VIRGINIA
IT AGENCY

Welcome to the June 12, 2024 ISOAG Meeting

Information Security Officer's Advisory Group

June 12, 2024

VIRGINIA IT AGENCY

Agenda	Presenter
Welcome/Opening Remarks	Erica Bland/ VITA
Five Key Vulnerabilities: How they are Selected and Processed	Matthew Umphlet/ VITA Andrew Wirz/VITA
Datapoint Trends	Amy Braden/ VITA
Cloud Access Security Broker (CASB)	Eric Culbertson/MSS
State and Local Cyber Security Grant Program	Mary Fain/VITA
Splunk Update	Richard White/VITA
Announcements/ Upcoming Events	Erica Bland/ VITA
Adjourn	

VIRGINIA
IT AGENCY

5 Key Vulnerabilities:
How the Top 5 are Selected

Matthew Umphlet

Threat Intelligence Analyst

06/12/24

How Top 5 are Selected

- Published Monthly
- Highest Risk to the Commonwealth
- Example Considerations
  - Ease of Exploit
  - Exploited in the Wild
  - Count inside of COV
  - Industry Peers Affected
  - Threat Intel Sources
- Every Agency/Tower may not be affected by something in the Top 5 Every Month
- Check Nucleus for an Up-to-Date count for your agency
- Reminder: Nucleus KB Article https://vccc.vita.virginia.gov/kb_view.do?sysparm_article=KB0019481

VIRGINIA
IT AGENCY

Top 5 Vulnerabilities

Escalation path: Who is contacted, and when

Andrew Wirz
Sr. IT Risk Analyst

Escalation Path

- Phase 1 – Day 0 – Initial email sent out to ISOs declaring top 5
- Phase 2 – Day 30 – Risk alert sent to ISO and AITR
- Phase 3 – Day 45 – Risk alert sent to agency head
- Phase 4 – Day 60 – Risk alert sent to secretary of administration and agency secretary
- Continuous phase – Day 67+ - Secretary reports are updated as needed, currently planned to be weekly

Datapoint Trends

VIRGINIA IT AGENCY

Amy Braden

Governance Director

June 12, 2024

VIRGINIA
IT AGENCY

CLOUD ACCESS SECURITY BROKER (CASB)

ERIC CULBERTSON, MSS
CHAD RASNICK, MSS

BILL STEWART, SERVICE OWNER

MANAGED SECURITY SERVICES

JUNE 11, 2024

The new cloud access security broker (CASB) will provide insight and visibility into cloud-based services.

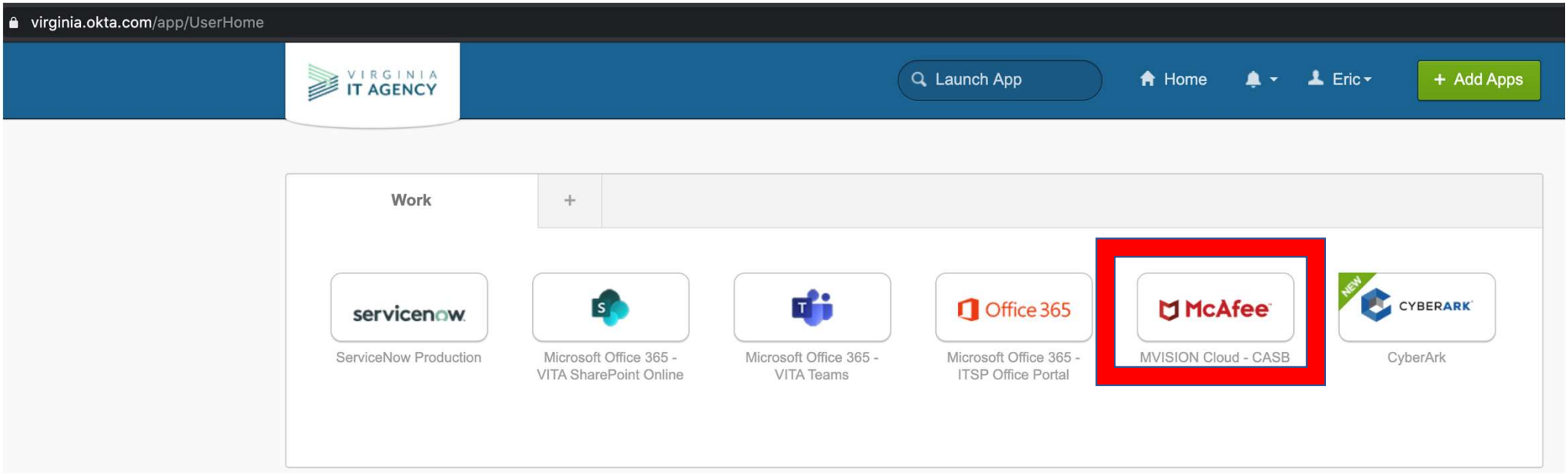
CASB will provide tools necessary for information security officers (ISOs) to take control of Data:

- An ISO can receive access to view data for their agency.
- An ISO can easily identify users using undesirable or risky web services.
- An ISO can easily identify web services being utilized within the agency.

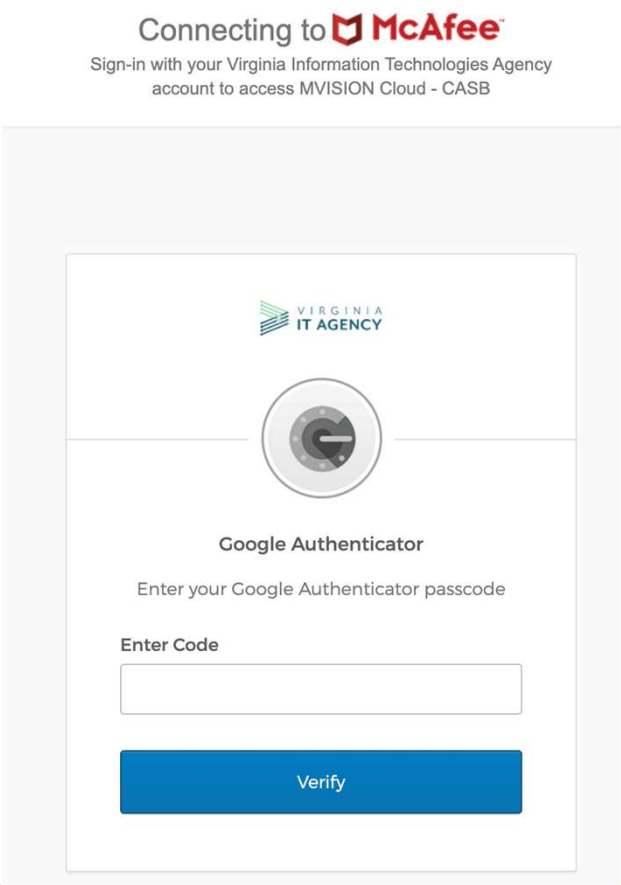
CASB dashboard access will only be provided to agencies that opt-in/request access:

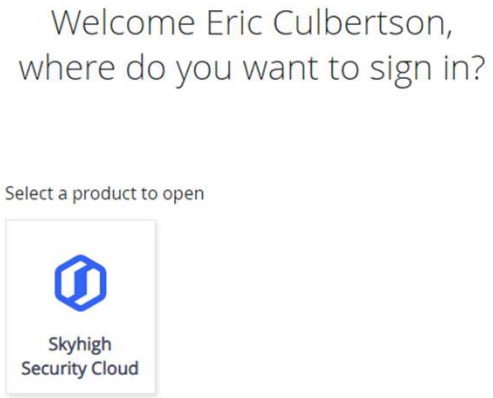
- An ISO can place a general service request to be added to CASB access.
- The request will generate two tasks.
- One task will be filled by Unisys for Okta app access and the other will be filled by Eviden.

Access CASB by logging into Okta then click “MVISION Cloud – CASB”.

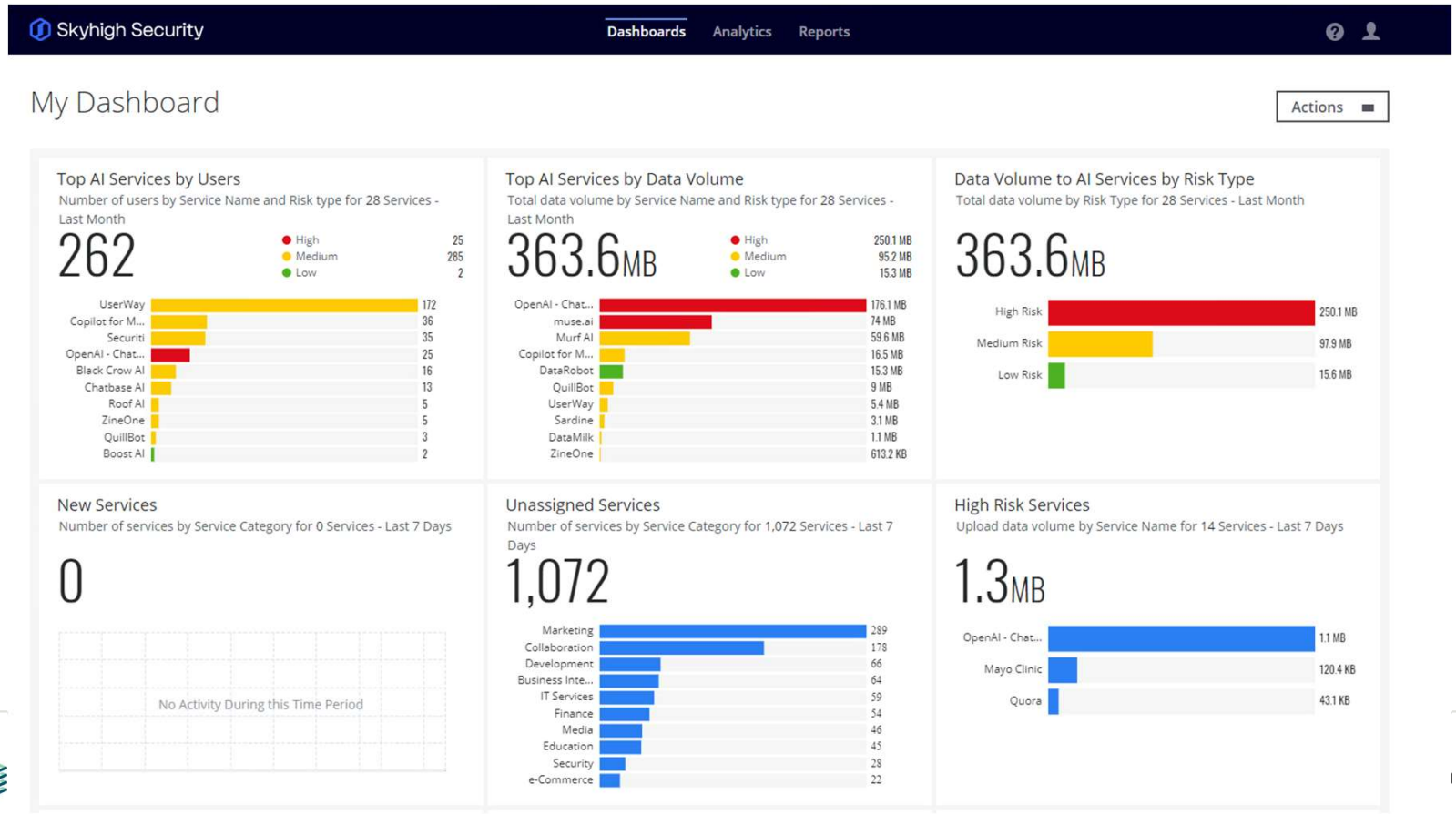


Provide One time password.

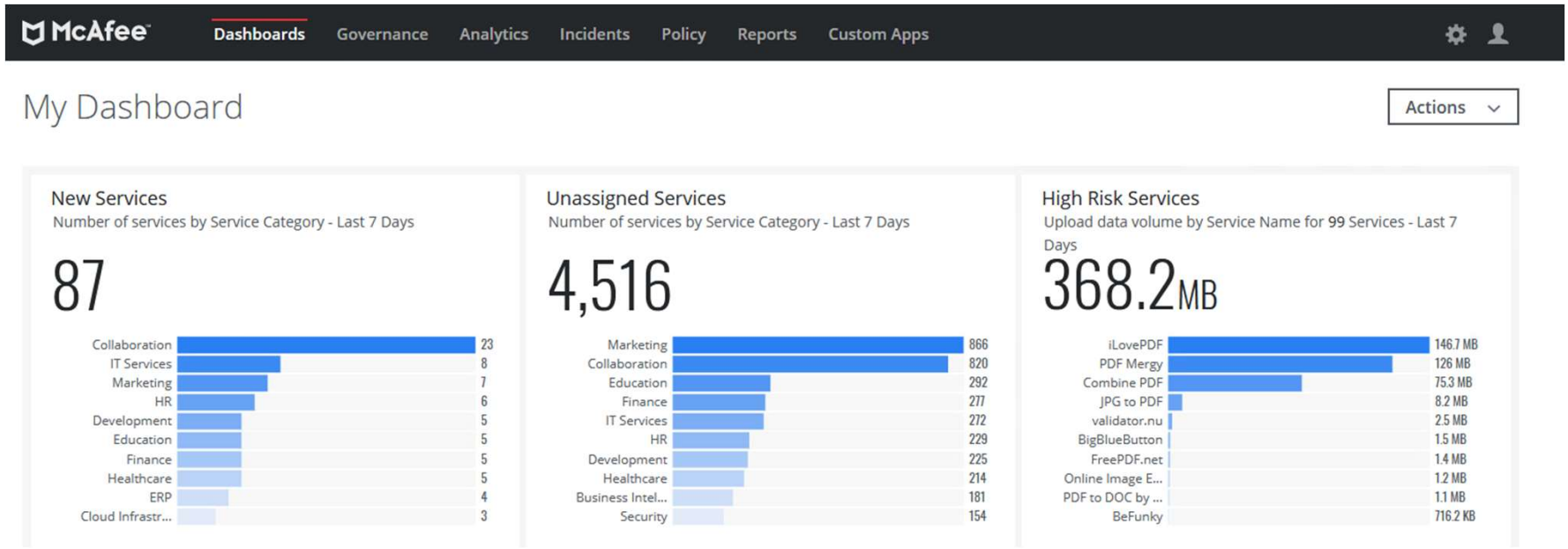




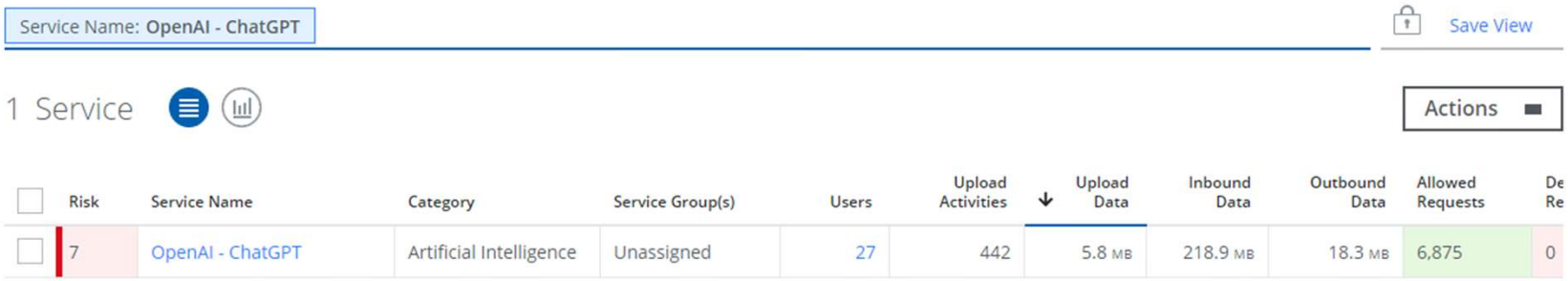
Below is a snapshot of the CASB dashboard with access to a single agency.



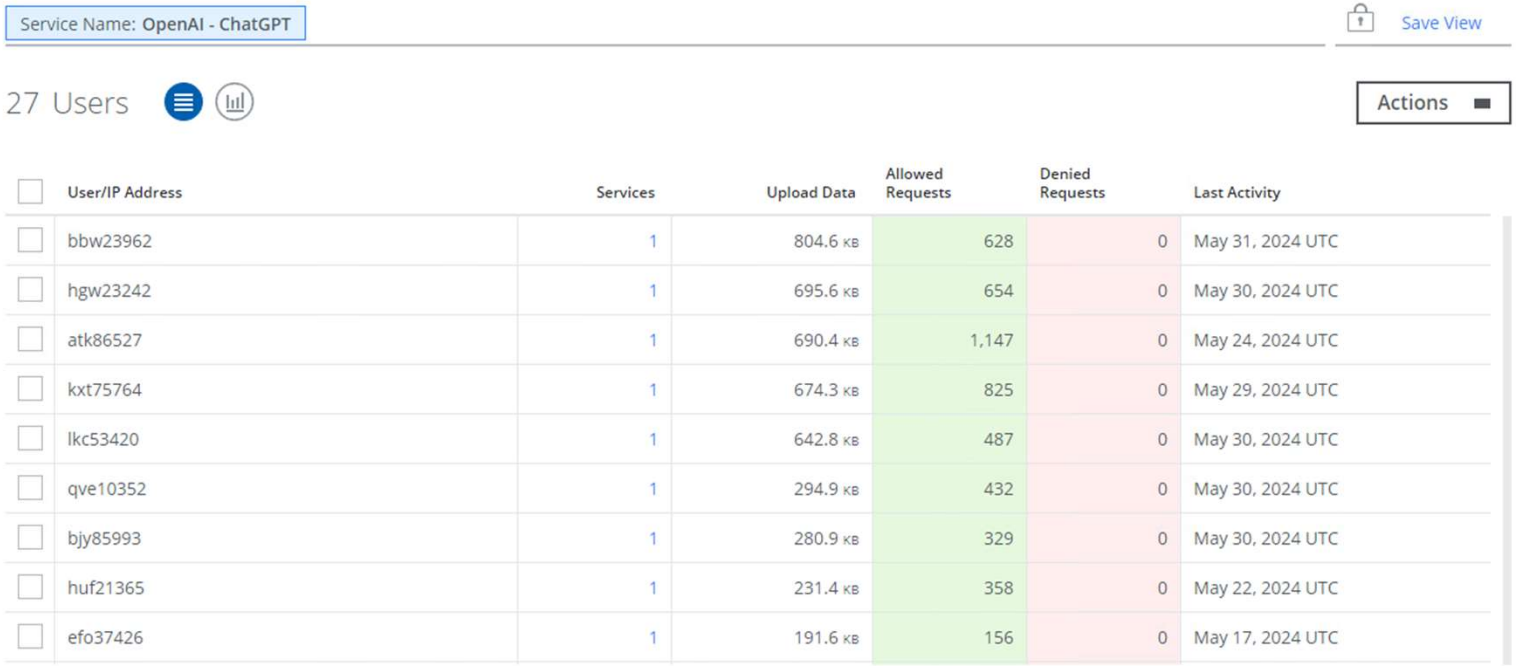
Below is a snapshot of the CASB dashboard with access to all data.



Below is a snapshot of the CASB dashboard with access to a single agency after clicking a High-risk service from the dashboard screen on the previous slide.

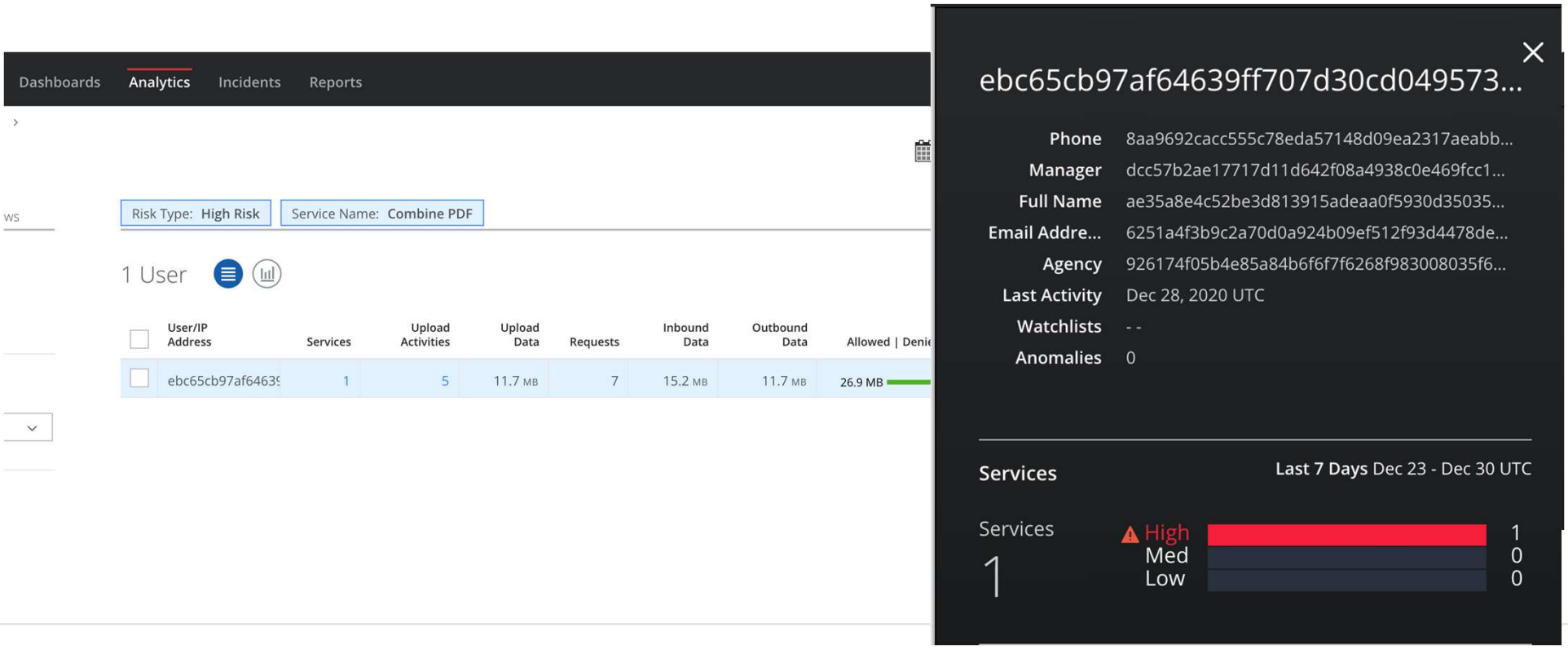


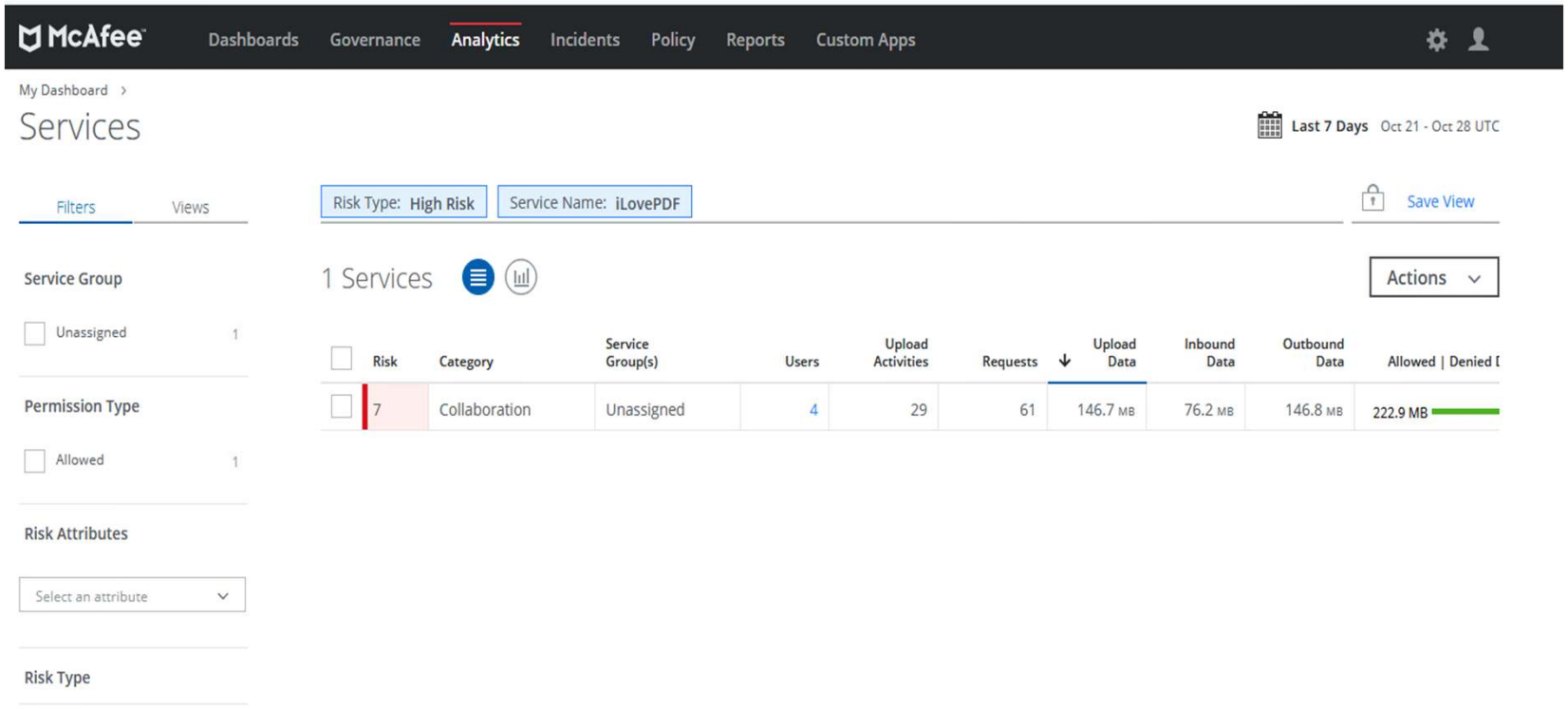
Below is a snapshot of the Users screen after clicking on the user from the previous slide. Please note the User ID is tokenized when accessed from outside COV.



User/IP Address	Services	Upload Data	Allowed Requests	Denied Requests	Last Activity
bbw23962	1	804.6 KB	628	0	May 31, 2024 UTC
hgw23242	1	695.6 KB	654	0	May 30, 2024 UTC
atk86527	1	690.4 KB	1,147	0	May 24, 2024 UTC
kxt75764	1	674.3 KB	825	0	May 29, 2024 UTC
lkc53420	1	642.8 KB	487	0	May 30, 2024 UTC
qve10352	1	294.9 KB	432	0	May 30, 2024 UTC
bjy85993	1	280.9 KB	329	0	May 30, 2024 UTC
huf21365	1	231.4 KB	358	0	May 22, 2024 UTC
efo37426	1	191.6 KB	156	0	May 17, 2024 UTC

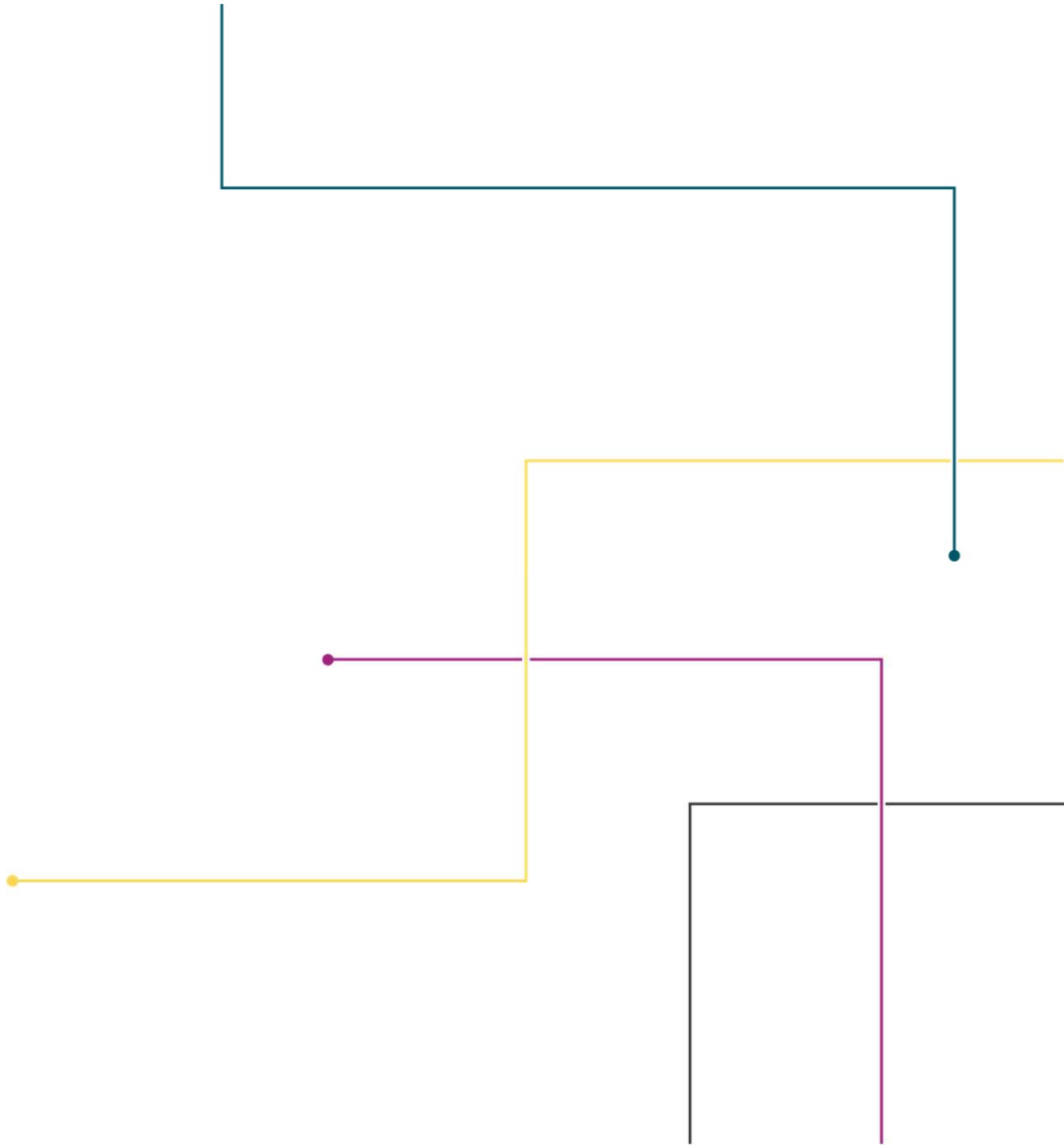
Highlighting the user will provide additional details including Manager, Phone and Full name from AD.



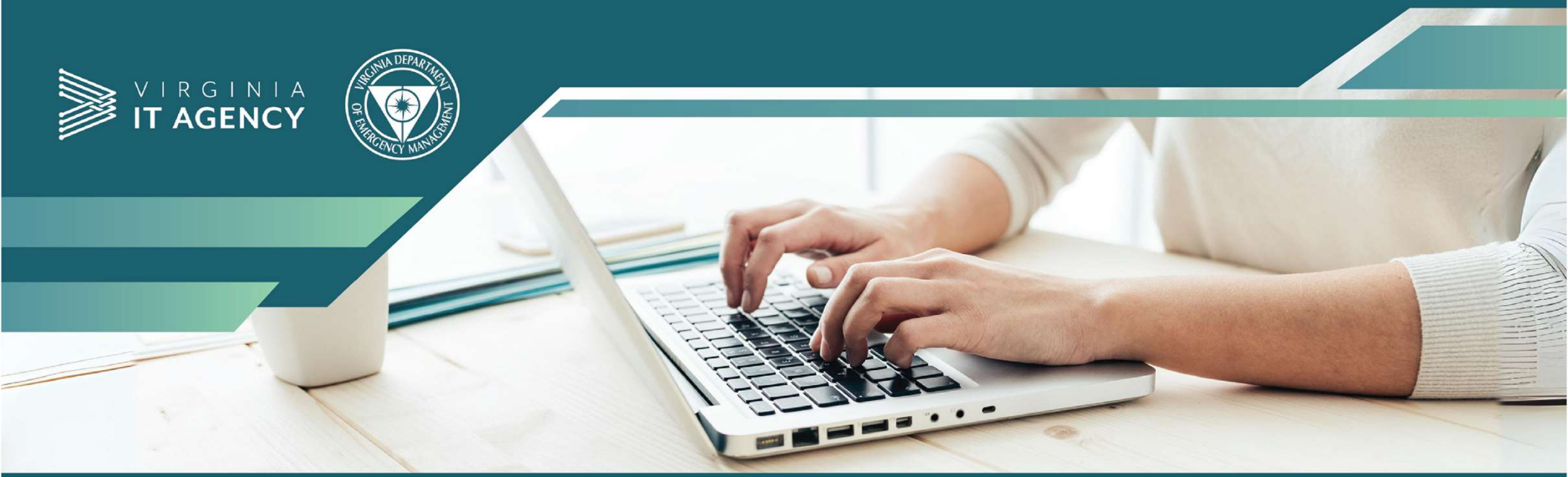

McAfee
Dashboards
Governance
Analytics
Incidents
Policy
Reports
Custom Apps
My Dashboard
Services
Last 7 Days Oct 21 - Oct 28 UTC
Filters
Views
Risk Type: High Risk
Service Name: iLovePDF
Save View
Service Group
Unassigned 1
Permission Type
Allowed 1
Risk Attributes
Select an attribute
Risk Type
1 Services
Actions
Risk
Category
Service Group(s)
Users
Upload Activities
Requests
Upload Data
Inbound Data
Outbound Data
Allowed | Denied
7
Collaboration
Unassigned
4
29
61
146.7 MB
76.2 MB
146.8 MB
222.9 MB

QUESTIONS?

Thank you!



VIRGINIA IT AGENCY



State and Local Cybersecurity Grant Program (SLCGP)

Update

Mary Fain
Project Manager
June 10, 2024

Virginia's Cybersecurity Plan defines focus areas for SLCGP funding

Vision for Improving Cybersecurity

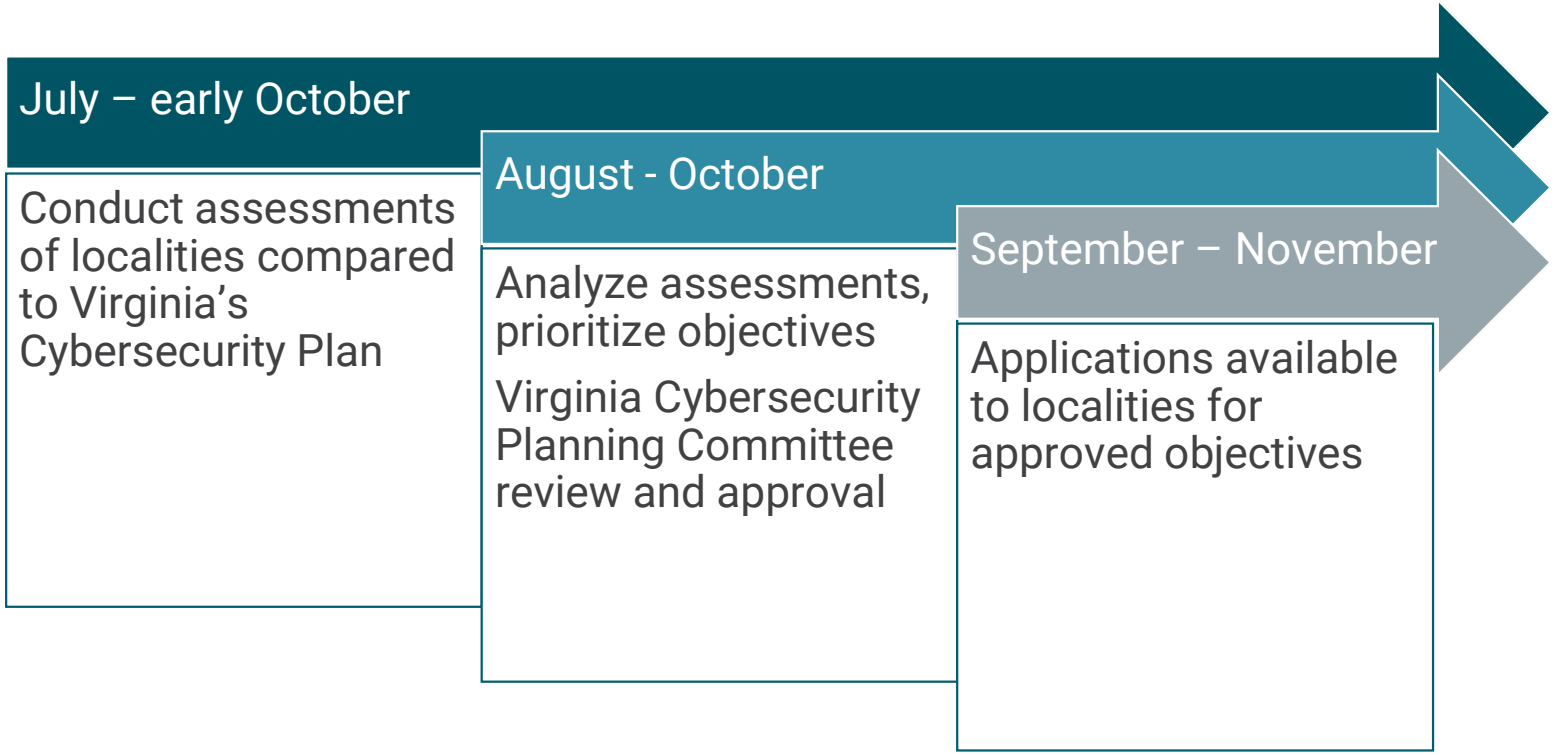
Create a cybersecurity ecosystem supporting a **whole of state** approach for state and local governments to safeguard critical infrastructure, protect Virginians' data, and ensure the continuity of essential services.

Includes actionable and measurable goals and objectives focused on:

- Inventory and control of technology assets
- Software and data
- Threat monitoring
- Threat protection and prevention
- Data recovery and continuity
- Understanding an organization's cybersecurity maturity level

To read the plan, visit https://www.vita.virginia.gov/media/vitavirginiagov/commonwealth-security/pdf/meetings/2022-Virginia-Cybersecurity-Plan.pdf

Localities will participate in assessments and then can apply for future projects*



*Participation in an assessment is not a requirement for future projects

Help Localities Connect to SLCGP

- Sign up for VDEM grant notifications
  Visit https://public.govdelivery.com/accounts/VADEM/subscriber/new. After submitting your email address, select the State & Local Cybersecurity Grant Program (SLCGP) from the topic list

- Attend Virginia Cybersecurity Planning Committee meetings
  Visit https://www.vita.virginia.gov/information-security/grant-programs/vcpc-meetings/ for more information about past and upcoming meetings, how to access the Webex links, and meeting materials

- Contact us with questions – cybercommittee@vita.virginia.gov

VIRGINIA
IT AGENCY

VITA Products and Services Update

Richard White

Director of Security Products and Services

June 2024

SPLUNK UPDATE JUNE 2024

Current Applications Being Ingested

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

SPLUNK UPDATE JUNE 2024

Agencies we are currently working with:

- DMAS
- TRS
- DOF
- DOA
- DPB
- DJJ
- UNISYS
- DSBSD
- VDH
- VDOT
- TAX
- CSA
- DSS
- VITA

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.

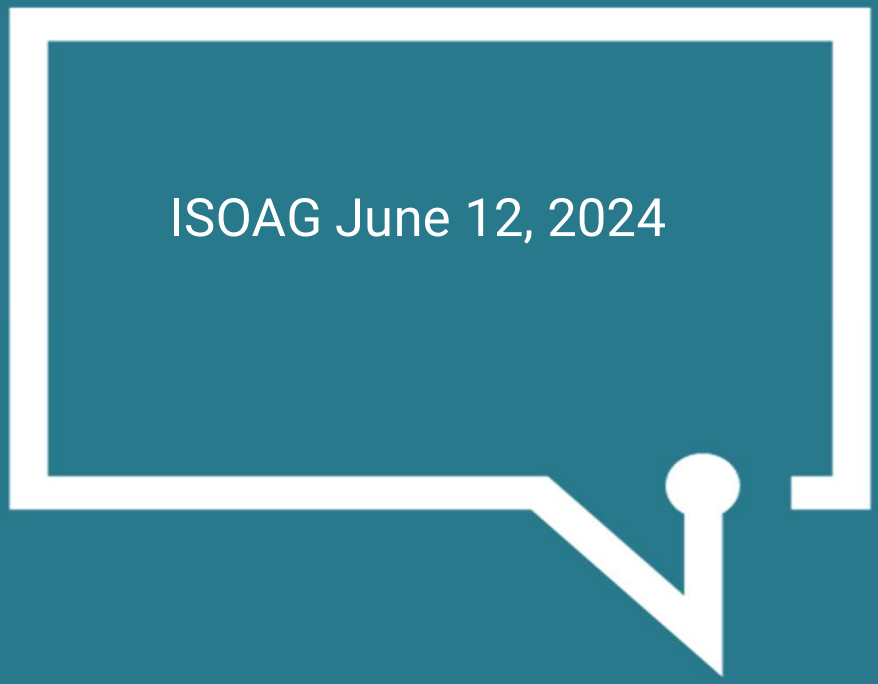
SPLUNK UPDATE JUNE 2024

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

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.

Questions?

Announcements



KnowBe4 Fresh New Content

KnowBe4 has added 60 new pieces of training content in May.

1. **Ransomware Ready**
2. **Insider Threat Foundations**
3. **World Wild Web: Using AI Tools that Work**

More information can be found by clicking the link below:

Your KnowBe4 Fresh Content Updates from May 2024

For Your Awareness

Effective June 28, Microsoft 365 applications and data will require that the device (computer or cellular device) access the service from a location in the United States. This is a critical security need that conforms to the latest federal security standards and guidance. An exception process is available.

All end users traveling outside of the U.S. and needing access to Microsoft 365 must submit an international travel form to their agency's information security officer with ample time to review and approve prior to the need.

Please contact Commonwealthsecurity@vita.virginia.gov with any questions.

New Names and Faces

It is Summer, that means we are welcoming our group of interns to VITA CSRM!

- Kervens Hyppolite (ISO Services)
- Joshua Kropka (Outreach & Communications)
- Mark Jeffrey (Governance)
- Hoang Ta (Threat Management)
- Jelica Calderon (Enterprise Architecture)

Welcome Interns!

Upcoming Events

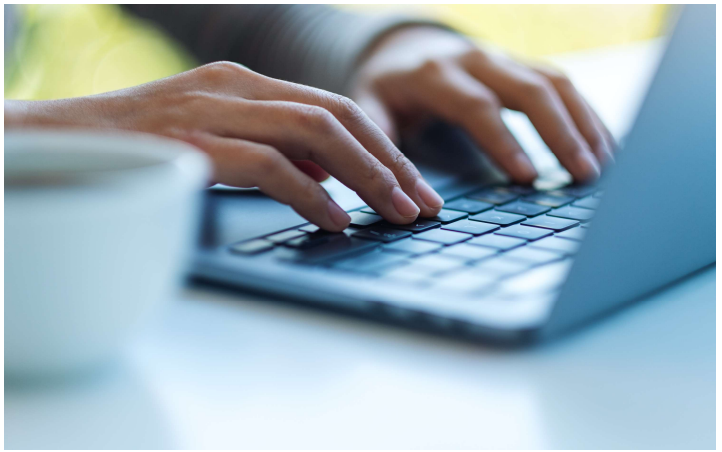
VIRGINIA
IT AGENCY
vita.virginia.gov

IS Orientation

The next IS Orientation is being held on June 26, 2024

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

https://covaconf.webex.com/weblink/register/r85904edc047089bb5c65f3261a80bd46



ISOAG Meeting: July 10, 2024

Presenters (subject to change):

- Michael Watson / VITA
- Richard White / VITA
- Marcus Thornton, Chris Burroughs, and Imran Afridi / ODGA
- Carrie Roth /Virginia Works
- Michael Wickham/Virginia Workers Compensation Commission

Please register at the link below:
https://covaconf.webex.com/weblink/register/r71a3e47d9c5fa906f96512528d386759

Service Tower SOC Report Review Sessions

The upcoming SOC review session is July 18, 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/r79ff348f2d49da7f1cc45197d77c5b07

Commonwealth of Virginia Information Security Conference 2024

Join us for the COV IS Conference 2024

Titled: "The Art of Cyber War"

- August 15, 2024, at the Hilton Richmond Hotel and Spa located at Short Pump:

  12042 West Broad Street,

  Richmond, VA 23233

Register at:

https://www.vita.virginia.gov/information-security/security-conference/

MEETING ADJOURNED

VIRGINIA
IT AGENCY