WELCOME TO THE Jan. 10, 2024 ISOAG MEETING

VIRGINIA IT AGENCY

Information Security Officer's Advisory Group

January 10, 2024

Agenda	Presenter
Welcome/Opening Remarks	Erica Bland/ VITA
Enterprise Security Data Lake at Scale w/ CrowdStrike	Rob Reynolds/CrowdStrike Logscale Sales Manager
Debut of COV RAMP Dashboard	Richard White/ VITA
KnowBe4 Phishing Lessons Learned	Kathy Bortle / VITA
SEC530 Updates	Amy Braden/ VITA
Workload Management (WM)	John C Del Grosso/VITA
Upcoming Events	Erica Bland/ VITA
Adjourn	

Enterprise Security Data Lake at Scale w/ Crowdstrike

Real-time Observability Is a Challenge

Falcon LogScale

Exponential Data Growth

- Limited data collected due to cost and lack of scalability
- Increase in blindspots
- Lack of metrics around MTTD and MTTR

Complexity and unknown unknowns

- Regulatory and compliance requirements
- Multi-cloud and cloud native technologies
- Increasing complexity of legacy deployments

Budget Pressures

- Continual compromises on what to analyze and how long to retain data
- Erosion of value on ingested data; no insights from inaccessible data

Traditional Vendors

- Elastic - Heavy index-based approach to log management
- Splunk - Compute and resource intensive with no incentive to optimize

Staffing Challenges

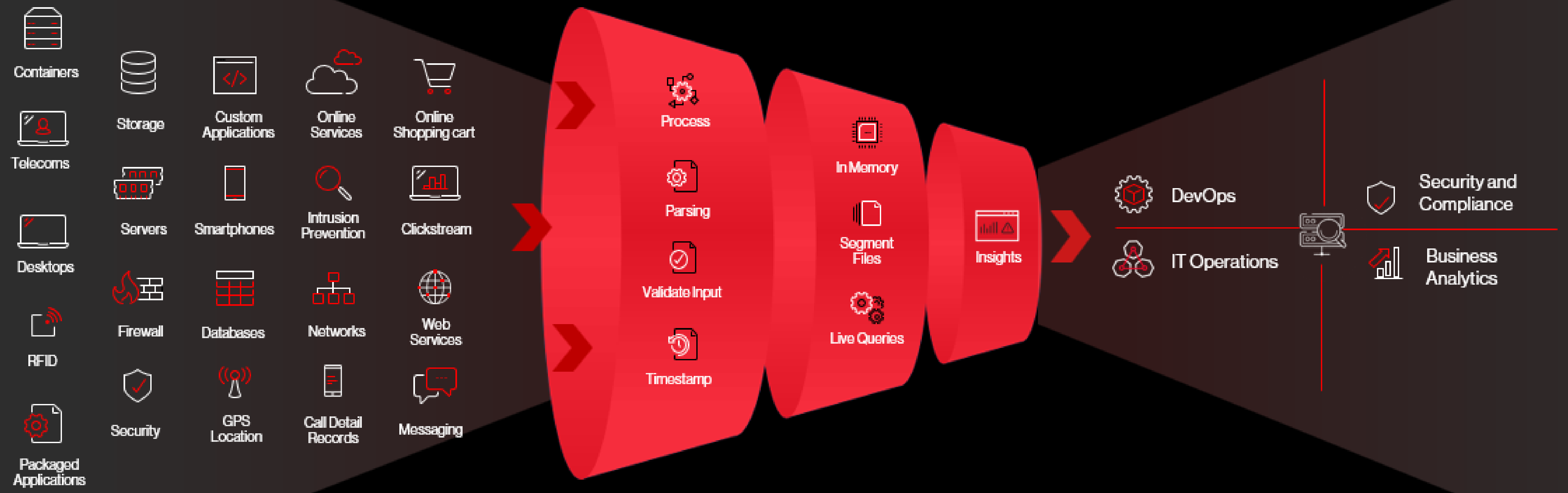
- Reactive opposed to proactive incident response
- Limited expertise available to maximize on valuable data

Answers Are in the Logs

Log Everything

In Real Time

Answer Anything



Containers

Telecoms

Desktops

RFID

Packaged Applications

Storage

Servers

Firewall

Security

Custom Applications

Smartphones

Databases

GPS Location

Online Services

Intrusion Prevention

Networks

Call Detail Records

Online Shopping cart

Clickstream

Web Services

Messaging

Process

Parsing

Validate Input

Timestamp

In Memory

Segment Files

Live Queries

Insights

DevOps

IT Operations

Security and Compliance

Business Analytics

STARDUST CHOLLIMA

A prolific North Korean nation-state group

- **Objective:** financial gain
- **Targets:** Cryptocurrency, financial services, technology, hospitality
- **Notable attacks:** SWIFT network attacks

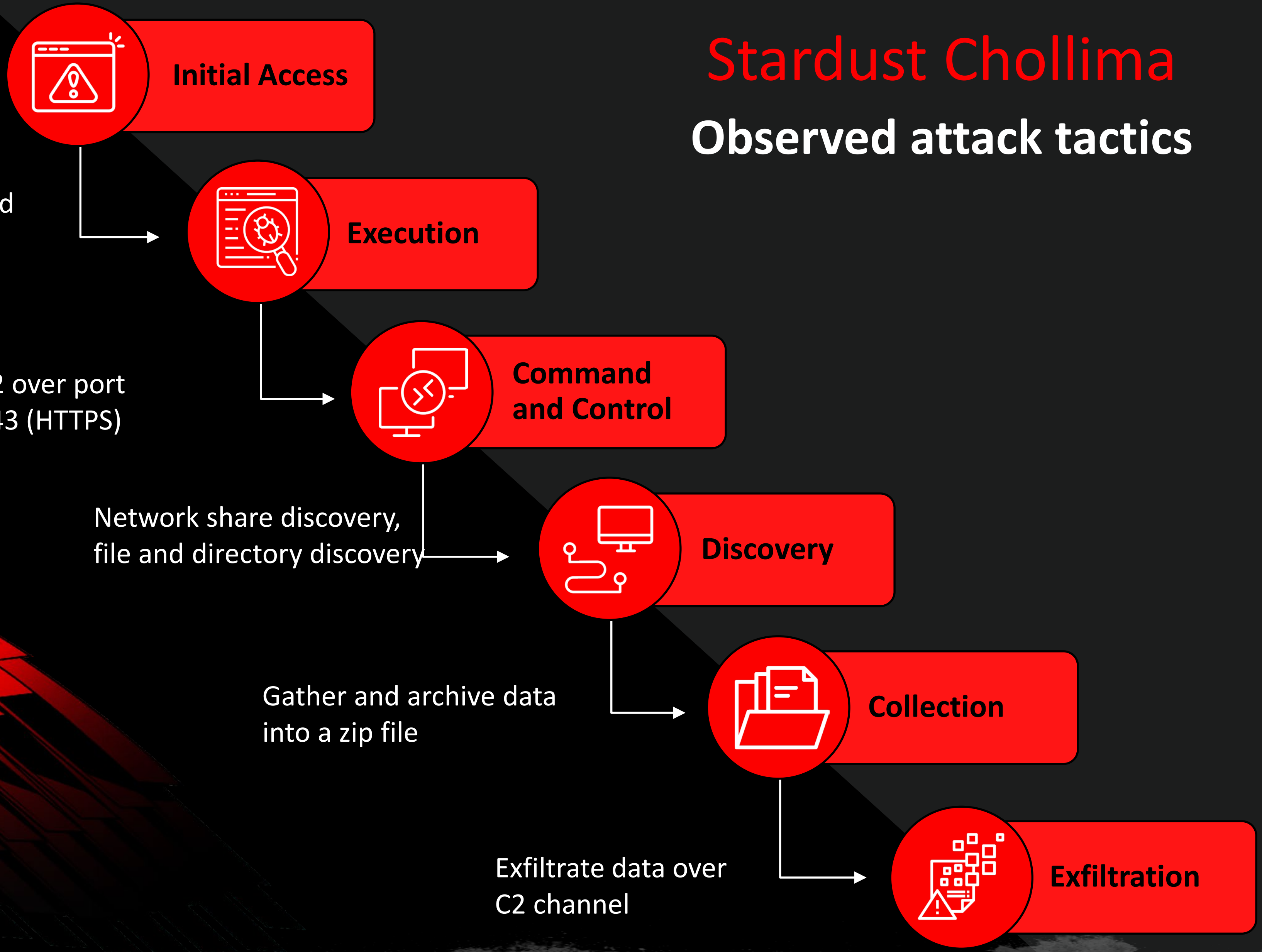
Nov 2015 First observed	6,368[1] Total indicators
Aug 2023 Last observed	224[1] Threat intel reports

[1] As of Aug 25, 2023

CROWDSTRIKE

Stardust Chollima

Observed attack tactics



Initial Access

Social engineering directs victim to download malicious code from a private GitHub repo

Execution

SpeedLog, RCUpdate and SwiftBucket macOS malware

Command and Control

C2 over port 443 (HTTPS)

Discovery

Network share discovery, file and directory discovery

Collection

Gather and archive data into a zip file

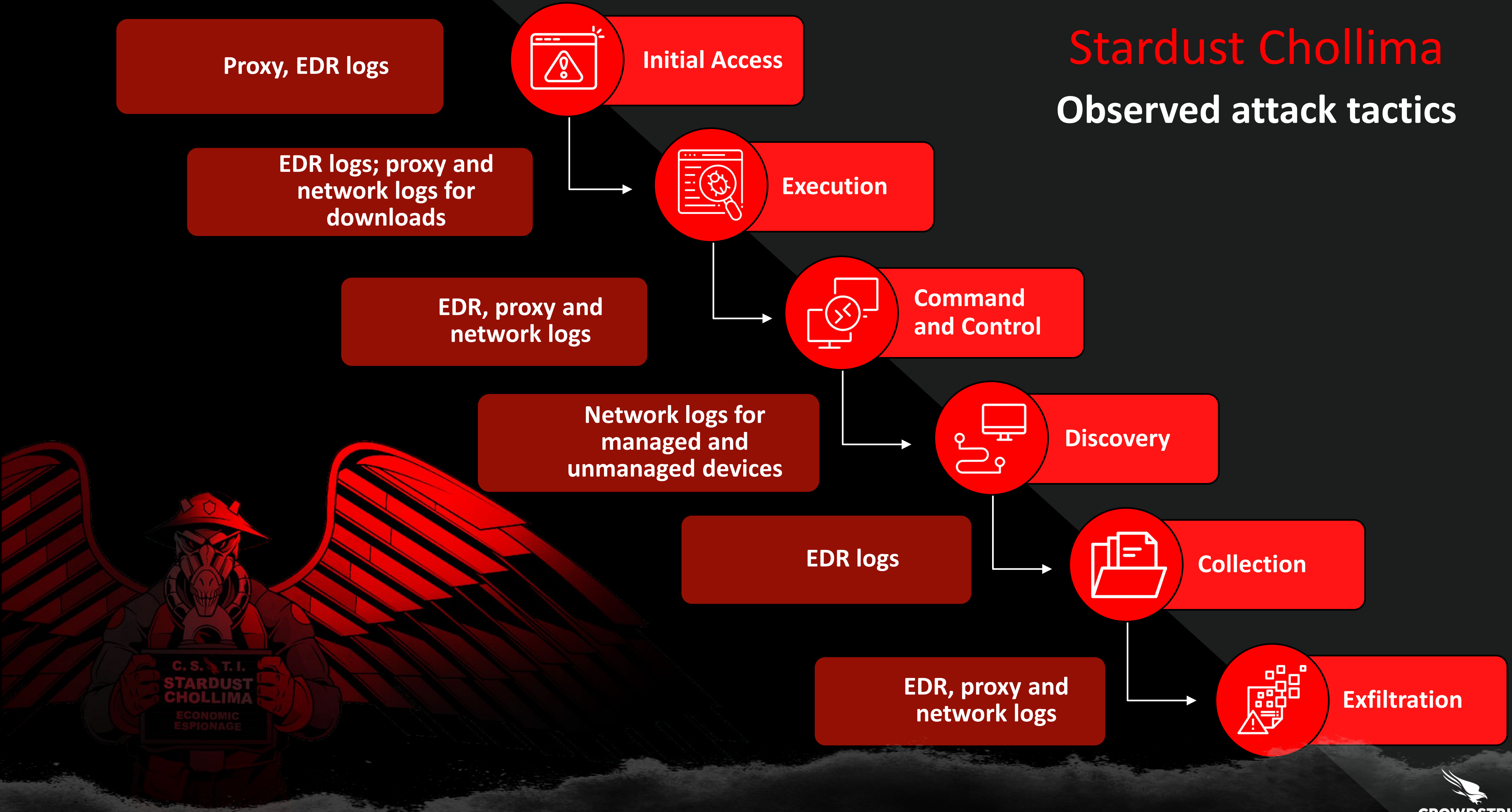
Exfiltration

Exfiltrate data over C2 channel

CROWDSTRIKE

Stardust Chollima

Observed attack tactics



Initial Access

Proxy, EDR logs

Execution

EDR logs; proxy and network logs for downloads

Command and Control

EDR, proxy and network logs

Discovery

Network logs for managed and unmanaged devices

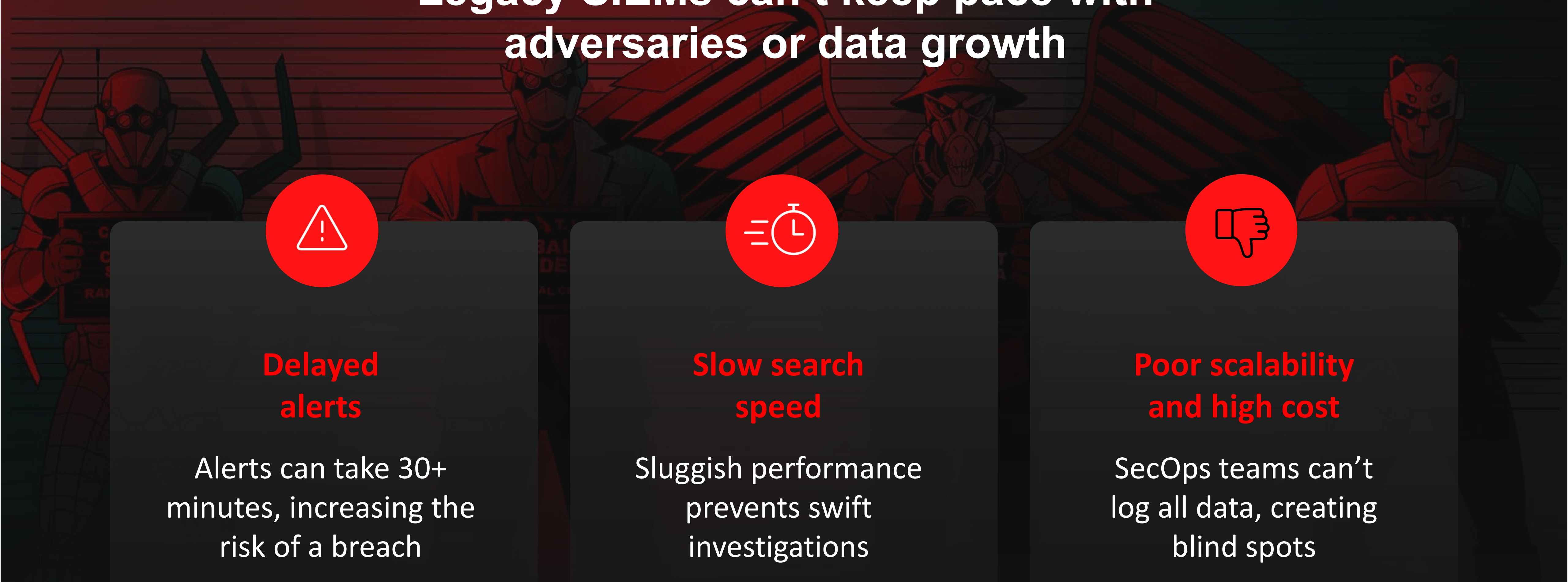
Collection

EDR logs

Exfiltration

EDR, proxy and network logs

Legacy SIEMs can’t keep pace with adversaries or data growth



Delayed alerts

Alerts can take 30+ minutes, increasing the risk of a breach

Slow search speed

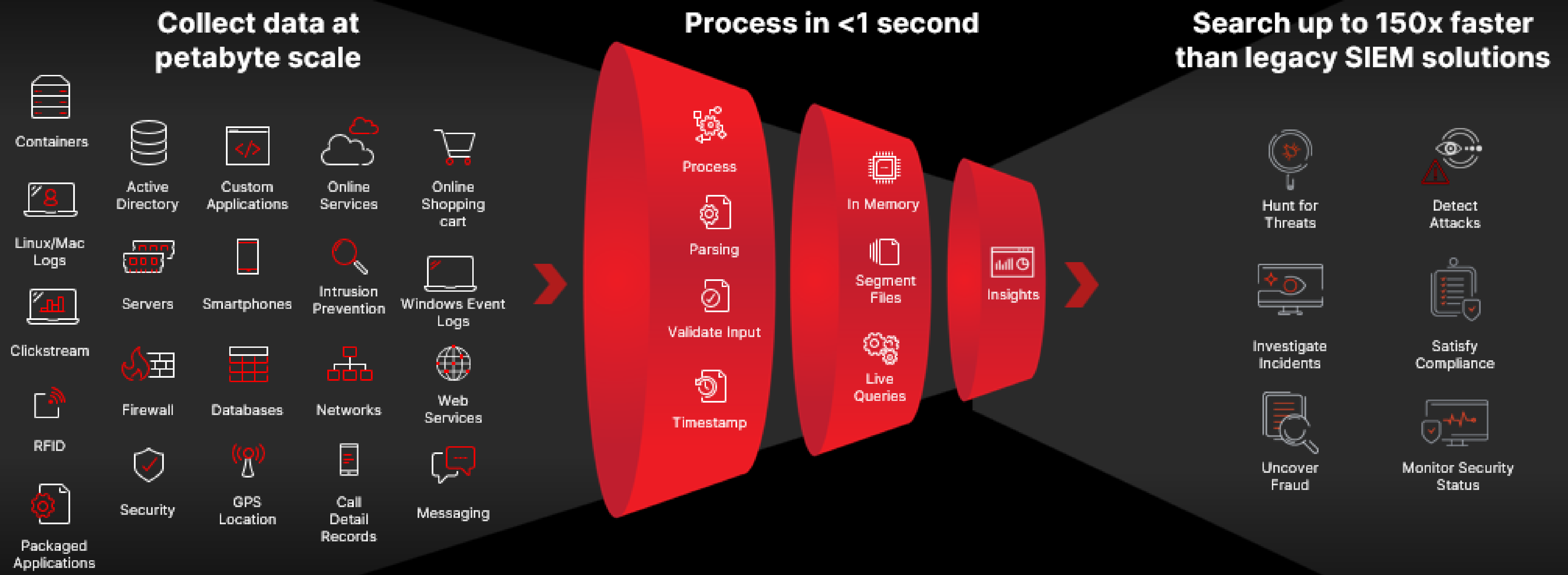
Sluggish performance prevents swift investigations

Poor scalability and high cost

SecOps teams can’t log all data, creating blind spots

Introducing Falcon LogScale

A modern security operations solution delivering real-time visibility and petabyte scale



Collect data at petabyte scale

Containers

Linux/Mac Logs

Clickstream

RFID

Packaged Applications

Active Directory

Servers

Firewall

Security

Custom Applications

Smartphones

Databases

GPS Location

Online Services

Intrusion Prevention

Networks

Call Detail Records

Online Shopping cart

Windows Event Logs

Web Services

Messaging

Process in <1 second

Process

Parsing

Validate Input

Timestamp

In Memory

Segment Files

Live Queries

Insights

Search up to 150x faster than legacy SIEM solutions

Hunt for Threats

Detect Attacks

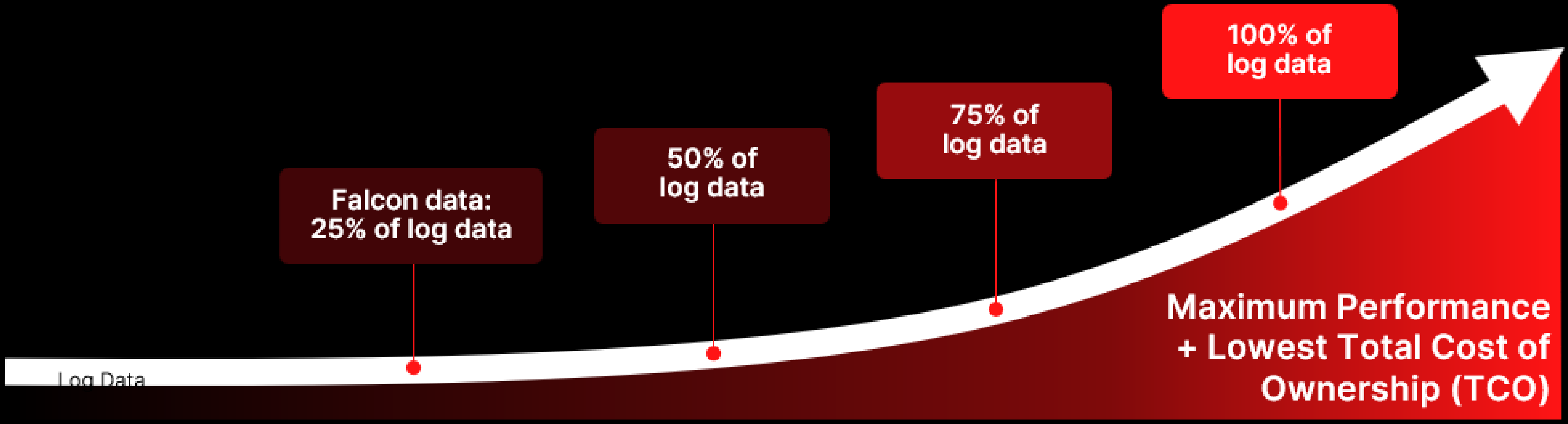
Investigate Incidents

Satisfy Compliance

Uncover Fraud

Monitor Security Status

Migrate from a high-cost SIEM to high-speed Falcon LogScale

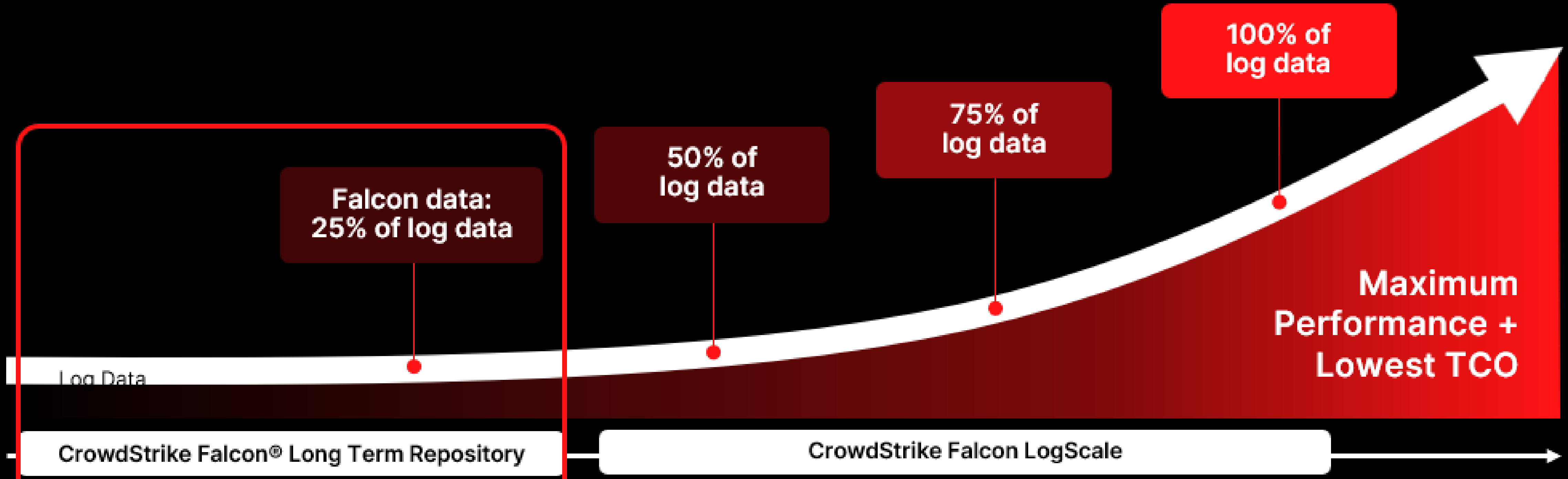

Log Data
Falcon data: 25% of log data
50% of log data
75% of log data
100% of log data
Maximum Performance + Lowest Total Cost of Ownership (TCO)

Migrate data from your SIEM solution to Falcon LogScale

Cost savings	◔	◑	◕	◕
Search speed	◔	◑	◕	●
Visibility	◑	◕	◕	●

CROWDSTRIKE

Migrate from a high-cost SIEM to high-speed Falcon LogScale



Falcon data: 25% of log data

50% of log data

75% of log data

100% of log data

Maximum Performance + Lowest TCO

CrowdStrike Falcon® Long Term Repository

CrowdStrike Falcon LogScale

The easy path to enhanced SecOps

Falcon EDR, identity data

25% SIEM data
Top use cases:

1. Malware
2. Insider threat

Proxy logs

15% SIEM data
Top use cases:

1. Command and control
2. Phishing

Firewall traffic logs

25% SIEM data
Top use cases:

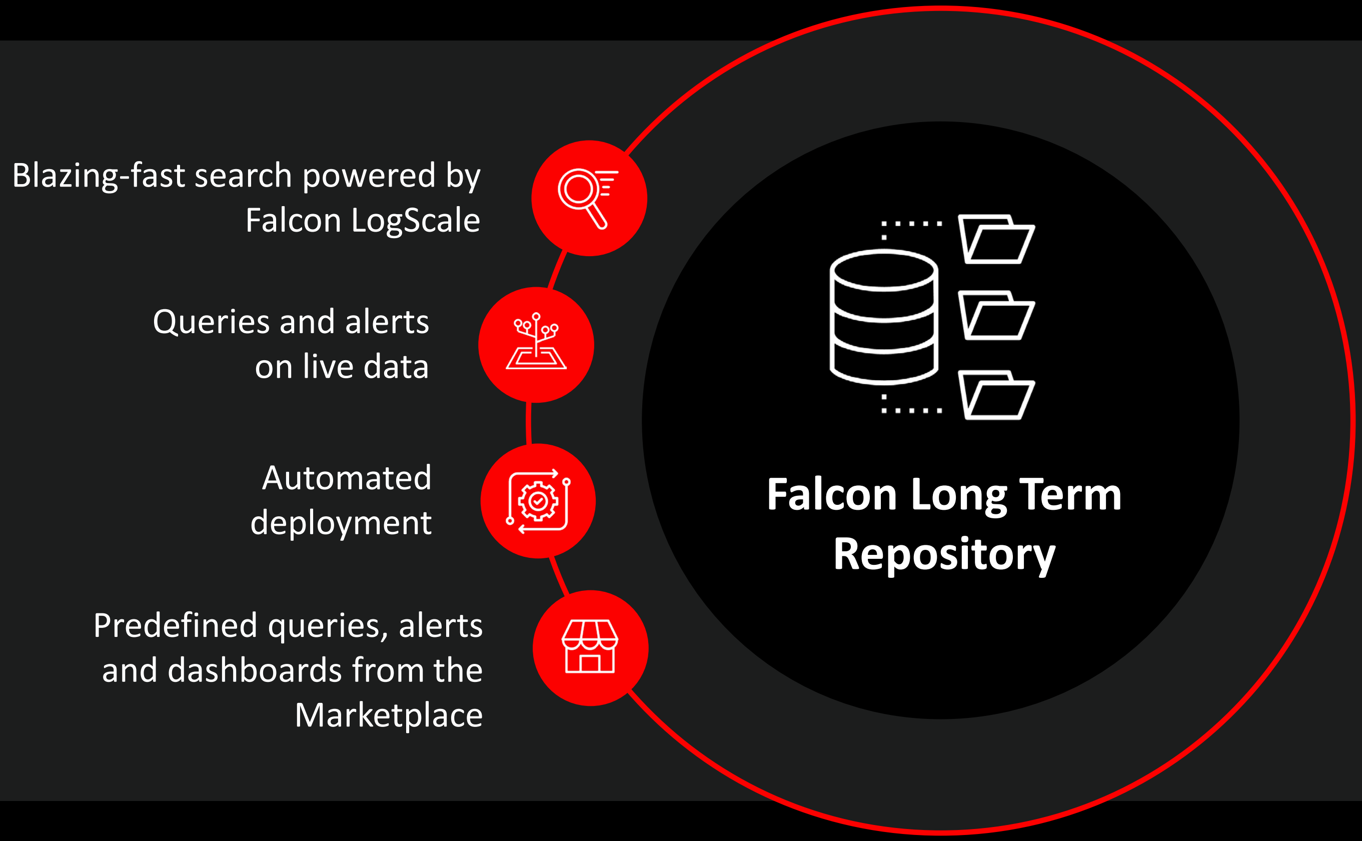
1. Network discovery
2. Command and control

50+

Marketplace packages to ease onboarding

Start your journey with Falcon Long Term Repository

Extend Falcon data retention to months or years for security and compliance



Blazing-fast search powered by Falcon LogScale

Queries and alerts on live data

Automated deployment

Predefined queries, alerts and dashboards from the Marketplace

Falcon Long Term Repository

Business Value

Search faster than legacy SIEM solutions

Reduce SIEM storage costs

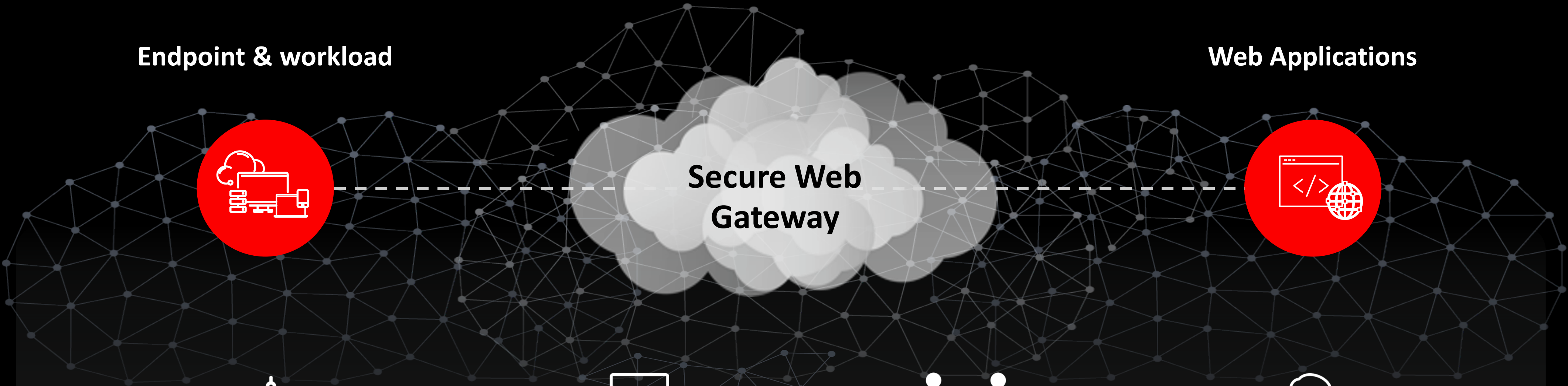
Achieve sub-second latency

Meet compliance

Extend to third-party data with Falcon LogScale

Continue your journey with third-party proxy logs

Move proxy data from your SIEM to Falcon LogScale to increase search speed and cut costs



Hunt for phishing attacks

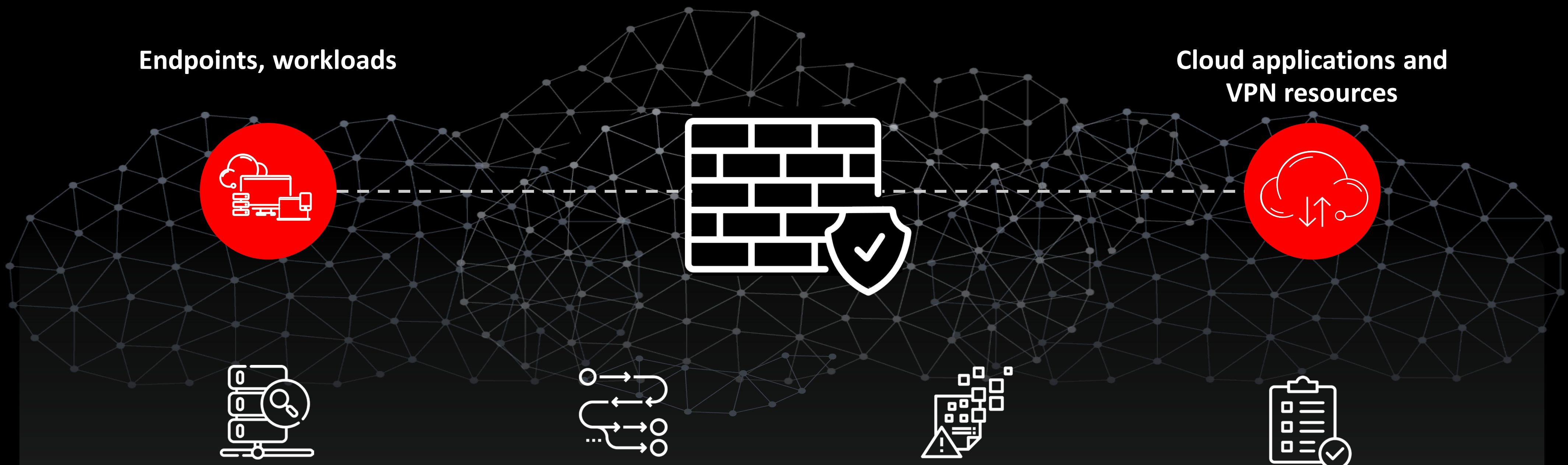
Detect command and control

Monitor web usage to boost productivity

Investigate insider threats

Cut incident response times by collecting firewall logs

Say goodbye to ingestion bottlenecks and dropped packets with petabyte-scale logging



Endpoints, workloads

Cloud applications and VPN resources

Find network discovery such as port scans

Hunt for lateral movement

Analyze north-south traffic for exfiltration

Store logs for compliance

The Future of the Platform

The Raptor Release

- **Modern data foundation:** Upgrades the platform’s data collection, search and storage capabilities
- **Lightning-fast search:** Accelerate hunting and investigations across all data sources
- **Petabyte-scale:** Offers data collection and storage that’s built for the era of AI
- **Generative AI and XDR innovations:** Fuels Charlotte AI, XDR for All, a new detection experience and Next-Gen SIEM

Falcon Next-Gen SIEM: The Future Of The SOC

One Platform

- Integrated EDR, XDR, SIEM, SOAR, ITDR + cloud security
- Affordable, petabyte-scale cloud service
- Time to value and reduced complexity

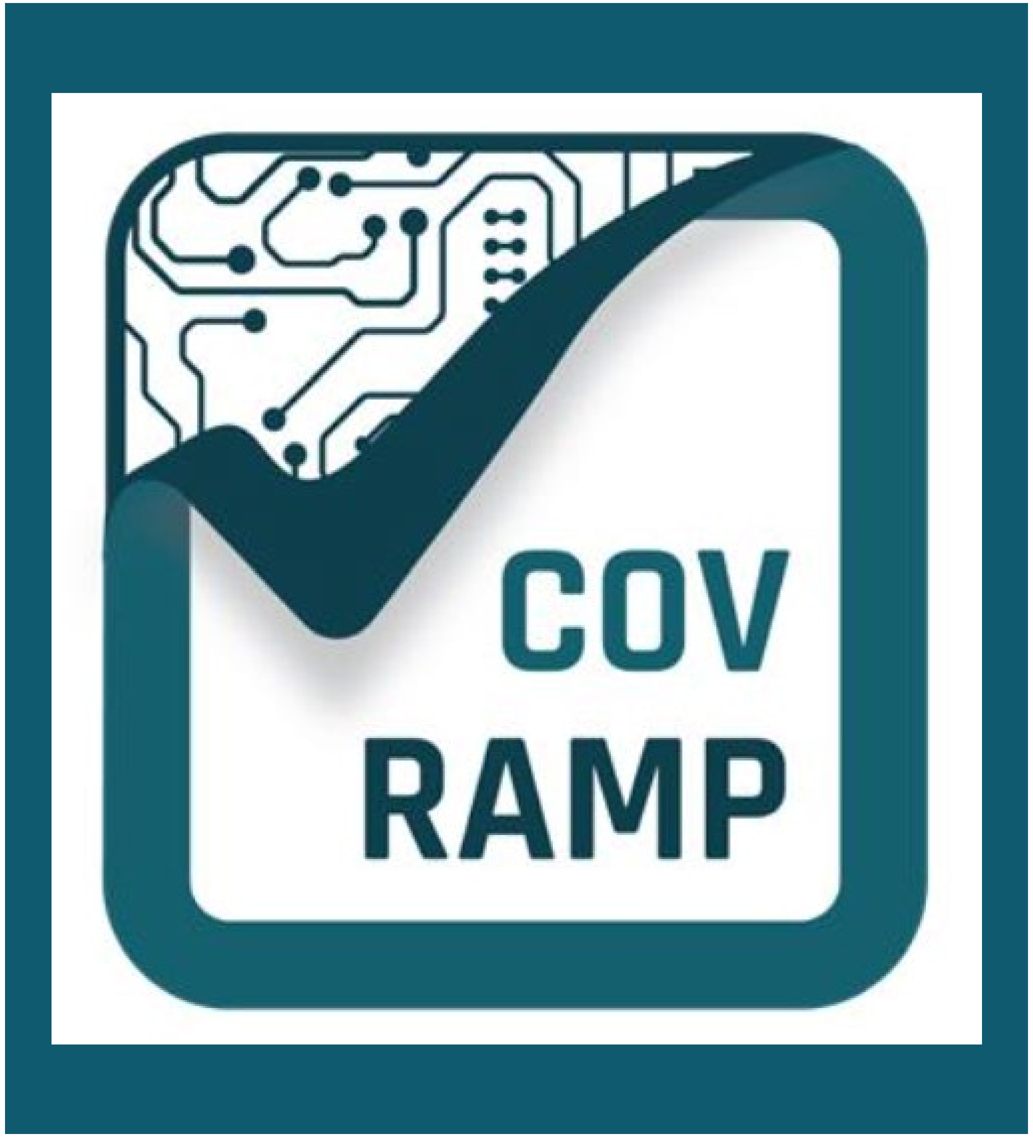
Industry-best Security

- Reduce business risk
- AI-powered EDR, XDR, identity detection models
- Elevated analyst experience
- Automation-first design

Superior Speed

- Real-time alerts and live dashboards to detect threats faster
- Blazing-fast search to accelerate threat hunting

Thank you



VIRGINIA
IT AGENCY

Debut of The COV RAMP Dashboard

Richard White

Director of Security Services and
Product Management

January 10, 2024

Splunk4Rookies Workshop

January 24, 2024

- Attendee's must register by January 16, 2024 for this lunch and learn opportunity.

  Register here

- Location is at VITA's office at the Boulders; however, seats are limited, and are on a first-come, first-served basis for those who register.
- Please bring your laptop for participation in the workshop.

VIRGINIA IT AGENCY

KNOWBE4 PHISHING LESSONS LEARNED

KATHY BORTLE

Manager, Threat Intelligence & Vulnerability Management

ISOAG MEETING

JAN 10TH, 2024

LESSONS LEARNED: USER PROVISIONING

User Provisioning with ADI-SYNC:

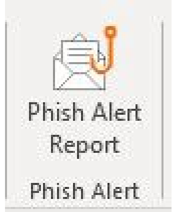
- All Executive Branch agencies that have requested assistance with ADI-Sync have been setup. Any agencies wanting to use ADI-Sync that aren't currently setup, please reach out to us so we can assist you with the setup.
- Any agencies who can't or don't want to use ADI-Sync but would like to have their users updated in KnowBe4 prior to the COV Q1 Phishing Campaign, please let us know.

Lessons Learned:

- Authentication Issues - Agencies should be using a service account with a password set to never expire for the ADI-Sync process. The ADI-Sync installation embeds the credentials in the configuration. If the password changes, the configuration utility must be re-run to incorporate the new credentials.
- Account Archiving Issues - Any users that do not have a valid email address or whose AD account is disabled will be archived by the ADI-Sync Utility. If these users need to be enabled in KnowBe4, the management of these accounts by ADI-Sync must be disabled. Any users that were archived by mistake, can be re-activated by unarchiving the account. All student records will remain intact.

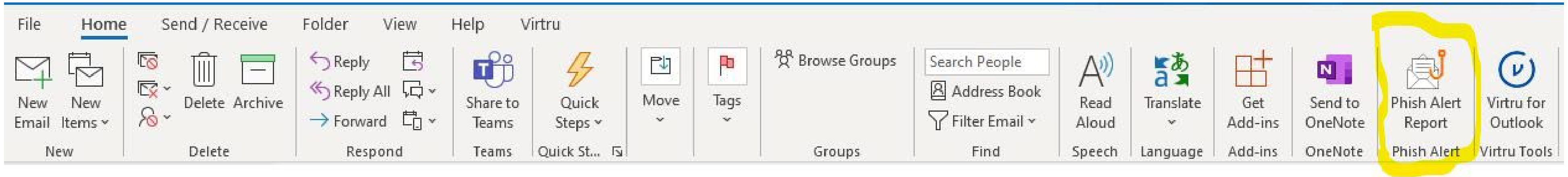
LESSONS LEARNED: PAB BUTTON

Phishing Alert Button (PAB) -



- **PAB Button Availability** – All agencies should have received the PAB button and should be instructing their users to utilize it when reporting SPAM/Phishing Messages.

- **PAB Button Location** differs by client –
  - Full Windows Desktop Client - the PAB button resides on the ribbon bar.

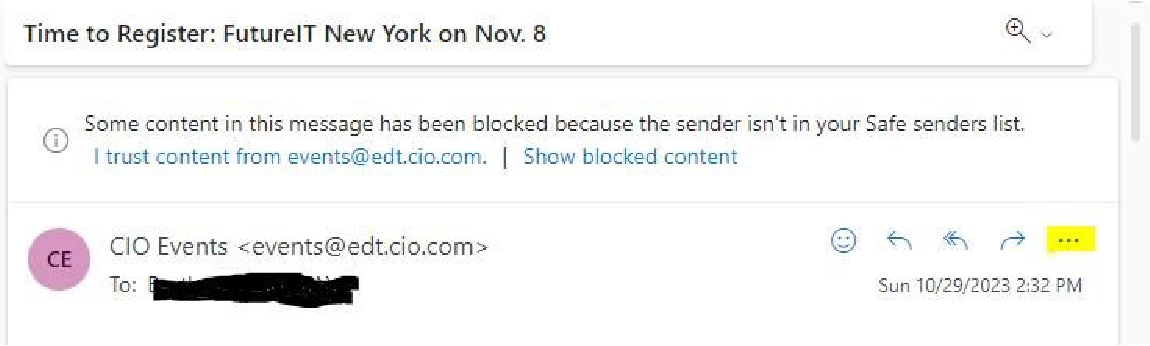


  - Web and Mobile Clients - the PAB button resides in the “More Actions” menu.

Phishing Alert Button (PAB) – More Actions Menu (web and mobile clients)

To access this menu option, you will need to do the following:

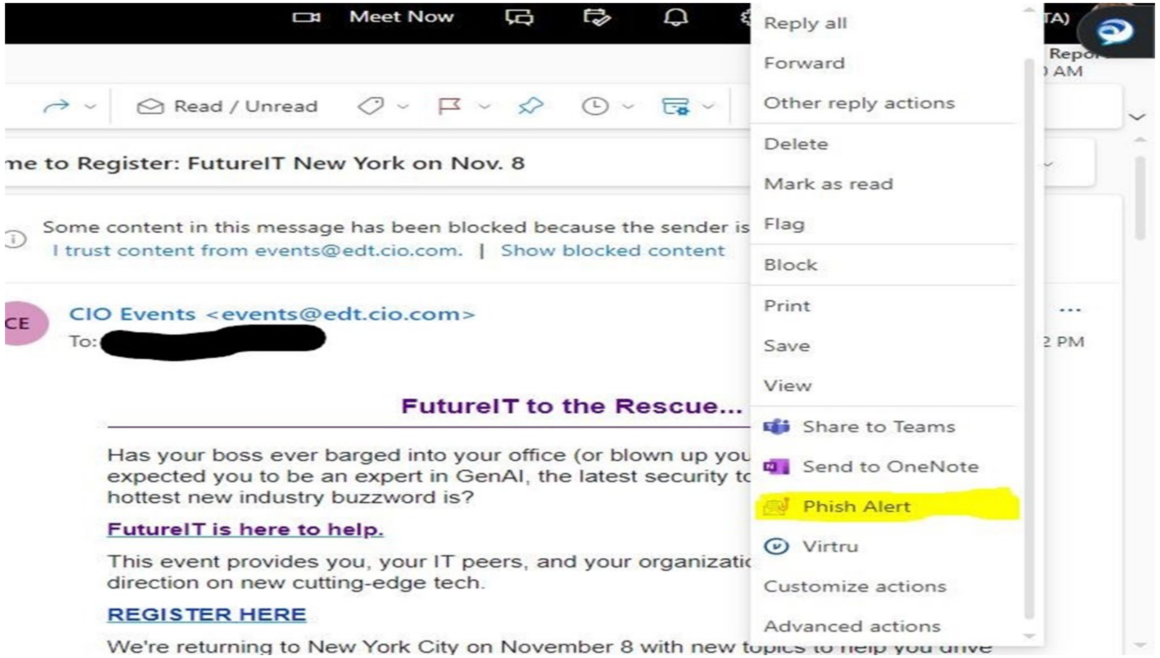
1. Open the message
2. Click on the three dots next to the sender's name. This launches the More Actions Menu.
3. Scroll down the menu until you see ""Phish Alert"
4. Click on Phish Alert
5. In the Phish Alert window that opens, select "Phishing/Suspicious" or "Spam" then click the button at the bottom of the window to submit.



Time to Register: FutureIT New York on Nov. 8

Some content in this message has been blocked because the sender isn't in your Safe senders list.
I trust content from events@edt.cio.com. | Show blocked content

CE CIO Events <events@edt.cio.com>
To: [redacted]
Sun 10/29/2023 2:32 PM



me to Register: FutureIT New York on Nov. 8

Some content in this message has been blocked because the sender is
I trust content from events@edt.cio.com. | Show blocked content

CE CIO Events <events@edt.cio.com>
To: [redacted]

FutureIT to the Rescue...

Has your boss ever barged into your office (or blown up you
expected you to be an expert in GenAI, the latest security to
hottest new industry buzzword is?

FutureIT is here to help.

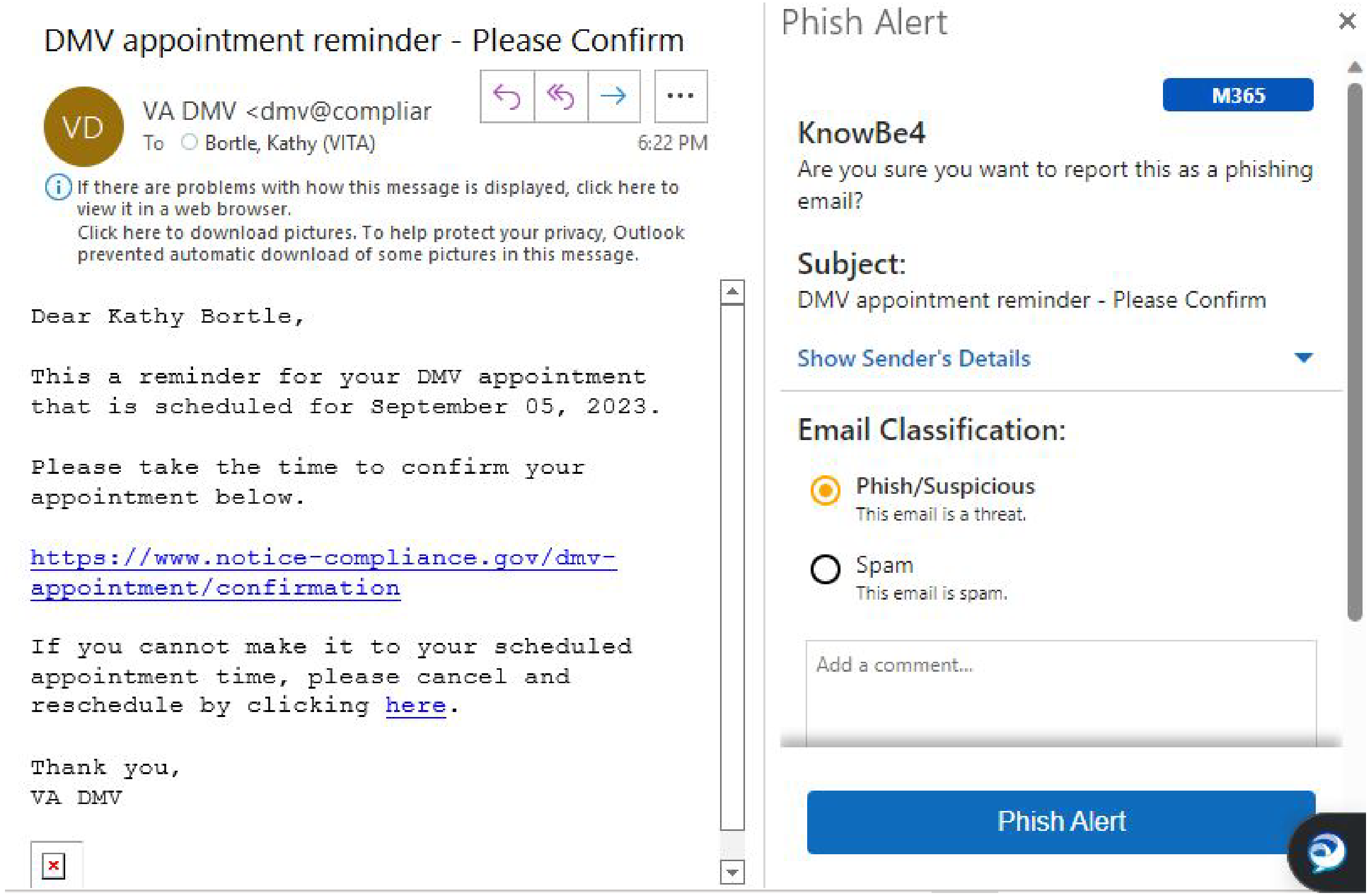
This event provides you, your IT peers, and your organizatio
direction on new cutting-edge tech.

REGISTER HERE

We're returning to New York City on November 8 with new topics to help you drive

LESSONS LEARNED: PAB BUTTON

PAB Button Window



DMV appointment reminder - Please Confirm

VA DMV <dmv@compliar

To ○ Bortle, Kathy (VITA)

6:22 PM

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

```
Dear Kathy Bortle,

This a reminder for your DMV appointment
that is scheduled for September 05, 2023.

Please take the time to confirm your
appointment below.

https://www.notice-compliance.gov/dmv-
appointment/confirmation

If you cannot make it to your scheduled
appointment time, please cancel and
reschedule by clicking here.

Thank you,
VA DMV
```

Phish Alert

M365

KnowBe4

Are you sure you want to report this as a phishing email?

Subject:
DMV appointment reminder - Please Confirm

Show Sender's Details

Email Classification:

● Phish/Suspicious
This email is a threat.

○ Spam
This email is spam.

Add a comment...

LESSONS LEARNED: PAB BUTTON (CONT.)

- PAB Button Terminology ---

  Phishing/Suspicious messages are an attempt by the phisher to solicit an action from the user. This may be in multiple ways that does not necessary require a user to click on a link. Here's some example of how attackers can solicit an action from the user:

  - Phone - Please contact me via phone at (999) 999-9999 to provide the information requested.
  - Email - Please email me your contact information so we can process your request.
  - Link Click - Please click on this link below to validate your account.
  - Scan QR Code - Please scan the QR code to register for your discounted interest rate
  - Open document – Please open the following attachment to see how much you have received for your Christmas bonus.

  Spam messages are normally unwanted emails that the user received. These messages are normally benign in nature and more of a nuisance than a threat. Examples of Spam messages include:

  - Marketing literature
  - Newsletters
  - Advertisements
  - Chain letters

LESSONS LEARNED: PAB BUTTON (CONT.)

- PAB Button Message Processing ---

  Campaign Messages reported via PAB --- KnowBe4 keeps track of the messages it sends as part of a phishing campaign. When a user reports one of these messages, it pops up a window "congratulating" the user from passing the phishing test. The window automatically stays open for 30 seconds to give the user a chance to read it. KnowBe4 then records it in the user's security awareness training record that they reported the message. The window closes and no further processing occurs.

  Non-Campaign messages reported via PAB –

  When the user clicks on the PAB button a window will open asking them if the message that they are reporting is "Phishing/Suspicious" or "Spam".

  - Messages reported as SPAM are sent to the incidents@vita.virginia.gov mailbox where the user receives an automated reply thanking them for their submission and instructing them on how to block it in their own mailboxes.

  - Messages reported as "Phishing/Suspicious" are sent to the VCCC. The VCCC has an automated process that looks for "Phish Alert" in the message subject. This tells KSE it is a phishing ticket. It automatically creates the KSE ticket and attaches a copy of the email with the headers to the ticket. The ticket is then routed to the SOC for investigation.

LESSONS LEARNED: PAB BUTTON (CONT.)

PAB Button Automated Processing issues –

While we have automated these processes to minimize the effort involved with running standard phishing campaigns, it appears that we have some issues that have surfaced. They are as follows:

1. **Calling/Emailing the VCCC instead of using the PAB button** to report the message. The VCCC has been instructed to instruct the user to re-submit their request via PAB and then close the ticket as a First Contact Resolution. Since the user circumvented the PAB button process, the automated processing of these tickets cannot occur. All information needed to investigate the report will not be available and the SOC will not be automatically notified of the report.

2. **Forwarding the messages to the VCCC instead of using PAB** – Messages that are forwarded to the VCCC, do not include the “Phish Alert” text in the subject. This breaks the automated process that creates the KSE ticket and forward it to the SOC for investigation. In addition, the forwarded message changes the original message headers and may not include everything that is needed to investigate the reported message.

To allow these automated processes to provide a timely response to reported messages, please encourage all users to use the PAB button. If the PAB button is not available, please have the user open a ticket to get their account fixed.

Phishing Campaign

- Phishing Beta – Opting into this module prevents an account from participating in a non-beta campaign.

- False Positives - false positives are triggered when the message and/or it's links are scanning. Domains must be whitelisted everywhere that the message can be scanned.

- Random Domain selection for sender, links and landing pages – KnowBe4 will pick any domain that is available in the console. If a domain has not been whitelisted, it needs to be hidden. Any domain that is not hidden can be used by this feature. If the domains in the list are not whitelisted, it can trigger a false positive for clicks.

- Downloading Pictures in messages – the Outlook client is configured to prevent the automatic downloading of pictures in the emails. This affects KnowBe4's ability to track whether the message has been opened. The only opened stats that are reliable are for those messages where the user clicked the link, opened an attachment or submitted data. When the user takes one of these actions, the system automatically marks the message as opened. Therefore, opened should not be included in any phishing test reports.

False Positives for Q4 2023 –

When setting up the Q4 campaign, I missed changing the sender's domain on 5 of the 10 messages used. While I tested all the messages to my team's accounts, this was not a sufficient volume for MS Defender to kick in and scan the messages that weren't whitelisted. As a result, when the campaign was launched to 65K users, it triggered MS Defender and caused the false positives. The Q4 campaign will be hidden from your phishing results as to not skew the numbers.

After working with NTTDATA on the false positives, they have asked if we can do another COV wide campaign in January to verify that all our whitelisting is working as required.

How NOT to create a Phishing Campaign –

Over the past six months we have discovered many ways to create phishing campaigns that were plagued with false positives. Some of which include the following:

- Lack of communication – when a large number of phishing messages are reported, this can trigger domains to be blocked . As blocks can be submitted by the SOC, NTTDATA and Area 1, the messaging staff may implement the block request if they are unaware of the authorized phishing campaign.
  - Lesson Leaned – notification to the ISOs only is insufficient. In addition to notifying the ISO, CSRM, the MSI and the service towers also need to know that an authorized phishing campaign is being conducted.
- Failure to configure KnowBe4 to hide non-whitelisted domains. - KnowBe4 is purchasing new domains on a routine basis. When the domains are purchased, they are automatically added to the KnowBe4 management console.
  - Lesson Learned - KnowBe4 will use any active domain as part of a campaign when the Random option is selected. This can cause False positives to occur. To prevent this, the new domains need to be hidden or a specific whitelisted domain must be selected in the template.

HOW "NOT" TO CREATE A PHISHING CAMPAIGN

- **Failure to change the Sender's domain in KnowBe4 (KB4) templates –** KB4 templates come with an email address and reply-to address automatically configured in the template. These email addresses can belong to any domain that KnowBe4 owns. Therefore, they may not be using one of the domains that we have whitelisted for our environment.
    - **Lesson Learned** – Testing these messages with a small number of accounts won't trigger Microsoft Defender. However, when sending to the entire COV, there are a sufficient number of messages to trigger Microsoft Defender to scan the messages. The only way to prevent MS Defender from scanning the messages is to use a whitelisted domain for the "Sender and Reply-To" addresses.
- **Failure to change the Landing Page's domain** – KnowBe4 templates also come with a pre-configure Landing Page domain. This domain needs to be changed to one of the whitelisted domains to allow the user to get to the landing page.
    - **Lesson Learned** – Failing to select a whitelisted domain means that the web gateway may block the landing page. KnowBe4 won't know that the access was blocked, it may record the attempt as a false positive.

How to create a Phishing Campaign –

In order to create a phishing campaign, you must first customize the email templates and landing pages (if desired) that will be used in the campaign.

When an agency creates a phishing campaign, they can select any of the pre-defined email templates and landing pages or they can create their own.   These templates come with a pre-defined level of difficulty and default settings However, due to the size and complexity of the COV environment, most of these templates will require modification before use.

There are 5 difficulty levels defined by the number of stars attached to the template.   The templates cover many industries, current events, attack types, etc.   The ISO should consider all these options when selecting a template for their campaign.   Once the template has been selected, the following information should be examined:

- Domain address for the sender’s address.
- Domain address for the reply to domain
- Domain address for the landing page

HOW "TO" CREATE A PHISHING CAMPAIGN

Modifying an email template for use in the COV environment -

Does the email template use one of the whitelisted domains in the sender and reply-to addresses?

YES - no modification is required.

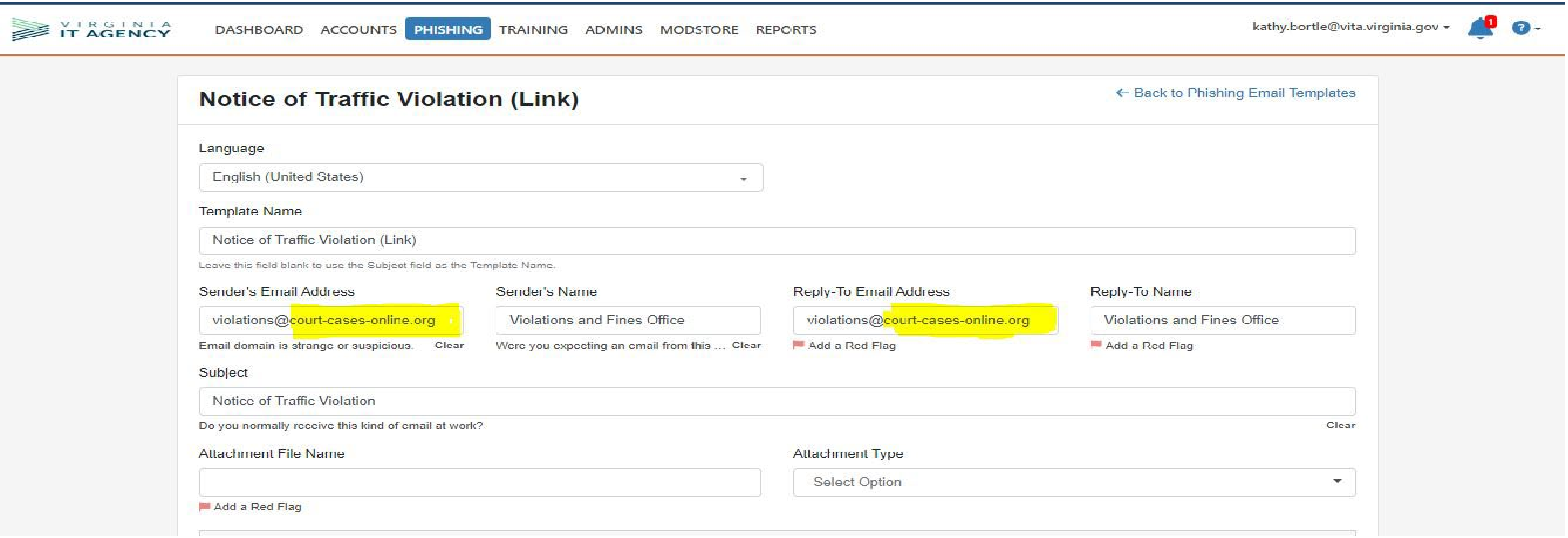
NO - change the sender and reply to addresses to use a whitelisted domain.

The next two slides show where the changes need to be made. These areas are highlighted in yellow to show the part of the addresses that need to be changed.

If you need to refer to the list of whitelisted domains, they can be found on the ISO Knowledge Center SharePoint site (https://covgov.sharepoint.com/sites/VITASec/ISOKnowledgeSharing/SitePages/Home.aspx)

HOW “TO” CREATE A PHISHING CAMPAIGN

Modifying sender and reply to email addresses –



Notice of Traffic Violation (Link)

Language

English (United States)

Template Name

Notice of Traffic Violation (Link)

Leave this field blank to use the Subject field as the Template Name.

Sender's Email Address: violations@court-cases-online.org

Email domain is strange or suspicious. Clear

Sender's Name: Violations and Fines Office

Were you expecting an email from this ... Clear

Reply-To Email Address: violations@court-cases-online.org

Add a Red Flag

Reply-To Name: Violations and Fines Office

Add a Red Flag

Subject

Notice of Traffic Violation

Do you normally receive this kind of email at work? Clear

Attachment File Name

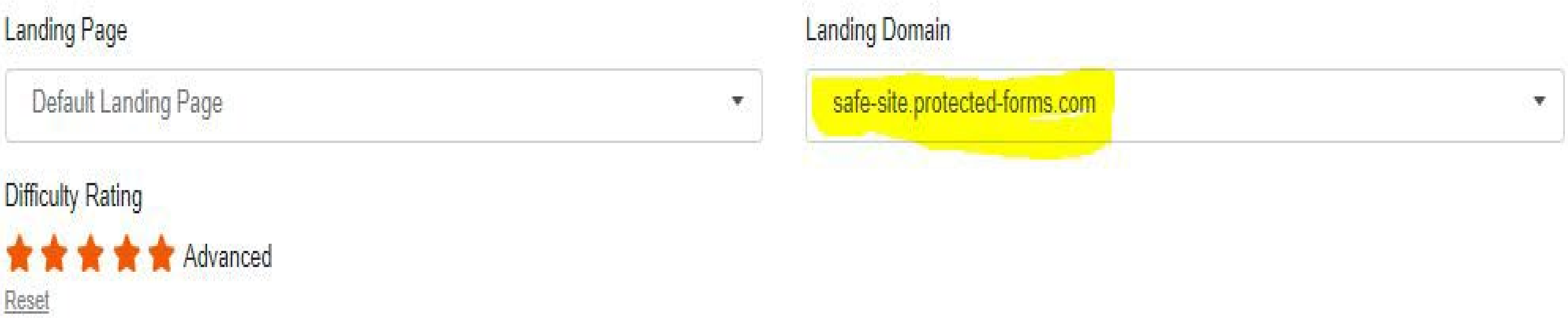
Add a Red Flag

Attachment Type

Select Option

Modifying a landing page’s domain address –

Use the down arrow to select one of the address that is in the whitelist.



Landing Page: Default Landing Page

Landing Domain: safe-site.protected-forms.com

Difficulty Rating: ★★★★★ Advanced

HOW "TO" CREATE A PHISHING CAMPAIGN

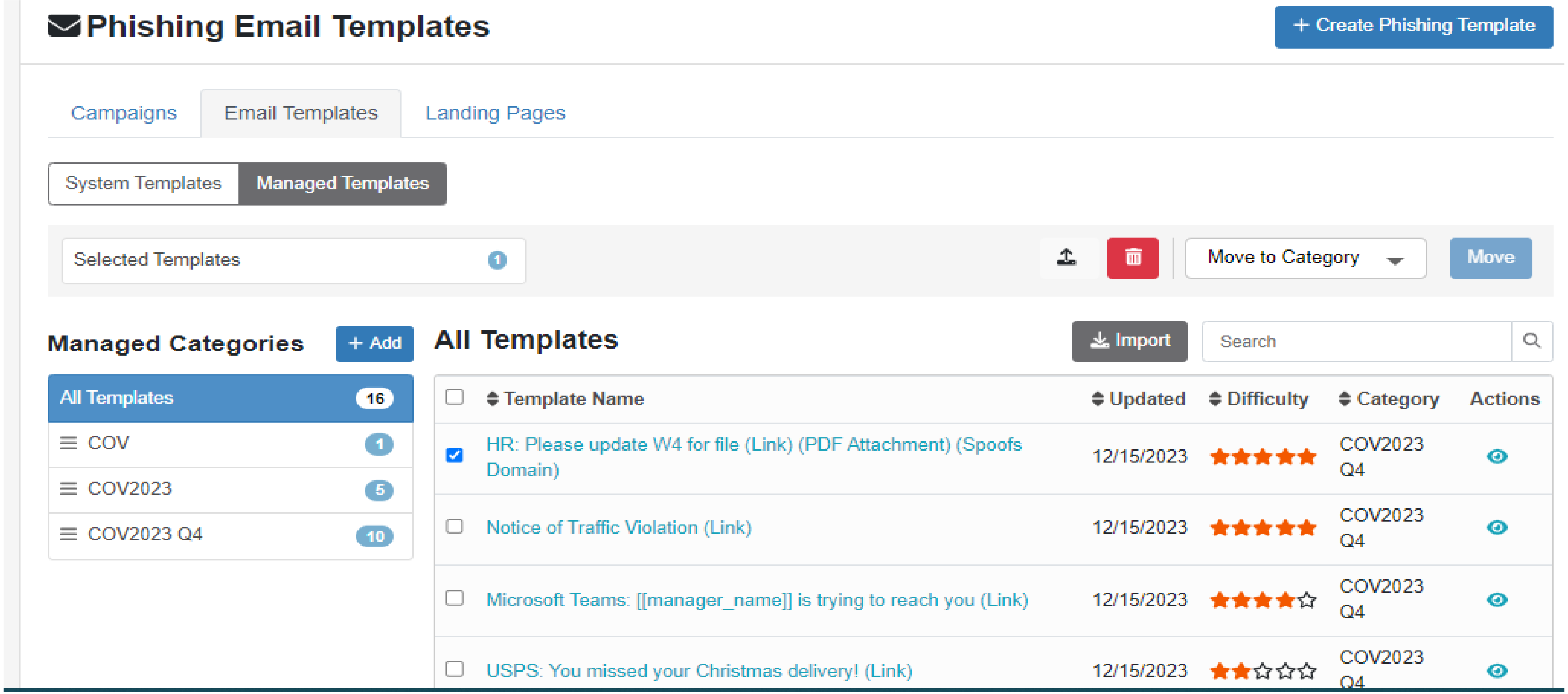
Completing your customized templates

When you have finished modifying the template, click the "save" button and save it with a new name.

To Organize the templates for ease of use…

1. Click on the Add Button beside "Manage Templates". This will create a new category for your templates.
2. Name the template category and save it.
3. Check the checkbox next to the template you modified.
4. Use the down arrow beside the "Move to Category" field to select the category you want to use.
5. Click the "Move" button the place the email template in that category
6. The template will be moved to the selected category.

* Note: When creating a phishing campaign, email templates can be selected by "category" . Creating a new category for each campaign will make it easy to select the messages to be used in the campaign.



Phishing Email Templates

Managed Categories	
All Templates	16
COV	1
COV2023	5
COV2023 Q4	10

All Templates

□	Template Name	Updated	Difficulty	Category	Actions
☑	HR: Please update W4 for file (Link) (PDF Attachment) (Spoofs Domain)	12/15/2023	★★★★★	COV2023 Q4	👁
□	Notice of Traffic Violation (Link)	12/15/2023	★★★★★	COV2023 Q4	👁
□	Microsoft Teams: [[manager_name]] is trying to reach you (Link)	12/15/2023	★★★★☆	COV2023 Q4	👁
□	USPS: You missed your Christmas delivery! (Link)	12/15/2023	★★☆☆☆	COV2023 Q4	👁

Landing Pages

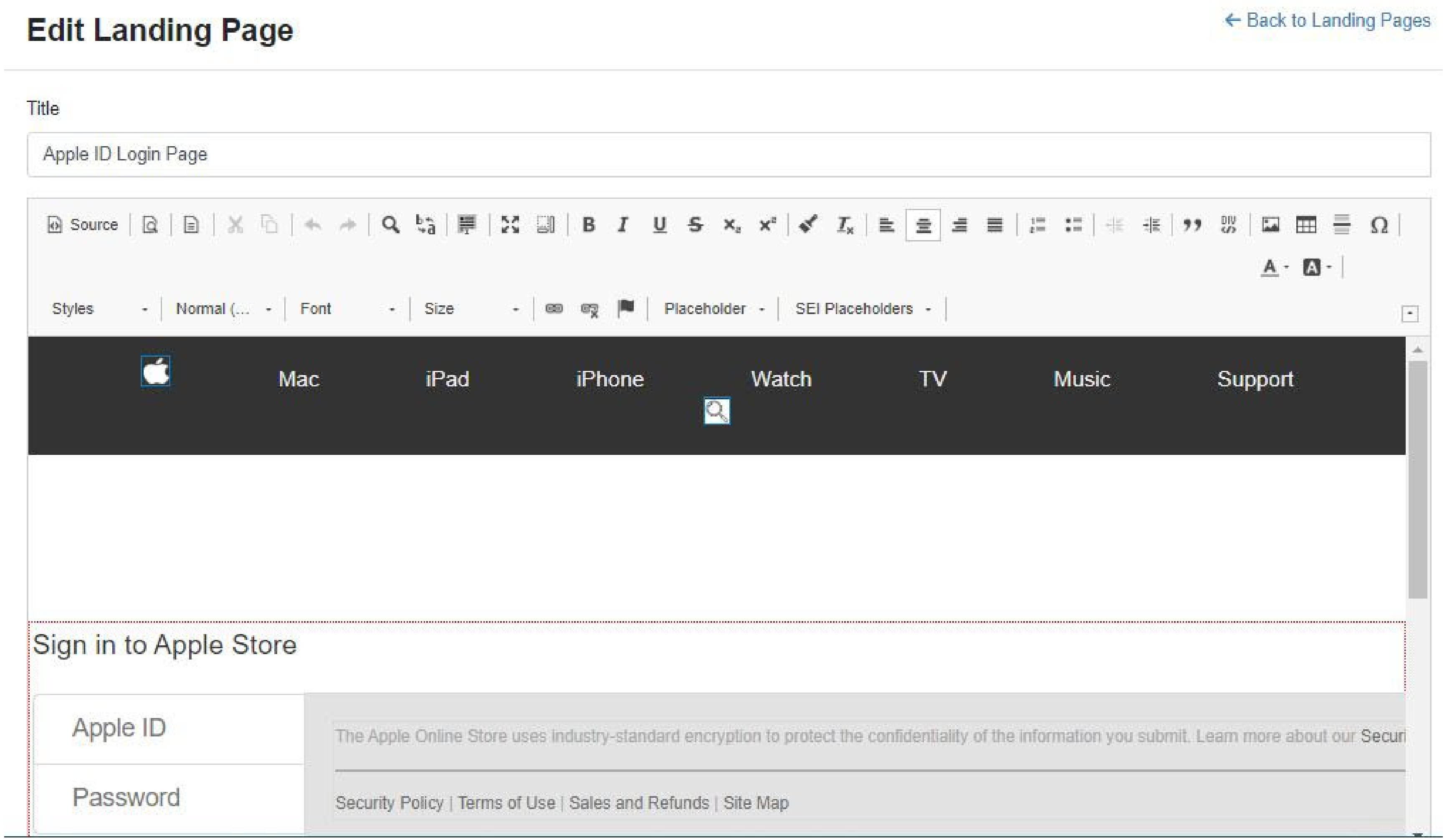
Landing Pages are web pages that will be displayed when a user takes an action on a phishing campaign message. To customize the landing page, first add it to the category you want to use. If the category doesn't exist, you will need to use the "Add" button to create it.

This works the same way as creating the category for Email templates.

Once the landing pages are added to the categories, they can be modified by clicking on the category name, then the name of the template.

This brings up the Edit Landing Page Window where you can customize the page. When finished click on the "Update" button to save your changes.

HOW "TO" CREATE A PHISHING CAMPAIGN



Edit Landing Page

← Back to Landing Pages

Title

Apple ID Login Page

Sign in to Apple Store

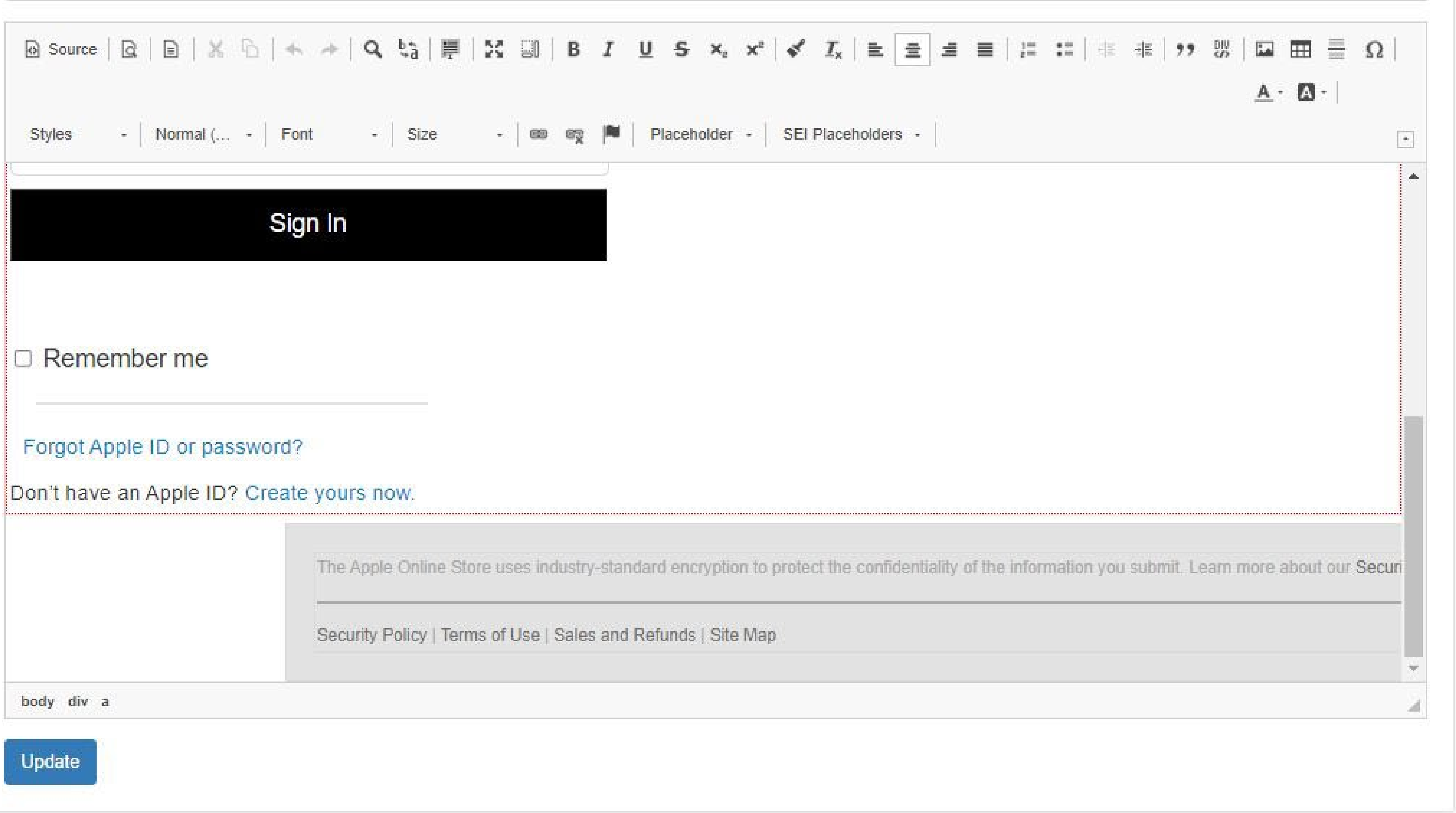
Apple ID

Password

The Apple Online Store uses industry-standard encryption to protect the confidentiality of the information you submit. Learn more about our Securi

Security Policy | Terms of Use | Sales and Refunds | Site Map

HOW "TO" CREATE A PHISHING CAMPAIGN



Sign In

□ Remember me

Forgot Apple ID or password?

Don't have an Apple ID? Create yours now.

The Apple Online Store uses industry-standard encryption to protect the confidentiality of the information you submit. Learn more about our Securi

Security Policy | Terms of Use | Sales and Refunds | Site Map

HOW “TO” CREATE A PHISHING CAMPAIGN

Creating a Campaign

Now that you have setup the email templates and the landing pages that you want to use, you are ready to create a campaign.

1. Click on the “Phishing” option from the menu bar across the top of the console.
2. The “Phishing Overview” page will appear.
3. On the Phishing Overview page, click on the “Campaigns” tab.
4. This opens the “Phishing Security Test Campaigns” window.
5. In the top right corner, there will be a button called “+Create New Campaign”.
6. Click on the “+Create New Campaign” button.

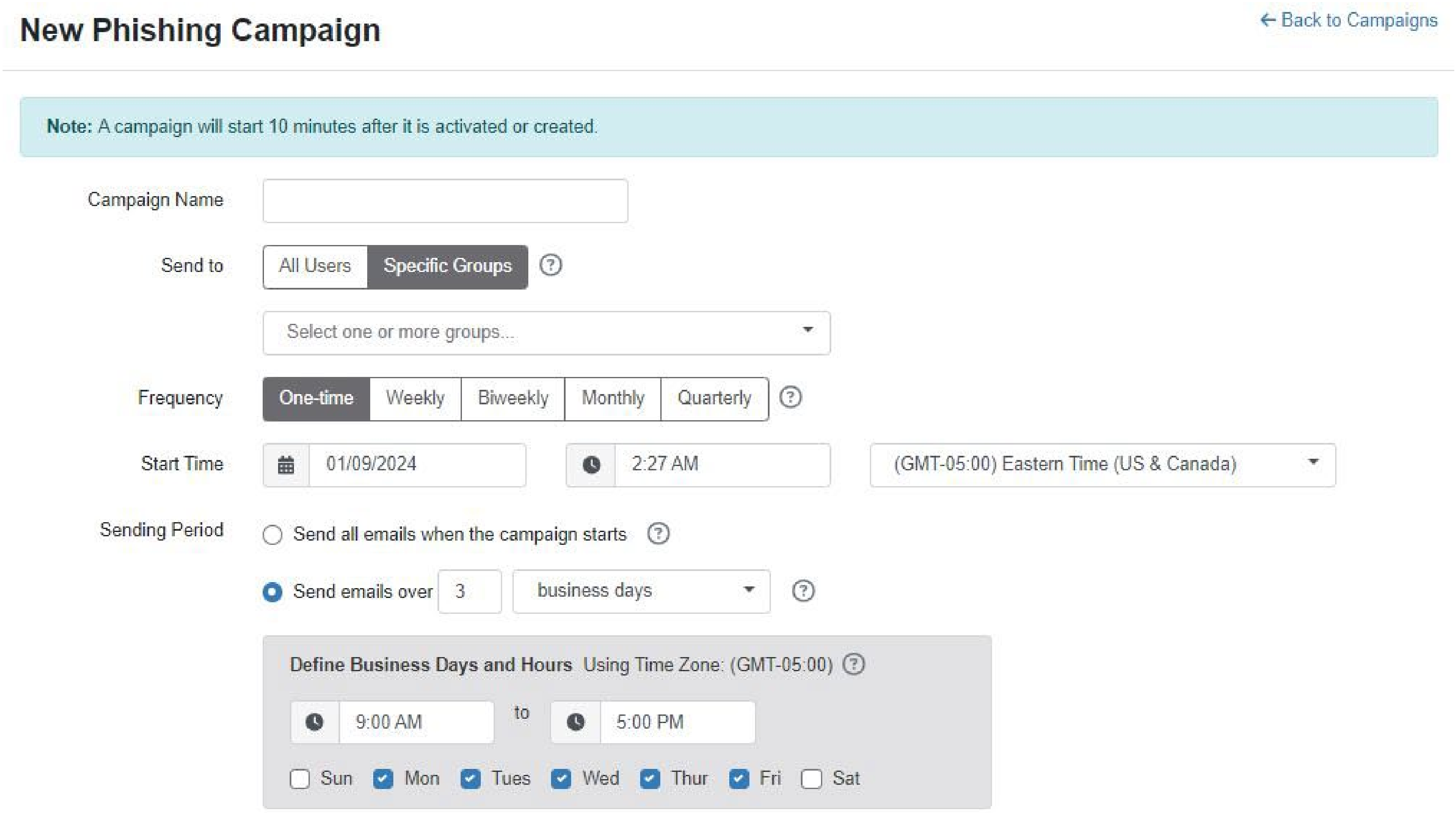
The “New Phishing Campaign Window” opens with a green banner indicating that the campaign will launch 10 minutes after it is activated or completed.

HOW “TO” CREATE A PHISHING CAMPAIGN

To create the campaign, you will need to provide the following information:

- Name for the campaign
- Select the users that are to receive the campaign
- Select the frequency for the campaign
- Select the date/time for the campaign to start
- Select the sending period options

HOW "TO" CREATE A PHISHING CAMPAIGN



New Phishing Campaign

← Back to Campaigns

Note: A campaign will start 10 minutes after it is activated or created.

Campaign Name:

Send to: All Users | [✓ Specific Groups] ?

Select one or more groups...

Frequency: [✓ One-time] | Weekly | Biweekly | Monthly | Quarterly ?

Start Time: 01/09/2024 | 2:27 AM | (GMT-05:00) Eastern Time (US & Canada)

Sending Period:

○ Send all emails when the campaign starts ?

● Send emails over 3 business days ?

Define Business Days and Hours Using Time Zone: (GMT-05:00) ?

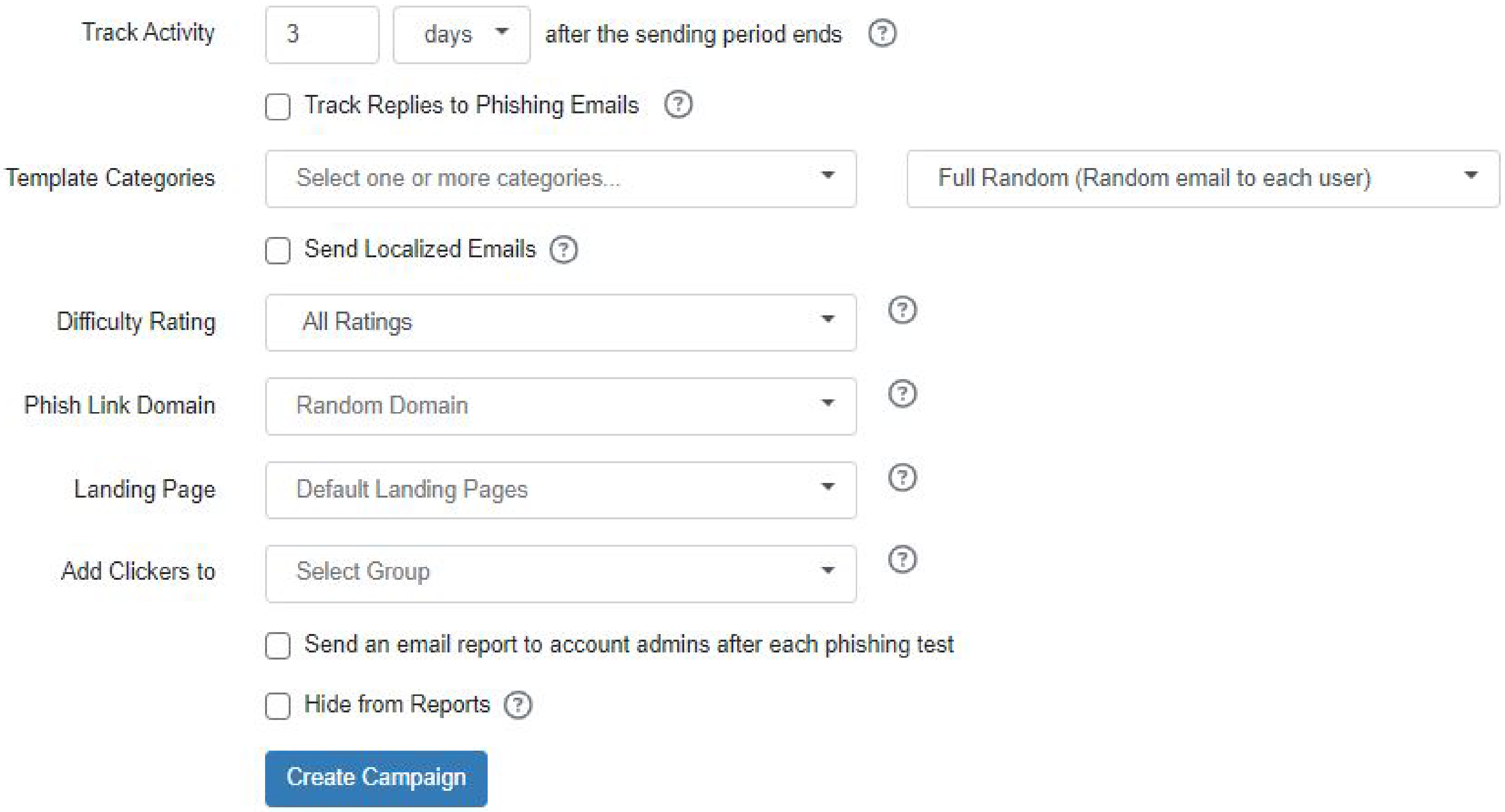
9:00 AM to 5:00 PM

☐ Sun ☑ Mon ☑ Tues ☑ Wed ☑ Thur ☑ Fri ☐ Sat

HOW "TO" CREATE A PHISHING CAMPAIGN

- Select the Tracking time for the campaign (following email delivery)
- To track replies, check the checkbox beside "Track Replies"
- Select the email template category to be used.
- Select the type of randomization of emails to be sent (Full randomization or random email to all users)
- Select the difficulty rating for the messages to be sent.
- Phishing Link Domain –
  - select "Random domain" if you have hidden all non-whitelisted domains
  - Select a specific domain if you have not hidden all non-whitelisted domains
- Landing page–
  - Select "Default Landing Pages" if you want to use the landing page that was created by KnowBe4 for that message.
  - Select a specific landing page if you want to select the landing page that all users will see for any message sent as part of the campaign.

HOW “TO” CREATE A PHISHING CAMPAIGN



Track Activity: 3 days ▾ after the sending period ends

□ Track Replies to Phishing Emails

Template Categories: Select one or more categories... ▾ | Full Random (Random email to each user) ▾

□ Send Localized Emails

Difficulty Rating: All Ratings ▾

Phish Link Domain: Random Domain ▾

Landing Page: Default Landing Pages ▾

Add Clickers to: Select Group ▾

□ Send an email report to account admins after each phishing test

□ Hide from Reports

HOW “TO” CREATE A PHISHING CAMPAIGN

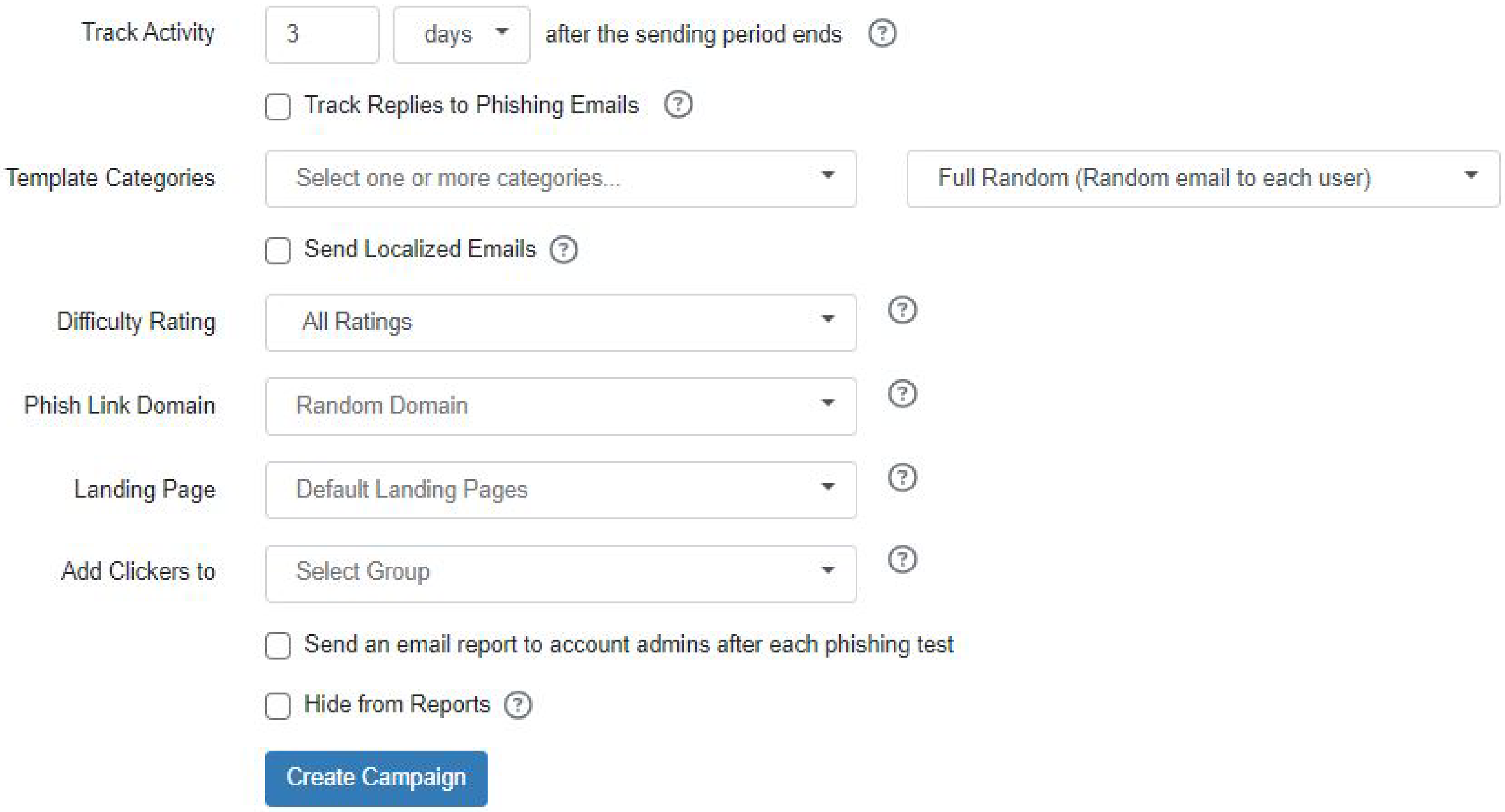
- Add Clickers To – select the group you want to add them to if to want to be able to target them separately.
- Send an email report to the account admins - check the box beside the statement to enable this.
- Hide from reports - check the box beside the statement to hide the campaign.

Now that all required information has been provided…

Click the “Create Campaign” button at the bottom of the page.

This will queue the campaign creation on the KnowBe4 servers. You will see the status go from pending to complete as you refresh the status screen.

HOW "TO" CREATE A PHISHING CAMPAIGN



Track Activity: 3 days after the sending period ends

□ Track Replies to Phishing Emails

Template Categories: Select one or more categories... | Full Random (Random email to each user)

□ Send Localized Emails

Difficulty Rating: All Ratings

Phish Link Domain: Random Domain

Landing Page: Default Landing Pages

Add Clickers to: Select Group

□ Send an email report to account admins after each phishing test

□ Hide from Reports

2024 SCHEDULE OF COV-WIDE PHISHING CAMPAIGNS

COV-wide Campaigns will occur the 3rd week of each quarter

A number of ISOs has asked if a schedule of COV-wide Campaigns could be published.

While the Security Standard calls for agencies to complete phishing campaigns once a year, CSRM has been and will continue to provide COV-wide phishing campaigns on a quarterly basis. In reviewing the holiday calendar for 2024, we have selected the third week of the quarter for these campaigns. This will also provide about 5 weeks should a campaign need to be re-scheduled or re-run.

The schedule for 2024 is as follows:

Q1 – week of January 22nd
Q2 – week of April 15th
Q3 – week of July 15th
Q4 – week of October 14th

QUESTIONS?

SEC530

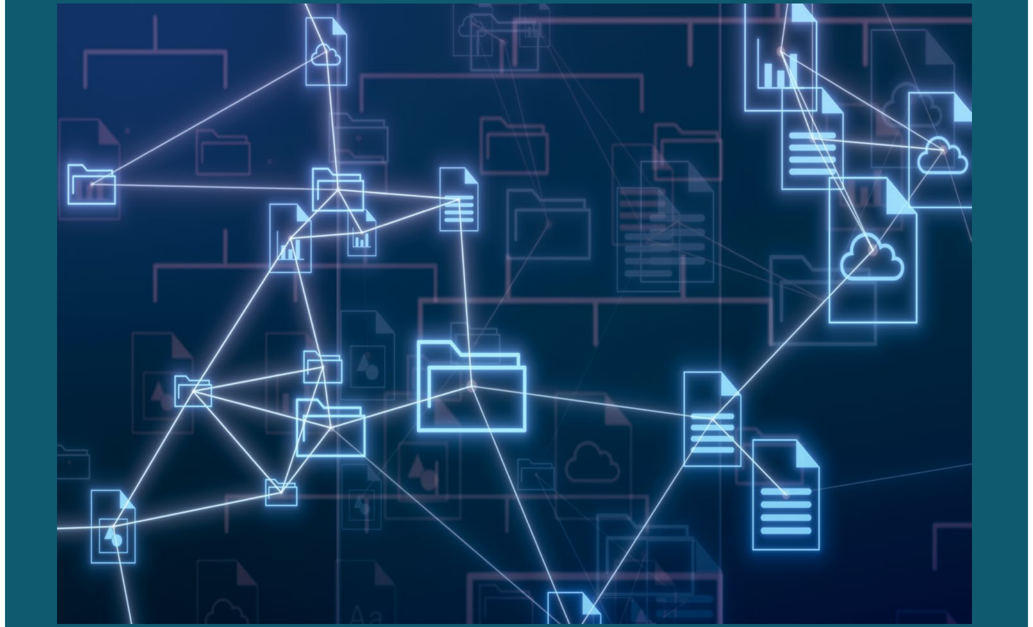
VIRGINIA IT AGENCY

SEC530 Update Announcement

Amy Braden

Director, Security Governance

January 10, 2024



VIRGINIA
IT AGENCY

Workload Management (WM)

January ISOAG

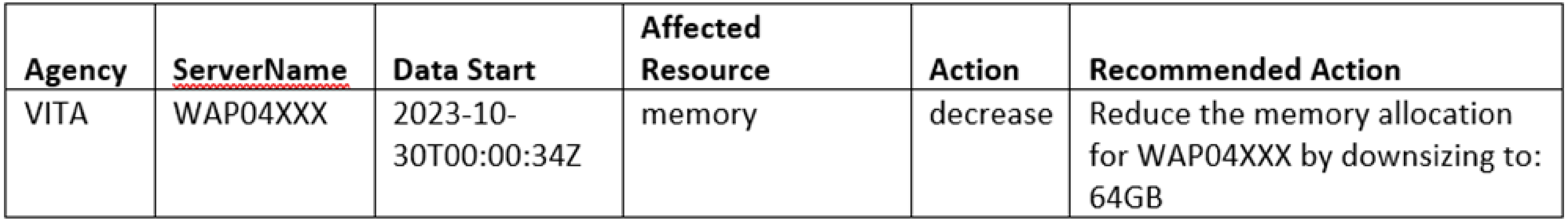
John C Del Grosso
Service Owner, Server Storage and Data Center Services

January 2024

Workload Management (WM): Overview

- Manages cloud servers by using real time and historical data to analyze the demand of resources
- Uses the data provided to make decisions on compute changes to maintain and maximize server and application performance
- Provides suggestions to increase or decrease the compute profile in a monthly report
  - Example suggestion: “Reduce the memory allocation for WAPXXXXX by downsizing to: XGB”
- As of January 2024, WM has 4-8 months of data history. To ensure accuracy, it is recommended for agencies to weigh their actual utilization over a longer term as to capture their server usage during surge and idle periods.

Example report



Agency	ServerName	Data Start	Affected Resource	Action	Recommended Action
VITA	WAP04XXX	2023-10-30T00:00:34Z	memory	decrease	Reduce the memory allocation for WAP04XXX by downsizing to: 64GB

Agency: Owning agency, derived from comparing the server name to the configuration management database (CMDB)

ServerName: Server name per CMDB

Data Start: The date the WM started collecting performance data

Affected Resource: This will be virtual random access memory (vRAM) or virtual central processing unit (vCPU)

Action: Decrease or increase the affected resource

Recommended Action: Specific detail of the action

WM: Agency workflow

- Reports are created monthly and provided to VITA’s server storage and data center (SSDC) team
- Reports will be distributed to agency users, customer account managers (CAMs), and business relationship managers (BRMs)
- To request an increase or decrease in a server compute profile, submit a general service request by following the steps documented in the workload management knowledge base article: KB0019508

Upcoming Events

VIRGINIA IT AGENCY

vita.virginia.gov

IS Council Meeting

The next IS Council Meeting will be held on January 17, 2024

The meeting will last from 12-1 pm and will cover information on the progress of the various committees.

If you need a link to attend this meeting, please request an invitation through the Commonwealth Security mailbox.

IS Orientation

The next IS Orientation will be held on March 27, 2024

- The Orientation will last two hours and be held remotely via WebEx.
- Please register to attend at:

https://covaconf.webex.com/weblink/register/rd212e769bb8f06f1b608aebd01be1cd7

IS Orientation

MEETING ADJOURNED

VIRGINIA IT AGENCY