VIRGINIA
IT AGENCY

WELCOME TO THE SEPT. 14, 2022

ISOAG MEETING

AGENDA	
Welcome	Ed Miller / VITA
The Data-first Approach; Managing the Tension Between Security and Productivity	Brian Vecci & Brandon Lapetina/ Varonis
Activities at the Virginia Smart Community Testbed	David Ihrie/CIT
A Dynamic Process for Minimizing the Likelihood and Impact of Cyber Attacks	Chris Jensen/Tenable
Upcoming Events	Ed Miller/VITA
Adjourn	

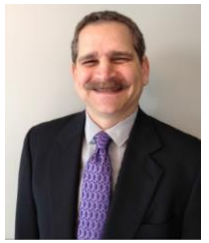
VIRGINIA IT AGENCY

There are no slides available for Varonis Presentation

IoT and Related Challenges For Cybersecurity

ISOAG Meeting
September 14, 2022

David Ihrie, CTO/CIO
David.Ihrie@VirginiaIPC.Org



Funding for many of the technologies incorporated into the Virginia Smart Community Testbed has been provided by the U.S. Department of Homeland Security, Science & Technology Directorate, under contract number 70RSAT19CB0000025

VIPC | VIRGINIA INNOVATION PARTNERSHIP CORPORATION
Connecting Innovators with Opportunity

Topics

- VIPC?
- So what have you been up to lately?
- Cybersecurity Implications
- Facing the Challenges

VIPC | VIRGINIA INNOVATION PARTNERSHIP CORPORATION
Connecting Innovators with Opportunity

VIPC | VIRGINIA INNOVATION PARTNERSHIP CORPORATION
Connecting Innovators with Opportunity

Virginia Innovation Partnership Authority

State legal authority

Virginia Innovation Partnership Corp.

Designated Not-for-Profit
VIPA Operating Entity

Entrepreneurial Ecosystems Division

Mission

Support and connection for entrepreneurial ecosystems and stakeholders around Virginia, including startup incubators and accelerators

Commercialization Division

Mission

Grant funding in support of tech-based research, development and commercialization to drive economic growth in Virginia

Investment Division

Mission

Seed and early-stage funding for Virginia-based companies with high potential for rapid growth and significant economic returns

Strategic Initiatives

Mission

Leadership for strategic initiatives that explore and shape programs designed to attract and grow innovation and new industries

Strategic Initiatives Current Portfolio

SCITI LABS

VIPC | Smart

VIRGINIA SMART COMMUNITY TESTBED STAFFORD, VA

VIPC | VIRGINIA INNOVATION PARTNERSHIP CORPORATION
PUBLIC SAFETY INNOVATION CENTER

Virginia Unmanned Systems Center at VIPC

Topics

- VIPC?
- So what have you been up to lately?
- Cybersecurity Implications
- Facing the Challenges

VIPC | VIRGINIA INNOVATION PARTNERSHIP CORPORATION
Connecting Innovators with Opportunity

WHAT IS THE TESTBED?

The Commonwealth's home for developing Smart Technology

Mission: Serves as Virginia's "living laboratory" to test new smart technology and be a "model smart community" by communities across the nation

Vision: Lead the county and Commonwealth in Smart Community implementation and serves to accelerate technology solutions for the Commonwealth

Purpose: Foster growth through public-private partnerships, sponsors, investors, entrepreneurs, and pilot projects opportunities

From Innovation to Impact Under One Virtual Roof

VIRGINIA SMART
COMMUNITY TESTBED
STAFFORD, VA

A GROWING SUCCESS STORY

Recently recognized as a 'Smart 50 Awards' recipient:
this award presented by Smart Cities Connect recognizes global smart city projects, honoring the most innovative and influential work.

Attracting global businesses:

VIRGINIA SMART
COMMUNITY TESTBED
STAFFORD, VA

Testbed Anniversary Event

*"One of the efforts we highlighted at INTERSCHUTZ was the Virginia Smart Community Testbed (VA Testbed), a dynamic lab showcasing innovations developed to provide new solutions for homeland security and dual-use technologies— **one of S&T's most successful public-private partnerships to date**. The idea for the VA Testbed was born more than three years ago, as S&T came together with the Virginia Innovation Partnership Corporation (VIPC), the Commonwealth of Virginia, and Stafford, Virginia, to convert a former convenience store into a cutting-edge testbed for technologies that can be applied to real-world uses benefiting the public."*

Dan Cotter

VIPC | VIRGINIA INNOVATION PARTNERSHIP CORPORATION
Connecting Innovators with Opportunity

A Network of Living Laboratories

Many made possible by DHS Support

Winchester Virginia

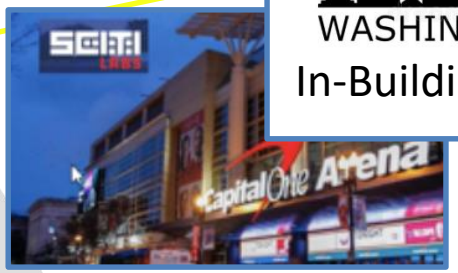
Municipal Drone Ops

Garrisonville

Smart Bases
Workforce Development
AR/VR/Immersive Tech

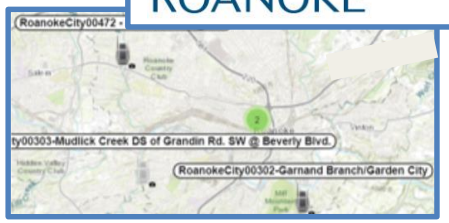
WASHINGTON DC

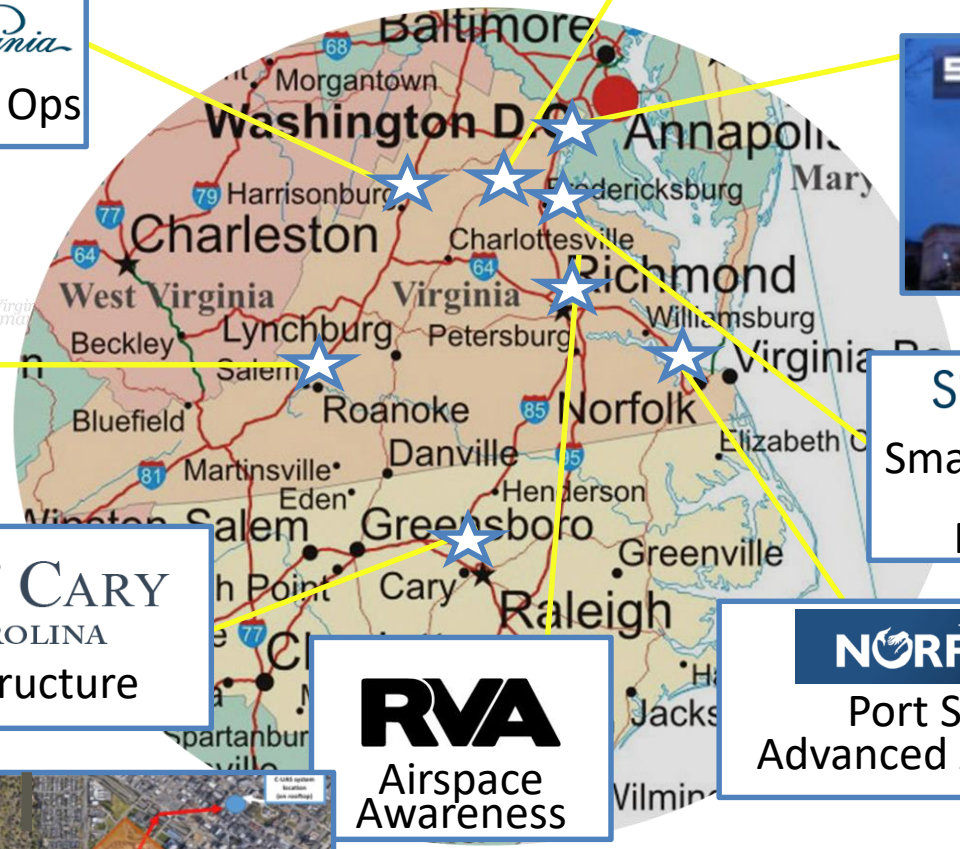
In-Building Sensors



ROANOKE

Integrated
Water
Management





STAFFORD
Virginia

Smart Communities
Secure IoT
Public Safety

TOWN of CARY
NORTH CAROLINA

Civic Infrastructure

RVA

Airspace
Awareness

THE CITY OF NORFOLK

Port Security
Advanced Air Mobility

VIPC | VIRGINIA INNOVATION PARTNERSHIP CORPORATION

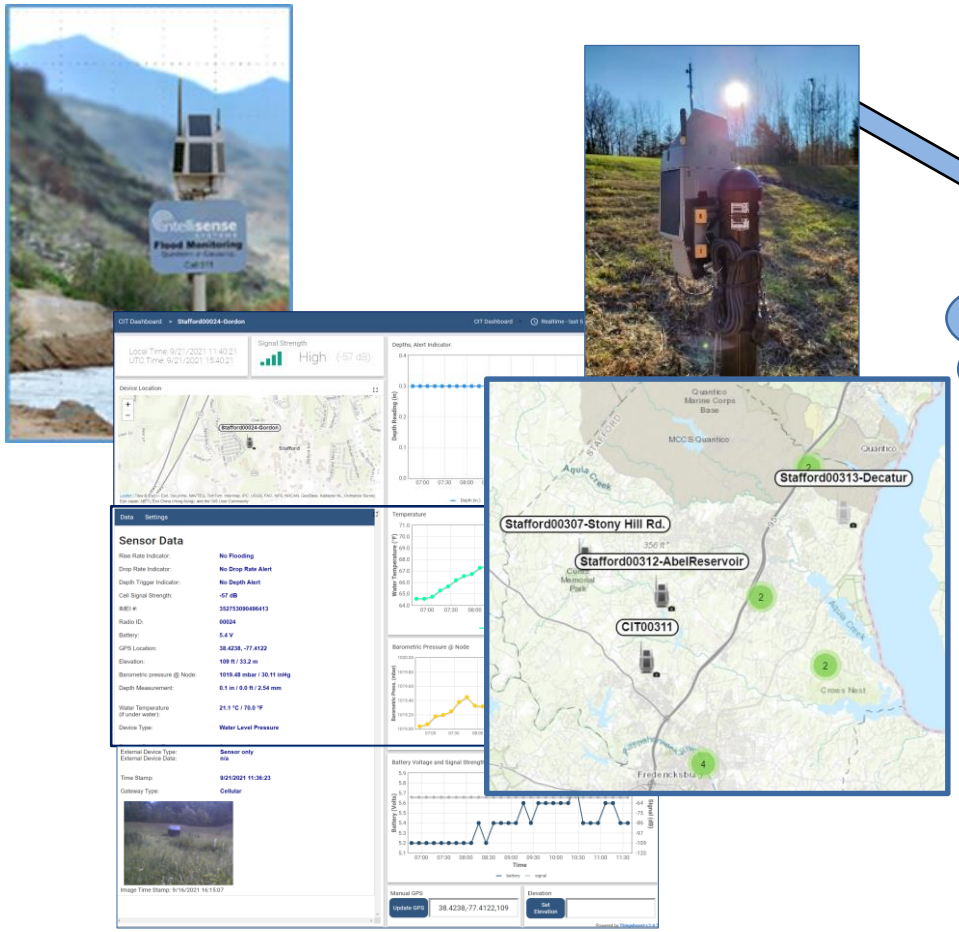
Connecting Innovators with Opportunity

Public-Private Partnership Deploys Flood Sensors

Homeland Security
Science and Technology

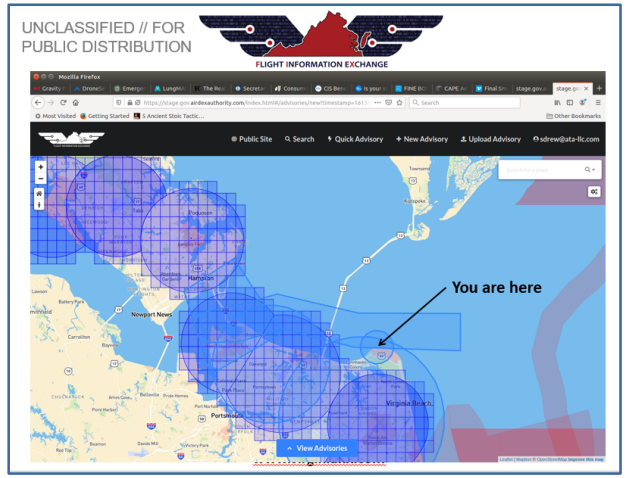
VIPC | VIRGINIA INNOVATION PARTNERSHIP CORPORATION

Commonwealth Investment



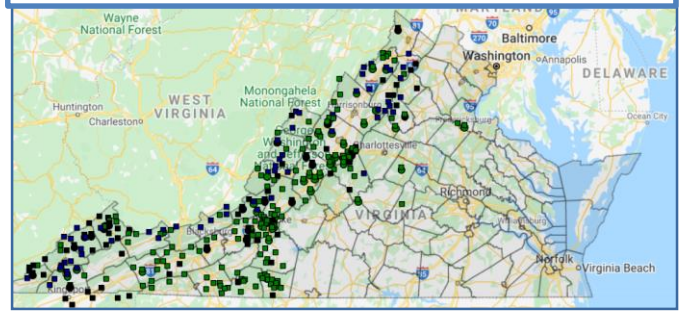
Stafford County Using Data for Emergency Management of Flooding

Commonwealth Data Trust



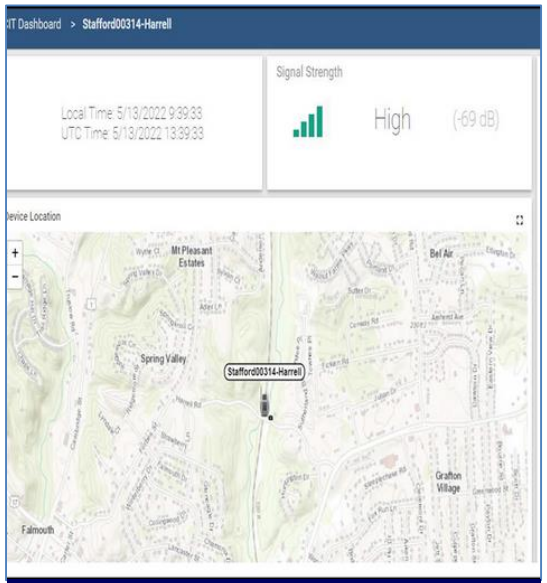
VA-FIX Supports Airspace Coordination For Drone Operators

Virginia Department of Emergency Management

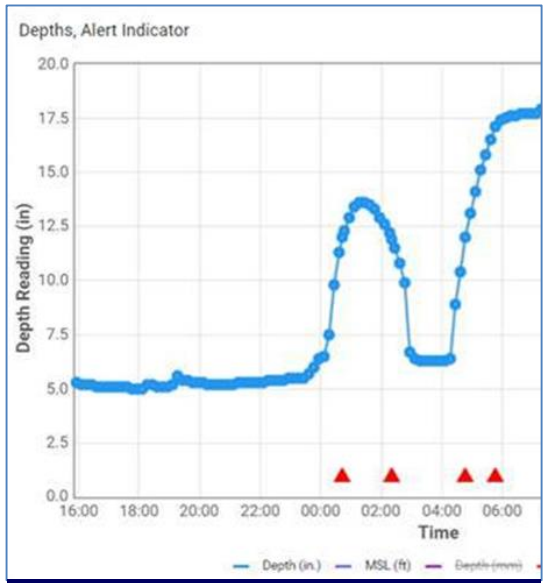


Legacy IFLOWS Network Informs NWS Flood Alerts

Flood Sensors in Operation

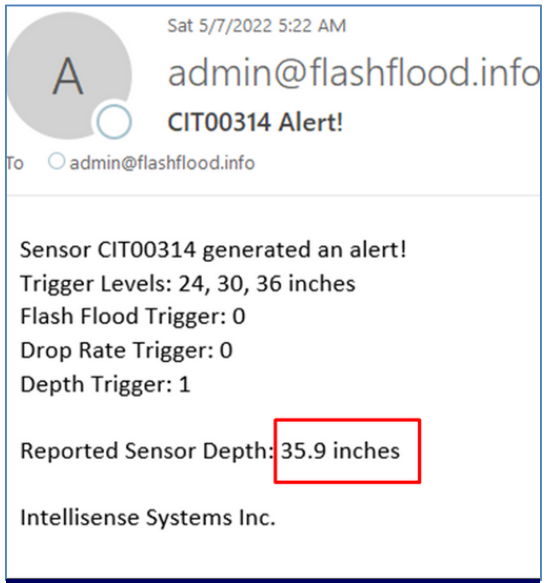


Flood map for Harrel Road

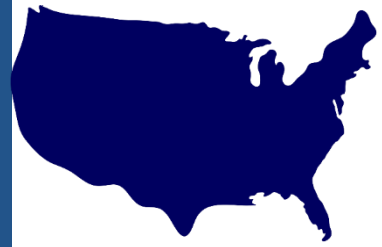


Flood chart for Brooke Road

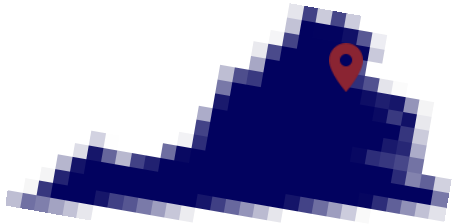
Harrel Road Sensor Activated



Email Alert Notification



400 Nationwide



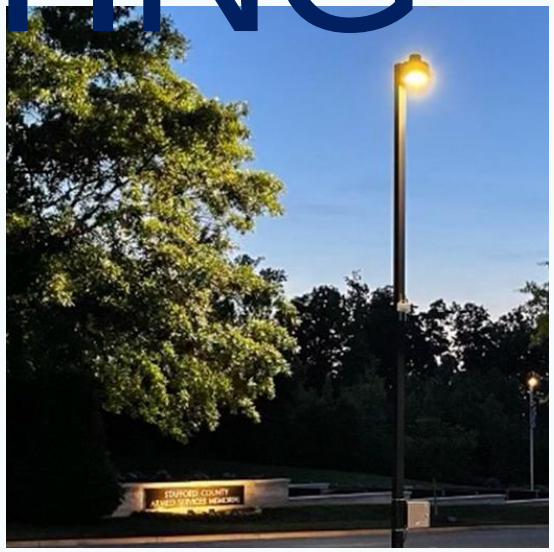
100 in Virginia
14 in Stafford County

VIPC | VIRGINIA INNOVATION PARTNERSHIP CORPORATION
Connecting Innovators with Opportunity

PROJECT

SMART LIGHTING

- First deployment of its kind in North America
- Reduced energy and increase cost savings
- Provides a wireless mesh broadband network
- 90% faster implementation of gigabit networks



VIRGINIA SMART
COMMUNITY TESTBED
STAFFORD, VA

Digital Transformation of Infrastructure

Air Quality/
Wildfire

Weather
Stations

Drone Video/Data

Smart Lighting/
WiFi

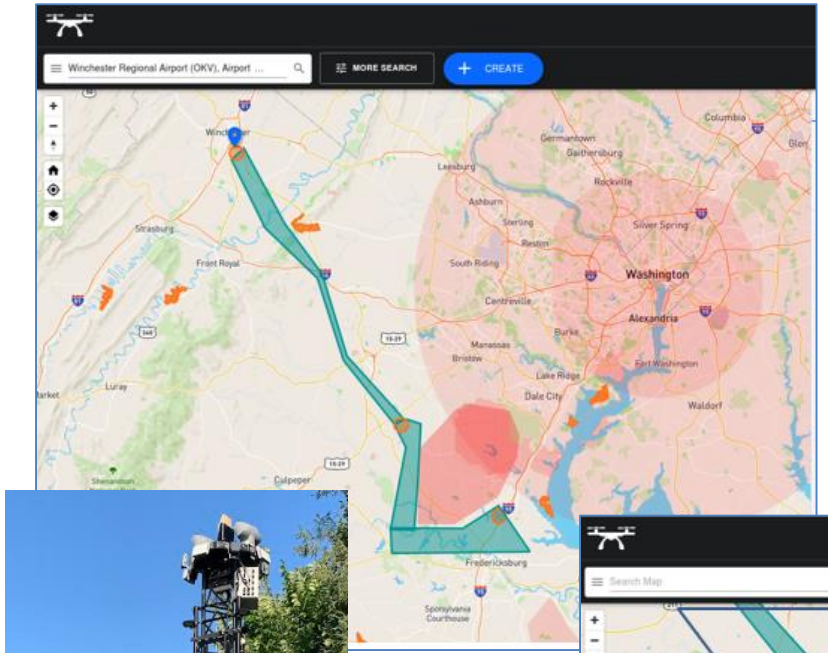
Flood

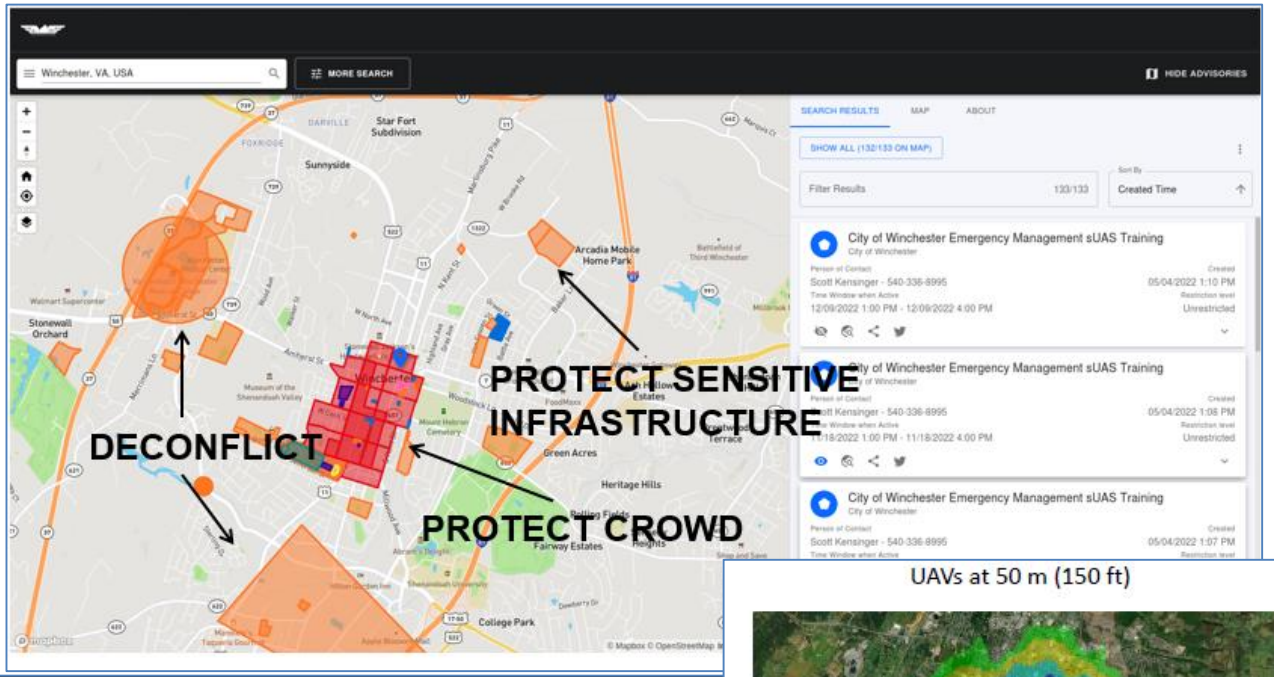
Information
Kiosks

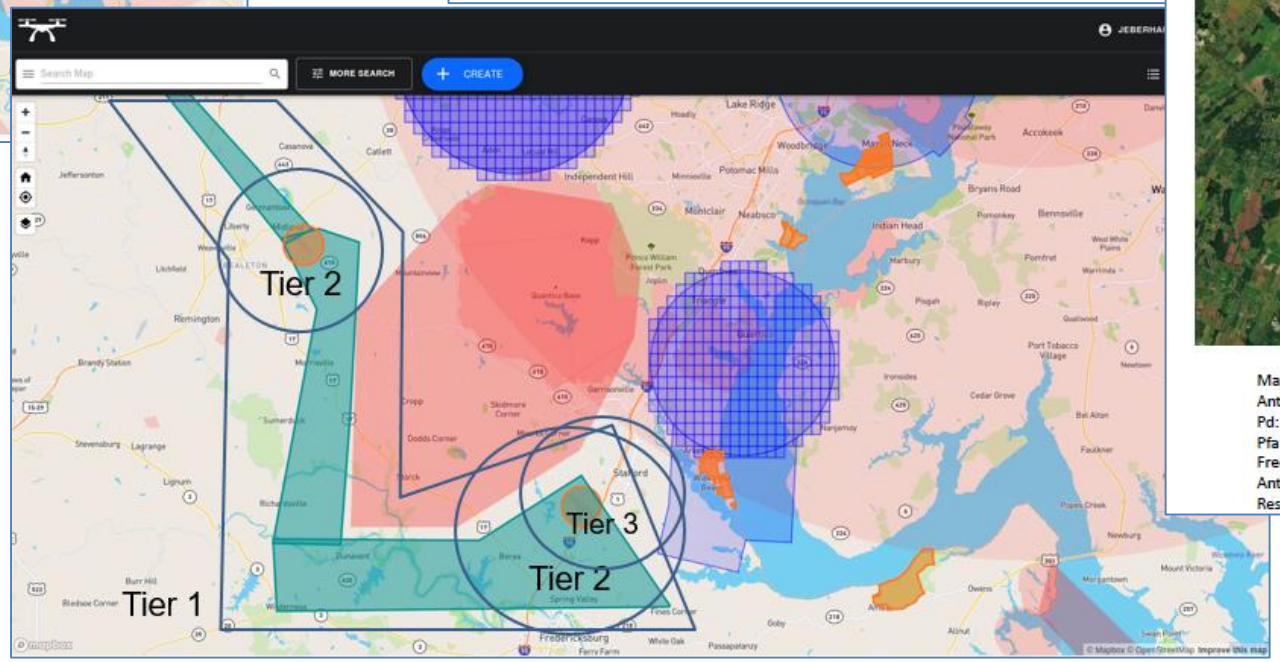
Robotic
Devices

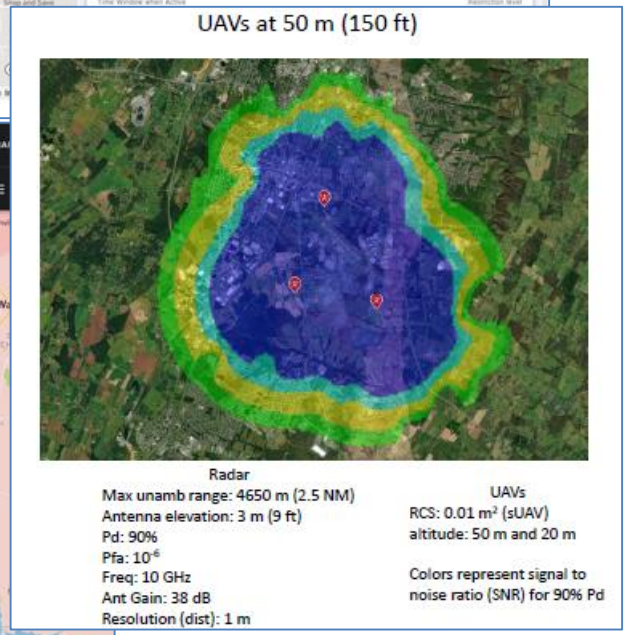
VIPC | VIRGINIA INNOVATION PARTNERSHIP CORPORATION
Connecting Innovators with Opportunity

AAM/Airspace Awareness





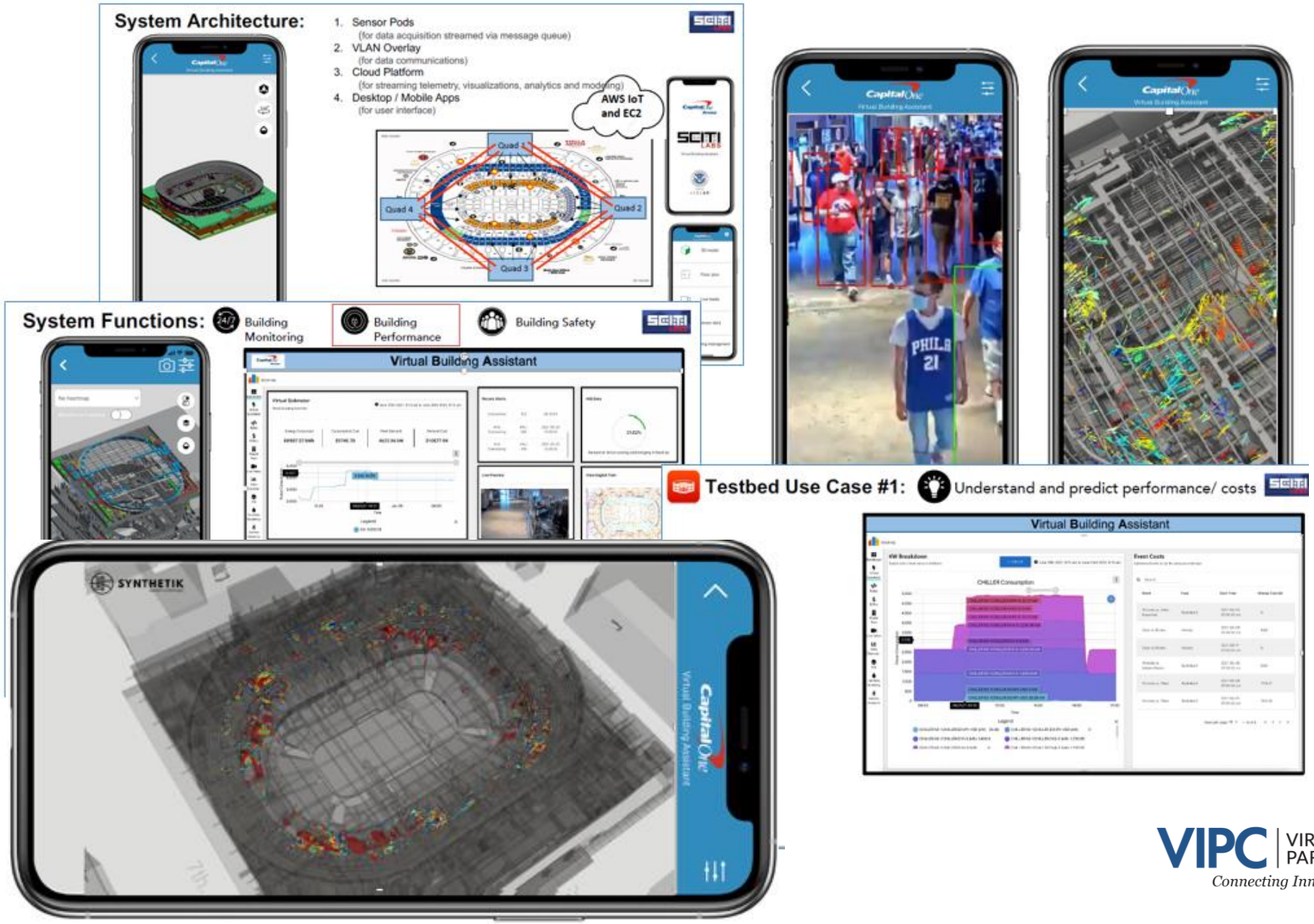




VIPC | VIRGINIA INNOVATION PARTNERSHIP CORPORATION

Connecting Innovators with Opportunity

Smart Facilities for Building Management and Public Safety

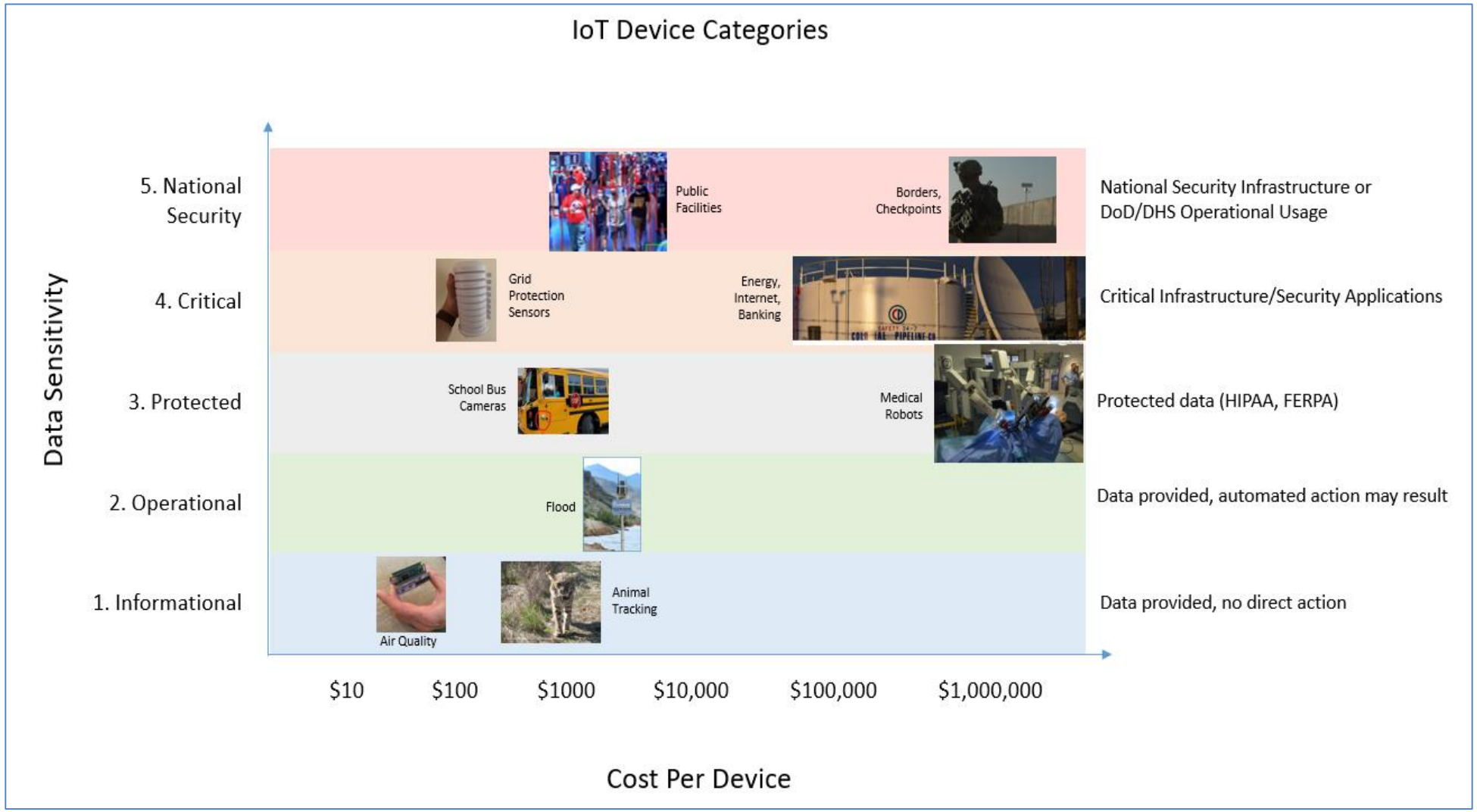


Topics

- VIPC?
- So what have you been up to lately?
- Cybersecurity Implications
- Facing the Challenges

VIPC | VIRGINIA INNOVATION PARTNERSHIP CORPORATION
Connecting Innovators with Opportunity

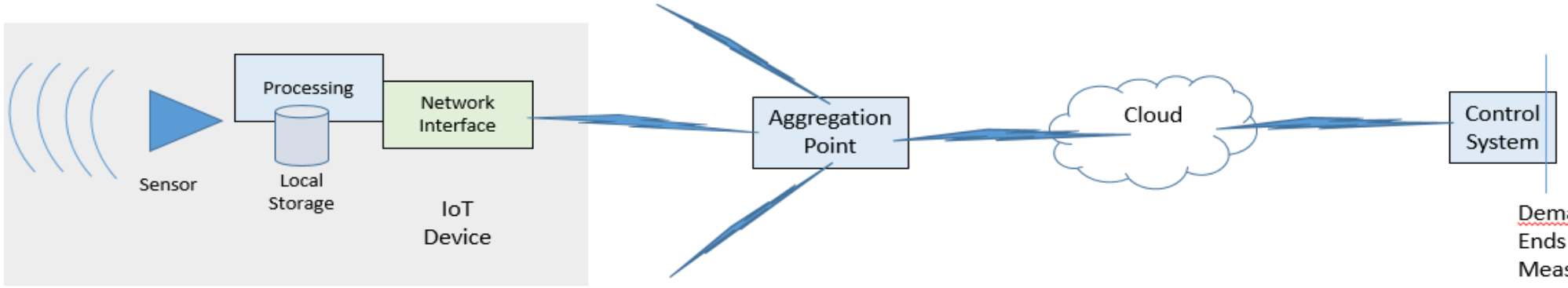
IoT / ICS Security at the Edge Challenge – Fit For Purpose Security



VIPC | VIRGINIA INNOVATION PARTNERSHIP CORPORATION
Connecting Innovators with Opportunity

Functional Block Diagram

IoT Block Diagram and Threats
(Not all elements present in all systems)

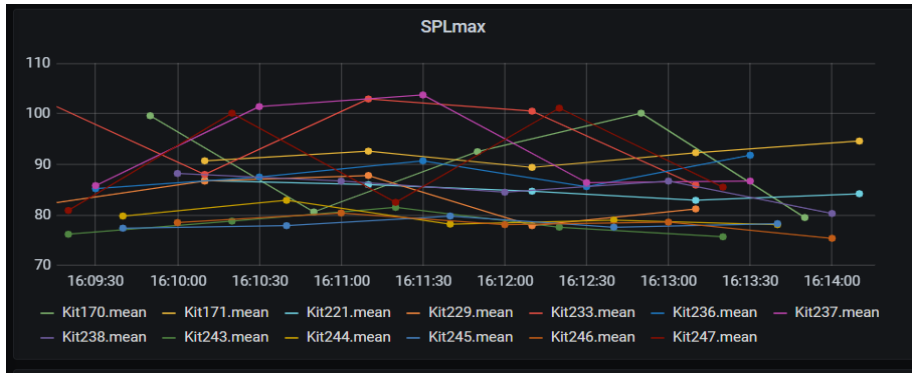


Point of Attack	Threat	Potential Solution	Applicable Device Category
Device	Data Skimming (Theft)	Device Storage Encrypted	3+
	Repurposed Infrastructure	Behavioral Controls on Data Flow	1+
	Bogus Commands	Data Diode	2+
	Corrupted Data	Operational Checks	1+
In Transit	Device Spoofing	Device Validation	2+
	Data skimming (Theft)	End-to-End Encryption	2+
System	Physical Access	Zero Trust	2+
	Data Leakage (Inappropriate Sharing)	Event-driven sharing	2+

- Assumes other security procedural controls in place (ie, personnel controls, training, response plans)
- Categories per prior diagram of data sensitivity

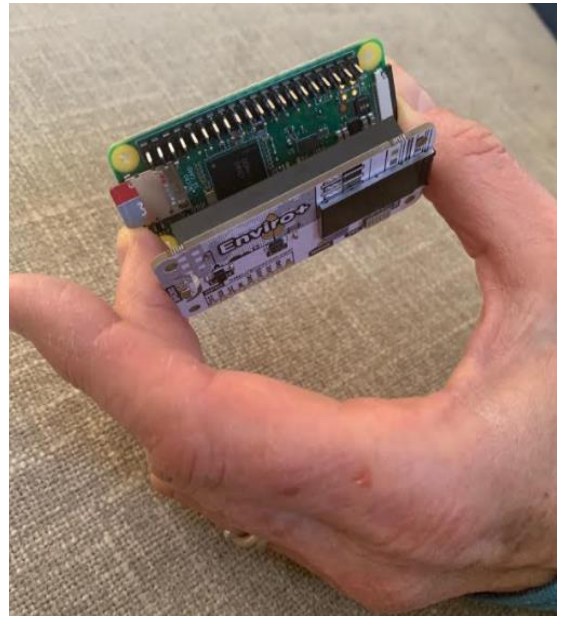
IoT/IIoT/ICS Security is *Different*

(-) Large numbers of devices
(-) Limited/no physical security
(-) Increasingly driving critical operations
(-) Public comms networks for data



(+/-) Autonomous operation
(+/-) Quantum computing

(+) Limited range of acceptable behaviors (for now)
(+) Network effect for self-healing
(+) Power at the edge
(+) No humans in the loop



Secure the Data

VIPC | VIRGINIA INNOVATION PARTNERSHIP CORPORATION
Connecting Innovators with Opportunity

Topics

- VIPC?
- So what have you been up to lately?
- Cybersecurity Implications
- Facing the Challenges

VIPC | VIRGINIA INNOVATION PARTNERSHIP CORPORATION
Connecting Innovators with Opportunity

Landscape Assessment Report

IoT Cybersecurity
LANDSCAPE AND STANDARDS ASSESSMENT

Table of Contents

Table of Figures

VIPC | VIRGINIA INNOVATION PARTNERSHIP CORPORATION
Connecting Innovators with Opportunity

Landscape Assessment Report

- Poor antenna design, implementation, and/or placement of transmitters and receivers

Intentional Radio Frequency Attacks

Intentional interference or jamming is performed by an entity with a deliberate intent to disrupt, disconnect, or degrade communications. Malicious jamming and nuisance jamming are the two types of intentional interference. Individuals with willful and criminal intent conduct malicious jamming, and such nefarious intent may be to prevent friendly organizations or systems from operating as required, conceal an ongoing criminal activity, or other possible motivations.

There are generally two types of intentional radio frequency attacks: transmission spoofing, where malicious nodes masquerade as authentic transmitters via high power RF transmissions that overpower legitimate transmissions and node cloning, where malicious nodes masquerade as authentic network members using cloned/manipulated RF characteristics.

Figure 3 - Various Types of Radio Frequency Jammers[1]

Bad actors target Wi-Fi networks using usually by directly affecting 802.11x Wi-Fi___33 devices (2.4MHz - 5GHz) to increase aggregate bit error rate or overpower individual devices' ability to transmit or receive. Common Wi-Fi___33 attacks include:

- De-authentication/DoS attacks: Force Wi-Fi___33 clients to disconnect from an authorized access point and attempt to reestablish the connection handshake, so an adversary can collect the resulting information or credential exchange.
- Rogue access points: Wireless access points that broadcast at a much higher decibel level, effectively overpowering and making invisible authorized access points and forcing Wi-Fi___33 clients to connect to the rogue access point.
- Access point impersonation Wireless access points that masquerade as authorized or otherwise innocuous access points to entice users to connect, so credentials or other protected information can be stolen, or sessions hijacked.
- MAC spoofing: Impersonating valid hardware identification to gain access to a secure network that uses a whitelist filter to only allow authorized clients to connect.
- WEP/WPA-PSK cracking: Collecting enough information over time to reconstruct network passwords.

[1] CISA SAFECOM NCSWIC. (2020). Radio frequency interference best practice guidebook. Cybersecurity and Infrastructure Security Agency (CISA) SAFECOM/National Council of Statewide Interoperability Coordinators. https://www.cisa.gov/sites/default/files/publications/safecom-ncswic_rf_interference_best_practices_guidebook_2.7.20_-_final_508c.pdf

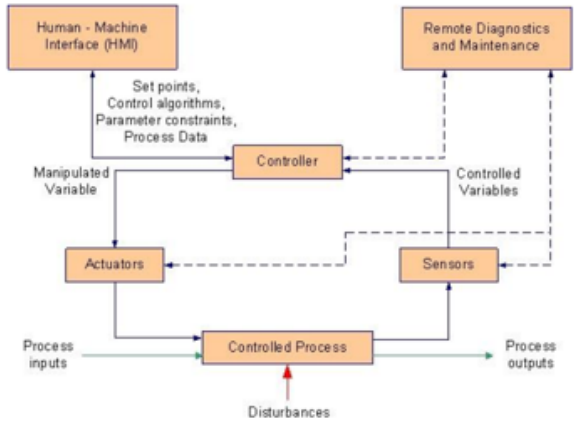


Figure 5 - ICS Operations[3]

Protecting Information and System Integrity in Industrial Control System Environments - NIST SP 1800-10

Intent/Approach and Main Concepts

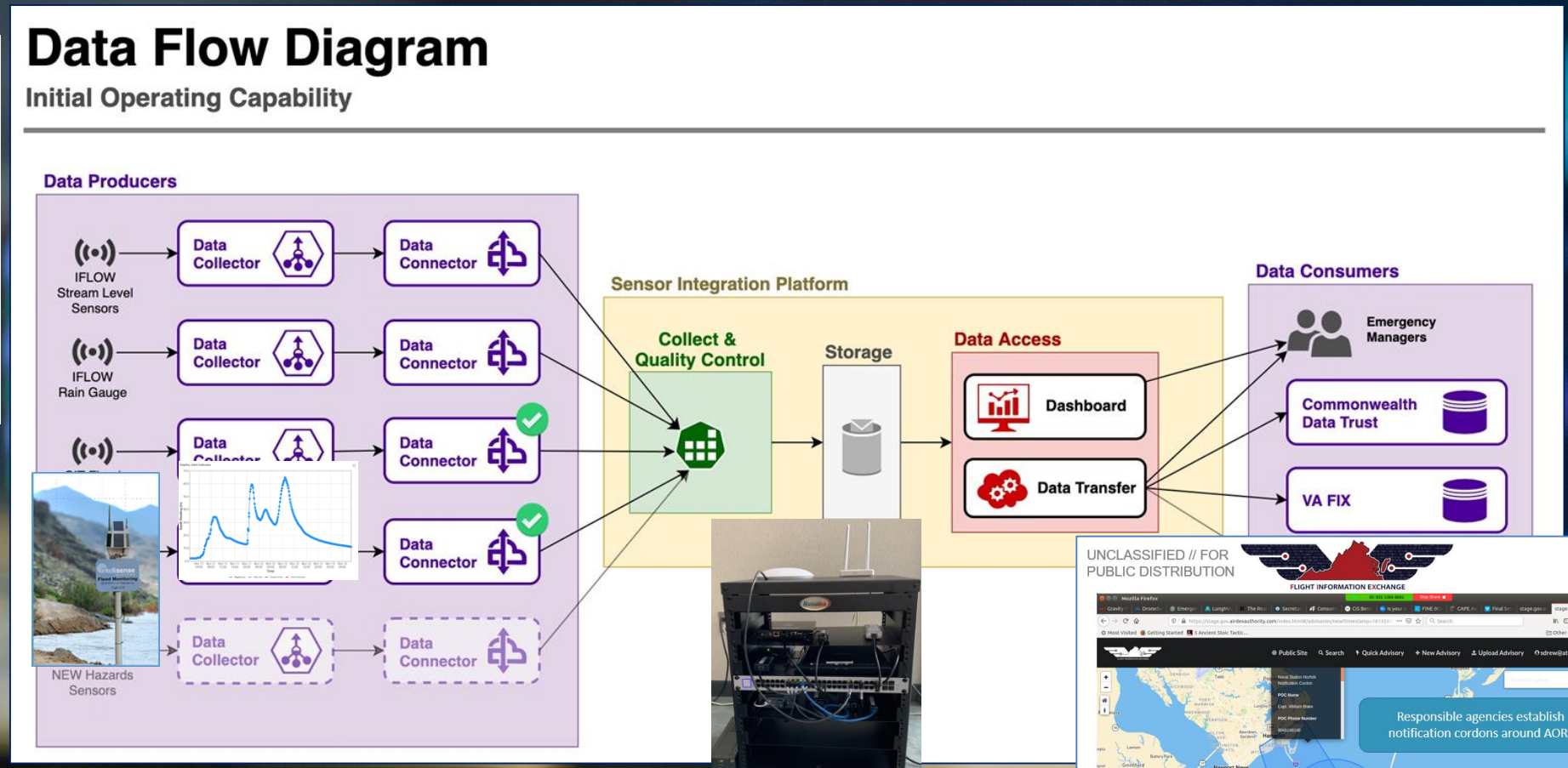
The goal of this NIST Cybersecurity Practice Guide is to help organizations protect the integrity of systems and information by securing historical system data, preventing execution or installation of unapproved software, detecting anomalous behavior on the network.

This publication is broken into three sections:

- **1800-10A** Executive Summary: Senior information technology (IT) executives, including chief information security and technology officers, will be interested in the Executive Summary, which describes the following topics: challenges that enterprises face in ICS environments in the manufacturing sector, example solution built at the National Cybersecurity Center of Excellent (NCCoE), benefits of adopting the example solution.
- Technology or security program managers might share the Executive Summary, NIST SP 1800-10A, with your leadership to help them understand the importance of adopting a standards-based solution. Doing so can strengthen their information and system integrity practices by leveraging capabilities that may already exist within their operating environment or by implementing new capabilities.
- **1800-10B** Approach, Architecture, and Security Characteristics: Technology or security program managers who are concerned with how to identify, understand, assess, and mitigate risk will be interested in this document, which describes what we did and why. The following

[3] NIST SP 800-82 R2, pg. 2-4, 2015

Controlled Data Sharing and Governance



- Real-time IoT Data streams shared via Data Trust permissions and governance
- VA-FIX now registered user, VIPC as Data Trust Member can upload streams or provide metadata for access

Zero Trust

Zero Trust concepts include:

- least privilege
- identity verification
- role-based authorization
- software attestation
- policy-based data protection

Zero Trust Will Yield Zero Results Without A Risk Analysis

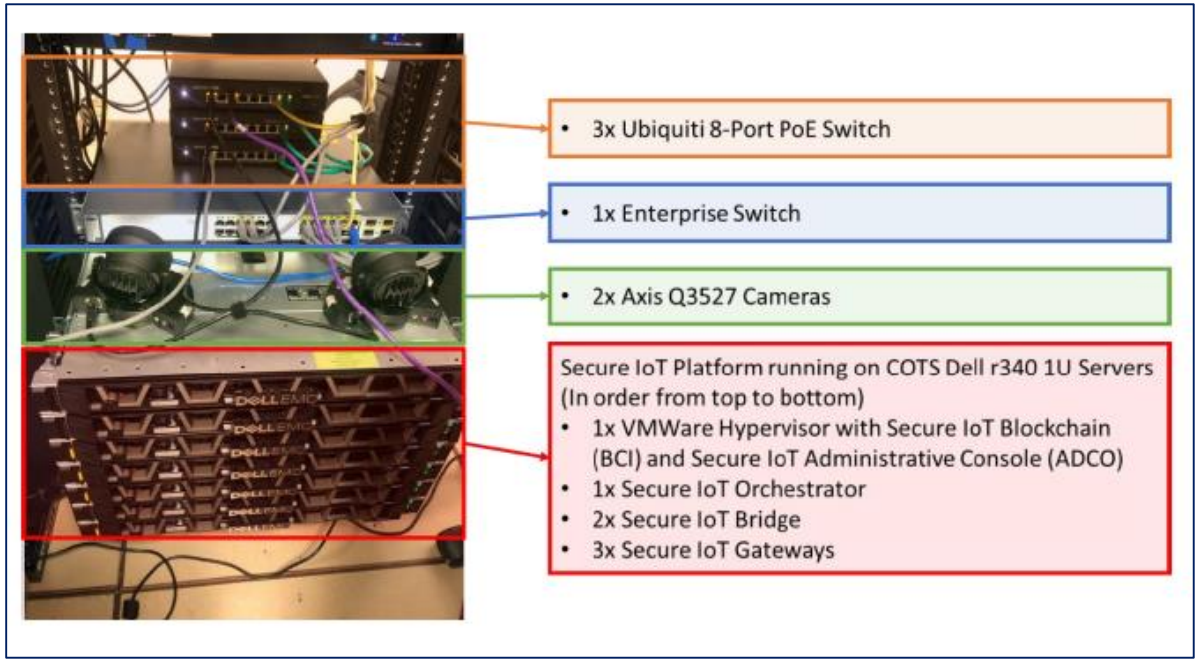
Over the past four years there has been an avalanche of new Zero Trust products. However during the same period there has been no measurable reduction in cyber breaches. To the contrary, ransomware, data exfiltration and lateral moving malware attacks seem to be increasing. If the emergence of Zero Trust was supposed to make us safer, it hasn't happened.

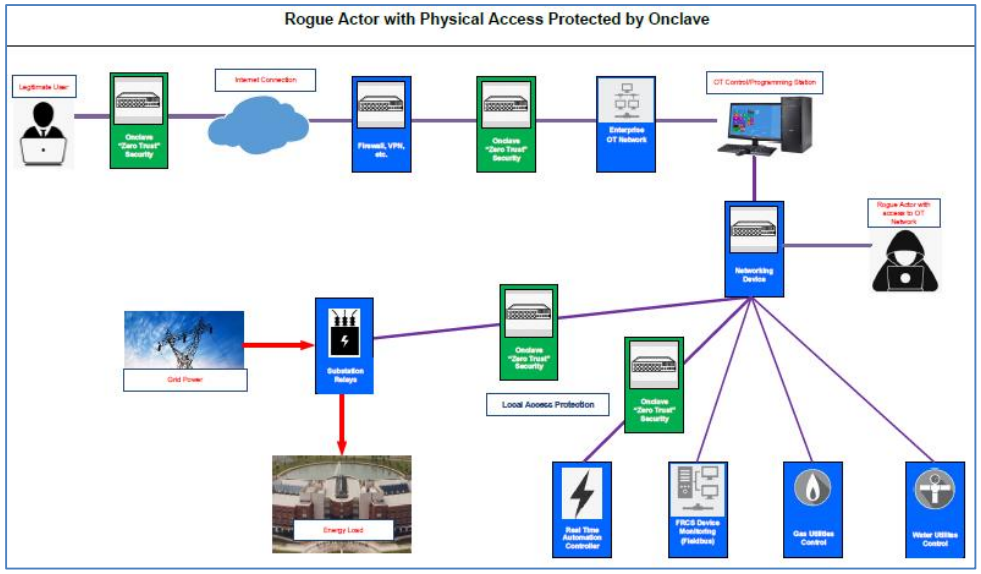
[Deep Edge - Zero Trust Will Yield Zero Results Without A Risk Analysis]

VIPC | VIRGINIA INNOVATION PARTNERSHIP CORPORATION
Connecting Innovators with Opportunity

IoT Critical Infrastructure Security

- "Zero Trust Security"
- Makes groups of IoT devices invisible to hackers
- Widespread adoption growing across many applications
- Critical infrastructure demo at Ft. Belvoir for power infrastructure





VIPC | VIRGINIA INNOVATION PARTNERSHIP CORPORATION
Connecting Innovators with Opportunity

Device Life Cycle Management

Provisioning the Network, Automatically

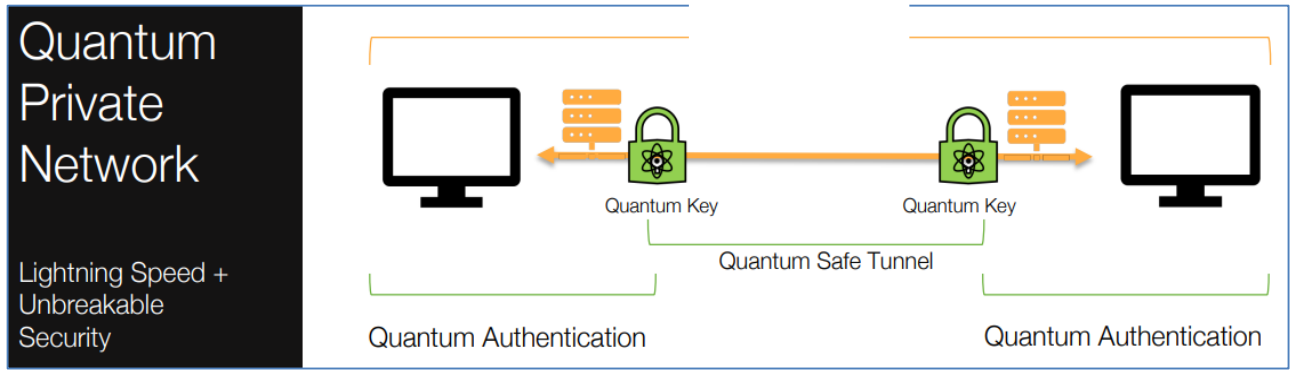
- Automated creation of strong machine identities at IoT scale, managed throughout the device life cycle

- Automated device provisioning, authentication, credential management, policy-based end-to-end data security, secure updated, anomalous behavior detection, automated de-provisioning/re-provisioning

VIPC | VIRGINIA INNOVATION PARTNERSHIP CORPORATION
Connecting Innovators with Opportunity

Quantum Computing

Threat and Opportunity

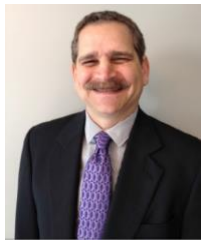


- May solve currently intractable computing problems
- Biggest advantage over traditional computing in “high-dimensionality” problems…those with lots of variables that need to be optimized at once, or…
- Public Key Encryption, making many current security architectures obsolete
- NIST has published approved list of 8….oops, 7…. Quantum-resistant encryption algorithms, such as AES 256
- We are working to validate key algorithms on intermediate computing platforms such as photonics as true quantum platforms evolve

IoT and Related Challenges For Cybersecurity

Questions?

David Ihrie, CTO/CIO
David.Ihrie@VirginiaIPC.Org



Funding for many of the technologies incorporated into the Virginia Smart Community Testbed has been provided by the U.S. Department of Homeland Security, Science & Technology Directorate, under contract number 70RSAT19CB0000025

VIPC | VIRGINIA INNOVATION PARTNERSHIP CORPORATION
Connecting Innovators with Opportunity

A Dynamic Process for Minimizing the Likelihood and Impact of Cyber Attacks

Chris Jensen

Public Sector Business Development

Agenda

Who is Tenable?

Start with Visibility

Risk-Based Vulnerability Management

Web Application Scanning

Securing Identity Systems

Steps to Reduce Cyber Risk

Who is Tenable?

Creator of the Nessus vulnerability scanner, Tenable is the first and only provider of Cyber Exposure solutions. We work with more than 40,000 organizations around the world to help them manage and measure cybersecurity risk in the digital era. We are building on our deep technology expertise as a pioneer in the vulnerability assessment and management market, providing broad visibility across the modern attack surface and deep insights to help security teams, as well as business and government executives, prioritize and measure Cyber Exposure.

Why Tenable?

TRUSTED BY OVER 40,000 ORGANIZATIONS WORLDWIDE

SEE
EVERYTHING

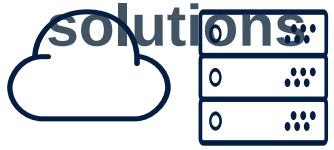
PREDICT
WHAT MATTERS

ACT
TO REDUCE RISK

VISIBILITY INTO YOUR ENTIRE ATTACK SURFACE

#1 in coverage, accuracy and zero day research

On-prem & cloud solutions*



#1 in VM Market Share*

100+ Integrations with leading industry partners

tenable

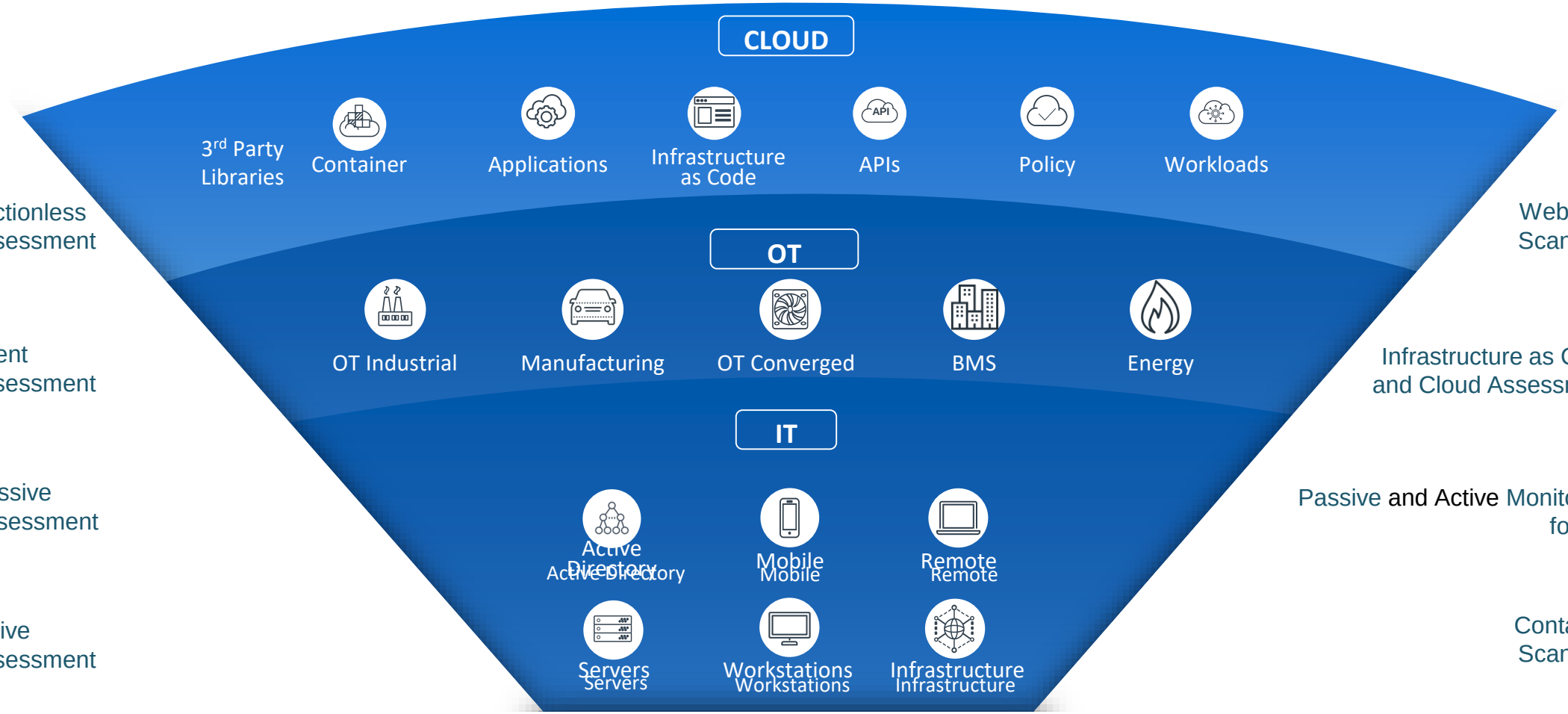
Start with Visibility

“You can’t protect what you can’t see”

tenable

THE MODERN ATTACK SURFACE

Adaptive approaches to assess assets across the modern attack surface



Frictionless Assessment

Agent Assessment

Passive Assessment

Active Assessment

Web App Scanning

Infrastructure as Code and Cloud Assessment

Passive and Active Monitoring for OT

Container Scanning

tenable

What is Risk-Based Vulnerability Management?

Attackers don’t choose from hundreds of thousands of vulnerabilities they could leverage, they choose a few they know will always work. These flaws are known and generally a fix is available but the sheer number of issues discovered and the complex environments operations teams are tasked with remediating means that it could take weeks or months to fix what matters most.

CVSS is NOT an Assessment of Risk

"CVSS is designed to identify the technical severity of a vulnerability. What people seem to want to know, instead, is the risk a vulnerability or flaw poses to them, or ***how quickly they should respond to a vulnerability***."

TOWARDS IMPROVING CVSS
SOFTWARE ENGINEERING INSTITUTE | CARNEGIE MELLON UNIVERSITY
December 2018

tenable

Risk-Based Vulnerability Management

A process that employs machine learning analytics
to automatically correlate:

- Assessments of traditional and modern assets across the entire attack surface
- Vulnerability severity
- Threat and exploit intelligence
- Asset criticality

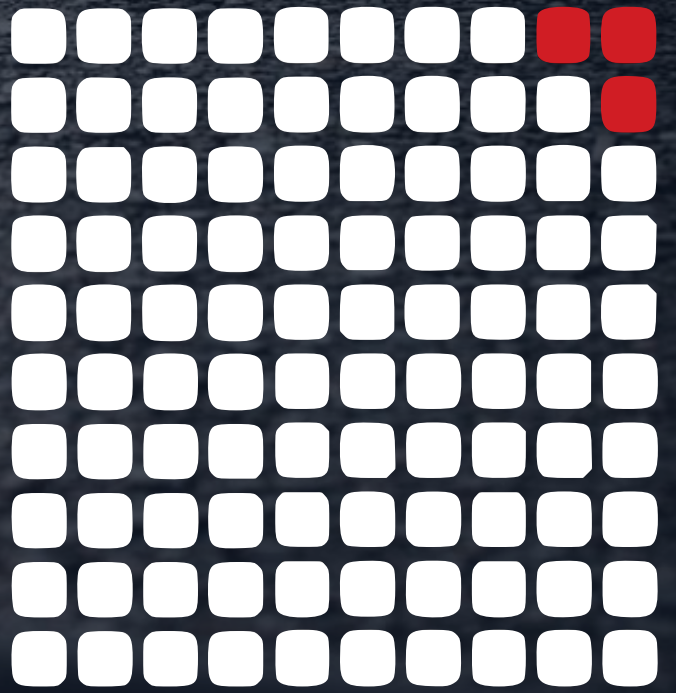
… to identify which vulnerabilities pose the greatest risk.

tenable

YOU'VE GOT **99 FLAWS** BUT ALL THEY NEED IS **ONE**

<3%

OF VULNERABILITIES
HAVE A HIGH PROBABILITY
OF BEING **LEVERAGED IN ATTACKS**



tenable

18K VULNERABILITIES DISCLOSED IN 2020

NEARLY **3X MORE** THAN 2016

CVSS 7+

- **WASTES 76%** OF THE SECURITY TEAM'S TIME
- **LEAVES 44%** OF RISKY VULNERABILITIES IN YOUR ENVIRONMENT

REMEDIATION POLICY

OF ALL VULNERABILITIES HAVE A **CVSS BASE SCORE OF 7 OR ABOVE**

20%

VULNERABILITIES HAVE AN **EXPLOIT AVAILABLE**

tenable

Conti Ransomware as a Service - Vulnerabilities Utilized

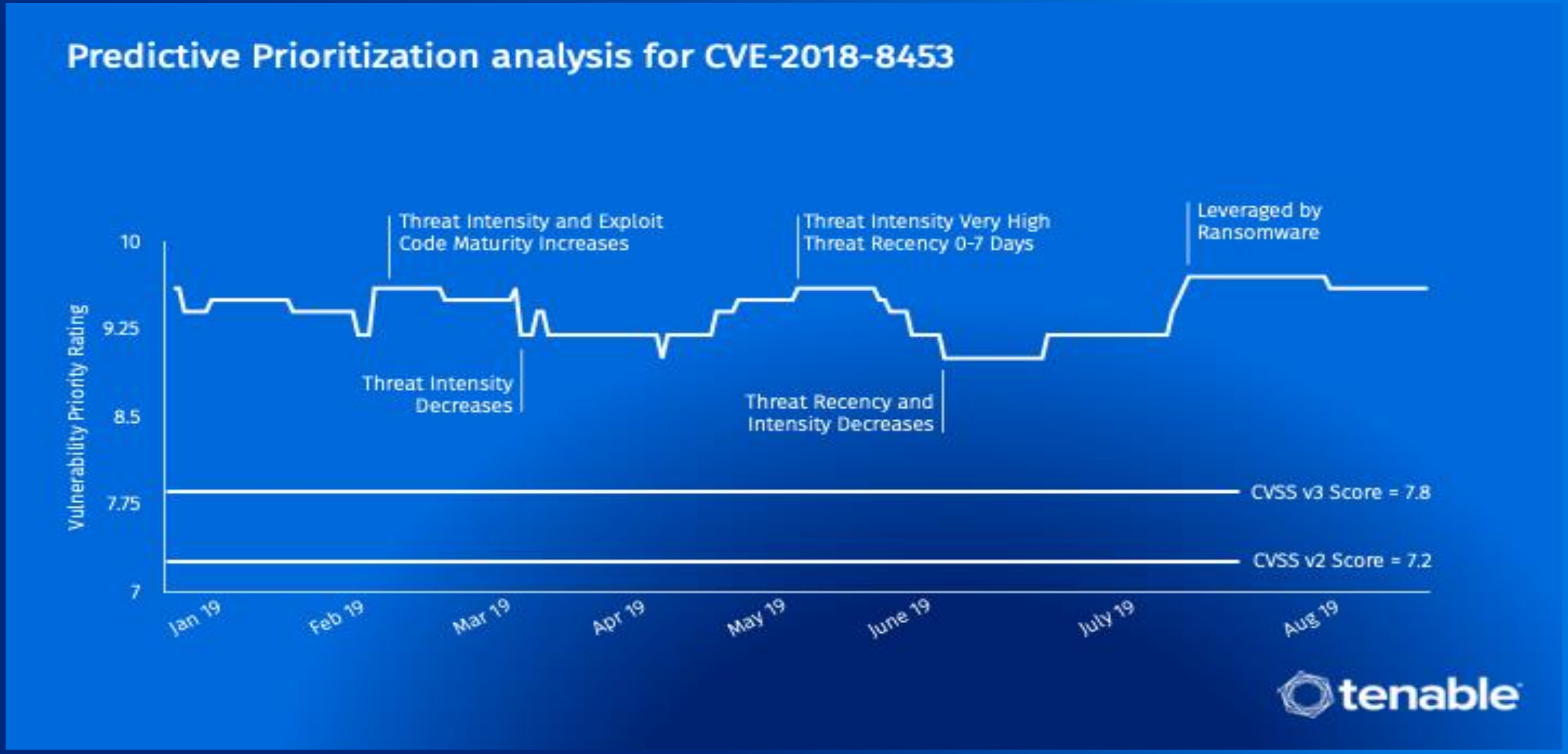
- 6 out of 7 - VPR ‘Critical’
- 1 - CVSS Critical

2017 Microsoft Windows SMB 1.0 server vulnerabilities		
	CVSSv3 Score	**VPR Score**
CVE-2017-0143	8.1	**9.8**
CVE- 2017-0144	8.3	**9.8**
CVE- 2017-0145	8.1	**9.2**
CVE- 2017-0146	8.1	**9.2**
CVE- 2017-0147	5.9	**7.4**
2021 Microsoft Windows Print Spooler (“PrintNightmare”)		
	CVSSv3 Score	**VPR Score**
CVE-2021-34527	8.8	**10.0**
2020 Microsoft Active Directory DC (“Zerologon”)		
	CVSSv3 Score	**VPR Score**
CVE-2020-1472	10.0	**10.0**

[CISA Advisory - Conti Ransomware, Sept 22, 2021]

tenable

Elevation of privilege vulnerability in Windows
Used in 2019 ransomware attacks



What A Modern VM Program Looks Like

Lower Effort, Higher ROI

More efficient use of security resources

Increased ROI and cost control by discovering common issues in minutes

Unified Visibility

A holistic view of your attack surface - including IT and cloud assets with web app components

Prioritize remediation for critical assets

Comprehensive Coverage

Detect both known and unknown vulnerabilities

Identify the greatest number of vulnerabilities with fewer false positives

tenable


Reactive
Proactive

Web Application Scanning

Dynamic Application Security Testing (DAST): A DAST crawls a running web application through the front end to create a site map with all of the pages, links and forms for testing. Once the DAST creates a site map, it interrogates the site through the front end to identify any vulnerabilities in the application custom code or known vulnerabilities in the third-party components that comprise the bulk of the application. **Only a DAST tool can identify runtime flaws, which are not apparent in a static environment.**

Static Application Security Testing (SAST): A SAST analyzes static environments, i.e., meaning the source code of an application. Used for periodic assessment, It looks at the application and searches for vulnerabilities in the code.

DAST vs. SAST – Use the Right Tool for the Job

tenable

SECURE THE IDENTITY SYSTEMS THEMSELVES

"…Directory Services is the underlying infrastructure that supports authentication and authorization. Its compromise would de facto render any zero trust implementation ineffective."

- ***NSTAC Report to the President on Communications Resiliency, 2022***

But can you trust your identity system?

tenable

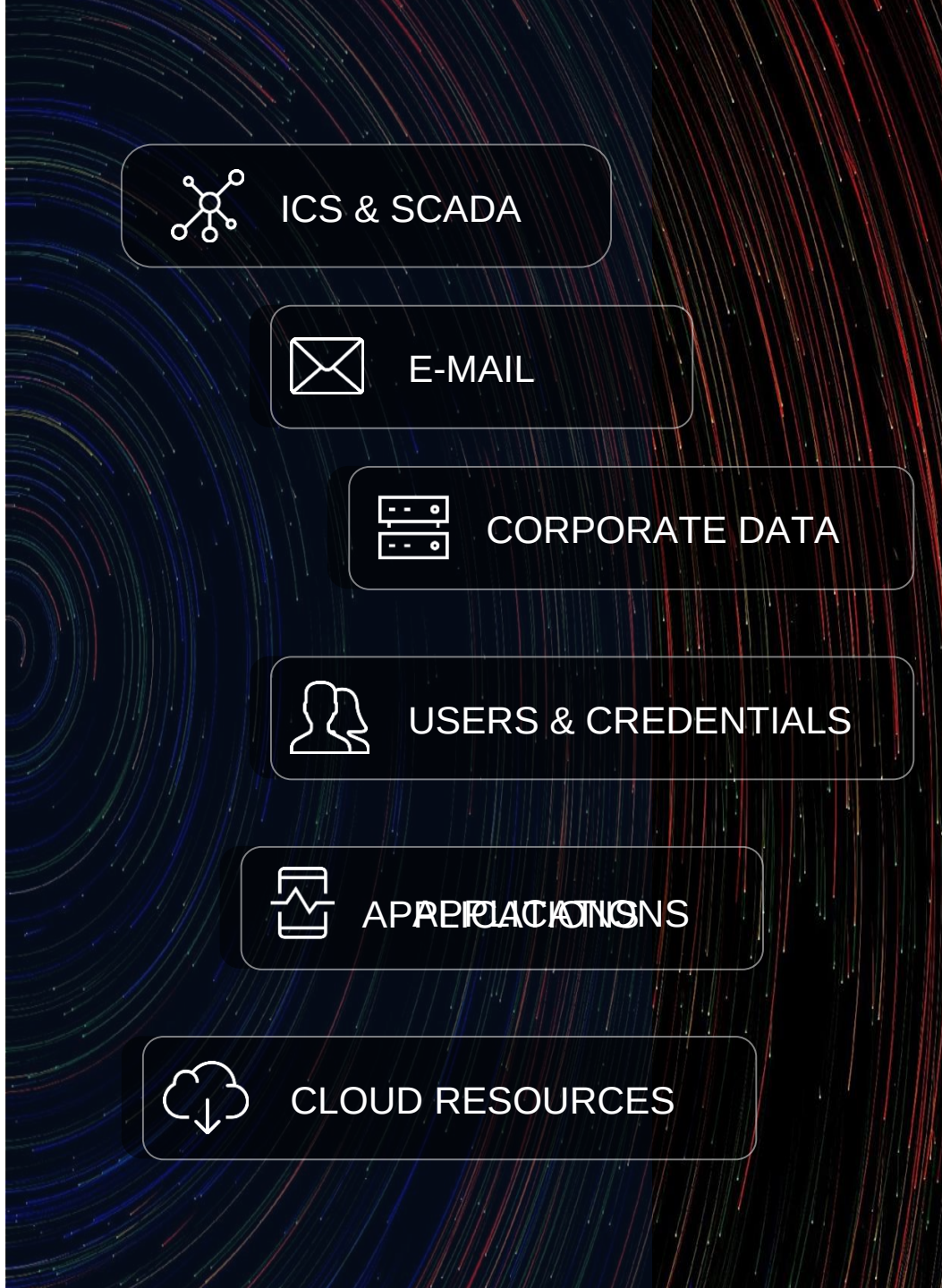
Secure the Trust Provider

Active Directory holds the **keys to everything**

- Governs authentication, holds all passwords
- Manages access rights to every vital asset
- Ensures the user is known and managed at all times

"... trusted identity management solutions are unquestionably foundational, as zero trust is based on a continuous cycle of credentialing, verifying, and authorizing identity for person and non-person entities."

-NSTAC Report to the President on Communications Resiliency, 2022



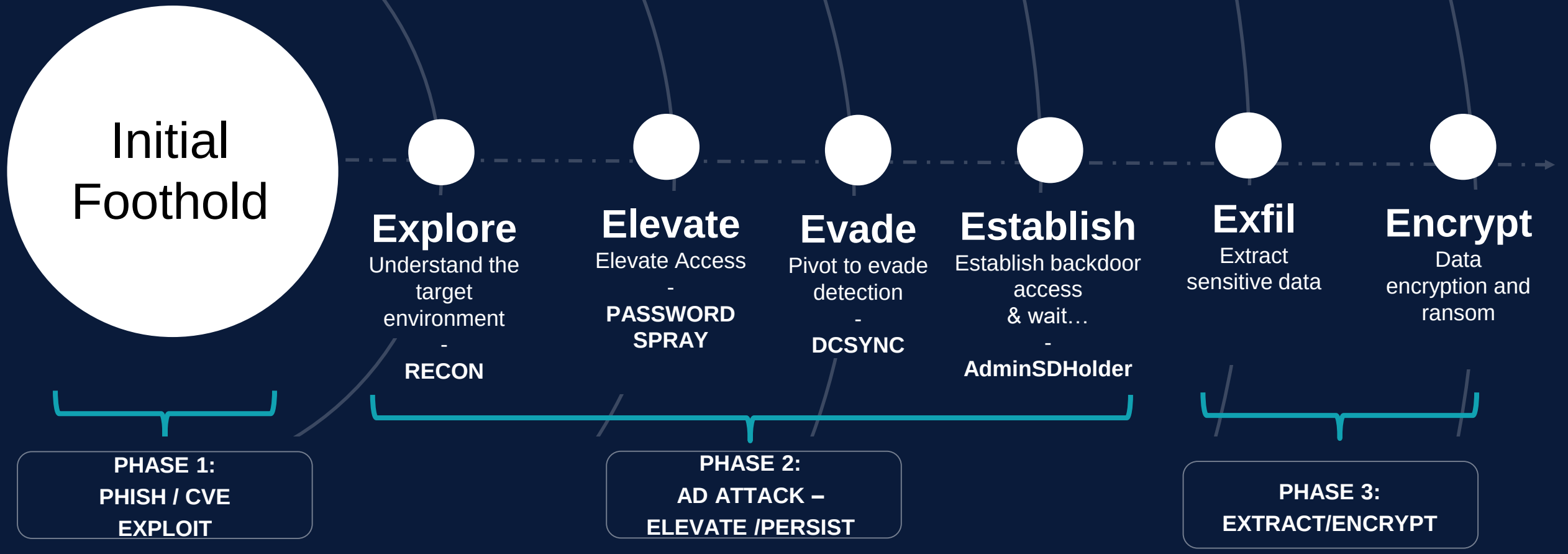
Recent Department of Commerce IG Report Recommendations to NOAA included:

1. Establish processes and procedures to **periodically review** all active directory accounts to ensure consistent adherence to the principle of least privilege per Department policy.

2. Determine the feasibility of requiring all NOAA line offices to use specialized active directory security tool(s) to conduct **periodic reviews.**

3. Establish procedures to **periodically review** active directories and ensure compliance with account management requirements as stated in the Department's policy and following industry best practices.

Understanding Common Attack Paths



Identity Access Management

Indicators of Exposure

1) FIND AND FIX EXISTING WEAKNESSES

>_ Immediately discover, map, and score existing weaknesses

>_ Follow step-by-step remediation tactics and prevent attacks

2) MAINTAIN HARDENED SECURITY SETTINGS

>_ Instantly detect new weaknesses and misconfigurations

>_ Break attack pathways and keep your threat exposure in check

Indicators of Attack

3) DETECT ATTACKS IN REAL-TIME

>_ Get real-time alerts and actionable remediation plans on AD attacks

>_ Visualize notifications and trigger responses in your SIEM / SOAR / SOC

4) ENHANCE INCIDENT RESPONSE & THREAT INVESTIGATIONS

>_ Trigger response playbooks in your SOAR

>_ Search and correlate AD changes at object and attribute levels

5) Disrupt Attack Pathways

- No Agents
- No Elevated Privs
- AD Native
- Near Real Time

Steps to Reduce Cyber Risk

1. **Start with visibility**
2. **Take a risk-based approach**
3. **Use a dynamic tool for a dynamic environment**
4. **Continuously monitor**

Thank You!

tenable

UPCOMING EVENTS

IS ORIENTATION

IS Orientation

Remote - WebEx

Sept. 29, 2022

Start time: 1:00 p.m.

End time: 3:00 p.m.

Instructor: Marlon Cole

https://covaconf.webex.com/covaconf/onstage/g.php?MTID=ecbe083f9321db08a0c81eca667f50575

The next scheduled meeting for the IS Council:

Sept. 21, 2022

Noon – 1p.m. (virtual)

If you would like an invite to the meeting contact:

tina.gaines@vita.virginia.gov

The next scheduled meeting for the ISOAG is:

Oct. 5, 2022

This is the annual mandatory meeting. All primary agency ISOs should attend. If you can't attend yourself, please be sure to delegate attendance to someone else in your agency. Please let us know if you can't attend and who will attend in your place.

Sept. 26th will start the statewide phishing campaign for the third quarter.

Please contact commonwealthsecurity@vita.Virginia.gov for more information.

ISO REMINDERS

Everyone needs to take steps to retain your ISO Certification for CY 2022. Please contact Tina Gaines (tina.gaines@vita.Virginia.gov to see what requirements you need to complete your certification.

Also, please complete your Security Awareness Training Solution Form by 9/30/2022. You may complete the form in Archer or by completing the form and emailing it Commonwealthsecurity@vita.Virginia.gov

OCTOBER IS CYBERSECURITY AWARENESS MONTH

VIRGINIA
IT AGENCY

MEETING ADJOURNED