VIRGINIA
IT AGENCY

Welcome to the Feb. 5, 2025 ISOAG Meeting

Information Security Officer's Advisory Group

VIRGINIA IT AGENCY

Agenda	Presenter
Welcome/Opening Remarks	Kendra Burgess/ VITA
Cyber Vault Services (CVS) New Service	John Del Grosso / VITA
Entrust/Distrust Final update & closeout	John Del Grosso / VITA
Email Quarantine Release Rules	Scott Brinkley/ VITA
Security Products and Services Update	Uma Seshakrishnan/ VITA
Announcements and Upcoming Events	Kendra Burgess/ VITA
Adjourn	

VIRGINIA IT AGENCY

Cyber Vault Service (CVS)
New VITA Service

Server, storage, and data center (SSDC)

John Del Grosso, VITA service owner, SSDC

February 5, 2025

Agenda

- Compliance to COV standards
- Overview
  - Use of a vault
  - The air-gap
  - Threat detection and notification
- Availability

Compliance to standards

EA 225

- All data assets tagged with “sensitive as to availability or integrity” in the system of record shall be protected by a COV data vault per enterprise architecture (EA) 225 guideline DA-38
- CVS qualifies as a cyber resilient backup service per EA 225 policy guidelines DA-43 through DA-53
- CVS is the third leg of the COV 4-2-1-1 Backup Rule for Sensitive Data

DA-21	All COV SaaS and storage providers shall apply the COV 4-2-1-1 Backup Rule to data tagged Sensitive as to Availability or Integrity. • First copy is production data • Second copy must be offsite (additional copies can also be offsite) • Third copy must be in a COV Data Vault (cyber protected) • Fourth copy must use a distinct media backup technology (vendor backup solution) from other three copies

SEC530

- CVS can be used for contingency planning and adheres to SEC530 CP-2

Benefits and use cases

Cyber Vault solution (CVS) will allow agencies to maintain mission-critical business data and technology configurations in a secure, air gapped vault that can be used for data recovery from the last non-infected dataset saved

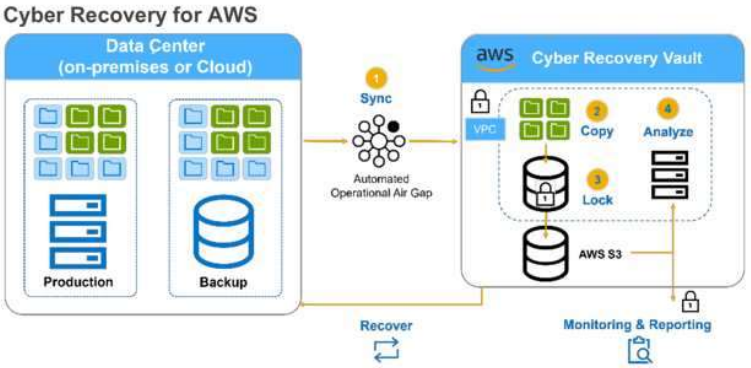
- Enable long-term archiving of sensitive information for business continuity
- Isolates essential systems from potential cyber threats.
- Safeguard citizen data, including personal identification details
- Data recovery from ransom and cyber attack(s)

How it works

Air-gap: An air-gap refers to a physical or logical separation between computer systems or networks to ensure their isolation from each other. In CVS, the air gap is a logical 'gap' where ports are de-activated to prevent access.

Cyber threat detection: Artificial intelligence (AI) is built in for automated real-time detection of cyber threats by detecting patterns of data access that are indicative of a cyber attack.

Notification: If a threat is detected – sends a notification to SSDC and ingested by SEIM



- **Questions?**

VIRGINIA IT AGENCY

Google Chrome browser Entrust Distrust

Transition from SSL.COM to DigiCert – Final Update

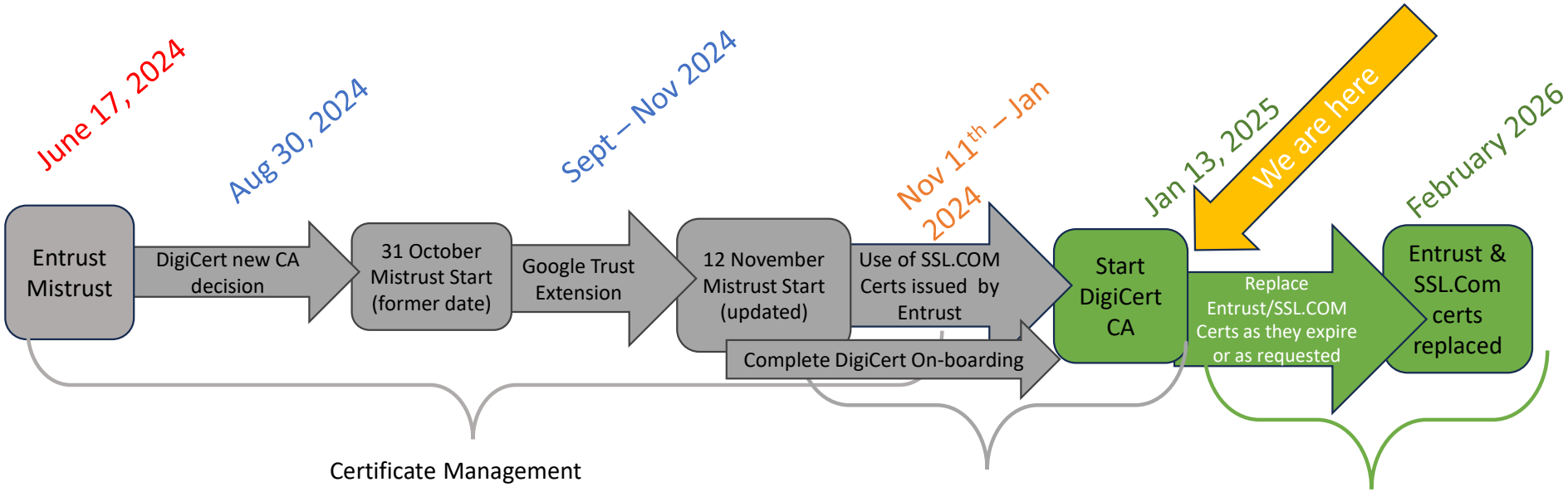
John C Del Grosso
john.c.delgrosso@vita.virginia.gov
VITA SSDC Service Owner

Jan 15, 2025

Post-“Entrust Mistrust” migration completed as planned

- ✓Entrust certificates installed until Nov 10, ‘24 in advance of the Nov 12th ‘Mistrust’
- ✓Unisys issued SSL.COM certs from Nov 12, ‘24 to Jan 10, ’25 while on-boarding to DigiCert
- ✓VITA/Unisys on-boarded DigiCert as the permanent new CA provider starting on 10 January 2025 (Domain Verification complete)
- ✓Moving Forward: DigiCert as sole provider of Certificates started January 13, 2025 and forward.

Entrust CA Mistrust replacement lifecycle



Certificate Management continues as normal – Entrust Certificates will continue to be installed

Certificate Management continues as normal – Entrust will provide SSL.COM after12 Nov. Unisys will install SSL.COM certificates until allocation is exhausted (Expected Year-End 2024)

DigiCert certs will begin to replace Entrust and SSL.COM certificates over the 12-13 months as they expire and thereafter.

Immediate and Long-Term Planning

- ✓ Immediate actions - COMPLETE
  - ✓ Immediate goal is to keep the subscription service in place as it exists today and get to a steady state with a single new CA, DigiCert – January 2025
- ➢ Long-term goal:

<u>Agencies have expressed a need for automated certificate management</u>

An end-to-end full-service CA (DigiCert) that utilizes automation, notification, and business processes built-in for true modernized certificate management by with DigiCert as the sole CA provider next year (2025).

Supplier has started to examine the DigiCert service offerings to reach this goal. More to come in Q2.

Certificate Notifications – no change

- Your Entrust/SSL.COM cert will continue to be trusted and operate, until it's expiration date.

- **Agencies will continue to receive notifications via Venafi regarding soon-to-be-expired certificates (30-day in advance of expiration)**
  - Please review your notification emails for currency by opening a General Service Request. Indicate your Agency and existing certificate name.
  - Request a verification of the Venifi contact email or provide new/alternates

- Upon notification of your certificate expiring, use the KSE Catalog to order the replacement or new certificate.
  - KSE SSL Server Certificate Service Item: SSL Certificate Catalog Item
  - Cert files will be provided through the REQ/RITM ticket (downloadable)

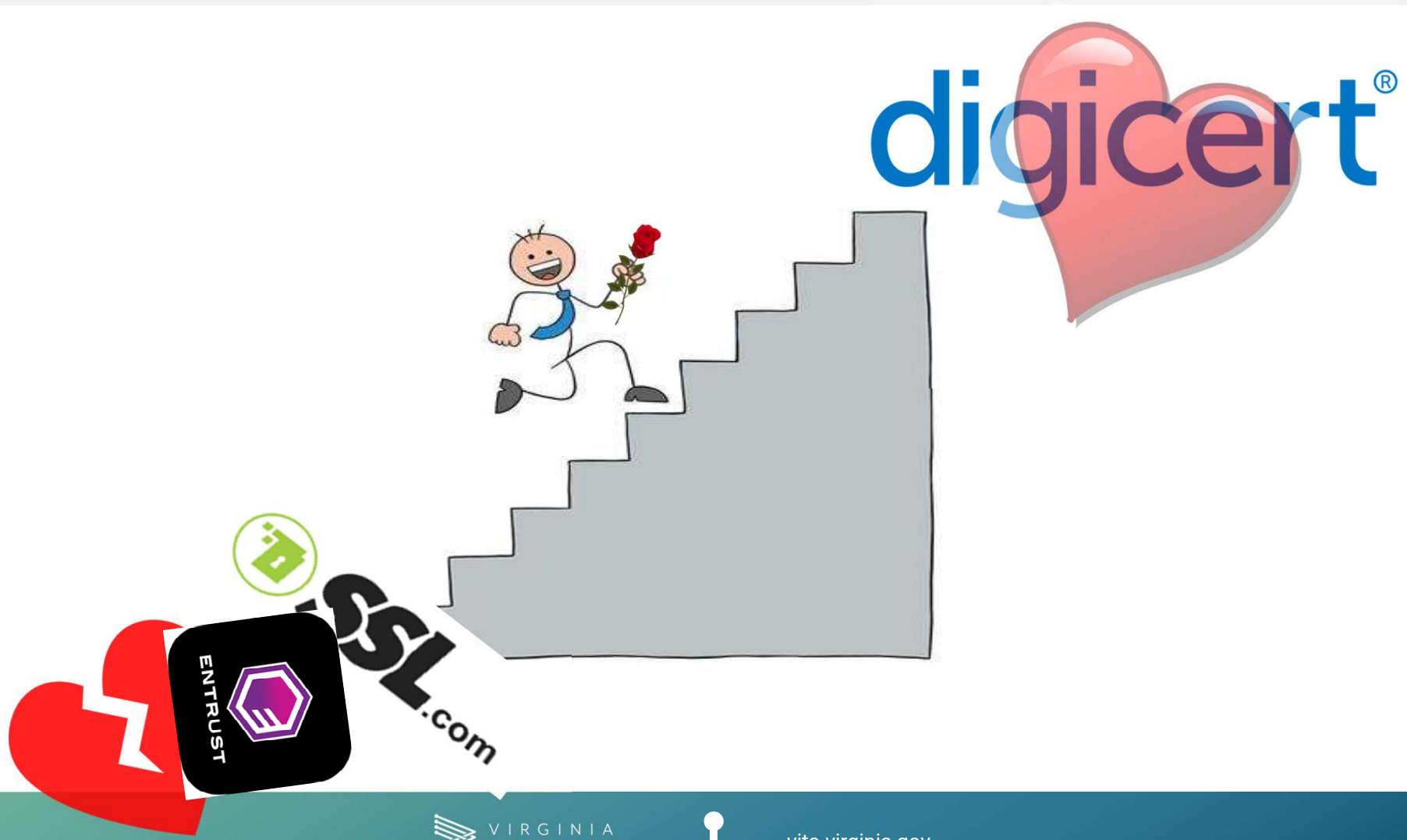
Certification Installation (New and Renewal)

Self-Installation

- Agencies with server admins and the technical knowledge are able to install new certificates and verify at their own schedule and discretion
- Use Change Management to schedule and perform the installation

Installation Service

- The SSDC Supplier can aid in the installation and verification of new and renewals for a nominal cost
- Request via the KSE Smart Hands service item: Smart Hands - Catalog Service Item
  - Work requested: Indicate the original REQ/RITM number the certificate was ordered under, add the affected servername and certificate name to be installed, day and time desired
  - Date needed by: Preferably a few days before the expiration of existing cert (during work week after business hours)
  - Hourly Duration requested: 1 hour
  - Supplier will reach out to Agency to plan the replacement via Change Management


digicert®
ENTRUST
.SSL.com

Questions?

Thank you for all your help and attention to this important migration!

VIRGINIA
IT AGENCY

Email Quarantine

Scott Brinkley – IR Manager

"Why are my emails unable to be released to me when I need them?"

February 5, 2025

How did we get here?

Microsoft Anti – SPAM Policy Implementation

- November 2024 - Microsoft's Anti-SPAM policy started to become more responsive to quarantine of emails as High Confidence Phish.

Training the Automaton

- Automatic training button is disabled for the Microsoft GOV tenants
- Each quarantined email must be ticketed individually through an email ticket with Microsoft. NTT is slowly working on this.
- NTT also has an open Design Change Request (DCR) with Microsoft to address the automatic submission potentially going to only a U.S.A. support ticket pool

Remediation

Manual Review

- KSE mass closure of tickets
- Release of High Confidence Phish after CSRM review

Policy Adjustment

- Messenging Tower has a Microsoft Ticket open
  - The goal being to make the Anti-SPAM policy's quarantine equally as strict as the Anti-Phish policy
  - Alternative: lower the responsiveness of High Confidence Phish label in the Anti-SPAM policy
  - As of January, Microsoft has informed us that they are unable to turn it off for our instance or reroute this quarantine to the Junk Email folder

Questions?

Email Quarantine

VIRGINIA
IT AGENCY

Security Products & Services - Team Updates

Uma Seshakrishnan
Product Manager, Security Services and Products

2/3/2024

Highlights

COMPLIANCE MANAGEMENT

PROCESS OPTIMIZATION

CUSTOMER ENGAGEMENT

CUSTOMER TRAINING & SUPPORT

COMPLIANCE MANAGEMENT

Completed product documentation for around 5 key products.

User guides for Nucleus, Archer, and Ardoq completed; Under internal review.

Strategized a plan to track products and ensure successful deployment.

PROCESS OPTIMIZATION

CUSTOMER ENGAGEMENT

INTAKE CHANNELS	Shared Email, Quarterly Surveys, Service Tickets, and Routine Group Calls
PROCESS LEADERSHIP	Spearheaded by the Products team
KEY OBJECTIVES	Ensure timely resolution of issues Identify recurring problem scenarios and proactively recommend product solutions to address customer needs.
SERIALIZED COMMUNICATION	Tailored process for each product to ensure clear communication

CUSTOMER TRAINING & SUPPORT

User guides for all CSRM products are on track for completion by June 2025.

The initial User guide release will include Nucleus, Ardoq, and Archer, targeted for completion by the end of March.

We will develop microlearning content and training videos to drive customer adoption and product engagement.

Conducted Splunk training on recent updates; additional sessions for other products are upcoming.

Questions?

Richard White
richard.white@vita.virginia.gov

Uma Seshakrishnan
uma.seshakrishnan@vita.virginia.gov

Announcements

SPLUNK UPDATE – DON'T LET YOUR LOGS HIBERNATE

Just like the groundhog pops up to check for spring, we're popping in to remind all agencies to identify the logs you want ingested into the VITA Splunk instance!

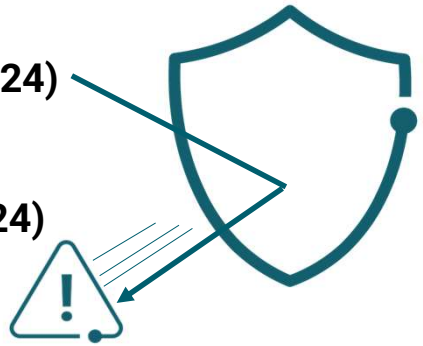
VITA is partnering with agencies to bring your application logs into Splunk, and now is the time to get started. Don't let your logs stay buried – reach out and let us know what you need ingested. We're always happy to schedule a call to discuss your options and ensure everything is ready to go!

Let's make sure your logs see the light of day this year!

Top 5 Vulnerabilities

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

- **Apache Solr 7.4 <= 7.7.3 /8.0.0 <= 8.11.0 RCE**
- **Spring Framework < 5.3.33 / 6.0.x < 6.0.18 / 6.1.x < 6.1.5 Open Redirect (CVE-2024-22243)**
- **Security Updates for Microsoft SQL Server OLE DB Driver (July 2024)**
- **KB5039227: Windows Server 2022 / Azure Stack HCI 22H2 Security Update (June 2024)**
- **KB5040437: Windows Server 2022 / Azure Stack HCI 22H2 Security Update (July 2024)**



Upcoming Events

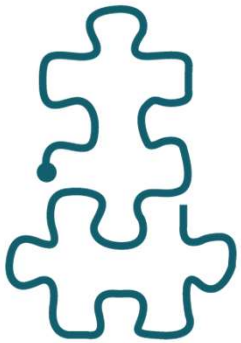
VIRGINIA
IT AGENCY
vita.virginia.gov

GovEssentials 2025: AI in Action –

Practical Applications Transforming the North American Public Sector

On February 20th at 2 pm there will be a 45-minute **virtual** Webinar

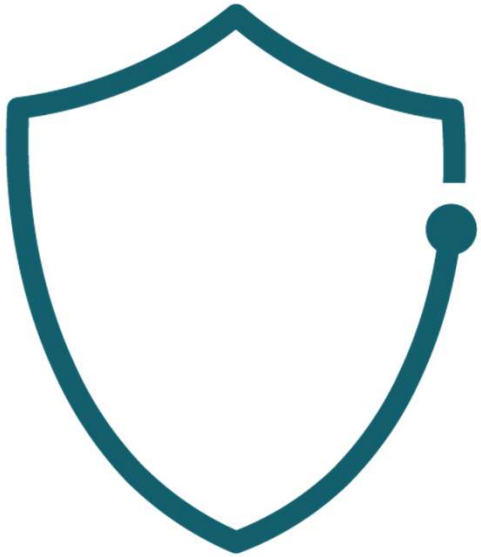
- The registration link is below, and attendance is free of charge.
- https://event.publicsectornetwork.com/govessentials-ai-in-action



CIS Center for Internet Security®
Creating Confidence in the Connected World.

NATIONWIDE CYBERSECURITY REVIEW

NCSR Assessments are Due Feb. 28, 2025



- Please submit your completed Assessment prior to end of month!

Information Security Officers Advisory Group

VIRGINIA IT AGENCY

The March 5th ISOAG meeting will be held on a new platform! Please join us on Microsoft Teams

Registration link:
https://events.gcc.teams.microsoft.com/event/13874801-26d9-4ebe-87f2-836ed5b855bb@620ae5a9-4ec1-4fa0-8641-5d9f386c7309

Service Tower SOC Report Review Sessions

The upcoming SOC review session is March 11th, 2025, and will be held remotely.

Please register at the link below

To register for this meeting, please click on the link below:
https://covaconf.webex.com/weblink/register/re1ad0ac90a496f42b7a8bcb25d01f763

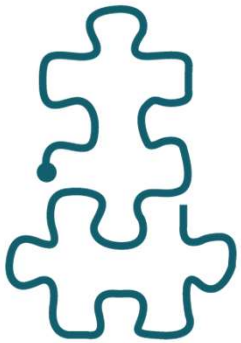
Government Cybersecurity Showcase Virginia
Elevating Virginia's Digital Defense

Public Sector Network is presenting: Government Cybersecurity Showcase Virginia

Held on Wednesday, April 9, 2025, at the **Downtown Richmond Marriott**

- The registration link is below

  Public Sector Network » Event - Government Cybersecurity Showcase Virginia



Commonwealth of Virginia Information Security Conference 2025

SAVE THE DATE!

August 14, 2025

Hilton Richmond Hotel, 12042 West

Broad St., Richmond, VA 23233

Registration will open soon!

MEETING ADJOURNED

VIRGINIA
IT AGENCY