VIRGINIA
IT AGENCY

Welcome to the October ISOAG Meeting

Information Security Officers
Advisory Group

VIRGINIA IT AGENCY

Information Security Officers Advisory Group Meeting
October 2, 2024

Welcome/opening remarks	Amy Braden
Governance & Compliance	Amy Braden
Enterprise Architecture	Stephen Smith
Centralized Audit services	Cory Rutledge
Threat Management	Dean Johnson or Kathy Bortle
Risk management	Matthew Steinbach
Security Architecture	Chandos Carrow
security products & services	Richard White
Recap	Trey Stevens
And	Mike Watson
Closing Remarks	

VIRGINIA
IT AGENCY

IT Security Governance & Compliance

Annual Update

Amy Braden, Director, IT Security Governance and Compliance

Welcome & Congratulations!

New to Governance

Amira Yagoub

Mark Jeffrey

Josh Kropka

Retirements

Tina Gaines

Renea Dickerson

Key Governance & Compliance Notes

Annual Grades

- Uptick in 2023 compliance grades!
- NCSR Assessment participation very low, approximately 29 organizations.
- Please plan now to submit deliverables **prior to 12/31/2024**.
- Increased in person opportunities 2025.

Security Awareness Training

It is that time of year to ensure SAT training is complete.

- A distinct SAT training campaign for phishing is now available. We recommend deploying and tracking campaign separately. Note this is expected to have immediate deadlines and additional reporting requirements.

- Please ensure all SAT monitoring and tracking is in place.

- Please contact Wesley.Dupree@vita.virginia.gov with any SAT questions.

Key Education & Communication Notes

Resource enhancements

- New VITA Connections site for AITRS and ISOs
- Increased interest for in-person ISO training
- Expect office hours with CSRM Governance staffers in 2025

Key CISS ISO Services Notes

- DBP change: general funding for still available but as part of agency budget. Please contact DBP for any questions regarding funding allocation or planning questions.
- CISS Team organized by functional area (vs. customer agency). We are continuing to backfill positions and are planning to grow the team.
- New MOU structured as SOW/project work for key security deliverables.

To the entire team and you, thank you!

VIRGINIA
IT AGENCY

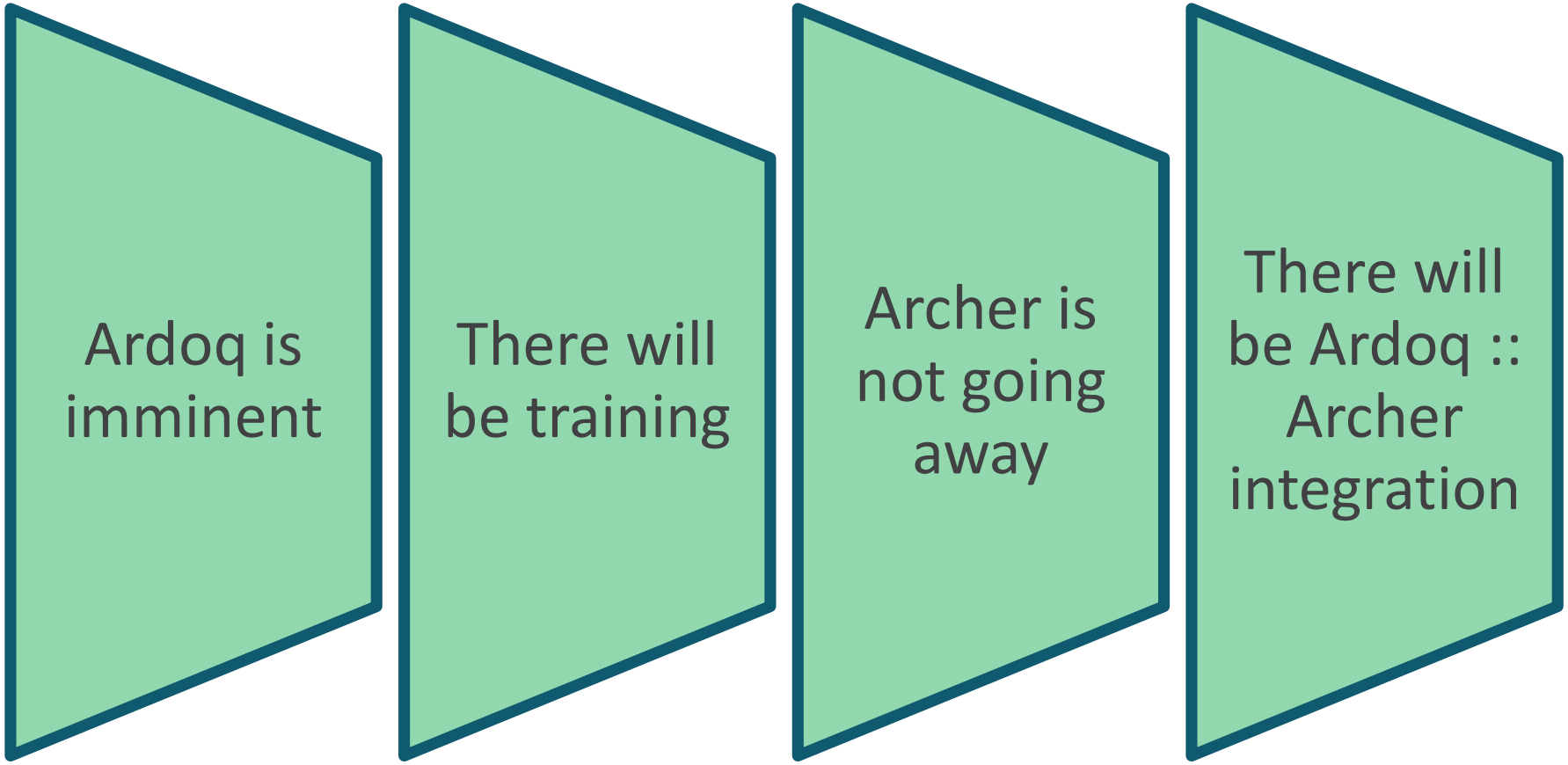
Ardoq (Again)!

ISOAG

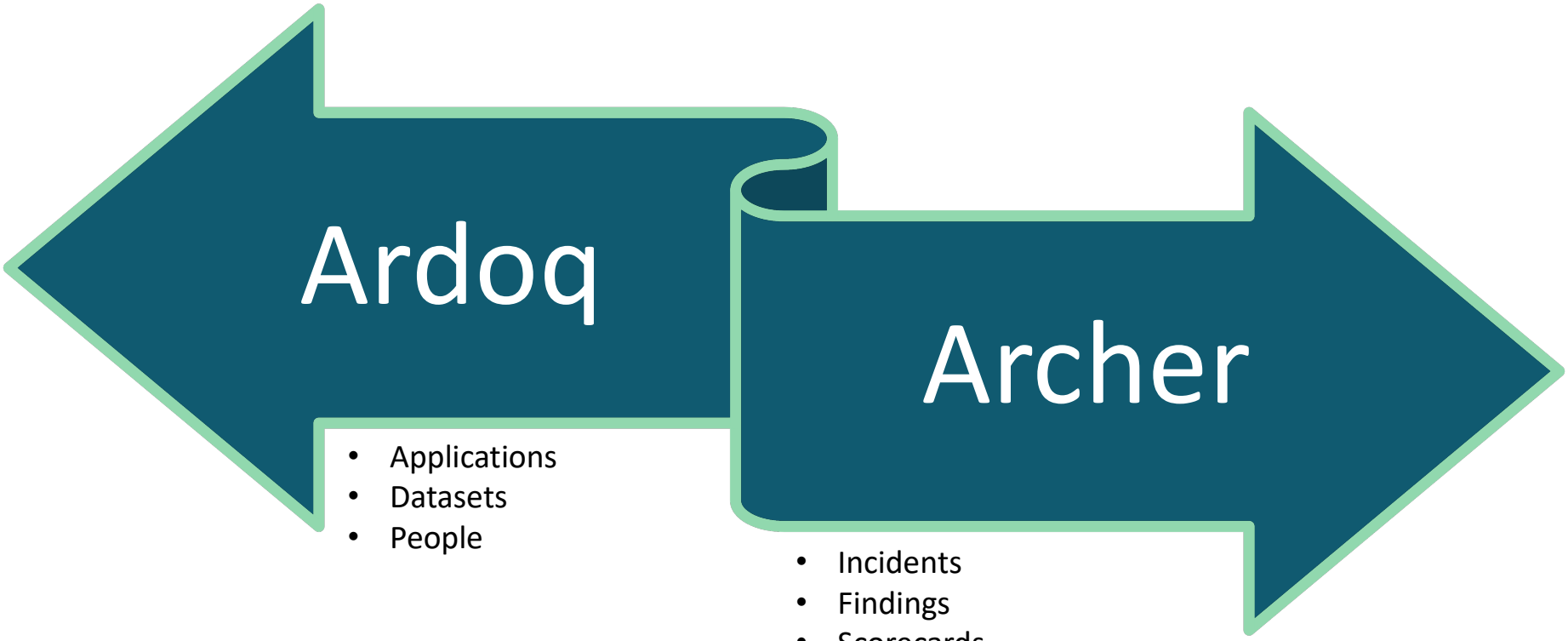
Stephen Smith
Enterprise Architecture Manager

October 2024

The one slide to remember



What it means for you



- Applications
- Datasets
- People

- Incidents
- Findings
- Scorecards
- Audits
- Business Processes

What's the value?

- Portfolio visibility
- Technology roadmaps
- Planning and versioning

Questions

???

VIRGINIA
IT AGENCY

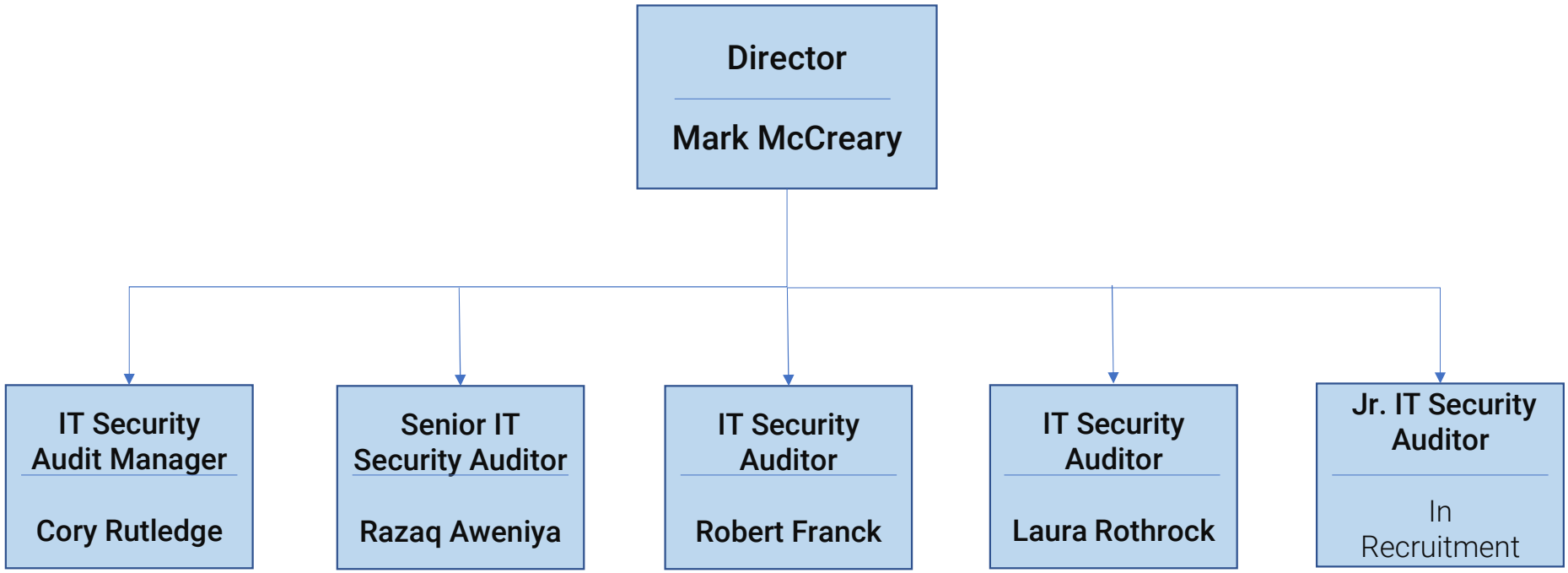
Centralized IT Security Audit Service

Mark McCreary, CISA®, CISSP®, CISM®
Director
Cory Rutledge, CISA®
Manager

Centralized IT Security Audit Service (CITSAS)

- Audit Team
- Mission Statement
- Memorandum of Understanding
- Risk-Based IT Security Audits
- Audit Plan Assistance

Audit Team


Director
Mark McCreary
IT Security Audit Manager
Cory Rutledge
Senior IT Security Auditor
Razaq Aweniya
IT Security Auditor
Robert Franck
IT Security Auditor
Laura Rothrock
Jr. IT Security Auditor
In Recruitment

CITSAS Mission Statement

To provide cost-effective evaluations of the controls protecting sensitive systems and data for the agencies we serve.

Memorandum of Understanding

- Identifies the in-scope sensitive systems.
- Covers the three-year Audit cycle.
- Deliverable = One Audit Report per cycle covering the in-scope systems.
- Total charge is spit into three installment payments.

Risk-Based IT Security Audits

We Determine High-Risk Areas By:

- Evaluating *Pre-Audit Internal Control Questionnaire(s)*
- Evaluating results of other audits or reviews
  - System and Organization Controls (SOC) Reports
  - Prior Audit Reports, Outstanding Findings
- Evaluating controls for Hosted Applications
  - Emphasis placed primarily on areas the agency controls, for example, Access Controls and Contingency Planning
- Reviewing Security Exceptions

Risk-Based IT Security Audits

We Conduct Our IT Security Audits By:

- Reviewing documented policies and procedures to determine completeness.
- Interviewing key personnel.
- Performing tests to determine compliance with COV Security Standards.
- Performing tests to determine whether internal controls function as intended.

Audit Plan Assistance

We Assist with Audit Plan Development By:

- Establishing and/or Updating Memoranda of Understanding with Customers.
- Providing Customers with Latest Planning and Budget Information.
- Confirming In-Scope Systems.
- Providing Estimated Audit Timeframes.

Common Issues

- No Formally Documented and Approved IT Security Policies and Procedures
- ISO does not report to the Agency Head
- Account Management
  - Inappropriate privileges for regular COV accounts.
  - Not Disabling Inactive Accounts
- Lack of Multifactor Authentication

Common Issues

- Findings Closed Before Remediation
- Security Exceptions Not Submitted
- No Alternate or Manual Procedures in COOP for MEFs
- No Implementation of Multifactor Authentication
- No Audit Log Review

Questions

Mark McCreary
Mark.McCreary@vita.virginia.gov
(804) 510-7095

Cory Rutledge
Cory.Rutledge@vita.virginia.gov
(804) 510-7257

VIRGINIA
IT AGENCY

Threat Management

Dean Johnson – Director, Threat Management

Kathy Bortle – Manager, Threat Intel and Vulnerability
Scott Brinkley – Manager, Incident Response

Incident Response

Incident Response Process Documentation Project 2024

- Rework of the original Incident Response Playbook with Subprocesses
- Flexibility in updates
- Not perfect

Incident Response Automation Initiative

- Forensic Investigative Authorization Request (FIAR)
- Splunk Incident Response Automation
  - Quick Visibility
  - Dashboard

Threat Intelligence and Vulnerability Management

Threat Intelligence

- Phishing (Ramped Up Campaigns)
- KnowBe4 (ADISync)

Vulnerability Management

- Acunetix 360 Scanning Upgrades - (Increased Scanning Capacity)
- Nucleus – Insight into Vulnerability

5 Key Vulnerabilities

For the Month of October, the Top 5 Key Vulnerabilities are:

- **Dropbear SSH Server < 2016.72 Multiple Vulnerabilities**
- **KB5039217: Windows 10 version 1809 / Windows Server 2019 Security Update (June 2024)**
- **Oracle Database Server (Apr 2024 CPU)**
- **IBM WebSphere Application Server 8.5.x < 8.5.5.20 / 9.x < 9.0.5.8 RCE (6891111)**
- **Apache 2.4.x < 2.4.60 Multiple Vulnerabilities**

Questions?

VIRGINIA
IT AGENCY

Risk Management Update

VITA Risk Management

Matt Steinbach

Manager, Risk Management

Risk Findings

Emphasis on analyzing threats and vulnerabilities as part of risk assessments

- Goal for 2025 is to move away from control-based risk findings to better emphasize threat and vulnerability models
- ISO input regarding these changes is welcome- feel free to reach out or discuss at the monthly risk council meeting
- Any 520 updates would go through ORCA

Risk analysts may review: Agency Risk Assessments, Risk Treatment Plans, and Risk Finding Updates

Risk Findings Cleanup

CSRM is working to close outdated findings, please help us in this effort

- Identify any applications that have been retired
- Close risk findings that are no longer applicable
- Close outdated risk findings that are stagnant
- Close risk findings that are no longer providing value to be tracked
- Any control-based finding that is still not remediated, file an exception and close the finding
- Risk analysts can work with you on a case by case basis
- Removed SCAN and Vuln-X findings and removed those source overrides.
    - Nucleus is now the system of record for findings

Risk Escalation & Risk Alerts

VITA and CSRM are implementing new and improved tools for agencies and CSRM to better assess vulnerabilities, issues and risks within the Commonwealth enterprise

- Agencies can expect an increase in risk notifications, escalations, and alerts from CSRM
- Some examples of issues that may warrant risk notification, escalations, or alerts are:
  - Security and risk program systemic issues (annual program scores/grades)
  - Findings remediation
  - Vulnerability scan remediation
  - Security incidents and remediation
  - Identity and access management

Nationwide Cybersecurity Review

The NCSR is a no-cost, anonymous, maturity based, annual self-assessment. All states (and agencies), local governments (and departments), tribal nations, and territorial (SLTT) governments are encouraged to participate. It is designed to measure gaps and capabilities of SLTT governments' cybersecurity programs and is based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)

Score	Maturity Level *The recommended minimum maturity level is set at a score of 5 and higher*
7	**Optimized:** Your organization has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness.
6	**Tested and Verified:** Your organization has formally documented policies, standards, and procedures. Implementation is tested and verified.
5	**Implementation in Process:** Your organization has formally documented policies, standards, and procedures and is in the process of implementation.
5	**Risk Formally Accepted:** Your organization has chosen not to implement based on a risk assessment.
4	**Partially Documented Standards and/or Procedures:** Your organization has a formal policy in place and begun the process of developing documented standards and/or procedures to support the policy.
3	**Documented Policy:** Your organization has a formal policy in place.
2	**Informally Performed:** Activities and processes may be substantially performed and technologies may be available to achieve this objective, but they are undocumented and/or not formally approved by management.
1	**Not Performed:** Activities, processes and technologies are not in place to achieve the referenced objective.

Nationwide Cybersecurity Review

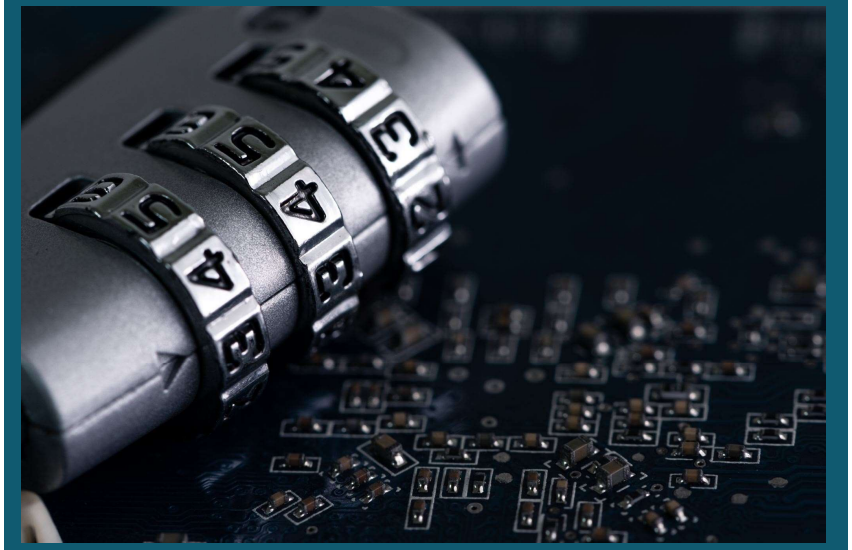
Benefits

- Receive metrics specific to your organization to identify gaps and develop a benchmark to gauge year-to-year progress, as well as anonymously measure your results against your peers.
- Attain reporting and resources that can help you prioritize next steps towards desired cybersecurity improvement. For HIPAA compliant agencies, translate your NCSR scores to the HIPAA Security Rule scores of an automatic self-assessment tool.
- Gain access to a repository of informative references, such as NIST 800-53, COBIT, and the CIS Controls that can assist in managing cybersecurity risk.
- Fulfill the NCSR assessment requirement for the Homeland Security Grant Program (HSGP). Additional information located here: https://www.fema.gov/homeland-security-grant-program.

2024 COV Cybersecurity Tabletop Exercise

Completed August 8, 2024

- Thank you to all the agencies who participated this year and thank you to SAIC and Iron Bow for running the exercise
- Please be on the lookout for signing up in Spring of 2025 to participate next year



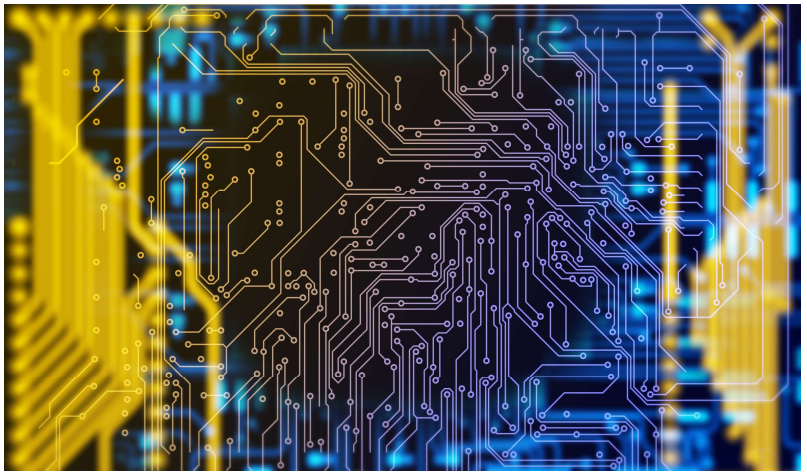
VIRGINIA
IT AGENCY

Security Architecture

Chandos Carrow
Security Architecture Manager

Updates from SA

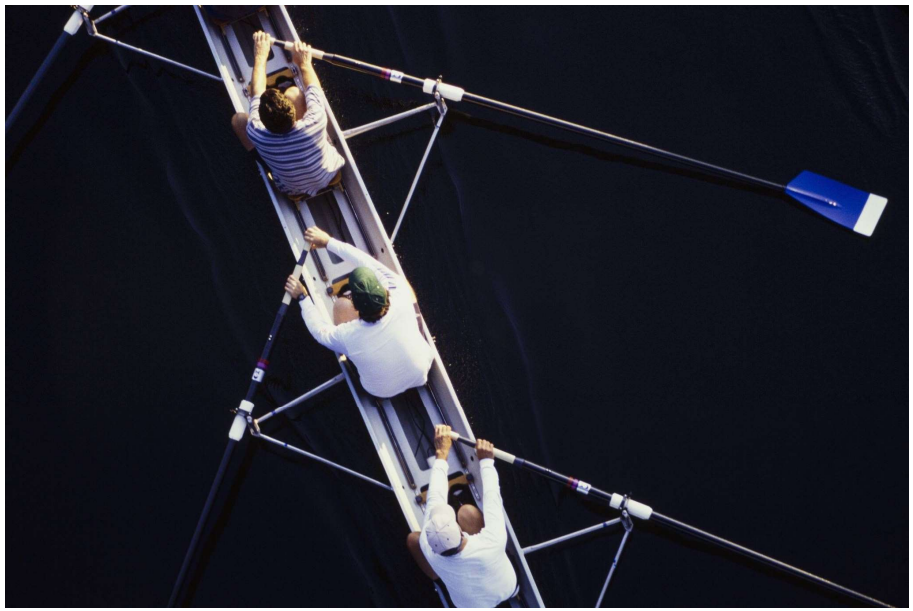
- System Security Plan templates
  - Four templates out on VITA website
- Administrative Changes to SEC530 on the way
- New Process for Security Exceptions
  - If a security exception or extension request has been in the status of Awaiting Agency Feedback for more than two weeks, the exception will be Withdrawn and a new exception will need to be filed
- Supplier SSP Evaluation Team



Thank you! And thank you to my team!

- Jacquelyn Esters
- Preston Talbott

- Questions?



VIRGINIA
IT AGENCY

VITA Products and Services Update

Richard White, Director of Security Products and Services


splunk>
Splunk Update
October 2024

• SPLUNK UPDATE OCTOBER 2024

Current Applications Being Ingested

- Box
- O365
- Azure
- AWS
- OCI
- CrowdStrike
- JAMF Pro
- OKTA
- Linux
- Windows
- AWS
- Docker
- InsightQ
- Area 1

• SPLUNK UPDATE OCTOBER 2024

Agencies we are currently working with:

- DMAS
- TRS
- DOF
- DOA
- DPB
- DJJ
- UNISYS
- DSBSD
- VDH
- VDOT
- TAX
- CSA
- DSS
- VITA
- VDA
- DPOR
- IRONBOW
- DHCD
- DCR
- DSBSD
- VSP

• SPLUNK UPDATE OCTOBER 2024

Splunk Enterprise Security

- Comprehensive visibility searching and analyzing any data at scale.
- Insights into risk with customizable dashboards, visualizations, and reports.
- Prioritize with context using risk-based alerting to focus on imminent threats.
- Unified threat detection, investigation and response using a modern work surface.

• SPLUNK UPDATE OCTOBER 2024

Splunk SOAR

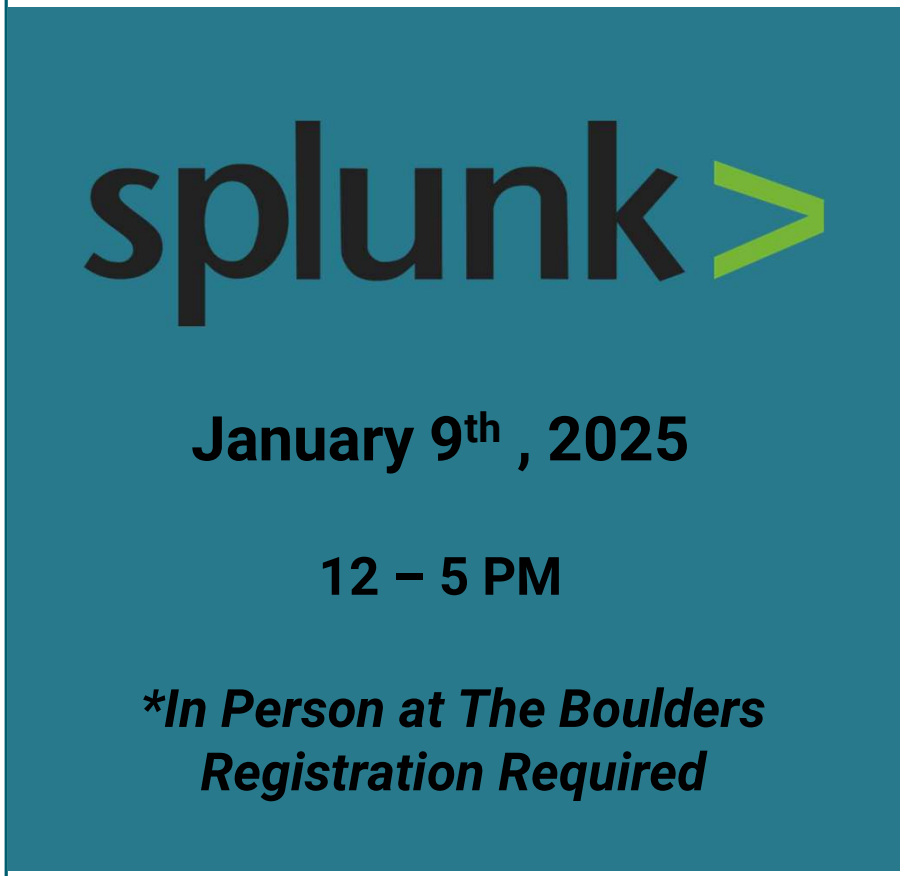
- Enhance team productivity with automation for speed and efficiency.
- Take prioritized actions to act on the most pressing threats.
- Respond with threat context for common threats automatically.
- Automate with ease using pre-built playbooks, integrations, or build customized playbooks.

- **SPLUNK UPDATE OCTOBER 2024**

WE WANT YOUR LOGS:

VITA is starting to work with agencies to ingest their application logs in to the VITA Splunk instance. We ask that all agencies start identifying what logs you would like to have ingested. We are always happy to schedule a call to review your options.

• SPLUNK UPDATE OCTOBER 2024



VITA will be hosting our fourth Splunk Lunch & Learn. This will be a continuation in the series. Investigating with Splunk pt.2 :

Investigating with Splunk is a modular, hands-on workshop designed to familiarize participants with how to investigate incidents using Splunk and open source. This workshop provides users a way to gain experience searching in Splunk to answer specific questions related to an investigation. These questions are similar to what would be asked in their own organizations. The workshop leverages the popular Boss of the SOC (BOTS) dataset in a question and answer format. Users will leave with a better understanding of how Splunk can be used to investigate in their enterprise.

SailPoint Update October 2024

SAILPOINT UPDATE OCTOBER 2024

What is SailPoint

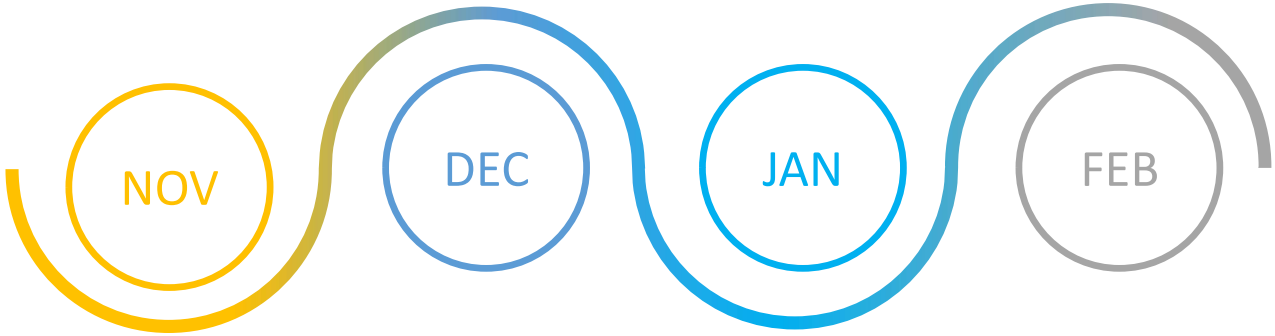
SailPoint enables automation of Identity and Access Management for the Commonwealth. COV Access enables agencies to directly manage and control access to critical systems and information.

Key Benefits of SailPoint IAM:

- **Role - Based Access Control**
  - Regulate Systems and Network Access based on roles and groups according to job function, authority and responsibility within the organization
  - Predefine Structured Users Groups to ensure secure access to within your agency.
- **Automation Lifecycle Management**
  - Allocate and retract user access rights, streamlining the access lifecycle management for all users
  - Allows for the automation of Onboarding, Offboarding of employees and Contractors
  - Automated Access Changes including Separation of duties
- **Cloud –Based Solution**
  - Cloud Based platform that benefit from enhanced infrastructure and Artificial Intelligence (AI).
- **Integrations with KSE**
- **Leveraging existing KSE Service Catalog forms for seamless automation and integration**

• SAILPOINT UPDATE OCTOBER 2024

Initial Deployment Timeline



VITA Internal Testing
VITA will test SailPoint for its staff.

Pilot Agencies
VITA will start working with pilot agencies on their implementation.

Pilot & Test Review
VITA will review feedback from internal staff and pilot agencies. Create plan for general roll out of MVP.

Remaining Agencies
VITA will start working with remaining agencies on their SailPoint deployment

SAILPOINT UPDATE OCTOBER 2024

Initial Deployment Functions

- **Automated Onboarding of Identities:** Automate and expedite the integration of new identities with streamlined onboarding processes.
- **Automated Off-boarding of Identities:** Ensure a secure and efficient departure process with our automated off-boarding feature.
- **Urgent Account Disablement:** Implement immediate account suspension with our rapid-response disablement capability.
- **Urgent Account Re-enablement:** Restore account access swiftly and securely with urgent re-enablement procedures.
- **COV AD Group Modifications:** Manage and adjust Active Directory groups with ease using our intuitive modification tools.
- **Employee/Non-employee Identity Collection:** Collect and differentiate between employee and non-employee identities with precision.
- **Cloud Source Connections:** Integrate effortlessly with various cloud services for a unified identity management experience.

SAILPOINT UPDATE OCTOBER 2024

What can you do to prepare?

- Define your Roles
  - Define standard and privileged roles used throughout your agency.
  - Determine default system privileges needed for resources based on roles and location.
- Review your Agency Security Groups
  - Security groups are used to organize user accounts, computer accounts and other groups into manageable units and to provide permissions and access to resources and tasks through AD
- Define location/ department-based entitlements
- Define your Key Stakeholders
- Validate Service Accounts

VIRGINIA
IT AGENCY

Closing Remarks

Mike Watson/Trey Stevens

Upcoming Events

VIRGINIA
IT AGENCY
vita.virginia.gov

October is Cybersecurity Awareness Month

October is Cybersecurity Awareness Month

- Theme: Secure Our World

- Four Simple Ways to Stay Safe Online:
  - 1. Use Strong Passwords and a Password Manager
  - 2. Turn on multifactor authentication
  - 3. Recognize and report phishing
  - 4. Update software

Cybersecurity Awareness Month Resources

- https://staysafeonline.org/
- Cybersecurity Awareness Month Kit 2024 (knowbe4.com)
- https://www.govtech.com/blogs/lohrmann-on-cybersecurity/secure-our-world-cybersecurity-awareness-month-2024

VASCAN

October 10 – October 11, 2024

William & Mary Alumni House

500 Richmond Rd, Williamsburg, VA 23185

VASCAN

Registration link:
https://vascan.org/vascan-2024/

• Service Tower SOC Report Review Sessions

The upcoming SOC review session is October 10, 2024, and will be held remotely via WebEx. Please register at the link below

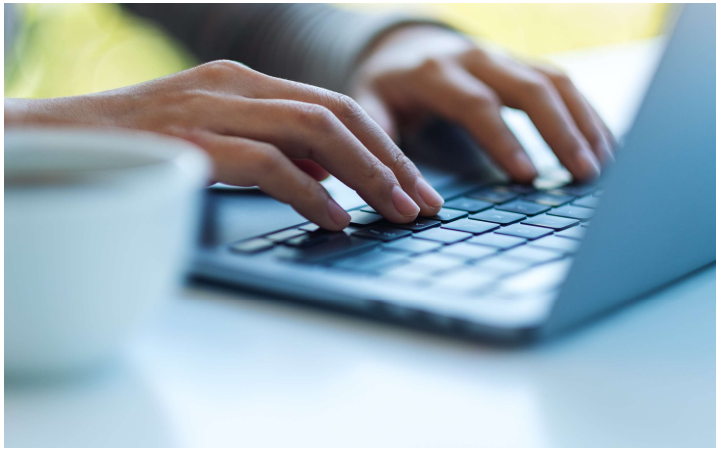
To register for this meeting, please click on the link below:
https://covaconf.webex.com/weblink/register/r9c8cb1394982eb22a7fa276a7f04fb91

IS Orientation

The next IS Orientation is being held on December 11th

- It will be held virtually via WebEx from 1pm-3pm
- Please register at the link below:

https://covaconf.webex.com/weblink/register/r95e66428081159841dc039e8b5d756d1



MEETING ADJOURNED

VIRGINIA
IT AGENCY