VIRGINIA IT AGENCY

WELCOME TO THE

June 1, 2022

ISOAG MEETING

Welcome/Introduction	
Cyber Risks to Operational Technology Systems and How Secure Them	Rick Tiene/Mission Secure
Access to Public Records under the Virginia Freedom of Information Act	Alan Gernhardt/Virginia Freedom of Information Advisory Council
NTT DATA Messaging Services	Jon Tomsu & Lee McMillian
2nd Line of Defense – IT Risk Management	Ben Sady, FORVIS
MSS Update	Darrell Raymond/ATOS Bill Stewart/VITA
Upcoming Events	Ed Miller/VITA
Adjourn	

Cyber Risks to Operational Technology Systems and How to Secure Them

Protecting OT networks and safeguarding operations with OT cybersecurity platform and 24/7 expert managed services.

Rick Tiene, VP, Mission Secure

Trends Driving the OT Cybersecurity Market

Industry 4.0 (IIoT)

Digital transformation is a competitive necessity and security is part of the foundation, but 64% of operations leader's report struggling to keep up with the security challenge.[1]

Risk Mitigation

Attacks targeting ICS and OT have increased by more than 2,000% since 2018. And insurance companies are dropping cyber coverage from policies and looking to not pay due to negligence.[2]

Regulations

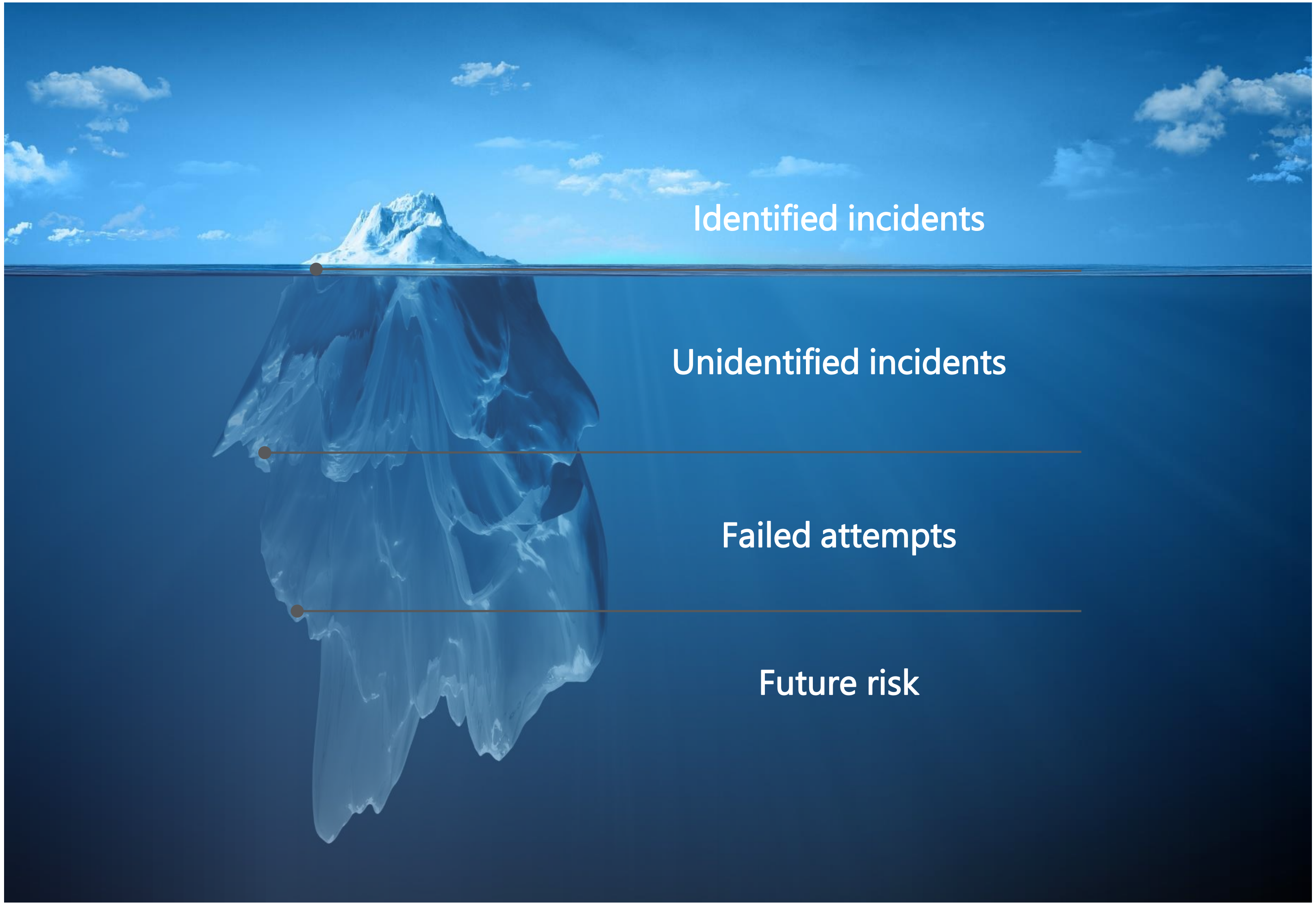
Efforts to improve OT cybersecurity now include government, vertical-specific, international, cross industry, and critical infrastructure regulatory requirements and standards.

Ownership

Collaboration between the IT and OT domains is essential, but questions of OT cybersecurity ownership persist. But 70% of organizations plan to make the CISO responsible for OT cybersecurity.[1]

1. SANS 2019 State of OT/ICS Cybersecurity Survey, June 2019
2. IBM X-Force Threat Intelligence Index 2020, February 2020

The Titanic Disaster Scenario



Challenges & Threats

Awareness

60%

Across all industry verticals about 60% of organizations are still in the awareness phase .[1]

Visibility

78%

78% of organizations have partial cybersecurity visibility into operational technology.[2]

Control

2/3

Two-thirds of companies have no device/ communications level controls on internal network.[2]

Vulnerabilities

↑33%

It is typical for organizations to deal with 1,000's of cyber asset / vulnerability decisions each year.[4] New industrial vulnerabilities up 33% in 2 years.[5]

Threats

↑2,000%

Industrial cyber-attacks up 2,000% in since 2018.[6] Ransomware is the most common cyber-attack method representing 23% of incidents.[7]

Let’s Look at Some Statistics (cont.)

92%

92% of estimated costs arising from a cyber-attack are uninsured

$130 B

US Government spending over last decade in relation to cyber security
US$ 130 billion

$17 B

US Government estimated spending in financial year 2020 US$ 17 billion in relation to cyber activities

The vectors and impacts of cyber threats

Attackers aim to enter the IT or OT network

IT Target → Steal Data, Ransomware, Corporate Secrets, Executive Personal Data, etc.
OT Target → Control HMI and Level 1 devices to take over the process.

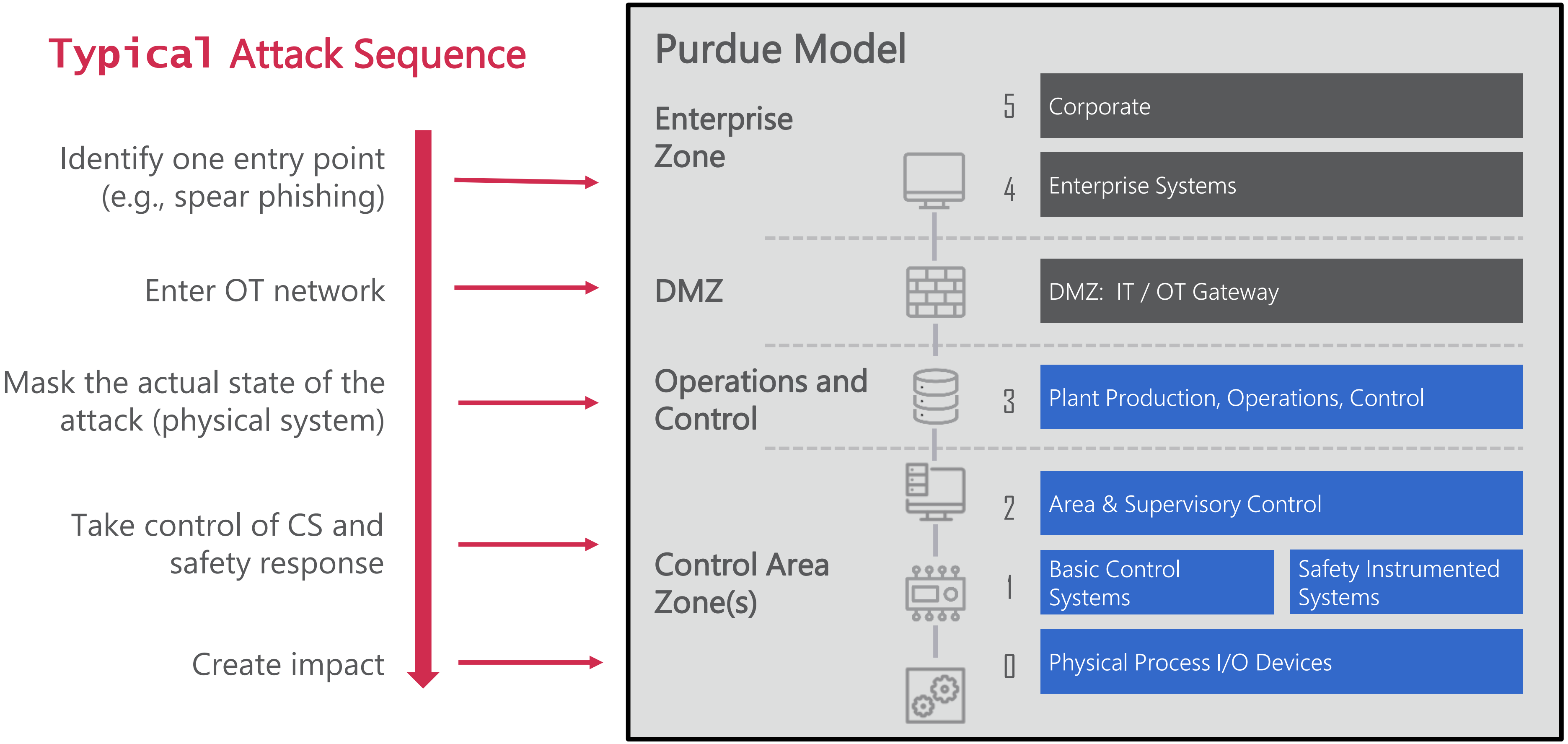
Incidents

Malware

Stuxnet
BlackEnergy 1, 2, 3
Havex
Industroyer
Triton
Shamoon 1&2
WannaCry, NotPetya

Events

Aurora
German Steel Plant
Ukraine 2015 & 2016
Dragonfly 1, 2



Typical Attack Sequence

Identify one entry point (e.g., spear phishing)

Enter OT network

Mask the actual state of the attack (physical system)

Take control of CS and safety response

Create impact

Purdue Model

Enterprise Zone
5 Corporate
4 Enterprise Systems

DMZ
DMZ: IT / OT Gateway

Operations and Control
3 Plant Production, Operations, Control

Control Area Zone(s)
2 Area & Supervisory Control
1 Basic Control Systems | Safety Instrumented Systems
0 Physical Process I/O Devices

OT System Vulnerabilities

Issue	Problem	Impact
No true "closed" system	• RF / Wireless • Vendor/contractor access • Third party carriers • Other regions/partners • Drill or universal keys $ online • Ops center network risks	• Easy to gain access to field cabinet and take control • **Backhaul to ops. Center and all other cabinets** • **Take control of entire system**
No authentication / UDP / unsecured communications	• Anyone can access controller / issue commands / connect / change/wipe • Control the power management systems • Man in the middle attacks	• Take over sections of the grid • Crash mode / must physically go to cabinets to reset / would not know • **Change/wipe configs/OS. Own controller and UPS** • Multiple power system manipulations
Extra unsecured services on controller	• Telnet, FTP, basic security	• Easy access for adversaries to critical functions/configs.

OT System Vulnerabilities - continued

Issue	Problem	Impact
No OT network monitoring	- Lack OT traffic visibility	- Don’t know if being attacked or recon underway
No prevention	- No way to stop an attack - Can’t block access - Can’t block rogue commands - Can’t block ransomware/malware	- Change commands, go dark - Lock up controllers - Wipe controllers - Power issues - Overcharge/blow up batteries
No restoration capability	- Must go to all cabinets, manually restore	- Huge time and resource issues, may not solve issue just reset and then attack replay
No forensics	- No idea where attack came from, how, where else it may be	- Guessing about the cause, where it could happen next, how to recover
Physical access risks	- Access by contractors, police, fire, rescue - Remote locations - Physical security challenge	- Hundreds/thousands of opportunities to install rouge devices and go up/down network

The Goal: Stop OT Cyber Threats Head-On

Protect OT networks and safeguarding operations.

What Makes That Possible?

Inline Policy Enforcement & Segmentation

- Inline network protection
- Failsafe security appliances

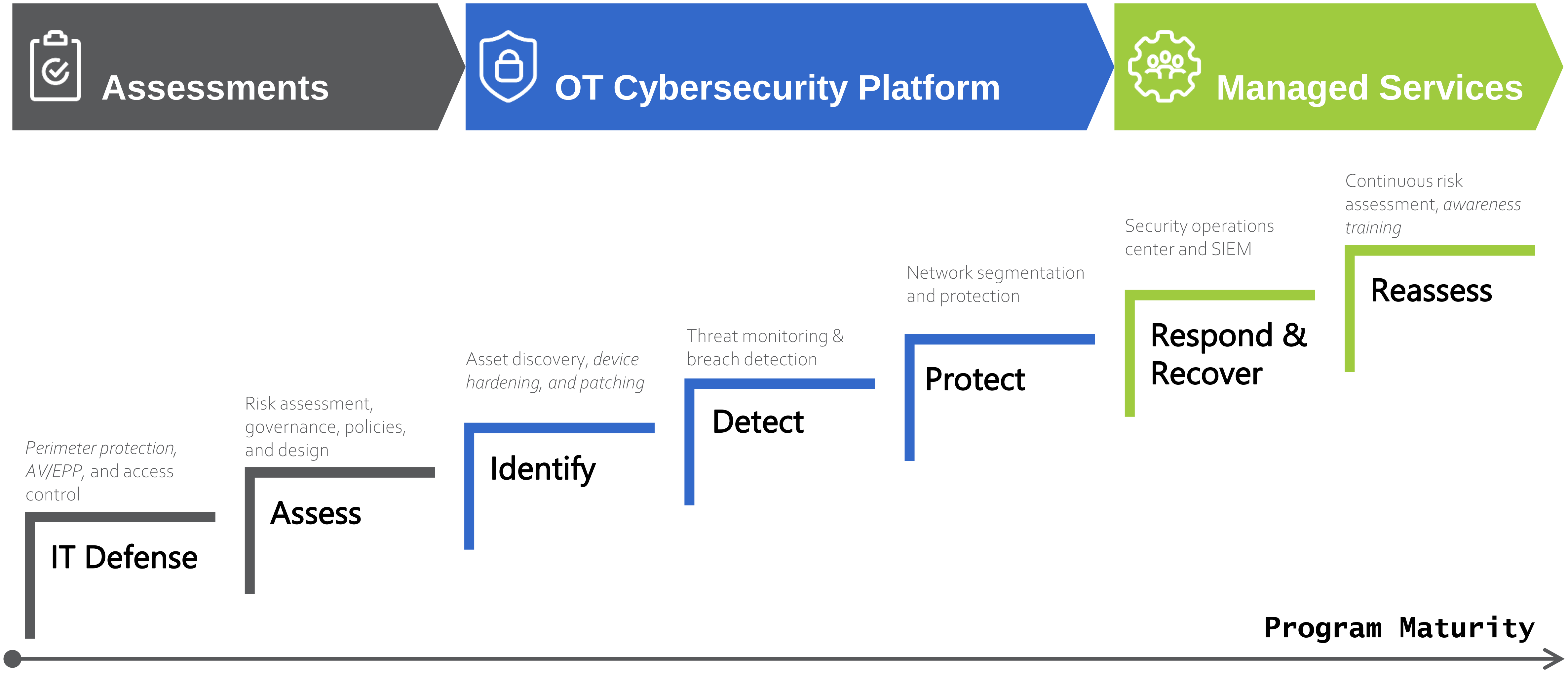
Level 0 Monitoring and Threat Detection

- Signal integrity and signal validation monitoring

24/7 Expertise and Monitoring

- OT Cyber Experts monitoring, protections, investigations, and help guide the response

Traditional Three Steps in the Process – Too Slow? Can they be compressed for efficiency and security?



Assessments

OT Cybersecurity Platform

Managed Services

Perimeter protection, AV/EPP, and access control

IT Defense

Risk assessment, governance, policies, and design

Assess

Asset discovery, *device hardening, and patching*

Identify

Threat monitoring & breach detection

Detect

Network segmentation and protection

Protect

Security operations center and SIEM

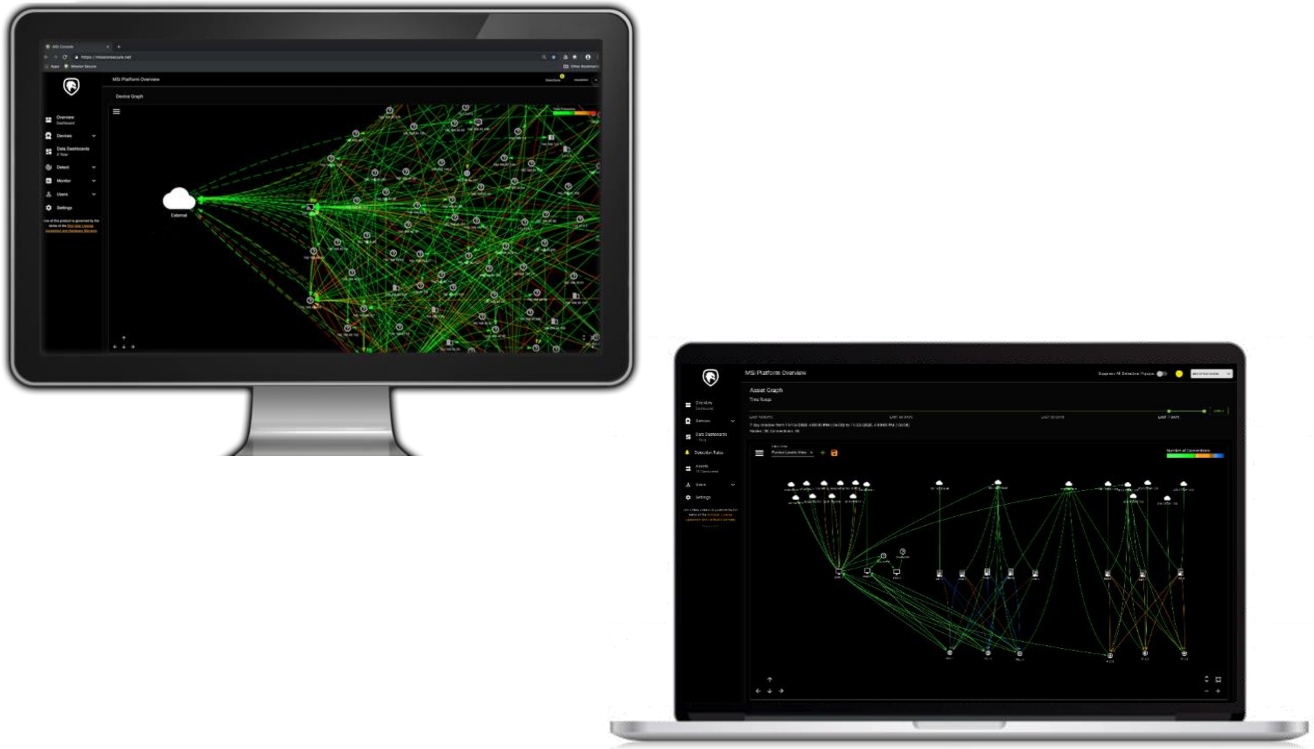
Respond & Recover

Continuous risk assessment, *awareness training*

Reassess

Program Maturity

OT Cyber Defense Platform Components



Security Management Console

Central Management

Primary user interface for visibility, and used to manage segmentations, protections, and signal-integrity monitoring.

Security Appliance

Visibility, Segmentation and Protection

Passively monitors OT traffic on the IP network, and provides inline network segmentation and protection of OT assets.

Signal-Integrity Sensor

Continuous Signal-Integrity Monitoring

Passively monitors electric signals at the physical level (Level 0) to detect changes that may indicate possible compromise or failure.

Note:
The Mission Secure Platform is a patented product of Mission Secure, Inc. covered by US Patents No. 9697355, 9942262, 10205733, 10250619, and 10530749.

OT Cybersecurity Platform with 24/7 Managed Services

24/7 Managed Services

Managed Protection & Incident Response – Add-on service to augment internal teams monitoring visibility and protections; and providing investigations and remediations.

Security Management Console

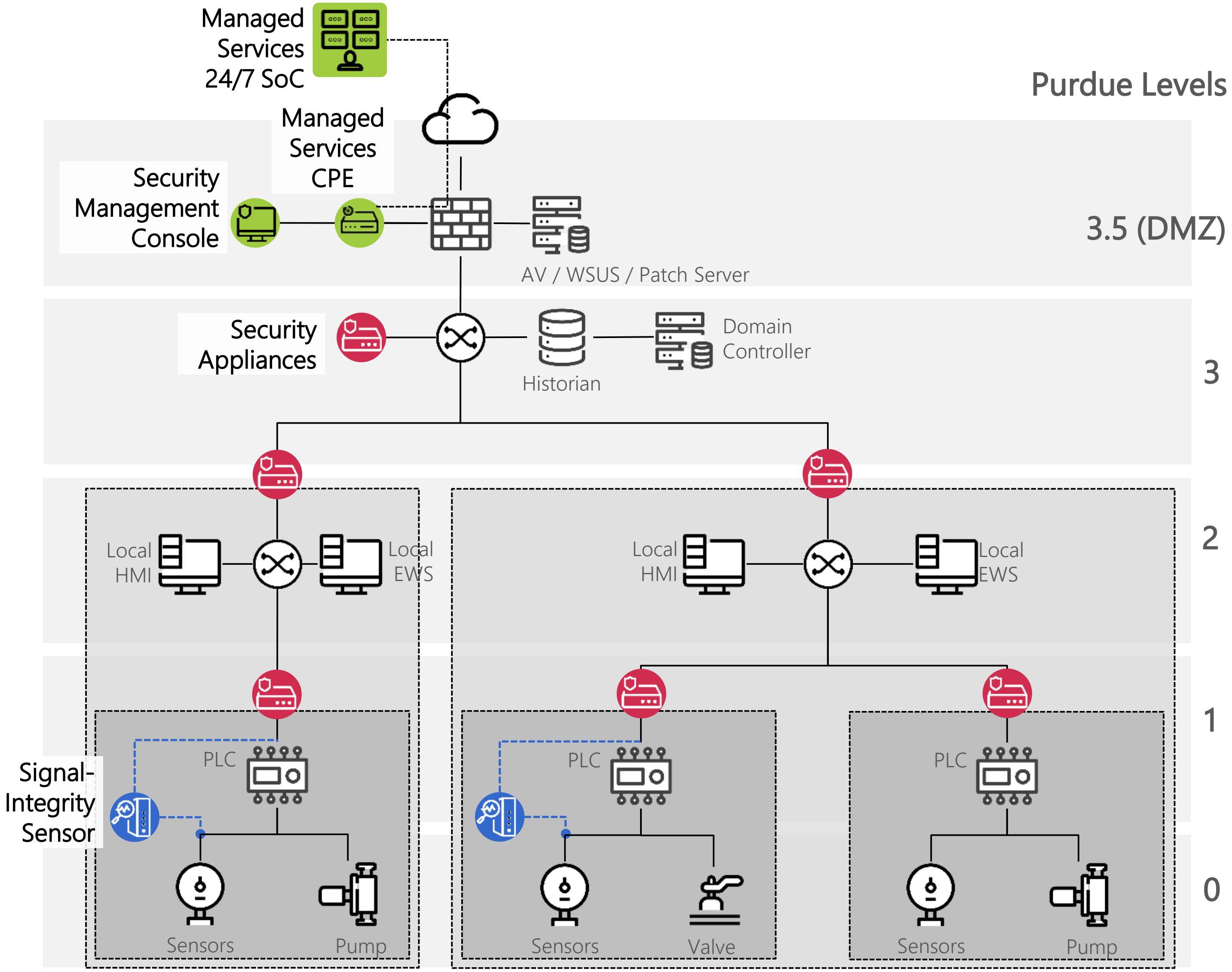
Central Management – Primary user interface for visibility, and used to manage segmentations, protections, and signal-integrity monitoring.

Security Appliance

Visibility, Segmentation & Protection –
-Passively monitors OT traffic on the IP network,
-Provides active inline network segmentation and protection of OT assets.

Signal-Integrity Sensor

Signal-Integrity Monitoring – Passively monitors electric signals at the physical level (Level 0) to detect changes that may indicate possible compromise or failure.



Managed Services

24/7

Remote OT cybersecurity coverage

2

Redundant threat management centers

Named security engineer + our expert team

Managed Visibility – continuous OT asset, and communications monitoring

Managed Protection – baselining, analysis, configurations and tuning

Analysis and Hunting – on-going OT network analysis, threat hunting, and reporting

Response and Support – security incident response, investigation and support

Contact information

Mission
Secure

1770 St. James Place
Suite 420
Houston, TX 77056
www.missionsecure.com

300 Preston Avenue
Suite 500
Charlottesville, VA 22902

Rick Tiene
VP, Smart Cities, Government,
and Critical Infrastructure
tiene@MissionSecure.com
m. 703.618.9100
www.missionsecure.com

Access to Public Records

Virginia Freedom of Information Act

Virginia Freedom of Information Advisory Council

http://foiacouncil.dls.virginia.gov/

foiacouncil@dls.virginia.gov

(804) 698-1810

Introduction to Records & FOIA

- All public records are presumed open unless specifically exempt.
- Definition of “public record” (§ 2.2-3701)
  - all writings and recordings that consist of letters, words or numbers, or their equivalent . . . however stored, and regardless of physical form or characteristics, prepared or owned by, or in the possession of a public body or its officers, employees or agents in the transaction of public business.

Requesting Records
§ 2.2-3704

- Who can make a request?
  - Citizens of the Commonwealth
  - Representatives of newspapers & magazines with circulation in the Commonwealth
  - Representatives of radio & television stations broadcasting in or into the Commonwealth
- How to make a request
  - Identify records with reasonable specificity
  - Name & legal address may be required

Responding to Requests

- Five working days to respond
- Five permissible responses to a request

Five Permissible Responses

1. Provide the requested records
2. Requested records are being entirely withheld
3. Requested records are being provided in part and withheld in part
4. Requested records could not be found or do not exist
5. Additional time needed to search for/produce records

How to Respond to a Request

- If any part of the answer is “no,” the response must:
  - Be in writing
  - Identify with reasonable particularity the subject matter of the withheld records; AND
  - Cite the specific section(s) of the Code of Virginia that authorizes the records to be withheld
- **NOTE:** if being entirely withheld, response must identify with reasonable particularity the volume of the withheld records

How to Respond to a Request

- If the records cannot be found or do not exist, the response must:
  - Be in writing, AND
  - If the public body knows that another public body has the records, it must provide contact information for the other public body.
- If the public body needs more time, the response must:
  - Be in writing, AND
  - Specify the conditions that make production of the records within the five-working-day period impossible.

Responding to Requests

- Five working days to respond ☑
- Five permissible responses to a request ☑
- Creation of new records not required ☑
- Charges for records

Charging for Records

- A public body may make reasonable charges not to exceed its actual cost incurred in accessing, duplicating, supplying, or searching for the requested records.
- May charge for exclusion review (*ATI v. UVA*, Va. Supreme Ct., 2014)
- Requester may ask for estimate in advance
  - Time period is tolled from time estimate is sent until requester responds
  - If no response within 30 days, request deemed withdrawn
- Public body may request a deposit for charges in excess of $200
  - Time period is tolled until deposit is paid
- Unpaid amounts for previous record requests

Electronic Records

- Requester may choose any format the public body uses in the regular course of business
- Use and retention of e-mail
  - Virginia Public Records Act, §§ 42.1-76, et seq.
    - Definition of "public record"
    - Retention schedules set by the Library of Virginia
  - Tips for using and managing email

Exemptions of General Application

- Personnel records
- Attorney-client privilege
- Legal memoranda and other work product
- Contract negotiation records
- Procurement records
- Account & routing numbers
- Economic development and retention

Q&A

VIRGINIA IT AGENCY

NTT DATA MESSAGING SERVICES

JON TOMSU & LEE MCMILLIAN

NTT DATA

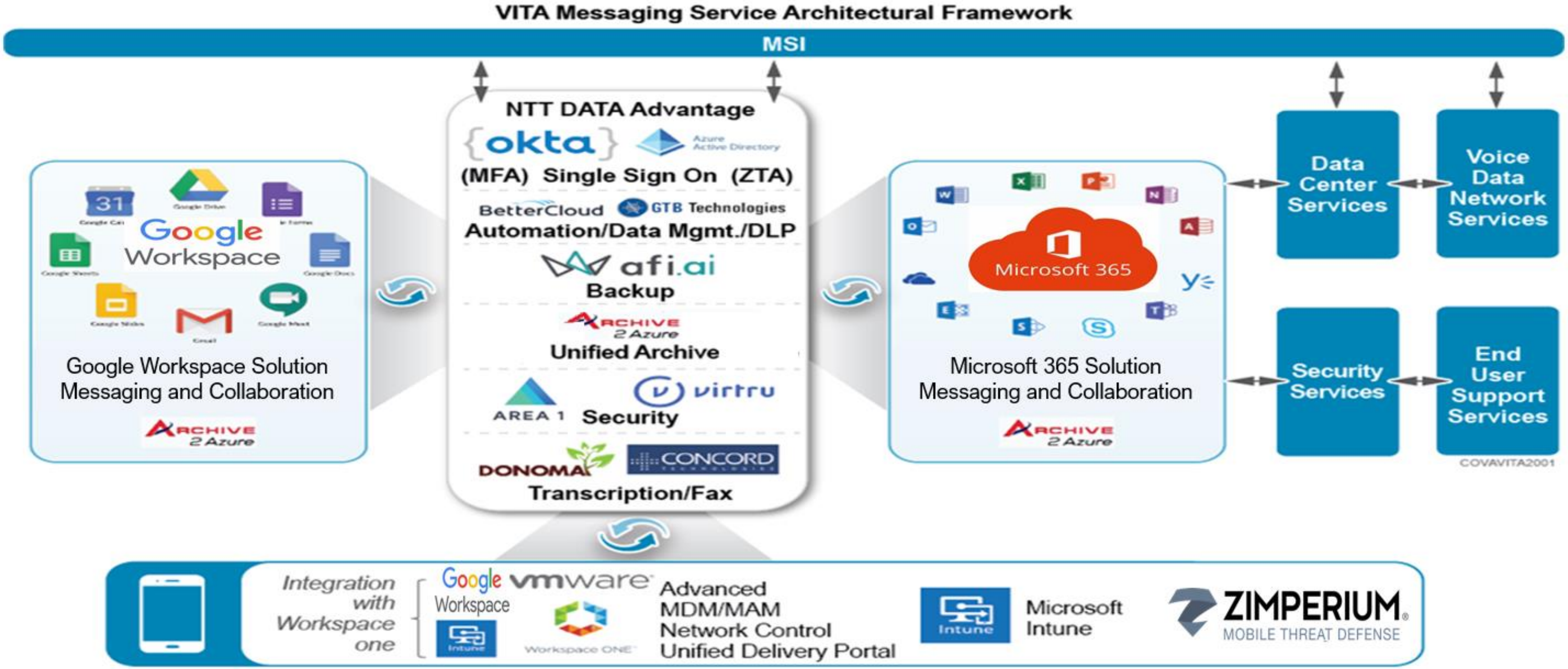
JUNE 2022

1 Messaging Solution Update

2 Where We Are Today

3 Pilot Migrations

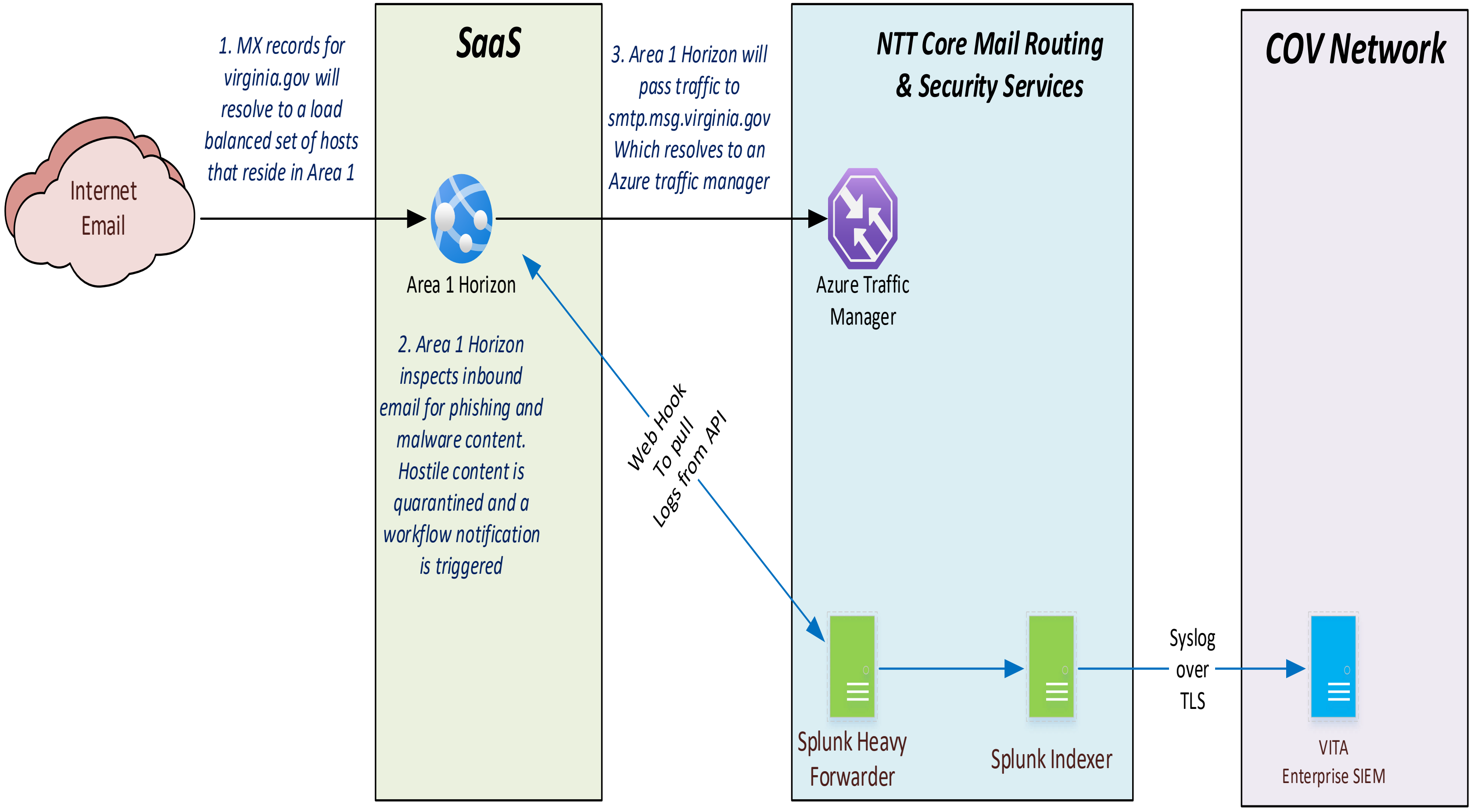
4 Q&A


VITA Messaging Service Architectural Framework
MSI
NTT DATA Advantage
okta
Azure Active Directory
(MFA) Single Sign On (ZTA)
BetterCloud
GTB Technologies
Automation/Data Mgmt./DLP
afi.ai
Backup
Archive 2 Azure
Unified Archive
AREA 1
virtru
Security
DONOMA
CONCORD
Transcription/Fax
Google Workspace
Google Workspace Solution
Messaging and Collaboration
Archive 2 Azure
Microsoft 365
Microsoft 365 Solution
Messaging and Collaboration
Archive 2 Azure
Data Center Services
Voice Data Network Services
Security Services
End User Support Services
COVAVITA2001
Integration with Workspace one
Google Workspace
vmware
Intune
Workspace ONE
Advanced
MDM/MAM
Network Control
Unified Delivery Portal
Intune
Microsoft Intune
ZIMPERIUM
MOBILE THREAT DEFENSE

WHERE WE ARE TODAY

- NTT DATA Messaging Solution went live on April 29, 2022
- Existing environment was documented with as-is baselines approved for where the existing environment was on April 29, 2022
  - Planning for hardening the security posture of the existing environment will start in August
  - Detailed recommended changes will be coming as part of the plan after August
- Reenabling native Google spam/phish reporting
- Virtru encryption at the enterprise level
- Migrations of data for pilot agencies has begun

SECURITY - AREA 1



Internet Email
1. MX records for virginia.gov will resolve to a load balanced set of hosts that reside in Area 1
SaaS
Area 1 Horizon
2. Area 1 Horizon inspects inbound email for phishing and malware content. Hostile content is quarantined and a workflow notification is triggered
3. Area 1 Horizon will pass traffic to smtp.msg.virginia.gov Which resolves to an Azure traffic manager
Web Hook To pull Logs from API
NTT Core Mail Routing & Security Services
Azure Traffic Manager
Splunk Heavy Forwarder
Splunk Indexer
Syslog over TLS
COV Network
VITA Enterprise SIEM

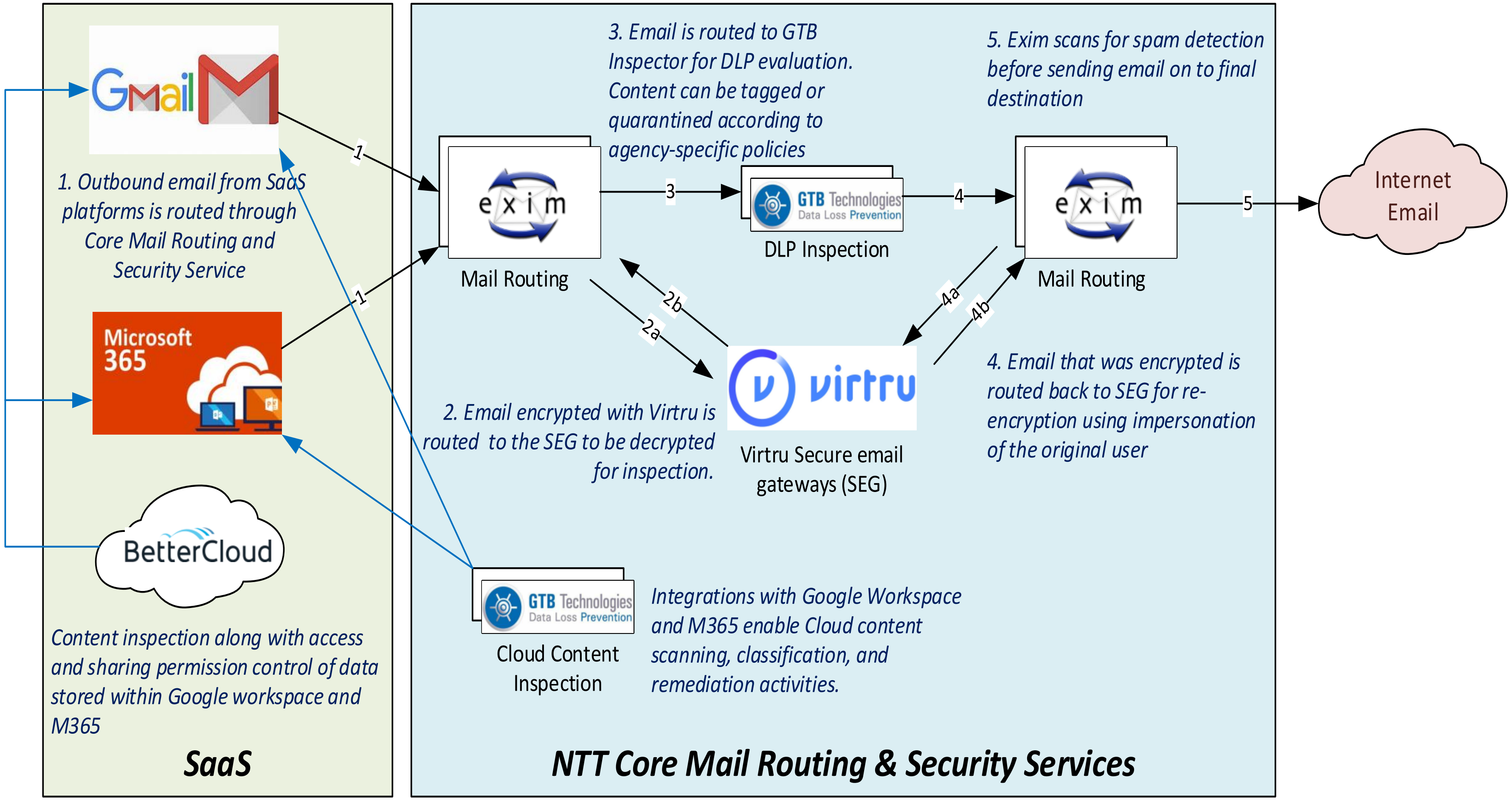
Area 1 includes:

- Provides anti-malware and anti-phishing and spam interdiction
- Integration with the messaging platform APIs to provide an avenue for users to report a message as SPAM or phishing

Agency Requirements:

- Can be configured for agency specific requirements.

DATA MANAGEMENT & DATA LOSS PREVENTION


Gmail
Microsoft 365
BetterCloud
exim
Mail Routing
GTB Technologies Data Loss Prevention
DLP Inspection
exim
Mail Routing
Internet Email
virtru
Virtru Secure email gateways (SEG)
GTB Technologies Data Loss Prevention
Cloud Content Inspection
1
1
2a
2b
3
4
4a
4b
5
SaaS
NTT Core Mail Routing & Security Services

1. Outbound email from SaaS platforms is routed through Core Mail Routing and Security Service

2. Email encrypted with Virtru is routed to the SEG to be decrypted for inspection.

3. Email is routed to GTB Inspector for DLP evaluation. Content can be tagged or quarantined according to agency-specific policies

4. Email that was encrypted is routed back to SEG for re-encryption using impersonation of the original user

5. Exim scans for spam detection before sending email on to final destination

Content inspection along with access and sharing permission control of data stored within Google workspace and M365

Integrations with Google Workspace and M365 enable Cloud content scanning, classification, and remediation activities.

DLP includes:

- Content scanning of data stored in cloud.
- Access and permission inspection and remediation.
- Inspection classification of content in-transit with and remediation – warning, quarantining and encrypting.
- Allows inspection and journaling of encrypted email.
- Enhanced anti-malware, anti-phish, and anti-spam services.
- All components to be integrated with VITA enterprise SIEM

Agency Requirements:

- GTB and BetterCloud can be configured to provide agency specific requirements.

CURRENT SCHEDULED PILOT MIGRATIONS

- The current schedule migrations with cut over scheduled are:
  - VITA June 3
  - DOLI June 10
  - VADOC
    - Wave 1 June 11
    - Wave 2 June 15
    - Wave 3 June 22

THANK YOU!

Thank
You
Merci
Gracias
Takk
aDank
Mèsi
Chokrane
Kiitos
Grazie
Xièxie
Dziakuju
GratiasAgimus
Spacibo
Danke
KamSahHamnida
Arigato
Hvala
TerimaKasih
ThintKo
Buznyg
Blagodaram
Rahmat
Malondo
Mercé
Taiku
Dakujem
Gràcies
Faleminderit
Efharisto
NajisTuke
Grandmercé
Tanemirt
Tenki
Bayarlalaa
Nirringrazzjak
Obrigado
Salamat
Saha
Multumesc
CámOn
Gracie
GratiasAgo
KopKhunKha
Tak
Sagolun
Motashakkeram
Dankie
Aciū
TänanVäga
Chnorakaloutioun
Barkal
Mauruuru
Grazzi
Murakoze
Koszonom
TapadhLeat
WaadMahadsantahay
BarakAllahuFiik
Aabhar
Graťzias

FORVIS

Advisory

2nd Line of Defense: IT Risk Management

ISOAG, Richmond, VA

JUNE 1, 2022

Introductions & Presentation Overview

FORVIS

Agenda for Today’s Discussion

Objective

Technology and data play a crucial role in today’s organization. Managing IT Risk within your company and also within your third parties is essential to managing and reducing your overall risk profile. The objective of our discussion will be to outline the Second Line of Defense (2LOD) model for IT Risk Management, including IT risk management strategies, frameworks and technologies, risk identification, monitoring, and GRC software.

Agenda

/ Introductions & Presentation Overview

/ 2LOD Model for IT Risk Management

/ Presentation Wrap Up

FORVIS

Speaker Bios

Ben Sady, CRISC, CISA, CIA, PMP
Principal, Advisory

ben.sady@forvis.com

- Ben is a Principal within FORVIS Advisory that has over 18 years of professional experience providing technology consulting and risk advisory services to organizations
- Ben has worked with 20+ public companies and 30+ Government Agencies in Technology & Risk Consulting
- Leader of FORVIS' IT Risk Management solutions activities including establishing IT Risk Frameworks and Monitoring programs
- Assisted companies with Audit technology and GRC system evaluation and implementation
- Examples of projects include IT Governance Consulting, Cyber Risk Assessment, Security Awareness Program Road Map, IT Issue Management Process Improvement, Enterprise Resilience Consulting, and Third Party – IT Risk Consulting

FORVIS

About FORVIS Advisory

FORVIS combines deep industry experience, comprehensive advisory services, and a strong commitment to client service. Our professionals are a global community of advisors driven by a shared passion to serve premier companies on industry-leading projects. We offer the resources of a Big Four firm with the responsiveness and focus on creating an exceptional client experience that a personal relationship demands. When working with FORVIS advisors, you will get a collaborative team bringing the strengths of their unique skillsets to help your organization achieve its goals.

- **Dedicated Advisory Professionals**
- **High-quality Delivery**
- **Solution-focused**

Key FORVIS Hubs

- Atlanta, GA
- Charlotte, NC
- Chicago, IL
- Dallas, TX
- London, UK
- Los Angeles, CA
- New York, NY
- Washington, D.C.

Key Praxity Hubs

- Dublin
- Paris
- Singapore

60,530+
Professionals

850+
Offices

110+
Countries

IT Risk Management

FORVIS

Risk Architecture & Technology

RISK & COMPLIANCE LANDSCAPE

First Line

Second Line

Third Line

Compliance Risk

Ops Risk

IT Risk

Third Party Risk

ESG Risk

Financial Risk

Internal Audit

RISK ARCHITECTURE & TECHNOLOGY

Technology Platforms, Software & Reporting Solutions

Data Inputs, Analytics, Automation & Business Intelligence

FORVIS SOLUTIONS

Risk Architecture Consulting

Risk Analytics & Automation Consulting

Technology Selection & Implementation Consulting

Managed Services

IT Risk Management / Moving Towards a Future State

Current state IT Risk Management functions may have room for improvement to achieve IT Risk Management goals.

Current State

- Standard Setting
- Coordination with Auditors
- IT Risk Training
- IT Control Testing & Reporting

→

Potential opportunities to mature the IT Risk Management function

Future State

- Policy Governance & Management
- IT Risk Management Methodology
- Risk Identification
- Risk Assessment
- IT Control Definition and Documentation
- IT Control Testing & Reporting

- Issue Management & Remediation Tracking
- Monitoring & Analyzing Metrics / Data Points
- Reporting to Executive Leaders
- Implementation of a GRC Software Tool
- Consideration of Analytics and Automation

FORVIS

IT Risk Management

Information Technology Risk is any risk related to information technology that can compromise IT in some way and therefore cause adverse impacts to the organization's products, services, internal business processes, or the organization's mission. IT Risk Management practices help organizations to identify risk, manage risk, and make risk-aware business and productdecisions.

DEVELOP YOUR STRATEGY & FRAMEWORK

- IT Risk Strategy & Target Operating Model
- IT Standard Setting & Policy Governance
- IT Risk Awareness & Training
- IT Risk Awareness Identification & Control Mapping
- IT Risk Monitoring & Response
- IT Risk Analytics & Reporting
- IT Risk Technology Software

IDENTIFY YOUR IT RISK AREAS

- IT Strategy & Governance Risks
- Cyber & Information Security Risks
- IT Operations & Service Delivery Risks
- IT Program & Project Delivery Risks
- IT Resiliency & Recovery Risks
- IT Risks for Products & Services
- IT Risks for Third-Party Management

PERFORM SPECIFIC IT RISK MANAGEMENT ACTIVITIES

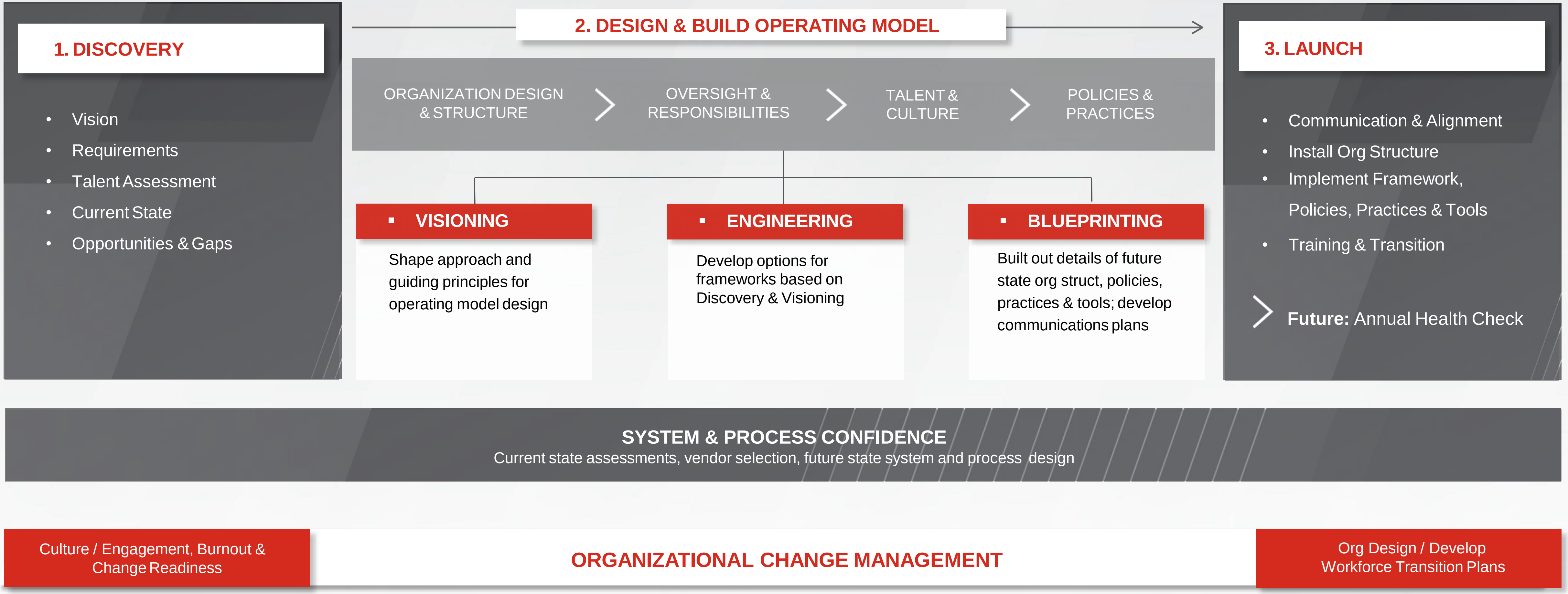
IT RISK WORKFLOW

1. Identify IT Risks
2. Map IT Risk to IT Control
3. Identify IT Key Risk Indicators (KRI)
4. Monitor IT KRIs and Assess IT Controls
5. Issue Management & Tracking
6. Report & Communicate IT Risks

FORVIS

IT Risk Strategy & Target Operating Model

Operating models are intended to put a structure, responsibilities, framework, tools, policies, and practices in place for an organization to operationalize their strategy. FORVIS can perform this exercise as part of strategy consulting (in depth, larger process) and then on an annual health check basis going forward to confirm strategy and target operating model are still aligned.



1. DISCOVERY

- Vision
- Requirements
- Talent Assessment
- Current State
- Opportunities & Gaps

2. DESIGN & BUILD OPERATING MODEL

ORGANIZATION DESIGN & STRUCTURE > OVERSIGHT & RESPONSIBILITIES > TALENT & CULTURE > POLICIES & PRACTICES

▪ VISIONING

Shape approach and guiding principles for operating model design

▪ ENGINEERING

Develop options for frameworks based on Discovery & Visioning

▪ BLUEPRINTING

Built out details of future state org struct, policies, practices & tools; develop communications plans

3. LAUNCH

- Communication & Alignment
- Install Org Structure
- Implement Framework, Policies, Practices & Tools
- Training & Transition

> **Future:** Annual Health Check

SYSTEM & PROCESS CONFIDENCE

Current state assessments, vendor selection, future state system and process design

Culture / Engagement, Burnout & Change Readiness

ORGANIZATIONAL CHANGE MANAGEMENT

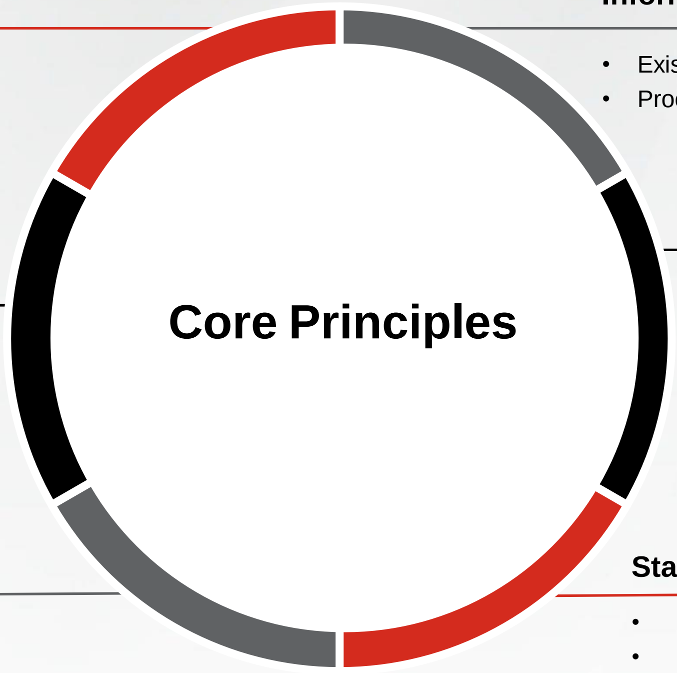
Org Design / Develop Workforce Transition Plans

FORVIS

IT Standard Setting & Policy Governance

Documentation Project

- **Consistency:** Consistency in message to stakeholders through standardized documentation
- **Input & Buy-In:** Input and buy-in from key stakeholders and senior management is imperative



Project Planning

- Key stakeholder engagement
- Document inventory
- Change management tracking

Information Gathering

- Existing documentation
- Process & policy walkthroughs

Governance Review & Approval

- Does document capture relevant risks & controls?
- Is the business / process accurately and completely reflected?

Document Drafting

- Documentation template
- Data / process flows
- Supporting information
  - + Process initiation
  - + Key dependencies
  - + Control points

Incorporate Feedback

- Enhance documentation

Standards Review

- Process owners
- Requirements

Policy Governance Software

- Repository of standards and policies
- Assign ownership of standards and policies
- Create workflows and reminders for review and approval
- Provides access to appropriate individuals to edit, review, and approve

Policy Governance-as-a-Service

- Manage the standard and policy update process
- Manage the standard and policy approval process
- Manage the standard and policy governance software
  - + Access
  - + Document uploads
  - + Workflows

IT Risk Awareness & Training

Focus Areas

- Ownership, Roles & Responsibilities
- Marketing & Email Communications
- Live Training & In Person Activities
- Videos & Computer Based Training
- Phishing Campaigns
- Social Engineering Testing
- Tool & Vendor Selection
- Metrics, Monitoring, & Continuous Improvement
- Leadership Reporting

Security Awareness-as-a-Service

- Manage the marketing and email communication process
- Manage training and events. Design, schedule, procure/partner, track attendance, and measure results
- Manage phishing campaigns and social engineering testing
- Provide metrics, dashboards, and reporting

PROGRAM MATURITY ASSESSMENT

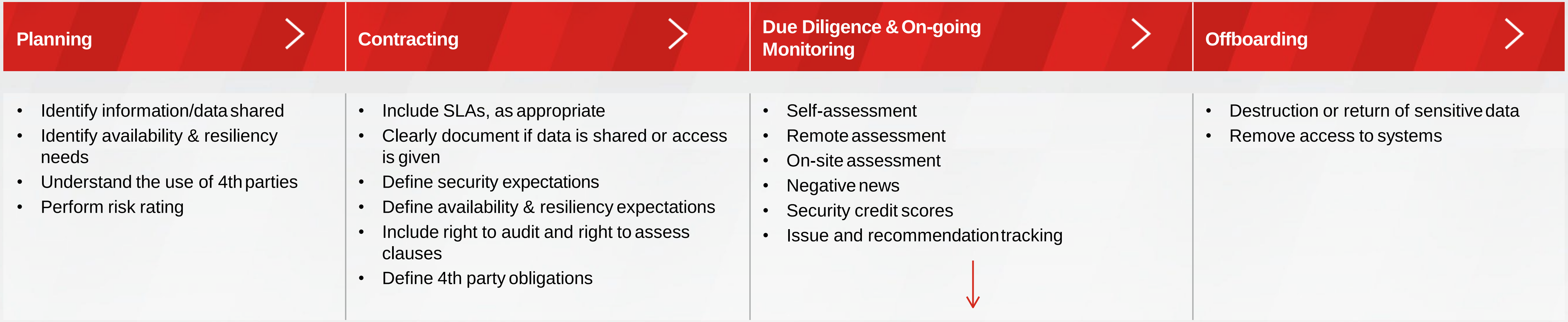
1. Understanding of Current Security Awareness Program
2. Evaluate against Industry Frameworks & Maturity Model
3. Hold Security Awareness Workshops to Gather Feedback

4. Provide Feedback on Program and Metrics Enhancements
5. Perform Security Awareness Testing (if desired)
6. Project Reporting

IT Risks for Third Party Management (IT TPRM)

FORVIS

TPRM Lifecycle Overview / IT Risk Considerations



Planning

- Identify information/data shared
- Identify availability & resiliency needs
- Understand the use of 4th parties
- Perform risk rating

Contracting

- Include SLAs, as appropriate
- Clearly document if data is shared or access is given
- Define security expectations
- Define availability & resiliency expectations
- Include right to audit and right to assess clauses
- Define 4th party obligations

Due Diligence & On-going Monitoring

- Self-assessment
- Remote assessment
- On-site assessment
- Negative news
- Security credit scores
- Issue and recommendation tracking

Offboarding

- Destruction or return of sensitive data
- Remove access to systems

IT Control Assessment Areas for Due Diligence & On-going Monitoring

- Org Charts and System Maps
- IT Risk Compliance Requirements
- Policies and Procedures
- Cybersecurity
- Network Security and Monitoring
- Logical Access Security to Sensitive Data & Systems
- Segregation of Duties
- Data Security
- Vulnerability Management

- Incident Response
- Use of Outsourced Vendors (4th party)
- Physical Security of Computer Equipment
- Backups and Restorations
- Disaster Recovery and Resiliency
- IT Change Management
- Recent/Future Changes to IT Systems
- Automated Data Transfers and System Interfaces
- Human Resources Policies

FORVIS Solutions for IT TPRM

Project Consulting:

- IT TPRM Program Development
- Identification of Third Parties and Data Sharing
- IT Risk Rating & Assessment
- IT Security Assessment of Third Parties
- Issue & Recommendation Tracking
- Metrics, Reporting & Dashboards

Outsourced Solutions

IT-TPRM-as-a-Service

- Build program governance, templates, and guidelines
- Risk assess existing third parties according to methodology
- Provide leadership reporting
- Risk assess new third parties
- Perform IT Security Assessments, per guidelines
- TPRM / GRC Software Solutions

IT Security Assessment Assistance

- Understanding of risk, contract terms & data sharing practices
- Planning, scheduling & logistics
- Review of self-assessment questionnaire (off-site)
- Perform remote or on-site security assessment
- Provide summary report on security maturity level
- Global tracking and analyzing of issues & recommendations

TPRM Outsourcing Solution Spectrum

Fully outsourced **Customized project execution** **Client designed and led**

FORVIS

Resiliency & Recovery

FORVIS

Why Enterprise Resilience

Business disruption threats have always been present. However, in recent years, pandemic and cyber threats have elevated the need for many organizations to increase their focus on Enterprise Resilience.

For some companies, the increased focus has highlighted complex people, process, and technology challenges.

By improving Enterprise Resilience, organizations are proactively monitoring and thereby improving their ability to minimize the impact of disruptions and respond, recover, and maintain business operations after a major disruption that may broadly impact an entire organization for prolonged periods.oring and managing

Drivers

- Need to create a comprehensive plan to assess, respond, and adjust after short-term or long-term business disruptions.
- Need to assess and improve an organization's continuity and recovery plans in the wake of the major threats.
- Increased regulatory focus to improve the quality and control procedures for resilience.

Benefits

- Comprehensive plan to mitigate business disruptions and minimize damage or loss.
- Ensure the continuation of critical business functions as expected by the organization's stakeholders.
- Ensure continuity and recovery readiness through training and test exercises.

How is Enterprise Resiliency Different?

Q: How does Enterprise Resiliency relate to Operational Risk Management (ORM), Enterprise Risk Management (ERM), Disaster Recovery Planning (DRP), and Business Continuity Planning (BCP)?

A: Enterprise Resiliency is a framework for an integrated and coordinated approach to manage major threats and disruptions to the Company. Enterprise Resiliency frameworks should include Risk Management (ERM & ORM), Disaster Recovery, Business Continuity, and also additional areas such as Human Resources, Legal, Public Relations, and Supply Chain.

Relationship To …	How is Enterprise Resiliency Different?
ORM & ERM – these are key risk management functions that operate on a daily basis to manage risk.	Enterprise Resiliency is not a day-to-day operation, but a framework to respond to and manage through major threats and disruptions. Risk Management teams are a critical piece of Enterprise Resiliency plans, but they are not the only piece involved.
DRP – this is specifically related to technology recovery after a disruption.	While DRP and BCP are key components of responding to and recovering from disruptions, they are not typically equipped to manage major disruptions that may last weeks, months, or longer than a year. In contrast, Enterprise Resiliency is a framework to respond to and manage larger and longer lasting disruptions. In those cases, DRP and BCP are components of an Enterprise Resiliency Plan.
BCP – this is focused on getting operations back to normal after a disruption.	

Q: Is there a difference between Enterprise Resilience and the following terms: Business Resilience, Organizational Resilience?

A: These terms are synonymous with Enterprise Resilience. They are referring to the same frameworks and desired outcomes.

FORV/S

Potential Functional Areas that Require Resiliency

- Risk Management
- Finance & Accounting
- Supply Chain & Third-Party Management
- Legal & Insurance
- Marketing & Brand
- Public Relations & Communications

- Human Resource Management
- Technology Applications
- Technology Operations & Support
- Information Security
- Internal Audit

- Business Operations
- Research & Development
- Field / Branch Operations / Home Offices

Above are examples of high-level functional areas that may be evaluated for Enterprise Resiliency enhancements, with a particular focus on People and Processes in addition to Technology. These areas are critical components of an Enterprise Resiliency program, each with specific activities, metrics, and monitoring being performed during a disruption, with the goal to manage risk, communicate, and ultimately return to normal operations.

FORVIS

Thank You!

forvis.com

The information set forth in this presentation contains the analysis and conclusions of the author(s) based upon his/her/their research and analysis of industry information and legal authorities. Such analysis and conclusions should not be deemed opinions or conclusions by FORVIS or the author(s) as to any individual situation as situations are fact specific. The reader should perform its own analysis and form its own conclusions regarding any specific situation. Further, the author(s) conclusions may be revised without notice with or without changes in industry information and legal authorities.
FORVIS has been registered in the U.S. Patent and Trademark Office, which registration is pending.

FORV/S

Assurance / Tax / Advisory

VIRGINIA IT AGENCY

MANAGED SECURITY SERVICES ISOAG UPDATE

DARRELL RAYMOND, ATOS
SERVICE DELIVERY MANAGER

BILL STEWART, VITA
MANAGED SECURITY SERVICE OWNER

JUNE 1, 2022

AGENDA

- CrowdStrike rollout update
- Cloud web proxy migration (UCE)
- Web application firewall (Silverline)
- Compliance testing - network (CTN)

CrowdStrike rollout update

CROWDSTRIKE ROLLOUT

- CrowdStrike Falcon agent installed and active on over 95% of qualified endpoints
- All but five agencies are in full blocking mode
  - Remaining agencies have active pilots
  - Working with each to move the remainder to blocking mode
- CrowdStrike data available on the VITA security dashboard

Cloud web proxy migration (Unified Cloud Edge – UCE)

What is happening?

The web proxy service at VITA are being migrating from on-premise devices to a new cloud-based service (Unified Cloud Edge).

Benefits of this move include **lower latency** and a **consistent experience** both on and off the COV network.

The migration will initially focus on workstations already managed by the McAfee client proxy. Clients will now be sent to the cloud by default and only to on-premise for specific items such as Okta (to avoid multifactor authentication (MFA) while in the office) and subscription services. After the workstation migration, servers and other devices will be moved to the new cloud-based proxy.

How will this be done?

This migration occurs in the background and will be transparent to end users. Commonwealth devices are already using this solution when off the COV network.

A policy update will be pushed from McAfee EPO to workstations that will redirect web traffic on ports 80 and 443 to a cloud-based proxy. The web proxy behavior after the change will mimic behavior when users are off the network today.

This migration will direct internet traffic to the cloud as the default path.

What will be different?

The major difference with the cloud-based service is that coaching will not be in effect.

Agency information technology resources (AITRs) and information security officers (ISOs) who are accustomed to retrieving data from the content security reporter will find that it will only have data for workstations in the office or on COV AnyConnect virtual private network. Reports for workstations that are not on the network will need to be requested via the VITA customer care center (VCCC).

When will I be moved?

The migration will be performed on an agency-by-agency basis

The migration has been piloted at several agencies with only a few issues reported

Three of the agencies have had all workstations migrated at this time

A proposed schedule for the agency migrations will be provided in early June

Web application firewall (WAF – Silverline)

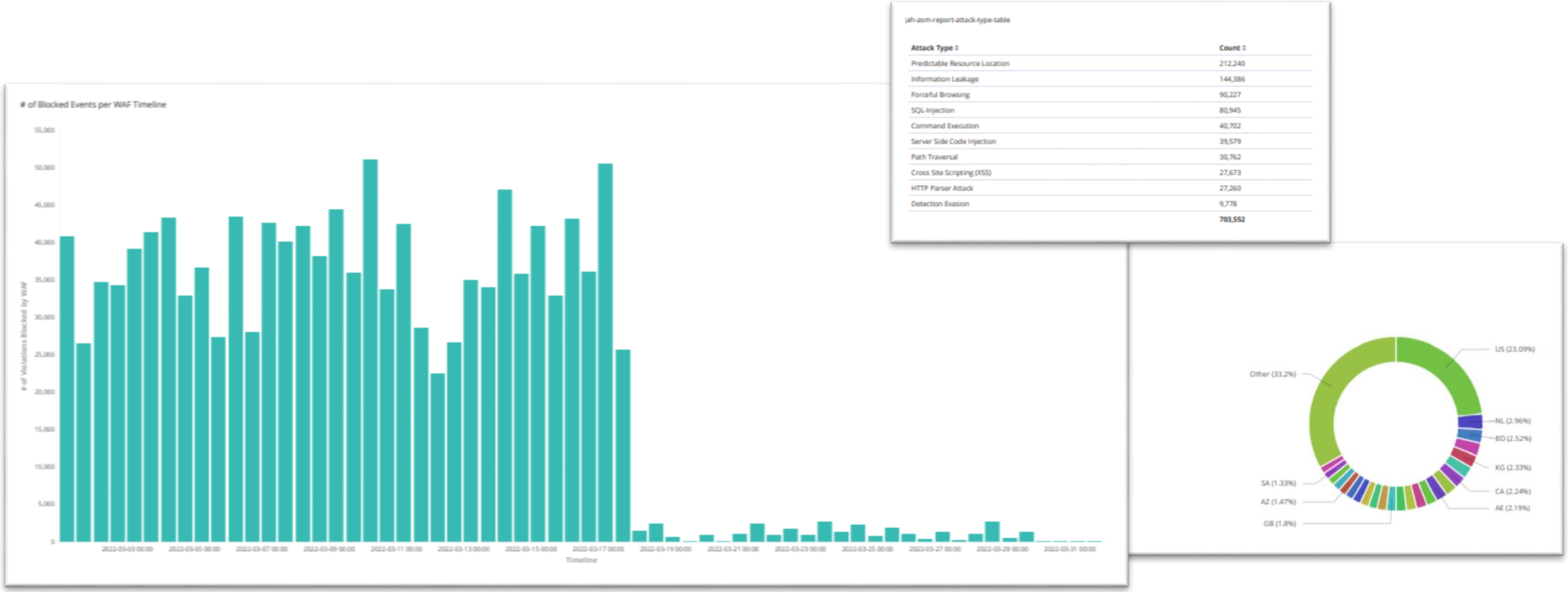
WEB APPLICATION FIREWALL (WAF - SILVERLINE)

Service overview:

- DDoS always-available (for WAF proxy coverage) at 125 Mbps clean bandwidth
- Managed WAF (50 FQDNs) at 125 Mbps clean bandwidth
- Threat intelligence add-on
- Advanced governance plus (US-based resources)

WEB APPLICATION FIREWALL (WAF - SILVERLINE)

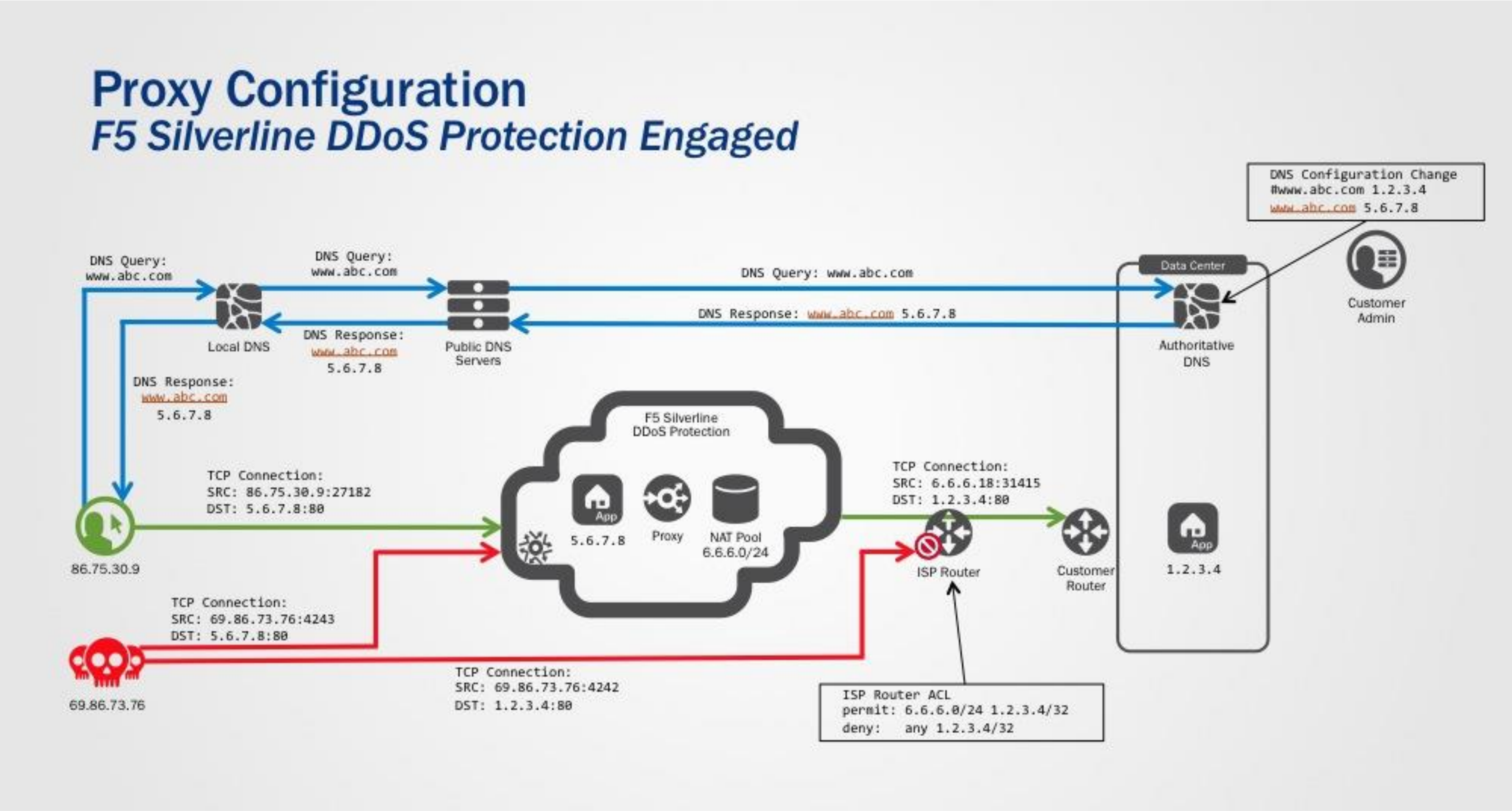
Sample reporting:



jah-asm-report-attack-type-table

Attack Type ⇕	Count ⇕
Predictable Resource Location	212,240
Information Leakage	144,386
Forceful Browsing	90,227
SQL-Injection	80,945
Command Execution	40,702
Server Side Code Injection	39,579
Path Traversal	30,762
Cross Site Scripting (XSS)	27,673
HTTP Parser Attack	27,260
Detection Evasion	9,778
	703,552

WEB APPLICATION FIREWALL (WAF – SILVERLINE)



Proxy Configuration

F5 Silverline DDoS Protection Engaged

```
DNS Configuration Change
#www.abc.com 1.2.3.4
www.abc.com 5.6.7.8
```

```
ISP Router ACL
permit: 6.6.6.0/24 1.2.3.4/32
deny:   any 1.2.3.4/32
```

© F5 Networks, Inc

10

Compliance testing – network (CTN)

COMPLIANCE TESTING – NETWORK (CTN)

What is CTN?

Compliance testing network (CTN) is a network access control tool that verifies compliance with COV security standards prior to providing access to COV network resources.

How does it work?

CTN uses administrative credentials to obtains detailed information regarding the security posture of the device:

- Device type
- Location
- User
- Agency domain membership
- Policy compliance status

COMPLIANCE TESTING - NETWORK (CTN)

Status

CTN is being deployed using multiple projects (aka phases)

✓ Discovery - Through a series of reports and integration points, CTN will be used to identify, document and report on the devices that are on your agency's network (complete – reports on request and via the VITA security dashboard)

➢ Reconciliation - Utilizing the compliance report, the non-compliant devices will be remediated (agencies currently reviewing for CMDB compliance)

- Enforcement – All non-compliant devices will be moved from the COV network to an alternate network (date TBD based on agency, VITA and MSS collaboration)

QUESTIONS?

Thank you!

REGISTRATION IS OPEN

2022 COMMONWEALTH VIRTUAL INFORMATION SECURITY CONFERENCE – AUG. 18, 2022

HTTPS://WWW.VITA.VIRGINIA.GOV/INFORMATION-SECURITY/SECURITY-CONFERENCE/

More details on presenters and keynotes will be forthcoming. If you have questions about the conference, contact: covsecurityconference@vita.virginia.gov

If you are interested in presenting or know of someone you would like to present, contact:

isconferencecfp@vita.virginia.gov

IS ORIENTATION

IS Orientation

Remote - WebEx

June 30, 2022

start time: 1:00 PM

end time: 3:00 PM

Instructor: Marlon Cole

https://covaconf.webex.com/covaconf/onstage/g.hp?MTID=e401af82c17ac0ab6aef3cab1555acea4

IS COUNCIL COMMITTEE

The next scheduled meeting for the IS Council:

June 8, 2022

12 – 1 p.m. via Google Meet

If you would like an invite to the meeting, contact:

tina.gaines@vita.virginia.gov

ISO/AITR APPROVERS LIST

Please make sure your approver’s list is updated and current. If there are personnel changes in your agency, work with your CAM to make sure the changes are reflective on your list.

You may request a copy of your agency’s ISO/AITR Approvers list from the VCCC@vita.virginia.gov or tina.gaines@vita.virginia.gov

JULY 2022 ISOAG

July 13, 2022, from 1 to 4 p.m.
MACH 37 Partnership Meeting

Presenters:

Randy Marchany - Speaker
Topic:
University Information Technology Security Officer
Virginia Tech
marchany@vt.edu
1:00

MACH 37 (Partnership Meeting)
2:00

Milty Brizan - Speaker
Robert West - Contact
Topic:
Amazon Web Services
Sr. SLG Enterprise Account Executive, VA, MD and DE
brizanm@amazon.com
wstrobe@amazon.com
3:00

VIRGINIA
IT AGENCY

THANK YOU FOR ATTENDING!