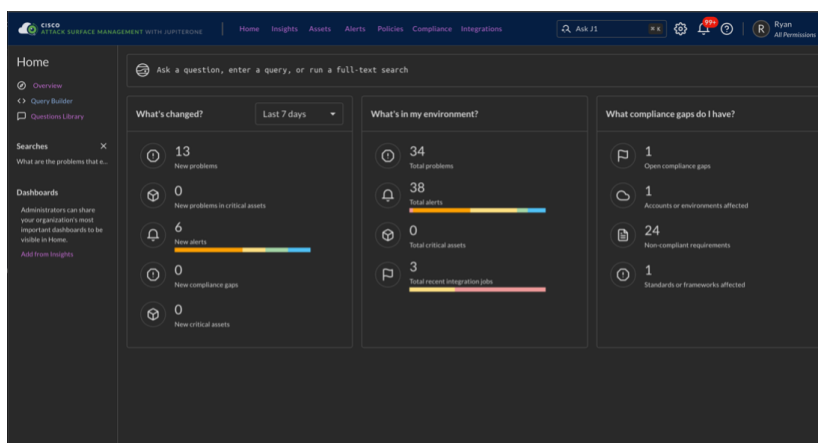
Multicloud Defense is Cisco's cloud native firewall offering. It makes deploying a firewall into the cloud and keeping them highly available easy. It also has similar features to what you would see with our FTD product. Leveraging the ease of deployment and the feature set Multicloud Defense provides,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



Attack Surface Management

You can think of it like an atlas. In an atlas it has countries, cities, roads, rivers, businesses, mountains, and the list goes on. Attack Surface Management (ASM) is the same as an atlas, as it finds all the entities in your environment and creates a map so we can easily find our assets and determine how they are related to each other. These assets can be a VM, API Key, IAM Role, firewall rules, and many more. Using ASM we proactively determine what kinds of relationships we have in our environment and validate that we do not have anything that will cause us problems or allow unintended access to our environment.

The second function we use in ASM are the problems and compliance gaps. Sure, we can find relationships for specific assets we know about, but there are shadow assets we might not think about or even knew existed. ASM is able to find those and let us know we have an issue. An example is having API keys that have not been rotated out in a specified amount of time. Not only does ASM consider it problem, but it falls into the compliance gap section too. Using ASM we can fix these issues and make sure our posture is up to snuff and nothing surprises us later.



Conclusion

Over the past few years, we've seen incremental progress in the adoption of encryption and secure protocols. However, 2024 marked a regression compared to 2023 and 2022. While we have the potential to make significant strides toward enhanced security, it is crucial that we learn to safeguard our valuable information more effectively. Our analysis of the free public wireless network reveals a concerning trend: we are still leaking an excessive amount of sensitive data. This is a call to action for all of us 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 only rose two percent to 80 percent. Encrypt, encrypt...trust, but verify!

As threat actors evolve, we as an industry need to stay ahead of them which requires ongoing learning and collaboration amongst teams. The collaboration within the SOC has led to many advancements in our technologies which our customers benefit from. As AI advances we can leverage it to analyze large amounts of data and provide a result, 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 next year's RSAC and reporting the results to you. The SOC Team at RSA 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 2025!

Acknowledgments

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



Cisco Staff and Report Contributors:

Jessica Bair Oppenheimer	<i>Cisco SOC Leader</i>
Christian Clasen	<i>Team Manager</i>
Aditya Sankar / Ben Greenbaum / Steve Nowell	<i>Breach Protection Suite</i>
Justin Murphy	<i>User Protection Suite</i>
Dinkar Sharma / Adam Kilgore	<i>Cisco Secure Firewall</i>
Sayed Khadem	<i>Splunk / Cloud Protection Suite</i>
Ryan Maclennan	<i>Innovation / Cloud Protection Suite</i>

Special Thanks to Eric Kostlan for essential SOC in a Box hardware support.

NetWitness Staff

Steve Fink, NetWitness SOC Leader

Jack Riley

Andrew Jackman

Alessandro Zatti

Alessandro Contini

Marco Faggian

Steve Baer

IBM Threat Hunter

Neil 'Grifter' Wyler



©2024 NetWitness LLC. All rights reserved. NetWitness and the NetWitness logo, are registered trademarks or trademarks of NetWitness LLC. All rights reserved. in the United States and other countries. All other trademarks are the property of their respective owners. NetWitness believes the information in this document is accurate. The information is subject to change without notice. NetWitness provides comprehensive and highly scalable threat detection and response capabilities for organizations around the world. The NetWitness Platform delivers complete visibility combined with applied threat intelligence and user behavior analytics to detect, prioritize, investigate threats, and automate response. This empowers security analysts to be more efficient and stay ahead of business-impacting threats.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R) 1417746854 09/24