RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **MASH-R05**

EXPOSURE: The 3rd Annual RSAC SOC Report

Steve Fink
Regional VP
NetWitness
@InfoSecFink

Jessica Bair Oppenheimer
Director, Technical Alliances
Cisco Secure
@jessicambair

Dave Glover
Principal System Engineer
NetWitness
@rsa_logfather

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

RSAC SOC

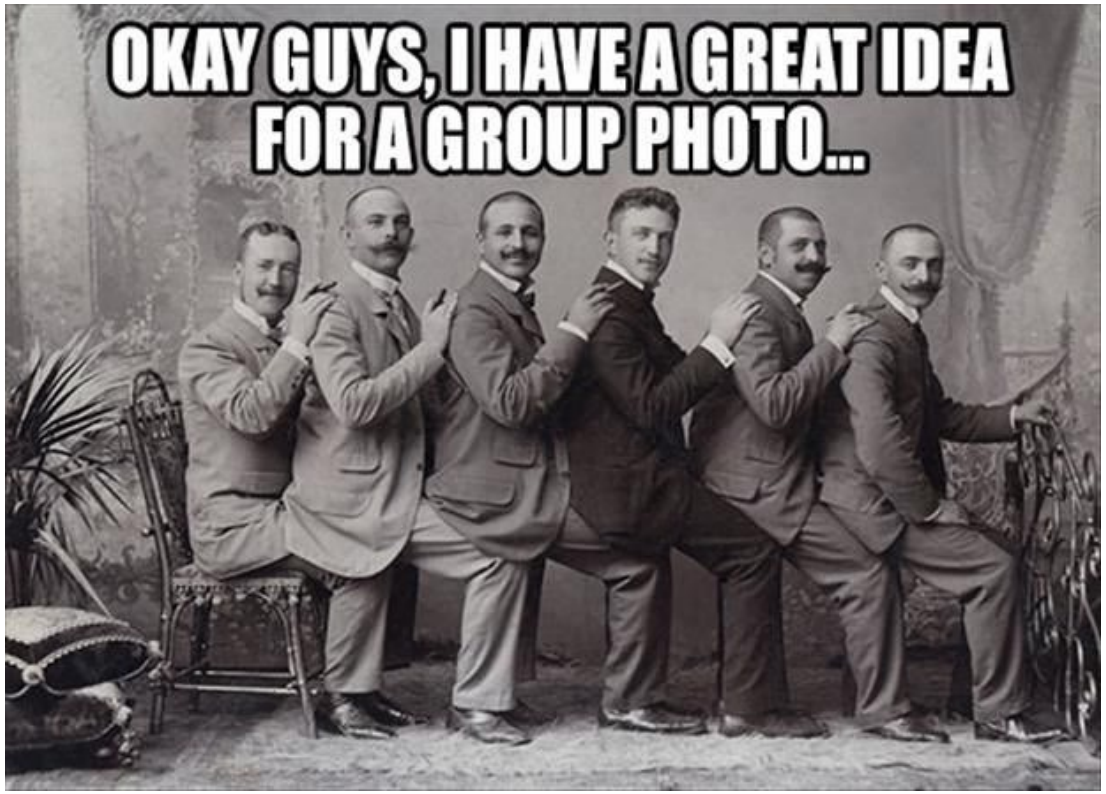
- 7 Years Running
- 10 Tours: 20-50 people each
- Countless “Private” Tours
- Multiple Press Interviews
- Annual Findings Report

- Conference Span/TAP
- NetWitness Platform XDR
- NetWitness Orchestrator
- Cisco SecureX XDR
- Cisco Secure Malware Analytics/Threat Grid

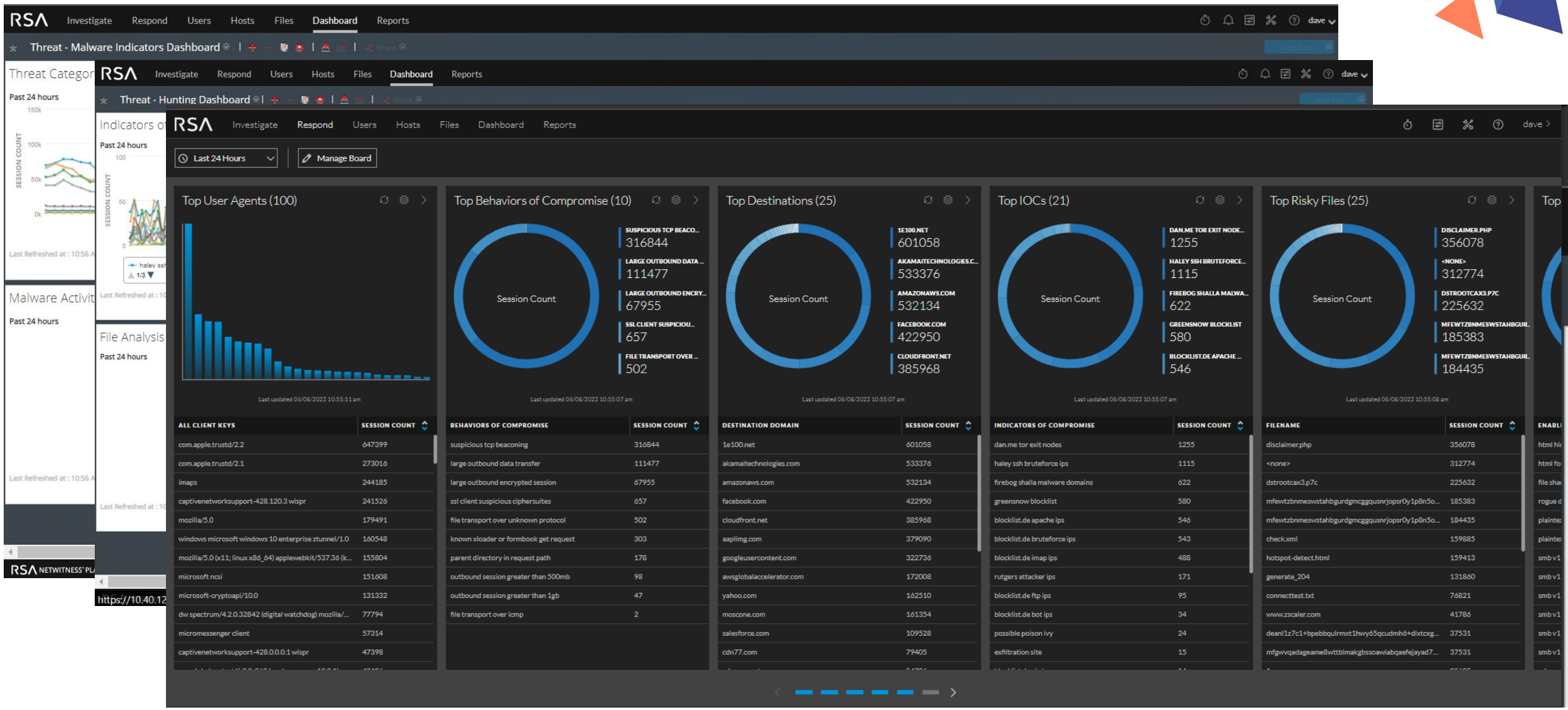
- Cisco Umbrella DNS
- Cisco Secure Firewall – Intrusion Detection
- Cisco Talos Intelligence
- IBM X-Force Exchange
- alphaMountain.ai
- Recorded Future

The Team

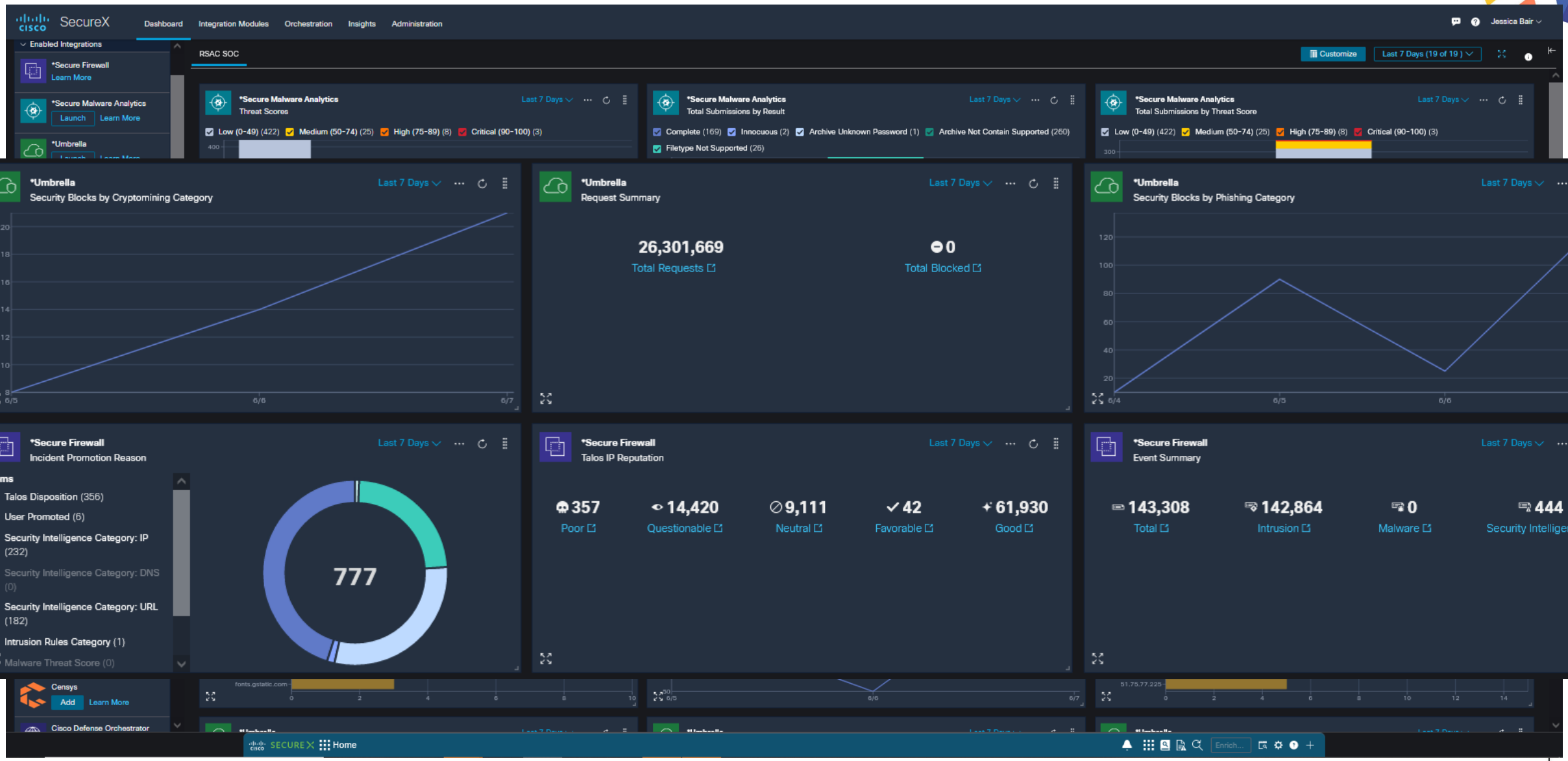
- 5 NetWitness Analysts
- 9 Cisco Analysts
- 1 IBM Threat Hunter



The Dashboards

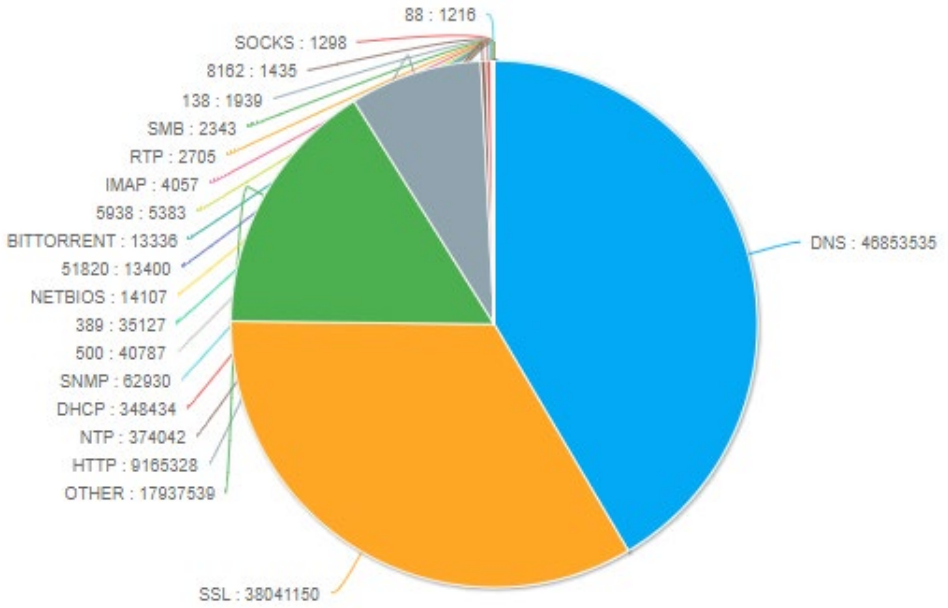


More Dashboards!!!



The Stats

- Total Packets Captured: 11.8 Billion
- Total Logs Captured: 108 Million
- Total Sessions: 187,301,858
- 13,253 Unique Devices
- 7.39 TB of packet data
- 508 GB of log data

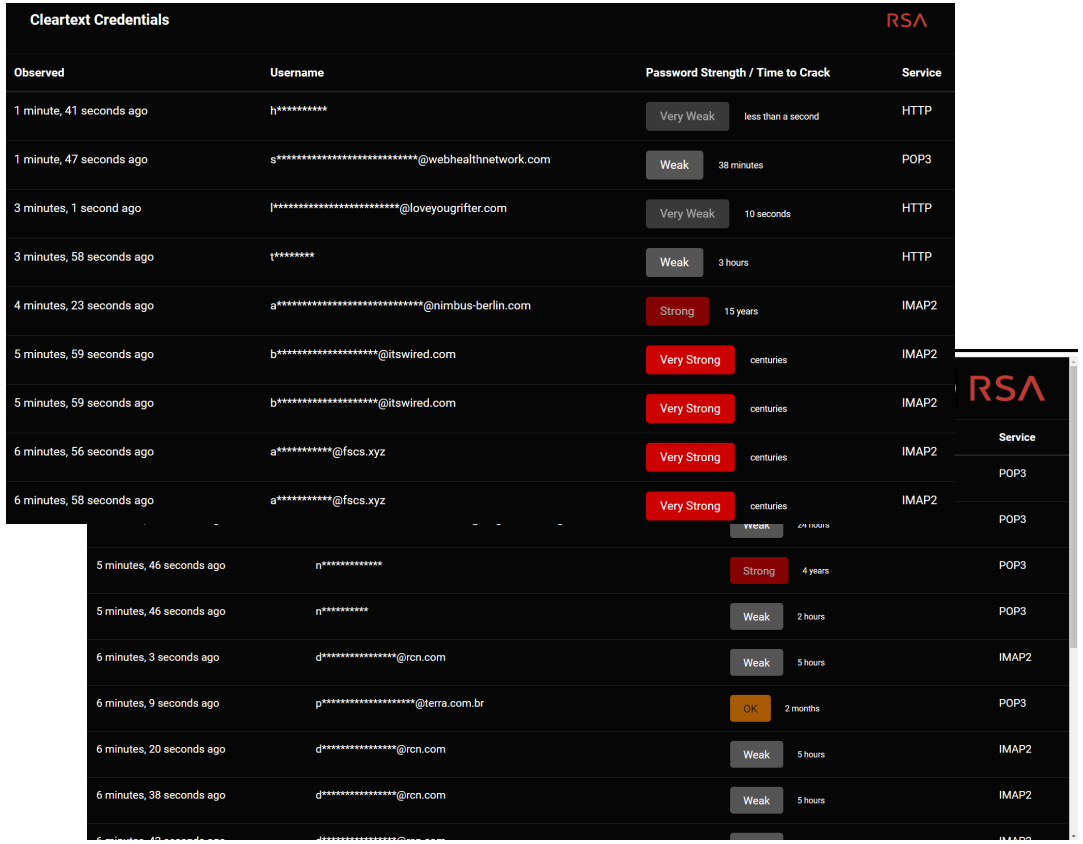


- Peak Bandwidth Usage: 1.35Gbps
- - Similar to 2020
- ~46 Million DNS Requests

- ~80% Encrypted Traffic
- ~20% Mayhem

- SSL & TLS
  - Version - Session Count
    - SSL 3.0 - 5059
    - TLS 1.0 - 169653
    - TLS 1.1 - 3209
    - TLS 1.2 - 22352887
    - TLS 1.3 - 15703469

It’s Raining Passwords



Cleartext Credentials RSA

Observed	Username	Password Strength / Time to Crack	Service
1 minute, 41 seconds ago	h*********	Very Weak less than a second	HTTP
1 minute, 47 seconds ago	s**********@webhealthnetwork.com	Weak 38 minutes	POP3
3 minutes, 1 second ago	l**********@loveyougrifter.com	Very Weak 10 seconds	HTTP
3 minutes, 58 seconds ago	t********	Weak 3 hours	HTTP
4 minutes, 23 seconds ago	a**********@nimbus-berlin.com	Strong 15 years	IMAP2
5 minutes, 59 seconds ago	b**********@itswired.com	Very Strong centuries	IMAP2
5 minutes, 59 seconds ago	b**********@itswired.com	Very Strong centuries	IMAP2
6 minutes, 56 seconds ago	a**********@fscs.xyz	Very Strong centuries	IMAP2
6 minutes, 58 seconds ago	a**********@fscs.xyz	Very Strong centuries	IMAP2

RSA

Service
POP3
POP3
POP3
POP3
IMAP2
POP3
IMAP2
IMAP2

5 minutes, 46 seconds ago	n**********	Strong 4 years	POP3
5 minutes, 46 seconds ago	n*********	Weak 2 hours	POP3
6 minutes, 3 seconds ago	d**********@rcn.com	Weak 5 hours	IMAP2
6 minutes, 9 seconds ago	p**********@terra.com.br	OK 2 months	POP3
6 minutes, 20 seconds ago	d**********@rcn.com	Weak 5 hours	IMAP2
6 minutes, 38 seconds ago	d**********@rcn.com	Weak 5 hours	IMAP2

2022

55,525 - Cleartext Passwords

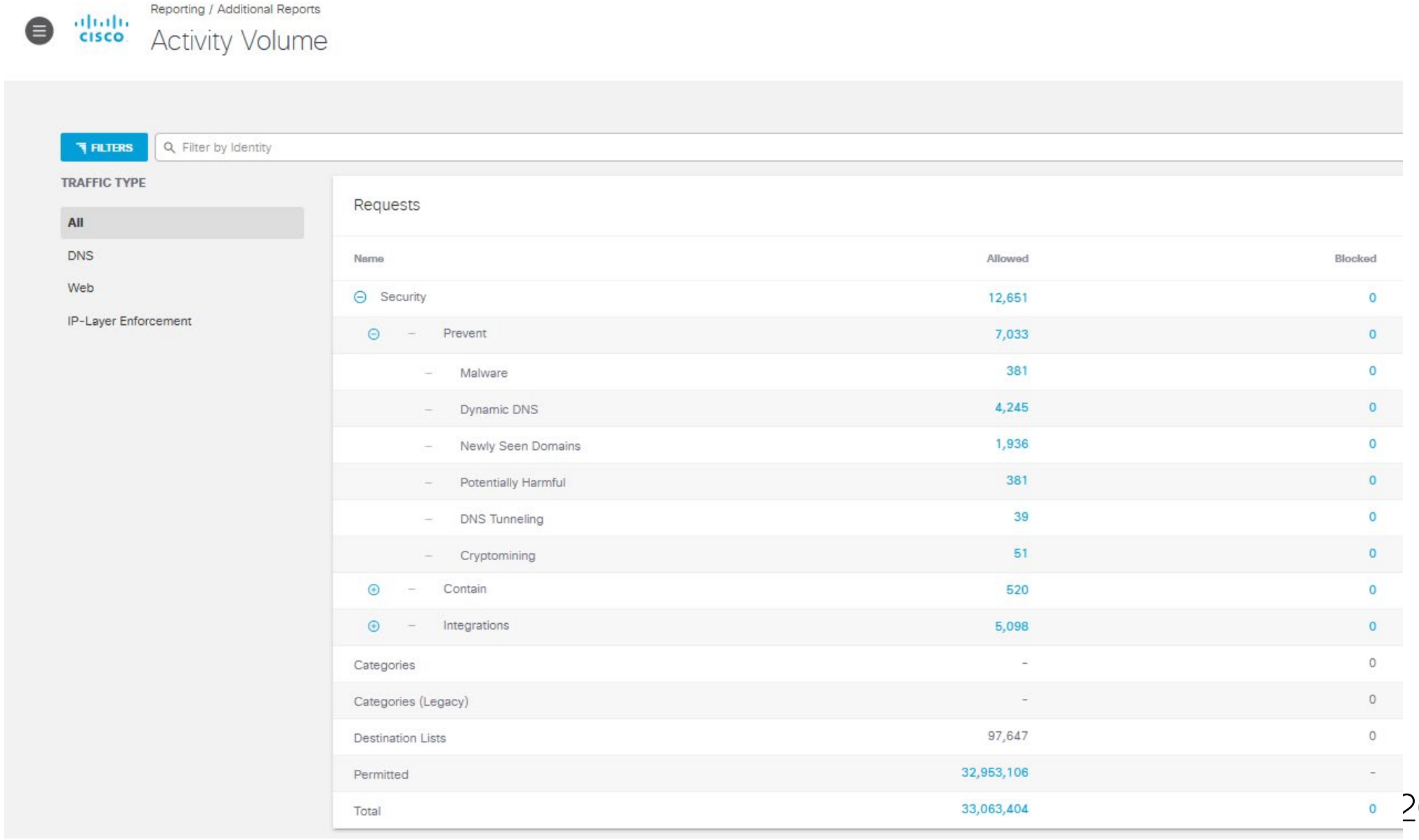
2,210 - Unique Accounts

2020

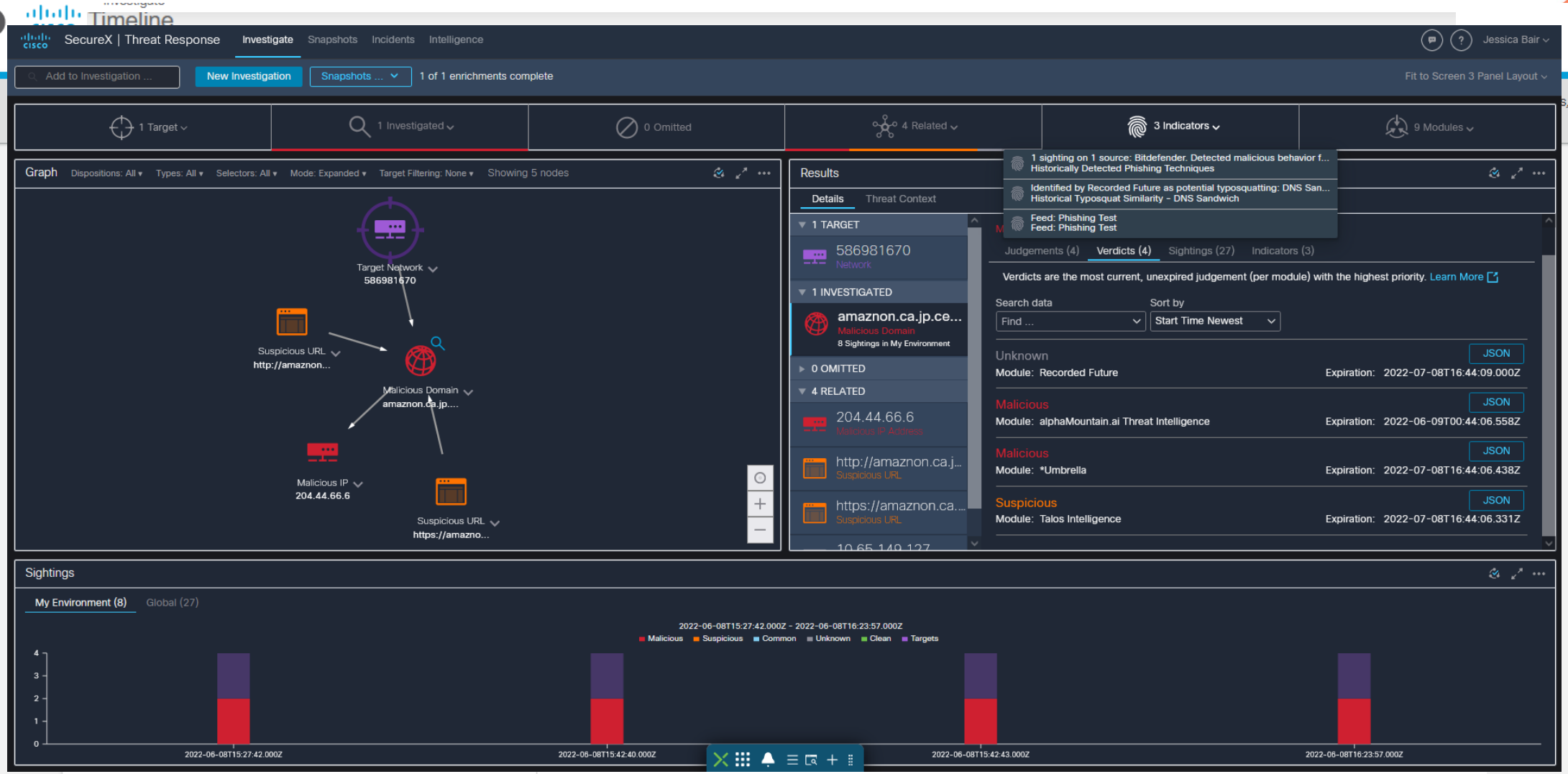
96,361 - Cleartext Passwords

2,178 - Unique Accounts

Umbrella Total Requests ~32m (~37m in 2020)



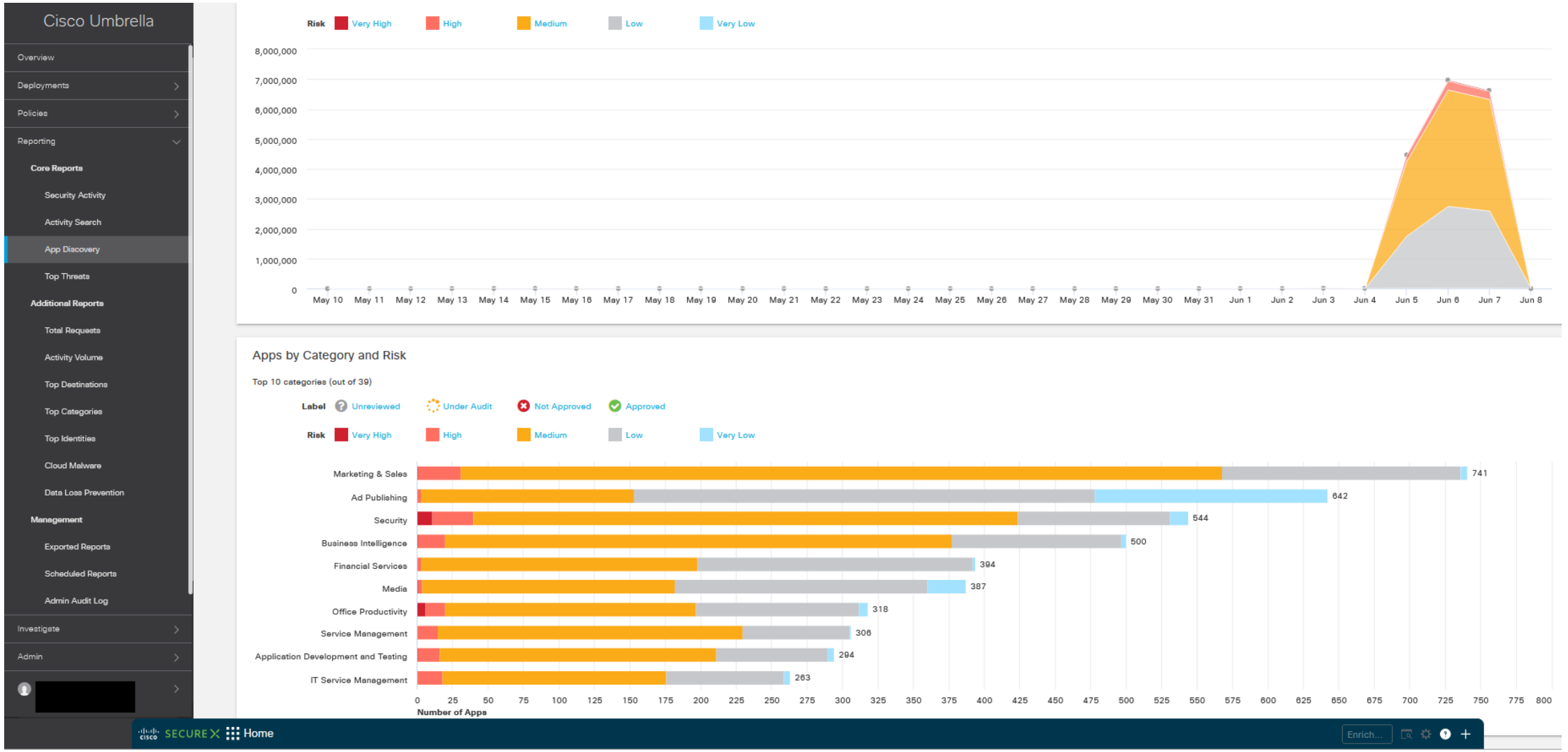
Block or not to Block, that is the Question



Awards

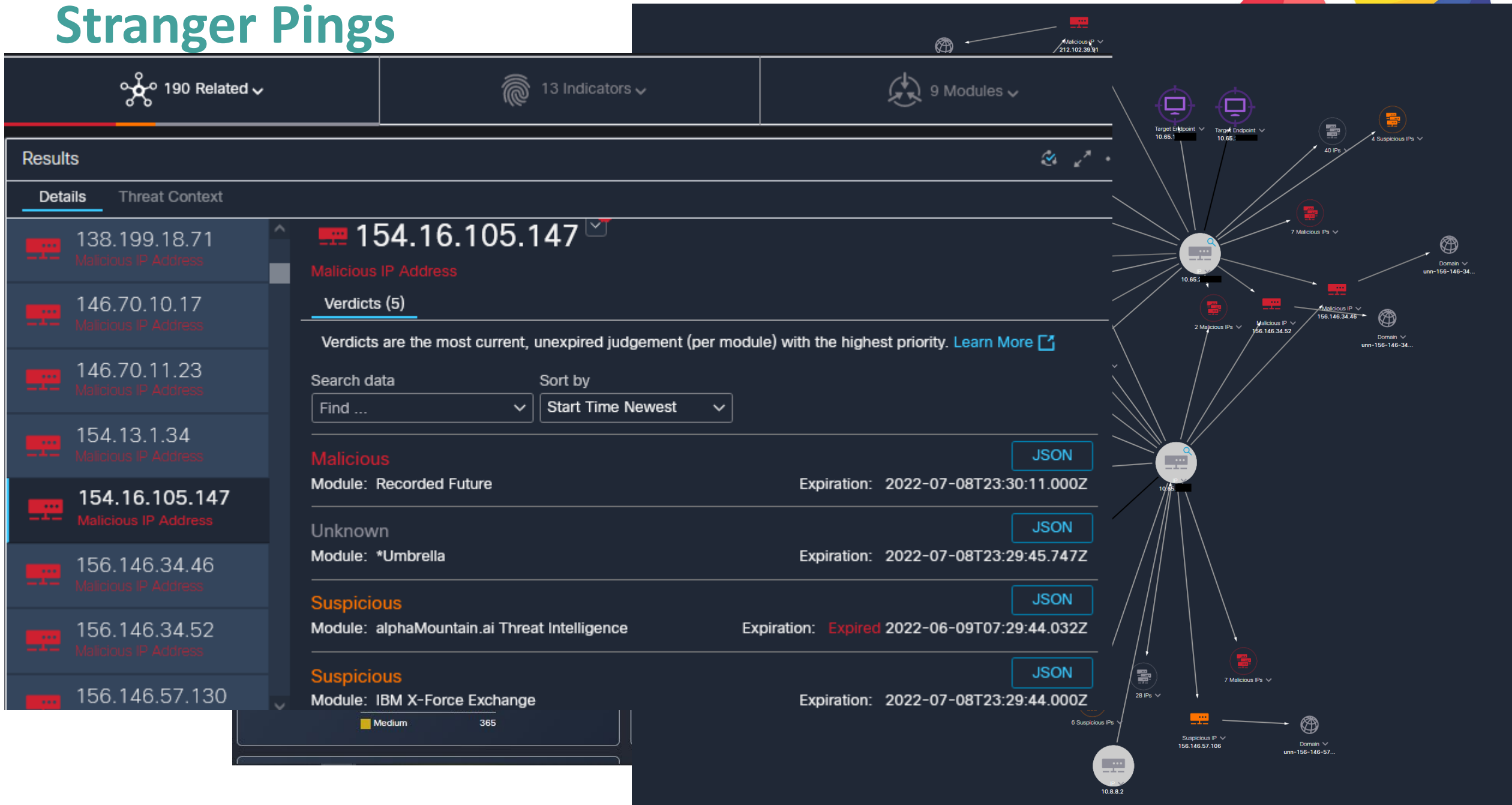
- #1 App: Office365
- #1 Chat: WhatsApp
- #1 Cryptomining: NiceHash
- #1 Dating: grindr
- #1 Porn: xvideos

DNS App Discovery - Over 7K Applications (~4K in 2020)



Firewall: Firepower Intrusion Detection

Stranger Pings

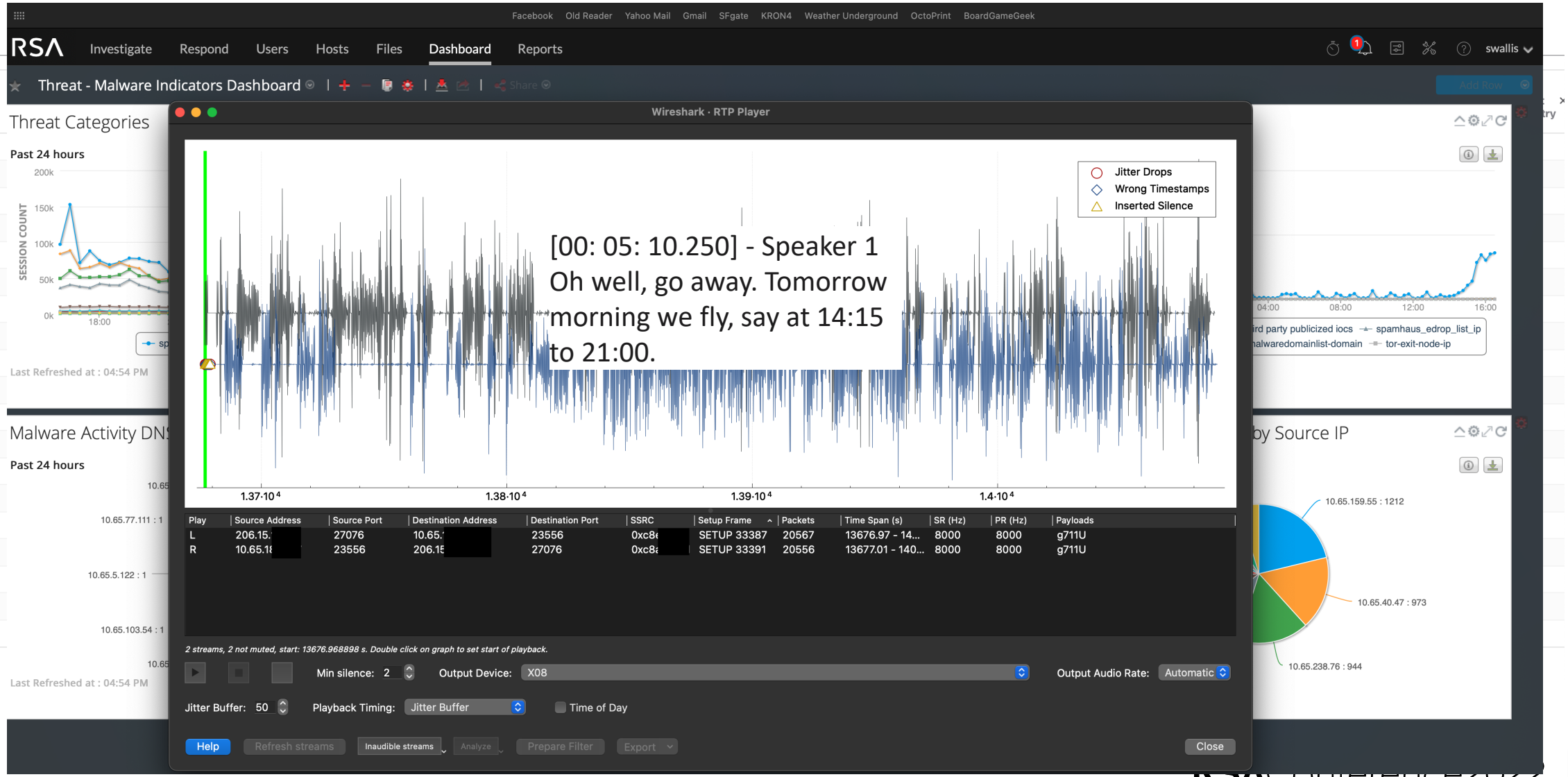


RSAConference2022

Story time

Tales from the SOC

Can you hear me now?!?



How are things back home? Laundry Day?

Event Reconstruction

service	id	type	source	destination	service	first packet time	last packet time	packet size	payload size	packet count	flags
NW-HU - Broker	123399301	Network Session	10.65[redacted] 62120	82.65.[redacted] : 5000	80	2022-06-08T16:27:22.731	2022-06-08T16:27:23.567	67,878 bytes	62,374 bytes	82	Keep, Assembled, App Meta, Network Meta

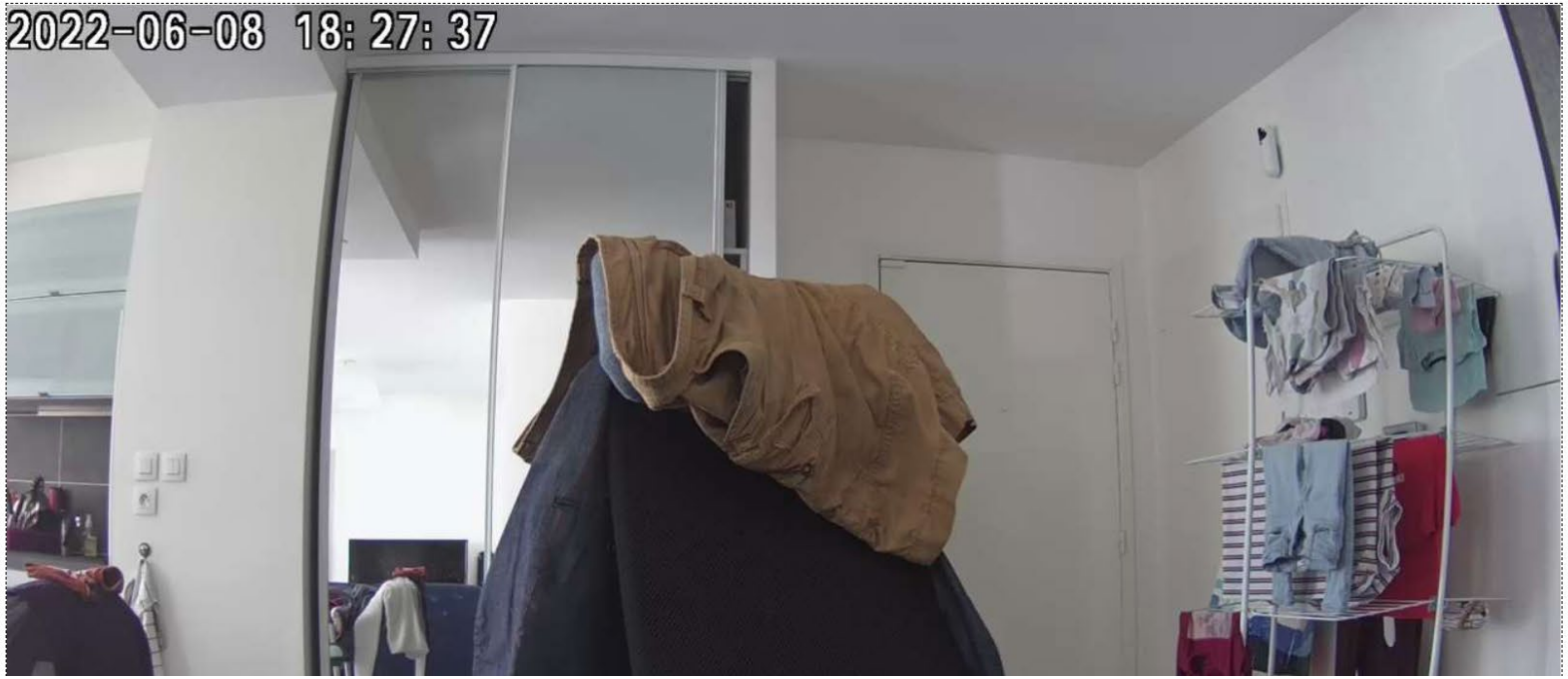
Request & Response | Top To Bottom | View Web | Actions

Request

```
GET /[redacted]SurveillanceStation.SnapShot&version=1&method=GetPushServSnapshot&supportNotiEncrypt=true&snapshotId=20749&_sid=2TTbHmeSSZTZdjE1Y_rPEQ0r6FA2qLDbU5NFQKuFpz09uSYQ2m7R3QaF0pKdlwHvNlk19F957aOPHwKd00ZIEE
(host: 82.65.[redacted]5000)
```

Response

Content-Type: image/jpeg




```
"ip": "82.65.[redacted]",
"country_name": "France",
"state_prov": "Ile-de-France",
"city": "Paris",
"latitude": "48.[redacted]",
"longitude": "2.[redacted]",
"time_zone": "Europe/Paris",
"isp": "Free SAS",
"currency": "Euro",
"country_flag":
```

Internet of Pets…I mean Things

RSA Investigate Respond Users Hosts Files Dashboard Reports spooner

NAVIGATE LEGACY EVENTS EVENTS MALWARE ANALYSIS

Event Reconstruction

service	id	type	source	destination	service	first packet time	last packet time	packet size	payload size	packet count	flags
NW-PKH - Concentrator	104743931	Network Session	10.65.[redacted] : 65329	47.254.[redacted] : 8088	80	2022-06-07T14:50:08.096	2022-06-07T14:50:11.356	6,602 bytes	4,236 bytes	35	Keep, Assembled, App Meta, Network Meta

Request & Response | Top To Bottom | View Web | Actions

Request

GET /[redacted]_Server/server.php?cmd=random&userid=[redacted]@gmail.com&platform=mail&appn=[redacted]
(host: 47.254.44.196:8088)

Response

Content-Type: text/html

{"cmd":1002, "code":20000, "msg":"f6a2451b"}

Request

GET /[redacted]_Server/server.php?cmd=login&platform=mail&userid=[redacted]@gmail.com&passwd=[redacted]&appn=[redacted]
(host: 47.254.44.196:8088)

Response

Content-Type: text/html

{"cmd":1003, "code":20000, "msg":[{"devid":"XK8XXG186SN1FW7V111A", "devusr":"admin", "devpw":"[redacted]", "devconn":"p2p", "devchnl":"0", "devstream":"main", "devalias":"Dog Camera", "devtype":"pack", "unittype":"LSD01", "tzsec":"", "location":"", "sndeffect":"yes", "petid":"61ad791d27a4c2d070e7cd747735f075"}]}

Request

GET /[redacted]t_Server/server.php?cmd=iconname&platform=mail&userid=[redacted]@gmail.com&petid=[redacted]&appn=[redacted]
(host: 47.254.44.196:8088)

Help! I need a Medic!

Certificado de Seguro de [redacted]

Nombre y Domicilio del Contratante	Póliza No.	Certificado No.
[redacted]. DE R.L. DE C.V.	M09[redacted]	[redacted]18

Nombre del asegurado Titular:	Subgrupo
[redacted]	004

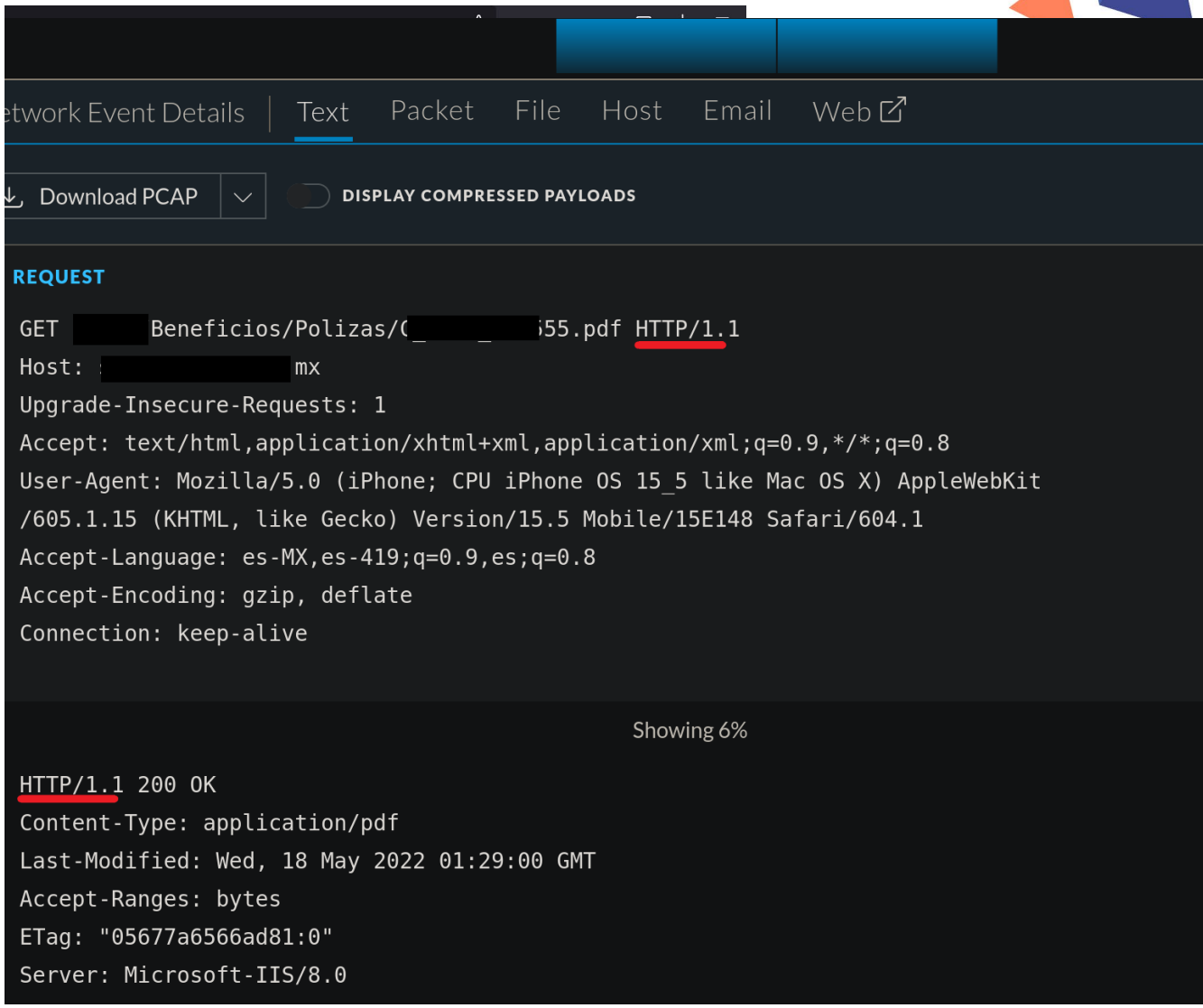
Sexo:	Estado Civil:	Fecha de Nacimiento: Día Mes Año	Fecha de Ingreso a la colectividad asegurada Día Mes Año	Vigencia de la póliza Desde las 12:00 hrs. Día Mes Año	Hasta las 12:00 hrs. Día Mes Año
MASCULINO	NO APLICA	[redacted]	[redacted]	04 04 2022	04 04 2023

RELACION DE ASEGURADOS

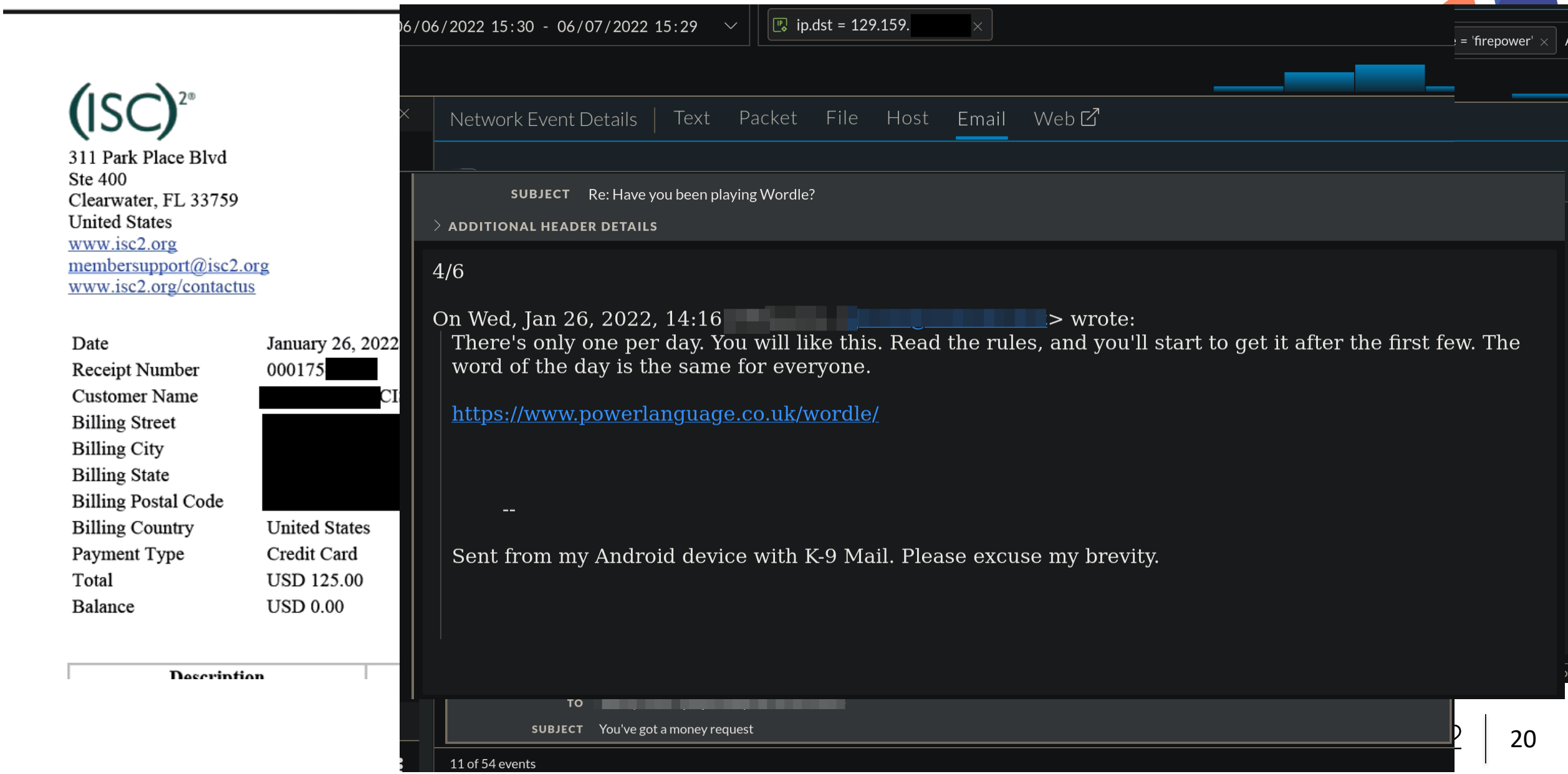
Nombre(s), apellido paterno y apellido materno	Sexo	Parentesco	Fecha de Nacimiento	Fecha de Antiguedad al Seguro
[redacted]	MASC.	TIT.	[redacted]	01 06 20[redacted]
	FEM.	CONY.		01 06 20
	FEM.	HIJO		01 06 20

Características del Seguro Contratado
Características del plan

TIPO DE PLAN CONTRATADO	EJECUTIVO
SUMA ASEGURADA	50,000 U.M.A.M.
SUMA ASEGURADA INTERNACIONAL GERENTES	300,000.00 DLLS.
DEDUCIBLE	4 U.M.A.M.
COASEGURO	10%
HONORARIOS QUIRURGICOS	G.U.A. [redacted]
TRE01	
EMERGENCIA EN EL EXTRANJERO ZONA " B "	AMPARADA
DERECHO DE CONVERSIÓN	AMPARADO
ASISTENCIA INTEGRAL	AMPARADA



Chewing through email…



(ISC)²
311 Park Place Blvd
Ste 400
Clearwater, FL 33759
United States
www.isc2.org
membersupport@isc2.org
www.isc2.org/contactus

Date	January 26, 2022
Receipt Number	000175[redacted]
Customer Name	[redacted]CI
Billing Street	[redacted]
Billing City	
Billing State	
Billing Postal Code	
Billing Country	United States
Payment Type	Credit Card
Total	USD 125.00
Balance	USD 0.00

Description

06/06/2022 15:30 - 06/07/2022 15:29

ip.dst = 129.159.[redacted]

= 'firepower'

Network Event Details | Text | Packet | File | Host | Email | Web

SUBJECT Re: Have you been playing Wordle?

ADDITIONAL HEADER DETAILS

4/6

On Wed, Jan 26, 2022, 14:16 [redacted] > wrote:

There's only one per day. You will like this. Read the rules, and you'll start to get it after the first few. The word of the day is the same for everyone.

https://www.powerlanguage.co.uk/wordle/

--

Sent from my Android device with K-9 Mail. Please excuse my brevity.

TO [redacted]

SUBJECT You've got a money request

11 of 54 events

Spear Phishing, Anyone?

of 1995, Pub. L. No. 104-13, 44 U.S.C. § 3501, et seq. Public reporting burden for this collection of information is estimated to average 4.5 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, completing, and reviewing the collecti of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the report burden to the Federal Communications Commission, Performance Evaluation and Records Management, Washington, DC 20554. We also will accept your comments via the email if you send them to PRA@FCC.gov. DO NOT SEND COMPLETED WORKSHEETS TO THESE ADDRESSES.

Authorized Person

Title: Chief Technology Officer

Name: [redacted]

Phone: [redacted]687-[redacted]

Email: [redacted]org

Address: [redacted]

Employer: [redacted]SCHOOL DISTRICT [redacted]

Certified Timestamp

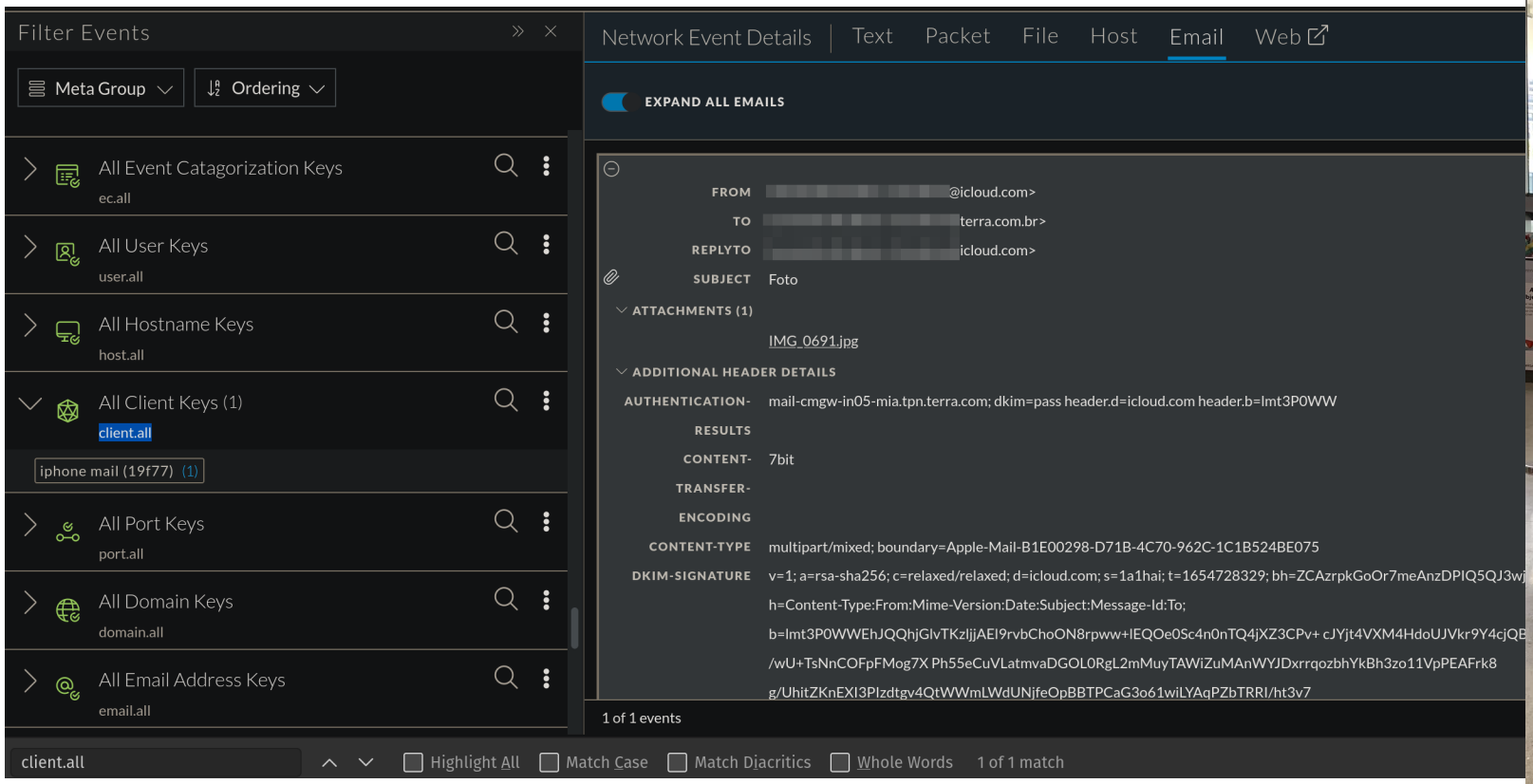
13-May-2022 20:15:04 EDT

which funding is sought

The equipment and services the school, library, or consortium purchases or will purchase using Emergency Connectivity Fund support will be used primarily for educational purposes and will not be sold, resold, or transferred in consideration for money or any other thing of value, except as allowed by ## 54.1713.

		Total Student Count	Urban or Rural
[redacted]	[redacted]SCHOOL DISTRICT [redacted]	1286	Urban

How do you make iPhone email insecure?!?



Important! The wireless network available at the Moscone Center is an open, unsecured 5 GHz network.

Also note that this year, 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.

“Apply” Slide