VIRGINIA IT AGENCY

WELCOME TO THE DEC. 7, 2022

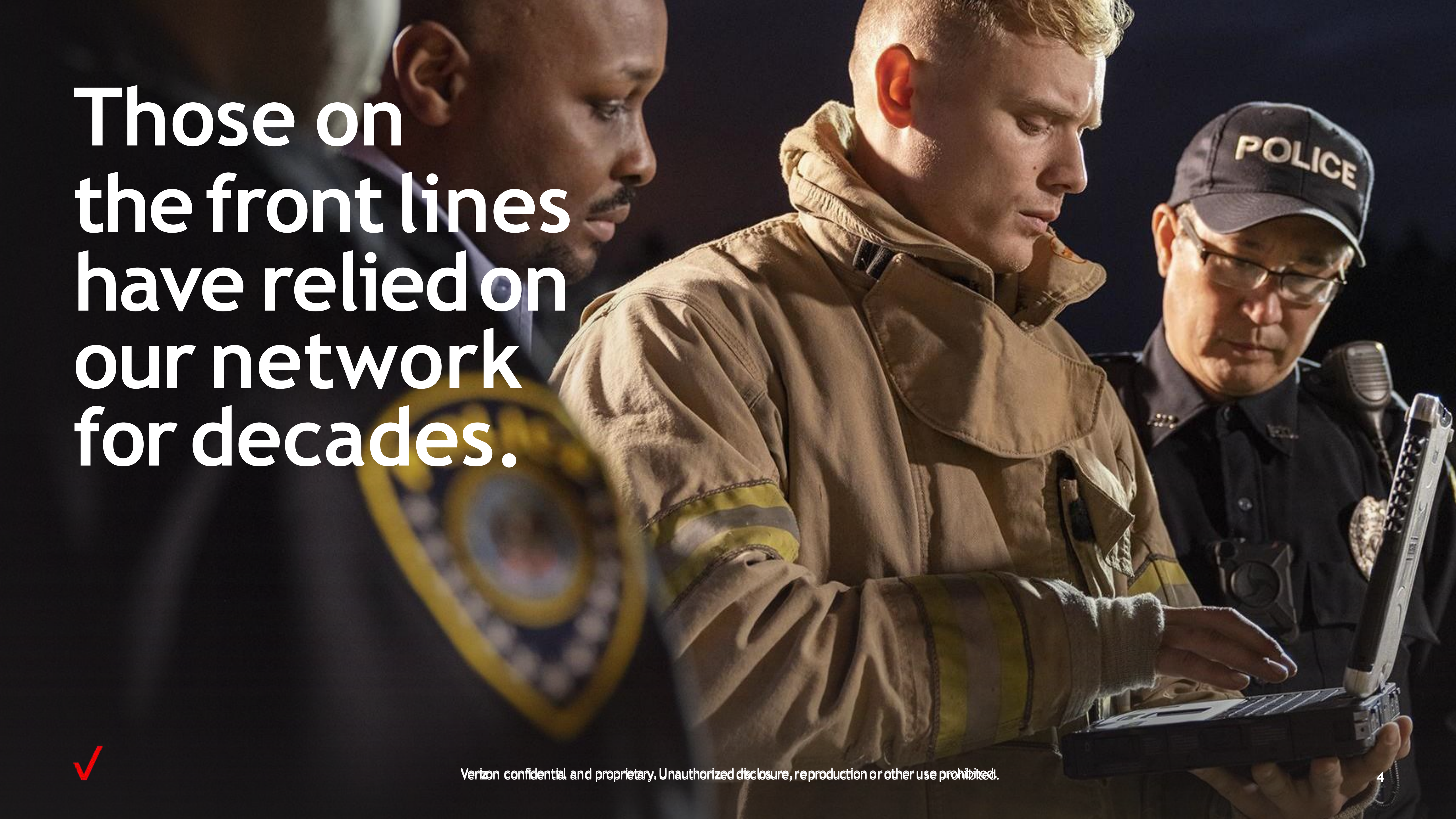
ISOAG MEETING

VIRGINIA
IT AGENCY

AGENDA	
Welcome	Ed Miller / VITA
Crisis Response	Tetoya Gibson/ Verizon
Website Modernization Program	Joshua Jones/ VITA
Security Heroes: Empowering employees in cyber defense	Dan Han/ VCU
AlgoSec Firewall Analyzer	Darrell Raymond, Rob Sullivan & Kevin McLess/ATOS
Upcoming Events	Ed Miller/ VITA
Adjourn	

Verizon Frontline

Tetoya Gibson
Crisis Response Manager
Virginia/W. Virginia/DOD



Those on the front lines have relied on our network for decades.

Verizon confidential and proprietary. Unauthorized disclosure, reproduction or other use prohibited.

Who is the Verizon Frontline Crisis Response Team?

Ready to Respond to the Frontline

We support first responders, the military, public safety professionals, government agencies and their communities. Our mission is to help them stay connected with Verizon Frontline technology during emergencies and planned events 24/7

Verizon Frontline Crisis Response Team Support includes:

- Nationwide 24/7 hotline: (800) 981-9558
- Loaner phones, data devices, & first responders solutions
- Enterprise grade 4G LTE routers with antenna solutions
- In-building solutions, COW/COLT, MCT
- Emergency Communications and Charging Centers
- Pre-event planning site assessments and exercise support
- VSAT Support - Missing Persons / SAR

Support Model

1K+	600+	5K+	42
YTD '22 Customer Engagements	YTD '22 Customer Deployments	YTD '22 Solutions Loaned	YTD '22 States Supported

Prepare

- Joint Training with First Responder Agencies
- Proactive Customer Engagements
- Augmented Solutions to Adapt to Changing/ Scaled Needs

Respond

- First Responder Emergency Support
- Virtual Emergency Operation Center Activation
- Enhanced Connectivity & Coverage Solutions

Mitigate

- Post Event Debrief with Emergency Management
- Customer Awareness Meetings
- Virtual Environment Planning & Disaster Response Planning

Recover

- FEMA Emergency Support Function
- Pre-staged Evacuation & Shelter Support
- Testing Center Support
- After Action Reviews

Disaster Response

Priorities

- SAR Operations
- EOC Support
- Shelter Support - Private/State
- Rebuild Phase - Utilities

Assets Available

- Satellite Communications
- Phones/MiFi's/Tablets
- Enterprise Routers
- sUAS Support
- Complete EOC Communications

Remote Area Support

Priorities

- SAR Operations
- EOC Support
- Rebuild Phase - Utilities

Assets Available

- Satellite Communications
- Phones/MiFi's/Tablets
- Enterprise Routers
- sUAS Support
- Complete EOC Communications

Verizon Frontline Crisis Response

Hurricane Ian Response:

Engagements: **200+**

Agencies: **70+**

Deployments: **90+**

Verizon Frontline Solutions: **400+**

States: **5**

Verizon Frontline Solutions:

Deployables

Routers

Phones

Jetpacks

LEO

Drones

eFemtos

PDNs

Charging Stations

Dejero

Verizon Frontline

Innovation Through Partnerships

Operation Allies Welcome (OAW)

Overview On August 29, 2021, President Biden directed the Department of Homeland Security (DHS) to lead implementation of ongoing efforts across the federal government to support vulnerable Afghans, including those who worked alongside us in Afghanistan for the past two decades, as they safely resettle in the United States.

These coordinated efforts will be known as Operation Allies Welcome. At the President’s direction, the Secretary of Homeland Security will work with representatives from across the government to coordinate our response and ensure unity of effort across the federal government.*

Problem:

Lack of network connectivity to support the Afghan Nationals and the representatives from federal agencies supporting OAR efforts

DOS / DHS / HHS / DOD

- Ability conduct screening and in processing of the Afghan Nationals as they arrive
- Help with applying for immigration status, workforce authorization & essential coverage
- COVID-19 Testing, Vaccinations, and Other Medical Services
- Relocation Support / Resettlement Processing

Marine Corps Base Quantico - Camp Upshur, Virginia

Teams Deployed:

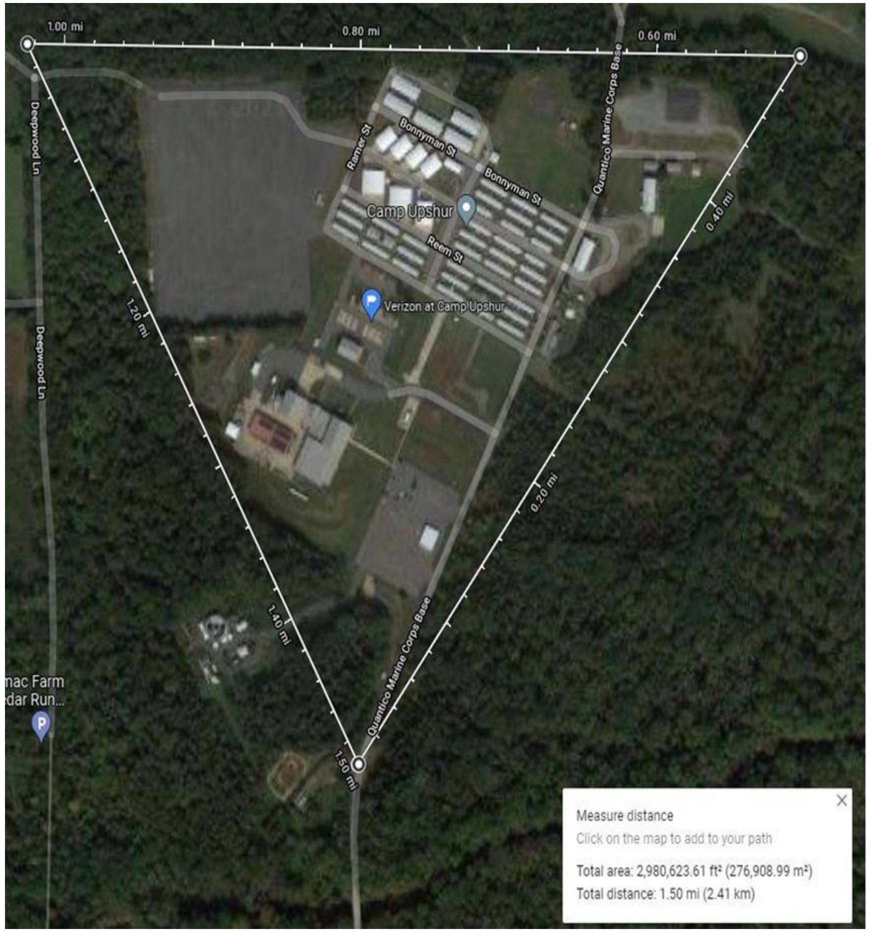
Crisis Response Team

5G Response Innovation

CradlePoint

Wireless Network Ops

AWS



Measure distance

Click on the map to add to your path

Total area: 2,980,623.61 ft² (276,908.99 m²)

Total distance: 1.50 mi (2.41 km)

0.60 mi
0.50 mi
0.70 mi
0.40 mi
0.80 mi
0.30 mi
0.90 mi
0.20 mi
1.00 mi
0.10 mi
1.10 mi
1.20 mi
1.31 mi
Lucky Run
Lucky Run

Measure distance

Click on the map to add to your path

Total area: 2,144,723.02 ft² (199,251.29 m²)

Total distance: 1.31 mi (2.10 km)

Assets Deployed:

SNOW • THOR • 2x SATCOM Trailers • ICARUS • Enterprise 5G Adapters & Routers • Wi-Fi Access points • Wi-Fi Mesh • AWS Snowball • Ubiquiti Mesh • Osmosis Mesh • MANET

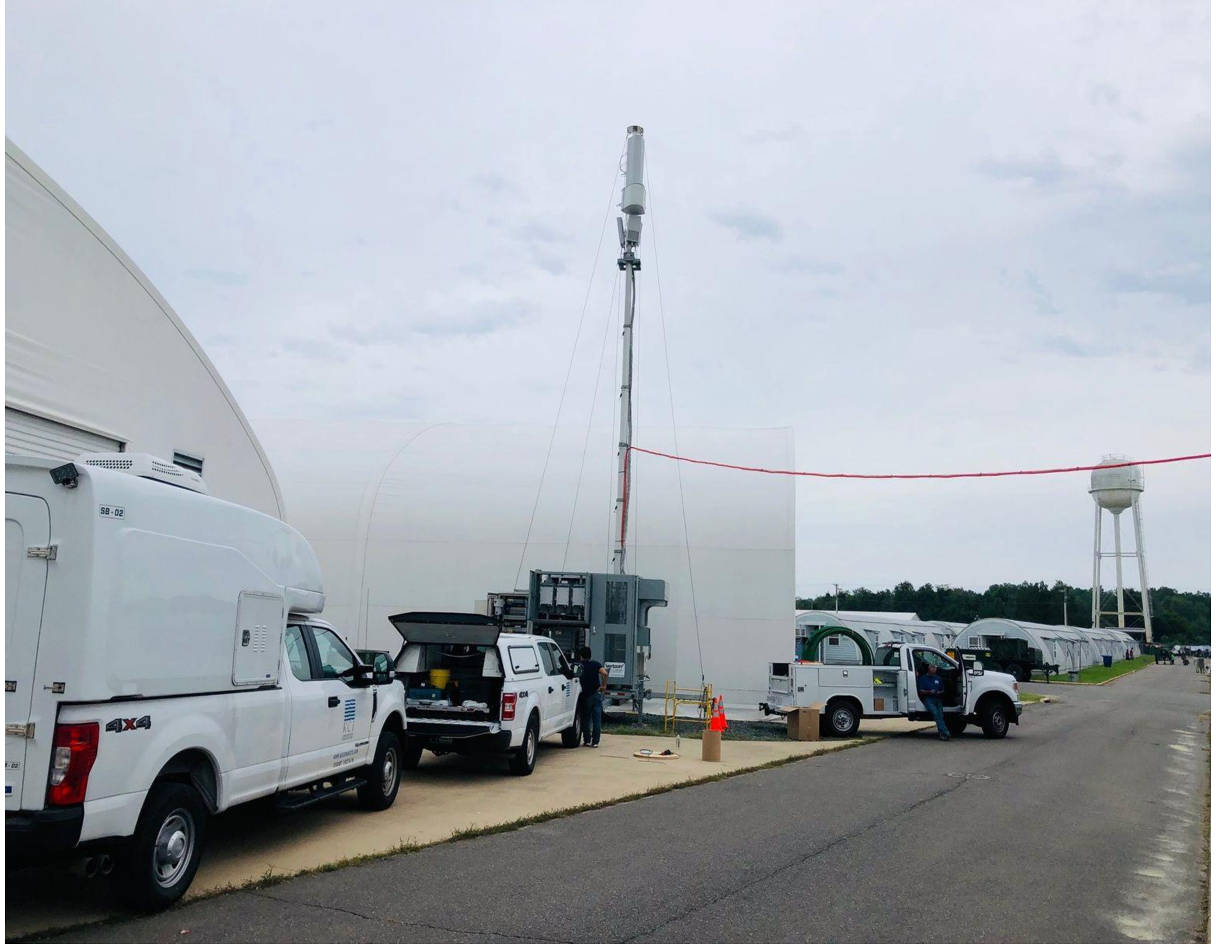
Verizon confidential and proprietary. Unauthorized disclosure, reproduction or other use prohibited.

ICARUS (Incident Command Asymmetric Response Unmanned Systems)

Monitoring mesh networks Resource platform for unconventional communications deployment

SNOW (Small Network on Wheels)

- Citizens Broadband Radio Service (CBRS
- Fiber Backhaul 12 miles + last 200m aerial
- 10 GB circuit
- 4G LTE
- 5G



Verizon Frontline Innovation Program
Ashburn, VA

The Program will focus on new, innovative technologies that provide solutions to public safety agencies.

- Provide Public Safety with hands-on experience on new technologies
- Develop new public safety partnerships

Real solutions, real deployments. **Verizon Frontline Innovation Program** will do more than just enable technology; we'll make sure that technology is what first responders truly need, and we'll make sure it's available for every agency. That's our commitment to public safety

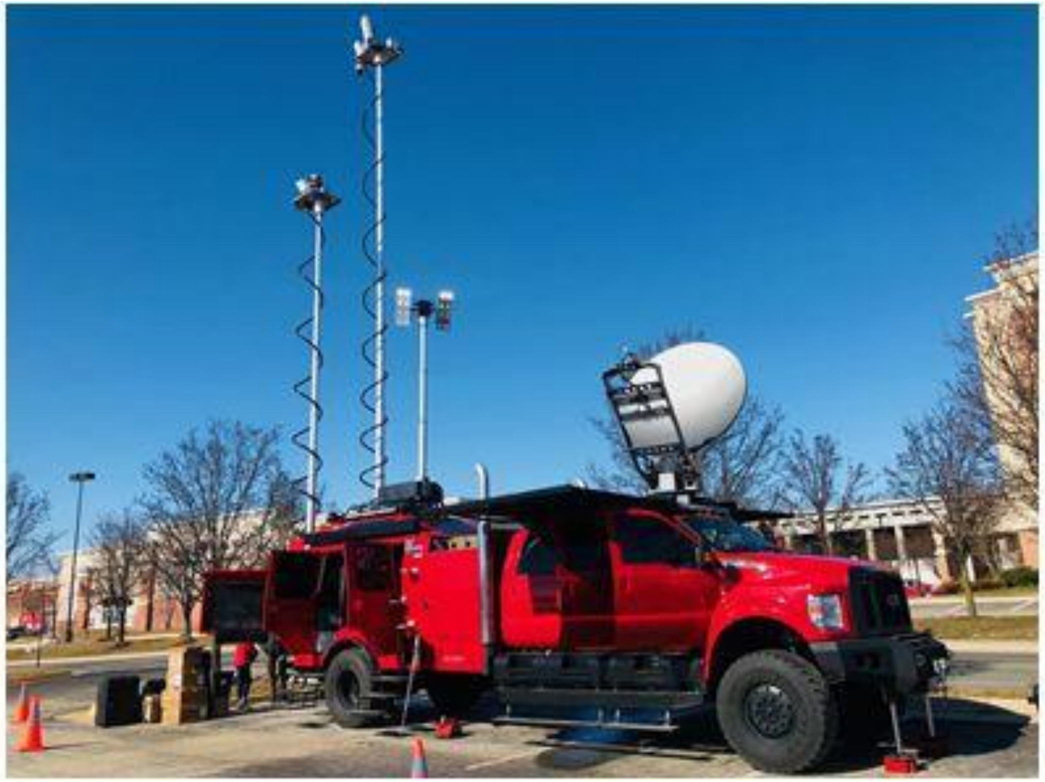
MUTT (Mobile Utility Technology Transport)

Cruiser of the future allowing multiple connectivity options for mission critical communications

VerizonFrontline
The advanced network for first responders on the front lines

THOR (Tactical Humanitarian Operations Response)

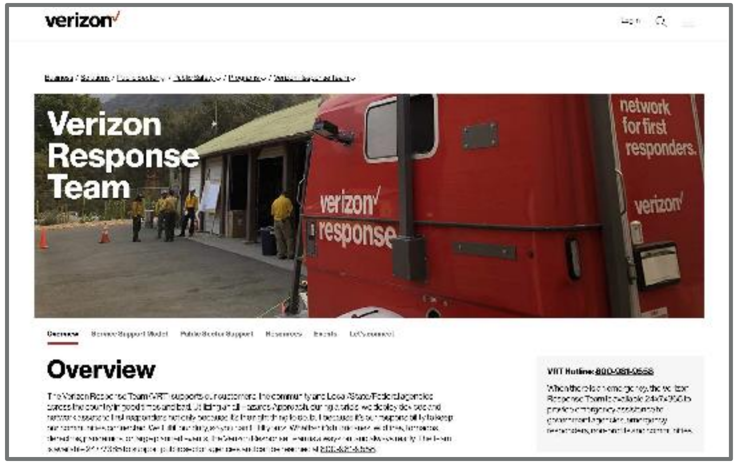
First Private 5G / MEC Disaster Response Command Center Vehicle.



VerizonFrontline Portfolio Evolution

	Today	Evolution	Future
Network Connectivity	• Dedicated Private Core • QoS, Priority and Preemption (QPP) • Fixed Wireless Access (FWA) • LTE / 5G and Private Networks	»	• Dedicated Public Safety Network Slice • QPP Expansion • FWA with Priority Access • 5G C-Band Coverage
Advanced Response	• THOR / Hammer / MUTT • Deployables • Fleet Management • 5G Mobile Edge Compute (MEC)	»	• Purpose Built Devices • In-building Services Expansion • Low Earth Orbit Satellite Alliance • 5G MEC Solutions
Secure Communications	• Interoperability Solutions • Mission Critical Push to Talk (MCPTT) • Mobile Device Management	»	• Remote Device Management • SIM Security Enhancements • Mobile Private Networks with MCPTT
Situational Awareness	• Location Based Services • Video Surveillance • Wireless Network Performance Tool	»	• Data Plan Optimization • Verizon Frontline Management Tools • Emergency Preparedness Solutions

Stay Connected with the Verizon Frontline Crisis Response Team



verizon

Verizon Response Team

Overview Service Support Model Public Sector Support Resources Events Let's connect

Overview

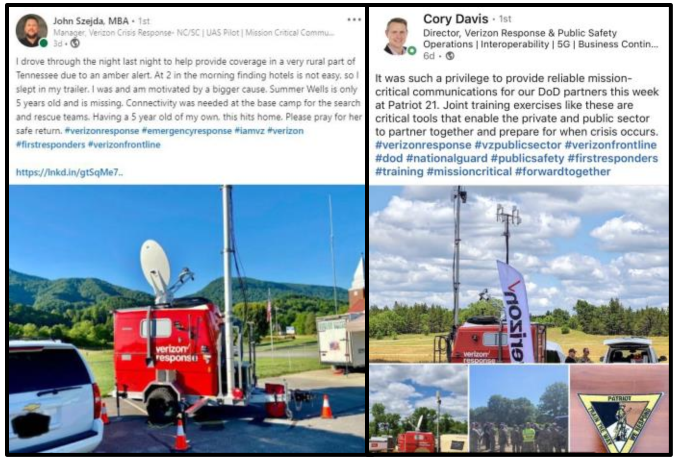
[illegible]

VRT Hotline: 800-981-9558

[illegible]

Website

verizon.com/responseteam



John Szejda, MBA • 1st
Manager, Verizon Crisis Response- NC/SC | UAS Pilot | Mission Critical Commu...
3d •

I drove through the night last night to help provide coverage in a very rural part of Tennessee due to an amber alert. At 2 in the morning finding hotels is not easy. so I slept in my trailer. I was and am motivated by a bigger cause. Summer Wells is only 5 years old and is missing. Connectivity was needed at the base camp for the search and rescue teams. Having a 5 year old of my own. this hits home. Please pray for her safe return. #verizonresponse #emergencyresponse #iamvz #verizon #firstresponders #verizonfrontline

https://lnkd.in/gtSqMe7..

Cory Davis • 1st
Director, Verizon Response & Public Safety Operations | Interoperability | 5G | Business Contin...
6d •

It was such a privilege to provide reliable mission-critical communications for our DoD partners this week at Patriot 21. Joint training exercises like these are critical tools that enable the private and public sector to partner together and prepare for when crisis occurs. #verizonresponse #vzpublicsector #verizonfrontline #dod #nationalguard #publicsafety #firstresponders #training #missioncritical #forwardtogether

Social

#Verizonfrontline

@vzfrontline

#VerizonResponse

Verizon Response Hotline
Device & Network Requests 24/7/365

Frontline CRT

verizon response

Verizon Response Hotline

1 (800) 981-9558

VIRGINIA IT AGENCY

WEBSITE MODERNIZATION PROGRAM ISOAG MEETING

JOSHUA JONES

Program Manager

DECEMBER 8, 2022

WEBSITE MODERNIZATION PROGRAM OVERVIEW

Vision

- Build trust in Virginia government websites by using standards which will ensure secure, accessible, and easily identifiable state websites

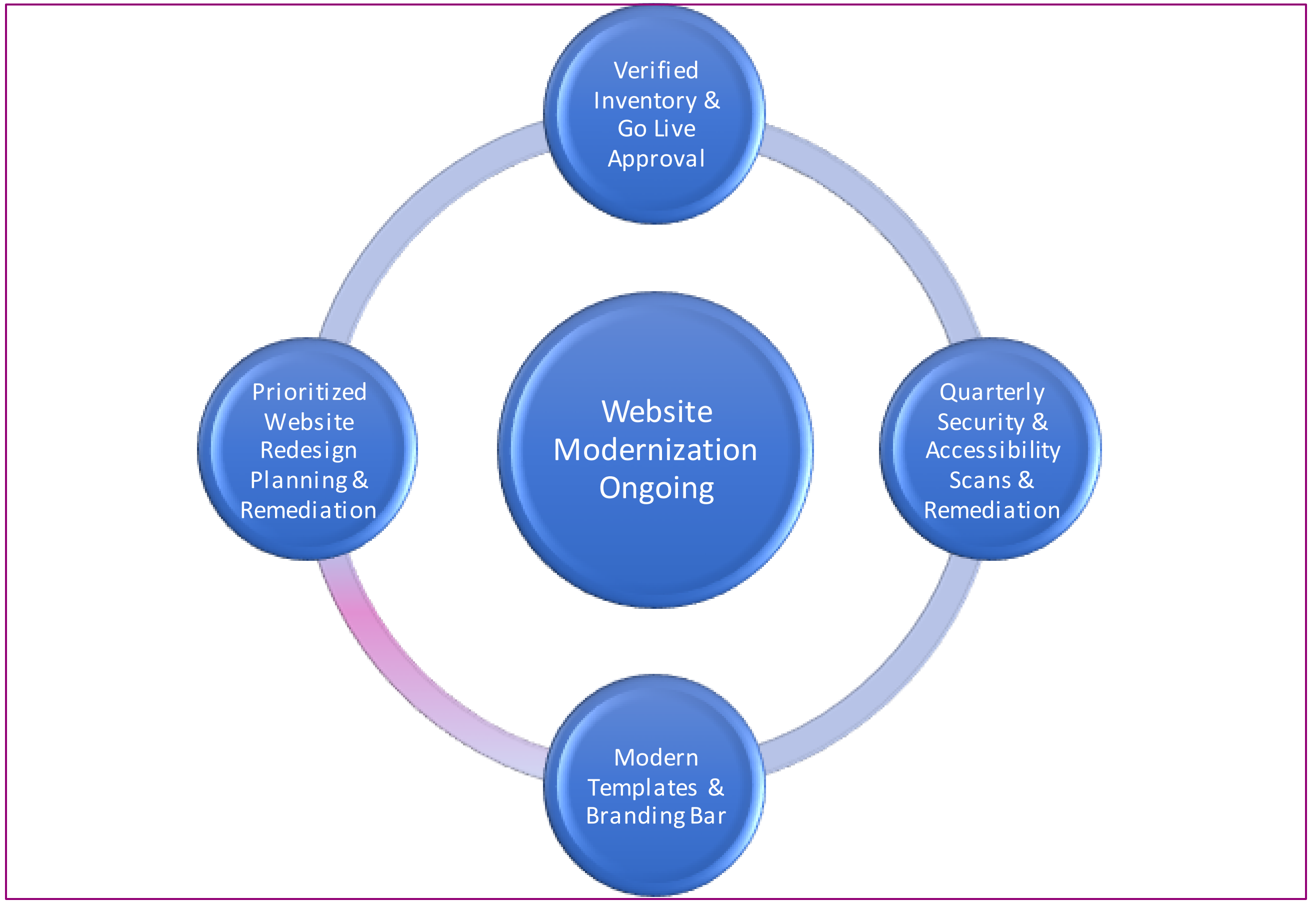
Goals

- Improve the citizen user experience across all Commonwealth public-facing websites
- Establish or clarify cybersecurity requirements for protecting state websites and public access
- Brand Virginia state websites for a world-class look and feel that is easily recognizable, with common design elements and the use of standard naming, such as .gov addresses
- Improve access to information and services on state government websites by providing language options and accessibility support
- Consolidate website footprint and retire underused old websites
- Train executive branch agencies how to create and maintain modern websites and provide all necessary knowledge resources, including templates, checklists, on-site demos, tools, and scans

WEBSITE MODERNIZATION PROGRAM OPERATIONAL SETUP

Program Oversight: Accenture as our Partner

- VITA Program Manager, Joshua Jones
- Accenture Project Manager, Accessibility, Security and UX Experts
- Four main website focus items:
  - ➢ Manage Website Inventory, Scans, & Monthly Remediation
  - ➢ Identify, Estimate & Track Prioritized List Of Websites That Need Wholesale Remediation
  - ➢ Manage Remediation Efforts With eGov Vendors & Cloud Based CMS Vendors. Capture Need & Costs.
  - ➢ Train Agencies On Updated Enterprise Standards For Websites
- Other Key Activities
  - ➢ Monthly Status Meetings With Agencies; Individual And Group
  - ➢ In Depth Analysis With Agencies Of The State Of Their Websites; Strategy for modernization.
  - ➢ Branding Bar & Website Template Rollout
- Oversee Quarterly Scanning
  - ➢ CSRM for Security
  - ➢ Accenture for 508/Accessibility Compliance
  - ➢ VITA Web Team for Banner Compliance



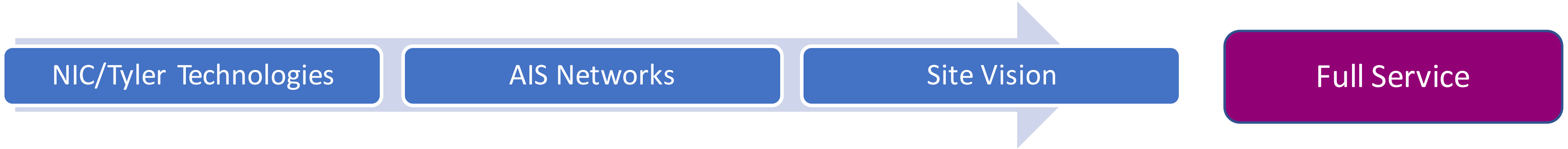
Verified Inventory & Go Live Approval
Prioritized Website Redesign Planning & Remediation
Website Modernization Ongoing
Quarterly Security & Accessibility Scans & Remediation
Modern Templates & Branding Bar

WEBSITE MODERNIZATION PROGRAM OPERATIONAL SETUP: MODERNIZATION & REMEDIATION OPTIONS

Modernization Program Office will work with seven suppliers to help agencies modernize their websites.

Leveraging existing website support ecosystems including offering each of the suppliers the new branding bar as well as the Virginia.gov website template:

1. Three eGov Website Vendors Offering Turnkey Website Design, Support, and Hosting. CMS Optional. ***Work already begun on fixes***.



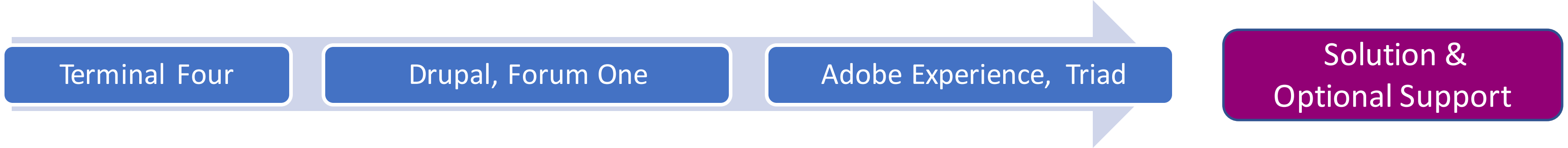
NIC/Tyler Technologies

AIS Networks

Site Vision

Full Service

2. Three Website Content Management Systems, Hosted in AWS, (T4, Drupal, and Adobe) With Optional Professional Services * New, March 2022.



Terminal Four

Drupal, Forum One

Adobe Experience, Triad

Solution & Optional Support

3. Computer Aid Associates: Offering SOW operational support or individual specialty staff.

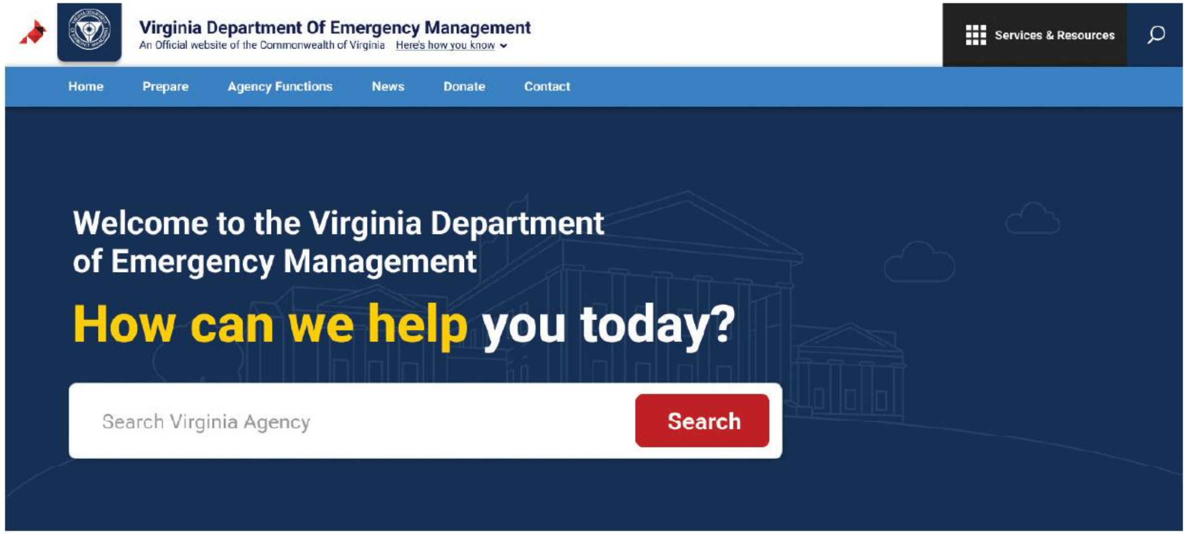
   Adding overall remediation SOW with multiple vendors to help with the effort.

Staff Only

WEBSITE MODERNIZATION PROGRAM OPERATIONAL SETUP

Concierge Web Modernization Service

- New eGov Manager to work with agencies on best fit solution and remediation for their websites. Guided process to help with the vendors.
- Industry standard process to implement modern websites with focus groups, useability (UX), security, accessibility, and information architecture designs.
- Free, secure, accessible and modern website template to be used by any of the vendors.
- Template below is a sample mockup. Colors are not final. Key components were state logo, agency logo, square services, main agency search and enterprise search.



Welcome to the Virginia Department of Emergency Management

How can we help you today?

CURRENT STATUS

Completed Efforts

- Initial assessment of all agency websites for security, accessibility, and design issues
- Security scan results shared with agencies for remediation
- Draft Web Standards completed and posted to ORCA for public review and comment
- Draft branding bar, color palette and website template prototype completed and approved
- Accenture on-boarded to provide program support
- 10 agencies identified for pilot program, with additional 10 agencies prioritized for remediation

In Progress

- Prioritized list of all remaining agencies being finalized
- Executive Order to require agency website modernization under review
- VITA Website Modernization Concierge Service being created
- Contract negotiation for expanded use of Security, Accessibility and Design scanning tools in progress
- Governance framework, compliance checklist and training materials being developed

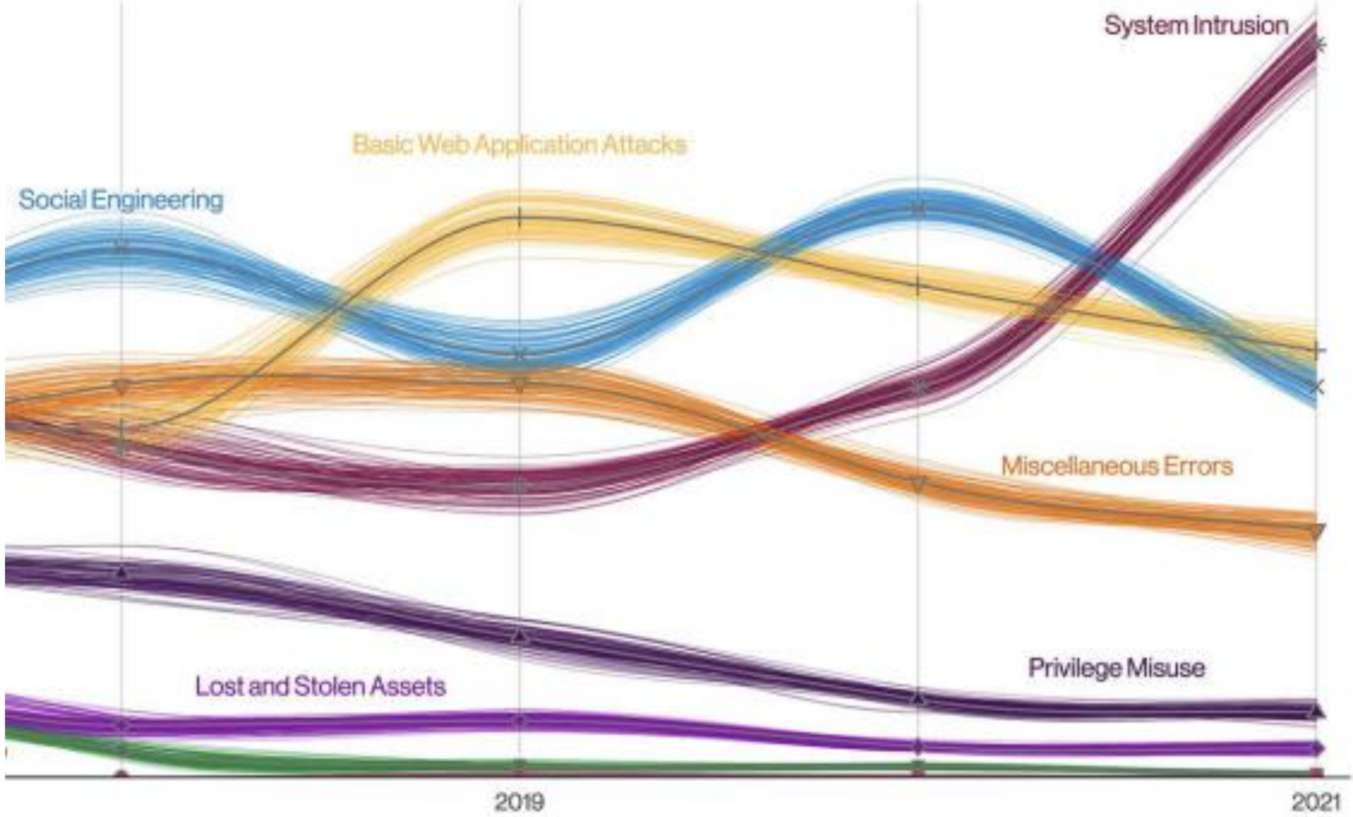
Security Heroes

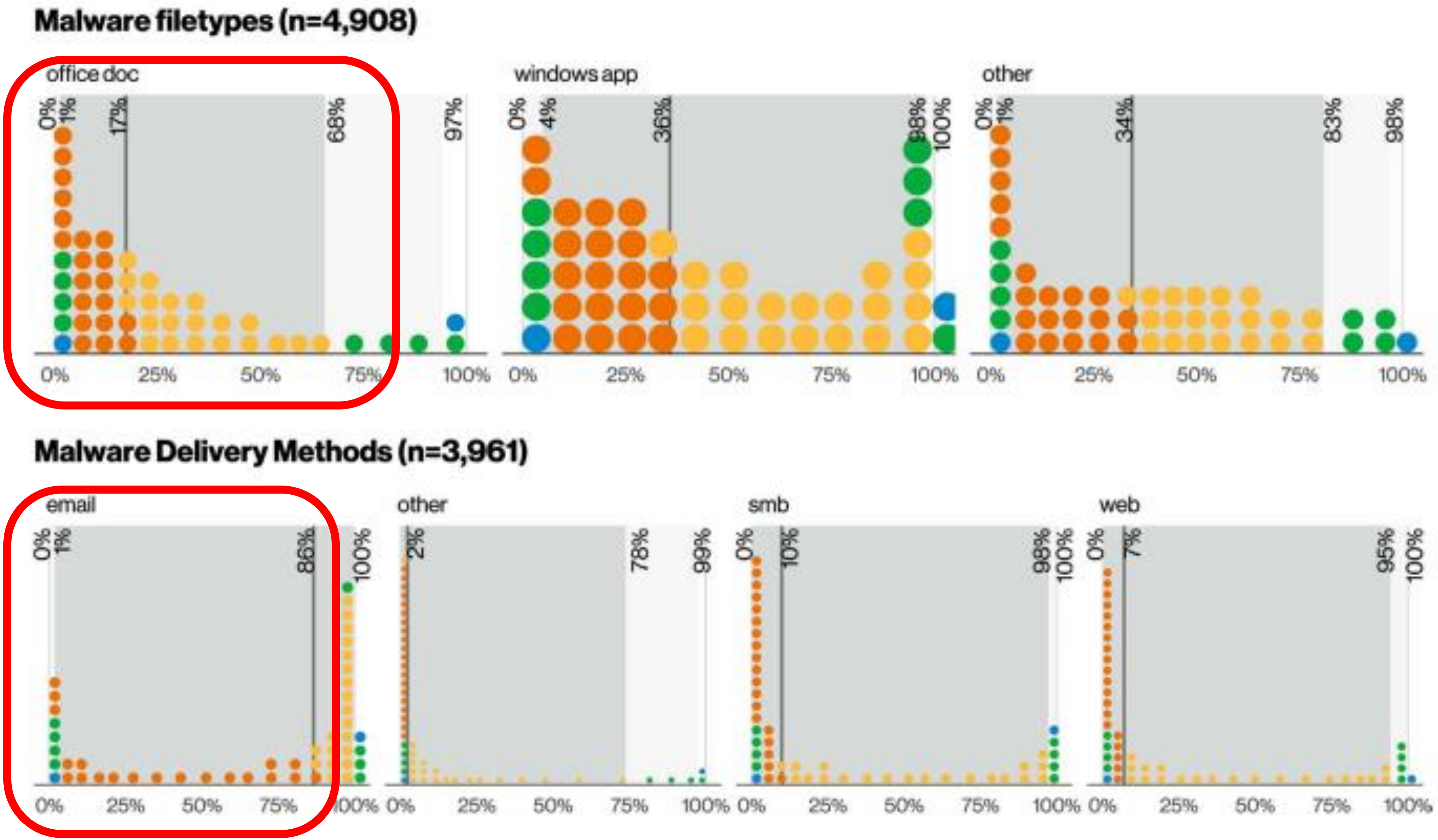
Empowering employees in cyber defense

Dan Han
Virginia Commonwealth Unviersity

DBIR on breaches

- The **<u>human element continues to be a key driver of 82% of breaches</u>** and this pattern captures a large percentage of those breaches. Additionally, **malware** and **stolen credentials** provide a great second step after a social attack gets the actor in the door, which emphasizes the importance of having a strong security awareness program



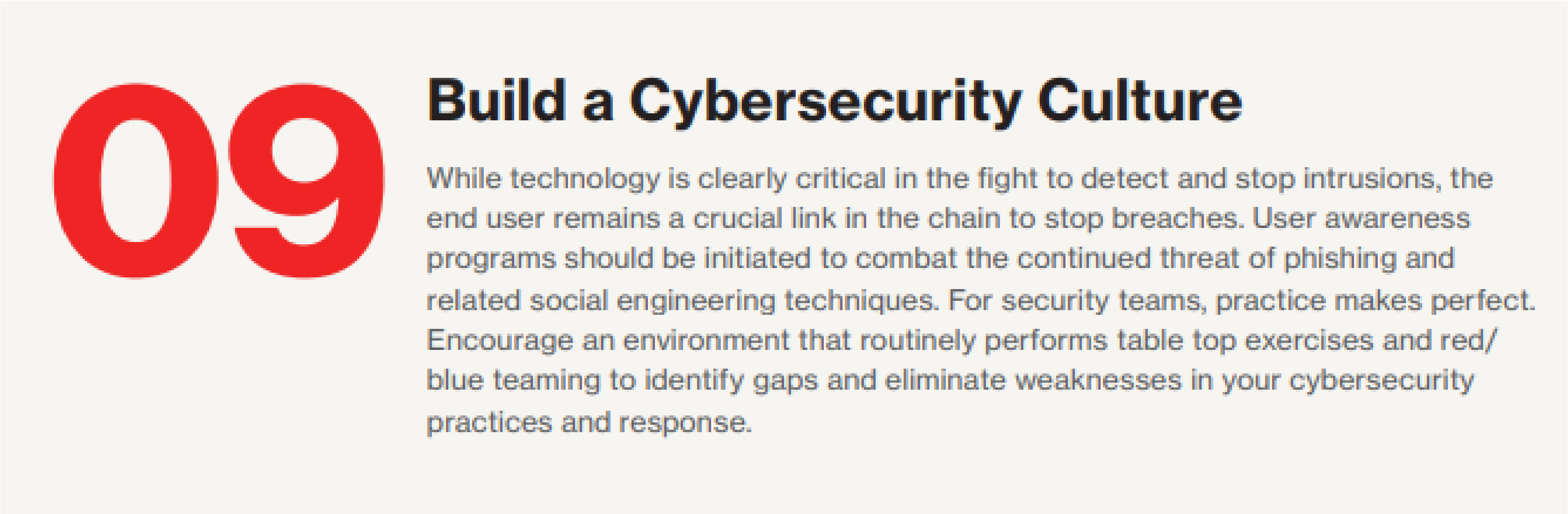


Malware filetypes (n=4,908)

Malware Delivery Methods (n=3,961)

Figure 37. Malware delivery method proportion per organization

CrowdStrike on Security Culture



09

Build a Cybersecurity Culture

While technology is clearly critical in the fight to detect and stop intrusions, the end user remains a crucial link in the chain to stop breaches. User awareness programs should be initiated to combat the continued threat of phishing and related social engineering techniques. For security teams, practice makes perfect. Encourage an environment that routinely performs table top exercises and red/ blue teaming to identify gaps and eliminate weaknesses in your cybersecurity practices and response.

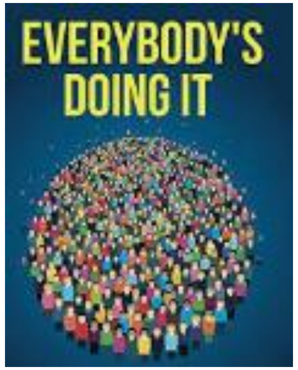
The threats against an organization

- Phishing and social engineering is still very much at the core of many security incidents and data breaches

What have we done?

- Training and Education?
- Multi-Factor Authentication?
- Monitoring and Response?

But why are we doing these things?



From a pure defense perspective

- **Increase our resiliency against threats?**
- **Decrease the dwell time of existing threats?**
- Ideally **<u>Time needed for compromise > Dwell time</u>**

- **We will focus on the reduction of dwell time today…**

From a threat perspective

- Dwell Time is the amount of time a threat exists in your environment.

  Dwell Time = <u>Time until discovery</u> + <u>Time until completion of response</u>

Therefore…

- To reduce dwell time, we have a couple of options:
  - **Reduce the time of discovery**
  - **Reduce the time of completion of your response**

Time of discovery

- Time until discovery is closely related to the probability of discovery.
  - *If a threat is present for an infinite amount of time, then eventually it will be discovered… As the probability of discovery is unlikely **zero***
  - The attacker's goal is to **increase the time a threat can be present** so the attacker can complete its operations.
  - The defender's goal is to **increase the time it will take for attackers to achieve their goal while decreasing the time a threat can be present**.

- An overly simplified equation for time until discovery:
  - **Time until discovery = 1 / Probability of discovery (%)**

From a threat perspective

- Probability of discovery has a proportional relationship to your monitoring capabilities and the impact caused by the adversaries

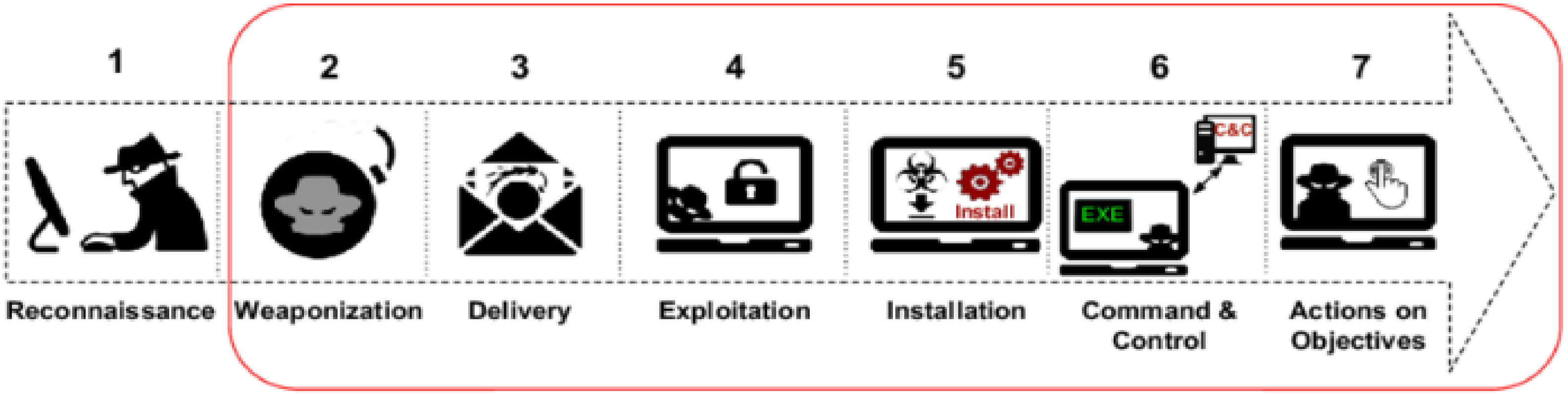
  Probability of discovery = Efficacy of monitoring x Impact of threat

Probability of discovery

- **The two factors:**
  - **Impact of Threat** – This is mostly controlled by the attacker…
  - **Efficacy of Monitoring –** This is controlled by the defender and is largely related to monitoring capabilities.
  - Detection likelihood increases when:
    - Impact of threat increases
    - Detection efficacy increases

- **Monitoring capabilities = non-human reporting + human reporting**
  - Efficacy of non-human reporting is largely related to the position and efficacy of sensors you put in place
  - Probability of human reporting is related to **the knowledge, ability, and will of the human**.

Shifting left with the kill chain…



- Just like with other things in IT, the earlier we can detect issues, the cheaper it is for us to recover and remediate
- The first three phases of the kill chain are Recon, Weaponization, and Delivery
- **From a defender’s view point, we won’t know of a definitive threat until delivery…**

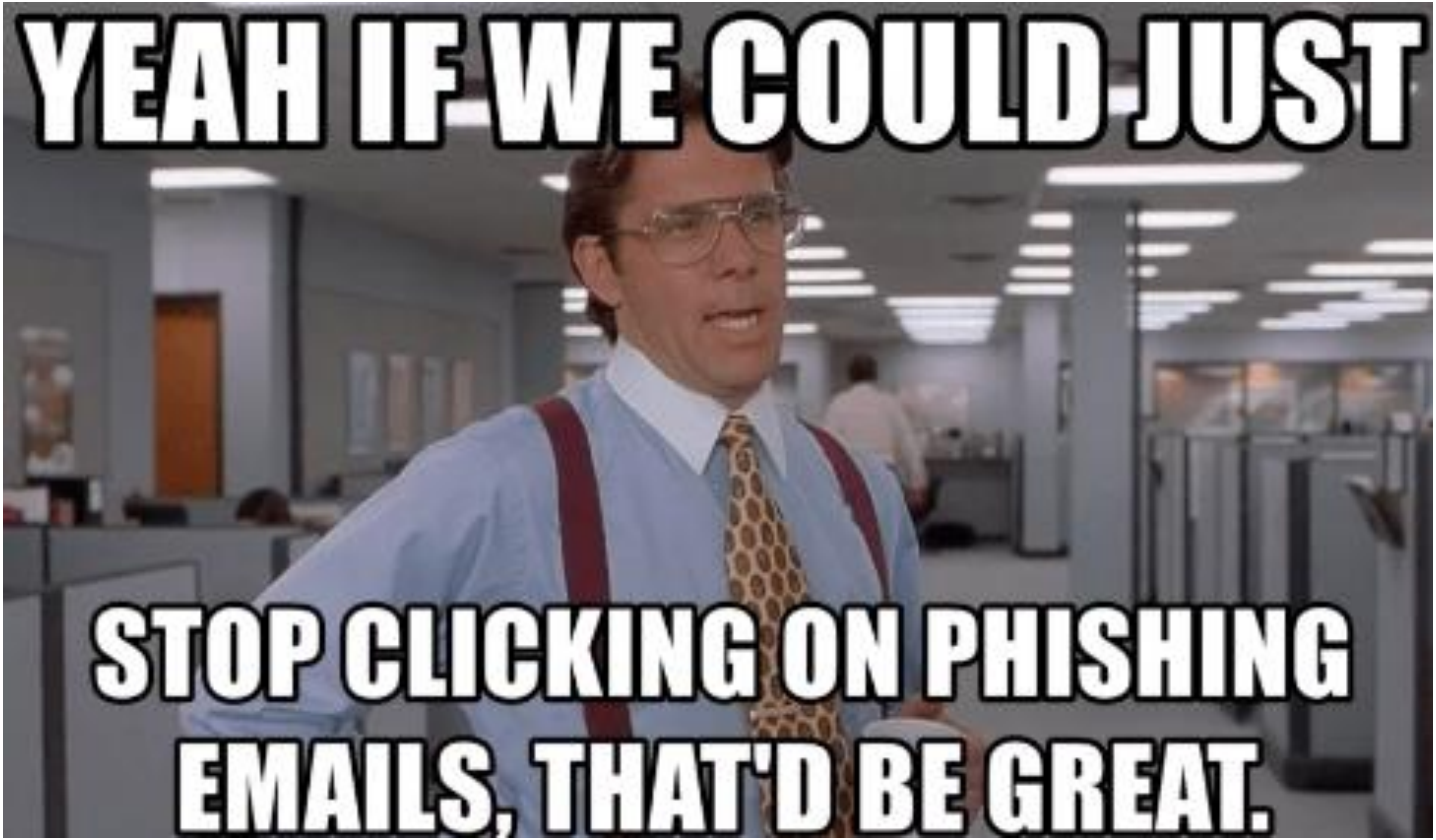
With social engineering attacks…

- Ideally, the attacker should achieve the following:
    - Have at least one of the targets perform the attacker’s desired action
        - Enticement of the lure
        - Vulnerability of the target
    - Trigger no detection, whether through technology or human reporting
        - The size of the target population
        - The obfuscation quality of the attack
- Ideally, for the defender:
    - Detect the threat through at least one form of control, whether technology or human reporting.
    - Have no targets fall for the attempt

From a technical controls perspective

- Mail gateways
- Anti-spam/anti-malware tools
- Threat detection tools such as EDR/NDR/XDR
- Multi-factor authentication
- Sure, all of these things are effective in their own means… but

But is that enough?


YEAH IF WE COULD JUST
STOP CLICKING ON PHISHING EMAILS, THAT'D BE GREAT.

Empowering employees in cyber defense

- Since Phishing is still one of the primary methods for attackers to launch their campaign…
- The target of phishing are humans
- Dwell time can be reduced when:
  - Rapid detection and response is achieved at this stage.
  - Enhanced resiliency at this stage
- **<u>Ultimately, the humans are both the initial targets and the greatest IDS/IPS with the highest fidelity data</u>**

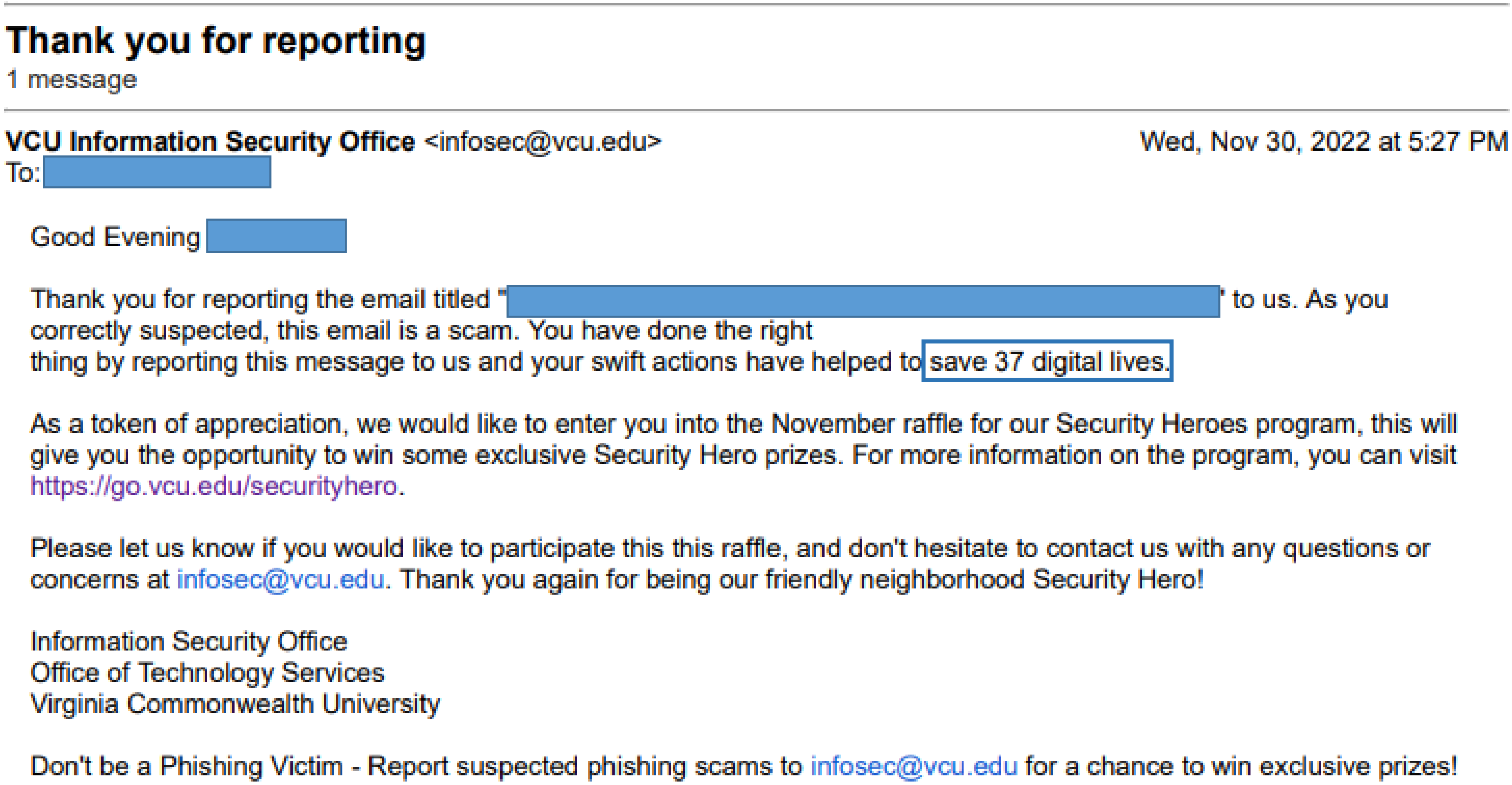
The social experiment

- Hypothesis
  - Positive reinforcement for threat reporting can decrease the mean time to report and increase the likelihood of reporting among employees
- Method
  - Establish a series of positive reinforcements for reporting of security threats
  - Measure the longitudinal impact of positive reinforcements on user behavior

The Security Heroes Project

- https://go.vcu.edu/securityhero
- Rewards program for phishing reporting
  - All reporters receive thank you email with the number of “**digital lives**” they saved.
  - All reporters are offered to participate in a monthly raffle for exclusive prizes
  - All consented winners are offered a spotlight on our website for public recognition.

The email



Thank you for reporting
1 message

VCU Information Security Office <infosec@vcu.edu> Wed, Nov 30, 2022 at 5:27 PM
To: [redacted]

Good Evening [redacted]

Thank you for reporting the email titled "[redacted]" to us. As you correctly suspected, this email is a scam. You have done the right thing by reporting this message to us and your swift actions have helped to save 37 digital lives.

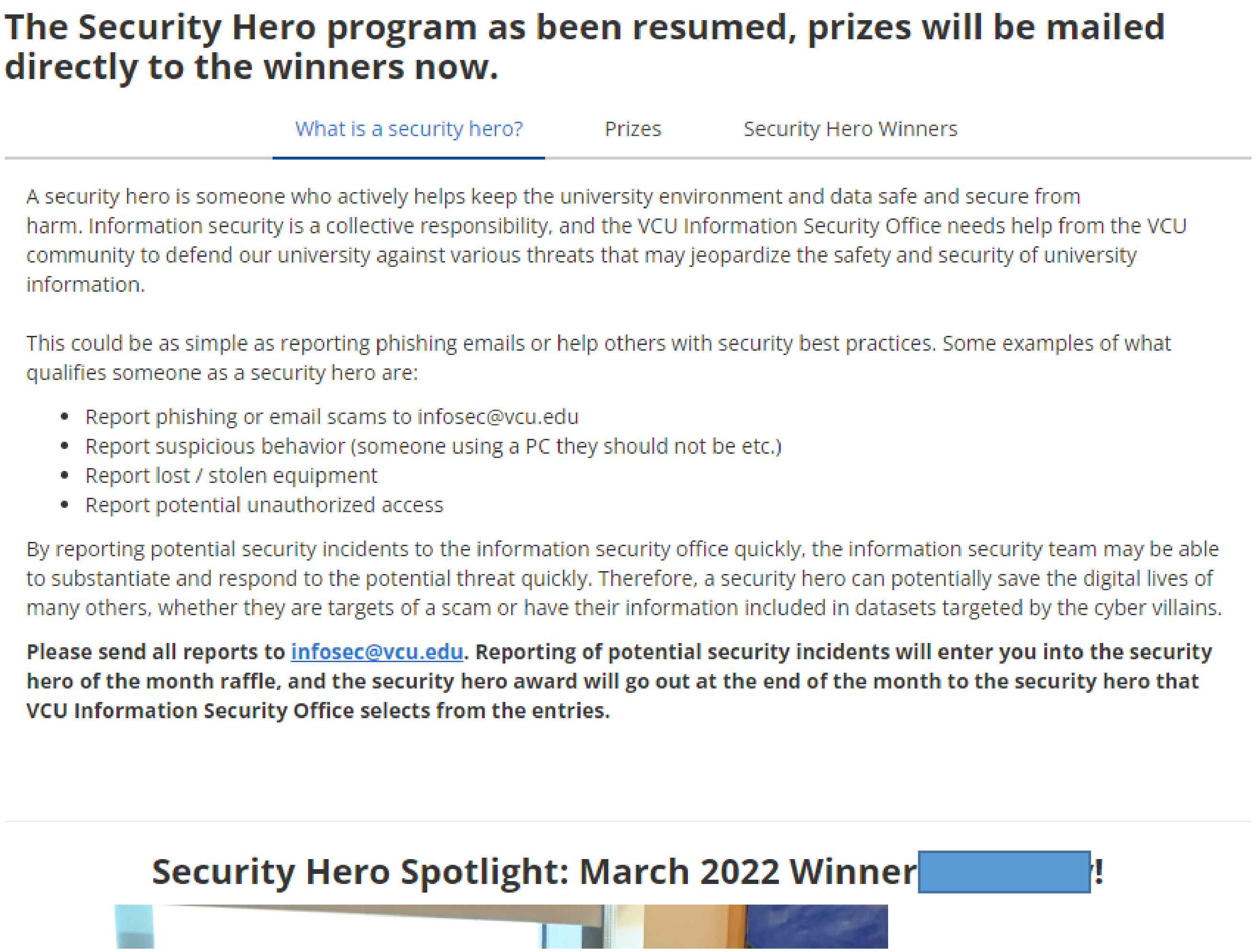
As a token of appreciation, we would like to enter you into the November raffle for our Security Heroes program, this will give you the opportunity to win some exclusive Security Hero prizes. For more information on the program, you can visit https://go.vcu.edu/securityhero.

Please let us know if you would like to participate this this raffle, and don't hesitate to contact us with any questions or concerns at infosec@vcu.edu. Thank you again for being our friendly neighborhood Security Hero!

Information Security Office
Office of Technology Services
Virginia Commonwealth University

Don't be a Phishing Victim - Report suspected phishing scams to infosec@vcu.edu for a chance to win exclusive prizes!

The website



The Security Hero program as been resumed, prizes will be mailed directly to the winners now.

A security hero is someone who actively helps keep the university environment and data safe and secure from harm. Information security is a collective responsibility, and the VCU Information Security Office needs help from the VCU community to defend our university against various threats that may jeopardize the safety and security of university information.

This could be as simple as reporting phishing emails or help others with security best practices. Some examples of what qualifies someone as a security hero are:

- Report phishing or email scams to infosec@vcu.edu
- Report suspicious behavior (someone using a PC they should not be etc.)
- Report lost / stolen equipment
- Report potential unauthorized access

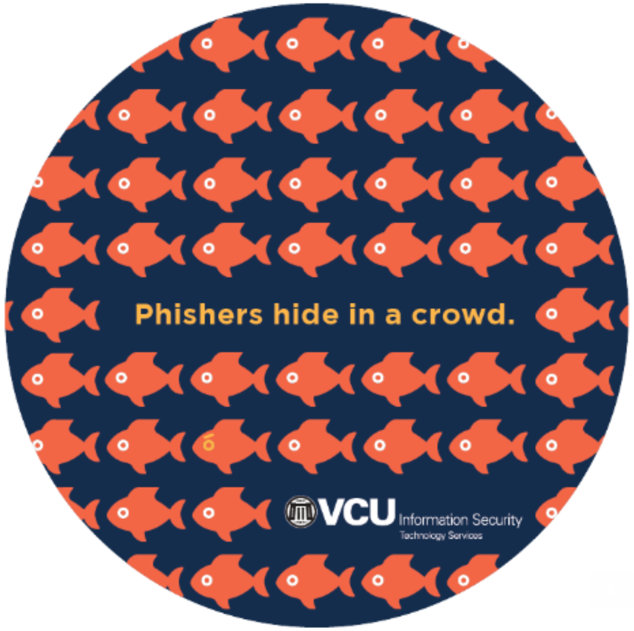
By reporting potential security incidents to the information security office quickly, the information security team may be able to substantiate and respond to the potential threat quickly. Therefore, a security hero can potentially save the digital lives of many others, whether they are targets of a scam or have their information included in datasets targeted by the cyber villains.

Please send all reports to infosec@vcu.edu. Reporting of potential security incidents will enter you into the security hero of the month raffle, and the security hero award will go out at the end of the month to the security hero that VCU Information Security Office selects from the entries.

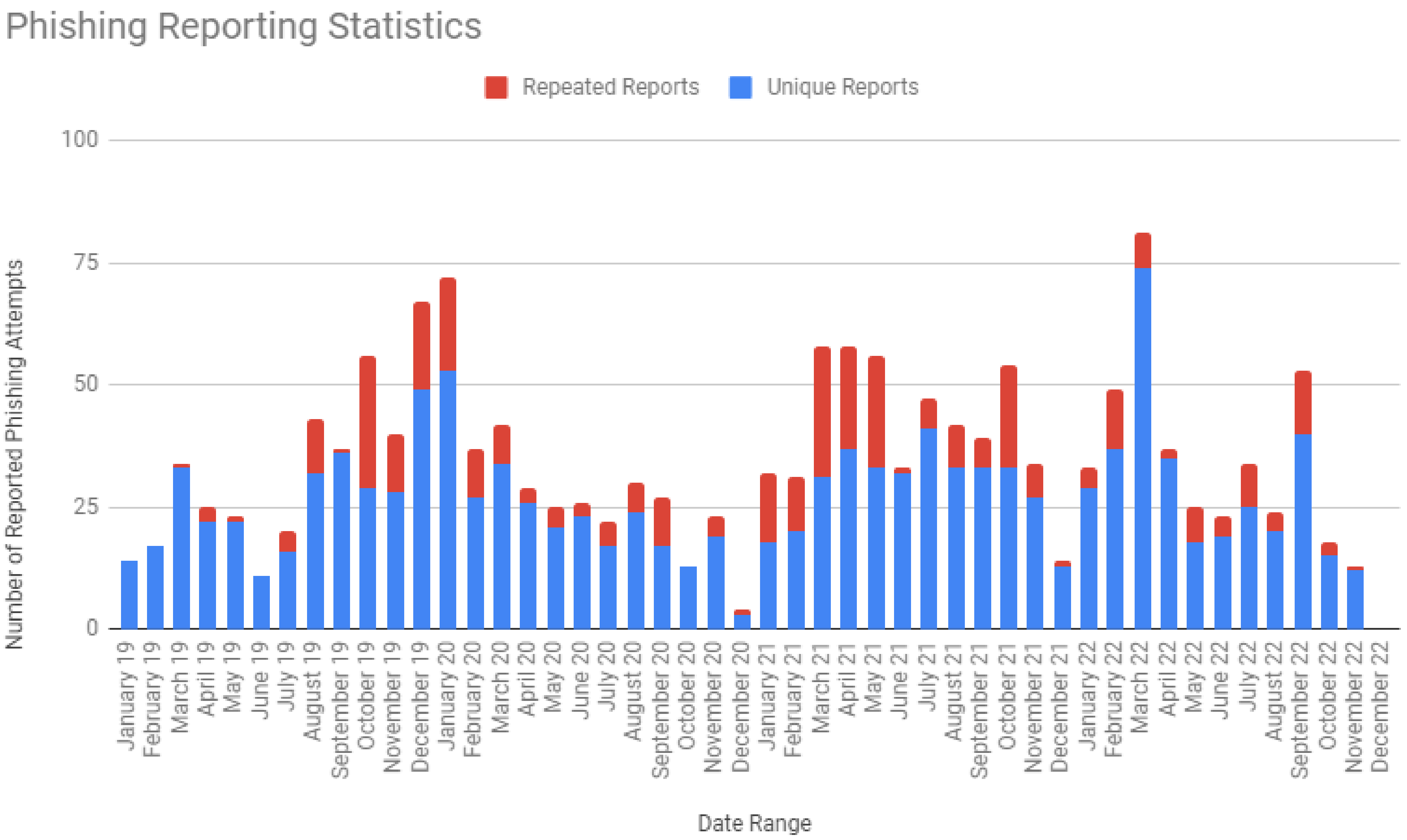
Security Hero Spotlight: March 2022 Winner [redacted]!

Program details

- Concept started in November of 2018
- Program launch and data tracking started in January 2019
- Continued until late 2020, due to staffing changes and pandemic, prize distribution paused
- Resumed in late 2021
- **Total of 1,635 threats reported, 1,271 unique (77.7%)**
- Tracked the following information:
  - Time of entry for the threat
  - Time of reporting for the threat
  - Time of response for the threat

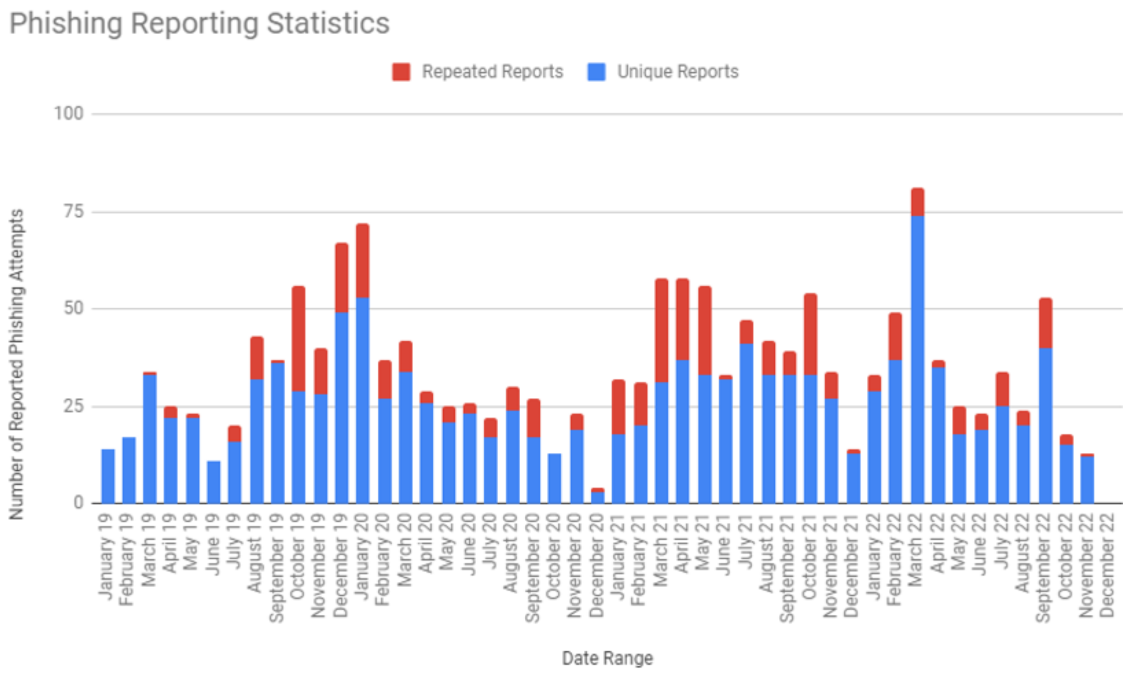


Number of reports

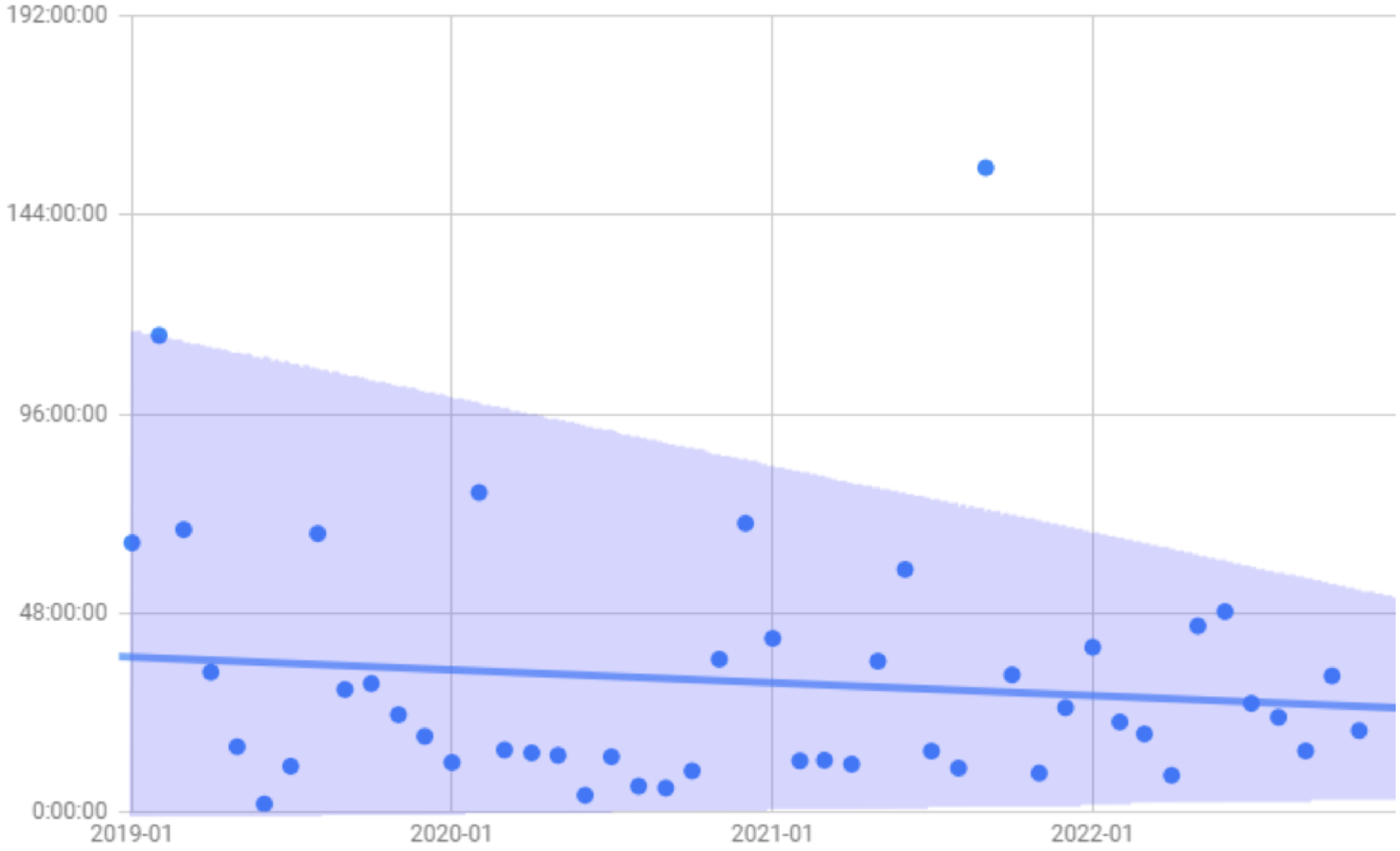


Number of reports - Takeaways

- No major increase or decrease in reporting
- Program ramp up may have led to some additional repeated reporting
- Participants at one point started to report emails in their spam box and their personal emails to increase their chances at winning

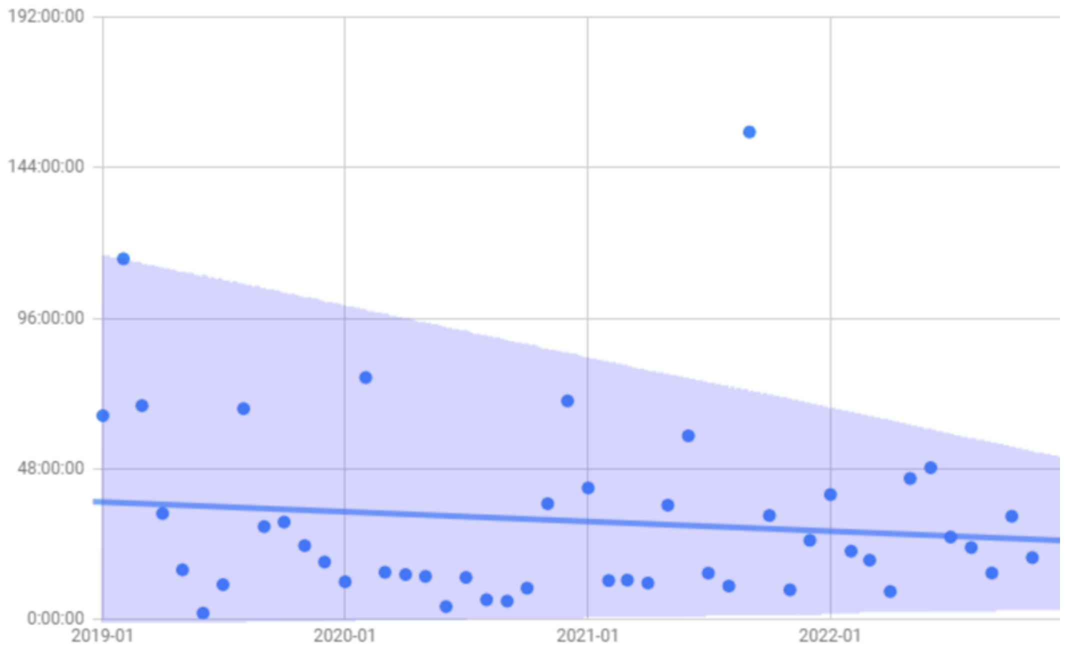


Monthly mean time to report

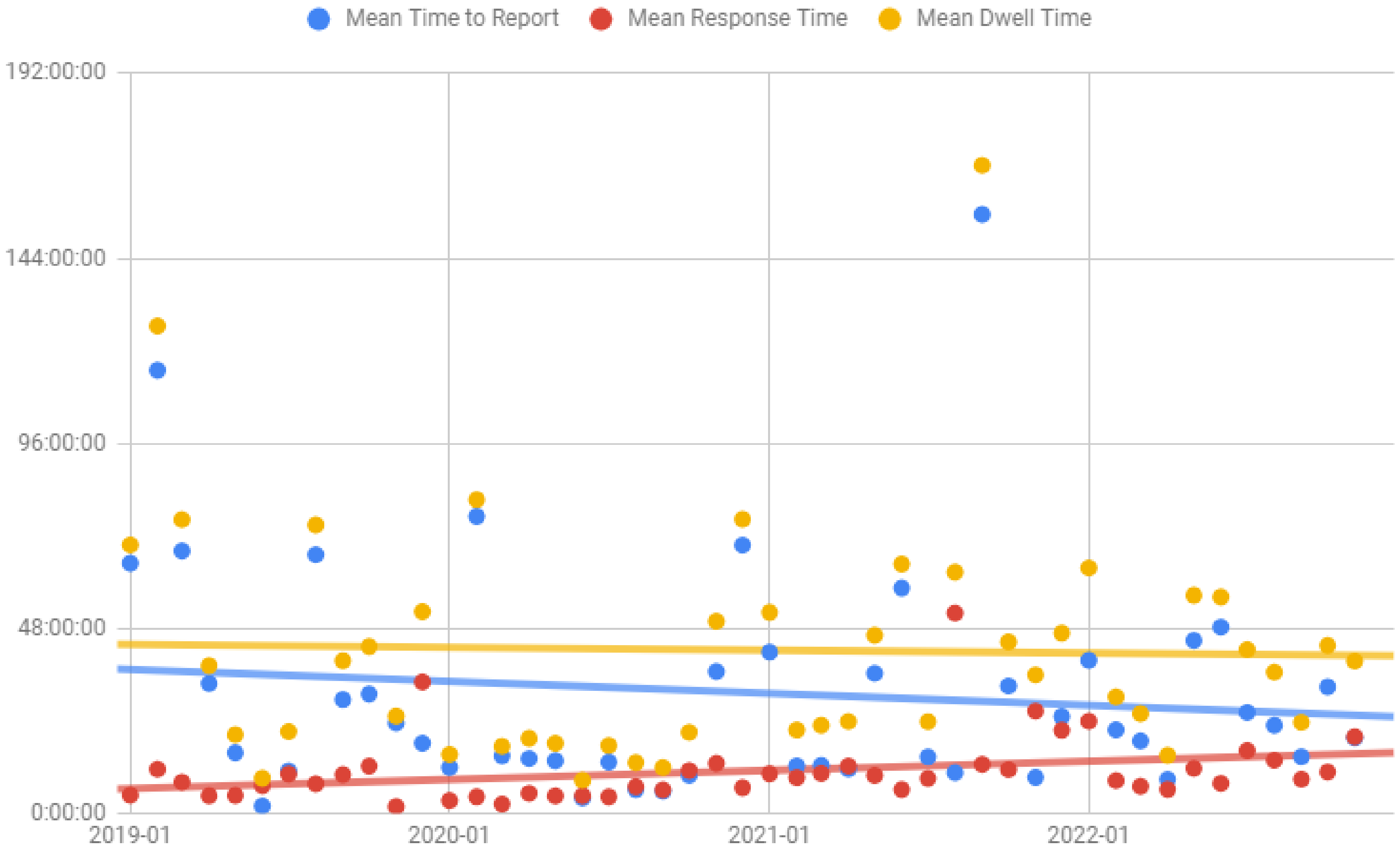


Monthly mean time to report – Takeaways

- Gradual decrease in monthly mean time to report. Trend started around **36 hours** for mean time to report, the time is reduced to less than **24 hours**
- Better clustering of individual and mean report times
- More predictability for half of the dwell time equation

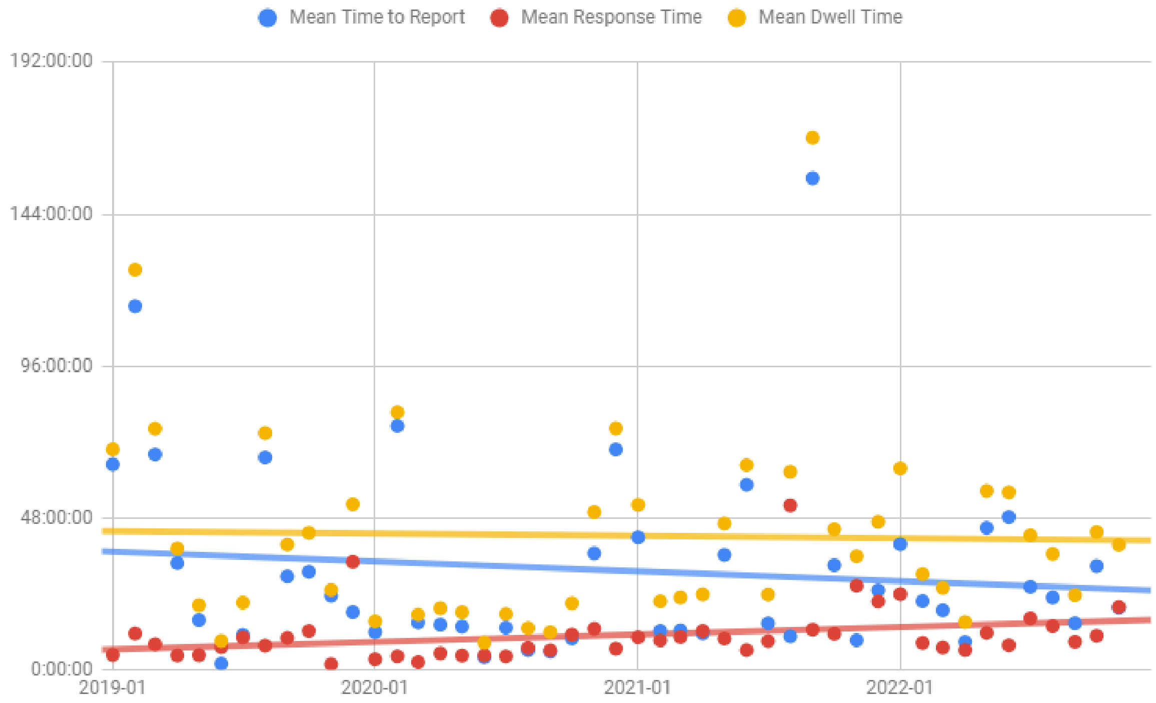


Measurement of mean dwell time



Mean dwell time - Takeaways

- More consistent average dwell time
- Increasing average response time (due to staffing changes)



Analysis of median values

ASSURA™

Cybersecurity uncompromised.

Improving Your Business Impact Analysis

How to Use BIA Data to Understand and Meet your Agency’s Needs

Assura and My Background

- Information Security and Risk Management Firm headquartered in Richmond, VA
- Assist organizations in development and management of their information security programs
- Technical Director of Governance, Risk, and Compliance at Assura
- Manage our team of Virtual ISOs in assisting public and private organizations

ASSURA™

Cybersecurity uncompromised.

Agenda

- What is a Business Impact Analysis (BIA) and why is it important?
- What are the problems I’m seeing out in the wild around BIAs?
- How can we remediate these problems?
- If you can have one takeaway from today’s talk, what is it?

What is a BIA and Why is it Important?

- An overview of all an organization's business functions
- Impact back to the organization if these functions are unavailable
- Recovery Time Objective (RTO) / Recovery Point Objective
- List of organization systems that support those functions
- Acts as the data of record for IT Disaster Recovery and Continuity Plans
- Informs Data Classifications and Risk Assessments

The Problems I See in the Wild

- BIAs that are only Technical Recovery Analysis
- BIAs that aren’t fresh
- BIAs that can’t communicate their data effectively to executives

BIA vs Technology Recovery Analysis

On paper, there are a lot of similarities

- Core functions listed
- Functions tied to supporting systems
- RTOs and RPOs

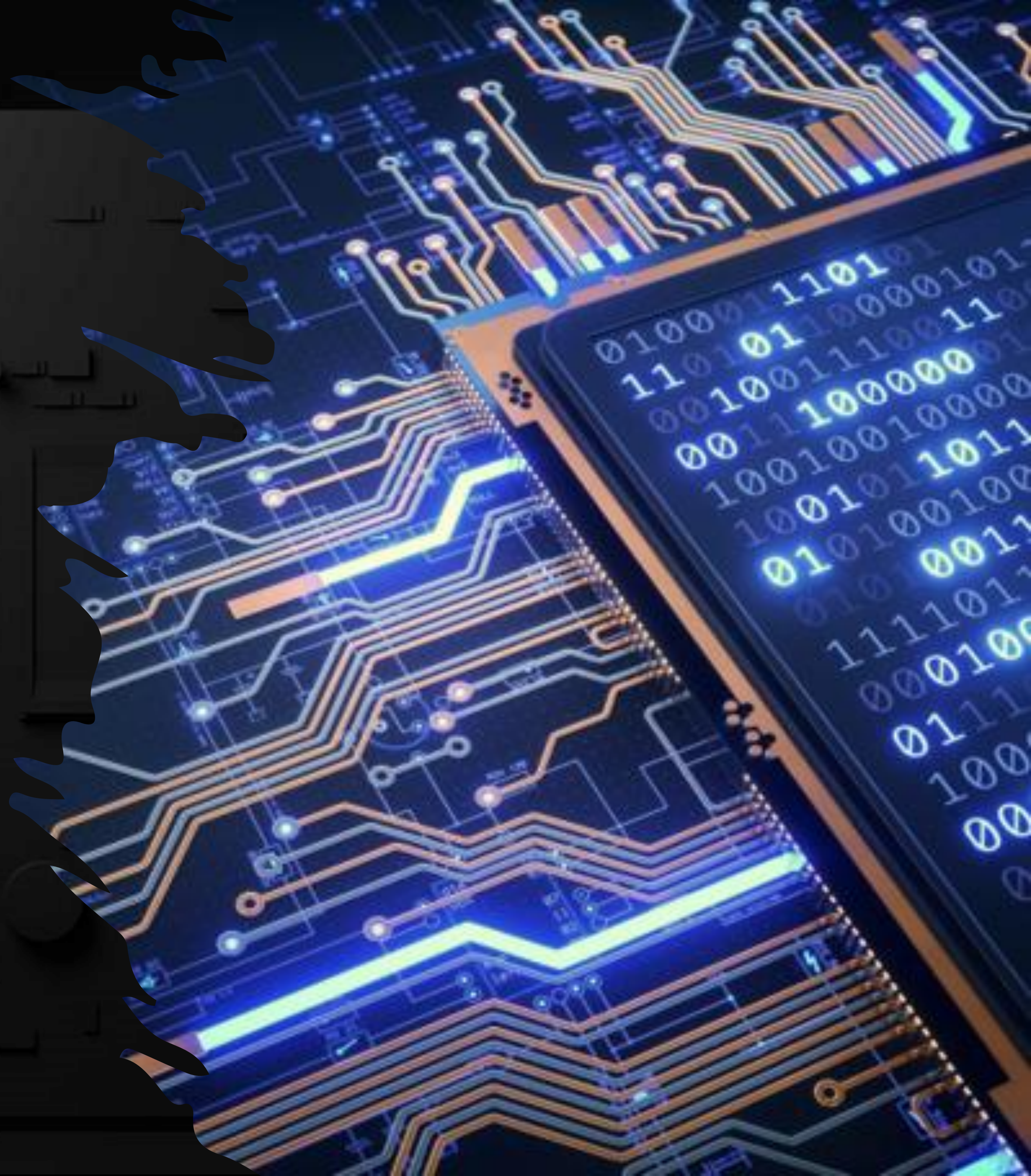
In practice, we run into issues

- IT Recovery Checklist is owned by IT, not the business owners
- Blinders to business needs outside of IT requirements
- May inform the IT DR plan, but falls short of supporting full Continuity Plans

How do we Fix it?

Ask around needs for full organizational continuity

- What vendors do you rely on?
  - Do we have an agency contact with their information in the event of an emergency?
- Who are you dependent on internally? Who is dependent on you internally?
- How are records managed?
- Peak Time sensitivity?
- What are your equipment needs?



Remember:
BIA→ IT DR→ Continuity Plan

- Common audit finding
- There must be alignment from the BIA data with IT DR and IT DR with Continuity Plan
- Collect Continuity Data during the BIA
- Having the source of data start at the BIA avoids older plans corrupting current data

Business Processes are Constantly Evolving

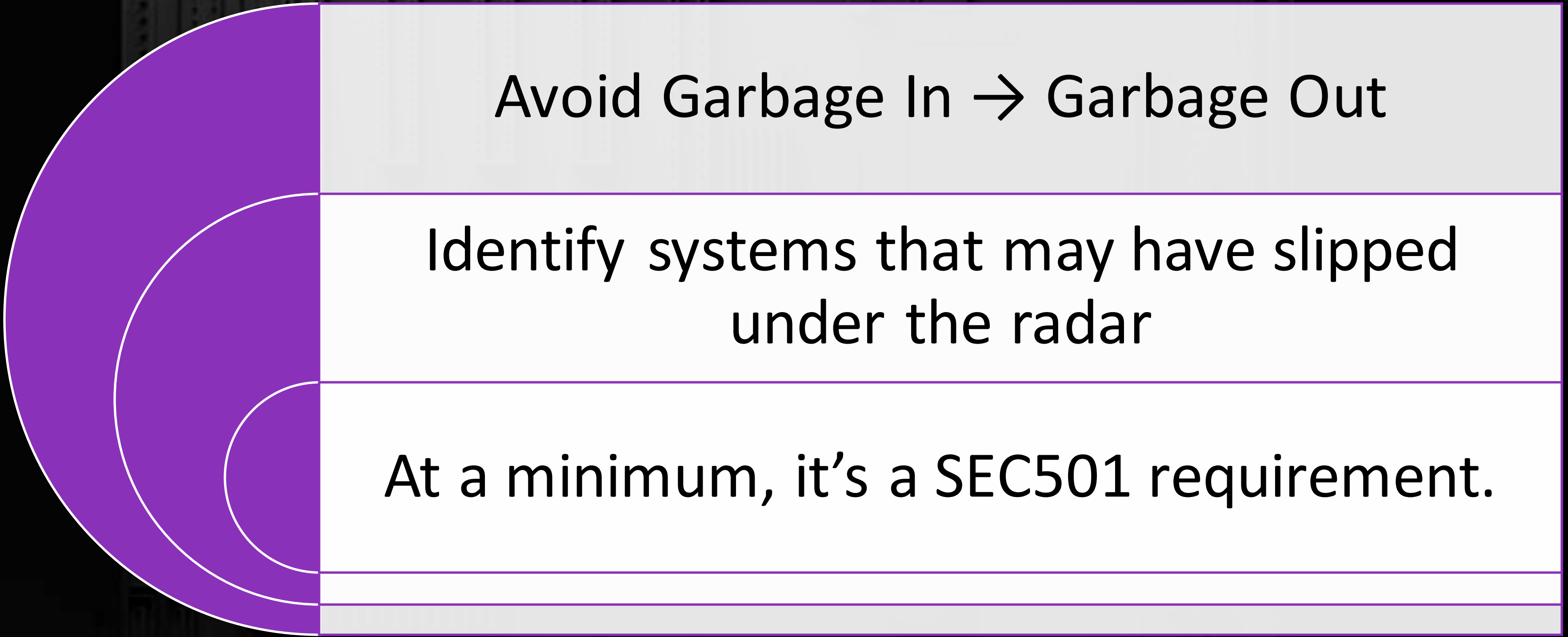
- How we work has shifted dramatically in the last 5-15 years
- That rate of change is accelerating
- New systems/applications improve efficiency and change underlying processes
- New business needs drive changes for everyone

Problem: Out of Date BIAs

Tons of changes, but these aren’t captured in the BIA

- “I can’t capture that change; we don’t have a column for that”
- “This process is a high impact because it was labeled that when I started in 2014”
- “I updated the BIA. John retired, and I put Patty as the owner of all his processes”

Full BIA Every Three Years



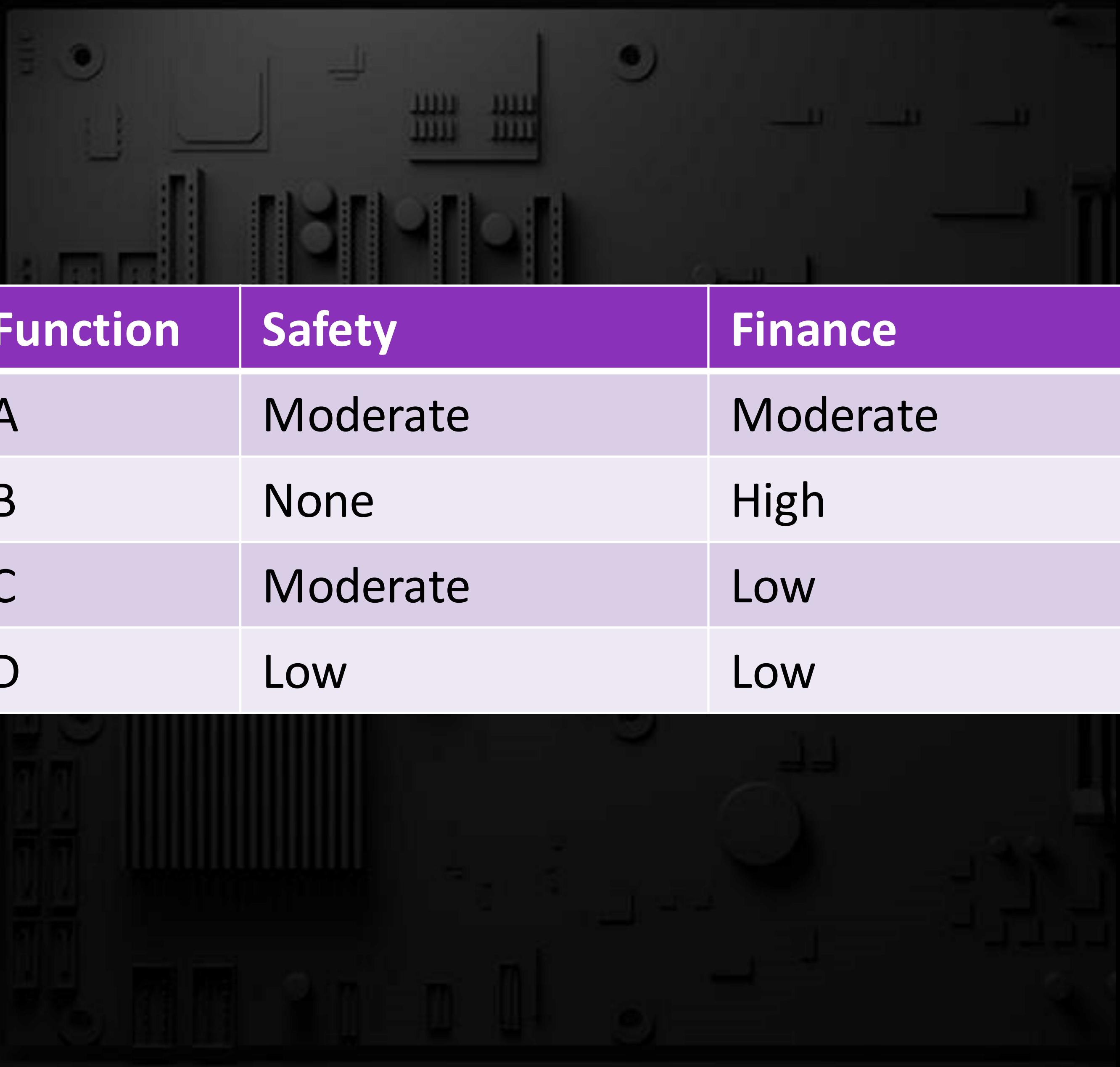
Avoid Garbage In → Garbage Out

Identify systems that may have slipped under the radar

At a minimum, it’s a SEC501 requirement.

Executive Communication

- We’ve discussed expanding the data we’re collecting and keeping it current.
- Now how do we communicate that data effectively to key parties?
- BIAs need to be reviewed by the Agency Head
- How is that data currently presented?
  - In a list?
  - Sorted by RTO or by Mission Essential Status?
  - GRC tool?



Business Function	Safety	Finance	Legality
Function A	Moderate	Moderate	Moderate
Function B	None	High	High
Function C	Moderate	Low	Moderate
Function D	Low	Low	Moderate

Problems With Listing

- Difficult to parse
- How, if at all, is function A more important than function B?
- Who makes that decision and why?
- Impact Statement can add context
- Assist Agency Head in making risk decisions

Business Function	Safety	Finance	Legality	Impact Statement
Function A	Moderate	Moderate	Moderate	Function A would have moderate financial and legal impacts for the agency, alongside introducing general safety risk for our users who rely on the availability of the Function.
Function B	None	High	High	Function B is vital to the agency performing its assigned mission, with heavy financial and legal impacts if services become unavailable.

Closing Tip

- Do the BIA data collection through interview, not an emailed questionnaire
- You know the expected results and can provide context through conversation
- You'll end up saving more time from not having to go back and correct data input errors

Conclusion

- The Business Impact Analysis is the data of record for all business recovery and information security program documentation.
- Expanding data collected, keeping that data fresh, and communicating it effectively will increase the data's effectiveness for your agency.

Contact Information
Bryan Carnahan
bryan.carnahan@assurainc.com
804-767-5040
LinkedIn

ASSURA™
Cybersecurity uncompromised.

VIRGINIA IT AGENCY

ALGOSEC FIREWALL ANALYZER

- Bill Stewart – VITA MSS service owner
- Darrell Raymond – Client delivery executive
- Kevin McLees – Business relationship manager
- Rob Sullivan – Project manager
- Scott Guthrow – Technical lead

DECEMBER 2022

ALGOSEC FIREWALL ANALYZER FUNCTIONALITY

AlgoSec firewall analyzer has been deployed in the VITA environment to provide the ability to view, analyze and report on firewall policies. This functionality is being made available to agency information security officers (ISOs) that have their own dedicated virtual system (VSys) on the internet facing firewalls (not currently configured on agency specific remote firewalls).

Among the capabilities that will be enabled for agency users are:

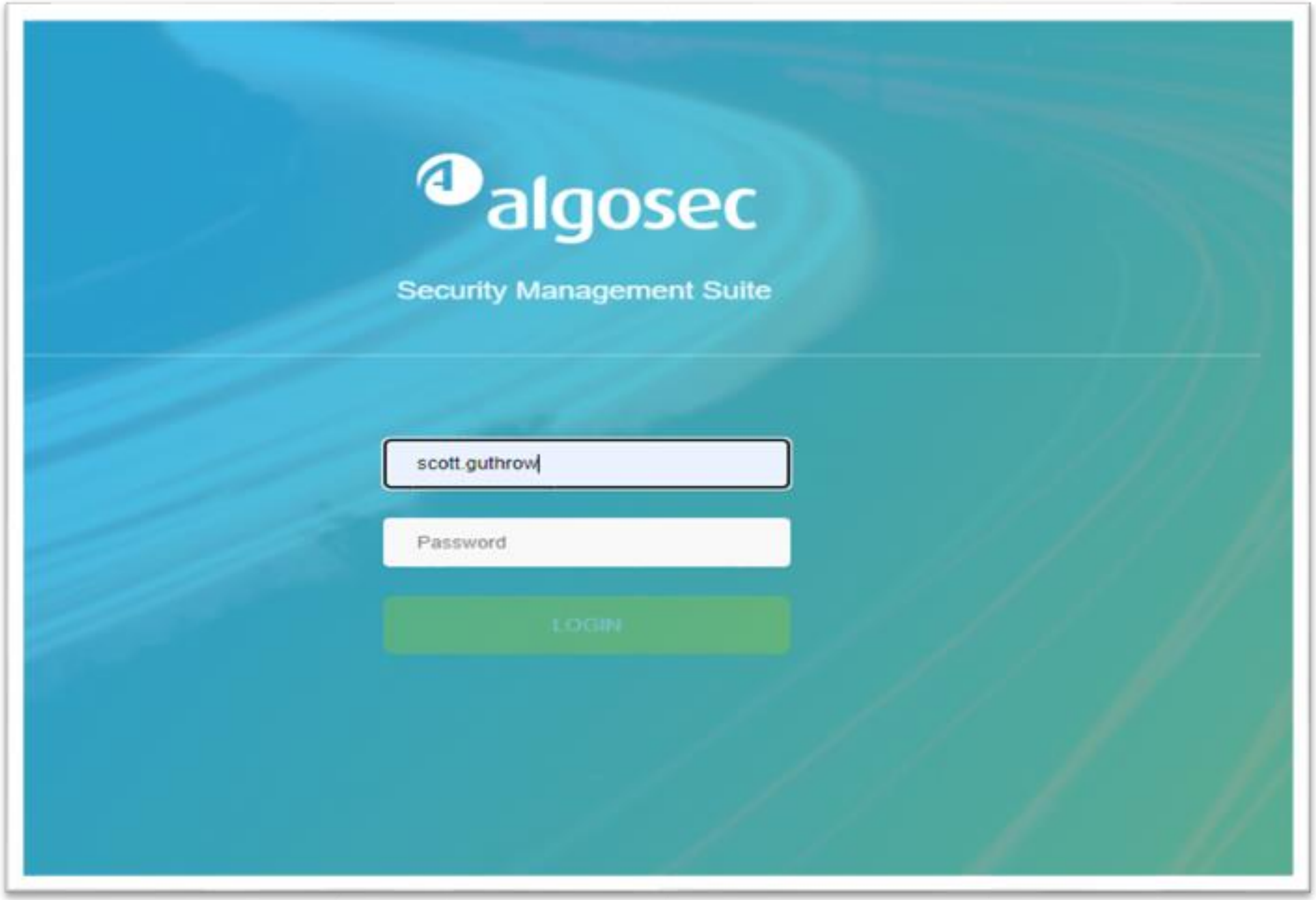
- View agency-specific firewall policies
- Simulate traffic
- Determine if existing policy supports proposed traffic
- Determine if a policy has been implemented
- Review optimization options

ACCESS TO ALGOSEC

- From the COV network, access AlgoSec: https://qts-algo-mgmt-01.cov.virginia.gov
- Username: first.last

  AlgoSec access is via two-factor authentication; your RSA Id will be your AlgoSec username.
- Password: 2-Factor authorization

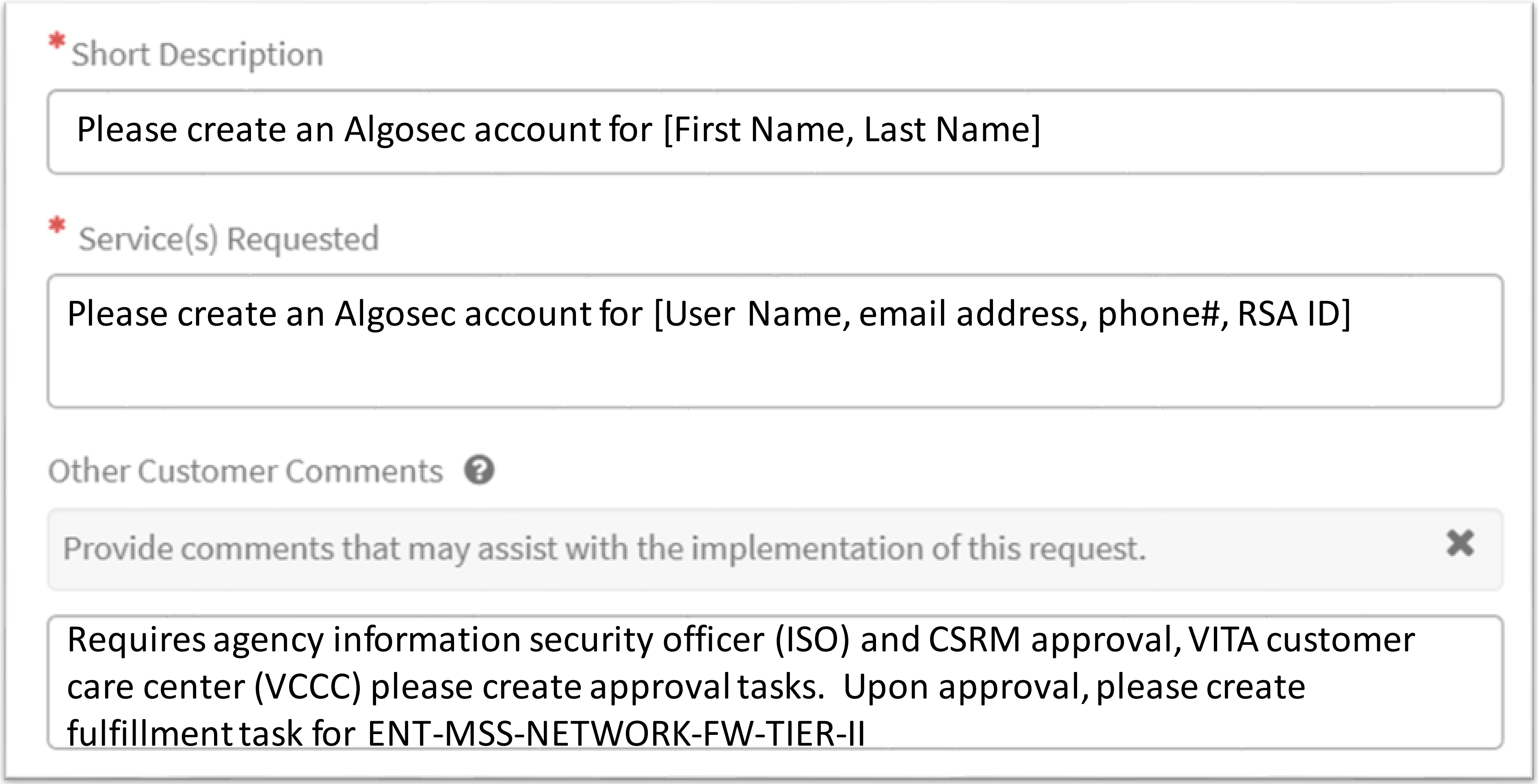
OKTA integration in progress



scott.guthrow

ACCESS REQUESTS

Until a specific VITA service catalog entry is created, submit a general service request (GSR):



* Short Description

Please create an Algosec account for [First Name, Last Name]

* Service(s) Requested

Please create an Algosec account for [User Name, email address, phone#, RSA ID]

Other Customer Comments ?

Provide comments that may assist with the implementation of this request. ✖

Requires agency information security officer (ISO) and CSRM approval, VITA customer care center (VCCC) please create approval tasks. Upon approval, please create fulfillment task for ENT-MSS-NETWORK-FW-TIER-II

DEMO

Live demo – screenshots in the appendix

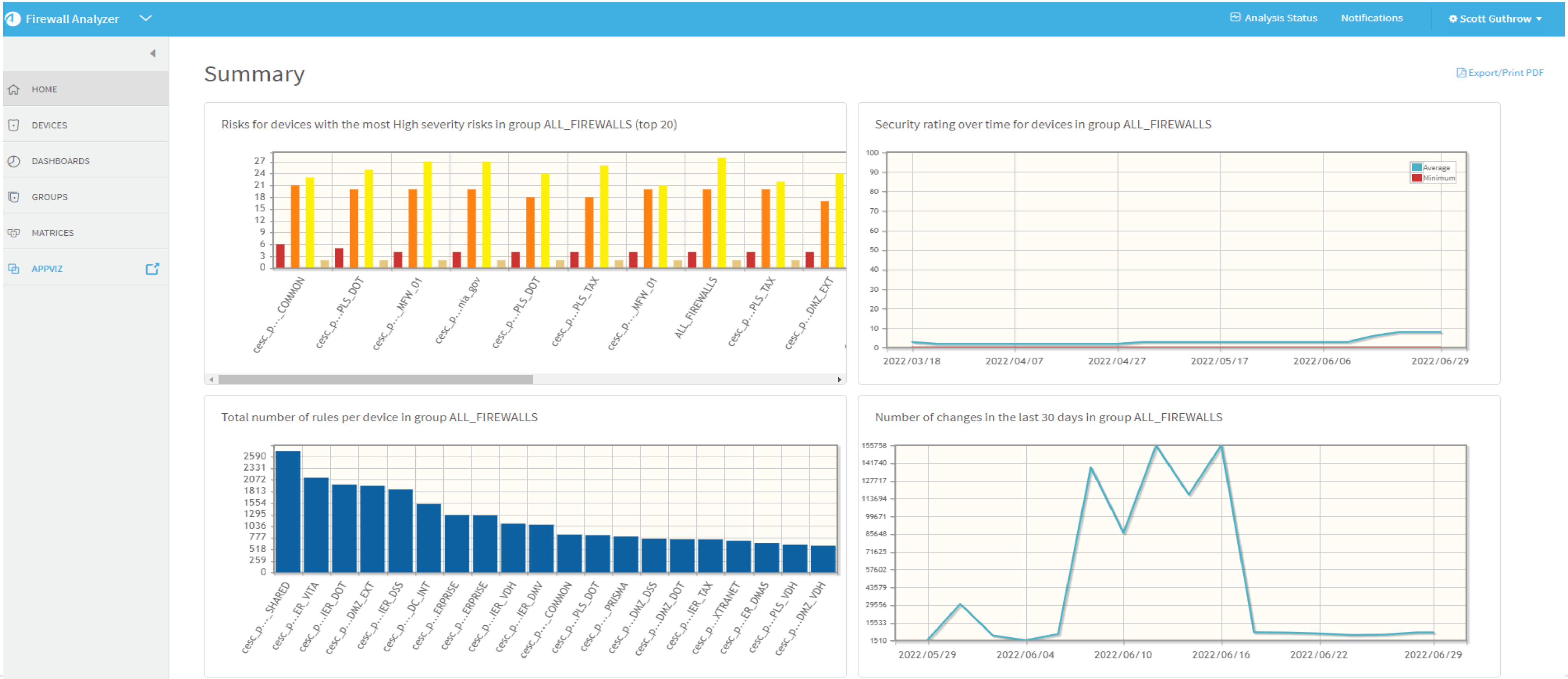
QUESTIONS?

Thank you!

APPENDIX

ALGOSEC HOME VIEW

Standard left-hand navigation – Agency-specific data views



Summary

Risks for devices with the most High severity risks in group ALL_FIREWALLS (top 20)

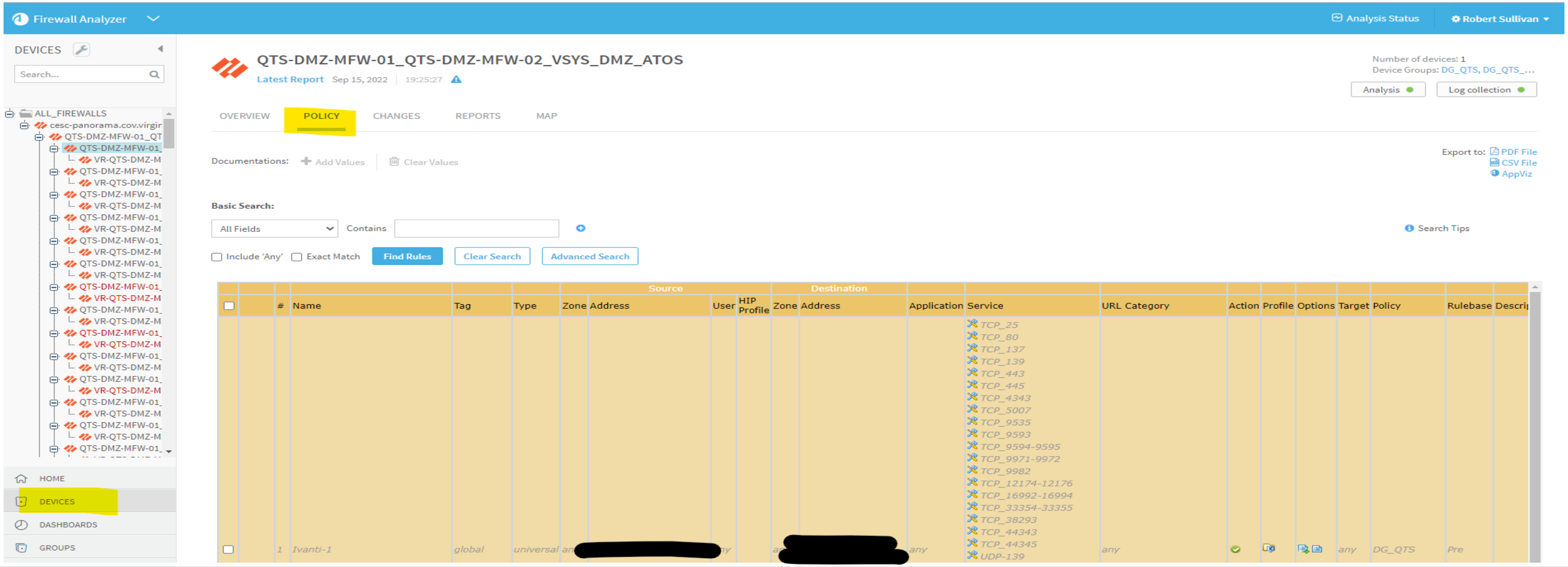
Security rating over time for devices in group ALL_FIREWALLS

Total number of rules per device in group ALL_FIREWALLS

Number of changes in the last 30 days in group ALL_FIREWALLS

VIEW AND REPORT ON FIREWALL RULES

- Selecting the **DEVICES** menu from the left navigation will display the firewalls you have access to
- Select the desired Firewall VSYS, then **POLICY,** which will display rules for the selected firewall
- You can customize the view as desired, then export the ruleset using the export function in the upper navigation



QTS-DMZ-MFW-01_QTS-DMZ-MFW-02_VSYS_DMZ_ATOS

Latest Report Sep 15, 2022 | 19:25:27

Number of devices: 1
Device Groups: DG_QTS, DG_QTS_...

Documentations:

Export to: PDF File
CSV File
AppViz

Basic Search:

☐ Include 'Any' ☐ Exact Match

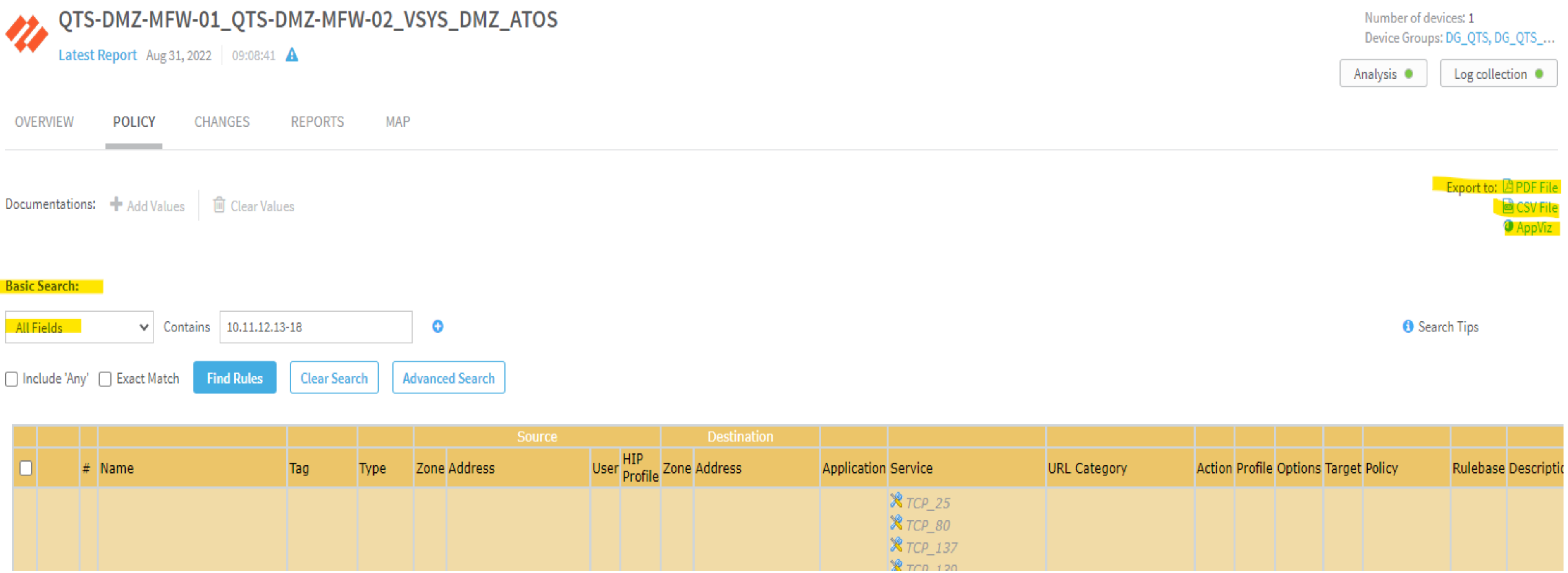
						Source				Destination											
☐		#	Name	Tag	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	URL Category	Action	Profile	Options	Target	Policy	Rulebase	Descri
☐		1	Ivanti-1	global	universal	an	[redacted]	ny		a	[redacted]	any	TCP_25 TCP_80 TCP_137 TCP_139 TCP_443 TCP_445 TCP_4343 TCP_5007 TCP_9535 TCP_9593 TCP_9594-9595 TCP_9971-9972 TCP_9982 TCP_12174-12176 TCP_16992-16994 TCP_33354-33355 TCP_38293 TCP_44343 TCP_44345 UDP-139	any	✓			any	DG_QTS	Pre	

VIRGINIA IT AGENCY

HOW TO RUN A REPORT ON MY AGENCY'S FIREWALL RULES

Export the ruleset using the export feature in the upper right-hand corner of the screen.

- If you are not looking to export the entire ruleset for the agency, you can specify a specific address or address range
- You may also add custom fields to your search by clicking the **+** button in the basic search field



QTS-DMZ-MFW-01_QTS-DMZ-MFW-02_VSYS_DMZ_ATOS

Latest Report Aug 31, 2022 | 09:08:41

Number of devices: 1
Device Groups: DG_QTS, DG_QTS_...

Documentations: + Add Values | Clear Values

Export to: PDF File
CSV File
AppViz

Basic Search:

All Fields Contains 10.11.12.13-18

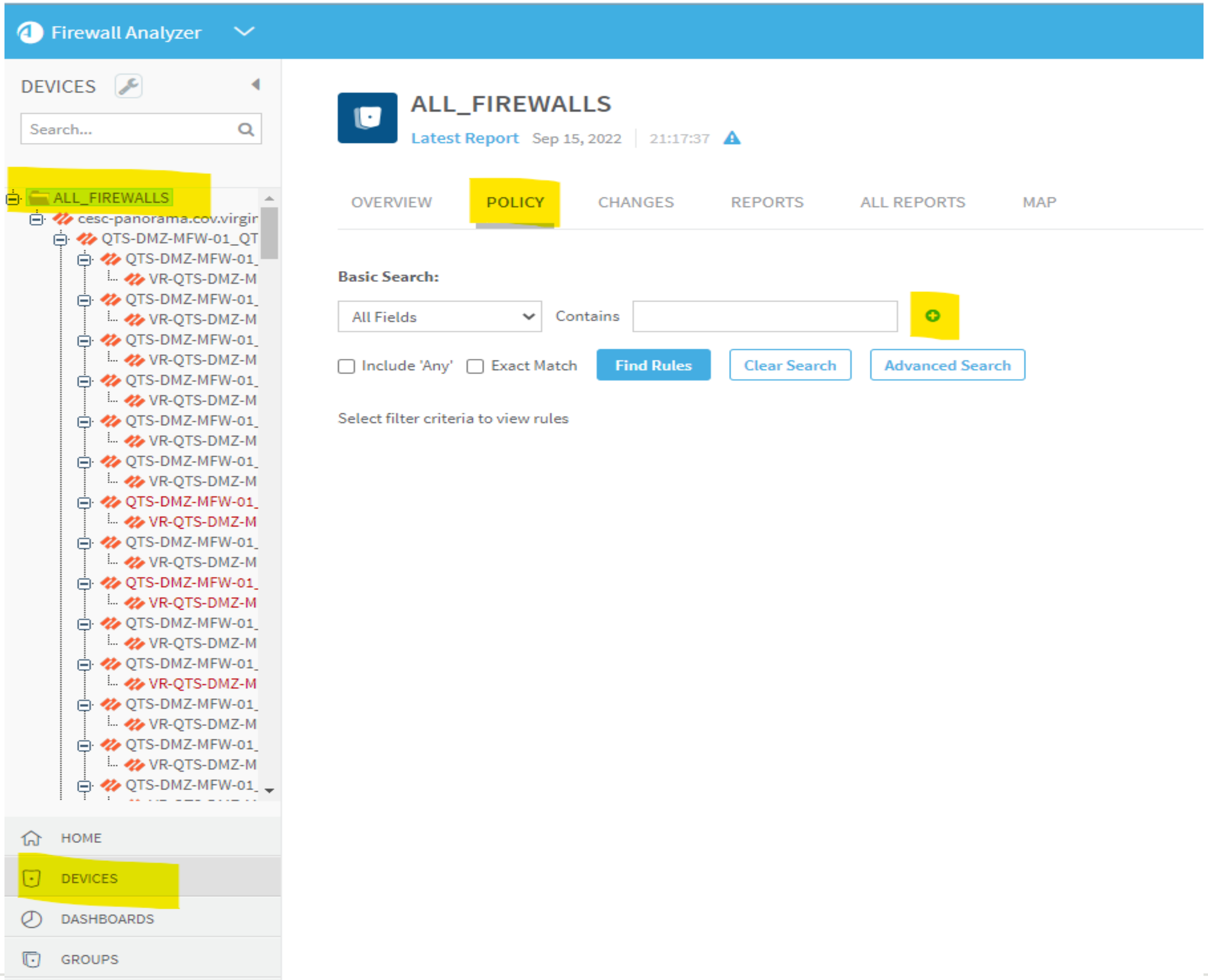
□ Include 'Any' □ Exact Match

						Source				Destination											
□		#	Name	Tag	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	URL Category	Action	Profile	Options	Target	Policy	Rulebase	Descriptic
													TCP_25 TCP_80 TCP_137 TCP_139								

SEARCHING FOR A FIREWALL RULE

From the **HOME** screen, click on **DEVICES**

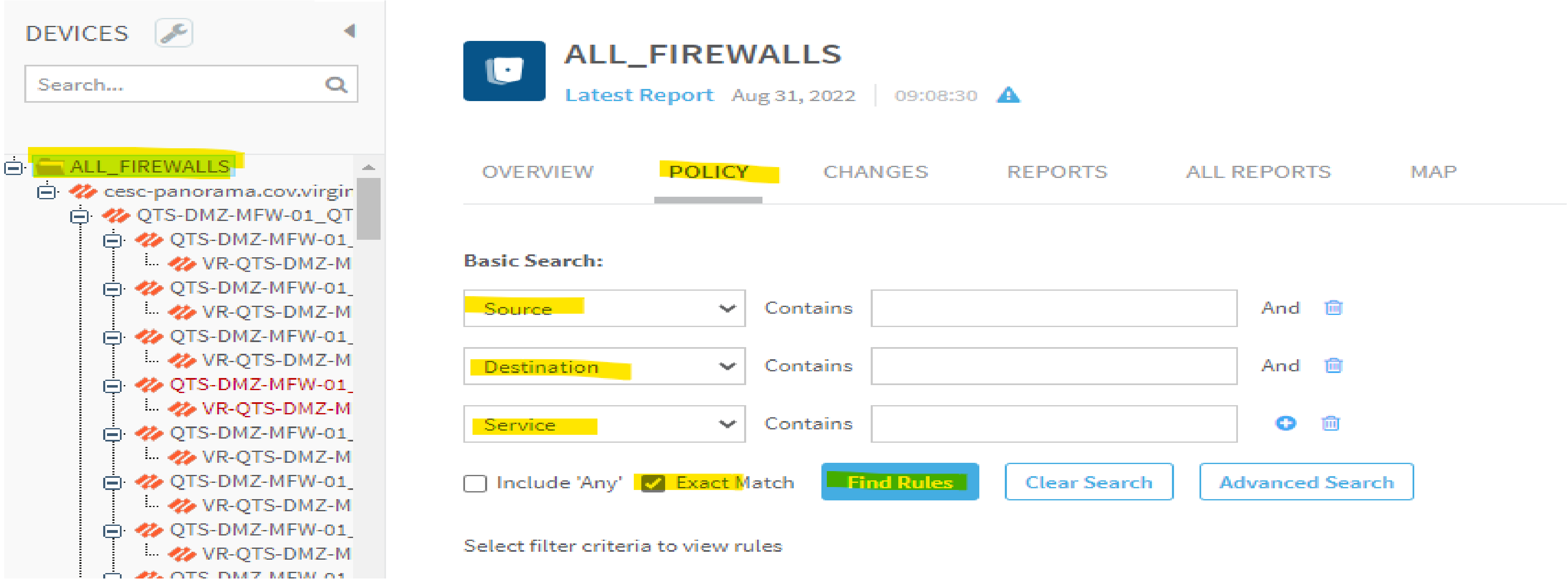
- From the **DEVICES** screen, click on **ALL_FIREWALLS** and **POLICY**
- To enter multiple search criteria, you can click on the **+** symbol to add additional search fields.



Select filter criteria to view rules

Adding additional search fields to search with 3 search fields:

- Change “All Fields” pull down to “Source,” and enter Source IP, then click on the + symbol
- Change “All Fields” pull down to “Destination” and enter Destination IP, then click on the + symbol
- Change “All Fields” pull down to “Service” and enter Port #



Basic Search:

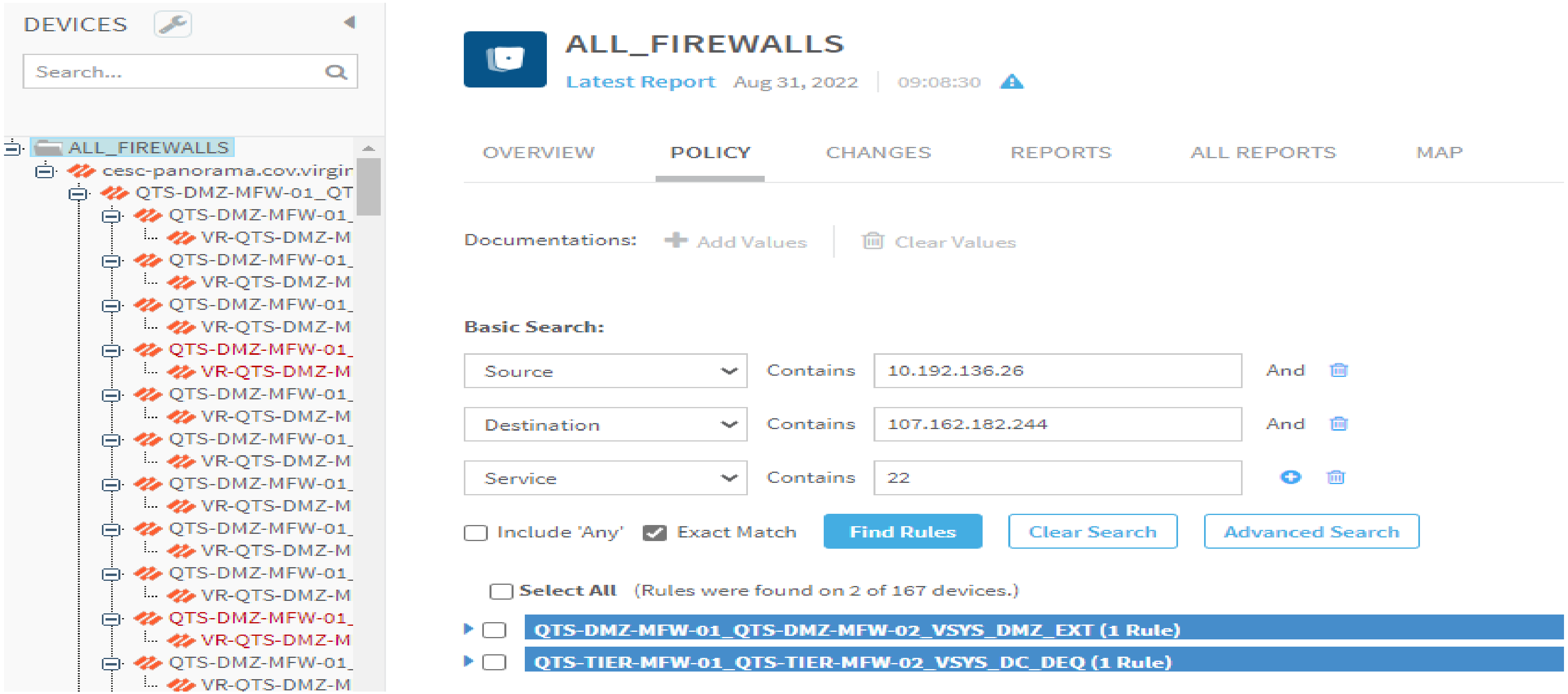
Source Contains And
Destination Contains And
Service Contains

☐ Include 'Any' ☑ Exact Match

Select filter criteria to view rules

FIREWALL RULE SEARCH RESULTS

Click on blue arrow to expand the search results



ALL_FIREWALLS

Latest Report Aug 31, 2022 | 09:08:30

Documentations: + Add Values | Clear Values

Basic Search:

Source Contains 10.192.136.26 And

Destination Contains 107.162.182.244 And

Service Contains 22

□ Include 'Any' ☑ Exact Match **Find Rules** Clear Search Advanced Search

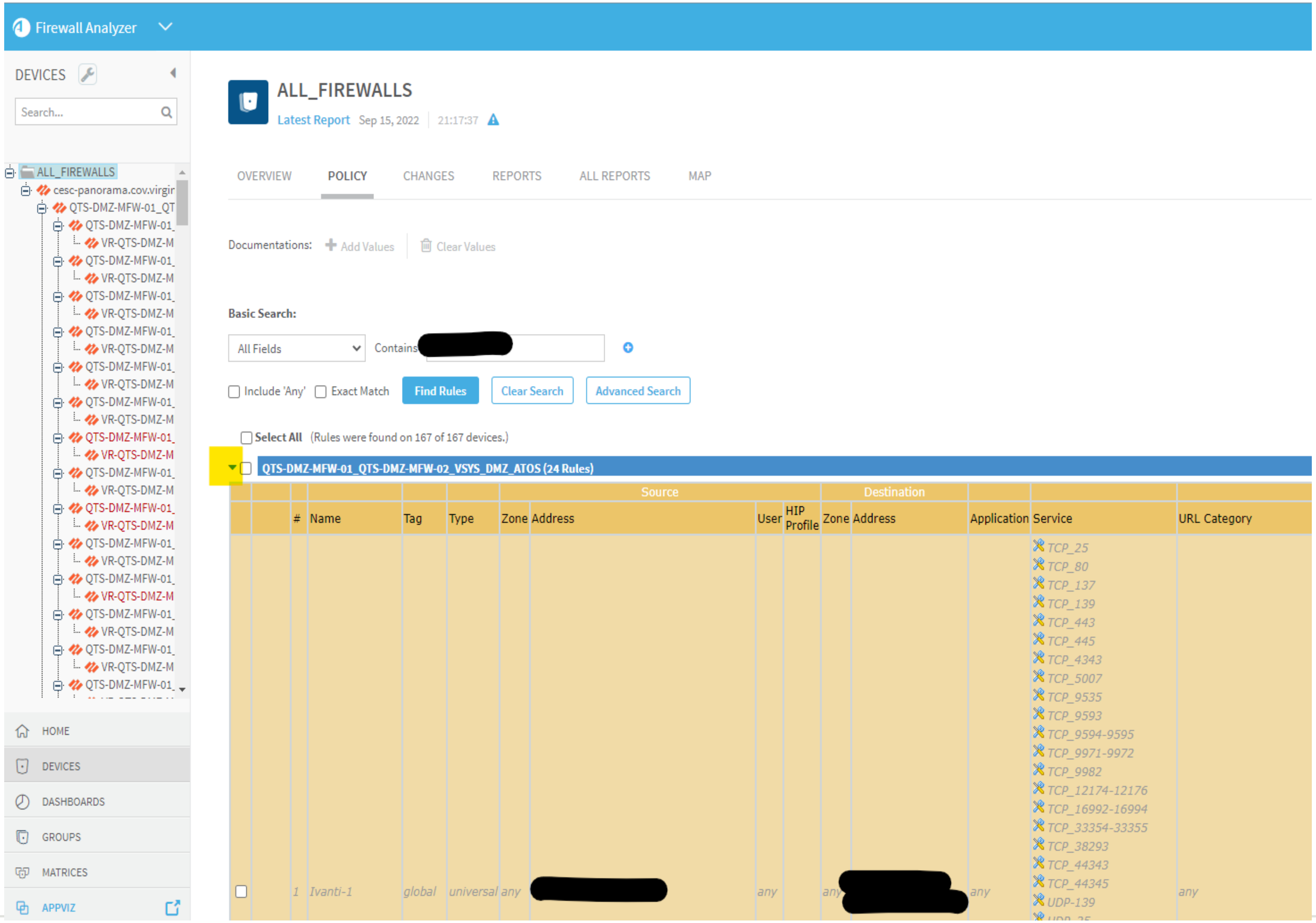
□ **Select All** (Rules were found on 2 of 167 devices.)

▸ □ **QTS-DMZ-MFW-01_QTS-DMZ-MFW-02_VSYS_DMZ_EXT (1 Rule)**

▸ □ **QTS-TIER-MFW-01_QTS-TIER-MFW-02_VSYS_DC_DEQ (1 Rule)**

HOW TO SEARCH FOR A FIREWALL RULE

- You can click on any of the blue fields and additional info will be revealed.
- In this example, we use the SCTASK number in the description to cross reference, the rule has valid approval.



Firewall Analyzer

DEVICES

Search...

ALL_FIREWALLS
cesc-panorama.cov.virgir
QTS-DMZ-MFW-01_QT
QTS-DMZ-MFW-01_
VR-QTS-DMZ-M
QTS-DMZ-MFW-01_
VR-QTS-DMZ-M
QTS-DMZ-MFW-01_
VR-QTS-DMZ-M
QTS-DMZ-MFW-01_
VR-QTS-DMZ-M
QTS-DMZ-MFW-01_
VR-QTS-DMZ-M
QTS-DMZ-MFW-01_
VR-QTS-DMZ-M
QTS-DMZ-MFW-01_
VR-QTS-DMZ-M
QTS-DMZ-MFW-01_
VR-QTS-DMZ-M
QTS-DMZ-MFW-01_
VR-QTS-DMZ-M
QTS-DMZ-MFW-01_
VR-QTS-DMZ-M
QTS-DMZ-MFW-01_
VR-QTS-DMZ-M
QTS-DMZ-MFW-01_
VR-QTS-DMZ-M
QTS-DMZ-MFW-01_
VR-QTS-DMZ-M
QTS-DMZ-MFW-01_

HOME
DEVICES
DASHBOARDS
GROUPS
MATRICES
APPVIZ

ALL_FIREWALLS
Latest Report Sep 15, 2022 | 21:17:37

OVERVIEW | POLICY | CHANGES | REPORTS | ALL REPORTS | MAP

Documentations: + Add Values | Clear Values

Basic Search:

All Fields | Contains [redacted]

□ Include 'Any' □ Exact Match | Find Rules | Clear Search | Advanced Search

□ Select All (Rules were found on 167 of 167 devices.)

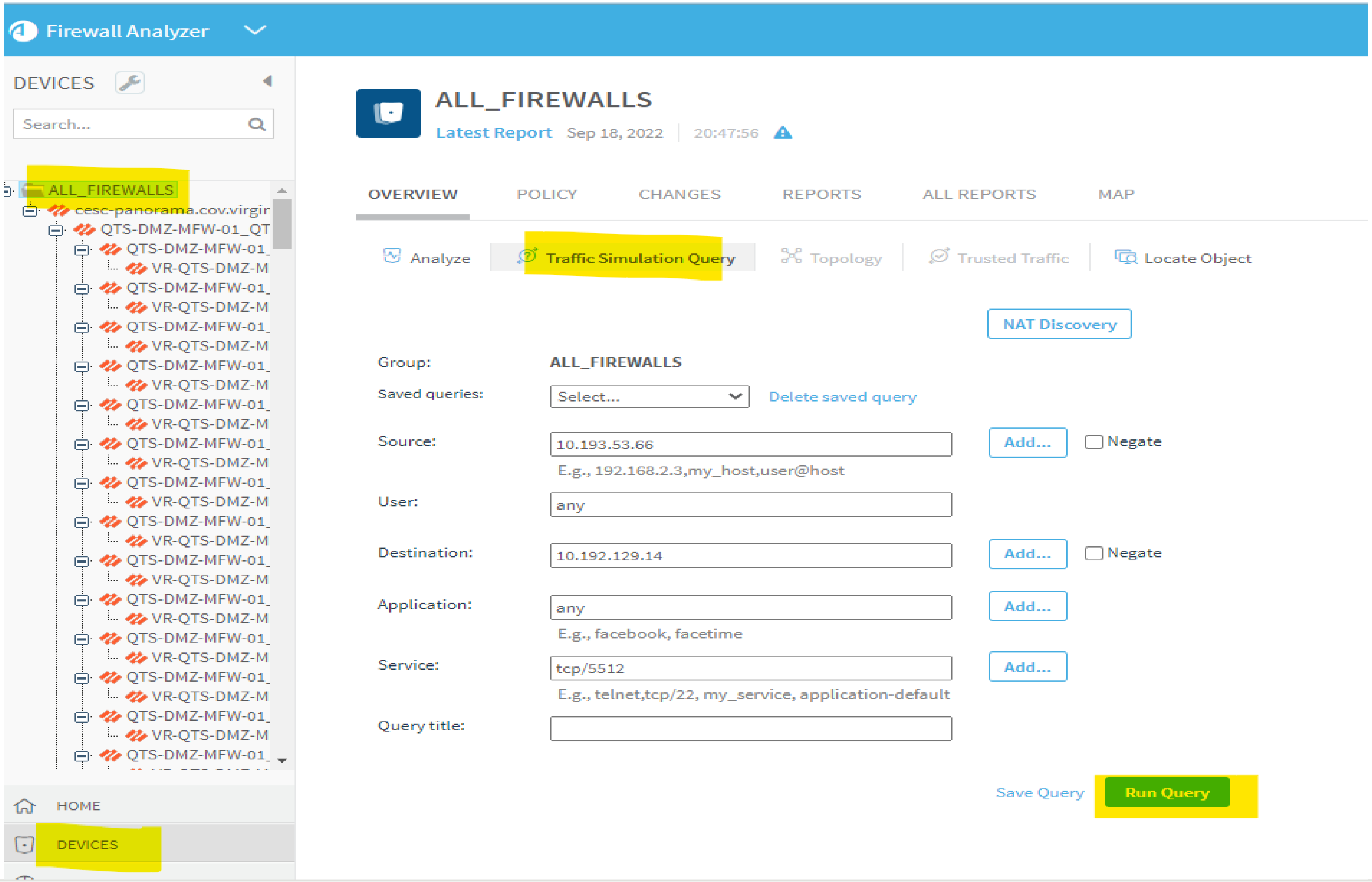
□ QTS-DMZ-MFW-01_QTS-DMZ-MFW-02_VSYS_DMZ_ATOS (24 Rules)

						Source				Destination				
		#	Name	Tag	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	URL Category
□		1	Ivanti-1	global	universal	any	[redacted]	any		any	[redacted]	any	TCP_25 TCP_80 TCP_137 TCP_139 TCP_443 TCP_445 TCP_4343 TCP_5007 TCP_9535 TCP_9593 TCP_9594-9595 TCP_9971-9972 TCP_9982 TCP_12174-12176 TCP_16992-16994 TCP_33354-33355 TCP_38293 TCP_44343 TCP_44345 UDP-139	any

TRAFFIC SIMULATION QUERY

A traffic simulation query can be used to determine if a policy already exists for certain traffic:

- Choose the firewalls you would like to query against
- Enter a valid source, destination and service port
- Run query



Group: ALL_FIREWALLS

Saved queries: Select...

Source: 10.193.53.66 □ Negate

E.g., 192.168.2.3,my_host,user@host

User: any

Destination: 10.192.129.14 □ Negate

Application: any

E.g., facebook, facetime

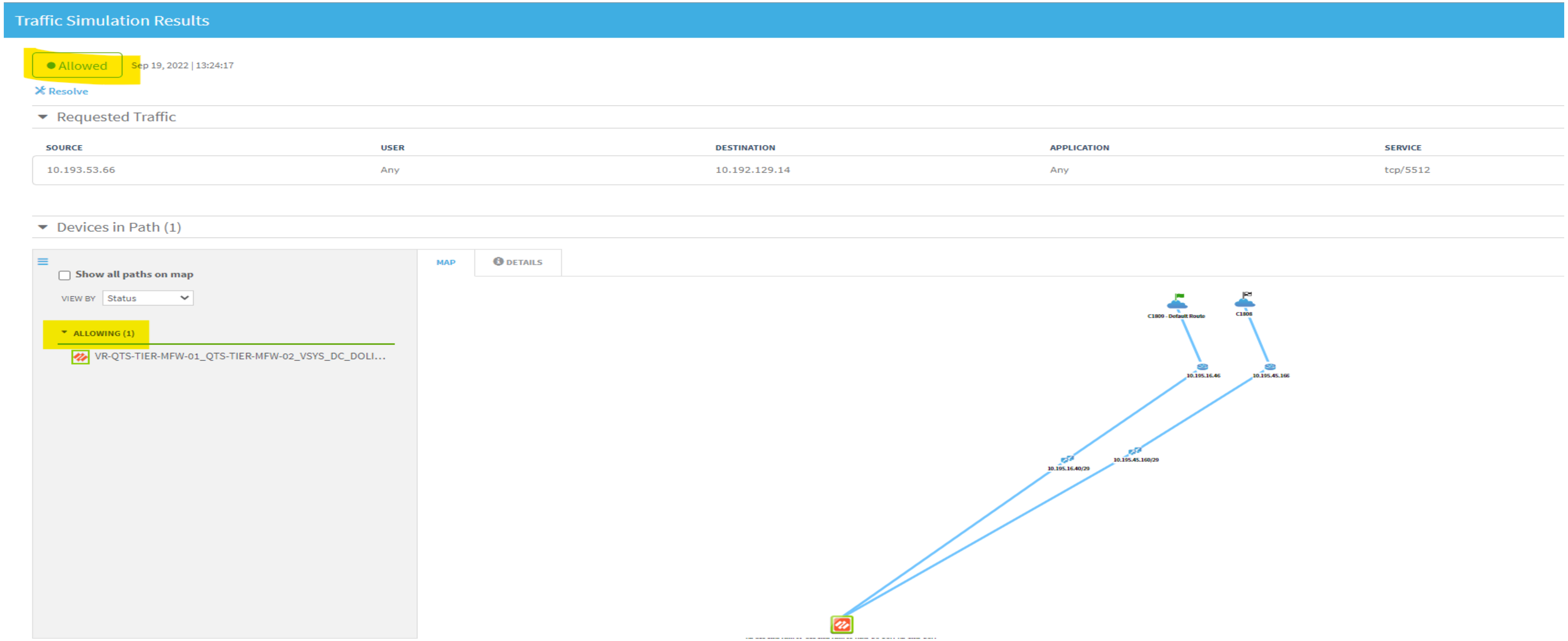
Service: tcp/5512

E.g., telnet,tcp/22, my_service, application-default

Query title:

QUERY RESULTS: ALLOWED

In this case, traffic is allowed and you can see the firewalls in path.



Traffic Simulation Results

● Allowed Sep 19, 2022 | 13:24:17

Resolve

Requested Traffic

SOURCE	USER	DESTINATION	APPLICATION	SERVICE
10.193.53.66	Any	10.192.129.14	Any	tcp/5512

Devices in Path (1)

☐ Show all paths on map

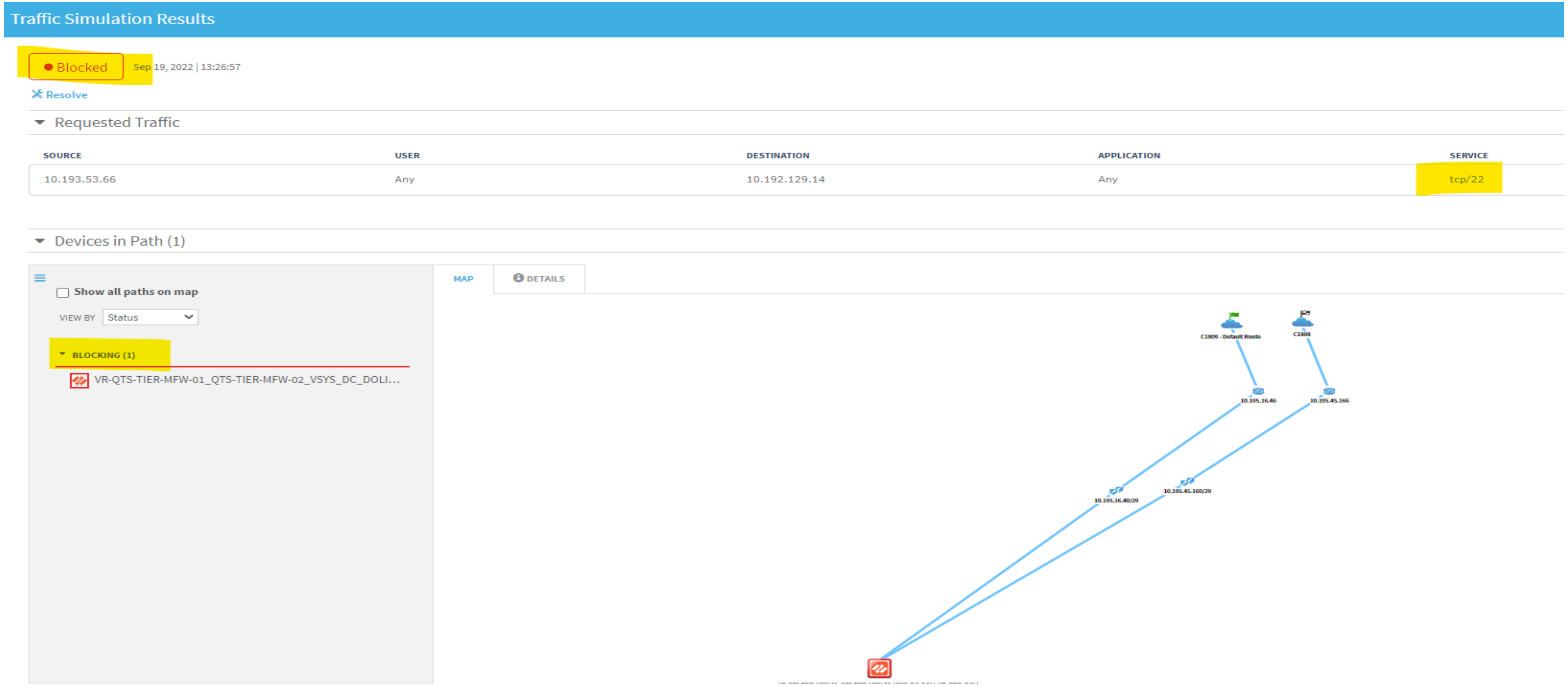
VIEW BY Status

ALLOWING (1)

VR-QTS-TIER-MFW-01_QTS-TIER-MFW-02_VSYS_DC_DOLI...

QUERY RESULTS: BLOCKED

In this case, traffic is blocked and you can see the firewall that will require a rule to allow this traffic.



Traffic Simulation Results

● Blocked Sep 19, 2022 | 13:26:57

Resolve

Requested Traffic

SOURCE	USER	DESTINATION	APPLICATION	SERVICE
10.193.53.66	Any	10.192.129.14	Any	tcp/22

Devices in Path (1)

☐ Show all paths on map

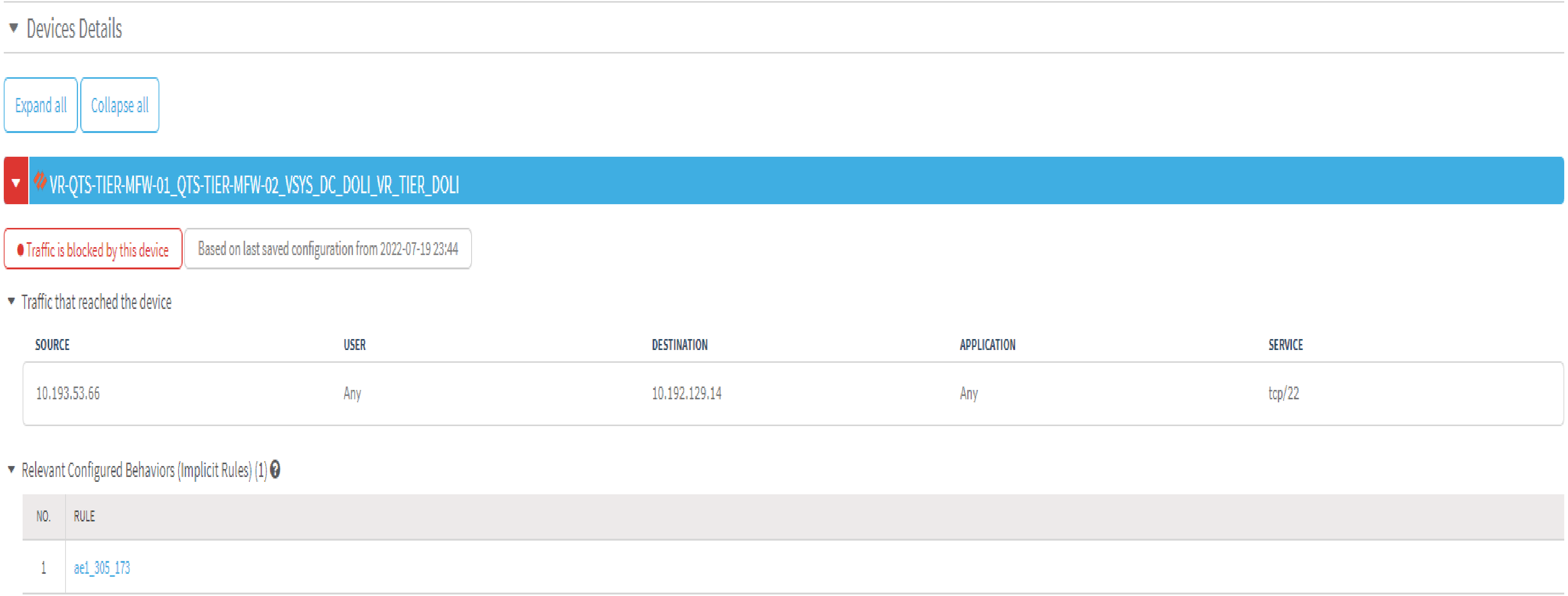
VIEW BY Status

BLOCKING (1)

VR-QTS-TIER-MFW-01_QTS-TIER-MFW-02_VSYS_DC_DOLI...

DEVICE BLOCKING

These are the details of the firewall and rule blocking the traffic.



▼ Devices Details

▼ VR-QTS-TIER-MFW-01_QTS-TIER-MFW-02_VSYS_DC_DOLI_VR_TIER_DOLI

● Traffic is blocked by this device

Based on last saved configuration from 2022-07-19 23:44

▼ Traffic that reached the device

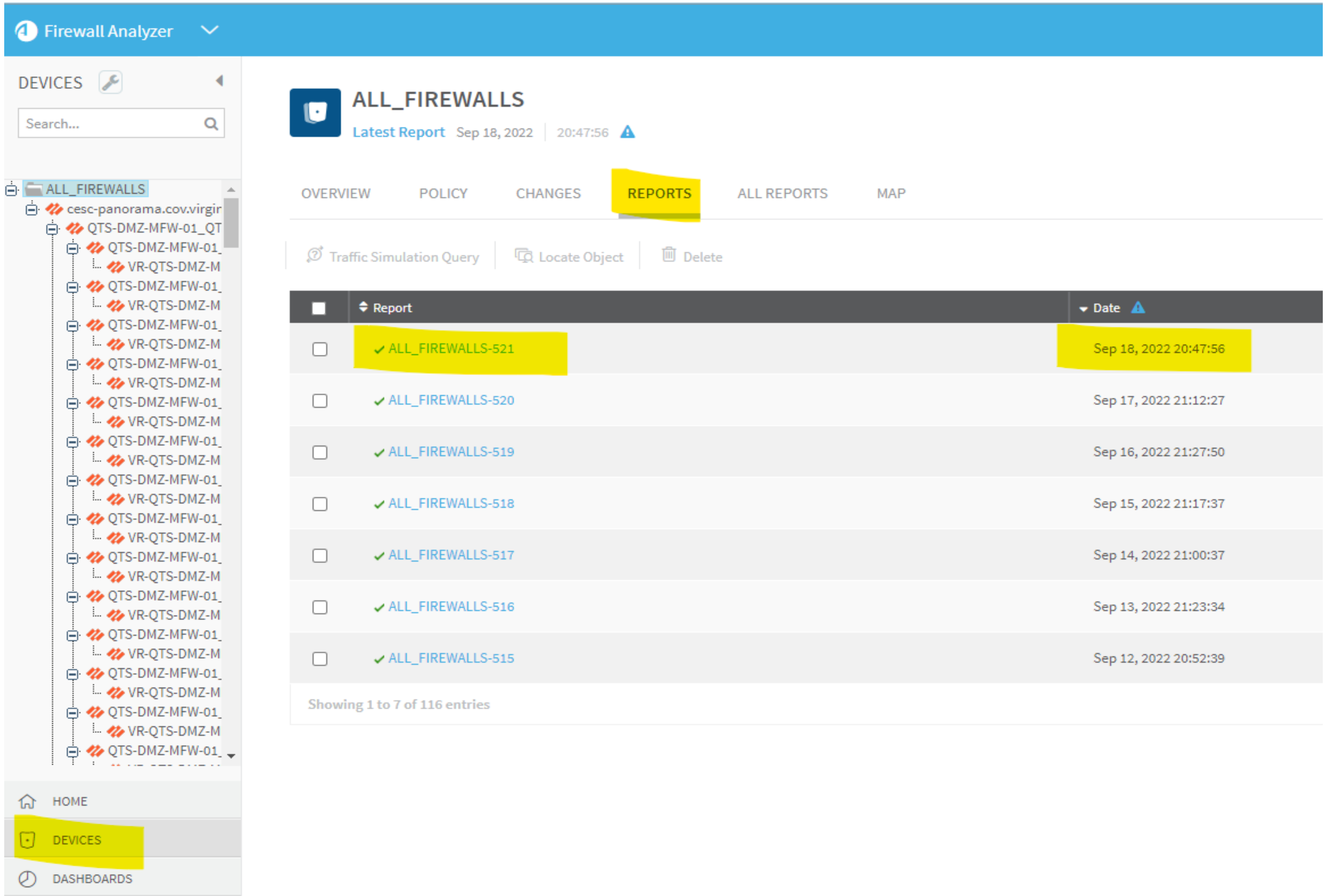
SOURCE	USER	DESTINATION	APPLICATION	SERVICE
10.193.53.66	Any	10.192.129.14	Any	tcp/22

▼ Relevant Configured Behaviors (Implicit Rules) (1)

NO.	RULE
1	ae1_305_173

POLICY OPTIMIZATION

Navigate to the **Policy Optimization** menu by going to **Devices / Reports** and clicking on the latest report.



ALL_FIREWALLS

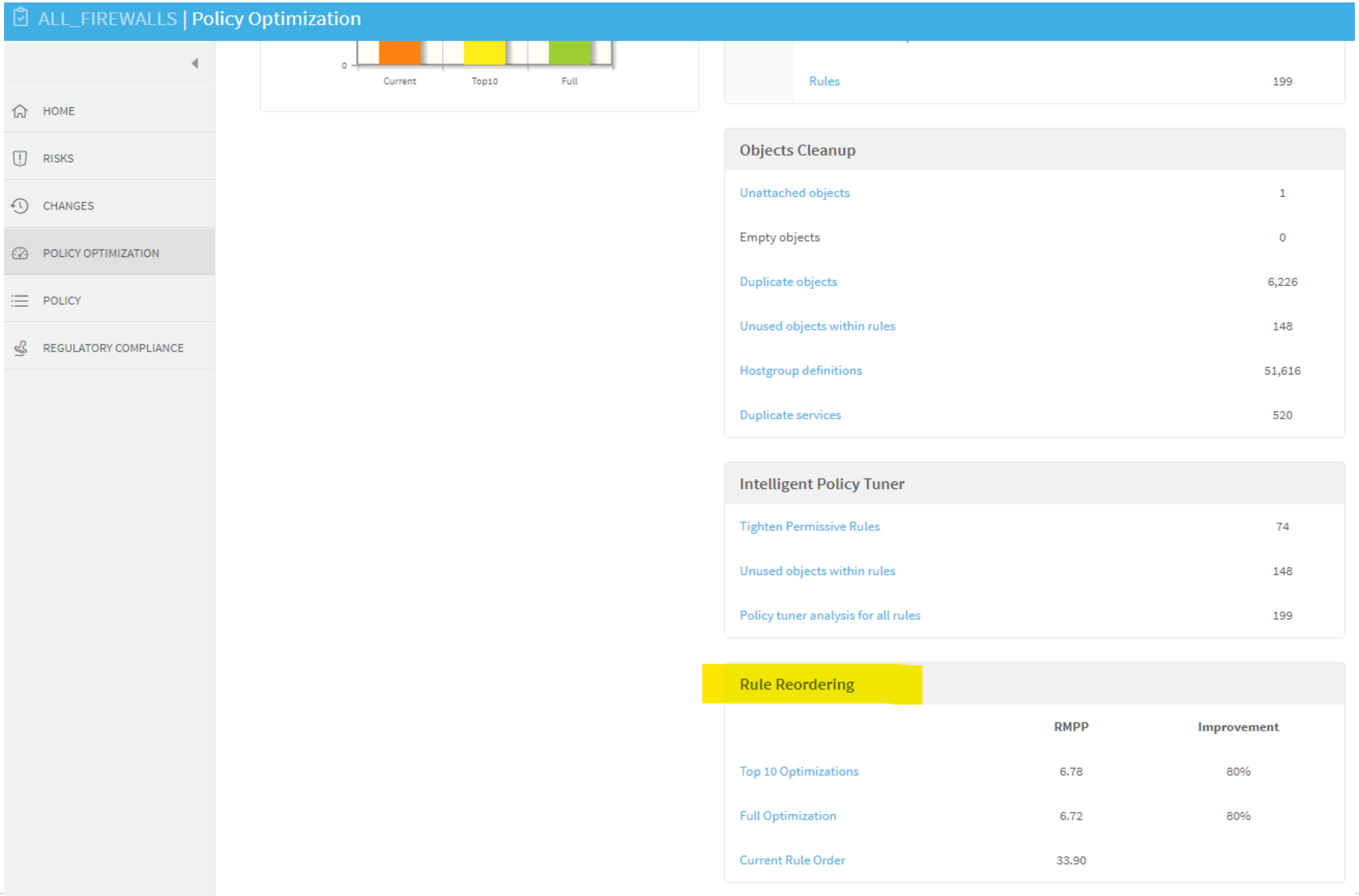
Latest Report Sep 18, 2022 | 20:47:56

□	Report	Date
□	✓ ALL_FIREWALLS-521	Sep 18, 2022 20:47:56
□	✓ ALL_FIREWALLS-520	Sep 17, 2022 21:12:27
□	✓ ALL_FIREWALLS-519	Sep 16, 2022 21:27:50
□	✓ ALL_FIREWALLS-518	Sep 15, 2022 21:17:37
□	✓ ALL_FIREWALLS-517	Sep 14, 2022 21:00:37
□	✓ ALL_FIREWALLS-516	Sep 13, 2022 21:23:34
□	✓ ALL_FIREWALLS-515	Sep 12, 2022 20:52:39

Showing 1 to 7 of 116 entries

POLICY OPTIMIZATION

Here you can review rule reordering to maximize efficiency of the firewalls as well as options to tighten overly permissive rules



Rules	199

Objects Cleanup	
Unattached objects	1
Empty objects	0
Duplicate objects	6,226
Unused objects within rules	148
Hostgroup definitions	51,616
Duplicate services	520

Intelligent Policy Tuner	
Tighten Permissive Rules	74
Unused objects within rules	148
Policy tuner analysis for all rules	199

Rule Reordering

	RMPP	Improvement
Top 10 Optimizations	6.78	80%
Full Optimization	6.72	80%
Current Rule Order	33.90	

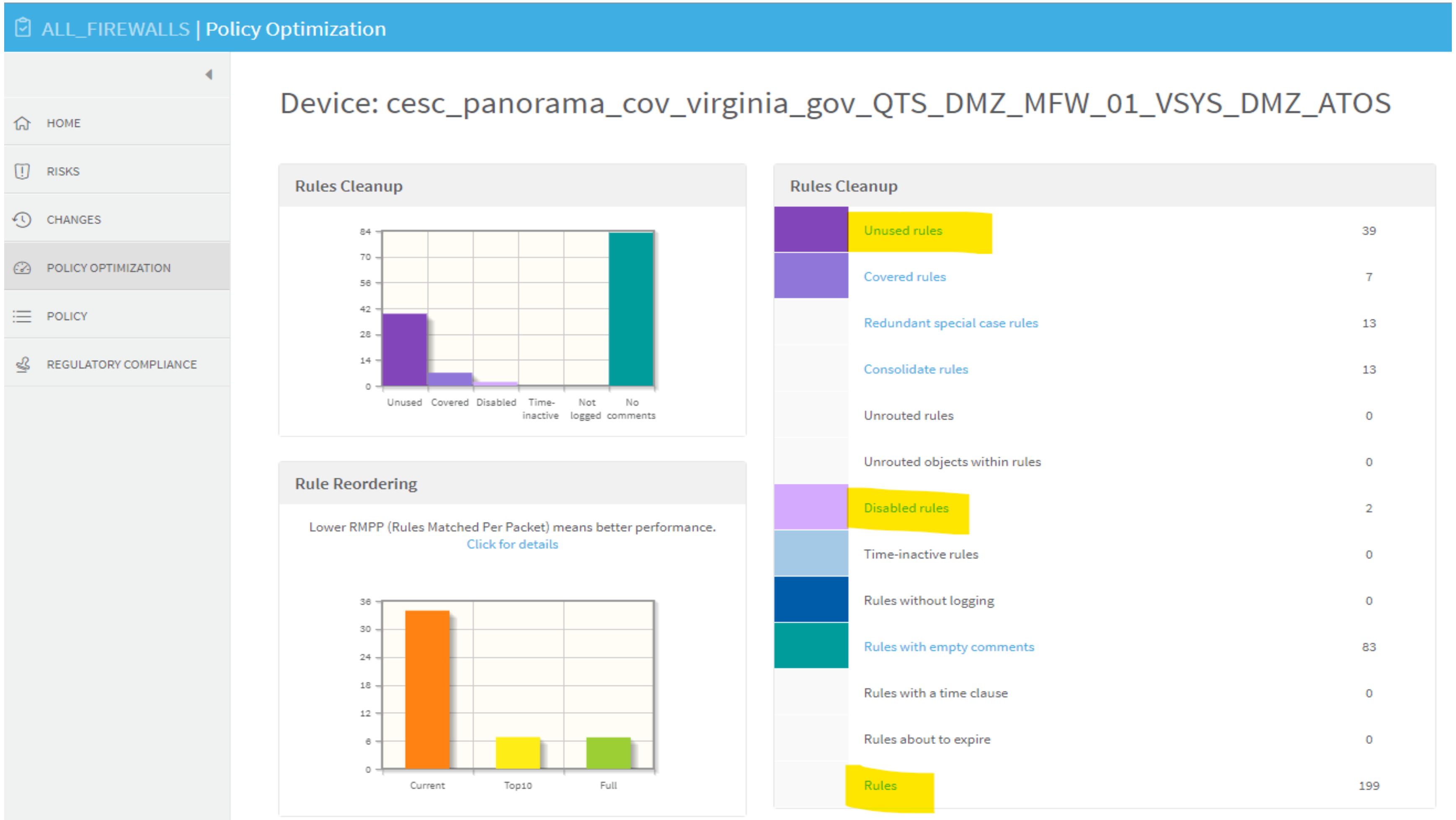
POLICY OPTIMIZATION

From the policy optimization menu option you can see:

1. Unused rules
2. Disabled rules
3. Total number of rules

Scroll down further to see:

- Least used rules
- Most used rules
- Unused rules



Device: cesc_panorama_cov_virginia_gov_QTS_DMZ_MFW_01_VSYS_DMZ_ATOS

Lower RMPP (Rules Matched Per Packet) means better performance.
Click for details

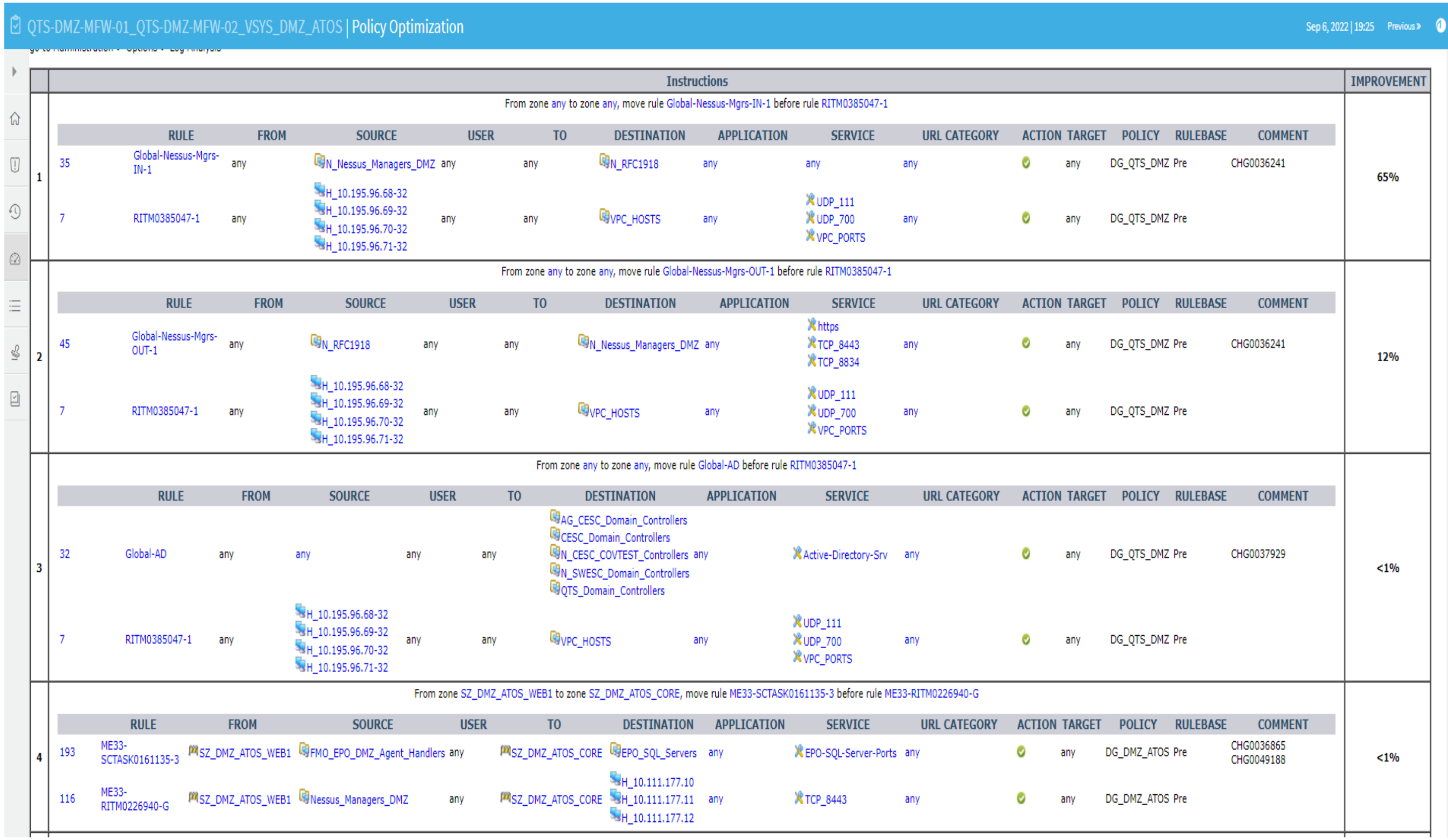
Rules Cleanup

🟪	Unused rules	39
🟪	Covered rules	7
	Redundant special case rules	13
	Consolidate rules	13
	Unrouted rules	0
	Unrouted objects within rules	0
🟪	Disabled rules	2
🟦	Time-inactive rules	0
🟦	Rules without logging	0
🟩	Rules with empty comments	83
	Rules with a time clause	0
	Rules about to expire	0
	Rules	199

POLICY OPTIMIZATION

AlgoSec determines efficiencies for rule reordering based on available information from firewall logs.

AlgoSec determines the improvement value of the adjustment should you choose to follow the recommendations.



QTS-DMZ-MFW-01_QTS-DMZ-MFW-02_VSYS_DMZ_ATOS | Policy Optimization

Sep 6, 2022 | 19:25 Previous »

Instructions

1 From zone any to zone any, move rule Global-Nessus-Mgrs-IN-1 before rule RITM0385047-1

	RULE		FROM	SOURCE	USER	TO	DESTINATION	APPLICATION	SERVICE	URL CATEGORY	ACTION	TARGET	POLICY	RULEBASE	COMMENT	IMPROVEMENT
1	35	Global-Nessus-Mgrs-IN-1	any	N_Nessus_Managers_DMZ	any	any	N_RFC1918	any	any	any	✓	any	DG_QTS_DMZ	Pre	CHG0036241	65%
	7	RITM0385047-1	any	H_10.195.96.68-32 H_10.195.96.69-32 H_10.195.96.70-32 H_10.195.96.71-32	any	any	VPC_HOSTS	any	UDP_111 UDP_700 VPC_PORTS	any	✓	any	DG_QTS_DMZ	Pre		

2 From zone any to zone any, move rule Global-Nessus-Mgrs-OUT-1 before rule RITM0385047-1

	RULE		FROM	SOURCE	USER	TO	DESTINATION	APPLICATION	SERVICE	URL CATEGORY	ACTION	TARGET	POLICY	RULEBASE	COMMENT	IMPROVEMENT
2	45	Global-Nessus-Mgrs-OUT-1	any	N_RFC1918	any	any	N_Nessus_Managers_DMZ	any	https TCP_8443 TCP_8834	any	✓	any	DG_QTS_DMZ	Pre	CHG0036241	12%
	7	RITM0385047-1	any	H_10.195.96.68-32 H_10.195.96.69-32 H_10.195.96.70-32 H_10.195.96.71-32	any	any	VPC_HOSTS	any	UDP_111 UDP_700 VPC_PORTS	any	✓	any	DG_QTS_DMZ	Pre		

3 From zone any to zone any, move rule Global-AD before rule RITM0385047-1

	RULE		FROM	SOURCE	USER	TO	DESTINATION	APPLICATION	SERVICE	URL CATEGORY	ACTION	TARGET	POLICY	RULEBASE	COMMENT	IMPROVEMENT
3	32	Global-AD	any	any	any	any	AG_CESC_Domain_Controllers CESC_Domain_Controllers N_CESC_COVTEST_Controllers N_SWESC_Domain_Controllers QTS_Domain_Controllers	any	Active-Directory-Srv	any	✓	any	DG_QTS_DMZ	Pre	CHG0037929	<1%
	7	RITM0385047-1	any	H_10.195.96.68-32 H_10.195.96.69-32 H_10.195.96.70-32 H_10.195.96.71-32	any	any	VPC_HOSTS	any	UDP_111 UDP_700 VPC_PORTS	any	✓	any	DG_QTS_DMZ	Pre		

4 From zone SZ_DMZ_ATOS_WEB1 to zone SZ_DMZ_ATOS_CORE, move rule ME33-SCTASK0161135-3 before rule ME33-RITM0226940-G

	RULE		FROM	SOURCE	USER	TO	DESTINATION	APPLICATION	SERVICE	URL CATEGORY	ACTION	TARGET	POLICY	RULEBASE	COMMENT	IMPROVEMENT
4	193	ME33-SCTASK0161135-3	SZ_DMZ_ATOS_WEB1	FMO_EPO_DMZ_Agent_Handlers	any	SZ_DMZ_ATOS_CORE	EPO_SQL_Servers	any	EPO-SQL-Server-Ports	any	✓	any	DG_DMZ_ATOS	Pre	CHG0036865 CHG0049188	<1%
	116	ME33-RITM0226940-G	SZ_DMZ_ATOS_WEB1	Nessus_Managers_DMZ	any	SZ_DMZ_ATOS_CORE	H_10.111.177.10 H_10.111.177.11 H_10.111.177.12	any	TCP_8443	any	✓	any	DG_DMZ_ATOS	Pre		

UPCOMING EVENTS

JANUARY ISOAG MEETING

THERE WILL BE NO MEETING IN JAN

NEXT MEETING IS FEB. 1 , 2023

NEXT ISO ORIENTATION

DEC. 12

TIME 1 - 3 P.M.

HOSTED BY – MARLON COLE

HTTPS://COVACONF.WEBEX.COM/COVACONF/ONSTAGE/G.PHP?MTID=E6299241BFEFDE9A4E45B6E1B8A81E7CB

VIRGINIA
IT AGENCY

MEETING ADJOURNED