VIRGINIA IT AGENCY

WELCOME TO THE September 6, 2023

ISOAG MEETING

VIRGINIA IT AGENCY

AGENDA	
Welcome/Opening Remarks	Erica Bland/ VITA
Update on KnowBe4	Kathy Bortle/VITA
Dynamic Defense – Six Steps to Achieving and Maintaining a Secure Network Environment	Sonya Hefferan/Joe Decker/Matt Kucik/Tenable Security Specialists
Live Demo for Acunetix	Juan Depazgonzalez/VITA
Services Offered by CISA	Arnold Webster / Cybersecurity and Infrastructure Security Agency
Keystone Edge Upgrade	Serena Singleton/ SAIC
Upcoming Events	Erica Bland/VITA
Adjourn	

VIRGINIA IT AGENCY

UPDATE ON KNOWBE4

KATHY BORTLE

Incident Response Specialist

ISOAG MEETING

SEPT 6TH, 2023

What is Single Sign On?

Single sign on provides the ability to login to applications with one user id and password

The single-sign on system passes the credentials to each application when launch through its application portal. The Commonwealth has chosen Okta as the single-sign on solution.

What is User Provisioning?

User Provisioning is the act of creating a user id is for accessing the application. User provisioning can be a manual or an automated process.

There are 3 options for user provisioning:

1. CSV File (manual process)
2. Okta (limited functionality)
3. Active Directory Integration (ADI) Sync (Automatic user creation but requires an COV AD account)

Option 1 - CSV File (manual process) –

Most applications will allow importing data via a CSV file. To create users, you will setup a spreadsheet with the fields that you want in the file (e.g. First Name, Last Name, Email Address, etc.) and then save the file as a CSV.
When you need to add new users, this would be done as another CSV import or manually. When users leave the agency, they would need to be manually archived (inactivated) in KnowBe4.

Recommended Uses:

- Initial bulk load of users
- Agencies that have little turn over
- Small agencies with just a few users

Option 2 - Okta (limited functionality) –

When the user logs into KnowBe4 via Okta, it will check to see if a user has a KnowBe4 account. If not, it will create it on first login and then prompt the user to create their password for KnowBe4.

Limitations with this option are as follows:

- User must login for the account to be created.
- Administrator must wait for the user login/account creation before training can be assigned.
- User will not have a manager's email address

The administrator must enter it manually into the user's account.. If it is not entered, the user's manager will not receive the training notification.

Recommendation:

- Okta is a single sign on product. It is not a user provisioning product. Therefor it is **not recommended** to use this option for user provisioning.

Option 3 - ADISync (AD accounts are automatically sync'd every six hours) –

ADISync is an application that runs as a service on Windows. The tool has an automatic six-hour sync cycle, and the service must be running for it to work. When the service logs in to Active Directory, it reads the information and synchronizes it to KnowBe4. If the user has a manager's email or is part of a specific group, that can be synchronized as well.

Requirements for this option: a Windows server in the DMZ with a service account.

While the application can be tested on a workstation with a normal user account, the credentials get encrypted into a configuration file. To update the password, the configuration utility needs to be re-run. Using this on a workstation would mean that the workstation would need to be up 7x24 to not miss the sync cycle and would need to have its configuration file re-done with every password change.

Benefits of this option:

- When a user is created in AD, they are automatically created in KnowBe4 at the next sync cycle.
- When a user's account is disabled in AD, the KnowBe4 account is automatically archived.
- If the user's account has a manager's email address in AD, it is automatically populated in KnowBe4.
- Automatic training assignment by synchronizing AD groups for training.

Example:

Step 1 - Agency sets up 3 training groups in KnowBe4 named General User, Administrator and Data Owner. They assign the appropriate training modules to each group.
Step 2 - Agency has 3 training groups in AD with the same names – General User, Administrator, Data Owner (names match)
Step 3 - ADISync is told to synch these groups to KnowBe4 as part of the configuration during installation.
Step 4 - Sally Smith is added to the AD group called “Data Owner”
Step 5 – Next ADISync cycle, Sally Smith’s group membership is synchronized, and Sally is automatically assigned the Data Owner training.

If the agency wants the user to be added to the group for them, they can do that as part of the initial user creation request or as a VCCC ticket. The agency can also administer the AD groups themselves if that is what they prefer.

Recommendation:

- Use both ADISync & Okta together to facilitate user provisioning and single sign-on.

CONFIGURING THE PHISHING MODULE

CSRM has configured the phishing module for all agencies as follows:

- Whitelisting

KnowBe4 contains 34 root domains in its product. The limit for Microsoft 365 and Microsoft Defender is 20. CSRM selected 10 domains to whitelist for phishing so that messages are not being flagged as clicked because of being scanned by Microsoft Defender 365. When a whitelisted domain is used, it does not generate the false positives some agencies were seeing.

- Domain Options in KnowBe4 Console

CSRM has hidden all non-whitelisted domains in agency accounts. This will allow agencies to use the canned templates without receiving false positives. The Random option for the domain for the phishing link will now only select one of the whitelisted domain.

THE FOLLOWING PHISHING DOMAINS HAVE BEEN WHITELISTED FOR USE WITH KNOWBE4

- com-onlinebanking.com
- com-token-auth.com
- donotreply.biz
- internalportal.net
- kb4.io
- msftemail.com
- my-cloud-mail.com
- net-login.com
- password.land
- protected-forms.com

PAB HYBRID CONFIGURATION

- In order to support all platforms (desktop, web and phone), the Hybrid configuration option has to be used.
- The PAB button has been configured for all agencies. It will use the KnowBe4 OKTA group for the agency to deploy the button to the Outlook Client, Microsoft 365 Web Client, Outlook for iOS and Outlook for Android.
- The PAB button will replace the Microsoft Message Report Button on Sept 18th.

- The PAB button will automatically include message headers when reporting the phish to the VCCC and Area 1.
- The reported phish will also be sent to an address of the agency's choosing. This will allow ISOs to see what type of phishing messages users are receiving. They can use these as examples for creating their own phishing campaigns.

Why PAB?

The PAB button is a free add-in product that integrates with KnowBe4 phishing campaigns It will provide similar functionality as the Microsoft Reporting Button but will include added functionality.

For simulated phishing messages:

- Reports of simulated phishing messages will be recorded as part of the user's training record.
- The user will receive immediate feedback to their submission.

For non-simulated messages, it facilitates easier phishing/spam reporting by:

- Reported messages will be automatically sent to the VCCC and an address of the agency's choosing (e.g. example@vita.virginia.gov)
- Message Headers and the subject are included with the body of the message
  (users won't have to acquire them and send them to the VCCC separately)
- Users will have the choice of "phishing or spam" for submissions.
- Users can include a comment if desired.
- User will receive a VCCC ticket # for the submission so that the SOC and NTTDATA can investigate the messages and apply appropriate blocking.

OUR ASK

Here is what we need from you to get this project to the finish line:

1. Add users for your agency to your agency's KnowBe4-account via one of the User Provisioning Methods.
2. Add users for your agency to the AD KnowBe4-Okta group.

NOTE: The KnowBe4-Okta group will be used for both Single Sign On and for Phish Alert Button (PAB) delivery.

Need assistance with any of these tasks:

Email the team at CommonwealthSecurity@vita.virginia.gov
Please include "KnowBe4" in the subject

Important Dates:

PAB Implementation: Sept 15th – 18th

- The PAB button will be pushed out by NTTDATA during the weekend of Sept 15th.
- It will automatically replace the Microsoft Reporting Button.
- It will be distributed to the Outlook Desktop Client, Outlook Web Client, Outlook for Android and Outlook for iOS
- It will not require a report.

COV 3rd Quarter Phishing Campaign – week of 9/25

Once the PAB button is implemented, agencies are free to conduct their own phishing campaigns on their own schedules. VITA/CSRM will continue to conduct quarterly phishing campaigns for agencies.

QUESTIONS?

tenable

Dynamic Defense – Six Steps to Achieving and Maintaining a Secure Network Environment

Matt Kucik
National Sales Director
Public Sector, State, Local & Education (SLED)
Joe Decker
Manager, Security Engineering - SLED

Agenda

Introductions

Tenable overview

1. It all starts with visibility
2. Build a dynamic, proactive vulnerability management program based on actual risk
3. Keep score to track progress
4. Use the right tool for the job
5. Look at your network from the attacker's perspective
6. Make sure your source of trust can be trusted

tenable

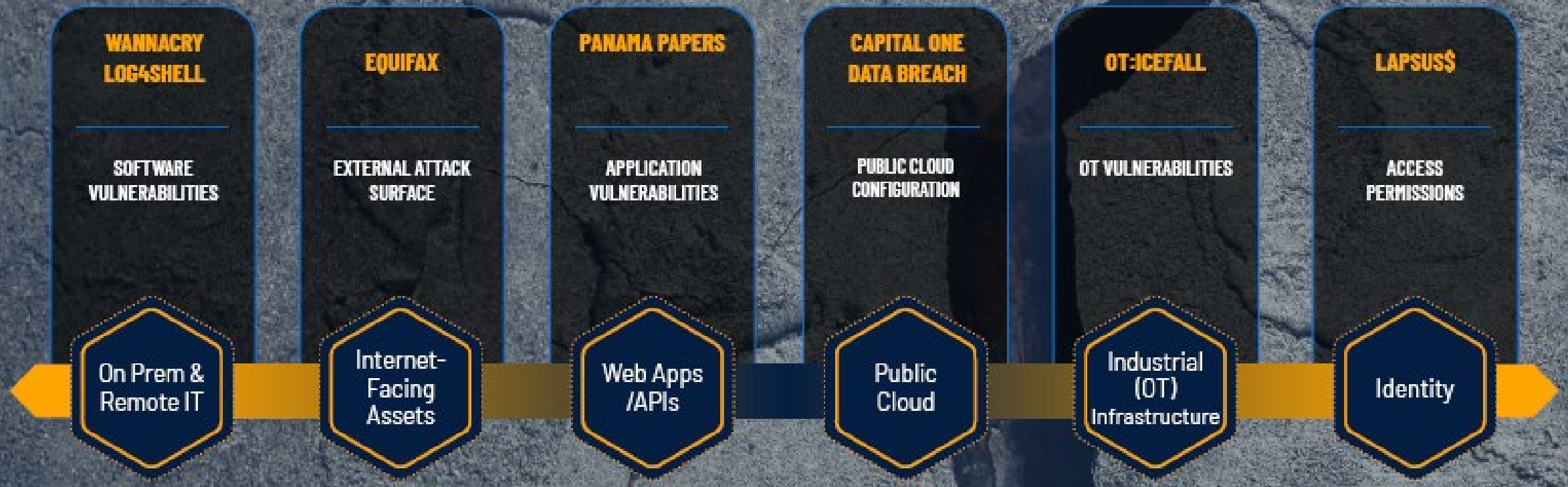
THE MODERN ATTACK SURFACE

3 attributes make the modern attack surface more difficult than ever to defend:

1. RAPIDLY **GROWING**
2. HIGHLY **DYNAMIC**
3. INCREASINGLY **INTERCONNECTED**

tenable

SIGNIFICANT BREACHES TARGET THE WEAKEST LINK ACROSS THE ENTIRE ATTACK SURFACE

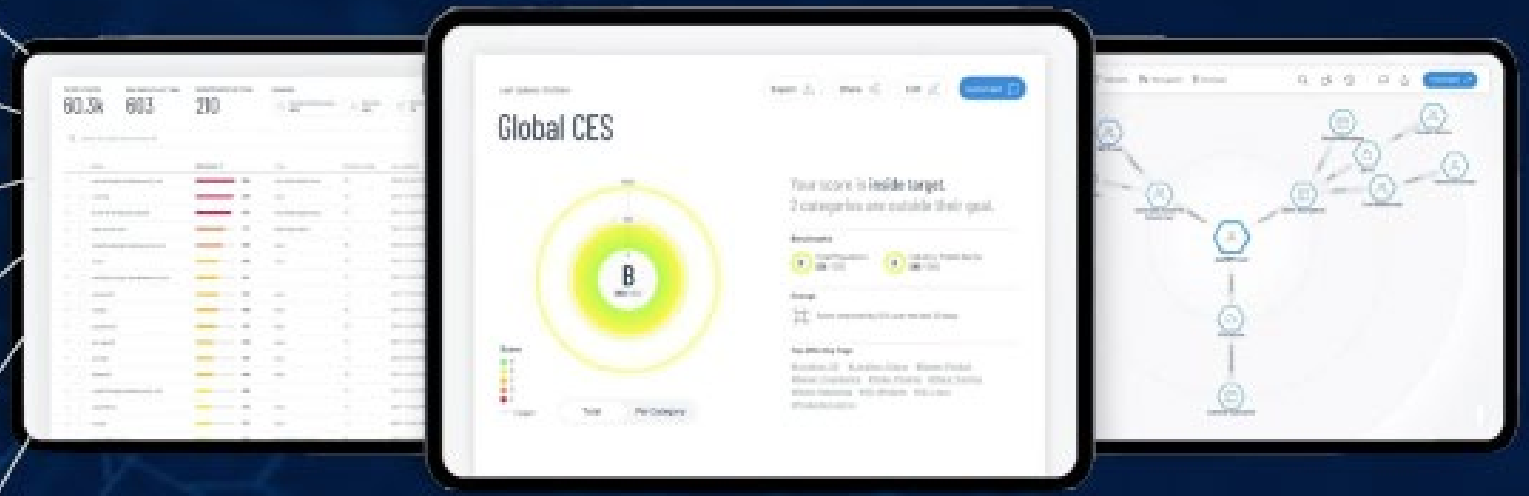


tenable

TenableOne High Level Overview

- On Prem & Remote IT
- Internet-Facing Assets
- Web Apps /APIs
- Public Cloud
- Industrial (OT) Infrastructure
- Identity

- SOFTWARE VULNERABILITIES
- External Attack Surface
- Application Vulnerabilities
- Public Cloud Configuration
- OT Vulnerabilities
- Access Permission



Answer the Questions

- How secure are we?
- Where am I vulnerable?
- Are we better today than we were yesterday?

tenable

EXPOSURE VIEW: GLOBAL CYBER EXPOSURE SCORE

Export
Share
Edit
Comment

Global CES

B

Your score is **inside target.**
2 categories are outside their goal.

Benchmarks

Change

Top Affecting Tags

Score

Target

Total
Per Category

nable

EXPOSURE VIEW: Trending

tenable

EXPOSURE VIEW: Remediation

Remediation SLA

SLA Efficiency | High Risks

EXPOSURE VIEW: GLOBAL CYBER EXPOSURE SCORE

Global Exposure View answers questions:

- Where do we stand?
- How is our score trending?
- How effective is our program maturity?

tenable

EXPOSURE VIEW: GLOBAL CYBER EXPOSURE SCORE

Global Exposure View answers questions:

- Where do we stand?
- How is our score trending?
- How effective is our program maturity?

tenable

PROTECT YOUR MODERN ATTACK SURFACE

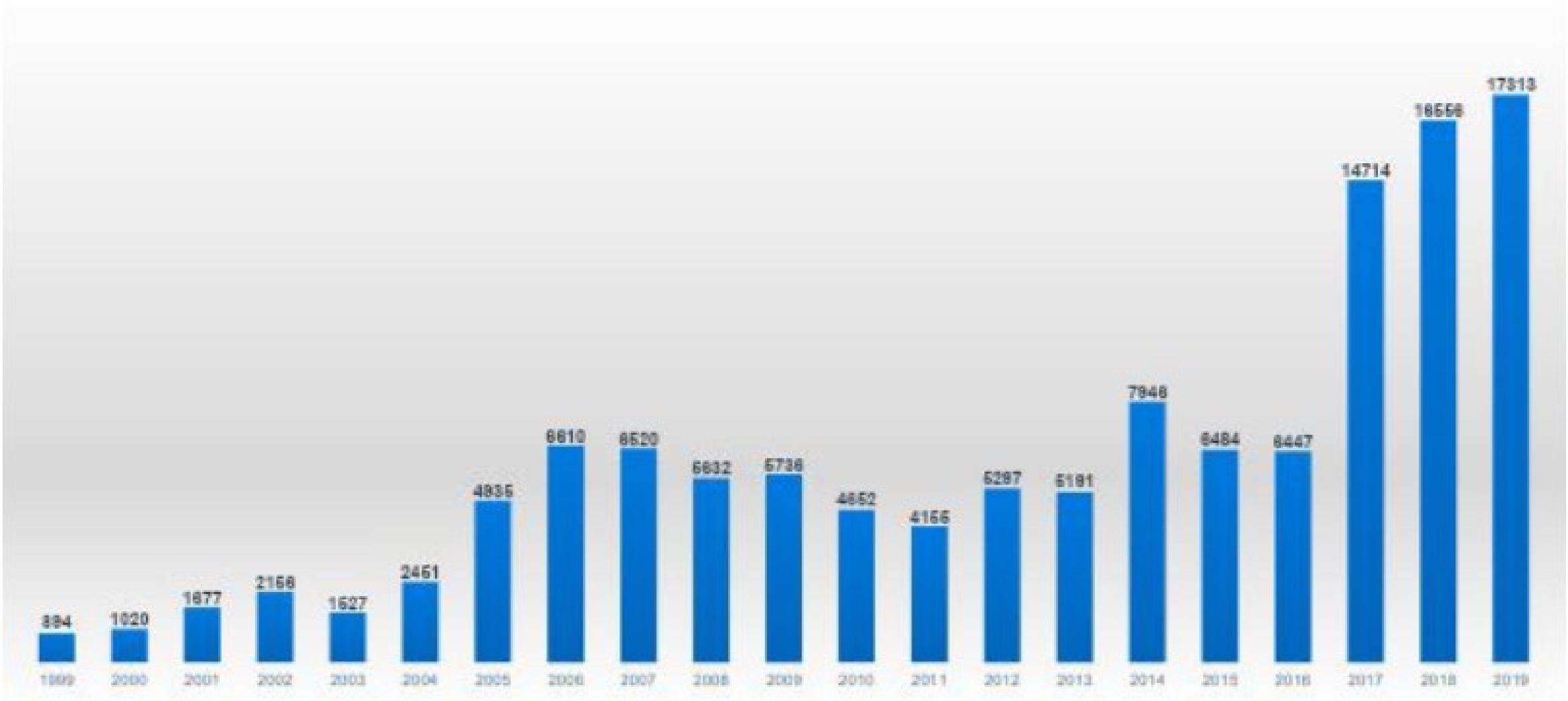
Gain visibility across the modern attack surface

Anticipate threats and prioritize efforts to prevent attacks

Communicate exposure risk to make better decisions

tenable

The Number of New Vulnerabilities Continues to Grow



Source: Vulnerability Intelligence Report, Tenable Research

tenable

CVSS is NOT an Assessment of Risk

"CVSS is designed to identify the technical severity of a vulnerability. What people seem to want to know, instead, is the risk a vulnerability or flaw poses to them, or ***how quickly they should respond to a vulnerability***."

TOWARDS IMPROVING CVSS
SOFTWARE ENGINEERING INSTITUTE | CARNEGIE MELLON UNIVERSITY
December 2018

tenable

What does NIST (National Institute of Standards and Technology) have to say about it?

"The Common Vulnerability Scoring System (CVSS) is a method used to supply a qualitative measure of severity. CVSS is not a measure of risk."

NIST NVD Webpage

tenable

18K VULNERABILITIES DISCLOSED IN 2020

NEARLY **3X MORE** THAN 2016

CVSS 7+ REMEDIATION POLICY

- **WASTES 76%** OF THE SECURITY TEAM'S TIME
- **LEAVES 44%** OF RISKY VULNERABILITIES IN YOUR ENVIRONMENT

57% OF ALL VULNERABILITIES HAVE A **CVSS BASE SCORE OF 7 OR ABOVE**

20% VULNERABILITIES HAVE AN **EXPLOIT AVAILABLE**

tenable

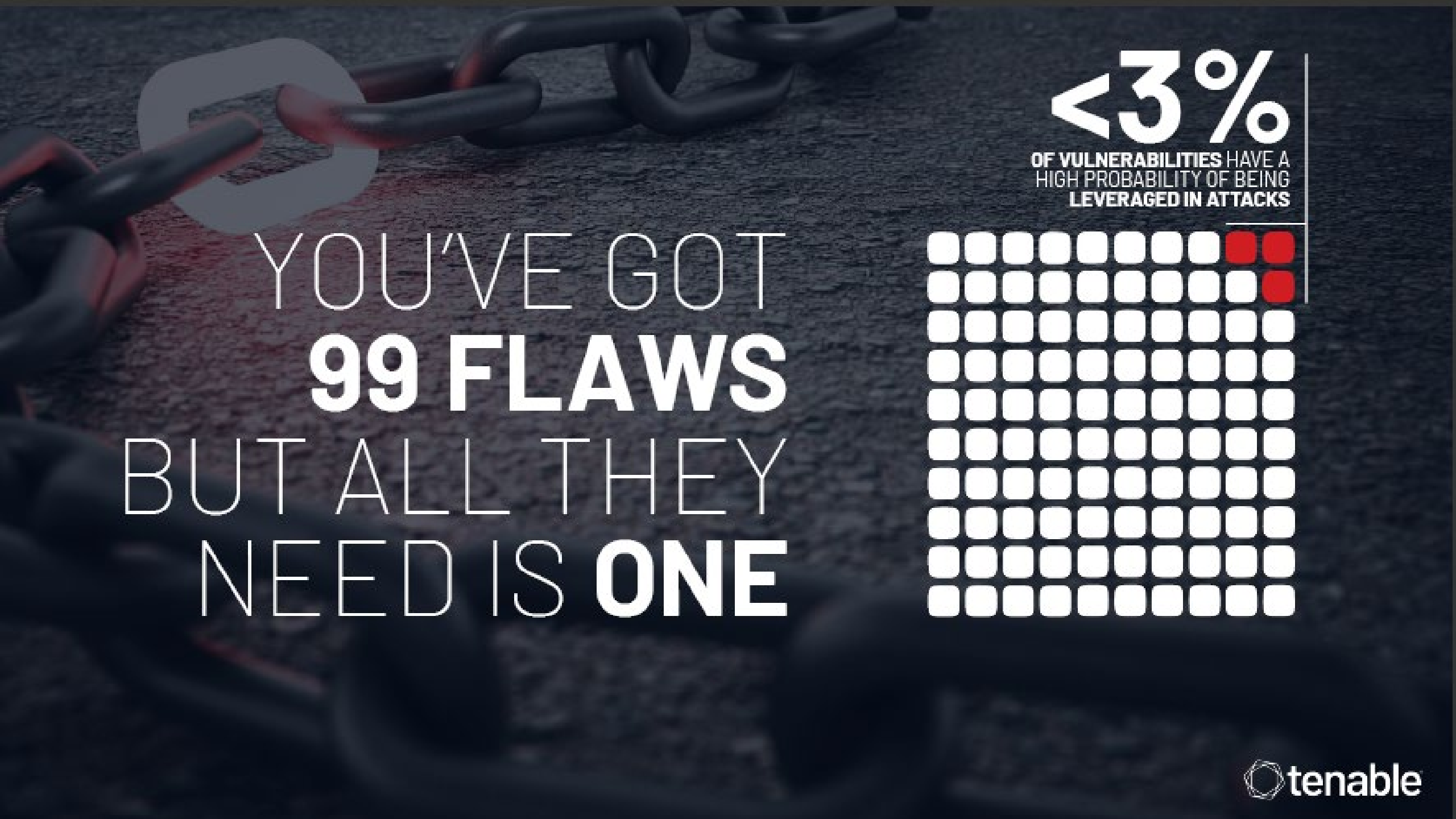
Risk-Based Vulnerability Management

A process that employs machine learning analytics to automatically correlate:

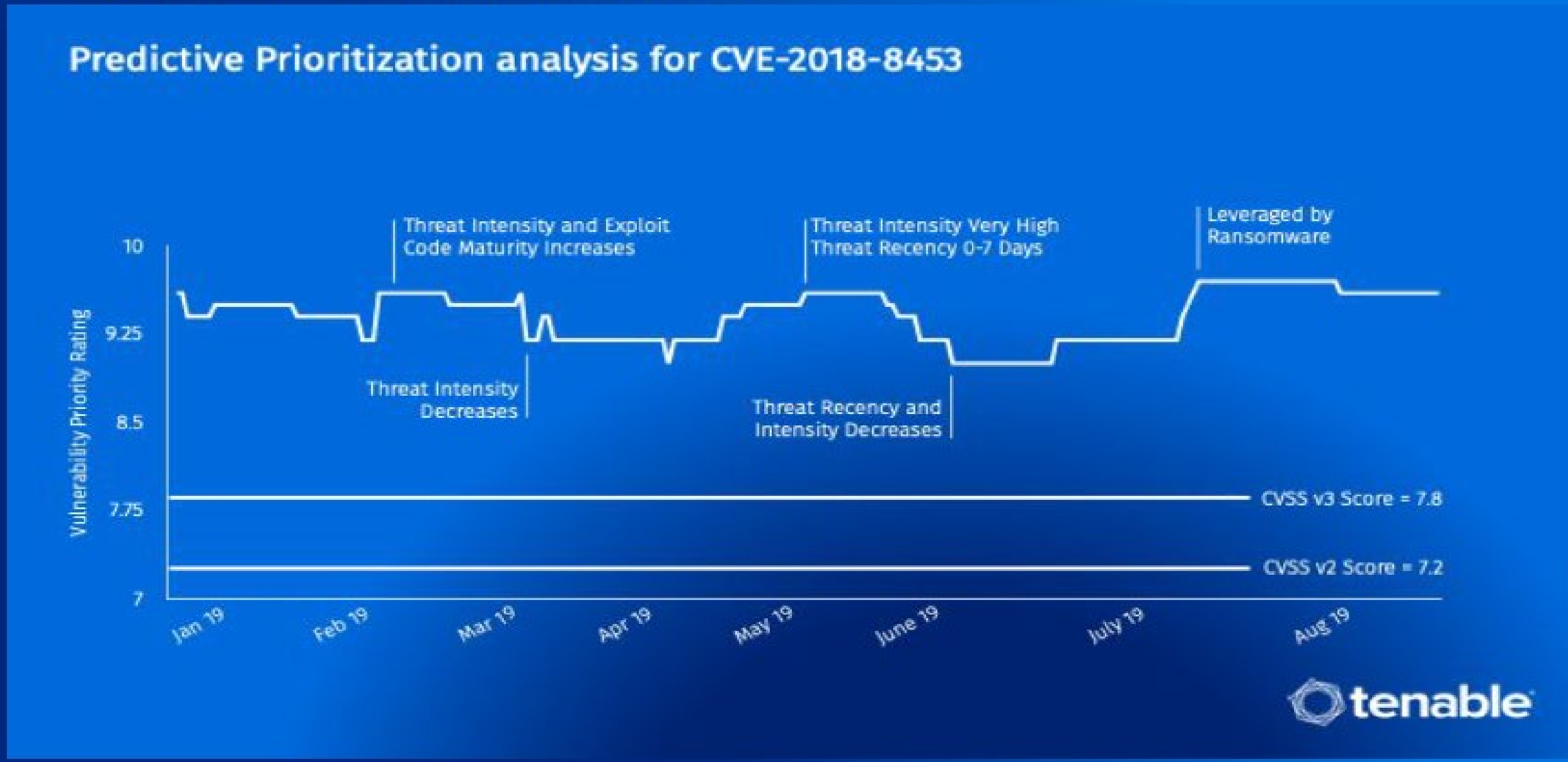
- Assessments of traditional and modern assets across the entire attack surface
- Vulnerability severity
- Threat and exploit intelligence
- Asset criticality

… to identify which vulnerabilities pose the greatest risk.

tenable


<3%
OF VULNERABILITIES HAVE A HIGH PROBABILITY OF BEING LEVERAGED IN ATTACKS
YOU'VE GOT
99 FLAWS
BUT ALL THEY
NEED IS ONE
tenable

Elevation of privilege vulnerability in Windows
Used in 2019 ransomware attacks



Demonstration of Risk-Based Vulnerability Management

tenable

PROTECT YOUR MODERN ATTACK SURFACE

Communicate exposure risk
to make better decisions

tenable


382
587
622
451
COMPARE
METRICS TO DRIVE ALIGNMENT AND IMPROVEMENT
tenable

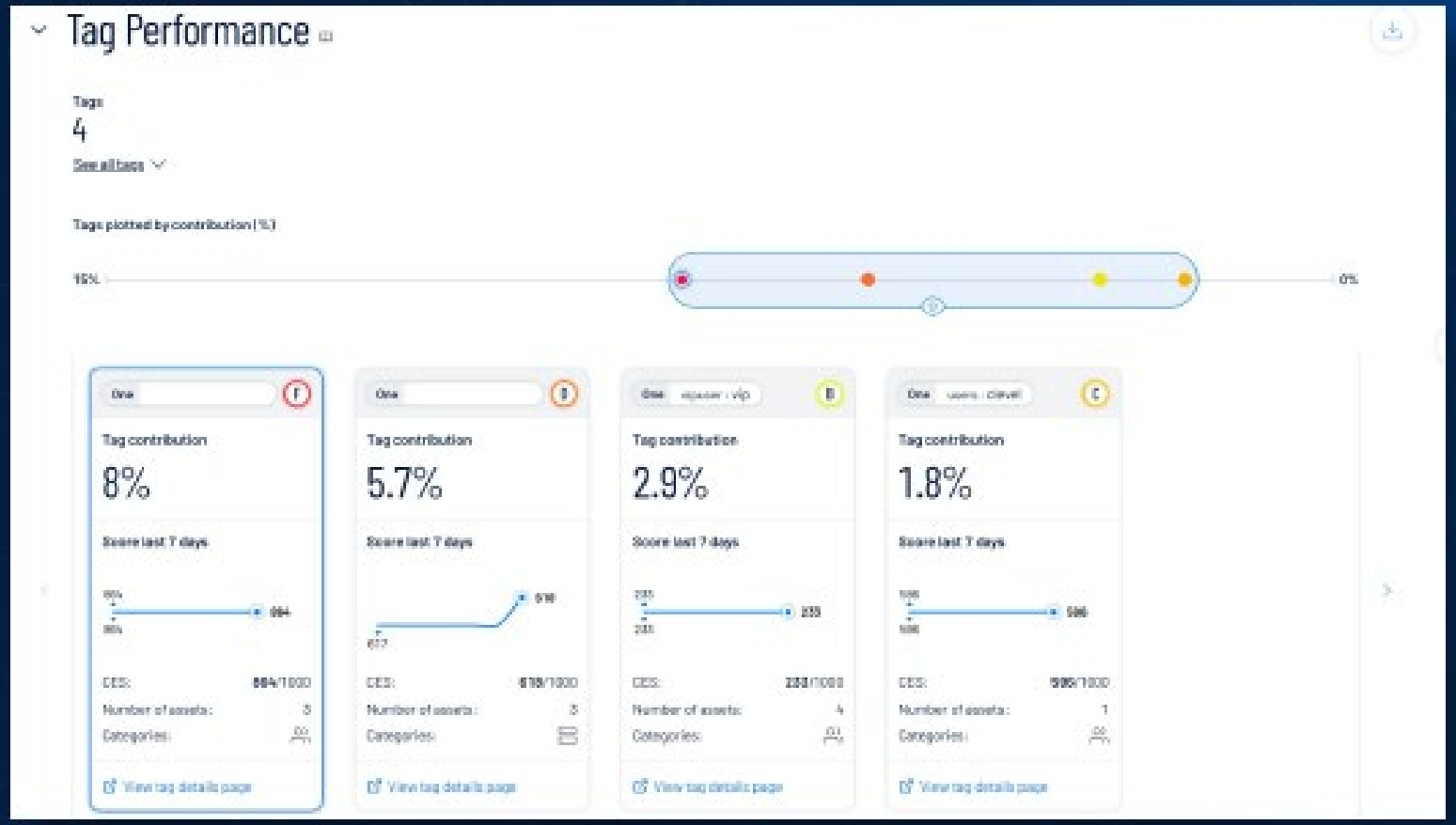
How to effectively communicate risk:
KEEP A CYBER EXPOSURE SCORE

Use a tool that answers key questions:

- Where do we stand?
- How is our score trending?
- How effective is our program maturity?

tenable

Assess Risk at a Granular Level:
Tag Performance



Tag Performance describes:

- What areas make up this Exposure View?
- Which areas are driving the score?
- Which areas require focus?

tenable

Demonstration of Cyber Exposure Scoring to Manage Risk

tenable

Web Application Scanning – Match the Tool to the Task

Dynamic Application Security Testing (DAST): A DAST crawls a running web application through the front end to create a site map with all of the pages, links and forms for testing. Once the DAST creates a site map, it interrogates the site through the front end to identify any vulnerabilities in the application custom code or known vulnerabilities in the third-party components that comprise the bulk of the application. **Only a DAST tool can identify runtime flaws, which are not apparent in a static environment.**

Static Application Security Testing (SAST): A SAST analyzes static environments, i.e., meaning the source code of an application. Used for periodic assessment, It looks at the application and searches for vulnerabilities in the code.

Use the Right Tool for the Job

tenable

EXTERNAL ATTACK SURFACE MANAGEMENT

As the modern attack surface continues to grow, most organizations now have a significant number of Internet-facing assets they don't even realize they have, let alone understand whether they are vulnerable to attack.

These unknown or poorly understood assets create a new dimension of risk, providing threat actors easy targets and the opportunity to access assets without anyone knowing.

tenable

People outside **know more about the organization's attack surface** than those within


Threat Intelligence | 5 MIN READ | ARTICLE

Log4j Attack Surface Remains Massive

Four months after the Log4Shell vulnerability was disclosed, most affected open source components remain unpatched, and companies continue to use vulnerable versions of the logging tool.

Link

90,000+ internet-exposed servers are still vulnerable


DR Tech | 6 MIN READ | ARTICLE

Exposed Kubernetes Clusters, Kubelet Ports Can Be Abused in Cyberattacks

Organizations must ensure their kubelets and related APIs aren't inadvertently exposed or lack proper access control, offering an easy access point for malicious actors.

Link

245,000 Kubernetes clusters are running publicly exposed


Half of security pros say their public clouds were breached during the pandemic

Steve Zurier March 22, 2022

Link

Unknown, unmanaged data is creating cloud risks via Shadow IT

tenable

See Your Network as Others See It

tenable

What if they get in?

Zero Trust Architecture – assumes that a breach has occurred

The attacker has infiltrated; how can we prevent data exfiltration or ransomware?

ACTIVE DIRECTORY – THE SOURCE OF TRUST

"…Directory Services is the underlying infrastructure that supports authentication and authorization. Its compromise would de facto render any zero trust implementation ineffective."

- ***NSTAC Report to the President on Communications Resiliency, 2022***

tenable

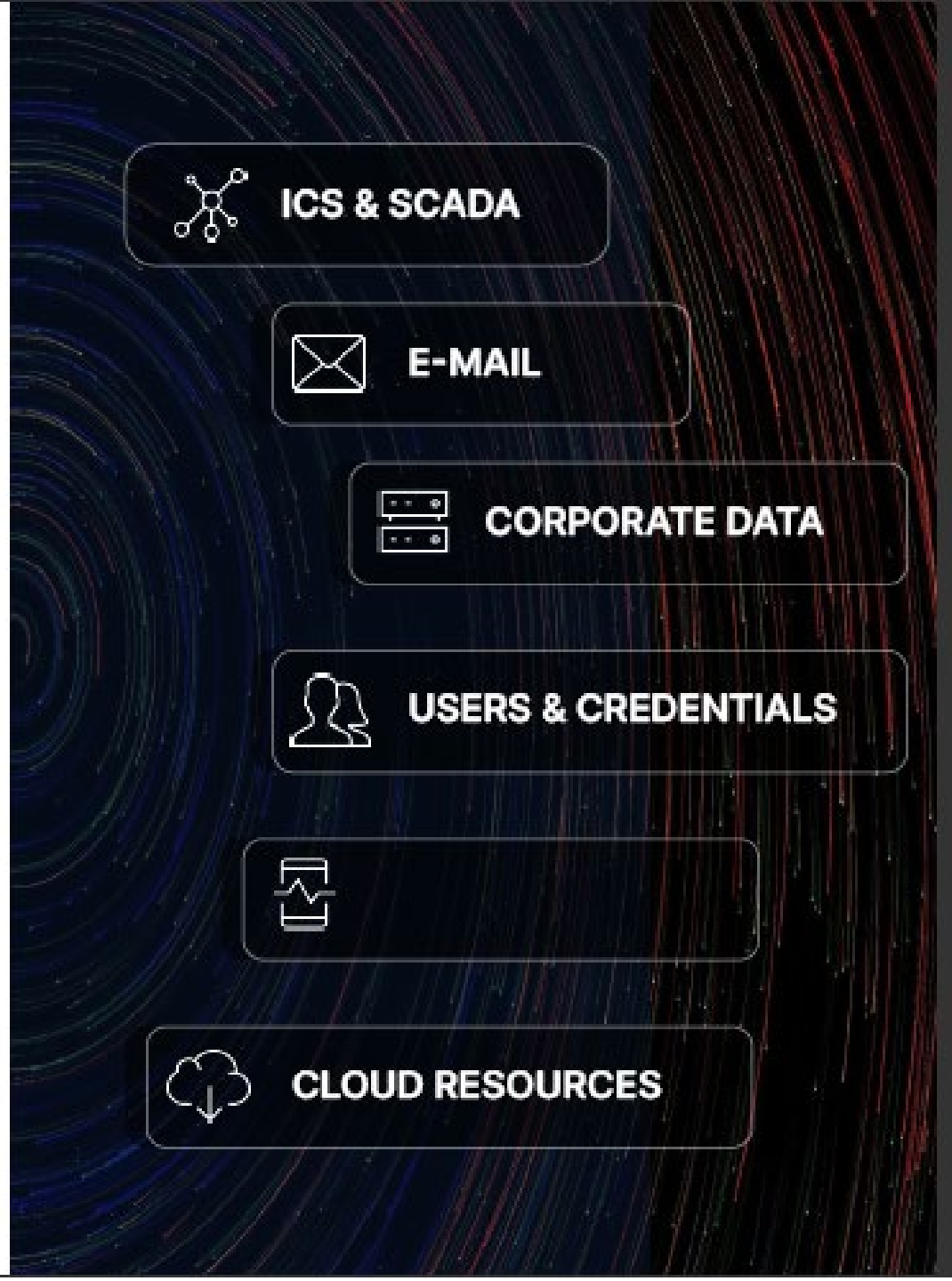
Secure the Trust Provider

Active Directory holds the **keys to everything**

- Governs authentication, holds all passwords
- Manages access rights to every vital asset
- Ensures the user is known and managed at all times

"... trusted identity management solutions are unquestionably foundational, as zero trust is based on a continuous cycle of credentialing, verifying, and authorizing identity for person and non-person entities."

–NSTAC Report to the President on Communications Resiliency, 2022



Can you trust your identity system?

If your identity system is compromised, attackers can escalate privileges and move laterally throughout your network.

Identity systems must be continuously assessed to ensure they have not been compromised; traditional periodic review processes leave significant gaps.

tenable

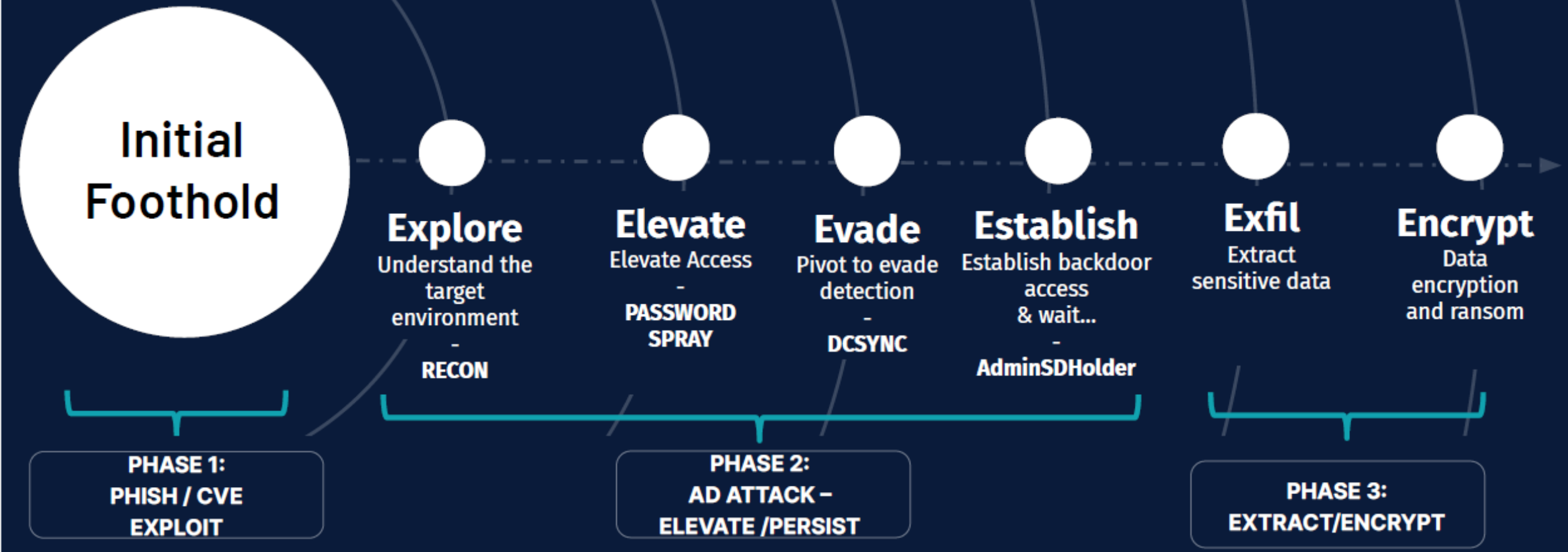
February 2022 Department of Commerce IG Report Recommendations to NOAA included:

1. Establish processes and procedures to **periodically review** all active directory accounts to ensure consistent adherence to the principle of least privilege per Department policy.

2. Determine the feasibility of requiring all NOAA line offices to use specialized active directory security tool(s) to conduct **periodic reviews.**

3. Establish procedures to **periodically review** active directories and ensure compliance with account management requirements as stated in the Department's policy and following industry best practices.

Understanding Common Attack Paths



Demonstration of the components of effective Active Directory security

tenable

Steps to Effective Dynamic Defense

1. **Start with comprehensive visibility**
2. **Take a dynamic, proactive, risk-based approach**
3. **Use risk scoring to check progress**
4. **Use the right tool for the job**
5. **Get an external view**
6. **Proactively protect your source of trust**

Thank You!

tenable

VIRGINIA IT AGENCY

ACUNETIX 360

JUAN DEPAZGONZALEZ & RILEY PFISTER

Web Scanning Team

VITA/CSRM /THREAT MANAGEMENT TEAM

FEBRUARY 1ST, 2023

ACCUNETIX 360

WHAT IS VULNERABILITY SCANNING?

- Using Automated tools to evaluate Web application Security
- Reporting findings to relevant parties for remediation
- Confirming fixes and remediation

WHAT IS ACUNETIX 360?

- On Demand SaaS DAST solution.
- Used for the Web Application Quarterly Scanning Requirement
- Multi tenant
- Limitless scanning

ACUNETIX 360

FUNCTIONALITIES

FUNCTIONALITIES

- Scan internal Applications
- Vulnerability Tracking
- Re scans on request
- Notifications
- Can support a wide range of users
- Scheduling scans
- Defining scan times

ISSUE TRACKING

- Every vulnerability can be assigned to a user and tracked within Acunetix 360
- Marked as Accepted, resolved, false positive...
- Ability to test remediation efforts and automatically resolve

SCAN OPTIONS

- Many custom configuration options for each target.
- Let's demo a few.

CONCLUSION

IMPROVEMENTS

- Vulnerabilities and remediation are tracked automatically within the application
- Enable each agency to scan at their discretion.
- Easily digestible findings within the application.
- Data can be filtered and exported through the web page.

FUTURE

- We will continue to develop and expand our scanning activities/ remediation efforts.
- More frequent scanning

QUESTIONS/CONTACT

Feel free to ask any questions

- Dean Johnson, Director of Threat Management
  Dean.Johnson@vita.Virginia.gov
  (804) 510-7093
- Juan Depazgonzalez, Web Scanning Team
  Juan.Depazgonzalez@vita.virginia.gov
  (804) 807-3892
- Riley Pfister, Web Scanning Team
  Riley.Pfister@vita.virginia.gov
  (804) 270-8427

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient infrastructure for the American people.

MISSION

We lead the National effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

OVERALL GOALS

GOAL 1

DEFEND TODAY

Defend against urgent threats and hazards

seconds | days | weeks

GOAL 2

SECURE TOMORROW

Strengthen critical infrastructure and address long-term risks

months | years | decades

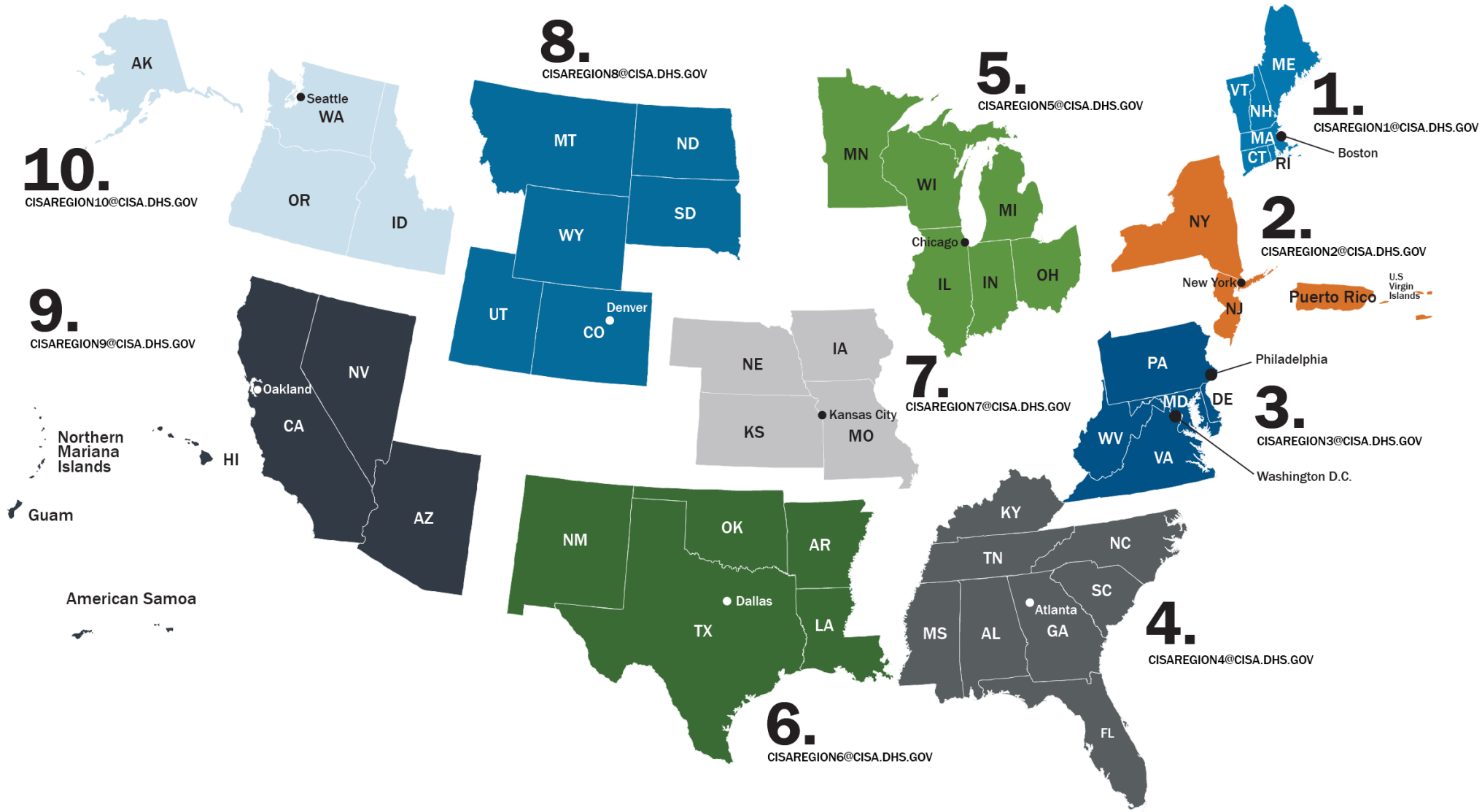
CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Our Work

The Cybersecurity and Infrastructure Security Agency (CISA) works with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future

CISA Regions

1	Boston, MA
2	New York, NY
3	Philadelphia, PA
4	Atlanta, GA
5	Chicago, IL
6	Dallas, TX
7	Kansas City, MO
8	Denver, CO
9	Oakland, CA
10	Seattle, WA



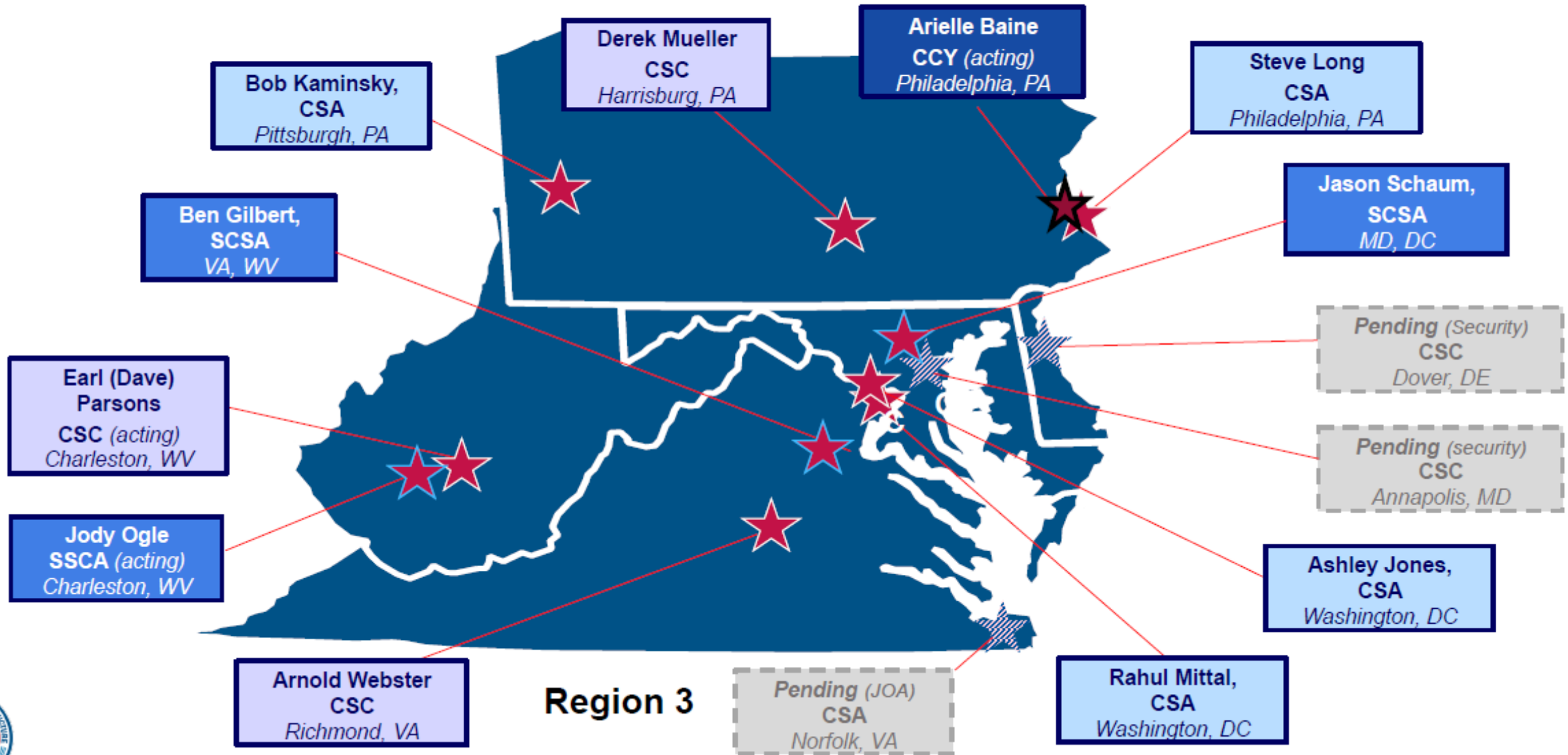
Cybersecurity State Coordinators and Cybersecurity Advisors

Established in Section 2215 of the 2021 National Defense Authorization Act, **Cybersecurity State Coordinators** are highly qualified CISA employees appointed to **serve in each state as the principal point of contact** with CISA on preparing, managing, and responding to cybersecurity risks and incidents.

Cybersecurity State Coordinators (CSCs) and Cybersecurity Advisors (CSAs):

- **Build** strategic public and private sector relationships,
- **Support** preparation, response, and remediation efforts relating to cybersecurity risks and incidents
- **Facilitate** cyber threat information sharing to improve understanding of ,cybersecurity risks and situational awareness
- **Raise** awareness of the financial, technical, and operational cybersecurity resources available to SLTT governments
- **Support** cybersecurity training and exercises
- **Assist** in developing and coordinating vulnerability disclosure programs consistent with Federal and information security industry standards
- **Assist** SLTT governments in developing and coordinating cybersecurity plans
- **Coordinate** and perform other duties as necessary to achieve the goal of managing cybersecurity risks in the United States

CISA Region 3 CSA/CSC Footprint (as of



TLP: GREEN

Cybersecurity State Coordinator and Cybersecurity Advisor Activities

Assessments

- Conducts Regionally Deployed Assessments:
  - Cyber Resilience Reviews (CRRs)
  - External Dependency Management Assessments (EDMs)
  - Cyber Infrastructure Surveys (CISs)
  - Cybersecurity Performance Goals assessments (CPGs)
  - Ransomware Readiness Assessments (RRAs)
  - Others
- Supports delivery of Enterprise and Nationally deployed services:
  - Cyber Hygiene Vulnerability Scanning and Web Application Scanning ,
  - Other technical services (e.g. pen testing and threat hunts)

Stakeholder Preparedness

- Cybersecurity Workshops
- **Vulnerability Disclosure Program Advisement for SLTT (CSCs)**
- Technical Exchange
- Introductory Visits and Cyber Protective Visits (CPVs)
- Cyber Exercises support
- Other Preparedness Activities

Strategic Messaging

- Resource Briefings
- Keynotes
- Panels
- Threat briefs
- Podcasts and Interviews
- Topic specific (e.g., CAM, SCRM/EDM, ICS, etc.)

Partnership Development

- Informational Exchanges (individual, group, etc.)
- Committees and Working Groups support
  - E.g., advisory member on SLCGP Planning Committee

Incident Response Coordination

- Incident Reporting Intake - CI stakeholder to CISA
- **Incident Coordination**
- **Proactive Notifications**
  - APT and ransomware actor tippers
  - Ransomware Vulnerability Warning Pilot (RVWP) program
  - Administrative Subpoena vulnerability notifications
- Special event support (on-site, virtual/remote)

CISA Offers No-Cost Cybersecurity Services

- **Preparedness Activities**
  - Cybersecurity Assessments
  - Cybersecurity Training and Awareness
  - Cyber Exercises and "Playbooks"
  - Cybersecurity Advisories and Alerts
  - Operational Products and Threat Indicator Sharing
  - Known Exploited Vulnerabilities (KEV) Catalog
  - Cybersecurity Performance Goals (CPGs)
  - Free Cybersecurity Tools and Services Catalog
  - Information Products and Recommended Practices

- **Response Assistance –** 24/7/365
  - Incident Coordination
  - Remote Assistance
  - Threat Intelligence Reporting and Information sharing
  - Malware Analysis

- **Cybersecurity State Coordinators and Cybersecurity Advisors**
  - Advisory Assistance
  - Cybersecurity Assessments
  - Incident Response Coordination
  - Working group collaboration
  - Public Private Partnership Development

Contact CISA to report a cyber incident

Call 1-888-282-0870 | email report@cisa.dhs.gov | visit https://www.cisa.gov

CISA Cyber Services: Right Organization. Right Service. Right time.

Regional Services

- Cyber Protective Visits
- Cyber Resilience Review
- External Dependencies Management Assessment
- Cyber Infrastructure Survey
- Workshops
  - Incident Management Workshop
  - Cyber Resilience Workshop
  - SLTT/ Cybersecurity Essentials Workshop
- Cyber Security Evaluations Tool (CPGs, RRA, CSF, etc.)

Enterprise Services

- Cyber Hygiene (Technical)
  - Vulnerability Scanning
  - Web Application Scanning
  - Continuous Phishing Campaign Assessment

National Services

- Remote Penetration Test
- Risk and Vulnerability Assessment
- Validated Architecture Design Review
- Red Team Assessment

STRATEGIC
(Management/C-Suite Level)

CSC/CSA Nominated

TECHNICAL
(Network-Administrator Level)

Cyber Exercise & Planning Program

CISA designs, develops, conducts, and evaluates cyber exercises ranging from small-scale, limited scope, discussion-based exercises to large-scale, internationally-scoped, operations-based exercises.

CISA offers the following services at no-cost on an as-needed and as-available basis:

- Cyber Storm Exercise (CISA's flagship national level cyber exercise)
- End-to-End Cyber Exercise Planning
- Cyber Exercise Consulting
- Cyber Planning Support
- **CISA Tabletop Exercise Packages (CTEPs)**

https://www.cisa.gov/cisa-tabletop-exercises-packages

Cybersecurity Training Resources

CISA is committed to providing the nation with access to cybersecurity training and workforce development efforts to develop a more resilient and capable cyber nation.

- **The NICCS website:** Searchable Training Catalog with over 6,000 cyber-related courses offered by nationwide cybersecurity educators
  - Interactive National Cybersecurity Workforce Framework
  - **FedVTE**
  - Scholarships for Service, Centers for Academic Excellence, and Cyber Competitions
  - Tools and resources for cyber managers
- Incident Response Training though IMR Series
- Industrial Control Systems (ICS) Training

For more information, visit https://www.cisa.gov/cybersecurity-training-exercises

Additional CISA Resources for SLTT

- **Cyber Incident Resource for Governors**
  - www.cisa.gov/files/cyber_incident_resource_guide_for_governors_508c
- **DotGov Program**
  - https://home.dotgov.gov/
- **Known Exploited Vulnerabilities (KEV) Catalog**
  - https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- **STOPRANSOMWARE.gov and #StopRansomware Guide**
  - https://www.cisa.gov/stopransomware
- **Catalog of FREE Cybersecurity Services and Tools**
  - https://www.cisa.gov/free-cybersecurity-services-and-tools

CISA CPGs

Cybersecurity Performance Goals (CPGs)

- A core set of cybersecurity practices with known risk-reduction value broadly applicable across sectors.
- A combination of recommended practices for IT and OT owners, including a prioritized set of security practices.
- Unique from other control frameworks
  - Clear, actionable, easily definable
  - Significantly and directly reduce the risk or impact caused by commonly observed, cross-sector threats and adversary TTPs
- **38 Performance Goals across 8 Categories:**
  - Account Security
  - Device Security
  - Data Security
  - Governance and Training
  - Vulnerability Management
  - Supply Chain/ Third Party
  - Response and Recovery
  - Other

WHERE TO START?: CSC/CSA-Led Cyber Protective Visits

Cyber Protective Visits

- 1–2-hour meetings (virtual or in-person) with critical infrastructure owners/operators
- CISA introduction and discussion around the organization's place in critical infrastructure
- Discussion on the organization's current capabilities and cybersecurity posture
- Direction the organization would like to move toward
- Identify and explore opportunities for future collaboration with CISA

Engage your CISA region and your local CSC/CSA!
https://www.cisa.gov/about/regions

WHERE TO START?: Cyber Hygiene-Vulnerability Scanning

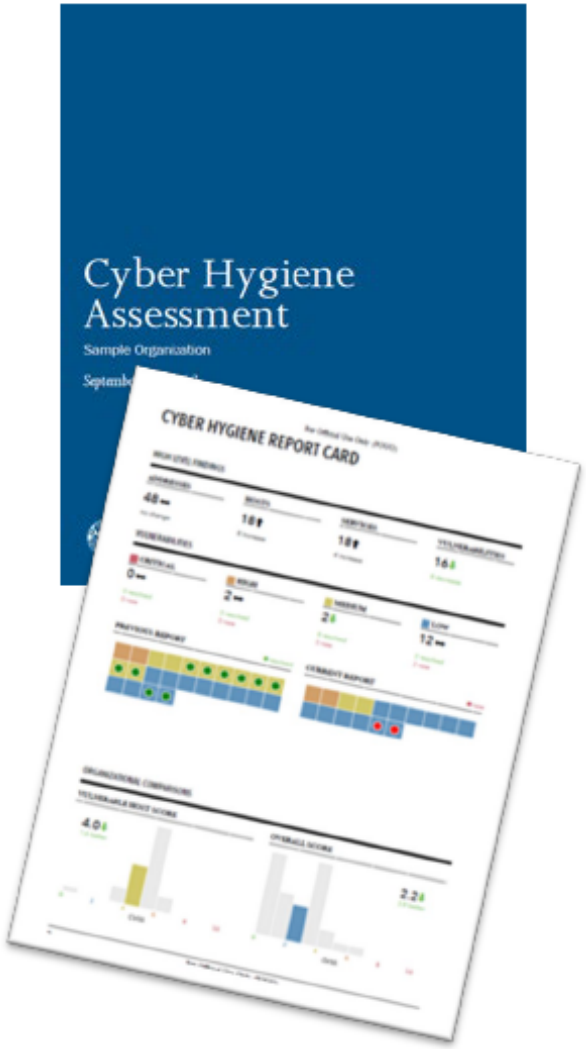
Purpose: Assess Internet-accessible systems for known vulnerabilities and configuration errors.

Delivery: Online by CISA

Benefits:

- Continual review of system to identify potential problems
- Weekly reports detailing current and previously mitigated vulnerabilities
- Recommended mitigation for identified vulnerabilities

  - **Network Vulnerability & Configuration Scanning**
    - Identify network vulnerabilities and weakness



Additional Information Sharing Opportunities

- **Multi-State Information Sharing and Analysis Center:**
  - Focal point for cyber threat prevention, protection, response and recovery for state, local, tribal, and territorial governments.
  - Operates 24 x7 cyber security operations center, providing real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response. For more information, visit www.cisecurity.org/ms-isac or email info@msisac.org

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Elections Infrastructure ISAC™

- **ISACs and ISAOs:**
  - **Information Sharing and Analysis Centers** (ISACs) or **Organizations** (ISAOs) are communities of interest sharing cybersecurity risk, threat information, and incident management to members. For more information on ISACs, visit www.nationalisacs.org. For more on ISAOs visit www.isao.org/about.

ONG-ISAC

National Defense ISAC

FS-ISAC

RETAIL & HOSPITALITY ISAC

Real Estate ISAC Information Sharing and Analysis Center
Serving the Commercial Facilities Sector

WATER ISAC

SPACE ISAC

CISA Cybersecurity & Infrastructure Security Agency

Maritime Transportation System Information Sharing and Analysis Center

ME ISAC MEDIA + ENTERTAINMENT INFORMATION SHARING ANALYSIS CENTER

REN-ISAC

IT ISAC

DNG-ISAC

H-ISAC HEALTH · ISAC

AVIATION ISAC

E-ISAC

AUTO-ISAC Automotive Information Sharing and Analysis Center

TLP: GREEN

State and Local Cybersecurity Grant Program

State and Local Cybersecurity Grant Program (SLCGP)

- Eligible recipients are States, territories and Federally-recognized tribes
- **Subawards made to counties and local governments**
- Multi-state/tribe projects also allowed
- $1B over 4 years
  - **FEMA administers** the grant program; **CISA serves as subject matter expert**
  - Baseline allocation plus population-based allocation formula
  - 80% passthrough to local entities
  - 25% of passthrough must go to rural areas (49 USC 5302)
  - SLTT cost share increases each year

Annual Funding	Federal Cost Share
• FY22: $200M	• FY22: 90%
• FY23: $400M	• FY23: 80%
• FY24: $300M	• FY24: 70%
• FY25: $100M	• FY25: 60%

- Allowed uses of funds
  - Develop and revise Cybersecurity Plan
  - Implement Cybersecurity Plan – individual projects
  - Grant administration (5%)
  - Address imminent cybersecurity threats, as confirmed by the DHS Secretary, acting through the CISA Director
  - Fund any other appropriate activity determined by the DHS Secretary, acting through the CISA Director

SHIELDS UP

To Wrap Up: Key Takeaways

1. Become familiar with CISA webpage and Subscribe to CISA Advisories
   - www.cisa.gov
2. Engage with your local CISA region and get in contact with your CSC/CSA
   - https://www.cisa.gov/cisa-regions
3. Sign-up for CISA's cyber hygiene services and other resilience services
   - Engage your local CSC
4. Sign up to be MS-ISAC member
   - https://www.cisecurity.org/ms-isac
5. Encourage lowering cyber incident reporting thresholds

No-Cost CISA Cybersecurity Services Available

- **Preparedness Resources**
  - Cybersecurity Assessments
  - Cybersecurity Training and Awareness
  - Cyber Exercises and "Playbooks"
  - Cybersecurity Advisories and Alerts
  - Operational Products / Threat Indicator Sharing
  - Known Exploited Vulnerabilities (KEV) Catalog
  - Cybersecurity Performance Goals (CPGs)
  - Free Cybersecurity Tools and Services Catalog
  - Information Products and Recommended Practices

- **Response Assistance**
  - 24/7 Response assistance and malware analysis
  - Incident Coordination
  - Threat intelligence and information sharing
- **Cybersecurity Advisors & Cybersecurity State Coordinators**
  - Advisory Assistance & Cyber Protective Visits
  - Cybersecurity Assessments and Workshops
  - Incident Response Coordination
  - Public Private Partnership Development

CISA Contact Information

Arnold Webster, CSC, Region 3 **General CISA Inquiries**	arnold.webster@cisa.dhs.gov CISARegion3@cisa.dhs.gov
CISA URL	https://www.cisa.gov
To Report a Cyber Incident to CISA	*Call 1-888-282-0870* *Email report@cisa.gov* *visit https://www.cisa.gov*

QUESTIONS?


CYBERSECURITY & INFRASTRUCTURE
SECURITY AGENCY
CISA

VIRGINIA IT AGENCY

2023 KEYSTONE EDGE UPGRADE

SERENA SINGLETON

MSI Program Manager

ISOAG ANNOUNCEMENT

SEPTEMBER 6, 2023

UPGRADE TO UTAH VERSION

- Upgrade Scheduled for Sept 29th at 11:15 pm
- 90-Minute Outage – Portal and Catalog will be unavailable
- VCCC will be available via phone and email
- Agency users will not notice changes; however, significant internal upgrades will be completed
- Additional communications and reminders will be sent closer to go-live

UPCOMING EVENTS

COVITS 2023
Wednesday, September 13, 2023
Open to Public Sector only.

Registration — $45

https://events.govtech.com/covits.html

The next scheduled meeting for the IS Council:

September 20, 2023

12 p.m. – 1 p.m. (virtual)

If you would like an invite to the meeting, contact:

commonwealthsecurity@vita.virginia.gov

IS ORIENTATION

IS Orientation

Remote – WebEx

Date: September 27, 2023

Start time: 1:00 p.m. End time: 3:00 p.m.

Instructors: Erica Bland, Renea Dickerson, and Tina Gaines

https://vita2.virginia.gov/Events/chooseSession?MeetingID=10

*There are IS Orientations scheduled every month until the end of the calendar year.

October ISOAG Meeting

OCTOBER ISOAG

The mandatory October ISOAG meeting held on Oct. 4, will be an in-person event!

We look forward to seeing everyone in person at the Brightpoint Community College's "Talley Workforce Center" at 13101 Route 1 Chester, Virginia 23831. This is an opportunity to catch up with your fellow Information Security Officers in person, to enjoy informative presentations, and mingle. Seating is limited to 200, please reserve your place at this in-person event! If you are unable to attend in person and need someone to attend in your place, please notify Commonwealth Security.

https://covaconf.webex.com/weblink/register/r4833c34fb6f35f38167b2799374e4962

Cybersecurity Awareness Month

1. If you are planning any events for Cybersecurity awareness month, please let Commonwealth Security know. We will add them to our upcoming events for the October ISOAG meeting.
2. If you are interested in participating in a video for Cybersecurity Awareness month, please send an email to commonwealthsecurity@vita.virginia.gov

2023 RVATech/Women in Technology

Date: October 25, 2023

Location: Dominion Energy Center, 600 East Grace Street

Featured Speakers: Amy Braden, Debi Smith, Diane Carnohan, and Stephanie Williams-Hayes.

https://rvatech.com/rvatech-events/2023-women-in-tech-conference/

MEETING ADJOURNED

VIRGINIA
IT AGENCY