RSA CONFERENCE™ 2023

SECURITY OPERATIONS CENTER FINDINGS REPORT

Published by

Written by
David Glover, Jessica Bair Oppenheimer, and Steve Fink

Contents

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®, a RSA Security LLC company ("NetWitness") and Cisco Systems, Inc. ("Cisco") that monitors network activity during the course of the RSA Conference event.
- By connecting to Moscone Center WIFI 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, except for Cisco Umbrella DNS, and only 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 a Findings Report issued by sponsors RSA and Cisco.
- The RSAC SOC team is not part of the RSAC security team. As such, the RSAC SOC acted as an educational exercise only 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 RSAC SOC has been wiped and a certificate of completion is held by RSAC.

THE NETWORK

The RSA CONFERENCE 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.

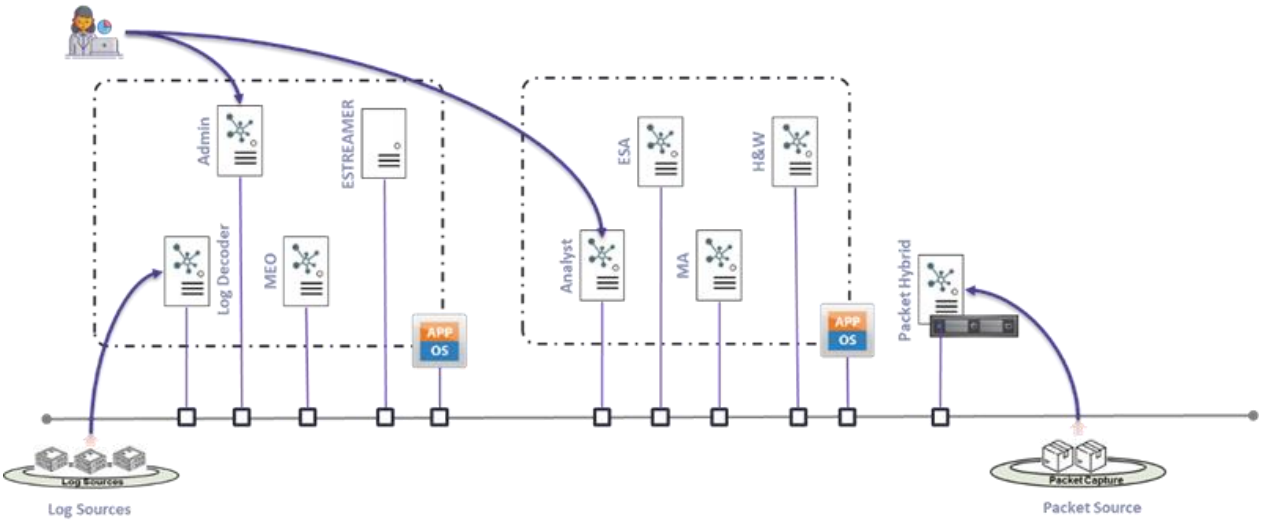
TECHNOLOGY USED IN THE RSAC SOC

The RSAC SOC team deployed the NetWitness platform, including NetWitness® Network, NetWitness® Logs and NetWitness® Orchestrator. Also, Cisco XDR, Cisco Secure Malware Analytics (formerly Cisco Threat Grid), Cisco Talos Intelligence, Cisco Firepower Threat Defense Intrusion Detection, Cisco Secure Cloud Analytics, Cisco Defense Orchestrator and Cisco Umbrella®.

For threat intelligence, the SOC received donated licenses from alphaMountain.ai, IBM X-Force Exchange, Recorded Future and Pulsedive, along with open-source threat intelligence.

NetWitness Logs 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 sessionized metadata that serves to accelerate alerting and analysis.

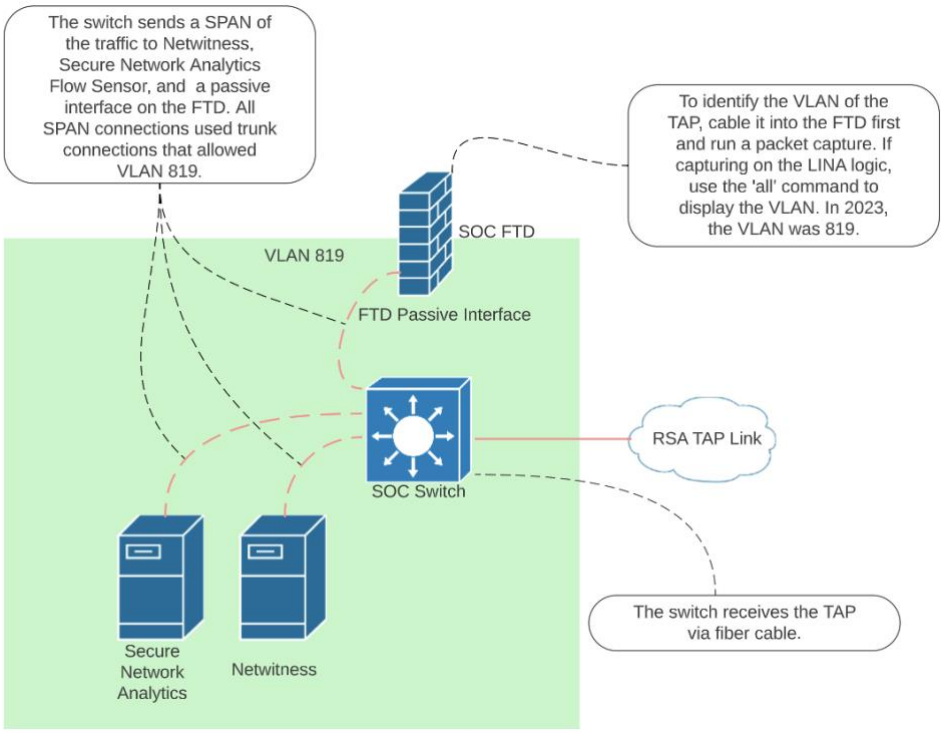
NetWitness Network provides real-time visibility into network traffic. It enables detection and threat hunting with streamlined workflows and automated investigation tools used to monitor the timing and movements of threat actors. NetWitness Network utilizes correlation, data science and threat intelligence to detect anomaly and speed response. The proprietary capability to reconstruct the full communication sessions permits to have a 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 a raw packet again. This capability permits also to extract file also if it's incapsulated in a non-standard/unknown protocol.



NetWitness Orchestrator built on ThreatConnect™ is a comprehensive security operation and automation technology that combines full case management, intelligent automation and orchestration, and collaborative investigation. Netwitness Orchestrator is not only a SOAR, it also implements a complete threat intelligence platform. NetWitness Orchestrator leverages threat intelligence across all orchestration and automation functions, for rich context and playbooks that adapt continually.

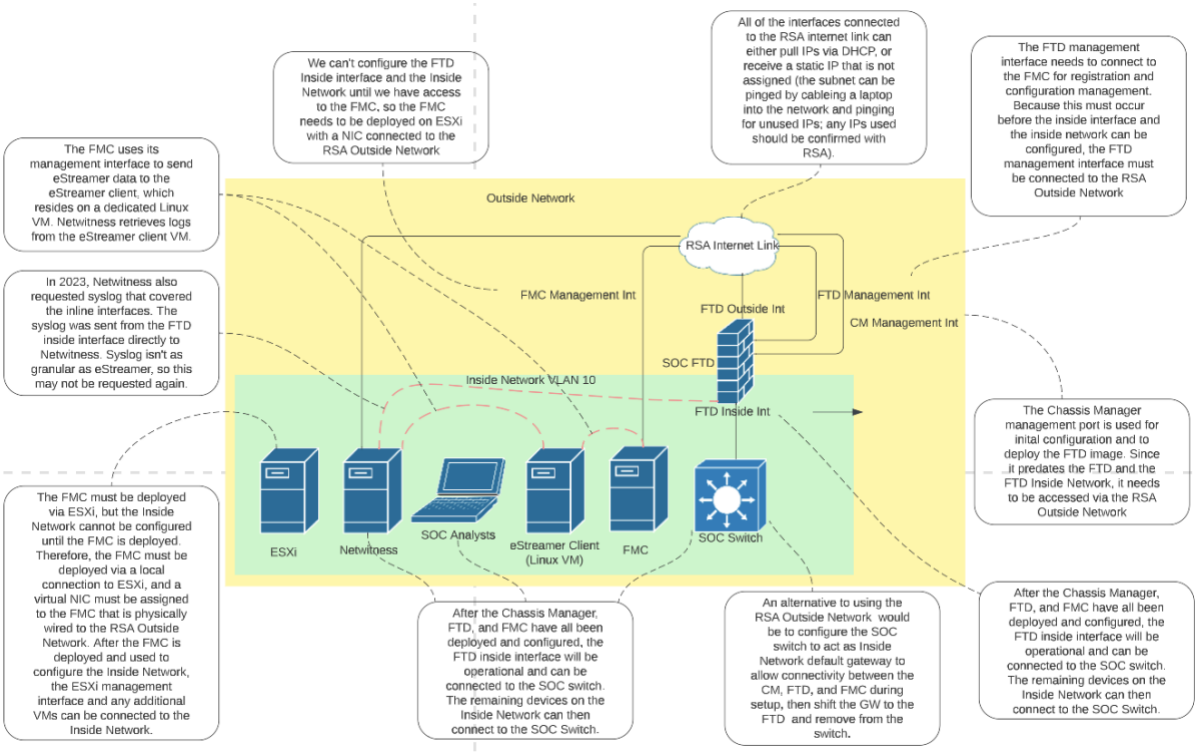
The RSAC installation of NetWitness was composed of a physical and virtual appliance. The physical one simplified the cabling to the traffic mirror port.

NetWitness collected all the raw network traffic from a switch port analyzer (SPAN) 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, the 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 checked 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 Secure Malware Analytics for dynamic malware analysis.

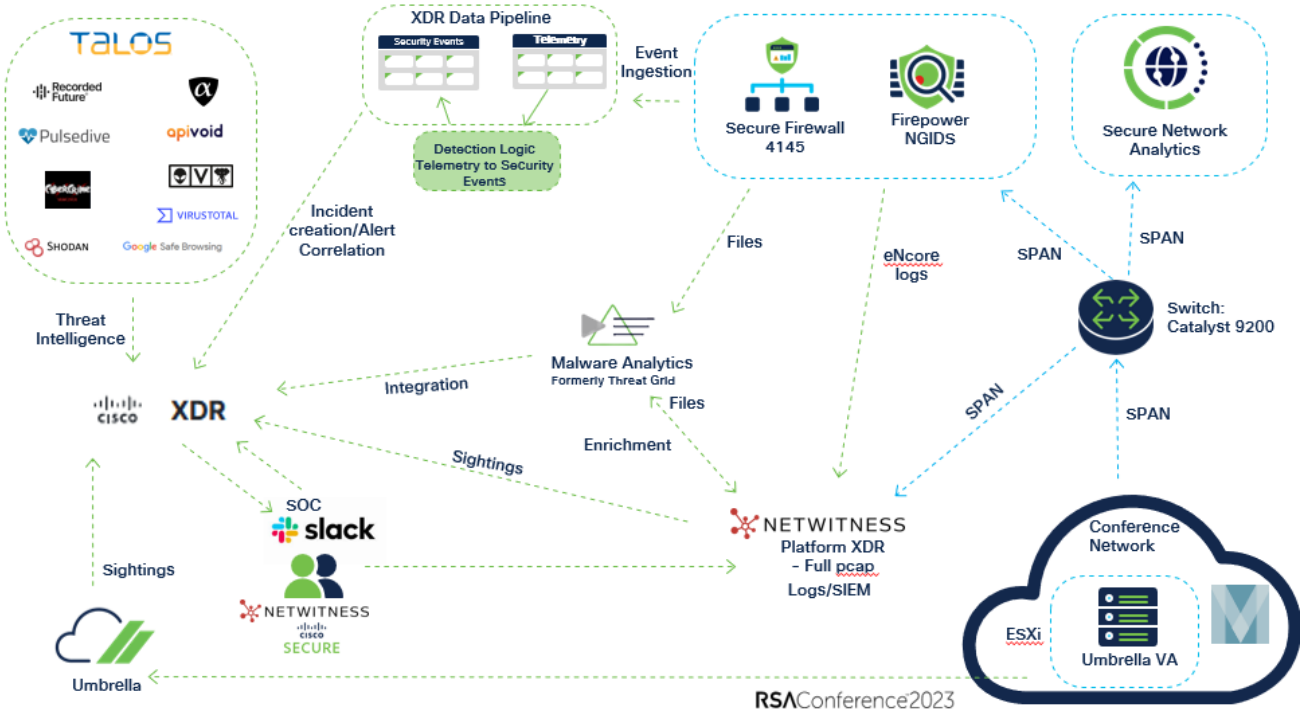
Secure Malware Analytics combined advanced sandboxing with threat intelligence in one unified solution to protect organizations from malware. It analyzed the behavior of a file against millions of samples and billions of malware artifacts. With Secure Malware Analytics, the RSAC SOC team had a global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

Secure Malware Analytics identified key behavioral indicators of malware and their associated campaigns, which enabled the RSAC SOC team to save time by quickly prioritizing attacks with the biggest potential impact. The built- in Glovebox user interaction tool made it possible to safely interact with samples and observe malware behavior directly.

Cisco Secure Firewall Firepower Threat Defense IDS received the same network SPAN as RSA NetWitness Network. The IDS inspected all wireless guest traffic from event attendees, configured in monitor-only mode. Firepower Threat Defense offered breach detection, threat discovery and security automation. Rich contextual information (such as applications, operating systems, vulnerabilities, intrusions, and transferred files) served the SOC to help uncover threats lurking on the network. The

Malware Analysis of the Secure Firewall Threat Defense also sent samples to Secure Malware Analytics for analysis.

Cisco Umbrella provided visibility into DNS activity, with default security blocking turned off. We also used Cisco XDR, which integrated threat intelligence from the Cisco Talos intelligence team and other sources, along with correlating sightings of indicators of compromise / observables from NetWitness and the Cisco Secure Firewall / Firepower logs and Umbrella DNS queries, along with the network visibility from Secure Cloud Analytics. Below is a visual representation of the technology used at the RSAC SOC.

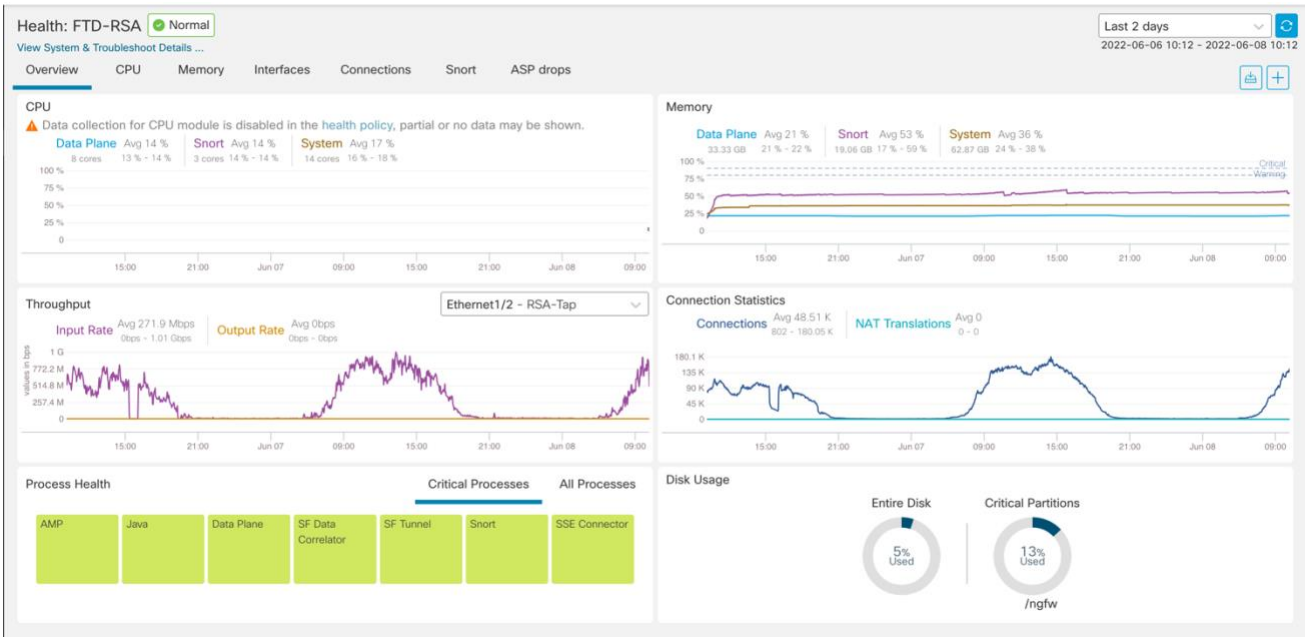


THE STATISTICS

A commonly requested RSAC SOC Findings session, attendees requested more statistics. The RSAC SOC team tried their best to provide more statistics and refined context and granularity.

2023 Stats

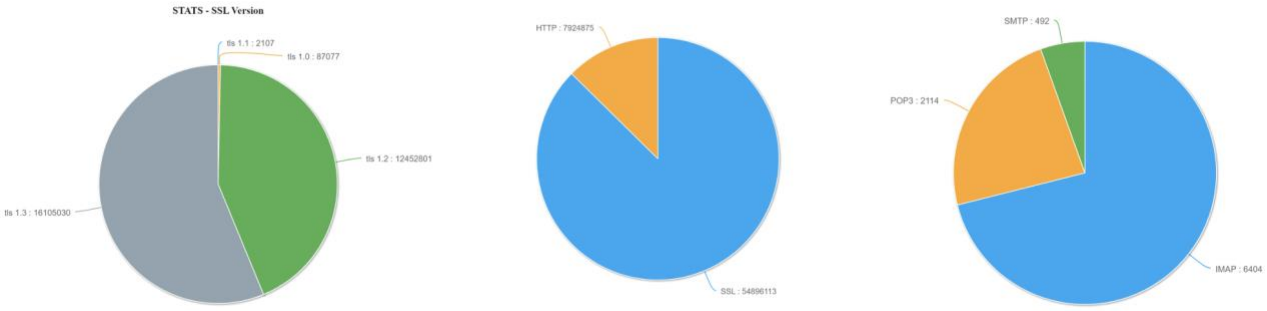
Year	**2023**	**2022**
Attendees	~39,000	**~19,000**
Total packets captured	18.5billion	**11.8 billion**
Total logs captured	214.7million	**108 million**
Total sessions	383 million	187.3 million
Total unique devices	~40k	13,253
Total packets written to disk	16.26 terabytes	**7.39 terabytes**
Total logs written to disk	774 gigabytes	50.8 gigabytes
Peak bandwidth utilization	1.8 Gbps	1.35 Gbps
DNS Requests	~61 million	**~46 million**
Total clear text username/passwords	20,040	**55,525**
Unique devices/accounts with clear text user names/passwords	317	**2,210**
Files sent for malware analysis	7,500+	**570+**



THE DATA

The RSAC SOC started analyzing all wireless traffic on Monday, April 24, and collected traffic through Thursday, April 27, 2023, at 3p.m. There were 383 million sessions during this period. Which was ~2 times the amount of traffic collected from RSAC 2022. This corresponds to a bandwidth utilization of 1.8 Gbps vs. 2020 of 1.3 Gbps and 740 Mbps in 2019.

Historically speaking, for events where this team has provided services like this, such as in the United States and the United Kingdom, the average percentage of encrypted vs. unencrypted traffic has varied from 60-78 percent encrypted and 22-40 percent unencrypted. For RSAC 2023, the SOC saw a downtrend in the amount of encrypted traffic, at 75 percent, from 78 percent in both RSAC 2019 and 2020. 55,029,102 of the 70,440,998 sessions were encrypted.



Encrypted vs. Unencrypted

Encryption of traffic is relevant because of the amount of information that RSAC attendees leak. The 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 allow the RSAC SOC 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. 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.

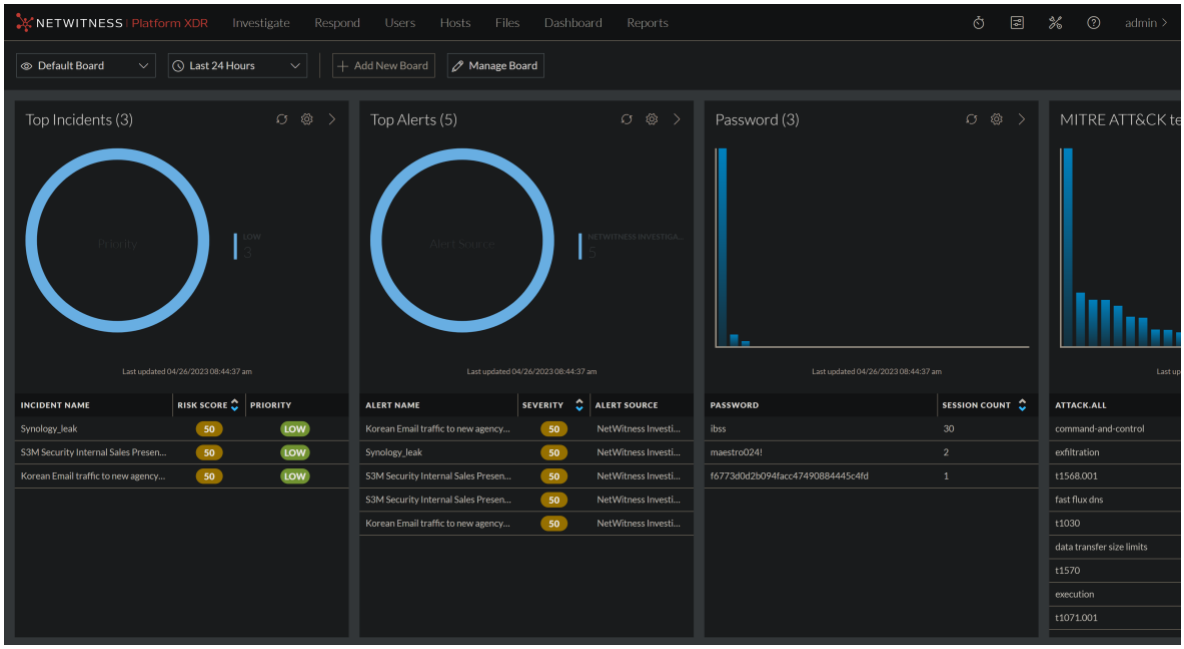
The role of the RSAC SOC around this issue is to help educate RSAC attendees about the information that is readily available on a public wireless network. In the past, we have spoken to many people on SOC tours about their mobile applications. We have seen mobile applications such as dating and home 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 RSAC SOC saw 20,040 cleartext passwords (down from 96,361 in 2020) from 317 unique accounts (down from 2,178 in 2020). Both are an improvement from 2019, when nobody on the RSAC SOC team wanted to figure out the number because it exceeded the counter that maxed out at 100,000+. There is a lot to discuss when throwing out a number this large for a four-day conference of security professionals on a public wireless network, so let's dig in.

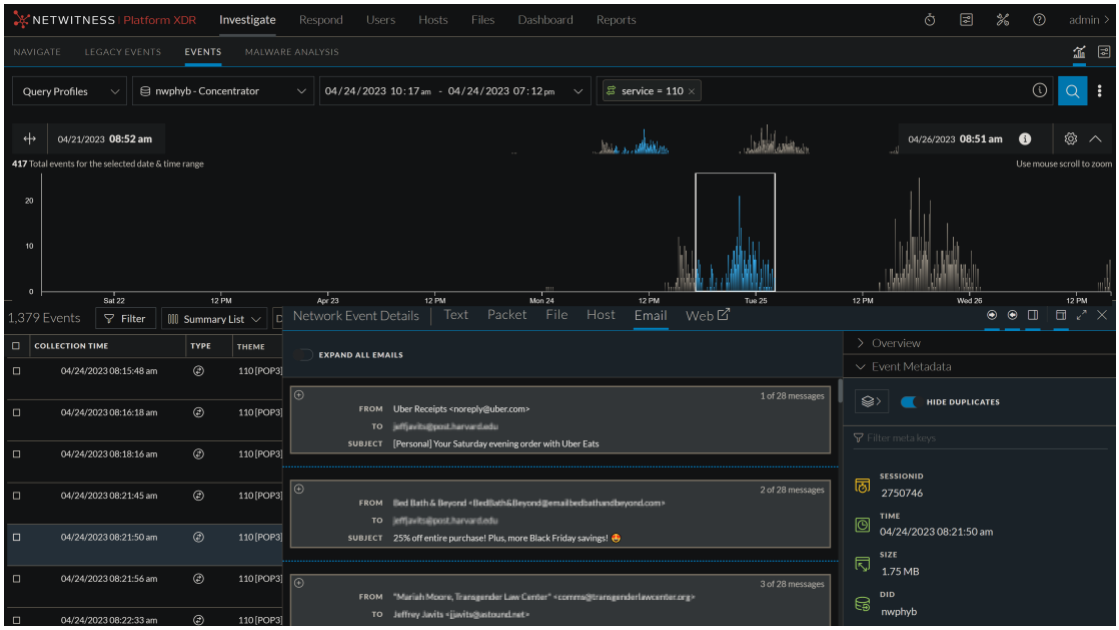
Cleartext Usernames and Passwords: SNMP

Some of the cleartext usernames and passwords came from corporate devices using older Simple Network Management Protocol (SNMP) versions 1 and 2. This is not necessarily a high-fidelity threat; however, it does leak information about the device as well as the organization with which it's trying to communicate. SNMPv3 adds security to the protocol, so this is something organizations can implement to avoid prying eyes.



MITRE Mapping

Security Events



Cleartext Usernames and Passwords: POP3/IMAP2/HTTP

Removing SNMP from the cleartext username and password totals, we can start to focus on the attendees' security posture.

	Password	Total events count
1	[redacted]	15806
2		778
3		633
4		286
5		278
6		278
7		180
8		158
9		153
10		128
11		113
12		113
13		111
14		103
15		94
16		93
17		78
18		60
19		57
20		56

Security conferences typically have many vendors displaying their wares on the expo floor. RSAC is no exception, and some of these cleartext usernames and passwords appeared to be from demo environments. Looking at other protocols, the majority of the cleartext usernames and passwords came from older protocols such as POP3, IMAP2, HTTP and FTP.

The use of POP3, IMAP2 and HTTP could provide an interesting conversation about who, what, where and why. It is difficult to send email in cleartext these days, and analyzing these incidents found similarities. Most of this traffic was to and from hosted domains. This means email services on domains that are family names or small businesses. The RSAC SOC team plans to work with RSAC to help notify those who are sending email in cleartext.

A nice consideration about this finding. Users are now also using strong and complex passwords. Unfortunately, you can use any kind of complex password but if no encryption is adopted no strong password is strong enough to protect data confidentiality.

Cleartext Usernames and Passwords: Password Security, Protocol Insecurity

Further investigation into the POP3, IMAP2 and HTTP protocols raised some interesting questions about users and their lack of understanding about password strength vs. protocol. Most major online email providers use Secure Socket Layer (SSL) security, and these providers, for the most part, are not in cleartext. So, what's the issue?

Once again, within the cleartext username and password data, there were passwords that were very complex. This means the passwords were long, and they had upper- and lower-case, numeric and

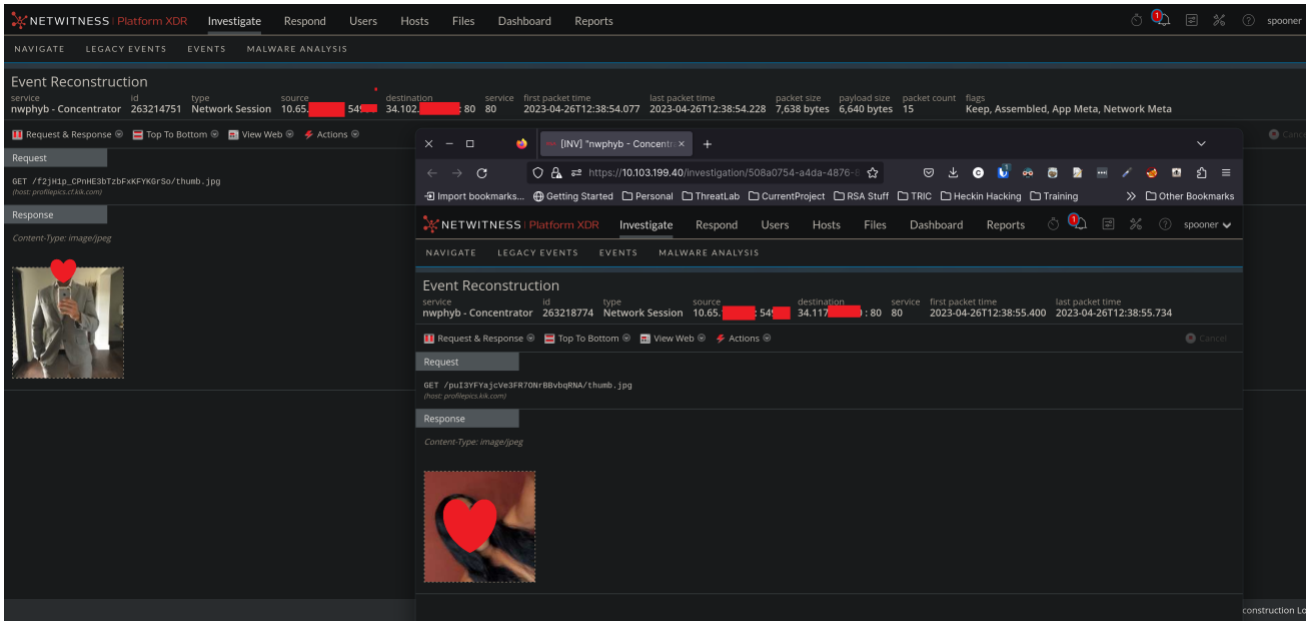
special characters. Password security is very important, but if we do not understand the protocols we use, our efforts in security education are wasted. The passwords are complex (red rectangles in the image above), but it doesn't matter because they were sending the data in cleartext. Ultimately, you must understand your device and its protocols, and use strong passwords—because as strong as some of these were, they were in cleartext.

Stories of Insecurity

During the RSAC, we observed evidence 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 some clear evidence of this.

Dating App, password (sometimes) strong but in Clear Text

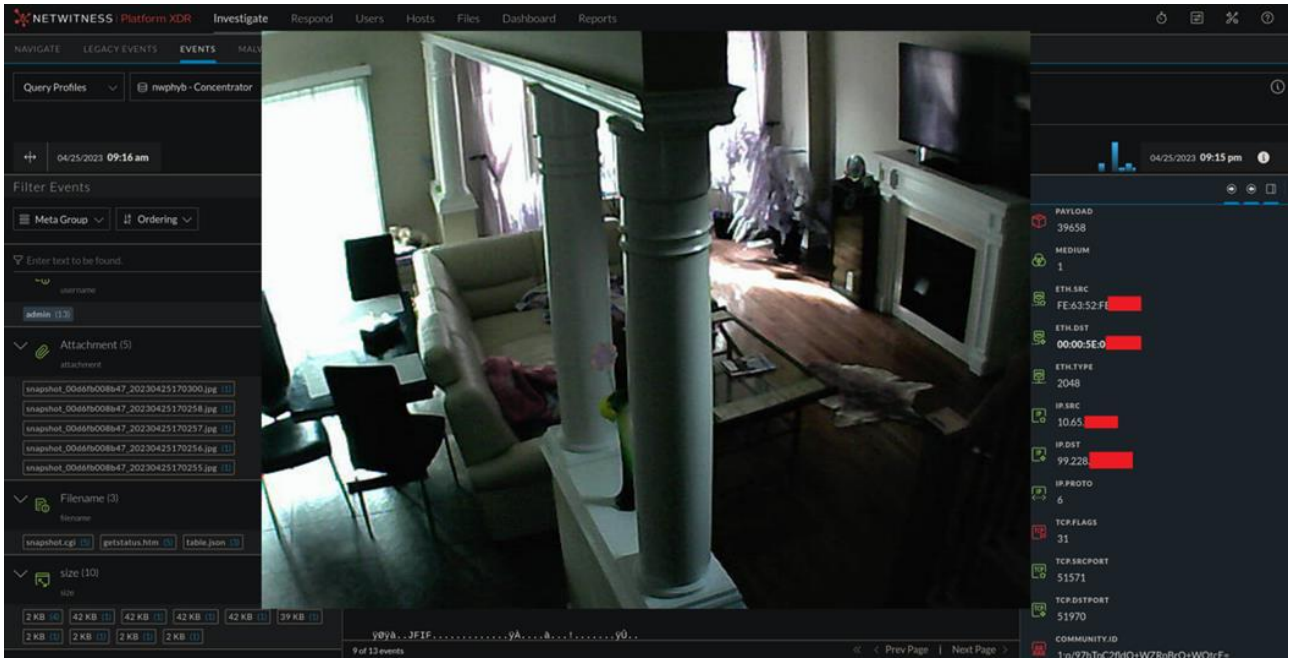
In a popular messaging dating App, the profile pictures transfer to the clear before the encrypted messages go through. Although we can't see what they're saying, it's interesting that we can potentially see who the person is visually talking to. Netwitness evidenced unencrypted traffic and the full session was reconstructed. In this specific scenario, users who configured a password are sure about the security, but they weren't aware of the clear text.



Internet of Things

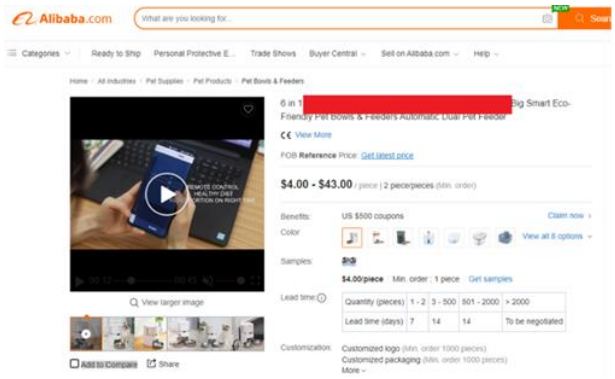
Also, IoT is affected by insecure protocols or misconfiguration. Someone's security cam must have been triggered via motion. There appears to be about 5 images ('snapshots') sent over when that occurs. The rest of the communication is encrypted, but the images and credentials move in the clear (password is both in the clear and in base64).

The username (full email address) was transmitted in the clear, with an encrypted password. However, the IOT device responded to the device's admin user and password in clear text.



This specific situation evidenced how not all the developers and engineers for IoT are adopting security development and a strong security. In these scenarios, we don't just have a behavior of compromise, but also a risk for the privacy.

Also, our pets are at risk for the privacy and…for the food. NetWitness platform found unencrypted traffic related to an app to manage our pets and their daily feeding. Also in this case, the credential was in clear text and the credential too.



Lesson Learned. Long story short. The user doesn't always know what an app, a platform, or a system is doing under the hood. An important suggestion when connecting to a public wifi is to limit the use to a secure and encrypted one. When this is not possible it is always best practice to start a VPN tunnel.

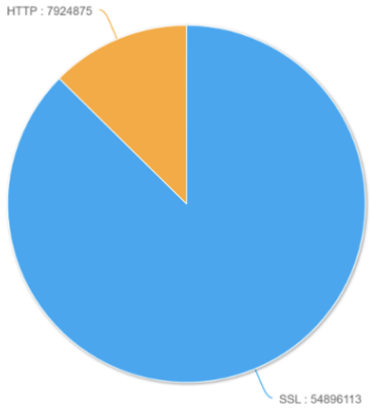
Unsecure Vendor

A user was using a VPN tunnel from a famous security enterprise vendor used by his company. Unfortunately, it wasn't working as expected. The application created the tunnel, but the traffic was not encrypted, and the communication was totally in clear text. You can also leverage on the famous security vendor, but you should always configure it in the best way possible.

Lesson Learned: Companies that adopt a security platform to protect the asset should also ensure that the system is working as expected and leverage the right competencies to guarantee the correct configuration. Also, proactive and periodical checks of the security posture of security tools are a good approach to ensure time by time everything is working as expected.

HTTPS -> HTTP

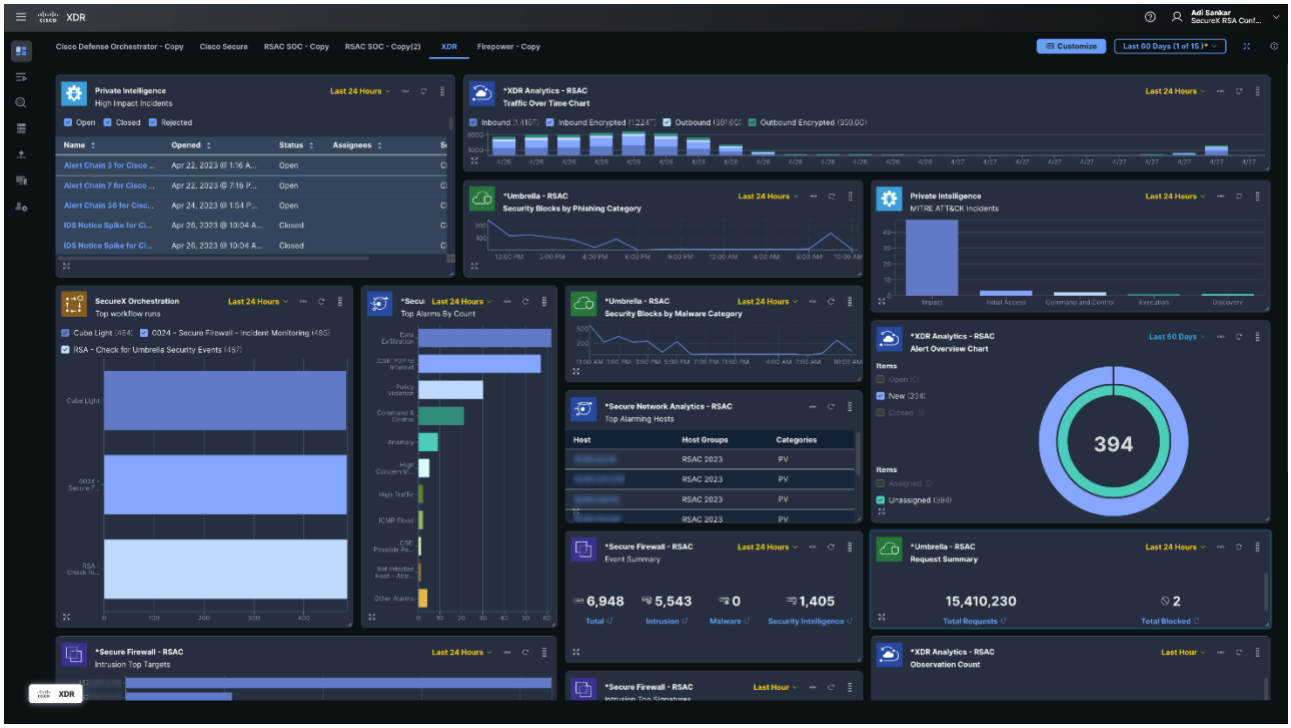
We are trained as security professionals to look for the HTTPS:// in the browser bar, especially when working with private information like our health care and family data.



INTEGRATION AND THREAT HUNTING

Cisco brought Cisco XDR, Umbrella, Secure Firewall, Secure Malware Analytics, Secure Cloud Analytics, Cisco Defense Orchestration, Secure Network Analytics, and Cisco Telemetry Broker, to provide visibility and integrate with NetWitness and threat intelligence partners.

The Cisco XDR Control Center widgets provided insights into the network data and any threats.



Widgets included network analytics, Umbrella DNS, Malware Analysis, and Firewall Intrusion Detection.

To aid in Threat Hunting, we integrated threat intelligence from several sources.

Cisco Secure Threat Intelligence

- Cisco XDR public intelligence
- Cisco Secure Endpoint's File Reputation Database
- Cisco Talos Intelligence

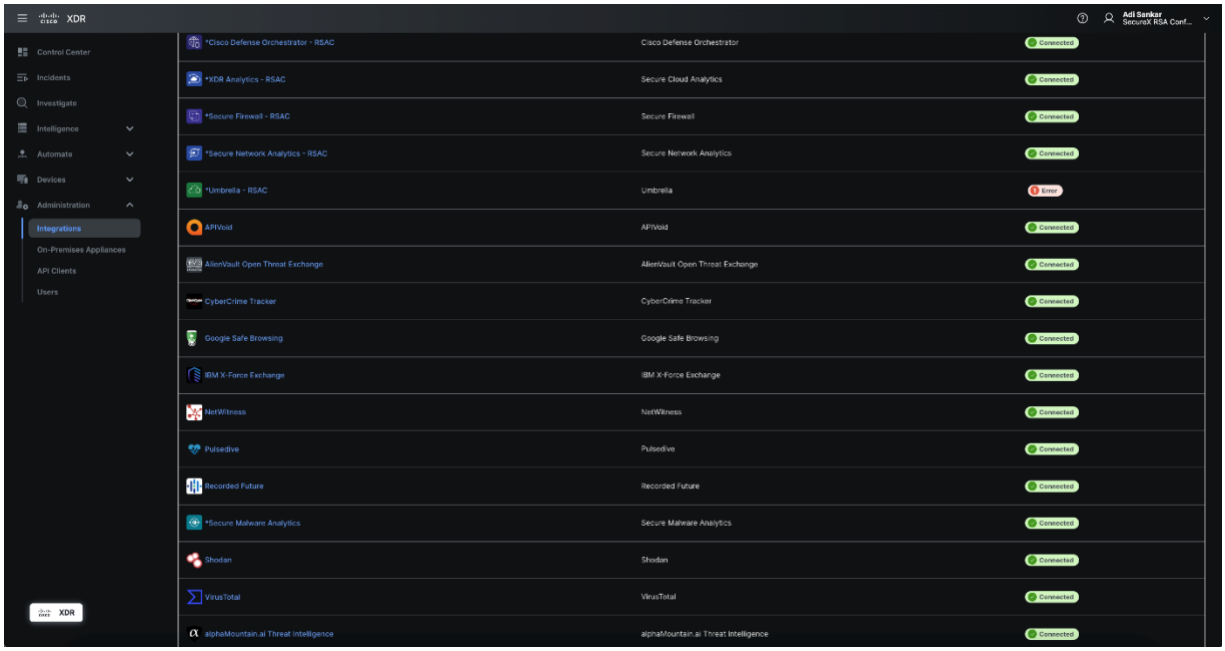
Donated Partner Threat Intelligence

- alphaMountain.ai threat intelligence
- IBM X-Force Exchange threat intelligence
- Pulsedive threat intelligence
- Recorded Future threat intelligence

Open-Source Threat Intelligence (correlated through Cisco XDR)

- APIVoid
- AlienVault Open Threat Exchange
- CyberCrime Tracker
- Google Safe Browsing
- Shodan
- Threatscore | Cyberprotect
- VirusTotal

The activated integrations are below.



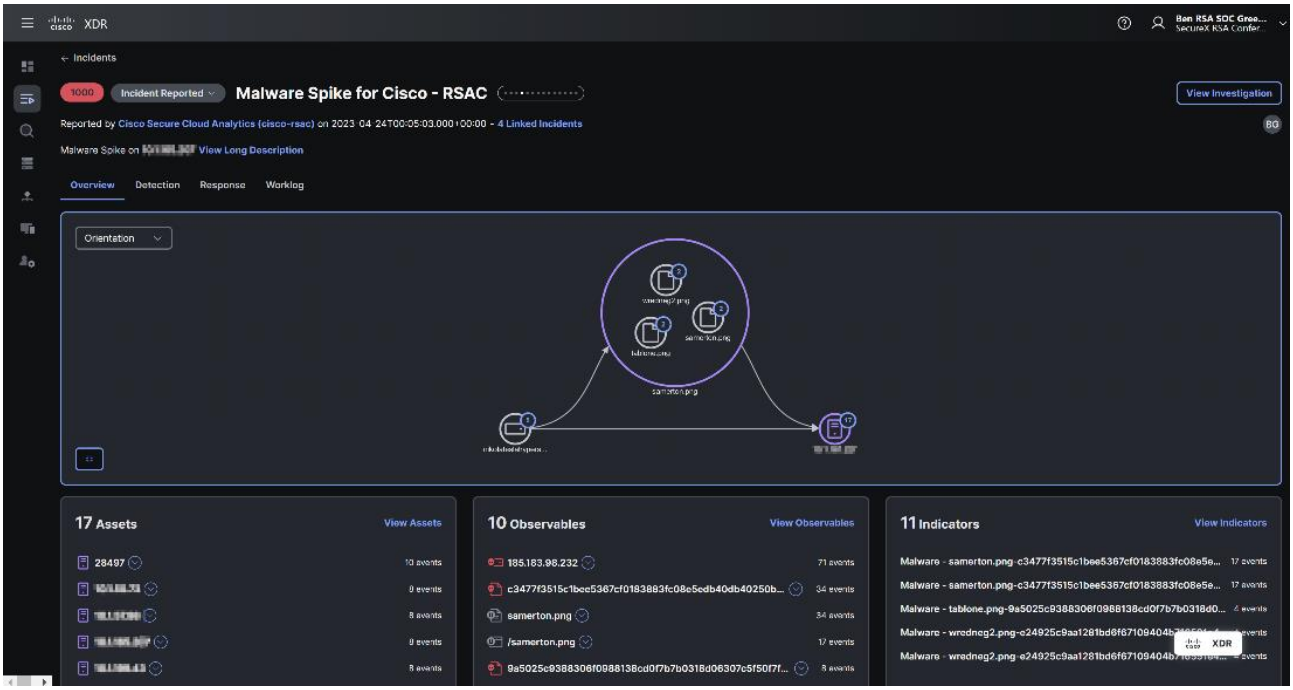
Cisco built a custom integration with NetWitness to visualize sightings, targets and relationships during investigations. This custom integration connects the NetWitness platform hosted at the RSAC conference, using Security Services Exchange.

Investigating Malware

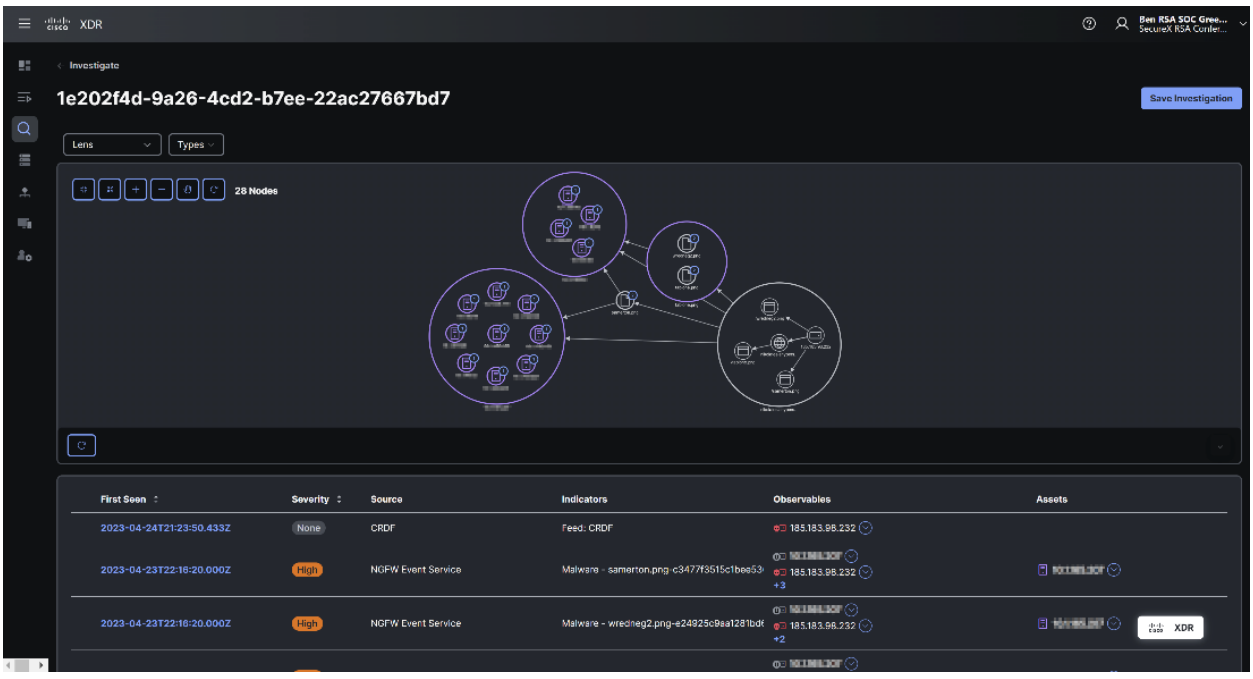
The SOC team received about 60 alerts about malware downloads and/or download attempts, over the course of 48 hours, from 13 endpoints -- always attempting to download one or more of the same three known malicious PNG files, from the same domain and URLs. We have to allow demonstrations/briefings/trainings on malware, but always investigate to ensure the network is not compromised and attendees are safe.

The malicious files were Trickbot, as identified by our integrations with Cisco Talos, Cisco Secure Endpoint's file reputation database, AlienVault and IBM X-Force Exchange.

Taken one at a time, over that period, (and mostly probably ignored individually) the pattern would have likely been missed by human operators. Cisco XDR Analytics detected this pattern of activity using telemetry from the Firewall and escalated it as a set to the SOC team for investigation.

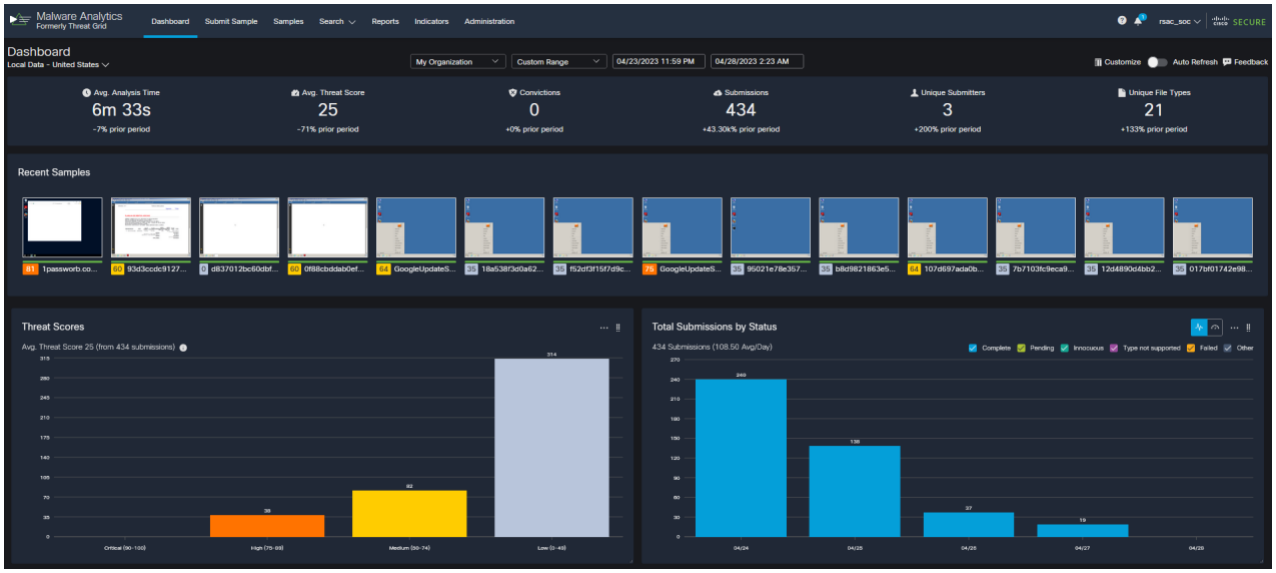


Easily explained in this case by "because vendor booth demos at a security conference", but in your environment, it might mean lateral movement – or a dedicated attacker trying the same attacks against multiple spear phished targets. The fact that it hadn't worked *yet* shouldn't keep you in the dark about a pattern of targeted attempts.

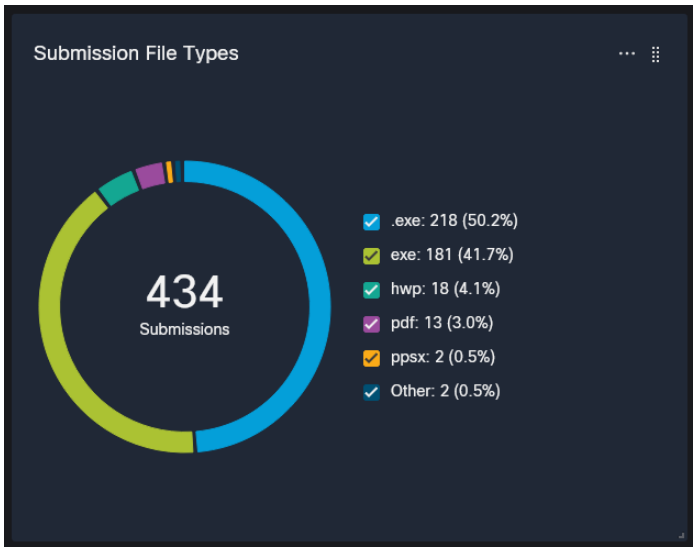


MALWARE ANALYSIS

The RSAC SOC team sent over 400 potentially malicious files to Secure Malware Analytics via the NetWitness platform and Secure Firewall, for automated behavioral analysis.

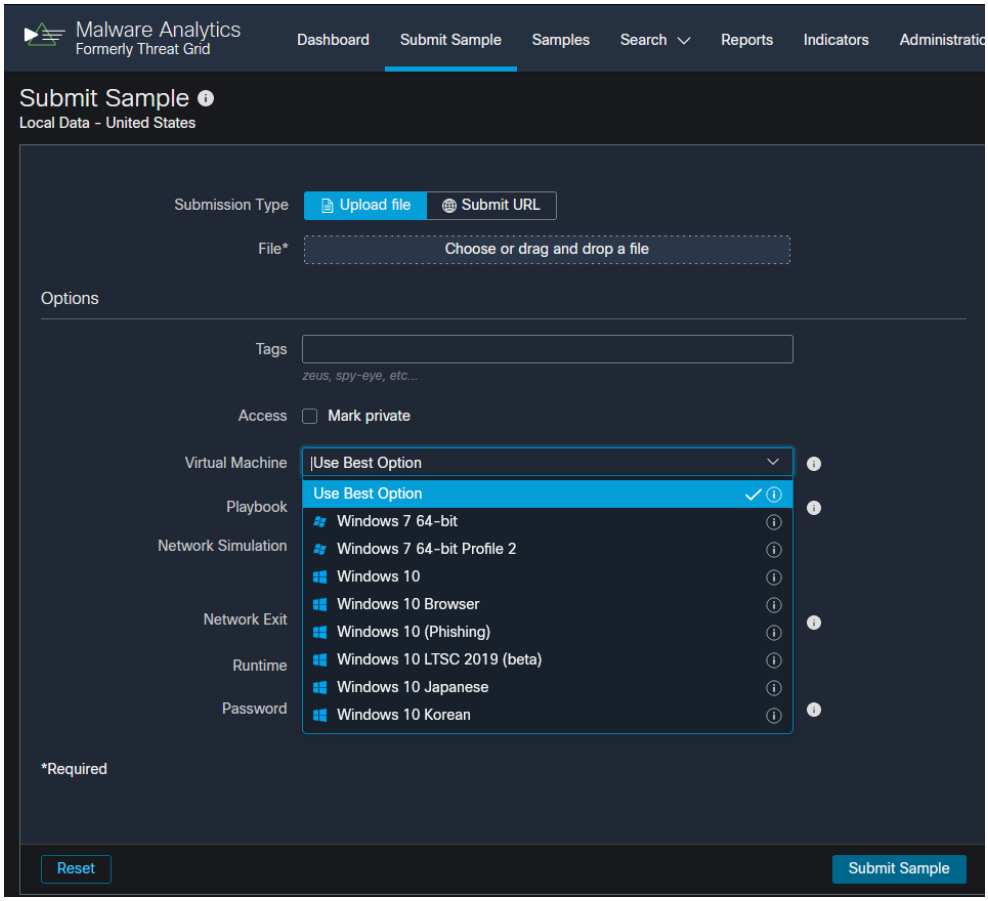


The breakdown of major file types is as follows.

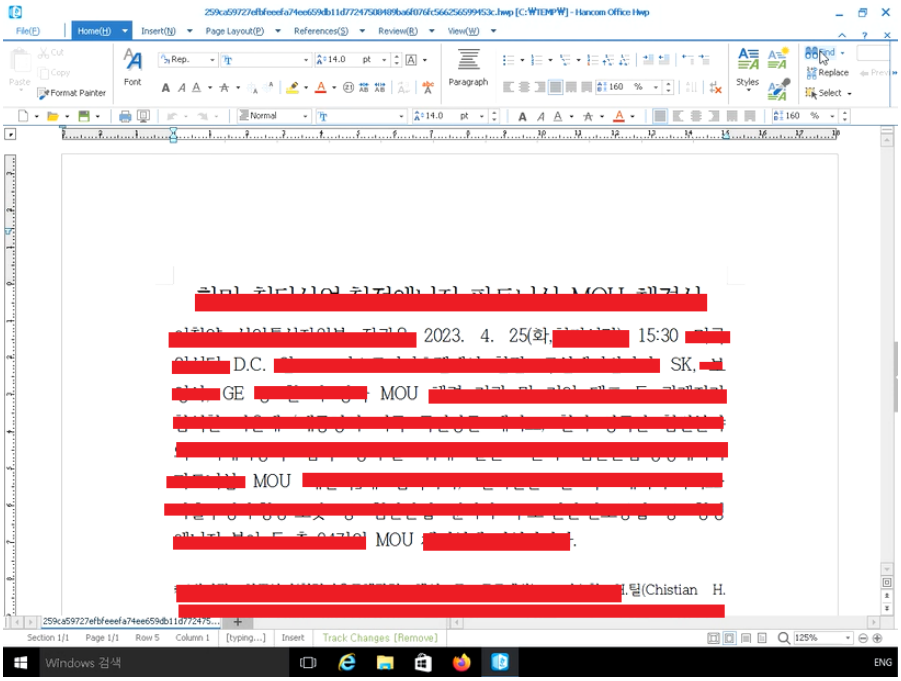


Documents in the Clear

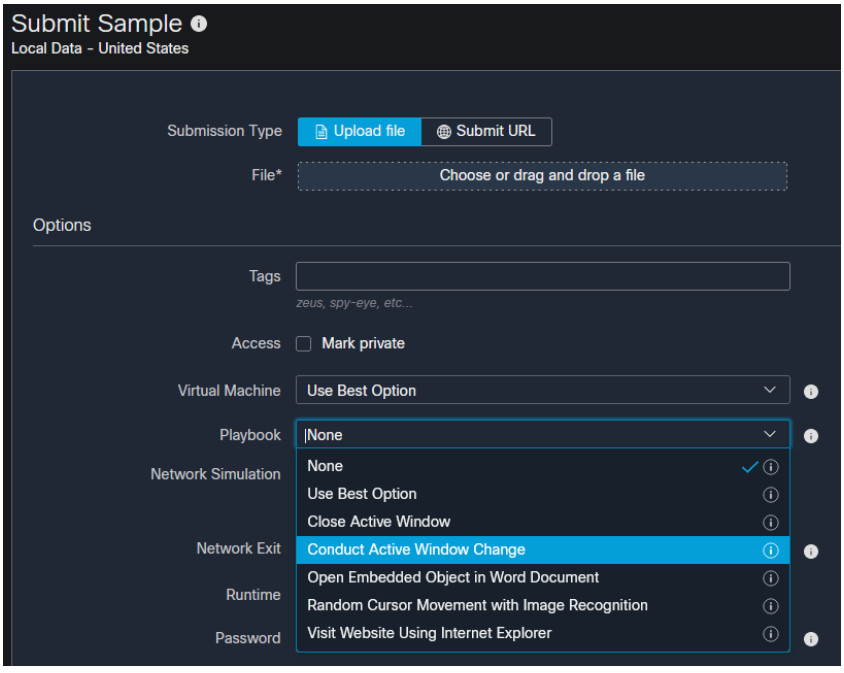
Most of the samples submitted by API were documents or updates to applications. The analysts also had the ability to submit samples manually, which is especially useful to investigate suspicious websites without infecting your machine. You can choose the operating system desired or use the best option.



The best option was useful when investigating Korean language documents, that were auto detected.

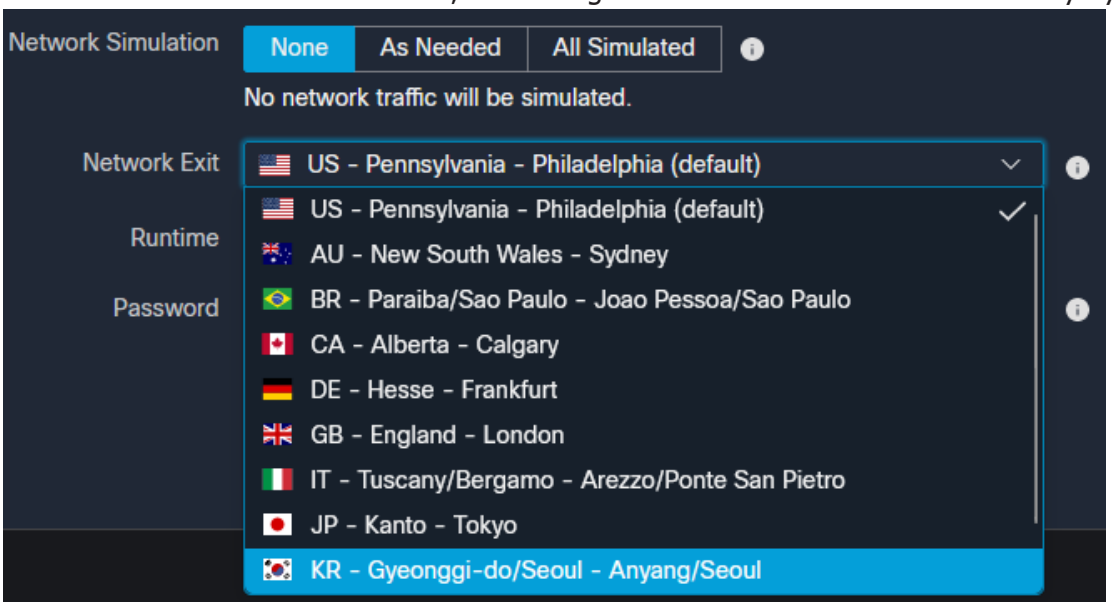


To emulate a user automatically during sample analysis, Secure Malware Analytics provides user emulation through playbooks, which are pre-defined steps that simulate user activity. A system with a user present appears vastly different from an automated analysis system (i.e., a sandbox). For example, 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.

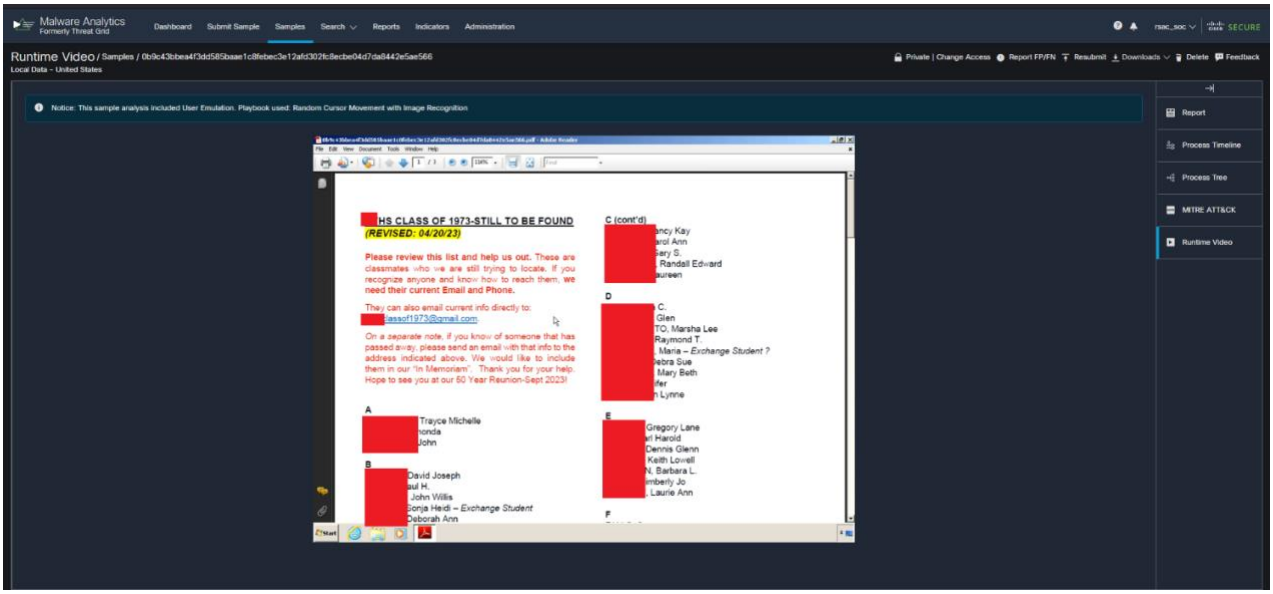


Playbooks automatically simulate user activity during sample analysis, which allows Secure Malware Analytics to behave as if a user were present and operating the keyboard and mouse during analysis.

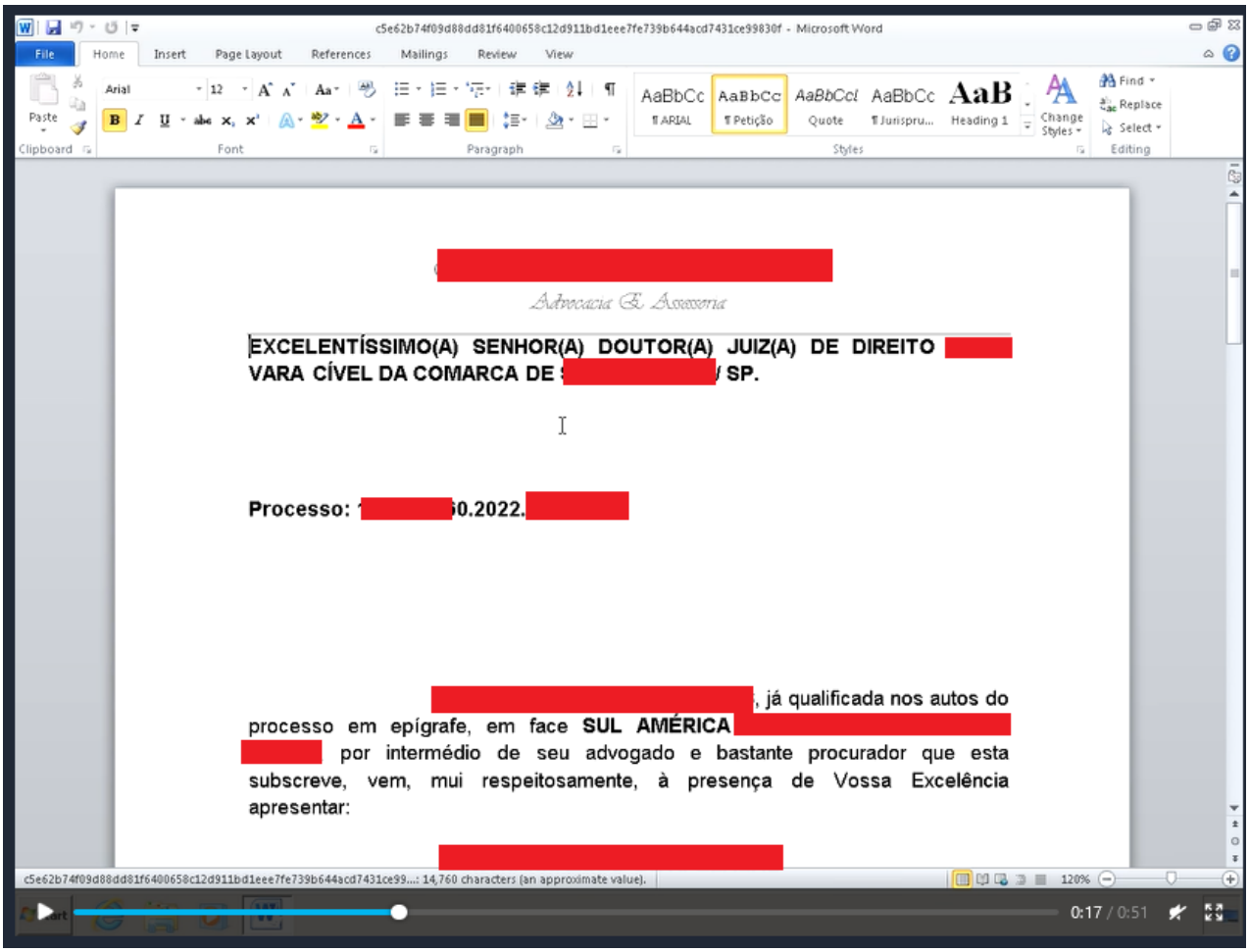
You can also select the Network Exit, to investigate malware that behaves differently by region.



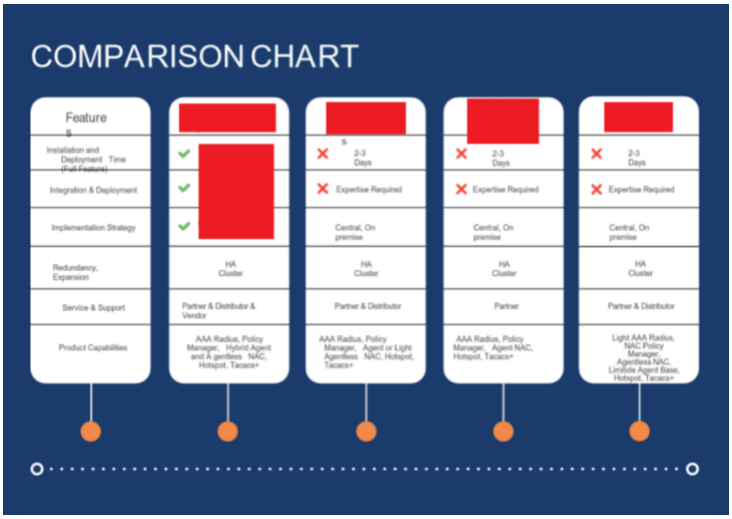
NetWitness found and analyzed many email attachments which were in the clear. Any attendee at the conference who had the right tools and knowledge, would have been able to view the attachments.



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.

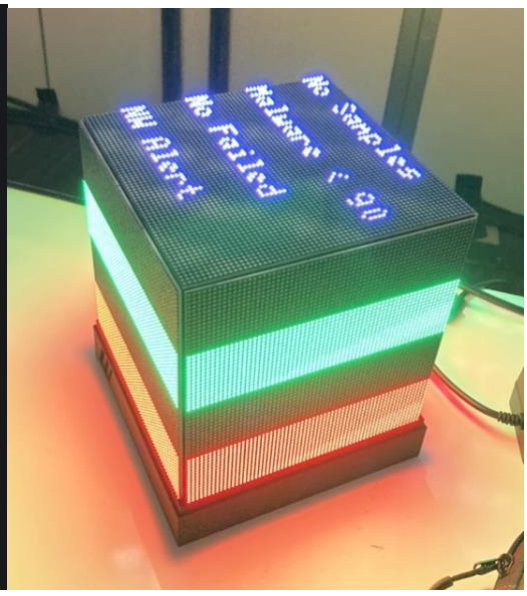


They also included confidential sales presentation, where a username and password were required to access the file server, but then the documents were downloaded in the clear.



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

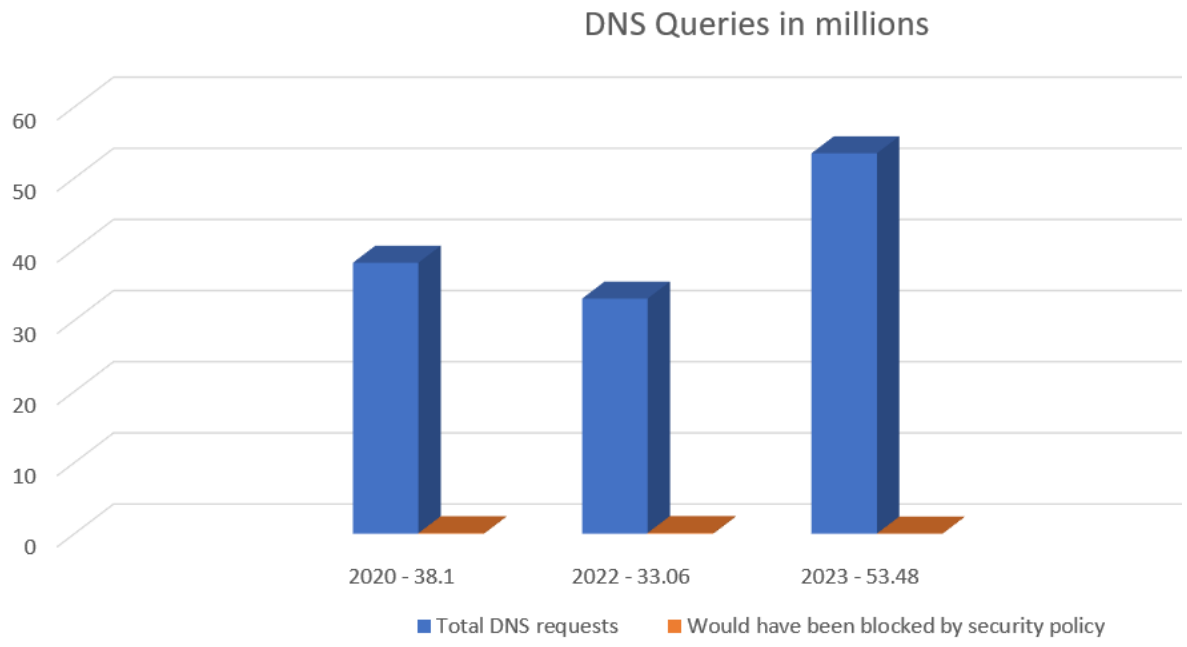
The Cisco team built an improved Tower Light. This year, five RGB Matrix panels, using more than 20,000 LED's, scrolled messages and simulated the Tower Light, using a custom Cisco XDR Automation workflow to interact with Secure Malware Analytics and NetWitness. When an alert occurred, the workflow caused the light to flash or pulse and indicate its status.



The Tower Light also provided updates to the team, on the time, weather, and schedule for SOC tours.

DOMAIN NAME SERVER (DNS)

The SOC had complete DNS visibility, thanks to the support of the Moscone Center agreeing to change their DNS to Cisco Umbrella and installing an Umbrella virtual appliance in the Network Operation Center. The default security settings for Cisco Umbrella are to block malware, command-and-control callback, and phishing attacks. All blocking was turned off for the conference network. We saw over 53 million DNS requests over the week, of which several thousand would have been blocked for security.



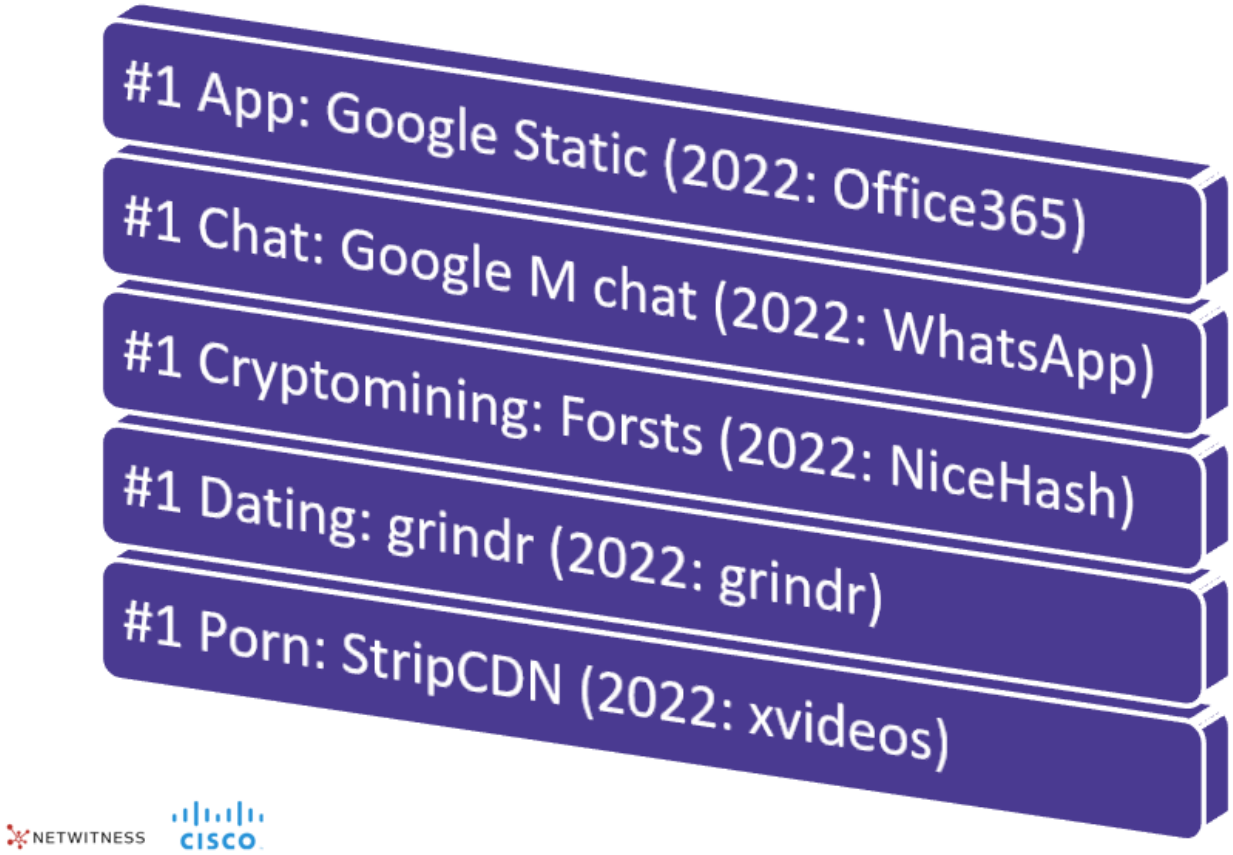
DNS is an area of the RSAC SOC, where preventive and protective measures could be taken, as in a production environment. However, we did not want to block any booth demonstrations, sessions or other training activity that relies on connecting to a malicious domain or IP address.

Requests

Name	Allowed	Blocked	Total	% of Total
Security	44,213	0	44,213	0.08%
– Prevent	18,961	0	18,961	0.04%
– Malware	5,100	0	5,100	0.0095%
– Dynamic DNS	2,836	0	2,836	0.0053%
– Newly Seen Domains	10,944	0	10,944	0.02%
– Potentially Harmful	0	0	0	0.00%
– DNS Tunneling	25	0	25	0.0000%
– Cryptomining	56	0	56	0.0001%
– Contain	2,380	0	2,380	0.0044%
– Command & Control	3	0	3	0.0000%
– Phishing	2,377	0	2,377	0.0044%
– Integrations	22,872	0	22,872	0.04%
– New Custom Integration	22,757	0	22,757	0.04%
– Threat Response	0	0	0	0.00%
– SECUREX	0	0	0	0.00%
– Cisco AMP Threat Grid	115	0	115	0.0002%
Categories	-	8	8	0.0000%
Categories (Legacy)	-	0	0	0.00%
Destination Lists	0	0	0	0.00%
Permitted	53,441,607	-	53,441,607	99.92%
Total	53,485,820	8	53,485,828	100%

Domains also could have been blocked for content, such as pornography, hate/discrimination or other such categories. It is not possible to turn off blocking for certain queries that are criminal in nature.

SOC issued awards to the top domains in the SOC session on 27 April 2023.



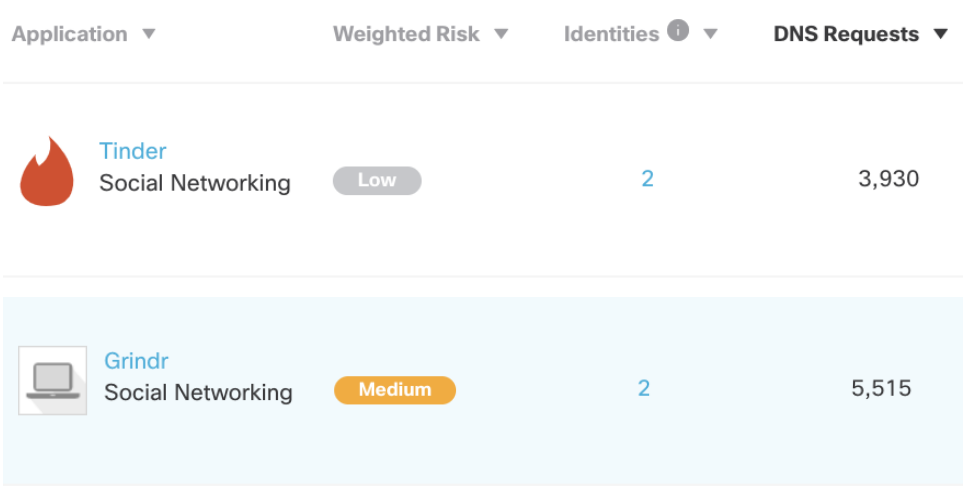
Personal Connections at RSA – Dating by the Numbers

After a couple years of Pandemic induced anxieties, we think it is safe to say RSA is back! With over 40,000 attendees roaming around San Francisco, the conference floor was on fire throughout Moscone. Swag bags were filled to the brim, booth presentation viewers were spilling out into walkways, the W and St. Regis lounge bars were shoulder to shoulder packed, and every 15 minutes we ran into someone we knew from a previous life. The annual RSA Conference/Reunion show has officially returned to its former glory.

And if there is any true indication that the pandemic is behind us, look no further than the RSA dating scene. Once again, Grindr's grinders topped the show with over 5,000 DNS requests made, more than every other dating app combined. Not far behind was Tinder at a little over 3,900, while the more serious dating apps took a back seat here.

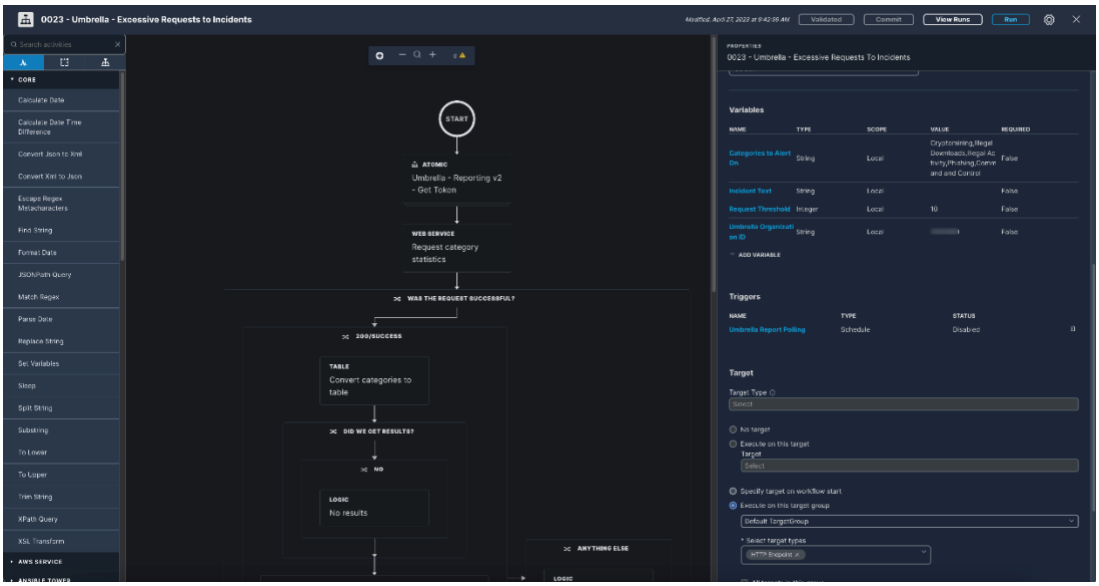
Outside all the late-night vendor parties and bars littered across SOMA, attendees were out in full force, and, in the words of Daft Punk and Pharrell, up all night to get lucky.

Dating App	DNS Requests
Grindr	5515
Tinder	3930
Hinge	427
OKCupid	96
PlentyOfFish	94
Match.com	57
Happn	41
Badoo	36
Adult Friendfinder	10
Zoosk	7
Skout	3
Lovemail.RU	2
Mamba	1

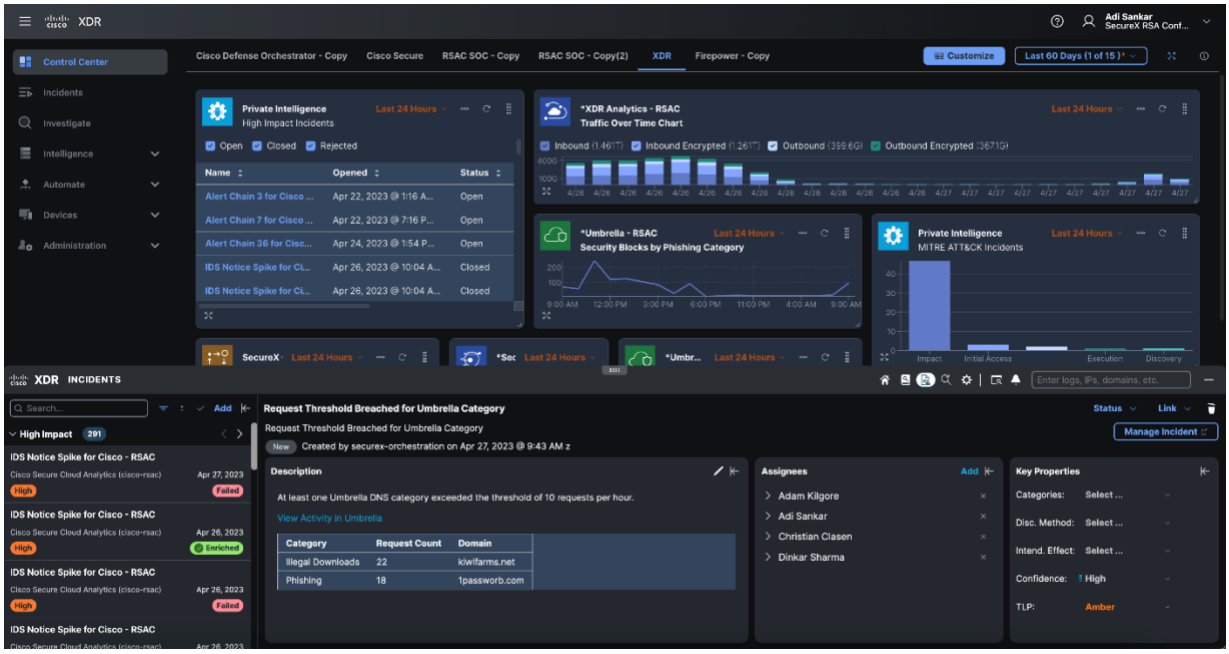


Automate, Automate

Every year, the RSAC SOC team finds more ways to improve efficacy. This year, a Cisco analyst created an automated workflow in Cisco XDR Automate to post to the RSAC SOC Slack Channel and Webex space when an Umbrella security category was activated with a DNS request or a Firewall detection was made. Additionally, an automation workflow to create XDR Incidents from Umbrella security activity was seen for certain categories. We configured the workflow to trigger if more than 10 DNS requests in the same category were made in made in the last hour.



Here is what the incident looks like in Cisco XDR.



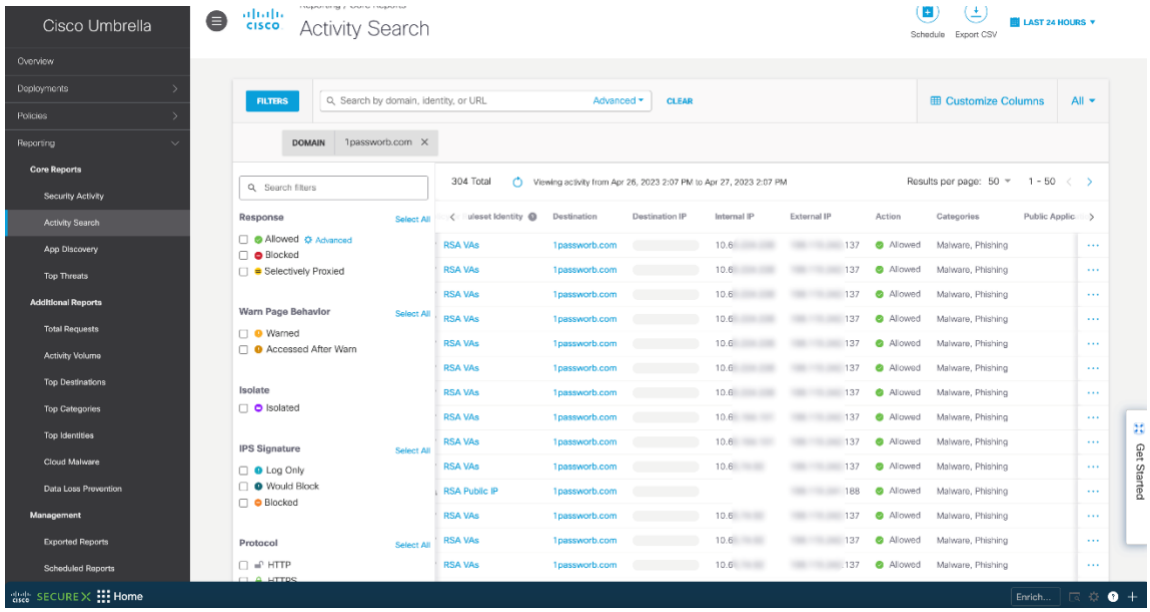
One such trigger was on a phishing domain, crafted to look like 1password.com to users.

Umbrella detected a DNS query matching the category: *Phishing*

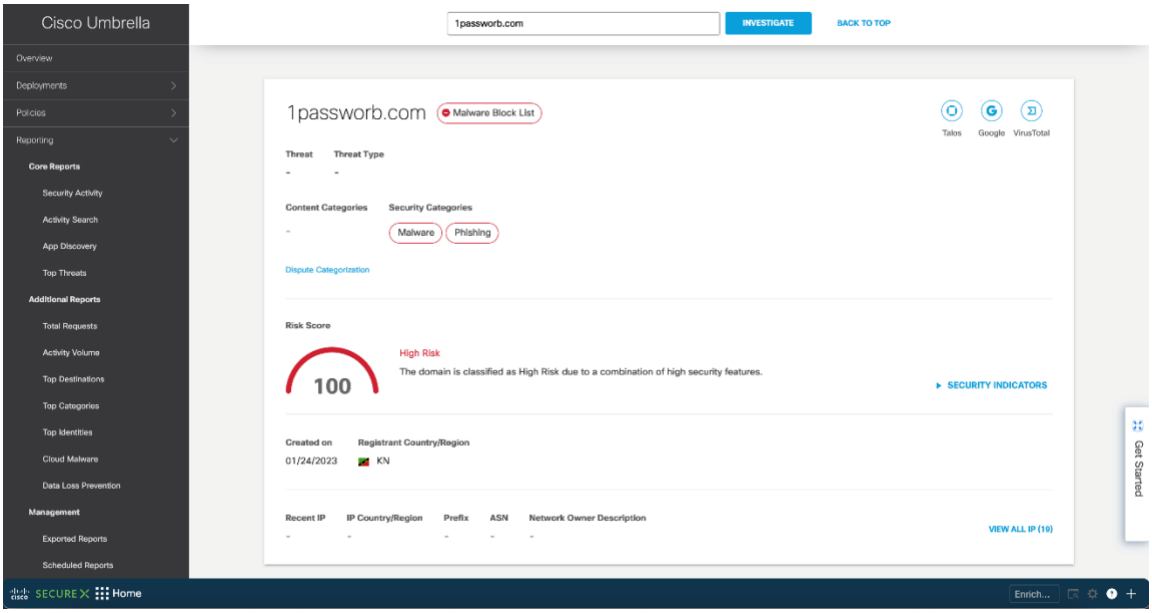
The following data was returned from Umbrella:

```
1   categories:Travel, domain:pavlatos-studios.gr, identities:RSA VAs, interna
2  categories:Travel, domain:1passworb.com, identities:RSA VAs, internalip:10.
3  categories:Travel, domain:www.1passworb.com, identities:RSA VAs, internalip
4  categories:Travel, domain:pavlatos-studios.gr, identities:RSA VAs, internal
5  categories:Travel, domain:pavlatos-studios.gr, identities:RSA VAs, internal
6  categories:Travel, domain:www.1passworb.com, identities:RSA VAs, internalip
7  categories:Travel, domain:1passworb.com, identities:RSA VAs, internalip:10.
8  categories:Travel, domain:www.1passworb.com, identities:RSA VAs, internalip
9  categories:Travel, domain:www.1passworb.com, identities:RSA VAs, internalip
10 categories:Travel, domain:1passworb.com, identities:RSA VAs, internalip:10.
```

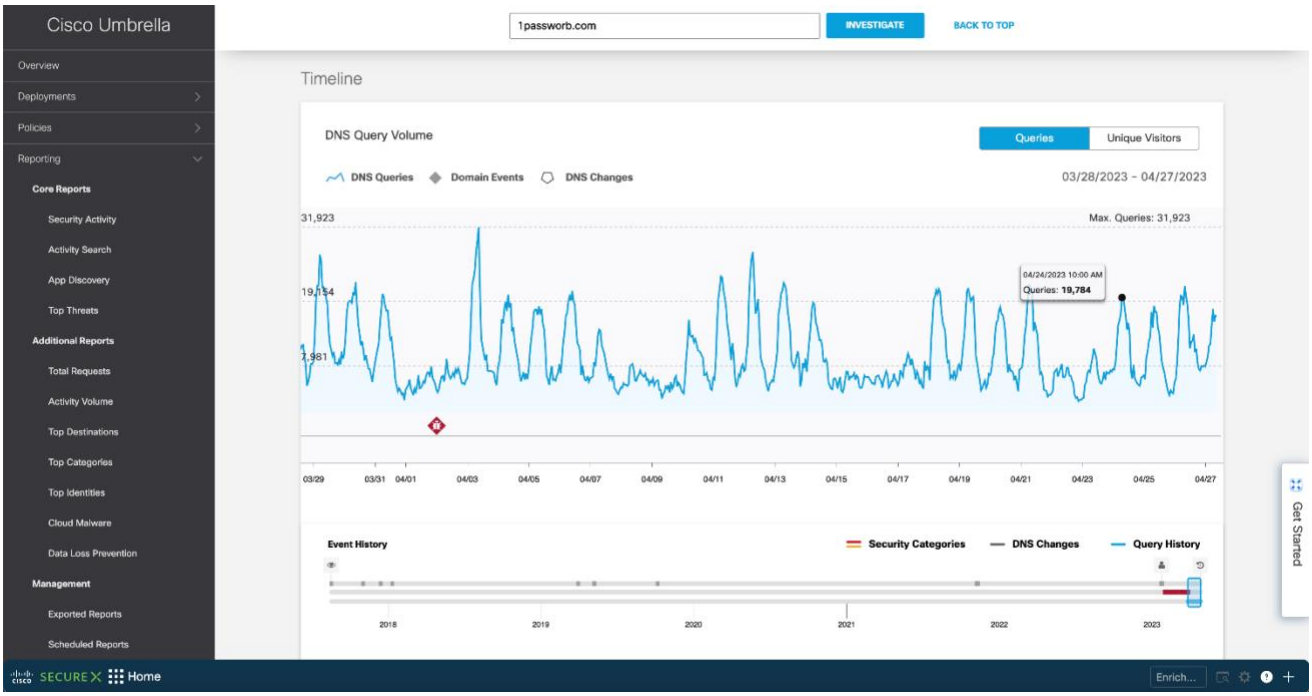
Investigation identified the IP address of the user and the frequency of the DNS requests.



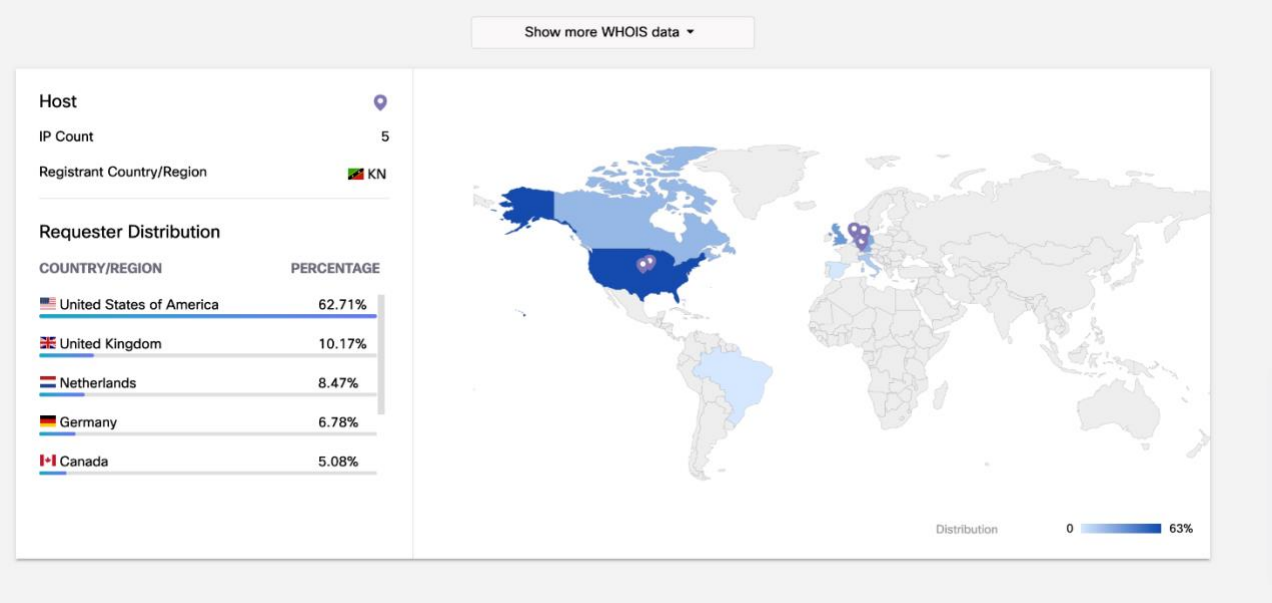
Pivoting to Umbrella Investigate, we were able to learn more about the phishing/malware domain.



This included the global query volume and that it was not a recently created domain.

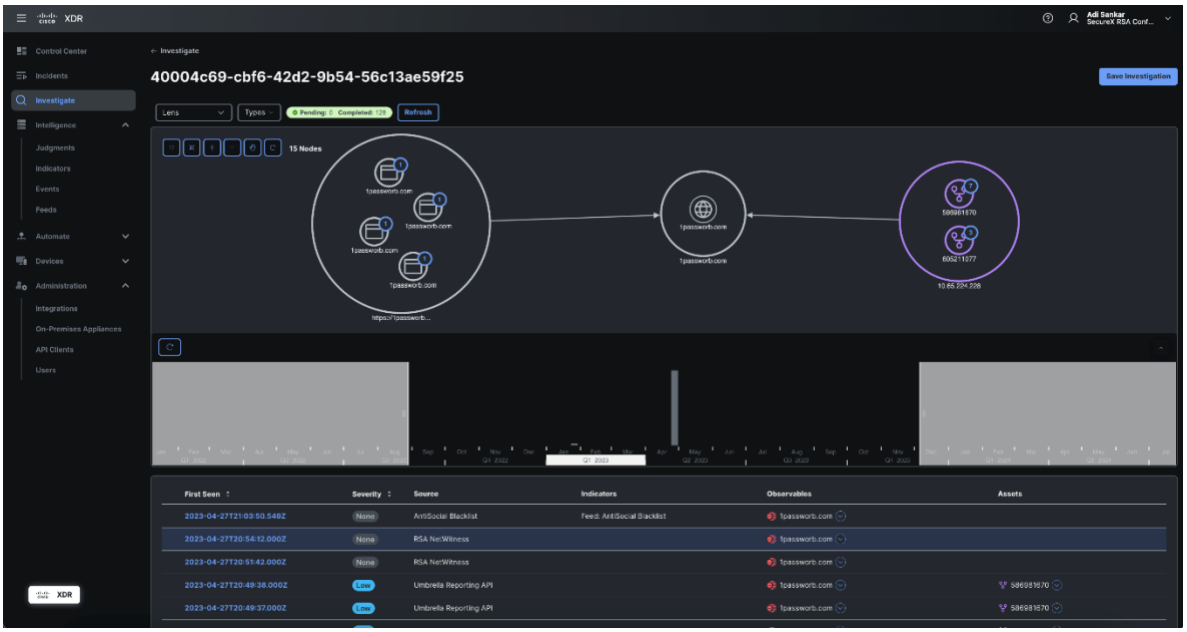


The domain was registered in Saint Kitts and Nevis and primarily targeted the USA and additional countries such as the UK, Germany, Canada, and the Netherlands.



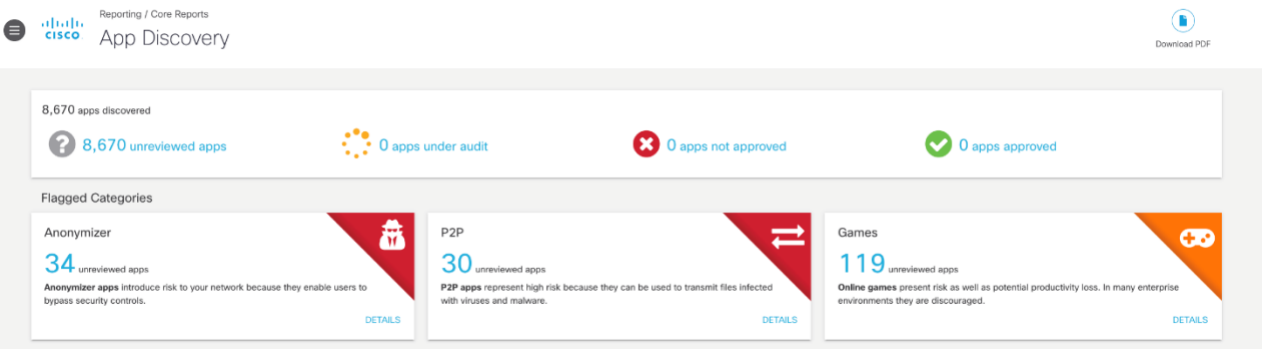
We dug in deeper with an investigation in Cisco XDR investigate, where we could see the threat intelligence about the domain and related artifacts. We could see multiple hosts requesting resolution for 1passworb.com, global threat intelligence from APIvoid and sightings from Netwitness in one view.

The investigation pointed to a demo in the Expo Hall, an acceptable use of the conference network.

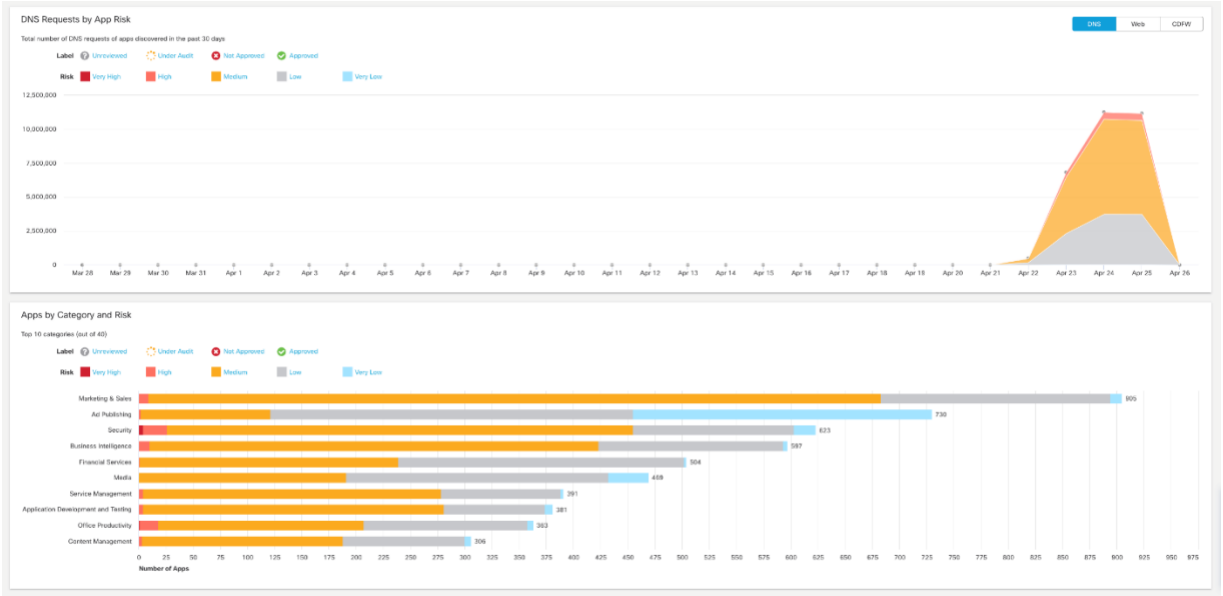


Apps, Apps and more Apps

About 8,760 applications were identified by the DNS queries at RSAC 2023. This is an increase from about 7,200 apps in 2022 and about 4,000 in 2020.



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.



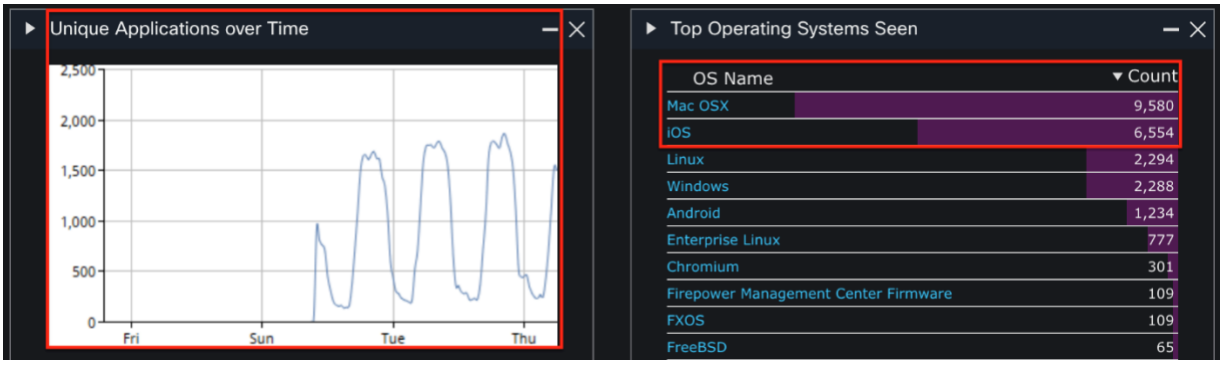
INTRUSION DETECTION

A Secure Firewall 4145 appliance, running Firepower Threat Defense software, was set up as the perimeter IDS device. The Firewall syslogs were sent to Secure Cloud analytics for further correlation.

The IDS inspected all wireless guest traffic from event attendees, configured in monitor-only mode. Firepower offers breach detection, threat discovery, malware sample submission to Secure Malware Analytics 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 Secure Cloud analytics reduces the volume of Firewall alerts to help the analysts focus on which alerts matter the most. In the future sending netflow directly to Secure Cloud analytics could produce behavioral detections based on machine learning.

Discovered Applications

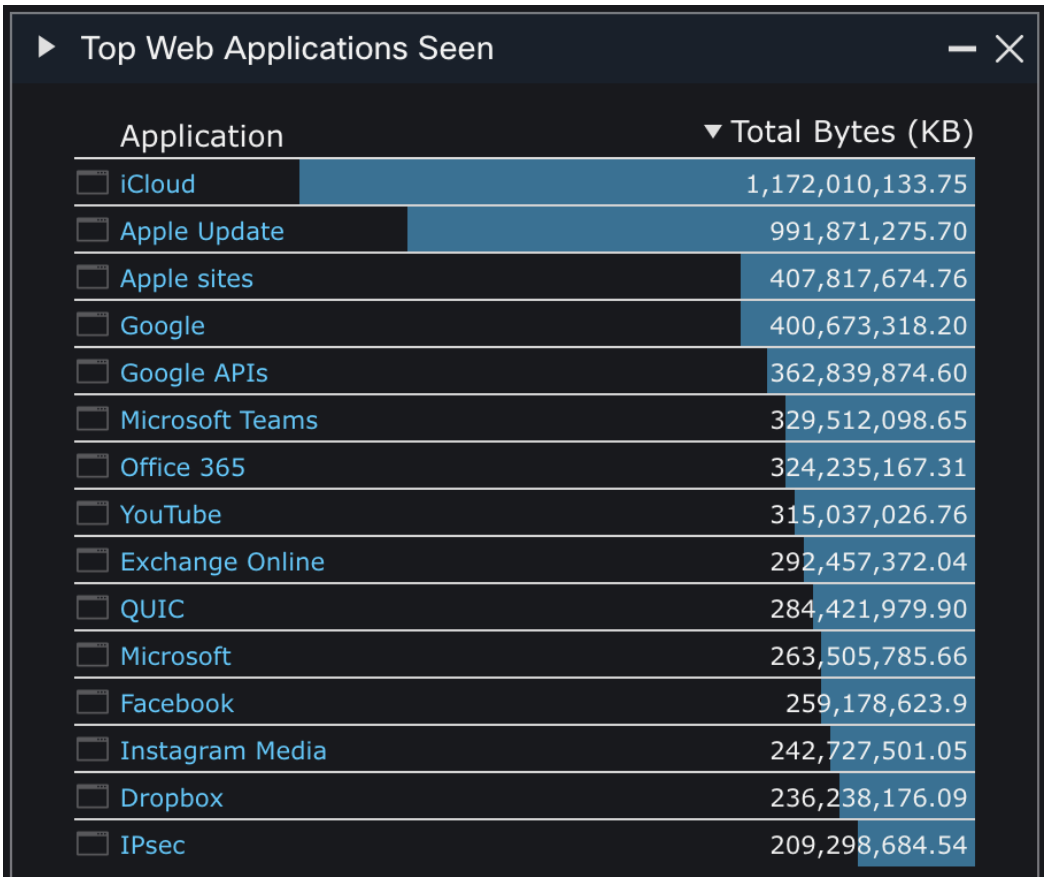
Firepower detected over 1,500 different applications during the conference, with the number of unique applications concurrently seen on the network spiking during conference hours each day. The operating systems generating application traffic were primarily Apple, which took the top two spots with Mac OSX and iOS.



Daily OS counts also help provide a rough number of how many attended the event for that day. However, the wireless session lease was only three hours, which makes it difficult to make more precise daily OS counts. The same user connected to RSAC Wi-Fi could show multiple counts in one day. It is recommended to configure a wireless lease of more than one day to help correlate events for a user the next day.

Web Application traffic was dominated by the major tech companies Apple, Google, and Microsoft. In social media, Facebook and Instagram took the top spots. IPsec also made the list, indicating that many visitors were using a VPN over the RSAC Wi-Fi.

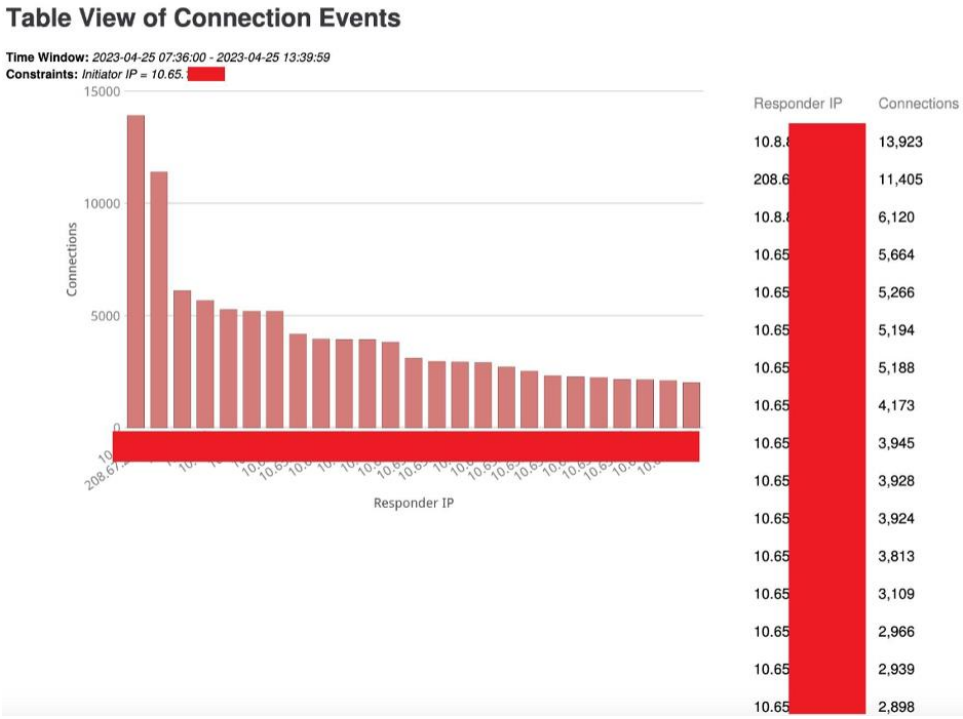
Using personal social media and sensitive websites on public Wi-Fi, without VPN, is not recommended because of common security issues.



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 over a terabyte of data over the course of the conference.

Port Scanning

On Monday, 24 April, an IP address was identified making connections to many IPs on the guest wireless network and connected subnets.



The scanning IP iterated through a list of well-known ports for each target. The most common scan made 204 connections to each target, although some IPs received larger scans.

Source Port / ICMP Type	Destination Port / ICMP Code	Initiator Packets	Responder Packets
8 (Echo Request) / icmp	0 (No Code) / icmp	1	0
8 (Echo Request) / icmp	0 (No Code) / icmp	1	0
17 (Address Mask Request) / icmp	0 (No Code) / icmp	1	0
17 (Address Mask Request) / icmp	0 (No Code) / icmp	1	0
56182 / tcp	7 (echo) / tcp	1	0
59436 / tcp	7 (echo) / tcp	1	0
48250 / tcp	9 (discard) / tcp	1	0
49788 / tcp	9 (discard) / tcp	1	0
48280 / tcp	13 (daytime) / tcp	1	0
51004 / tcp	13 (daytime) / tcp	1	0
35412 / tcp	21 (ftp) / tcp	1	0
38566 / tcp	21 (ftp) / tcp	1	0
55112 / tcp	22 (ssh) / tcp	1	0
59056 / tcp	22 (ssh) / tcp	1	0
35252 / tcp	23 (telnet) / tcp	1	0
38398 / tcp	23 (telnet) / tcp	1	0
56986 / tcp	25 (smtp) / tcp	1	0
60812 / tcp	25 (smtp) / tcp	1	0
35554 / tcp	26 / tcp	1	0
38832 / tcp	26 / tcp	1	0
32910 / tcp	37 (time) / tcp	1	0

However, no connection had more than 4 response packets, and it does not appear that logins were attempted or successful. Below is a screenshot of an SSH connection that progressed beyond the initial SYN packet, with the scanning device forcing a reset of the connection after receiving a TCP Window Update from the server.

No.	Time	Protocol	Length	Info
1	0.000000	TCP	74	35382 → 22 [SYN] Seq=0 Win=65535 Len=
2	0.004863	TCP	78	22 → 35382 [SYN, ACK] Seq=0 Ack=1 Wi
3	0.012896	TCP	66	35382 → 22 [ACK] Seq=1 Ack=1 Win=876
4	0.015048	TCP	66	[TCP Window Update] 22 → 35382 [ACK]
5	0.022662	TCP	60	35382 → 22 [RST] Seq=1 Win=0 Len=0
6	0.026563	TCP	66	35382 → 22 [RST, ACK] Seq=1 Ack=1 Wi

The scanning device also connected to the internet, where an HTTP GET request was recorded by NetWitness.

```
> Transmission Control Protocol, Src Port: 36016, Dst Port: 80, Seq: 1, Ack: 1, Le
v Hypertext Transfer Protocol
  > GET /favicon.ico HTTP/1.1\r\n
    Host: www.google.com\r\n
    Connection: keep-alive\r\n
    User-Agent: Mozilla/5.0 (Linux; Android 8.1.0; CyberScope Build/2.3.0.83; wv)
    Accept: image/webp,image/apng,image/*,*/*;q=0.8\r\n
    Referer: http://www.google.com/gen_204\r\n
```

The User Agent and MAC address of the device were both associated with a handheld scanning tool.

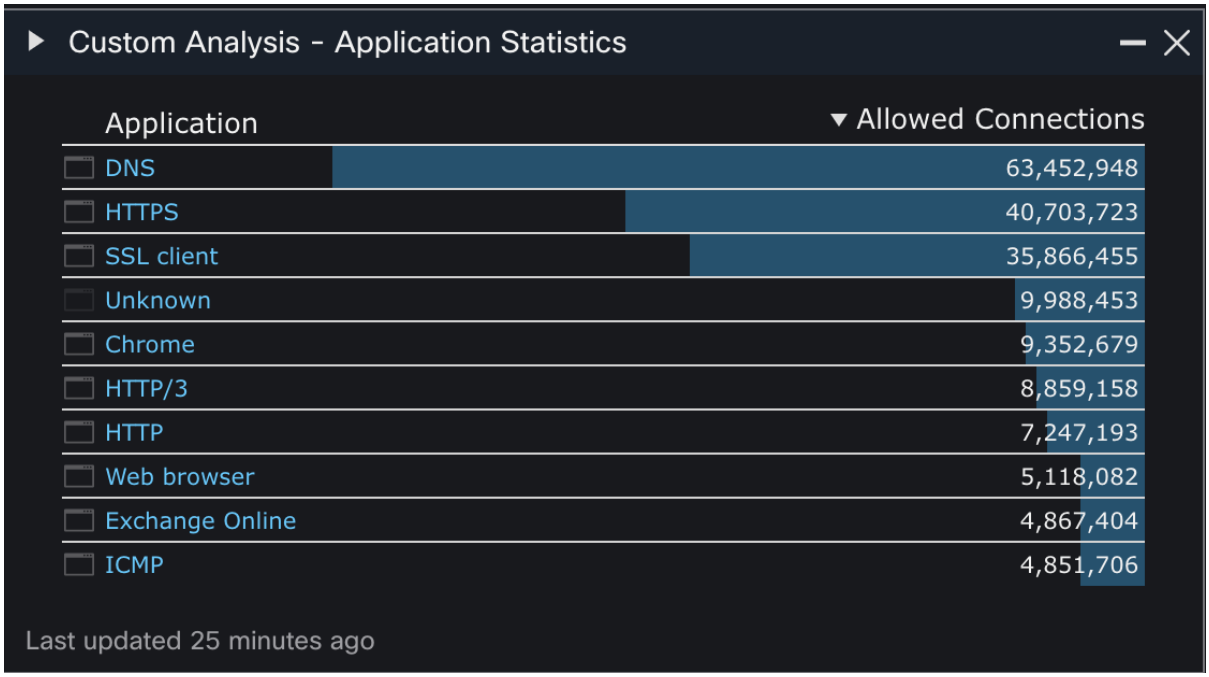
On Tuesday a second device with the same User Agent was found, scanning the network in similar patterns to Monday. This scan was reported to RSA and a block of the scanning devices was recommended. We also located the owners of the pictured devices and advised them to ensure their devices didn't initiate additional scanning of the network. No further large-scale scans were observed.

File Transfers

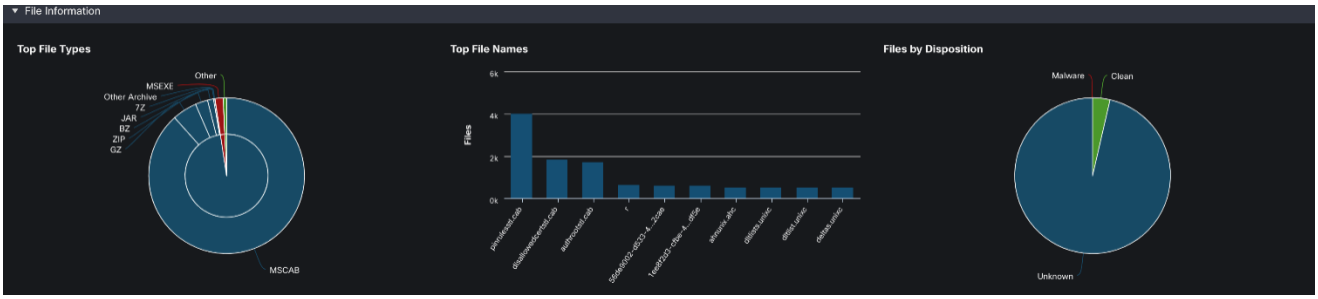
File monitoring and analysis yields valuable network monitoring information, as well as providing insight into the types of users in the network. The large number of locally spread malware files indicate that someone was downloading these files locally from inside the network.

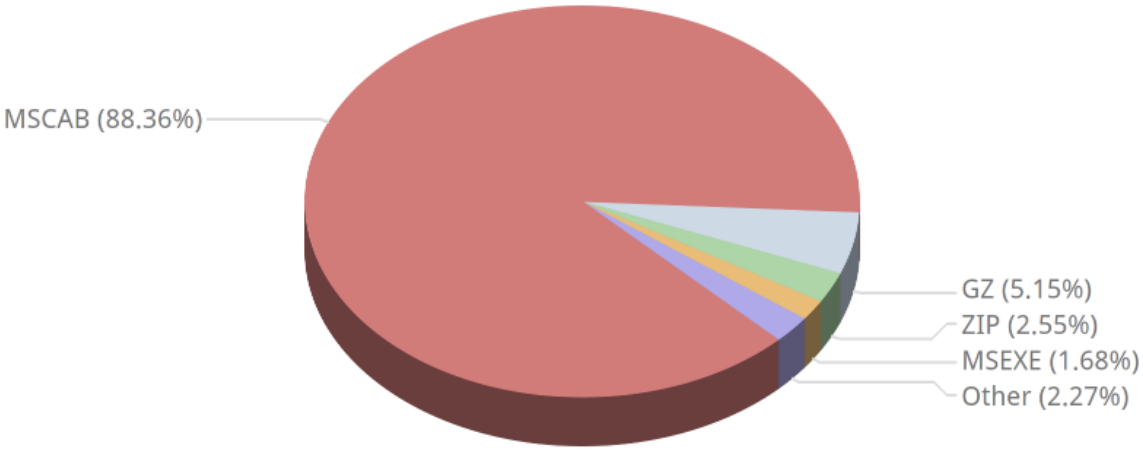
If it was not already known to the SOC who perpetrated the dump, these malware files could also provide other information such as:

- User education covering email security (what to click and what to not click.)
- Target analysis: Is the company network being targeted specifically with these files?
- Files with the help of our Cisco Secure Cloud Lookup and Talos Intelligence integration.



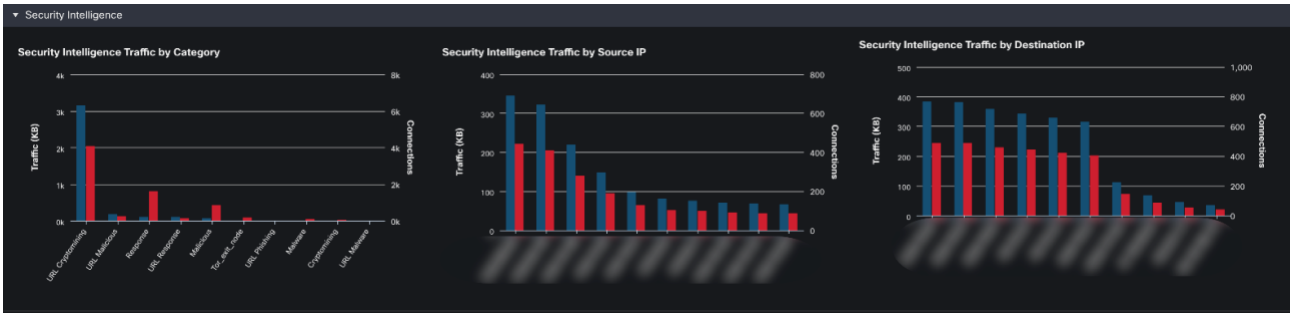
Returning to our RSAC findings, most malware files these days spread with HTTPS, and the RSAC SOC didn't enable any SSL decryption; this may explain why the malware/malicious files count was so low. Still, with 13 percent of traffic being over HTTP, we were able to catch a good number of these.

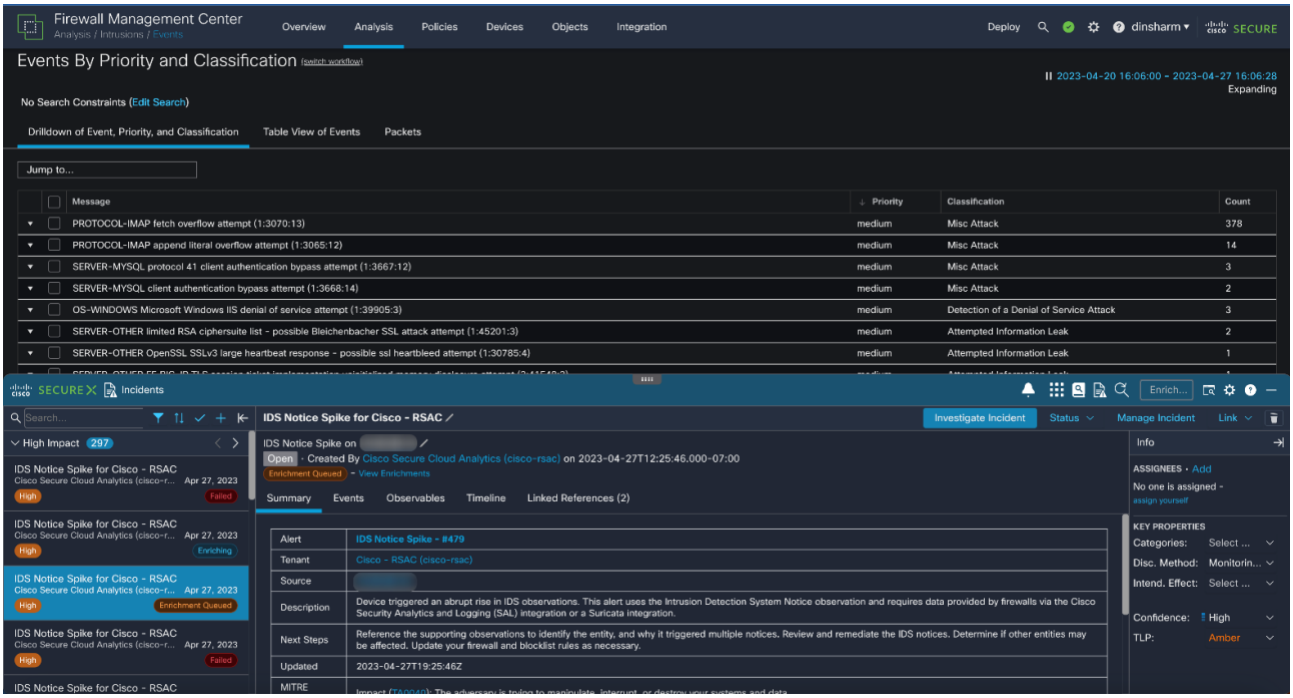




Intrusion Information

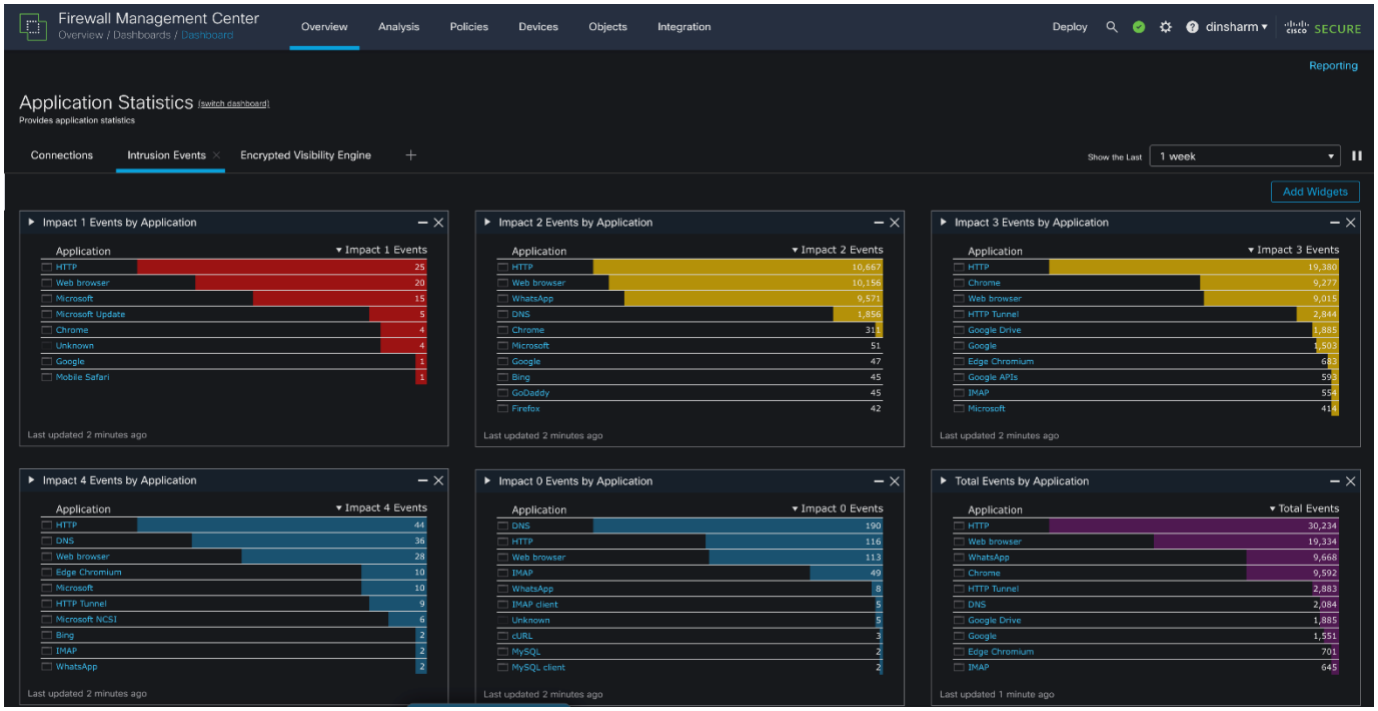
During the conference, several intrusion events were recorded by Firepower. Automated event analysis correlated threat events with contextual host profile data, to identify IPS events requiring immediate investigation. Whenever a working exploit targeted a vulnerable host on the guest network, an Impact 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 the RSAC SOC team, this helped cut through the noise and focus attention to save precious time.





Many "user privilege gain" attacks were detected, which indicated an attacker was trying to gain access to demo and other networking devices. This also calls attention to why you should never use default passwords.

Multiple intrusion events were categorized as high priority.



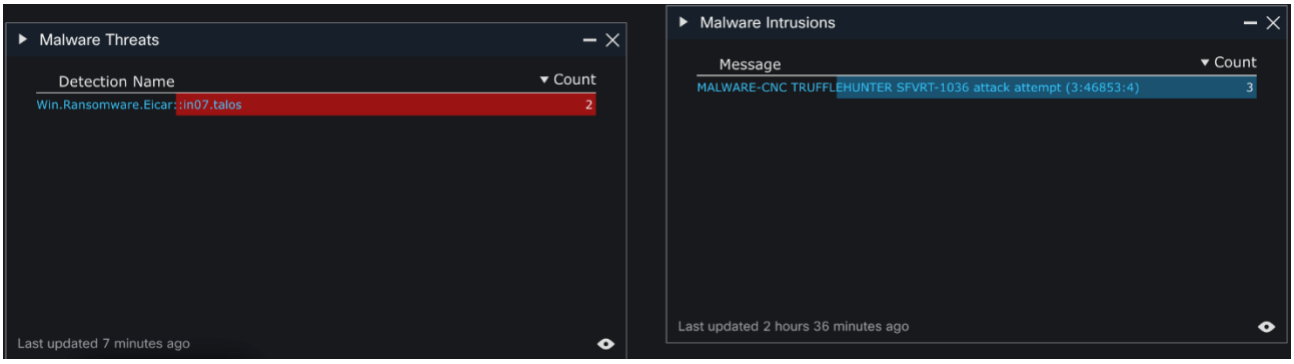
Malware Threats

Cisco Firepower Management Center (FMC) malware event dashboard showed us some serious malware intrusions, as well as threats live from the RSAC network.

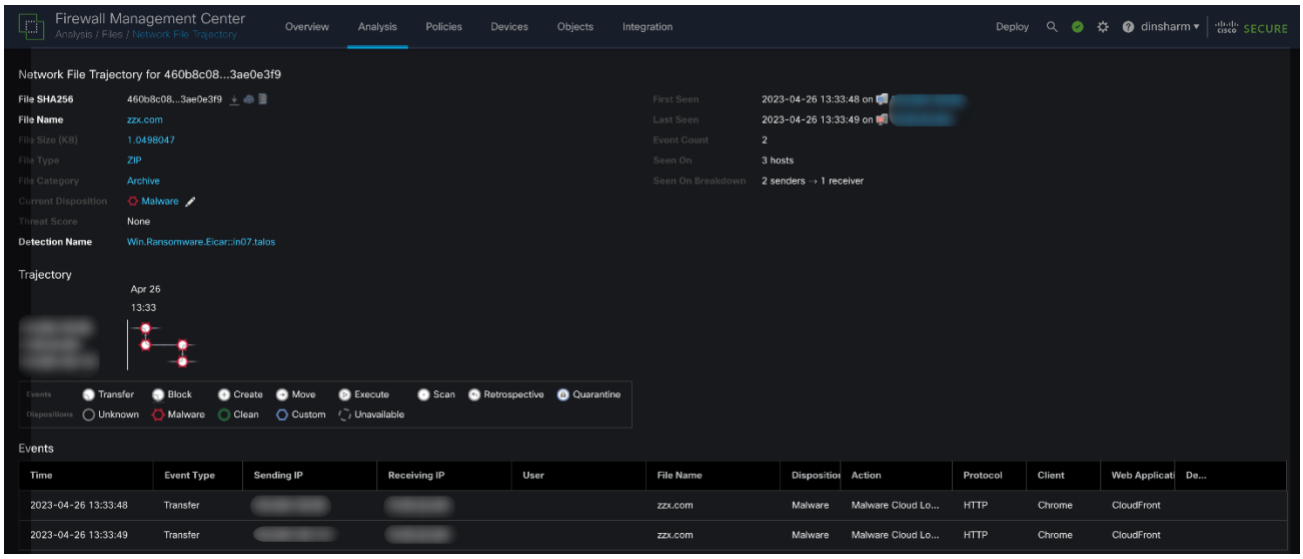
Secure Malware Analytics (formerly Threat Grid) was used in combination with the Cisco FMC to learn more details about the malware threats, reflected in the "Malware Threats" dashboard as analyzed files. Combining different security products and making them talk to each other creates a more secure and safe environment, along with the help of correlation from different products and their analysis. At times, a single tool may report a completely new "first-time-seen" file as a risk-free file. However, leveraging a combination of security tools can make it possible to dig deeper to see what is really going on.

A huge number of DNS request-based intrusions were seen on the network. Cisco Umbrella can be used along with other security devices to stop these types of attacks, as most of the DNS traffic is cleaned by Cisco Umbrella before it even enters our network/security devices or next-generation firewall devices.

Command-and-control events remain the top type of intrusion events at RSAC in 2022. Command-and- control communications are also used extensively for doing quiet cryptomining in the background of infected devices.



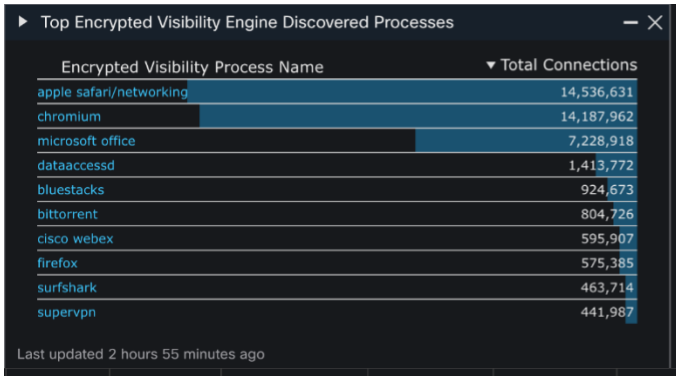
Using Firepower Management File Trajectory we can see which hosts are specifically targeted by mapping how the file traversed the network, identifying passing hosts on a time series graph that details potentially infected IPs and the frequency which those hosts were visited. Additionally, we can see telemetry on malware signature itself, including threat score, first and last occurrences, hash signature and current disposition.

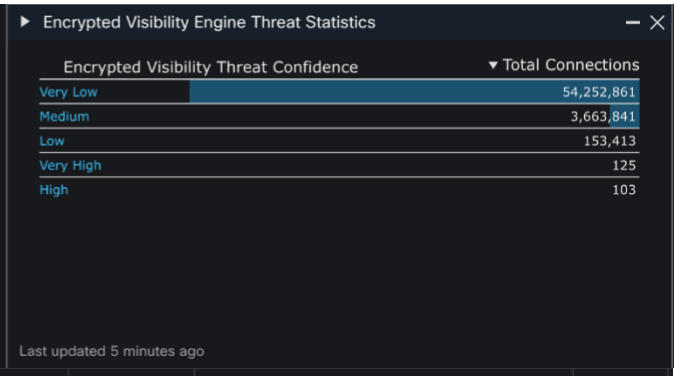


Firepower Encrypted Visibility Engine (EVE)

Firepower system also gained visibility into an encrypted session without needing to decrypt it using the Encrypted Visibility Engine (EVE) feature. The engine fingerprints and analyzes encrypted traffic and provides more visibility into encrypted traffic, including protocols such as TLS and QUIC and provides a list of all the applications, micro-apps and processes used within those applications. Firepower also tries to find any potential encrypted vulnerable traffic within that encrypted application traffic and assigns a Threat Confidence Score (0 –100) and categorizes them (Very Low – High).

At RSAC 2023, Cisco Secure Firewall's detected potential C2C and DGA (Domain Generation Algorithm) technique. We saw some hosts using DGA technique to generate new domain names and IP addresses for malware's command and control servers. Executed in a manner that is random.





Ingress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web Application	Application Risk	URL	IOC
RSA-Tap	60088 / tcp	9000 / tcp	SSL	SSL client	Unknown	Medium	https://www.pvcvcblzjn.com	Triggered
RSA-Tap	52361 / tcp	143 (imap) / tcp	SSL	SSL client	Unknown	Medium	https://www.4ljroh6my2riuwf4h74inm5cd.com	
RSA-Tap	52359 / tcp	9002 / tcp	SSL	SSL client	Unknown	Medium	https://www.ohyttpnxd7owfja4mlrr5j7.com	
RSA-Tap	52360 / tcp	443 (https) / tcp	HTTPS	SSL client	Web Browsing	Medium	https://www.crnqlts6t.com	
RSA-Tap	52358 / tcp	443 (https) / tcp	HTTPS	SSL client	Web Browsing	Medium	https://www.wsm2fnmrs7rdkij4qnla.com	Triggered
RSA-Tap	56551 / tcp	9001 / tcp	SSL	SSL client	Unknown	Medium	https://www.22fn5.com	
RSA-Tap	56550 / tcp	8443 / tcp	SSL	SSL client	Unknown	Medium	https://www.2dsw5fbx7cn7px.com	Triggered
RSA-Tap	56539 / tcp	443 (https) / tcp	HTTPS	SSL client	Web Browsing	Medium	https://www.u5ff.com	
RSA-Tap	56528 / tcp	443 (https) / tcp	HTTPS	SSL client	Web Browsing	Medium	https://www.dh6eabobiw5jhbiyf.com	
RSA-Tap	56515 / tcp	9001 / tcp	SSL	SSL client	Unknown	Medium	https://www.restez7xnk.com	
RSA-Tap	56466 / tcp	443 (https) / tcp	HTTPS	SSL client	Web Browsing	Medium	https://www.msgxb6trc5vgqb57czchsmb.com	
RSA-Tap	56453 / tcp	443 (https) / tcp	HTTPS	SSL client	Web Browsing	Medium	https://www.upmbhwfk3hmqy3ypzhf4vy.com	
RSA-Tap	56457 / tcp	9003 / tcp	SSL	SSL client	Unknown	Medium	https://www.7phwrryeou3r.com	
RSA-Tap	56444 / tcp	9001 / tcp	SSL	SSL client	Unknown	Medium	https://www.a3rpncisbh4mpm7j5.com	
RSA-Tap	56456 / tcp	9001 / tcp	SSL	SSL client	Unknown	Medium	https://www.panb2wjjkt7x.com	Triggered
RSA-Tap	55524 / tcp	443 (https) / tcp	HTTPS	SSL client	Web Browsing	Medium	https://www.l63a6b4jt2jbzajypir.com	Triggered

Firepower and NetWitness Integration

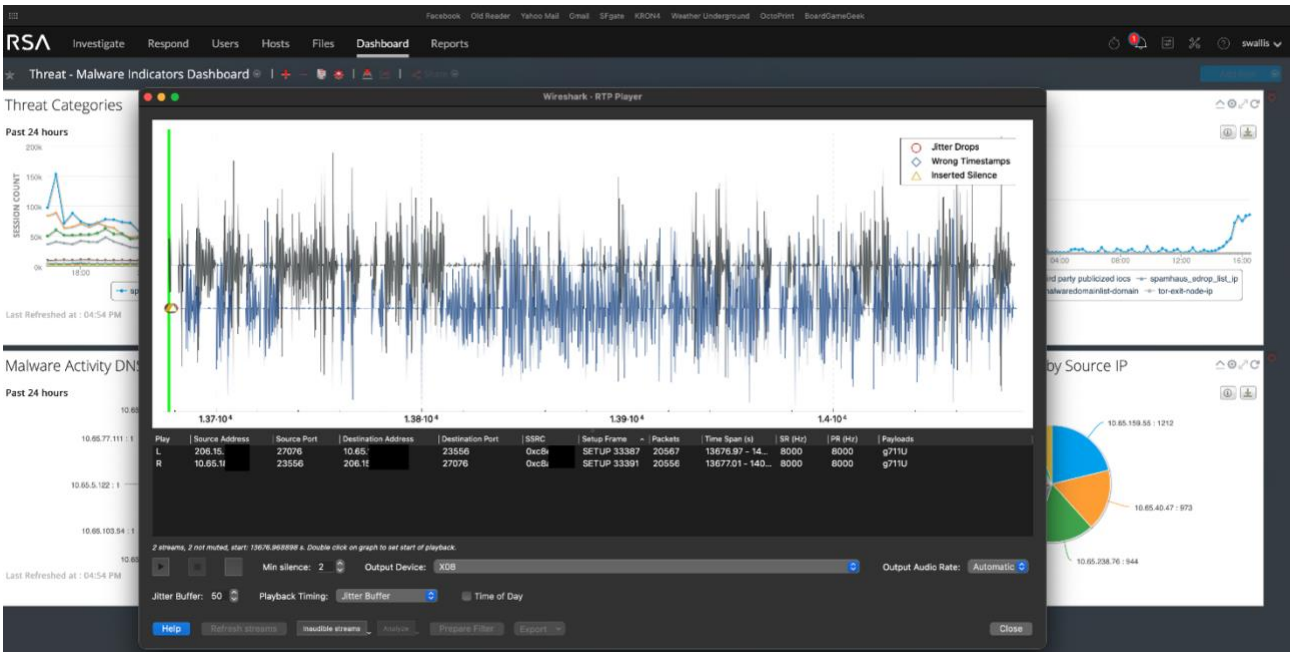
The Cisco Event Streamer (also known as eStreamer) enables users to stream Firepower System events to external client applications. You can stream host, discovery, correlation, compliance allow list, intrusion, user activity, file, malware, and connection data from a Management Center. This year at RSAC we took the opportunity to integrate eStreamer data with NetWitness to provide a cross check validation of events in real time.

The Cisco team was able to complete a direct integration of event data into NetWitness using the Firepower eStreamer protocol. Over 50 million+ events were sent to NetWitness Logs from Firepower, at an average event rate between 500-1100 events per second. This integration enables NetWitness SIEM analysts to directly query Firewall data and create mash up visualizations from both data sources. These can be used to identify gaps in policy and coverage between the product lines. The analytic below was created in NetWitness using Firepower data, and depicts a detailed analysis of events by volume, threat category and geolocation, and triggered Snort rule.

More SIP

In 2022, the SOC team members saw clear text Session Initiation Protocol (SIP) Control Channel (setting up audio call) under user activity in the Cisco Secure Firewall Management Center.

We could see their phone number and the connection with a SIP provider. The team correlated the time and IPs, very quickly finding the RTP/RTSP stream (Audio) using NetWitness, decoded and was able to replay the conversations.



From this experience, we again investigated SIP traffic. We found attendees connecting on a dating/marriage site via unencrypted SIP messages:

- Msg from RXXX DXXXX: "Hi, I liked the Profile that you have posted on SXXXX.com! Please visit my Profile and respond. https://t.sXXXXX.com/L/VKXXX"
- SIP server: 216.XX.XXX.XX

Other Firepower Statistics

Firewall User Activity

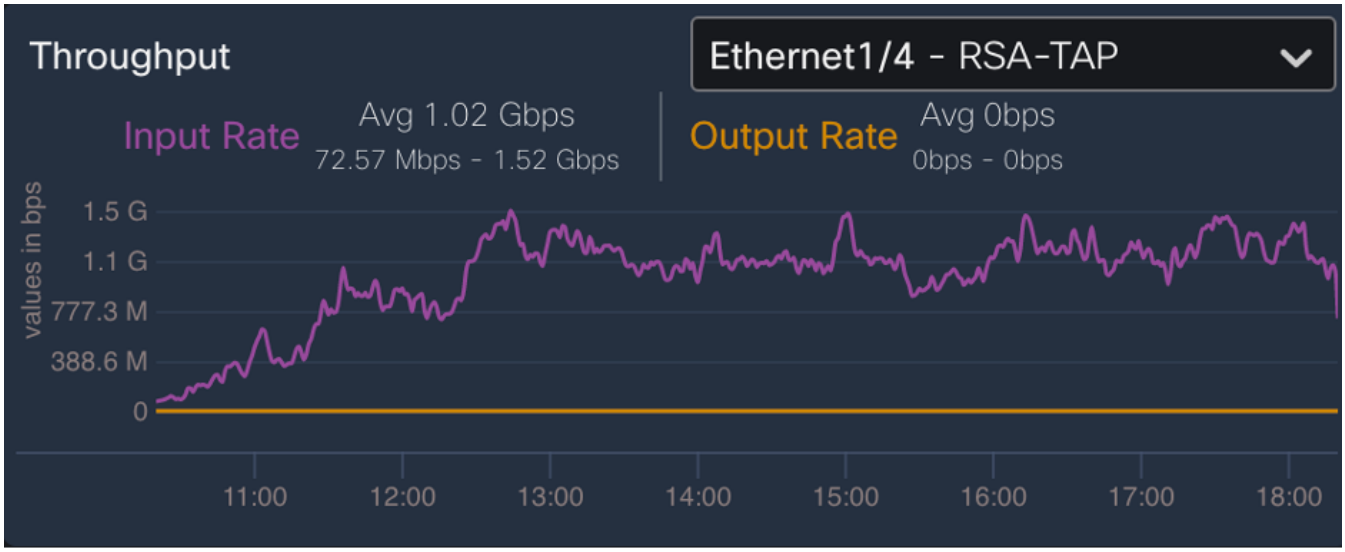
Firewall's deep packet inspection makes it capable of learning about every user's activity and capture details like Usernames/password from applications like FTP, SIP (VoIP), non-encrypted email (IMAP, POP3), API's not using encryption for many apps like an automatic dog feeder.

Time	Event	Username	Realm	Discovery Application	Authentication Type	IP Address	Start Port
2023-04-26 18:37:09	New User Identity	fstgmjtp6wfp	Discovered Identities	FTP	No Authentication		
2023-04-26 18:37:09	User Login	fstgmjtp6wfp	Discovered Identities	FTP	No Authentication	72.167.252.76	
2023-04-26 17:16:14	User Login	feeds@fsnradionews.com FSNNews@fsnradionews.com	Discovered Identities	FTP	No Authentication	192.249.116.25	
2023-04-26 17:16:12	New User Identity	feeds@fsnradionews.com FSNNews@fsnradionews.com	Discovered Identities	FTP	No Authentication		
2023-04-26 17:16:12	User Login	feeds@fsnradionews.com FSNNews@fsnradionews.com	Discovered Identities	FTP	No Authentication	192.249.116.25	
2023-04-26 17:16:12	New User Identity	FSNNews@fsnradionews.com	Discovered Identities	FTP	No Authentication		
2023-04-26 16:36:21	User Login	E832303400802@talk4free.com	Discovered Identities	SIP	No Authentication	216.234.74.8	
2023-04-26 11:50:20	New User Identity	7127248004@216.234.74.8	Discovered Identities	SIP	No Authentication		
2023-04-26 11:50:20	User Login	7127248004@216.234.74.8	Discovered Identities	SIP	No Authentication	216.234.74.8	
2023-04-25 19:08:47	New User Identity	+14162981210@208.77.2.81	Discovered Identities	SIP	No Authentication		
2023-04-25 19:08:47	User Login	+14162981210@208.77.2.81	Discovered Identities	SIP	No Authentication	208.77.1.134	

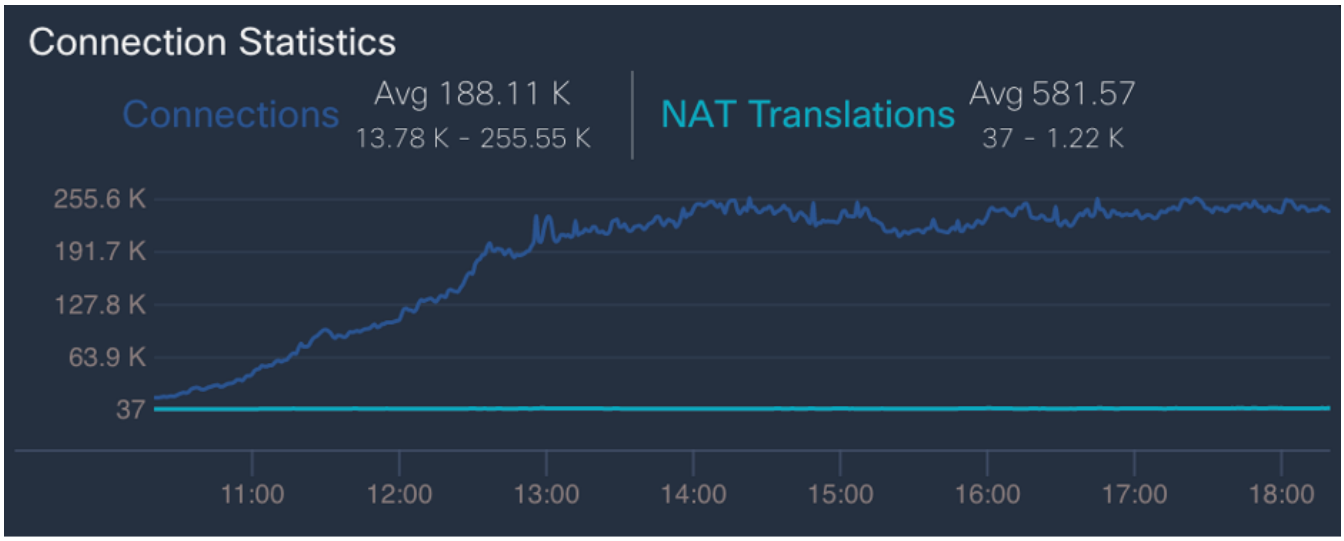
Firewall Traffic Summary

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

Peak Traffic: 1.52 Gbps

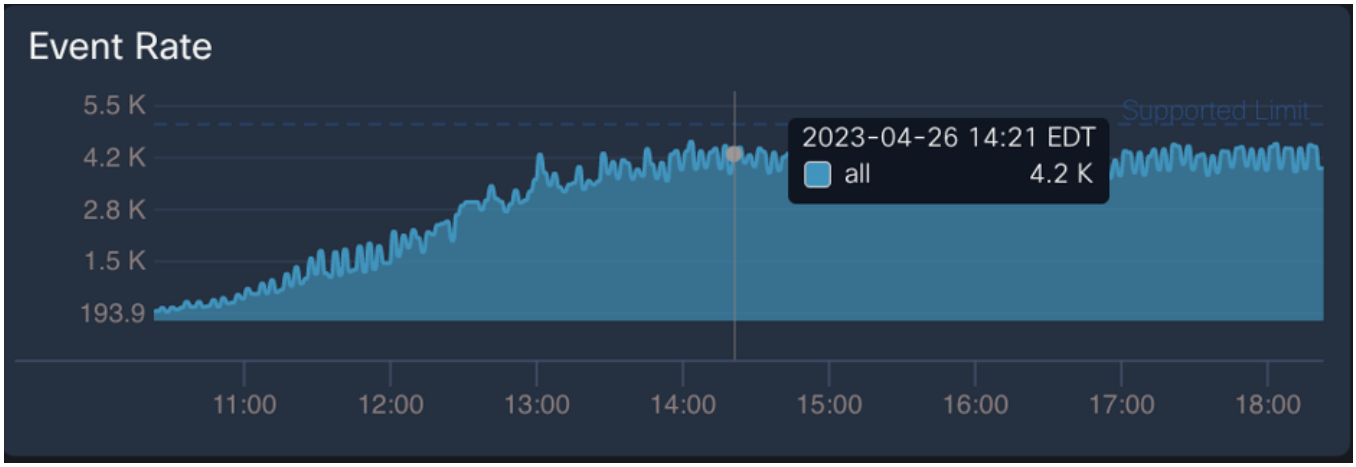


Peak Connections: 255K



Connections/sec: 2.37K

Event Rate: 4.4K/sec



CONCLUSION

After a few years of slight improvement with using encryption and secure protocols, 2023 was a step back. We can all make greater strides in becoming more secure, but we need to learn to stop giving away valuable information that can only hurt us. We have valuable information and—based on analysis of this free public wireless network—we are giving away way too much of that information.

The percentage of encrypted traffic rose two percent to 80 percent. Encrypt, encrypt…trust, but verify!
You can view the presentation and recording from the 4th Annual SOC Report here.

We're looking forward to monitoring traffic at next year's RSAC and reporting the results to you. The RSAC SOC team 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 2024!

ACKNOWLEDGEMENTS

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

NetWitness Staff

Steve Fink

Dave Glover

Iain Davison

Alessandro Zatti

Coody Spooner

Bart Stump

Bj Deonarain

Joseph Murphy

Theodore Hanibal

Kalyan Ramkumar

Cisco Staff

Jessica Bair Oppenheimer	*Cisco SOC Manager*
Ian Redden	*Team Lead & Integrations*
Aditya Sankar / Ben Greenbaum	*Cisco XDR, Secure Cloud Analytics & Malware Analytics*
Alejo Calaoagan / Christian Clasen	*Cisco Umbrella*
Dinkar Sharma / Adam Kilgore	*Cisco Secure Firewall*
Brian McMahon	*Threat Wall*

NETWITNESS

RSA

CISCO