



VIRGINIA IT AGENCY

**Welcome to the April 3rd, 2024
ISOAG Meeting**

Information Security Officer's
Advisory Group

April 3, 2024

Agenda

Presenter

Welcome/Opening Remarks

Erica Bland/ VITA

Ardoq

Stephen Smith / VITA

CSRM Connections Page

Kendra Burgess/ VITA

Update on Splunk

Richard White/ VITA

KnowBe4 Lessons Learned and Upcoming Phishing Dates

Matthew Umphlet/ VITA

Round Table

All Inclusive

Upcoming Events

Erica Bland/ VITA

Adjourn



VIRGINIA
IT AGENCY

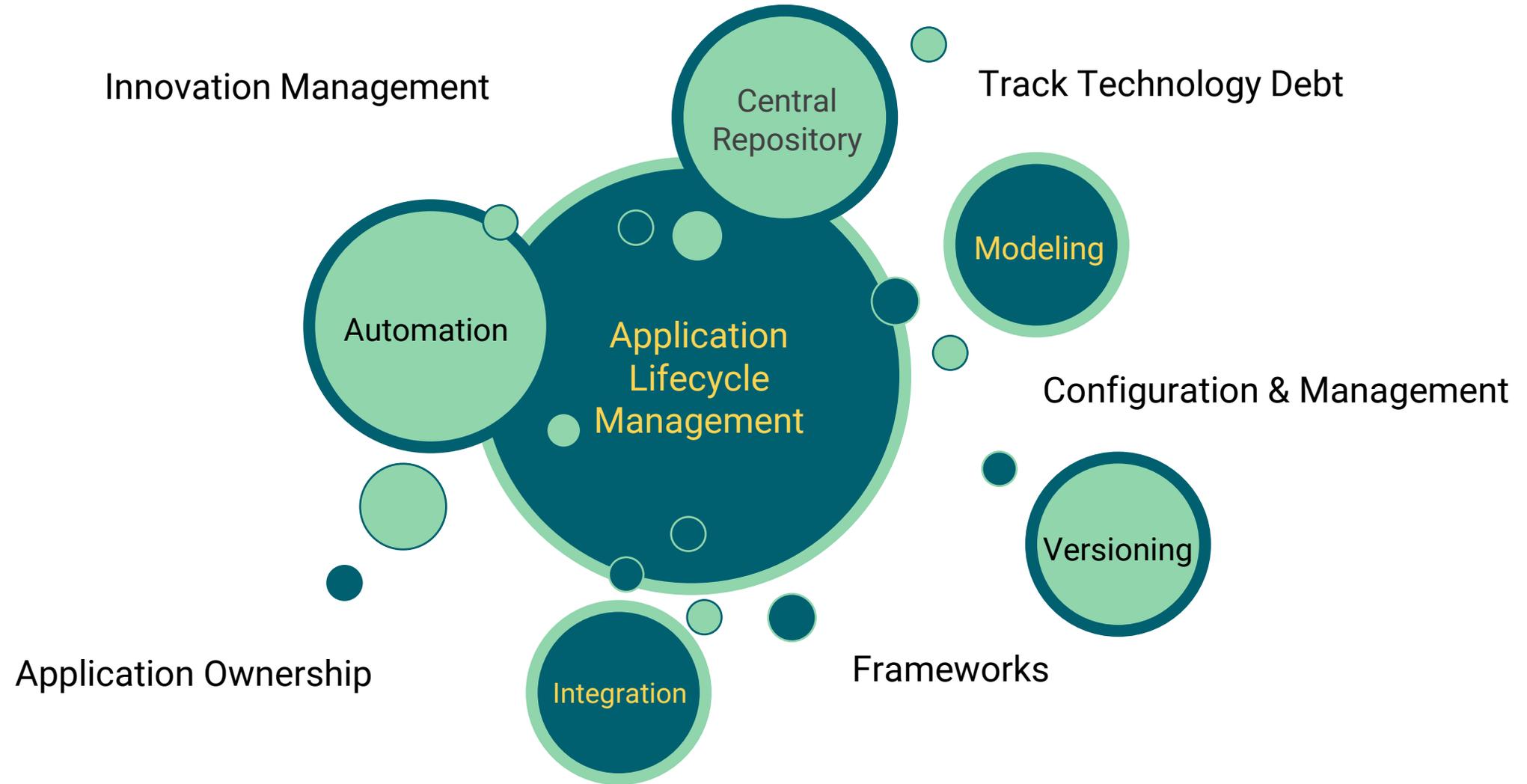
Introducing... Ardoq!

Architecture & Innovation Forum

Stephen Smith
Enterprise Architecture Manager

December 2023

System of Record



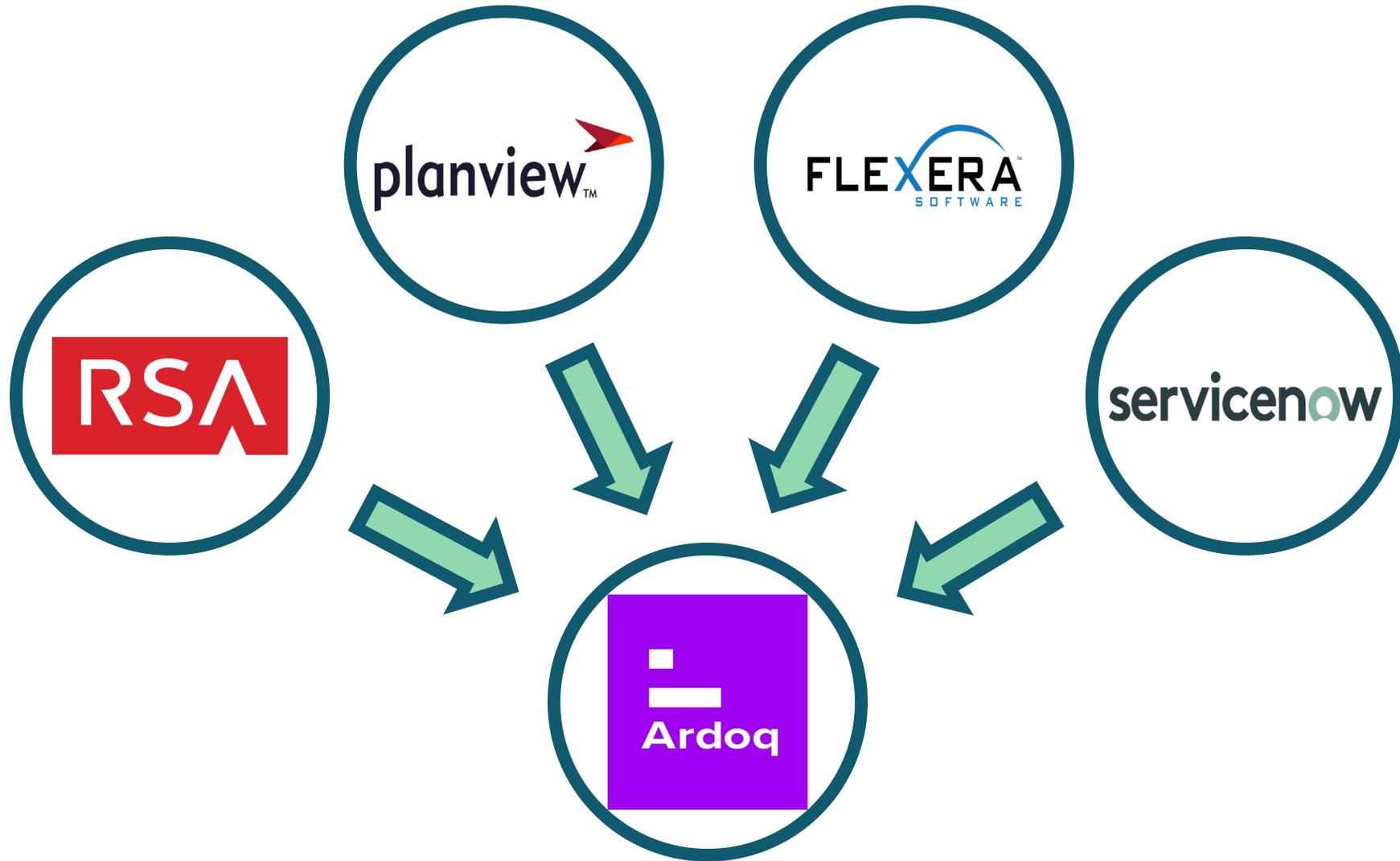
Magic

Founded 2013
Headquarters Oslo, Norway
Offices London
Copenhagen
New York



Proof of Value April 2023
Procured October 2023

Ingestion



Questions

???





Commonwealth Security and Risk Management Connections Page



VIRGINIA
IT AGENCY

CSRM Outreach and Communications

Kendra Burgess, VITA

Information Security Education and
Relationship Management Specialist

April 3, 2024



VIRGINIA IT AGENCY

VITA SPLUNK UPDATE

Richard White

Director of Security Products and Services

APRIL 2024

SPLUNK UPDATE APRIL 2024

VITA BOX LOGS ARE NOW AVAILABLE IN SPLUNK FOR BOX CUSTOMERS

Customers can access the following logs:

- Event Logs
- Access Logs
- Storage Totals
- User Location

The logo for VITA BOX, featuring the word "box" in a bold, blue, lowercase sans-serif font. The letters are thick and rounded, with a modern, clean aesthetic.

SPLUNK UPDATE APRIL 2024

Splunk Cloud Search Head CORE

splunk>cloud Apps Messages Settings Activity Find

Richard White Support & Services

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

Dashboards

Create New Dashboard

Dashboards include searches, visualizations, and input controls that capture and present available data.

Latest Resources

☆ Examples for Dashboard Studio

Browse examples of dashboards & visualizations. [Visit Example Hub](#)

Intro to Dashboard Studio

Learn how to build dashboards with Dashboard Studio. [Learn More](#)

Intro to Classic Dashboards

Learn how to build traditional Simple XML dashboards. [Learn More](#)

11 Dashboards

All Yours This App's box

i	Title ^	Actions	Owner	App	Sharing	Type
>	Analyze a Mailbox Database - Microsoft Exchange	Edit	nobody	DA-ITSI-CP-microsoft...	Global	Classic
>	Analyze a User Mailbox - Microsoft Exchange	Edit	nobody	DA-ITSI-CP-microsoft...	Global	Classic
>	Box Data Analysis	Edit	salamatu.bangura@vi...	search	Global	Classic
>	Mailbox Database Overview - Microsoft Exchange	Edit	nobody	DA-ITSI-CP-microsoft...	Global	Classic
>	Mailbox Quota Usage - Microsoft Exchange	Edit	nobody	DA-ITSI-CP-microsoft...	Global	Classic
>	Mailbox Stores - Microsoft Exchange	Edit	nobody	DA-ITSI-CP-microsoft...	Global	Classic
>	Multi-Mailbox Search Usage - Microsoft Exchange	Edit	nobody	DA-ITSI-CP-microsoft...	Global	Classic
>	Non-Owner Mailbox Access - Microsoft Exchange	Edit	nobody	DA-ITSI-CP-microsoft...	Global	Classic
>	Top Mailboxes and Folders by Size - Microsoft Exchange	Edit	nobody	DA-ITSI-CP-microsoft...	Global	Classic
>	Unused Mailboxes - Microsoft Exchange	Edit	nobody	DA-ITSI-CP-microsoft...	Global	Classic



MAY 9th, 2024

12 – 4 PM

**In Person at The Boulders
Registration Required**

VITA will be hosting our second Splunk Lunch & Learn. This will be a continuation in the series. The Splunk Security Course will cover the following:

- Familiarization with the Splunk interface
- Searching fundamentals
- Introduction to key Splunk commands
- Question and answer sessions throughout the workshop providing opportunities to write your own searches!



WE WANT YOUR LOGS:

VITA is starting to work with RMC member 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.

Questions?





VIRGINIA IT AGENCY

KnowBe4 Lessons Learned and Key dates for Phishing Campaign

Matthew Umphlet
Threat Intelligence Analyst

April 3, 2024

2024 Schedule of COV-wide PHISHING CAMPAIGNS

COV-wide Campaigns will occur the 3rd week of each quarter

A number of ISOs have asked if a schedule of COV-wide Campaigns could be published.

While the Security Standard calls for agencies to complete phishing campaigns once a year, CSRSM has been and will continue to provide COV-wide phishing campaigns on a quarterly basis. In reviewing the holiday calendar for 2024, we have selected the third week of the quarter for these campaigns. This will also provide about 5 weeks should a campaign need to be re-scheduled or re-run.

The schedule for 2024 is as follows:

~~Q1 – week of January 22nd~~

Q2 – week of April 15th

Q3 – week of July 15th

Q4 – week of October 14th

Updates About Phishing Campaign Content

- Engaging with KnowBe4, Microsoft, and the messaging tower for continuous improvement
- Updated mail delivery rules
- At this time, attachments that utilize macros are unable to be used
- URLs and QR Codes are not affected
- New Testing Process for templates sent out during quarterly campaigns
- External sender labeling will label KnowBe4 messages

Updates About Phishing Campaign Content

- External sender labeling will label KnowBe4 messages
- Currently there is no way to disable this function without completely disabling the External Senders Banner

Some content in this message has been blocked because the sender isn't in your Safe senders list. | Trust content from ad@secured-login.net. | Show blocked content

 Walmart <ad@secured-login.net>
To: Johnson, Annetta (DEQ)

  Reply  Reply all  Forward  
Wed 4/3/2024 9:21 AM

CAUTION: This Email originated from OUTSIDE of DEQ. Do not open attachments or click links unless this email comes from a known sender and you know the content is safe.

 Walmart Logo

Reporting Spam vs Phishing

- The Only way to submit Phishing and Spam reports is through the PAB button
- Users should take care in order to ensure that they are correctly reporting content

KnowBe4

Are you sure you want to report this as a phishing email?

Subject:

Investigation Request Submitted

Show Sender's Details

Email Classification:

Phish/Suspicious
This email is a threat.

Spam
This email is spam.

Add a comment...

0/360

PAB Button Terminology

Phishing/Suspicious messages are an attempt by the phisher to solicit an action from the user. This may be in multiple ways that does not necessary require a user to click on a link. Here's some example of how attackers can solicit an action from the user:

- Phone - Please contact me via phone at (999)999-9999 to provide the information requested.
- Email - Please email me your contact information so we can process your request.
- Link Click - Please click on this link below to validate your account.
- Scan QR Code - Please scan the QR code to register for your discounted interest rate
- Open document – Please open the following attachment to see how much you have received for your Christmas bonus.

Spam messages are normally unwanted emails that the user received. These messages are normally benign in nature and more of a nuisance than a threat. Examples of Spam messages include:

- Marketing literature
- Newsletters
- Advertisements
- Chain letters

Updates About Phishing Reporting Process

- PAB button is still active and must be used to submit Phishing and Spam reports
- MSS SOC will continue to evaluate phishing messages reported via the PAB button
- Archer tickets will continue to be generated to track reported phishing messages
- Spam messages will continue to be reported and blocked once the threshold is reached, users will still receive a message on how to mark as spam locally

Questions?

Contact:

- Matthew Umphlet (matthew.umphlet@vita.virginia.gov)
- Kathy Bortle (kathy.bortle@vita.virginia.gov)



You are a Part of
the Program!



VIRGINIA
IT AGENCY

Round Table Discussion

For the Hybrid ISOAG Meeting in April we will have a Round Table Discussion. Get answers to your questions!

April 3, 2024, ISOAG Meeting

Upcoming Events



VIRGINIA
IT AGENCY

vita.virginia.gov

- Commonwealth of Virginia Information Security Conference 2024

SAVE THE DATE!

August 15, 2024

Hilton Richmond Hotel

12042 West Broad St., Richmond, VA 23233

Registration to open soon!



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>



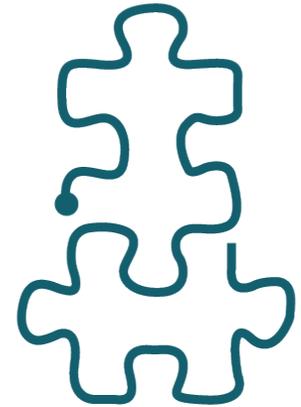
• Government Innovation Virginia

- Transforming Virginia: Bridging Innovation and Progress



Public Sector Network is presenting: Government Innovation Virginia

- Held on Wednesday, April 17, 2024, at the Downtown Richmond Marriott
- The registration link is below, and attendance is free of charge.
- [Government Innovation Virginia 2024 - Public Sector Network](#)



**MEETING
ADJOURNED**



**VIRGINIA
IT AGENCY**