WELCOME TO THE DEC. 6, 2023 ISOAG MEETING

VIRGINIA IT AGENCY

Information Security Officer's Advisory Group

December 6, 2023

VIRGINIA
IT AGENCY

Agenda	Presenter
Welcome/Opening Remarks	Tina Gaines/ VITA
Tenable Product Demo	Gerson Matos/ Tenable
EA Standards	Stephen Smith/ VITA
Data Classification Standards	Amy Braden/ VITA
Organizational Risks and Issues – ORIs	Jon Smith/ VITA
Demo Splunk: OKTA Add On	Richard White/ VITA
Agency Datapoints	Amy Braden/ VITA
Upcoming Events	Tina Gaines/ VITA
Adjourn	

tenable®

Dynamic Defense - Tenable One helps you Achieving and Maintaining a Secure Network Environment

Sonya Hefferan
Territory Manager - SLED
Gerson Matos
Security Engineer - SLED
Anthony Rodriguez
Tenable | Cloud Security Specialist
Jim Nowak
Principal Security Engineer - Cloud Security

Agenda

Introductions

1. Recap from previous ISOAG call
2. Tenable ONE Overview
3. Tenable Cloud Security
4. Q&A

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

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**

On Prem & Remote IT

Internet-Facing Assets

Web Apps /APIs

Public Cloud

Industrial (OT) Infrastructure

Identity

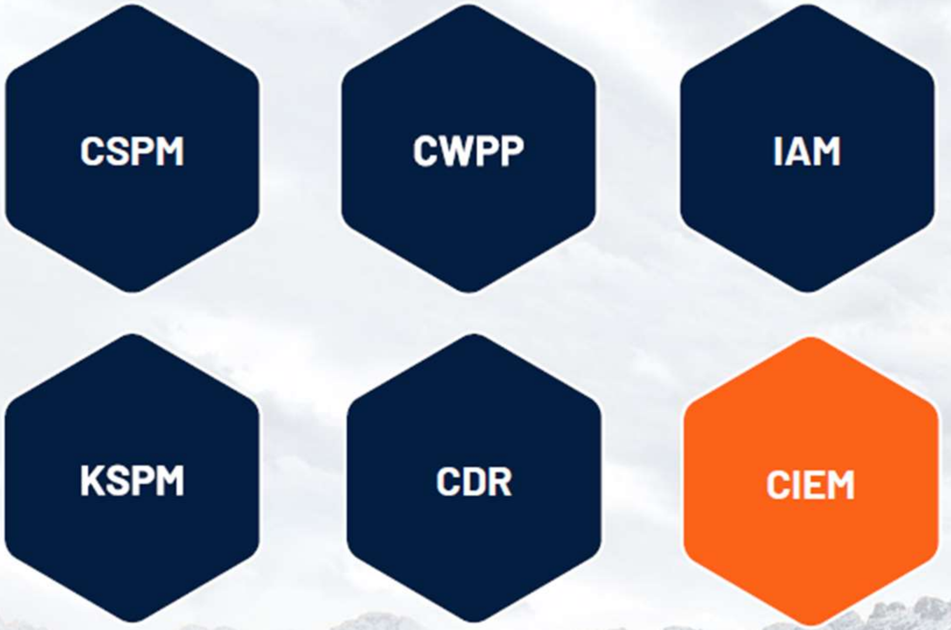
tenable

Use the Right Tool for the Job

Tenable One

Today's answers to these pains are point tools...

"< 30% have integrated security tools like CSPM, CWP, and CIEM across multiple cloud environments."
– CSA



CSPM

CWPP

IAM

KSPM

CDR

CIEM

"80% have suffered identity-related breaches in the last 12 months."
– IDSA Survey

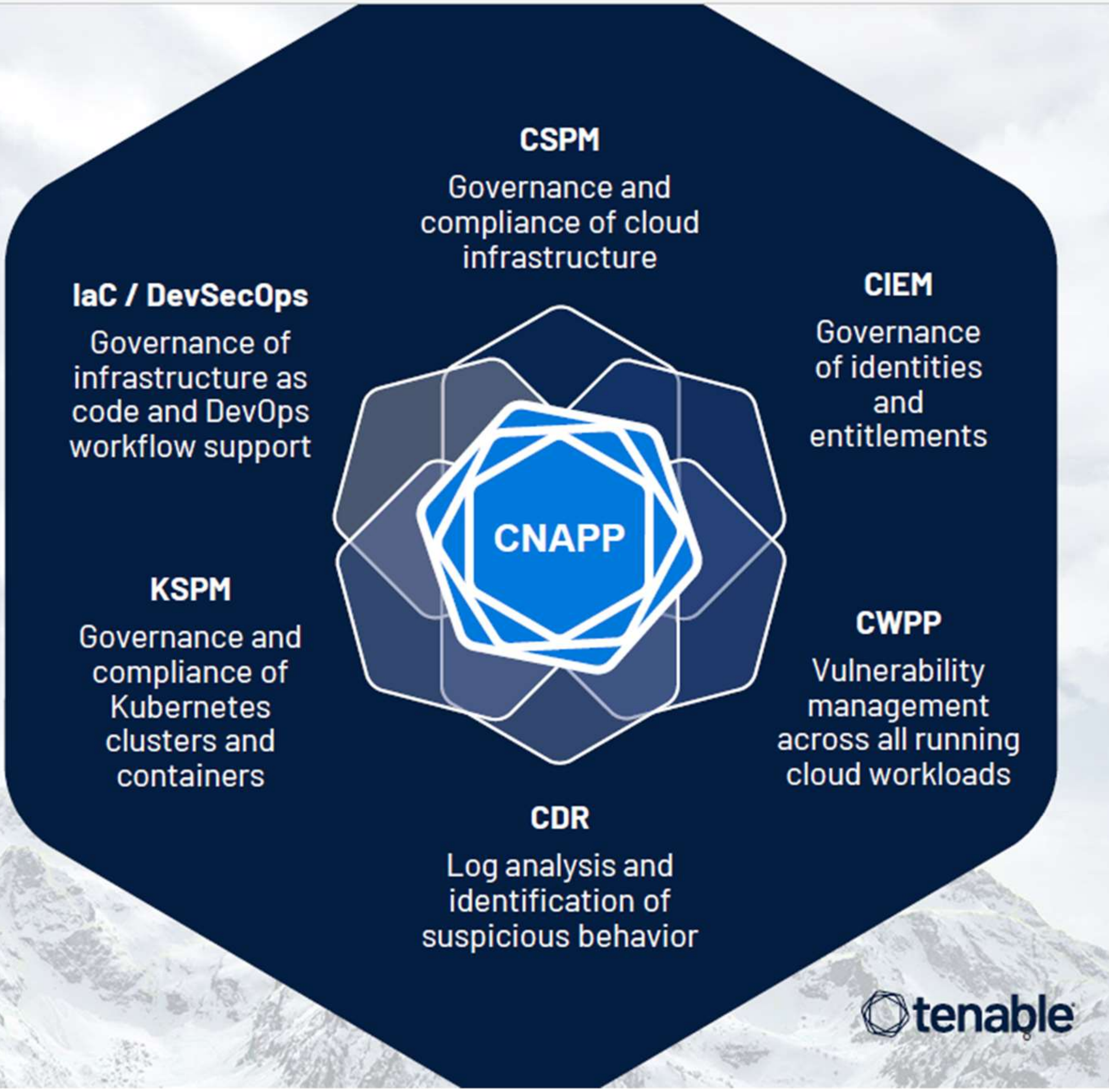
and lack sufficient identity security (CIEM)

*Sources: Cloud Security Alliance:: Cloud Native Application Protection Platform (CNAPP) Survey Report, August 2023
Identity Defined Security Alliance: 2022 Trends in Securing Digital Identities

Introducing the NEW Tenable Cloud Security

Holistic Protection for AWS, Azure and GCP in a **comprehensive CNAPP solution**.

AND the **industry leader in CIEM** to prevent identity-based breaches.



CSPM
Governance and compliance of cloud infrastructure

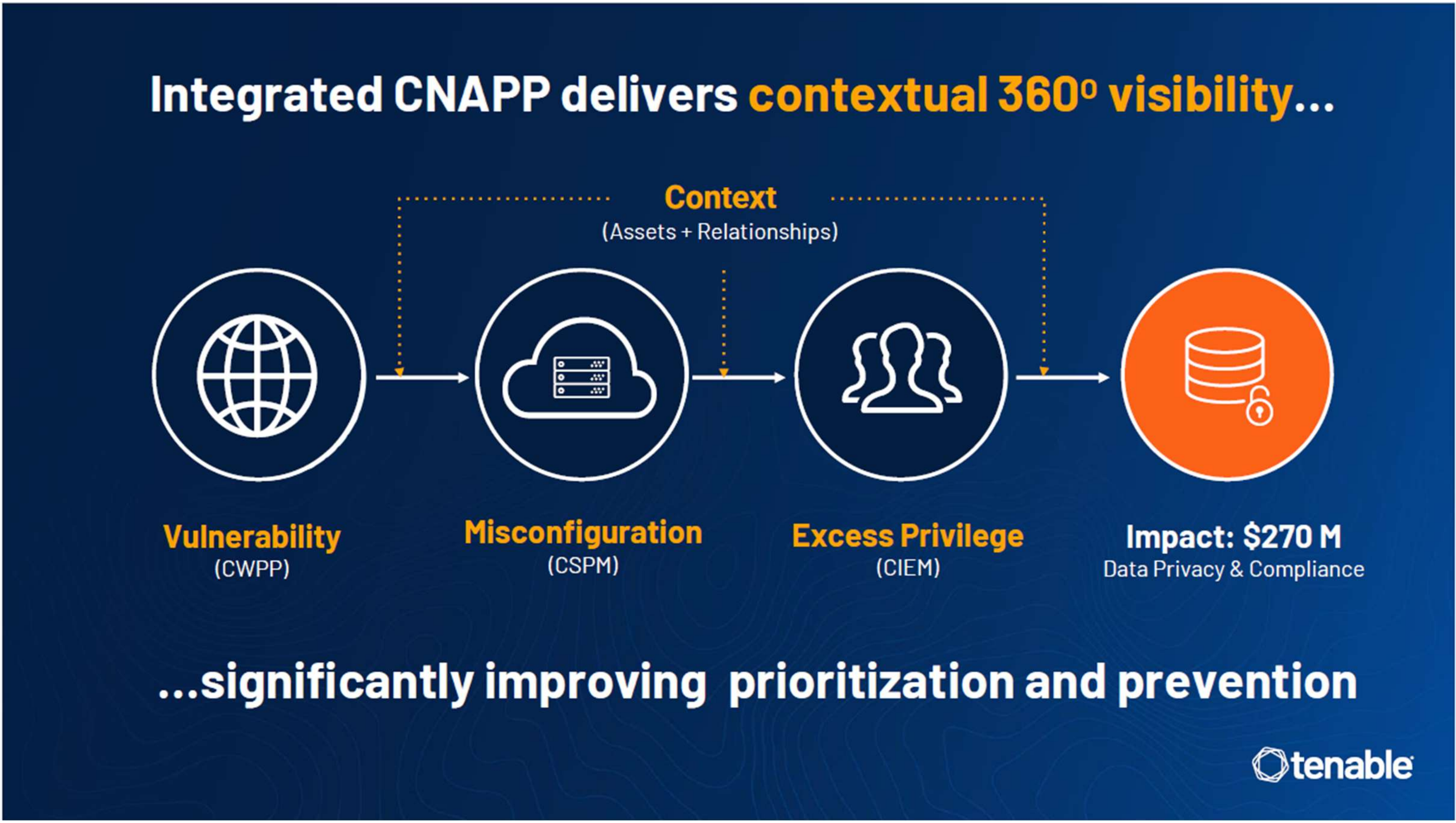
CIEM
Governance of identities and entitlements

CWPP
Vulnerability management across all running cloud workloads

CDR
Log analysis and identification of suspicious behavior

KSPM
Governance and compliance of Kubernetes clusters and containers

IaC / DevSecOps
Governance of infrastructure as code and DevOps workflow support



Integrated CNAPP delivers contextual 360° visibility...

Context

(Assets + Relationships)

Vulnerability

(CWPP)

Misconfiguration

(CSPM)

Excess Privilege

(CIEM)

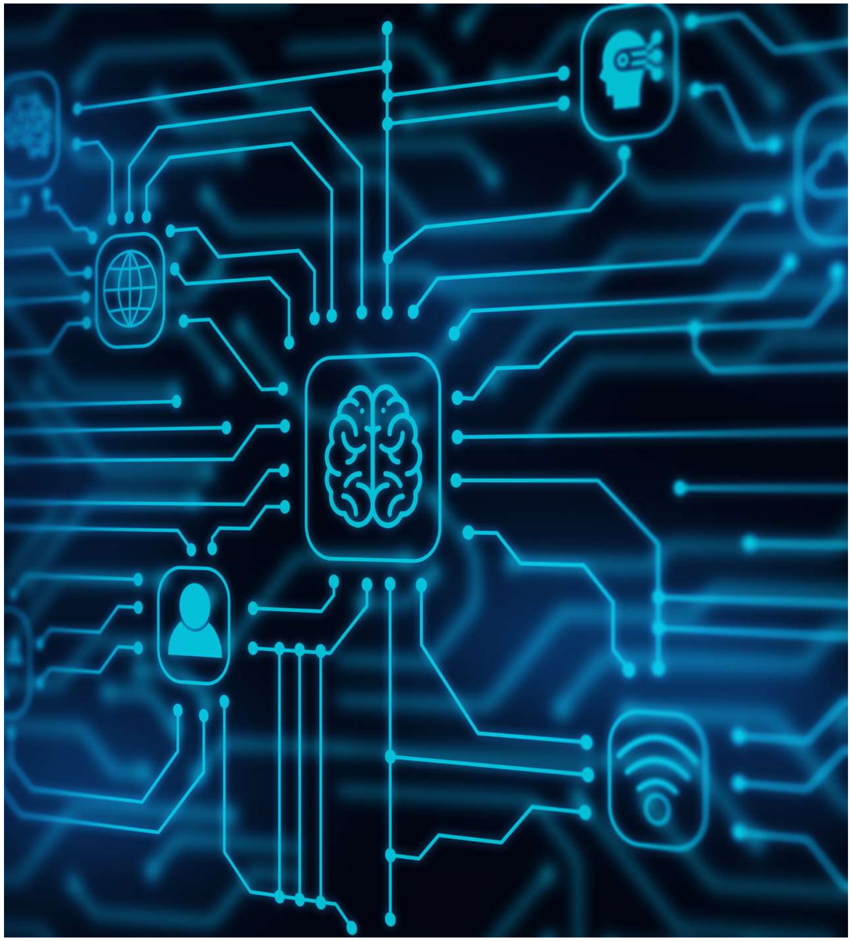
Impact: $270 M

Data Privacy & Compliance

...significantly improving prioritization and prevention

tenable

Thank You!



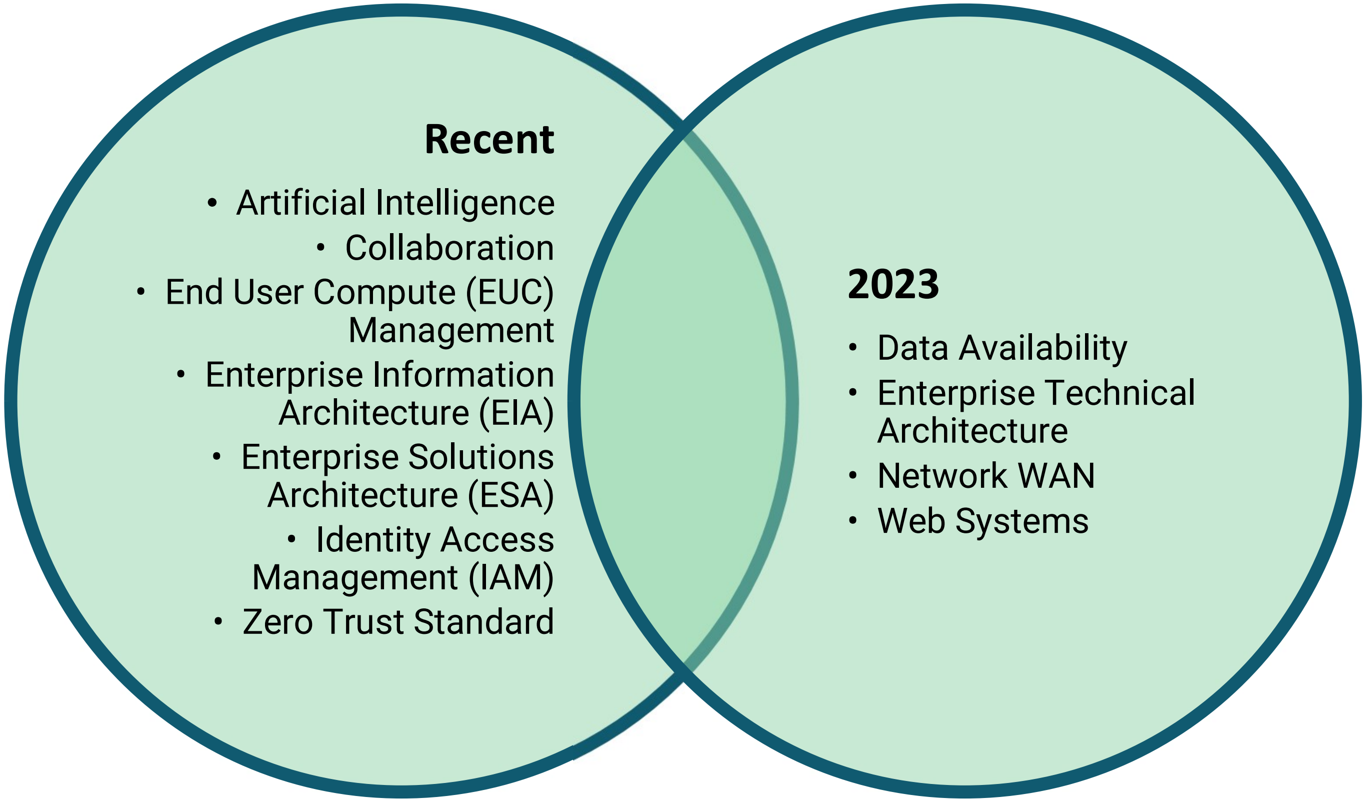
VIRGINIA IT AGENCY

New EA Standards!

Stephen Smith
Enterprise Architecture Manager

December 2023

Tidal Wave



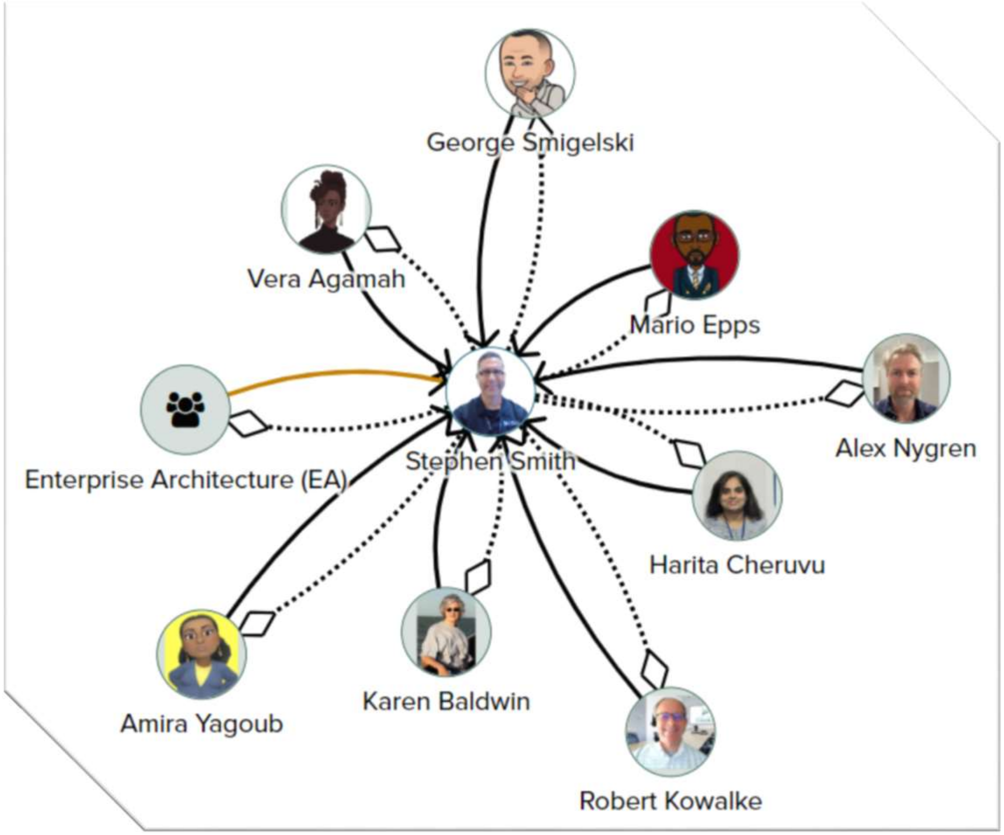
Recent

- Artificial Intelligence
- Collaboration
- End User Compute (EUC) Management
- Enterprise Information Architecture (EIA)
- Enterprise Solutions Architecture (ESA)
- Identity Access Management (IAM)
- Zero Trust Standard

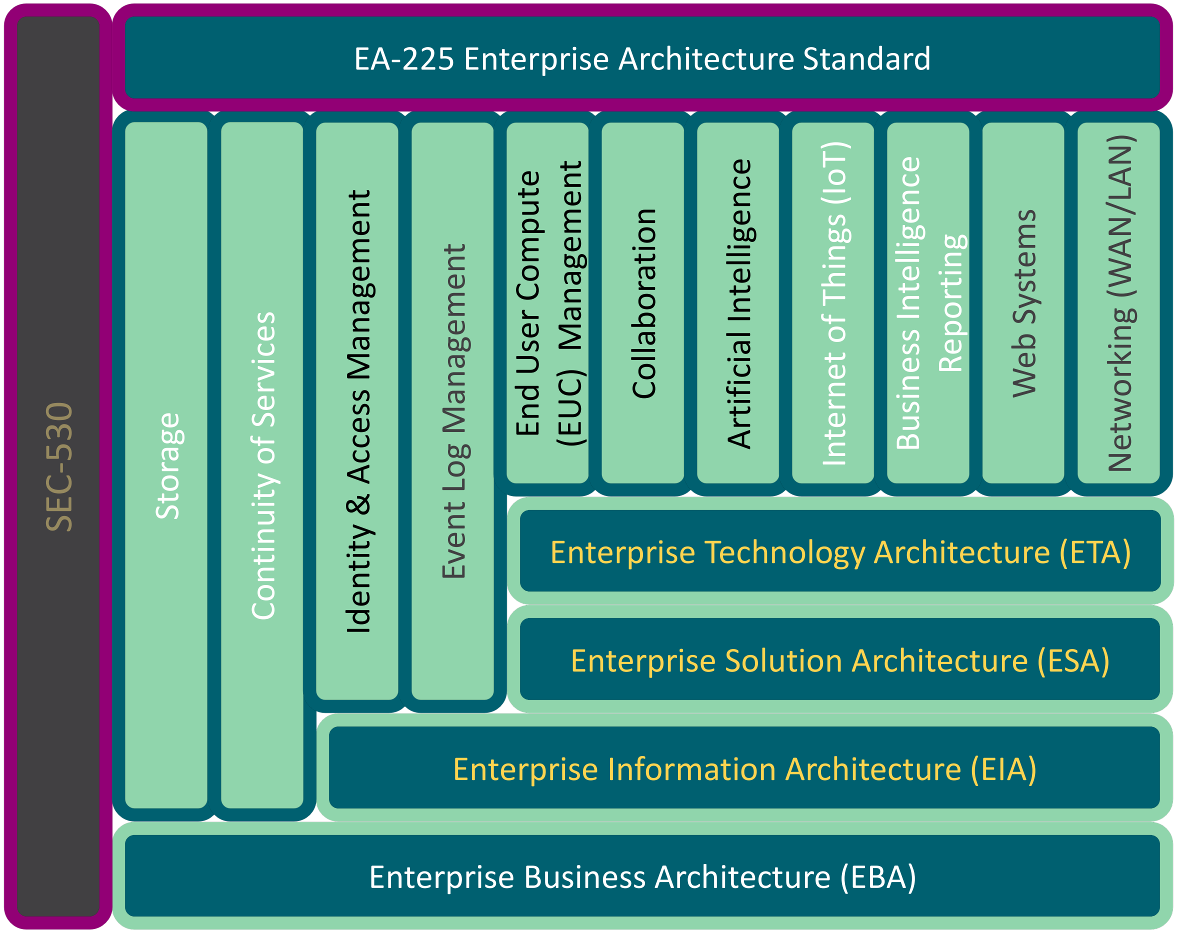
2023

- Data Availability
- Enterprise Technical Architecture
- Network WAN
- Web Systems

Fully Loaded



Standards Map



EA-225 Enterprise Architecture Standard

SEC-530

Storage

Continuity of Services

Identity & Access Management

Event Log Management

End User Compute (EUC) Management

Collaboration

Artificial Intelligence

Internet of Things (IoT)

Business Intelligence Reporting

Web Systems

Networking (WAN/LAN)

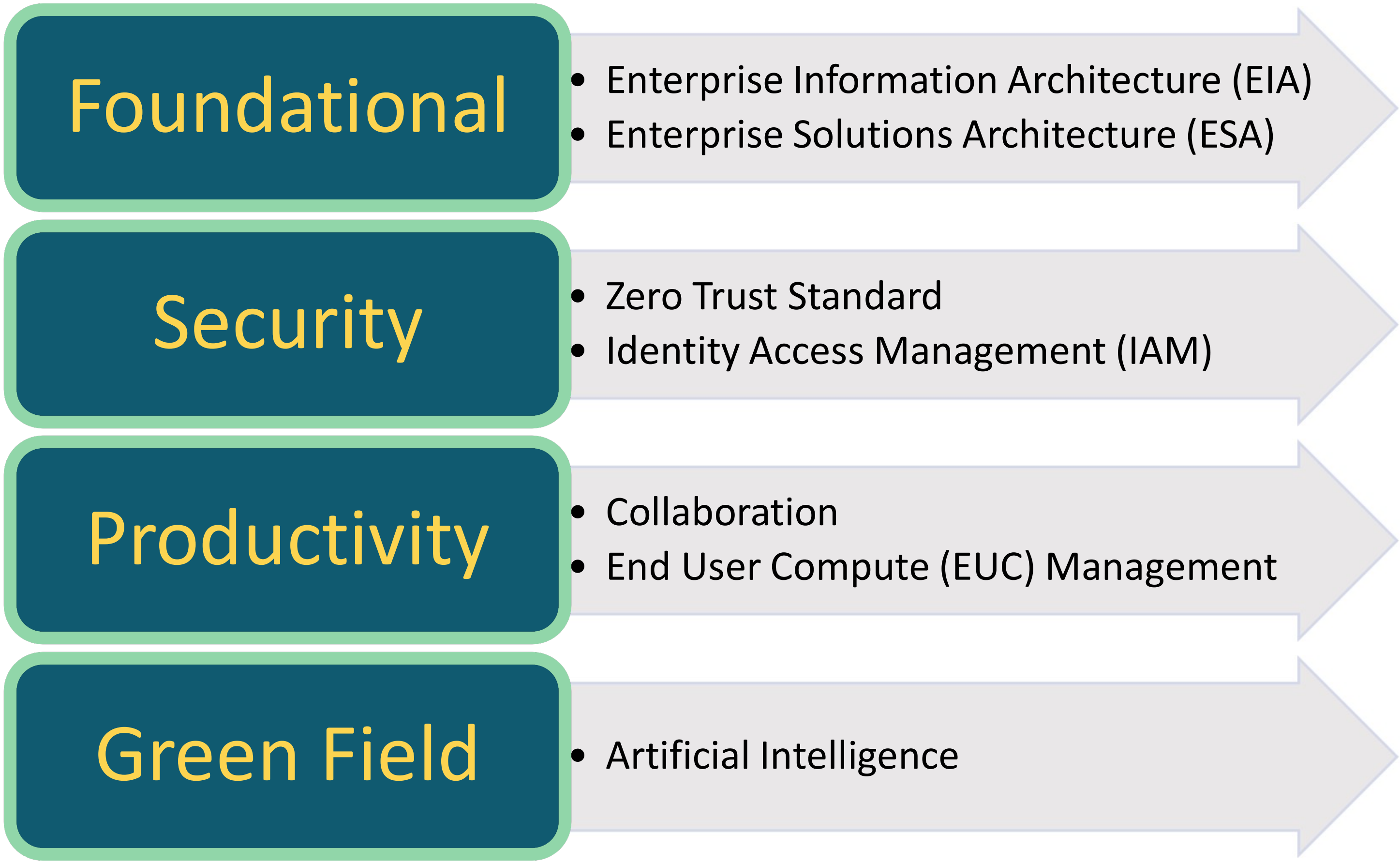
Enterprise Technology Architecture (ETA)

Enterprise Solution Architecture (ESA)

Enterprise Information Architecture (EIA)

Enterprise Business Architecture (EBA)

In Flight



Foundational
- Enterprise Information Architecture (EIA)
- Enterprise Solutions Architecture (ESA)

Security
- Zero Trust Standard
- Identity Access Management (IAM)

Productivity
- Collaboration
- End User Compute (EUC) Management

Green Field
- Artificial Intelligence

Questions

???

VIRGINIA IT AGENCY

Data Classification

For Data Loss Prevention

Commonwealth Security & Risk Management

December 2023

Agenda

- Overview of data loss prevention and data classification
- First steps planned to implement data loss prevention
    - Data Classification Standard
    - O365
- Questions

Purpose and Scope

The purpose of this presentation to provide an introduction of data loss prevention, review implementation approach, critical planning deliverables, and immediate next steps.

This presentation will be shared will AITRs, ISOs, CAMs, and CIOs throughout December.

What is data loss prevention (DLP)?

Data Loss Prevention is a combination of cybersecurity strategies and solutions designed to ***detect*** and ***prevent*** the loss, leakage, or misuse of data through data breaches, ex-filtration transmissions and ***unauthorized use*** of ***sensitive information***.

What are the key objectives of DLP?

- Identify and classify data to ensure sensitive information is protected appropriately
- Protect sensitive data while at rest, in transit, and during processing
- Prevent unauthorized disclosure of information by consistently:
  - Encrypting sensitive information
  - Storing data securely on authorized devices/media
  - Using appropriate destruction methods for sensitive information
  - Limiting access to authorized users, preventing unauthorized share or disclosure of sensitive information
  - Manage logging and audit of sensitive information consistently

What is data classification?

- Use a consistent taxonomy to quickly identify data sensitivity, authorized disclosure of information, and applicable protective measures.
- Classification determined based on most sensitive level of information.
- Declassification or reclassification may be necessary as information sensitivity changes
  - For example, contract information changes sensitivity level as contracts move from negotiations/red lines to award.

Common Taxonomies

Personal, Public, Internal, Confidential, Restricted

Public, Internal, Confidential, Highly Confidential

Public, General, Confidential, Highly Confidential

Data Types

Data types are used to identify privacy and protection requirements

Common data types:

Personal Identifiable Information (PII)
Bank account numbers
Federal Tax Information (FTI)

How will we use this standard?

- Standard will be used to help identify minimum classification taxonomy
  - Used to help establish enterprise configuration baseline for 0365
  - 0365 changes will include ability to apply data sensitivity labels and rules that identify sensitive information and handle appropriately
- Existing requests dependent on data classification
- DLP is *not* intended to address FOIA or data lifecycle management capabilities such as retention

What is our first step?

- Identify and classify data to ensure sensitive information is protected appropriately
- CSRM is drafting a data classification standard
  - Target release to Orca in January
  - Intended to provide simple, intuitive classification taxonomy that scales based on agency need

Impact

- Ultimately, this will impact every user and require significant partnership across teams
- VITA recognizes the challenges and impact, therefore is planning to include multiple teams throughout VITA and customer agencies
- CSRM is sponsoring DLP, but this will support other initiatives planned and in-flight

Questions?

VIRGINIA IT AGENCY

ORGANIZATIONAL RISKS AND ISSUES (ORI)

JONATHAN SMITH

Director, Risk Management

12/06/2023

SECURITY AND RISK ORGANIZATIONAL RISKS AND ISSUES (ORI)

Organizational Risks and Issues (ORIs) - Findings created to address agency organizational risks and issues identified by VITA governance bodies.

Security ORIs are typically systemic in nature and most often address (but not limited to):

- Address security audit and risk management programs the have a score below a ‘C’ grade for their programs
- Address end-of-live/end-of-support IT
- Address shadow IT or IT that should be running on enterprise services
- Address transformation issues

ORI’s can be generated by any of the IT governance bodies within VITA

ORI'S AND IT STRATEGIC PLANNING

- The IT strategic planning process requires that all open ORIs are addressed with a business requirement for existing technology (BReT) as part of Agency IT Strategic Plans
  - BReT should include what investments the agency must make to address the issue(s) in the ORI
    - Audit resources
    - Security/Risk Management resources
    - IT resources, project(s), etc
    - Prioritization of remediation efforts

ORI FINDING UPDATES AND CLOSURE

- Agencies should update ORI findings in Archer (same as other findings)
  - Remediation plan
  - Quarterly updated
- Closure of the ORI's is dependent on the agency remediating the risk or issue
  - Improve Annual report scores to a grade of 'C' or better
  - Update, replace, decommission EOL/EOS IT identified in the ORI
  - Address shadow IT or non-transformed IT
- Agency can submit ORI for closure
- CSRM will review to ensure closure is appropriate
- CSRM is developing additional supplemental guidance for the agencies to address the IT security related ORIs (expected Q1 CY 2024)

QUESTIONS

- If you have questions regarding ORIs, please consult your CSRM analyst or email questions to CommonwealthSecurity@vita.virginia.gov

VIRGINIA IT AGENCY

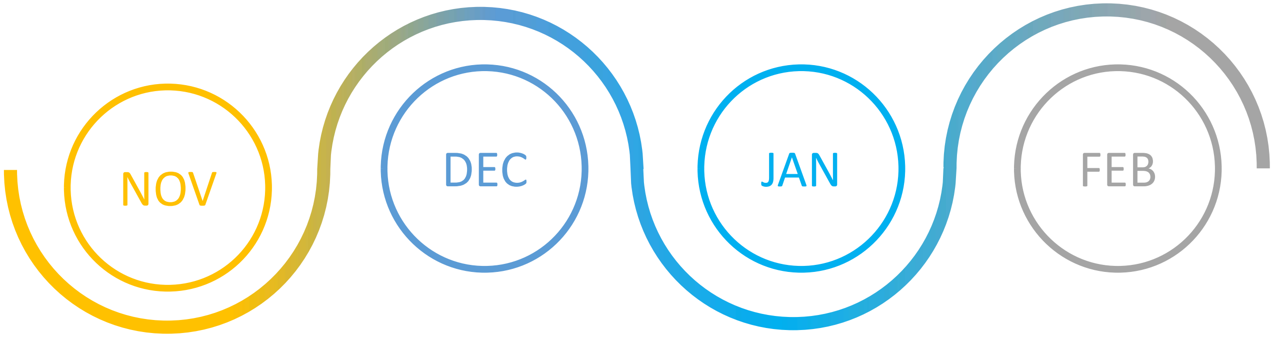
Splunk / OKTA Demonstration

Richard White

Security Services and Product Management Director

Dec. 6, 2023

Splunk Updated Roadmap



NOV

DEC

JAN

FEB

OKTA Dashbord

The roll out of the OKTA Dashboard to all agencies.

CrowdStike Dashboard

The roll out of the CrowdStrike Dashboard to all agencies.

Azure Dashboard / Pilot Agencies

Rollout of the Azure Dashboard and CSRM will start working with pilot agencies to import their system logs into the new Splunk instance

AWS Dashboard / Remaining Agencies

Rollout of the AWS Dashboard and CSRM will start working with all remaining state agencies to import their system logs into the new Splunk instance.

Access Requests Sent to VCCC

$$\underbrace{\textbf{AXXX}}_{\text{Agency Code}}\textbf{-AC-}\underbrace{\textbf{XXX}}_{\text{Agency Abbreviation}}\textbf{-SPLUNK-ANALYST-OKTA}$$

VIRGINIA IT AGENCY

AGENCY DATAPOINT REMINDER

ERICA BLAND

MANAGER IT SECURITY GOVERNANCE & COMPLIANCE

12/06/2023

AGENCY DATA POINTS REMINDER

ARCHER SCORECARD

Agency score card metrics are captured from Jan 1 to Dec 31 of each calendar year. Deliverables for calendar year 2023 will be accepted until January 31, 2024, please submit them to the CSRM mailbox, commonwealthsecurity@vita.virginia.gov.

As a friendly reminder, the metrics listed below reset at the beginning of each calendar year in Archer:

- Current Year Percentage of Risk Finding Updates Received;
- Current Year Percentage of Audit Finding Updates Received;
- ISO Certification Status.

Agency head approved audit and risk plans covering a three-year period are due annually.

Beginning January 1st, we will now only accept agency deliverables using the templates found on our website or by going directly into Archer. We have created a datapoint resource guide that details each scorecard metric, how each metric is calculated, and the acceptable formats that agency's can submit their deliverables. This document will be available on our website.

NATIONWIDE CYBER SECURITY REVIEW REMINDER

Nationwide Cyber Security Review is an annual self-assessment survey that is aligned with the NIST cybersecurity framework that evaluates an agency's cybersecurity posture. NCSR provides information about an agency's cybersecurity practices while also highlighting gaps in performance. The survey is given to all government agencies in every state, locality, tribal nation, and U.S. territory.

Performance Rankings: There are five categories that serve to highlight five core cybersecurity functions. Identify, Protect, Detect, Respond, and Recover. Each agency will evaluate itself in each category by evaluating itself on several activities that support each core function. The scoring scale is from 1 (the lowest) to 7 (the highest) and is highly policy focused. The minimum recommended score is 5.

The NCSR assessment is a requirement for the Homeland Security Grant Program (HSGP). Additional information located here: https://www.fema.gov/homeland-security-grant-program

NATIONWIDE CYBER SECURITY REVIEW REMINDER

CSRM analyzes and reports out on the NCSR data as it:

1. Provides the agencies the opportunity to complete a self assessment using the five cybersecurity framework (CSF) functions and sub categories;
2. Provides a commonwealth state peer comparison to the other 49 states;
3. Provides an agency peer comparison based on sub-sector (e.g., public safety, education, health, finance, IT, elections, etc.)

With increased participation, we can more easily see key gaps and trends related to security capabilities.

The NCSR self-assessment is due to the MS-ISAC by Thursday, February 29, 2024. The survey can be completed using this link https://cis.my.logicmanager.com/

If you have any questions or need assistance, please reach out to the CSRM mailbox, commonwealthsecurity@vita.virginia.gov

UPCOMING EVENTS

IS Orientation:

December 13, 2023

1p – 3p (virtual)

Presenters: CSRM

https://covaconf.webex.com/weblink/register/r81bb8fdb89a3b938cce6b0ed0a324e7d

ISOAG Meeting:

January 10, 2024

1p – 3p (virtual)

Presenters: TBD

https://covaconf.webex.com/weblink/register/r5cc9c6eadbf42c9b342792688a15741e

Welcome to KB4-CON Registration - KB4-CON 2024 (cventevents.com)

Happy Holidays
from
Commonwealth Security and Risk Management

MEETING ADJOURNED

VIRGINIA
IT AGENCY