



Virginia Information Technologies Agency

Welcome and Opening Remarks

Michael Watson

Commonwealth Information Security Officer

March 6, 2019



ISOAG March 6 , 2019 agenda

I. Welcome and Opening Remarks

Mike Watson, VITA

II. VP Business Development, Government and Critical Infrastructure

**Rick Tiene and Dave Jordan,
Mission Secure, Inc**

III. Security Governance Discussion

Barry Davis, DSS

IV. Exceptions in Depth

John Craft, VITA

V. Upcoming Events

Mike Watson, VITA



Cybersecurity for Operational Technology & Control Systems

VITA - Information Security Officers Advisory Group
March 6, 2019

The rise of Industry 4.0

The Industrial Internet of Things (IIoT) is ever-evolving. But with unprecedented connectedness comes new and unpredictable vulnerability.

To meet these risks head-on, we need a cybersecurity solution that delivers real visibility across the digital and physical components of the most influential global companies.

89%

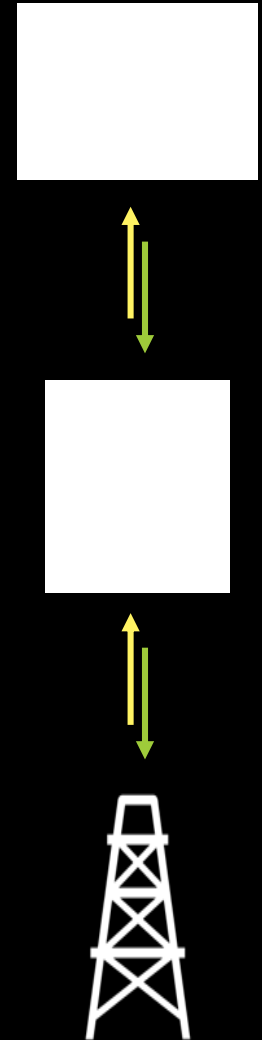
of industrial companies have experienced a cybersecurity breach in their control systems.

Source: Forrester Consulting on behalf of Fortinet, January 2018

IIoT digital automation risks

IIoT and automation have increased our attack surfaces and expanded vulnerabilities. So when it comes to cases like big oil and big data, we need bigger cybersecurity.

- Bringing down one site can bring down every site on the same network
- Access to real-time information could compromise assets, increasing the likelihood of stolen production data
- Next-generation control capabilities need stronger cybersecurity
- We need computing power at the edge (power/bandwidth constraints)
- Compromised data = garbage in/out = incorrect learning/AI
- Third-party access can be compromising and serve as conduits
- IT and OT have a critical need to collaborate





Mission Secure, Inc. provides a plug-and-play hardware-software solution that protects the world's most critical industrial assets against cyber attacks and disruptions. From Level 0 field devices to controllers and HMIs, components are monitored from a single, easy-to-use platform.

We deliver visibility and protection in three ways...



Assess

We monitor and assess control systems to identify the greatest cyber risks.

Design

We design comprehensive roadmaps to mitigate risks.

Deploy

We fully integrate the MSI Platform as a scalable and cost-effective cyber protection solution.

Initially focused on these three industries.



Energy



Defense



Smart Cities

MSi at a glance

Who we are

We are control system and cybersecurity experts focused on industrial cyber defense, based in Charlottesville, VA and Houston, TX

What we do

Protect control systems and their key physical assets

Our history

- R&D began 2010 at University of Virginia with U.S. Dept. of Defense
- Original research team founded MSi in 2014 and commercialized the product platform
- Expertise was further developed in offensive and defensive cybersecurity, and commercial, military, oil and gas, and complex industrial control systems
- Venture-backing was secured by Chevron Technology Ventures, Energy Innovation Capital, Blue Bear Capital and Macquarie Capital
- 2019 National Cyber Security Centre Cyber Accelerator, powered by Wayra began

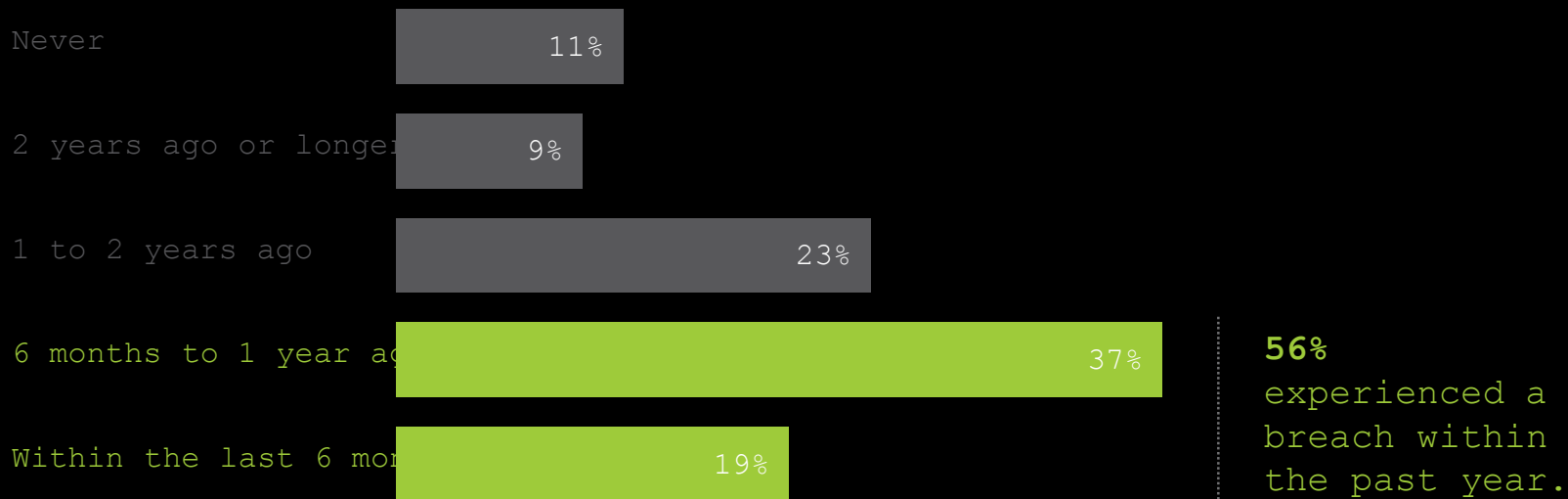


Systems are more
exposed
than most realize.

Chances are, you've been attacked

In the last year alone, 56% of organizations have experienced a security breach in their industrial control systems. The result? Physical damage, lost productivity, safety risks and even ransom. **And that number is only going up.**

When have you experienced a security breach?



Base: 429 global decision makers responsible for security of critical infrastructure. Source: Forrester Consulting on behalf of

Recent industry attacks



Cyberattacks Are 'Ticking Time Bombs' for Germany

Its pacifist tradition poses a dilemma for those charged with protecting the country from hackers.

The Cyberattack That Crippled Gas Pipelines Is Now Hitting Another Industry

Cyberattacks Put Russian Fingers on the Switch at Power Plants, U.S. Says

Cyberattack that crippled Ukrainian power grid was highly coordinated

Russian hackers infiltrated US power networks and had the ability to trigger massive blackouts

A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try.

Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say

Cyber Attack on German Steel Mill Leads to 'Massive' Real World Damage

A steel mill in Germany lost control of its blast furnace. Hackers had infiltrated the mill's control system, according to the German government's office for information security.

UK industrial control systems targeted, warns leaked NCSC document

The physical impact of cyber threats



Attackers aim to control HMI and Level 1 devices to take over the process.

Incidences

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

Attack Sequence

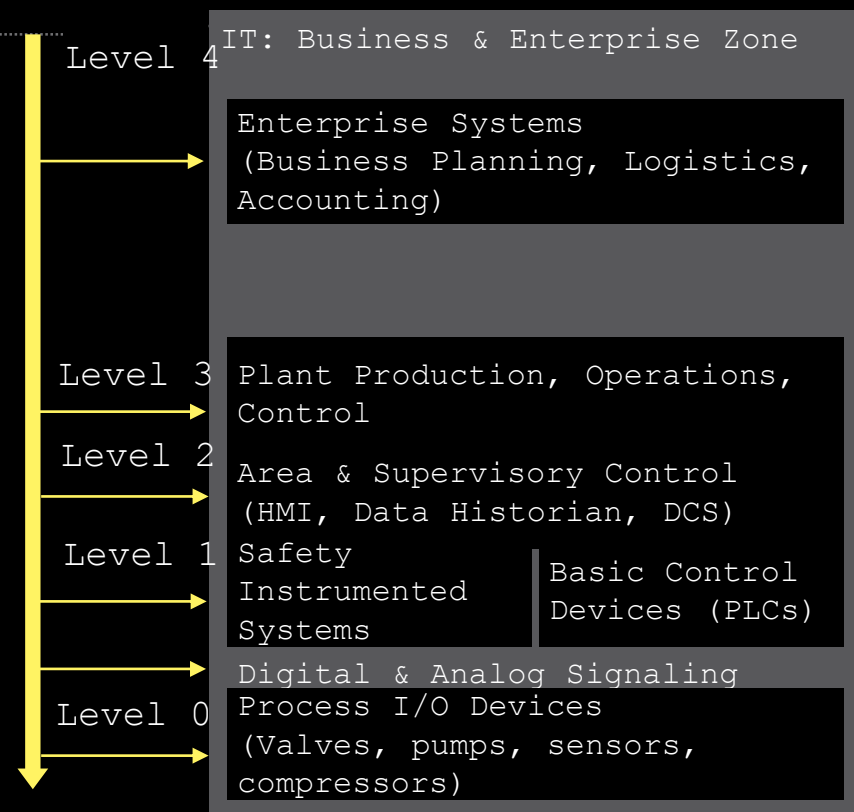
Identify one entry point
(e.g., spear phishing)

Mask the actual state of the attack
(physical system)

Take control of CS and safety response systems

Create impact

Purdue Control System Model



Impacts can be felt at all levels

HMI/ATMS/operator | LEVEL 2

- Loss of view
- False view
- Loss of control



Operator at the Human Machine Interface (HMI) / ATMS



Controller/PLC/ATC | LEVEL 1

- Instruct devices, change process, cause damage
- Send "normal" signals across network to HMI
- Steal sensitive data, report false data



Field device/process | LEVEL 0

- Remotely configurable sensor
- Get between sensor/ATC
- Sending false data to trick ATC



The goal is simple:
Prepare for and
protect
against cyberattacks.

Process to Secure the Operational Aspects of the Network



Assess

The OT system is significantly different than the IT one. Need to navigate this complex environment through a cost-effective assessment that uses live OT traffic analysis to detect previously unknown vulnerabilities and threat vectors.

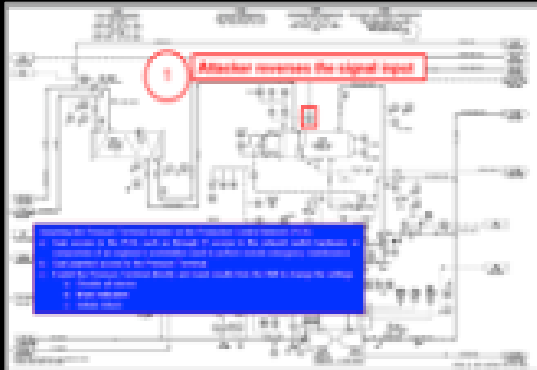
- Evaluate "as-is" architecture to identify security gaps
- Deep dive into P&IDs, network drawings, security settings
- Get optional hands-on red teaming
- Use NIST/DHS/IEC 62443 standards as basis for methodology
- Monitor developments with live, passive OT traffic analysis

Design

After a technology-based assessment, design a cybersecurity system that identifies immediate solutions, builds a "to-be" cyber architecture, and roadmaps an actionable plan.

- Strengthen existing protections
- Identify new mitigations
- Create scorecard and actionable, prioritized roadmap

Implementing best-in-class OT cybersecurity



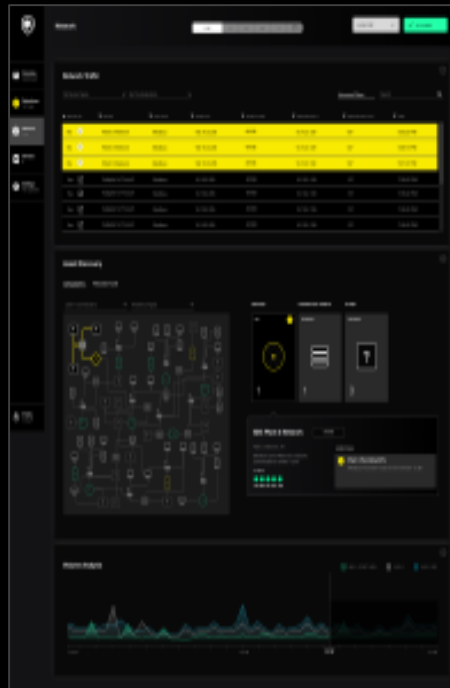
Current System Security Posture



Risk & Business Prioritization



Architecture & Solution Reco's



Real-Time OT Network Traffic Capture



Security Implementation Roadmap

The Platform Approach

To fully secure Operational Technology goes beyond just consulting and requires a platform that provides operational visibility and protection, down to Level 0 devices – starting with six points of action and awareness.



Protect

Restrict unauthorized access and block malware and ransomware from reaching important controllers and Level 1 devices.



Monitor

Continuously monitor network IP levels, alongside digital and analog signals with our secure, multi-layered system



Detect

Get real-time analysis and automated incident detection.



Inform

Keep trusted operators and cybersecurity professionals informed through dedicated communications systems.



Collect

Gather system data from digital and analog sensors and actuators, controllers, and OT network for forensic purposes.



Correct

Carry out automated or operator-guided responses, mission restorations, and system functions to safe operating states.

Note: The MSi Platform is a patented product of Mission Secure, Inc. covered by US Patent No. 9697355

How an True OT Cyber Protection Platform Works



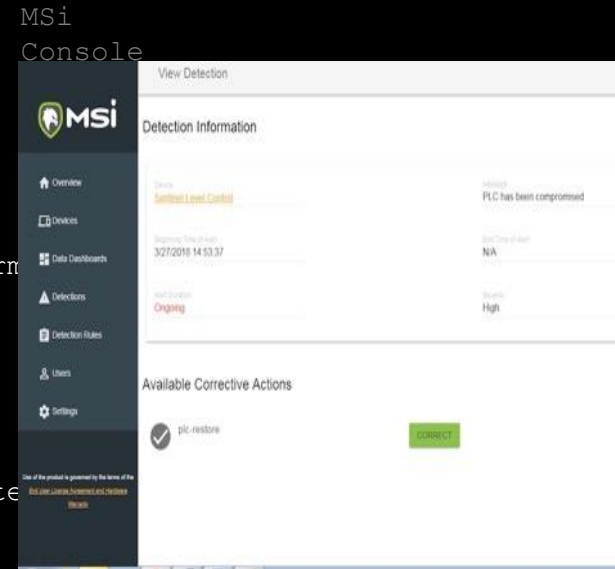
Visibility of OT network and Protection for key controllers

Software Console

- ✓ On premise or Platform-as-a-service
- ✓ Monitor network traffic, controller changes, OT visibility
- ✓ Centrally manage appliances, configuration, rules, software /firmware
- ✓ Notify MSi / IT manager / control engineer of attack or abnormal activity
- ✓ Remote trouble shooting for operational efficiencies
- ✓ Optional 24/7/365 monitoring

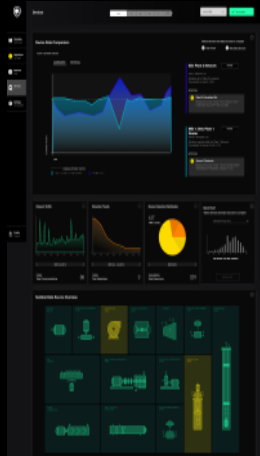
Install security appliances on site:

- ✓ Sit in front of key PLCs, safety system, flow controllers/meters
- ✓ Block unwanted activity (ingress and egress)
- ✓ Stop Malware or Ddos from attacking controllers
- ✓ Look for changes to controller settings
- ✓ Map normal traffic and monitor for abnormal behavior
- ✓ Understand true system state (i.e. pressure, valve open/closed)
- ✓ Encrypt traffic between controllers, engineer work stations
- ✓ Collect data for forensics around event
- ✓ Corrective action capabilities (human in the loop, or fully automated)
- ✓ Multiple protocols (Modbus, CIP, OPC, BacNet, Serial & Ethernet)



Real World Examples

Our Approach - The MSi Platform



MSi Console

For Central Management

As the main hub for the MSi platform, our console manages MSi device configurations, software, and firmware updates – while investigating incidents, troubleshooting issues, and setting automated corrective actions.



MSi IDS

For Visibility

Our MSi hardware passively monitors OT traffic through span ports or serial taps with no impact to operations. The MSi IDS collects OT network data – including IP addresses, commands, configuration and state information – and conducts deep packet inspection into OT protocols.



MSi 1

For Protection and Correction

Designed to protect endpoint devices, like programmable logic controllers (PLC) and safety instrumented systems (SIS), the MSi 1 provides Levels 1 and 2 security by blocking malicious traffic and stopping unwanted commands from reaching controllers.



MSi Sentinel

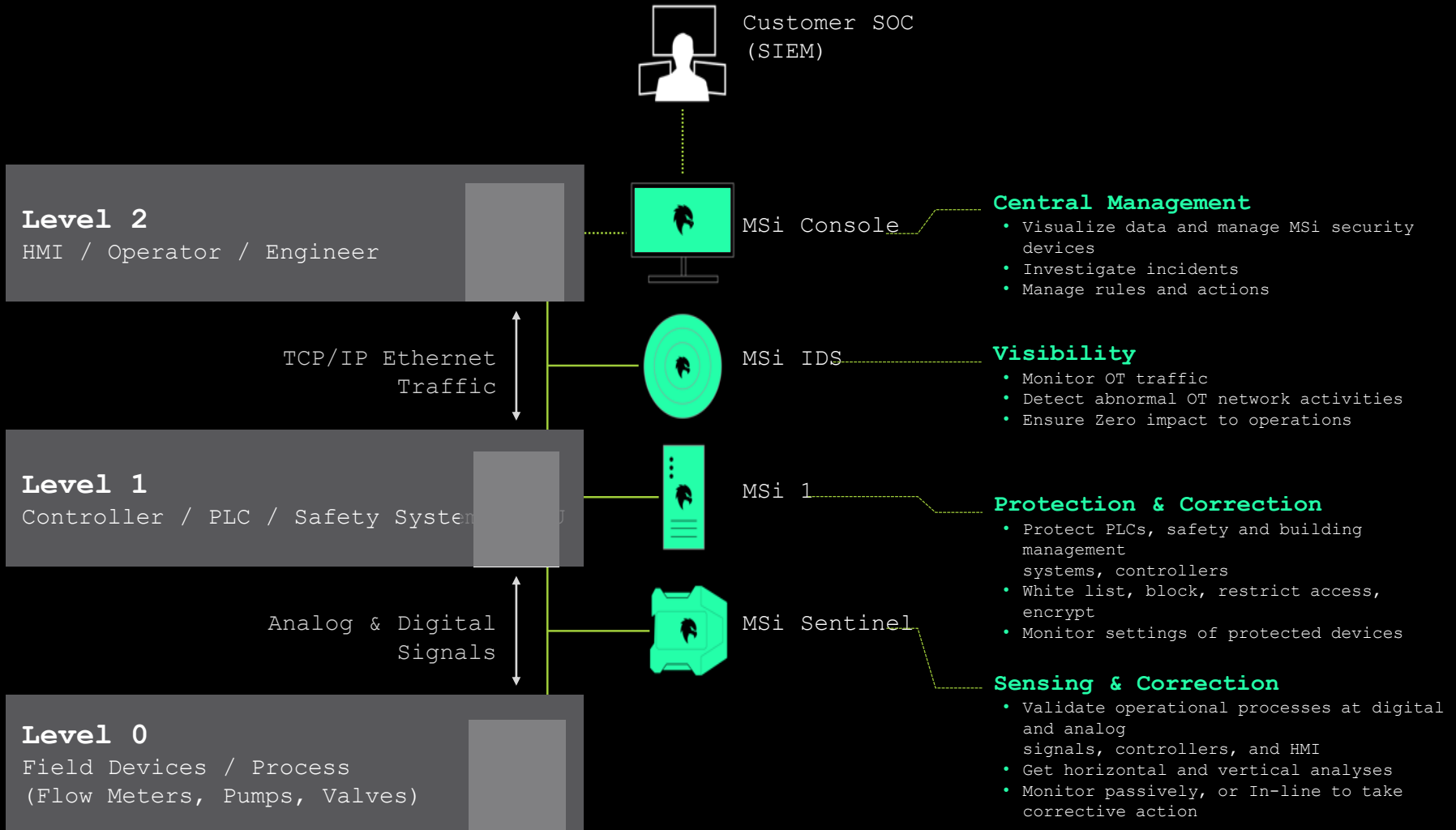
For Sensing and Correcting

Our on-site, cybersecurity device is installed between controllers and field instruments to detect changes at the physical level, even if the HMI has been compromised.



Note: The MSi Platform is a patented product of Mission Secure, Inc. covered by US Patent No. 9697355

The MSi Platform



Equipped for Operational Environments



Battle-tested against the harshest environments to provide industrial devices Level 0-2 protection, anywhere in the world.

Military Strength

Arizona Cyber Warfare Range (2017)

- Red team industry cyber experts performed month-long evaluation
- AZ CWR endorses MSi Platform as cyber solution for control systems

Millennium Corp. Comprehensive PEN Testing (August 2018)

Lockheed Martin PEN Testing (November 2018)

U.S. Department of Defense Information Systems Agency (DISA)

- DISA Security Technical Implementation Guide (STIG) is applied
- Numerous and detailed security features are implemented

Fortune 10 Supermajor

- Lab test, red team, internal audits and production testing are integrated

Industrial Grade

Industrial compute boards withstand -20° to +80° degrees Celsius

Mean time to failure rated at 13+ years, with mechanical failover and conformal coating

Supports multiple OT protocols, digital and analog signals, and ethernet and serial connections

Facilities use case



MSi Console

- Affords visibility, command, and control



MSi IDS

- Monitors OT traffic



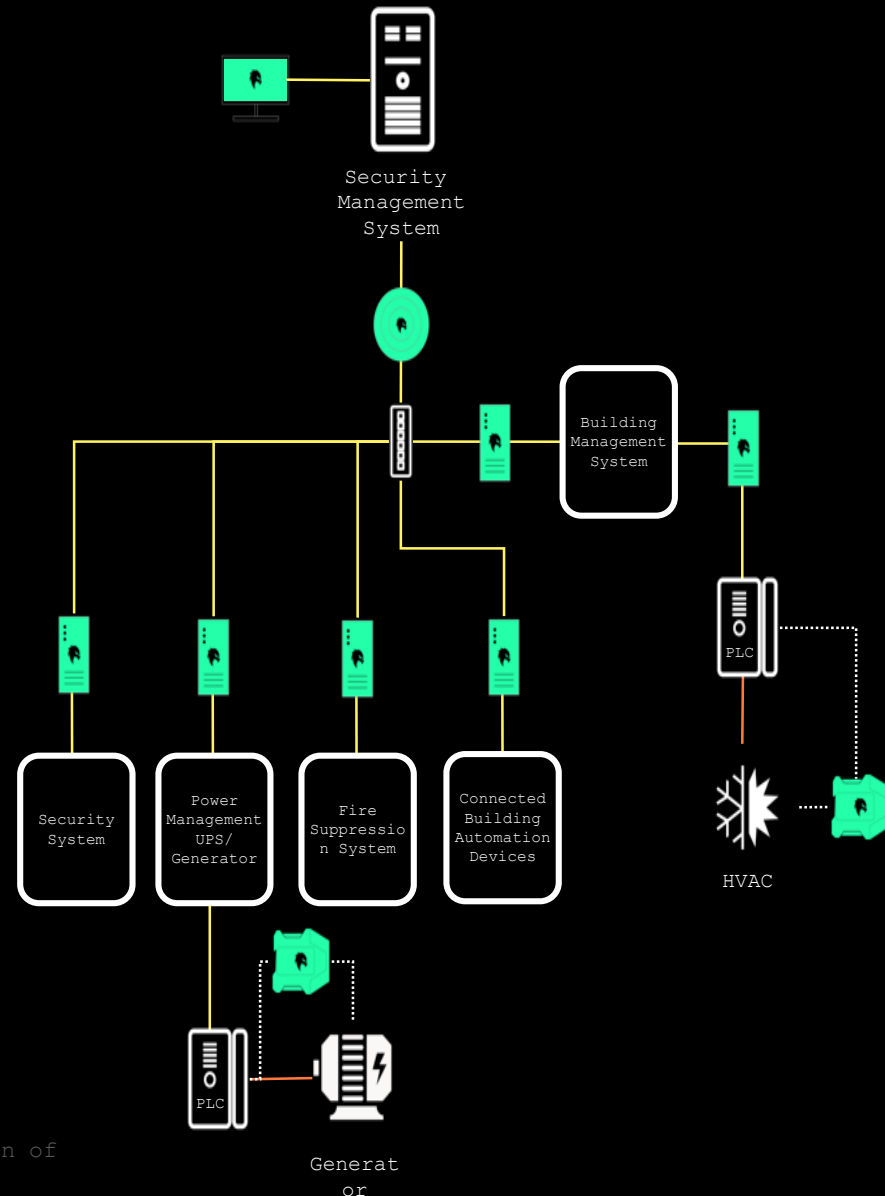
MSi 1

- Protects key connected facility control systems
- Protects egress back into IT/OT network

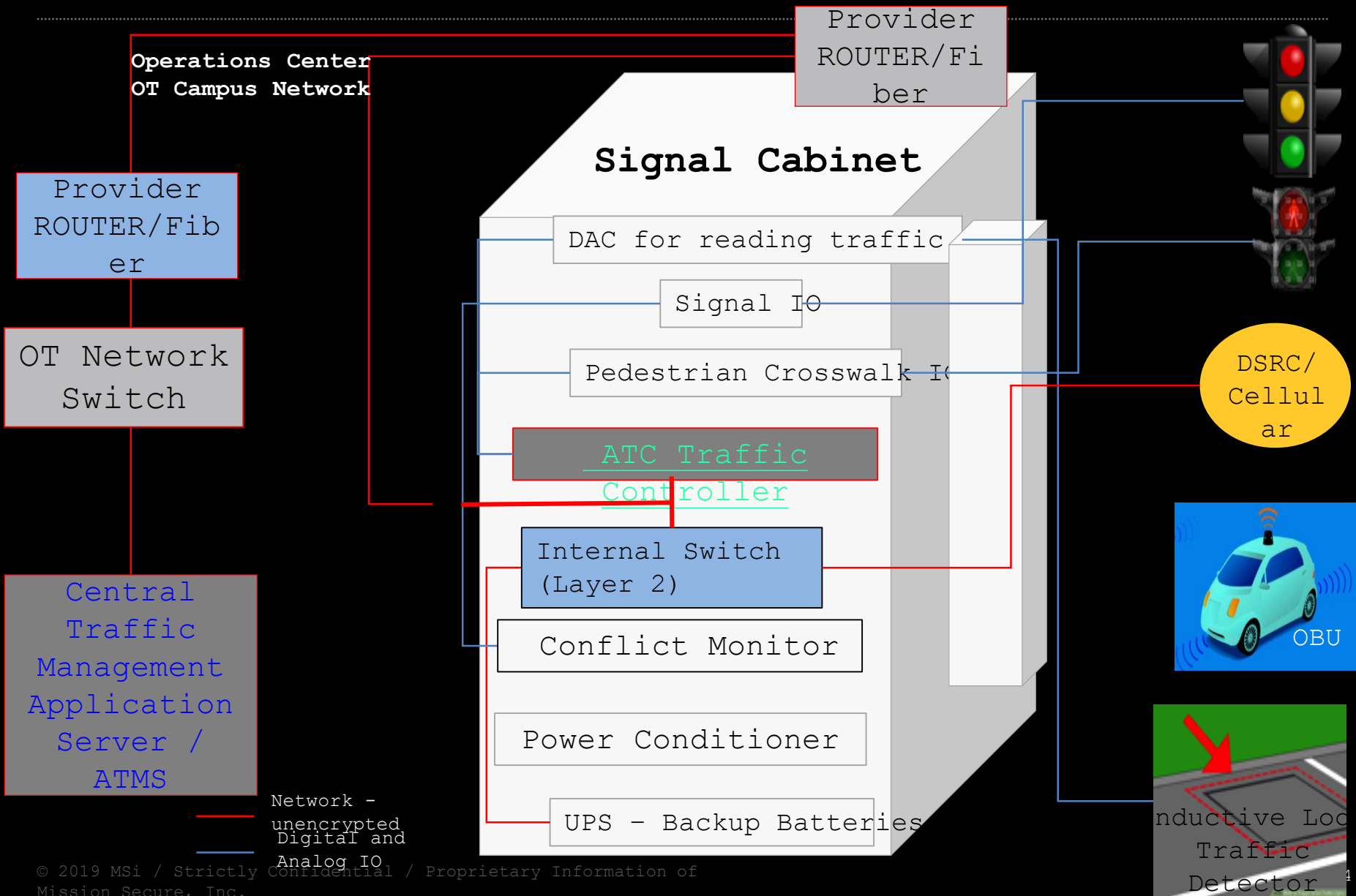


MSi Sentinel

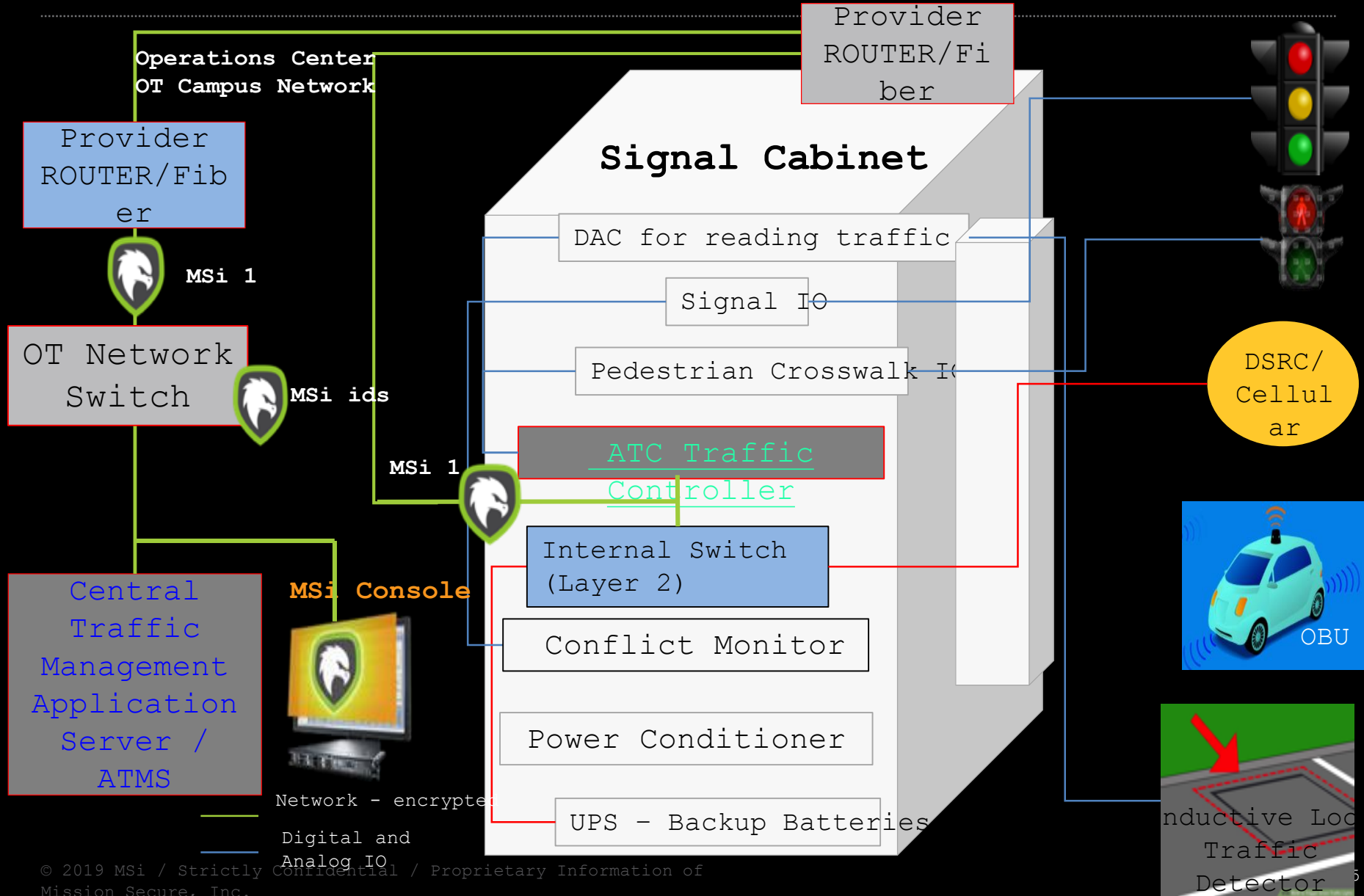
- Verifies HVAC settings and compares against PLC and HMI
- Detects false sensor data



Vulnerable Traffic System



Protected Traffic System






Requirements for a Reliable Solution



- Ability to automatically defeat malware and zero day attacks
- An experienced team using technology-based assessment methodology
- A successful track record of delivering insightful client recommendations
- Provides continuous OT monitoring and protection
- No impact to operations - The solution adapts to you, not the other way around
- Operates in harsh production environments
- Cost-effectively mitigates high-impact risks and closes the gaps
- On-premise or Cloud/edge solution
- Purpose-built for IIoT/Big Data/Digital initiatives
- Holds high-value third-party security certifications
- Validated by successful usage by large, cutting edge organizations in multiple usage models and varied environments

A Simple Plan to Protect Networks



	Phase	Deliverables	Duration
 Assess	Cyber Risk Assessment	<ul style="list-style-type: none"> • Take deep-dive approach to critical plants • Engage in site visits • Use NIST/DHS/IEC 62443 standards as methodology • Map "as-is" cyber architecture • Generate real-time OT network analysis • Compile Cyber Readiness scorecard 	1-2 Months
 Design	Cybersecurity Design	<ul style="list-style-type: none"> • Identify immediate solutions • Map "to-be" cyber architecture • Define actionable plan and prioritization • Create Reporting & Management briefings 	1 Months
 Protect	Detection & Protection	<ul style="list-style-type: none"> • Determine solutions based on Phases I & II • Install, test and cutover • Facilitate successful checkout and test results • Train and support • Provide ongoing monitoring and support 	1-2 Months
	Estimated Total		3-5 Months

Contact information



Houston Office

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

Charlottesville Office

300 Preston Avenue
Suite 500
Charlottesville, VA 22902

Rick Tiene

*VP Smart Cities, Government
and Critical Infrastructure*
rtiene@MissionSecure.com
m. 703.618.9100

Dave Jordan

VP Cyber Services
DavidJ@MissionSecure.com
434.284.8071 x740

George Mason University Cyber Security
Partnership

<https://care.gmu.edu/city-county-cybersecurity-partnership-project/>

Appendix

MSi Console



Tap into a centralized interface for the management, monitoring, and protection of your control systems across every level.

Deployed on-premise or as a Platform-as-a-Service (e.g., MSSP), you can monitor network traffic, controller changes, and OT visibility from Human Machine Interfaces (HMI), down to the physical Level 0 process.

Key Advantages

- Get an unprecedented and centralized overview of your network
- Gain additional visibility through asset discovery and inventory management
- Push software and firmware updates to every MSi device from a single console
- Retain control of remote MSi secure devices, configurations, and rules
- Notify MSi, IT manager, and control engineers of abnormal activity and attacks
- Troubleshoot remotely for operational efficiencies
- Configure remedial solutions through corrective action managers
- Deployment is simple – just plug the MSi console into your existing control network
- Review trusted data for trans- and post-attack forensic analysis

Integrations

- Integrates with IT cyber solutions, including SPLUNK, SIEM, and more
- Supports large numbers of MSi 1, MSi IDS, and Sentinel devices for a plant- and facility-wide, or production-control network deployment



MSi IDS (Intrusion Detection System)



Improve your awareness of operational network activities for greater insight into potential threats, network health, and troubleshooting.

Key Advantages

- Identify hostile reconnaissance on your OT network
- Detect abnormal OT network traffic
- See potential cyber attacks and operational bottlenecks
- Auto-generate suggested rules to block unwanted activity
- Get OT network visibility to monitor, detect, inform, and collect critical information within an enterprise OT network and remote field sites
- Save "Windshield Time" and gain insight into efficient operations and cost reductions through streamlined network traffic and remote troubleshooting

Features for OT-focused detection and network data capture:

- Passively monitor OT digital network traffic and detections – from Level 1 devices to the operator and HMI
- Troubleshoot "unseen" and abnormal OT network activity
- Gain asset discovery capabilities
- Combined with the MSi 1 and MSi Sentinel, get complete visibility from the engineer's workstation (HMI) down to Level 0 devices



MSi 1



The MSi 1 is an end-point cybersecurity solution that provides operational-level protection through integrated and on-site automation. Featuring conformal coating for enhanced durability, it's purpose-built for the harshest environments.

It starts by installing the MSi 1 on-site, in front of controllers – including key PLCs, RTUs, safety systems, flow controllers and meters.

Key Advantages

- Enable multi-factor authentication and secure, predictive IIoT capabilities
- Block unwanted activity (ingress and egress)
- Prevent Malware or DDOS attacks on controllers
- Identify changes to controller settings
- Map normal traffic and spot abnormal behavior
- Encrypt traffic between controllers and engineer work stations
- Collect data for forensics around events
- Take corrective action (manually or fully automated)
- Execute multiple protocols (Modbus, CIP, OPC, BacNet, Serial and Ethernet)
- Safeguard uptime with an integrated, mechanical fail-safe option



MSi Sentinel



For the most comprehensive defense, get true visibility into the lowest ICS levels – which remain otherwise unseen today.

The MSi Sentinel offers industrial-grade end-protection at the physical level, in extreme conditions from -4° F to 185° F (-20° to 85° C),

Key Advantages

- Read and translate digital and analog signals (IO), up to 32 IO per device
- Validate processes and reports by the PLC to operator
- Detect false or spoofed signals
- Compare physical attributes (flow, temperature, pressure) to identify operational abnormalities
- Minimize plant shutdowns, prevent damage, and avoid economic loss
- Ensure plant safety and avoid injuries

Level 0: Field Instrumented Devices Controlling the Physical Process

- Meters
- Sensors
- Valves
- Switches
- Pumps
- Motors



Information Security Strategy

a VDSS Experience



Presentation Objective: Create a shared awareness of the importance having an Information Security Strategy, and show one way of developing an agency Information Security Strategy.

Barry Davis, CISSP
DSS Chief Information Security Officer

ISOAG 3/06/2019

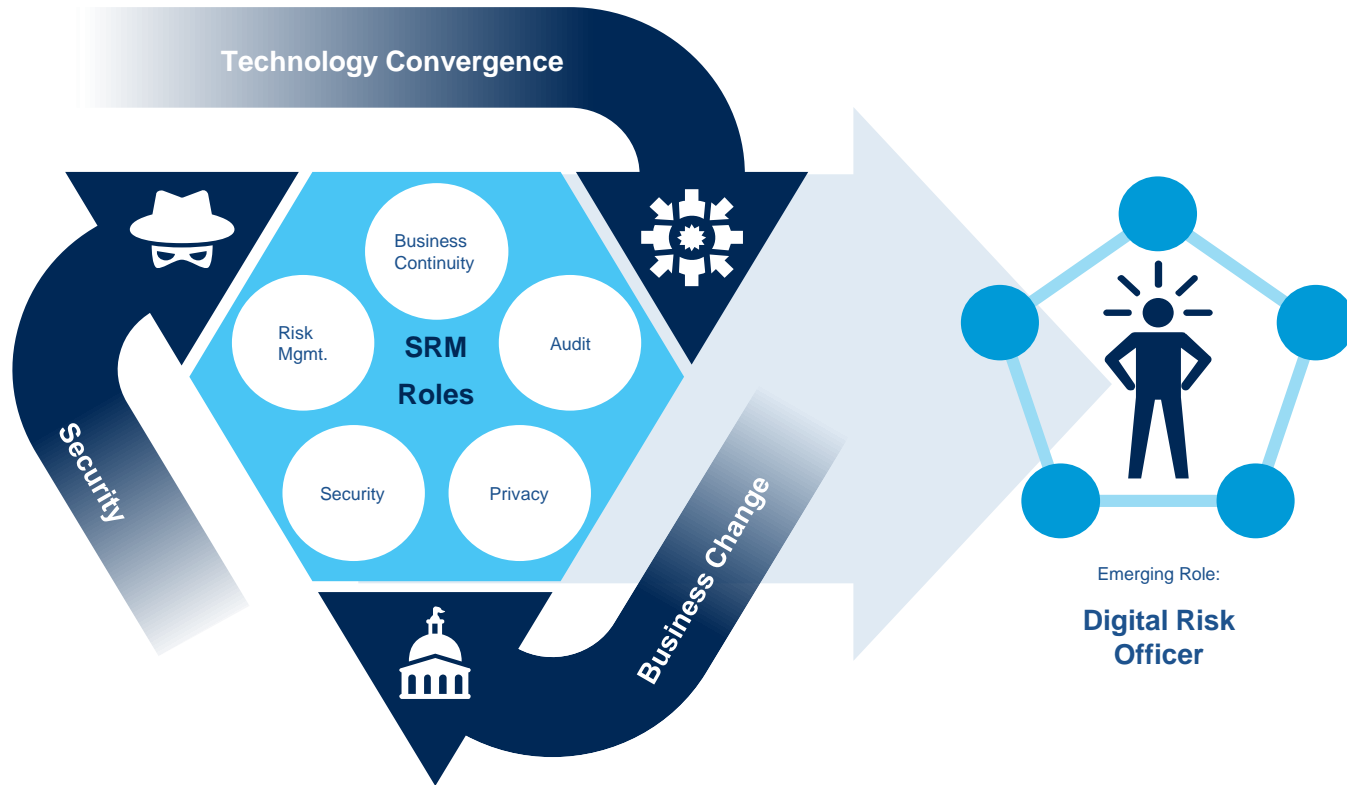


Agenda

- Why have a strategy?
- Organizing for the effort
- Guided Methodology Approach
- Phase 1
- Phase 2
- Phase 3
- Next Steps for DSS



Why have a strategy?





Why have a strategy?

THREAT ACTORS, ATTACK VECTORS, AND IT SYSTEM COMPLEXITY ARE CHANGING QUICKLY
ORGANIZATIONS THAT DON'T ADAPT WILL BE IMPLICITLY ACCEPTING HIGHER RISK OF A
BREACH

THREAT ACTORS

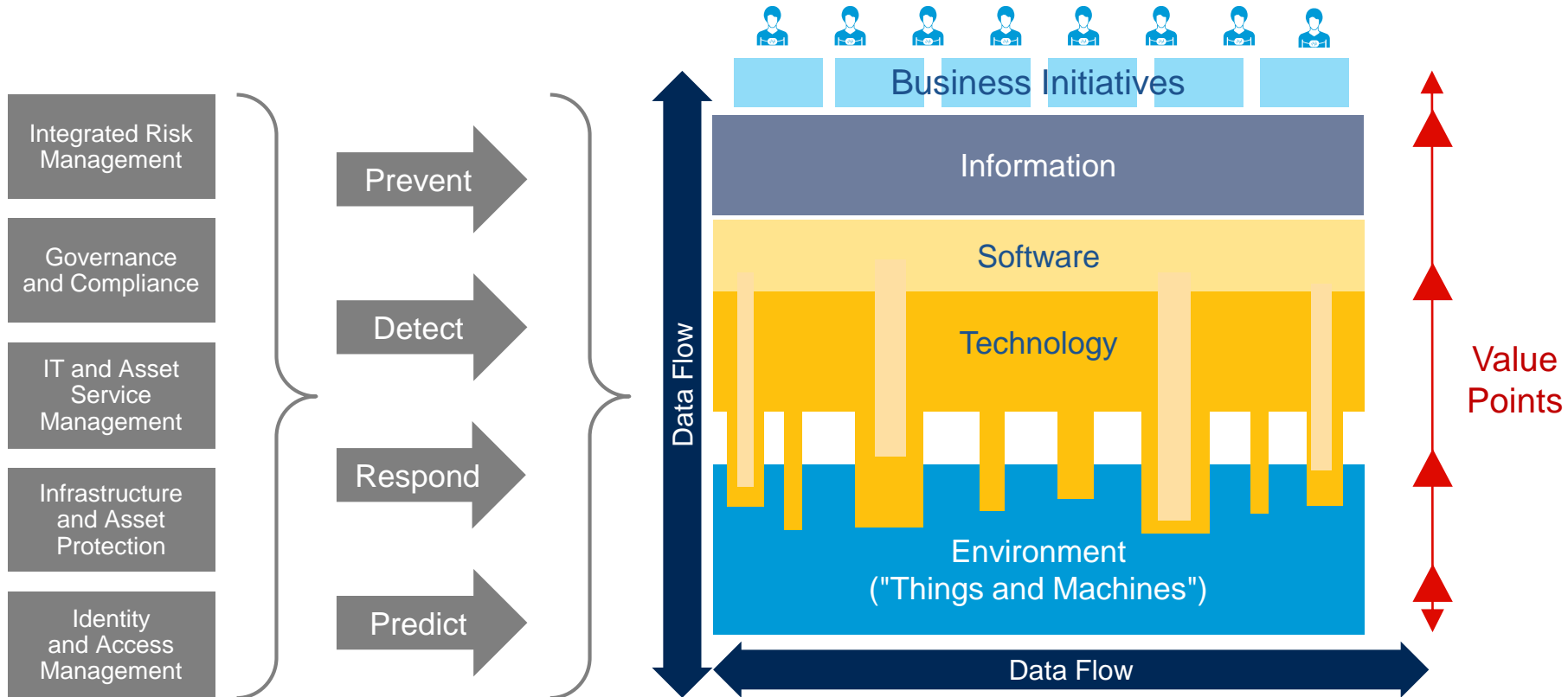
- Script kiddies are still out there, but well-funded organized crime and nation states are becoming more prevalent.
- Monetization of stolen data is easier than ever before, especially due to ransomware... this makes bad actors more willing to attack.
- Valuable information is everywhere! Any part of a system presents a desirable target.

IT SYSTEMS

- Data does not rest safely in storage... competing expectations for constant access and constant security are now the norm.
- Outsourced infrastructure, software, and managed services mean that security boundaries are ambiguous and responsibility is often shared.
- Valuable information is everywhere! IT systems must be thoroughly assessed.



Why have a strategy?





Organizing for the Effort -People

- ISO is the sponsor
- External Support Info-Tech facilitator as part of agency subscription (<https://www.infotech.com>)
- If you have staff, they should drive this effort
- Involvement = Buy-In
- Your staff will have a better assessment of maturity, be ready for this
- Let your boss know what you're doing
- This counts as a program assessment (Continuous Monitoring)



Organizing for the Effort

Information Security Framework

Governance

Context and Leadership

Information Security Charter

Information Security
Organizational Structure

Culture and Awareness

Evaluation and Direction

Security Risk Management

Security Policies

Security Strategy and
Communication

Compliance, Audit, and Review

Security Compliance
Management

Internal Security Audit

External Security Audit

Management Review of
Security

Management

Prevention

Identity Security

Identity and Access
Management

Data Security

Hardware Asset Management

Data Security & Privacy

Infrastructure Security

Network Security

Vulnerability Management

Endpoint Security

Cryptography Management

Malicious Code

Physical Security

Application Security

Cloud Security

HR Security

HR Security

Change and Support

Configuration and Change
Management

Vendor Management

Detection

Security Threat Detection

Log and Event Management

Response and Recovery

Security Incident Management

Information Security in BCM

Security eDiscovery and
Forensics

Backup and Recovery

Measurement

Metrics Program

Continuous Improvement

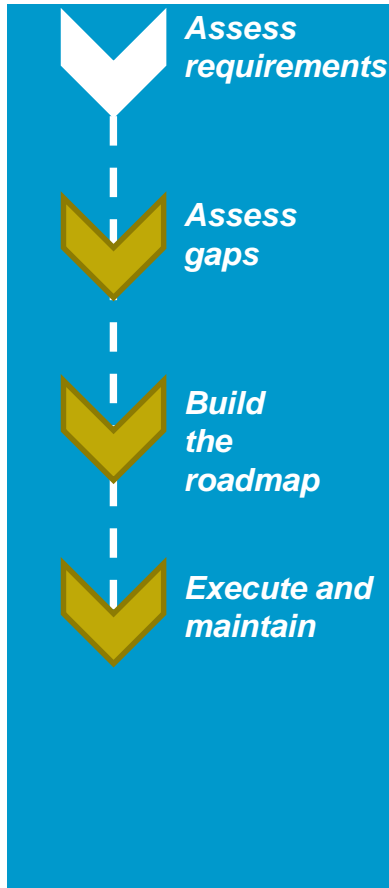


Organizing for the Effort

	Time, Effort, and Value Using Onsite Support				With Remote Support
Phase 1: Assess Security Requirements	1-5 people	½ day - 2 days	Fluctuation in assessment time is based on differences in organization's cultures.	Medium Value	1-2 weeks (may not be considered prior to starting strategy)
Phase 2: Build a Gap Initiative Strategy	1-5 people	2-3 days	Create multiple 3-4 hour meetings to work through the gap tool.	High Value	4-8 weeks
Phase 3: Prioritize Initiatives and Plan Roadmap	1-2 people	1 day	1-8 hours of security management's time.	High Value	1-2 weeks
Phase 4: Plan for the Transition	1-5 people	1-2 days	1-2 hours to bring together the team from Phase 1.	Medium Value	1-2 weeks
Iterative benefit.				Time & Effort Saved:	7-14 weeks



Strategy Step 1



Activities in this phase:

- 1.1 What do you want to get from your security strategy?
- 1.2 Assess your organization's current inherent pressure
- 1.3 Establish your goals, obligations, scope, and boundaries
- 1.4 Determine your organization's risk tolerance

Outcomes:

After completing this phase, you will have:

- ✓ A formalized understanding of your business, customer, and regulatory obligations.
- ✓ The external pressure your organization faces.
- ✓ A defined scope of the project.
- ✓ Your organization's risk tolerance.

Key benefits:

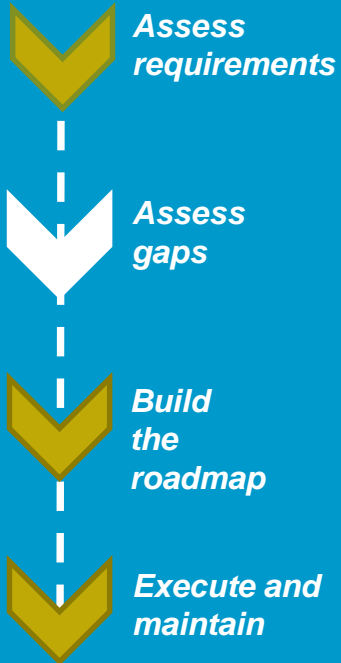
These activities will enable you to:

- ✓ **Understand** threat types, their motivations, and how they can impact your organization.
- ✓ **Build awareness** of your external pressure and internal risk tolerance among the IT team and business leaders.
- ✓ **Clarify** the security program's obligations and scope.

Compliance and organizational reputation create an intertwined relationship between the business and your security strategy. A future-proof security strategy is flexible, nimble, and elastic to adapt to changing environmental needs.



Strategy Step 2, Assess Gaps



Activities in this phase:

- 2.1 Review Info-Tech's framework
- 2.1 Understand your vulnerabilities
- 2.2 Assess your current state and define a target state
- 2.3 Use Info-Tech's prepopulated gap initiatives as a starting point to building your own
- 2.4 Review your current maturity level and maturity gap

Outcomes:

After completing this phase, you will have:

- ✓ An understanding of ways to assess existing vulnerabilities in the system
- ✓ The state of your current security program
- ✓ An identified ideal target state
- ✓ Comprehensive visuals of your maturity state gap

Key benefits:

These activities will enable you to gain:

- ✓ **Clarity** on your current state vs. target state and a high-level understanding of the gaps between states
- ✓ **Understanding** of common initiatives for each area of security

Nobody will tell you that their product/function is obsolete.

The security strategy should identify what you **don't** need, as well as what you **do** need, to provide the most value to your organization.

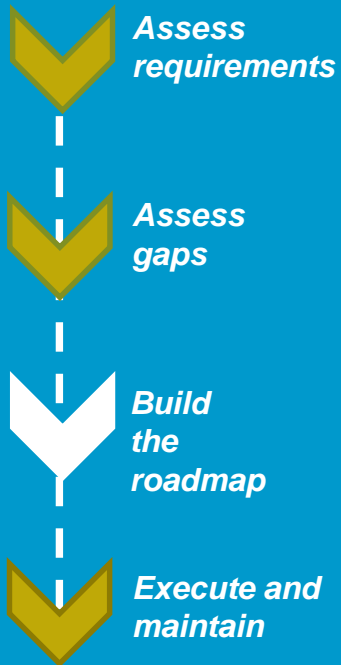


Gap Analysis Spreadsheet

1. Under each of the seven security practices listed below, assess yourself on each statement to determine your		2. For each control statement, indicate the level of maturity: 1 = Initial/Ad hoc 2 = Developing 3 = Defined 4 = Managed and Measurable 5 = Optimized		3. For each control statement where a maturity gap exists, determine a gap initiative that would allow you to achieve the target maturity state.		Target maturity = 3			
Click the +/- here to show/hide instructions		Fill 1-5		Free text	Fill 1-5		Free text		Free text
		Current Maturity	Current Average	Current State Comments	Target Maturity	Target Average	Gap Description	Common Gap Initiatives (current score, target score, and gap initiative)	Gap Initiative
Charter	The information security charter includes the expectation and requirements of interested parties and necessary business stakeholders.	1	1.0	While we have a mission statement, ISRM does not have an official charter	3	3.0	Must develop charter	1 - 3 Document and define an information security charter.	1 - 3 Document and define an information security charter
	The information security charter includes a statement describing the scope (including data, systems, locations, and organizational scope).	1		While we have a mission statement, ISRM does not have an official charter	3		Will include in charter development	1 - 3 Document and define an information security charter.	1 - 3 Document and define an information security charter
	The information security charter includes both the vision and mission for the security program.	1		While we have a mission statement, ISRM does not have an official charter	3		Will include in charter development	2 - 4 Define scope, vision, mission & objectives with business stakeholders to get buy-in.	2 - 4 Define scope, vision, mission & objectives with business stakeholders to get buy-in.
	The information security charter includes the objectives for the security program.	1		While we have a mission statement, ISRM does not have an official charter	3		Will include in charter development	2 - 4 Define scope, vision, mission & objectives with business stakeholders to get buy-in.	2 - 4 Define scope, vision, mission & objectives with business stakeholders to get buy-in.
	Commitment from senior management, the board, and any other senior leadership positions are defined and documented in the information security charter.	1		While we have a mission statement, ISRM does not have an official charter	3		Will include in charter development	2 - 4 Sign-off on charter document and provide dedicated resources to support implementation of the charter.	2 - 4 Sign-off on charter document and provide dedicated resources to support implementation of the charter.
	High-level responsibilities for the security program are outlined and assigned by role or group in the security charter (e.g. using a RACI chart).	1		While we have a mission statement, ISRM does not have an official charter	3		Will include in charter development	2 - 3 Document RACI chart. Assign responsibility for third-party group's security service providers. 2 - 3 Define high-level responsibilities with business stakeholders to get buy-in.	2 - 3 Document RACI chart. Assign responsibility for third-party group's security service providers. 2 - 3 Define high-level responsibilities with business stakeholders to get buy-in.
	Governing security principles (either custom to the organization or following recognized best practices) are included in the security charter.	1		While we have a mission statement, ISRM does not have an official charter	3		Will include in charter development	2 - 4 Define security principles with business stakeholders to get buy-in.	2 - 4 Define security principles with business stakeholders to get buy-in.
	The information security charter is communicated to the organization.	1		While we have a mission statement, ISRM does not have an official charter	3		Will include in charter development	1 - 4 Communicate and distribute security charter to the entire organization.	1 - 4 Communicate and distribute security charter to the entire organization.
	The information security charter is regularly reviewed, evaluated, and updated.	1		While we have a mission statement, ISRM does not have an official charter	3		Will include in charter development	2 - 4 Perform an annual review of the charter.	2 - 4 Perform an annual review of the charter.
				There is an org chart. There are systems and applications that may not function				Formalize the dissemination and understanding of the organizational structure.	



Strategy Step 3, Build your Roadmap



Activities in this phase:

- 3.1 Consolidate gap initiatives
- 3.2 Define cost, effort, alignment, and security benefit of each initiative
- 3.3 Create a cost : effort : alignment map for all initiatives
- 3.4 Based on your map, take the final step of building your prioritized security strategy roadmap

Outcomes:

After completing this activity, you will have:

- ✓ A succinct and consolidated list of gap initiatives that will collectively achieve your target state for security
- ✓ A formally documented set of estimated priority variables (cost, effort, business alignment)
- ✓ A fully prioritized security roadmap that is in alignment with business goals, and informed by the organization's needs and limitations

Key benefits:

These activities will enable you to:

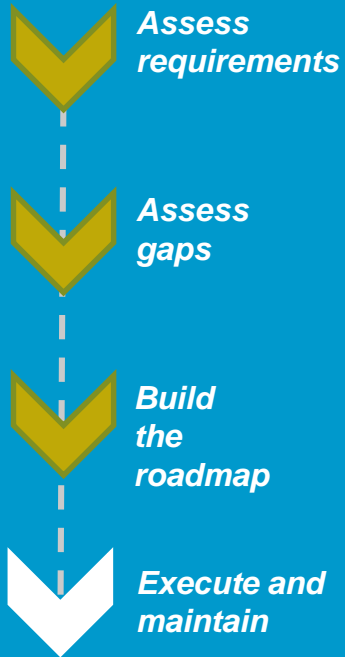
- ✓ **Support** your case for security initiatives by aggregating cost : effort : alignment data
- ✓ **Identify** easy win tasks and high value projects worth fighting for
- ✓ **Formalize** initiatives that will close your current/target state gap
- ✓ **Clarify** your decisions to begin, or *not* to begin, initiatives based on resourcing and alignment

You cannot do everything – and you probably wouldn't want to.

A good security program won't give you perfect security, but it *will* enable you to make educated decisions about which projects are most important, and *why*.



Strategy Step 4, Execute and maintain



In this phase:

- 4.1 Review strategy for ongoing use of Tab 10. Progress Tracker
- 4.2 Gain buy-in
- 4.3 Develop a security charter
- 4.4 Review links to Info-Tech resources to support your top initiatives

Outcomes:

After completing this phase, you will:

- ✓ Have a plan to take action on your security strategy.
- ✓ Understand how to use the *Gap Analysis Tool* in an ongoing way.
- ✓ Have direct links to Info-Tech resources, where we can help you take action on your strategy today.

Key benefits:

These activities will enable you to:

- ✓ **Support** your project management by gaining visibility into time and resource allocation.
- ✓ **Identify** where in the priority order to take on new projects.
- ✓ **Formalize** a realistic plan to address security concerns that can't be taken on today.
- ✓ **Clarify** Info-Tech resources that can help reduce the time and effort required to achieve your goals.

Security and flexibility aren't mutually exclusive.

Building from the right foundation will allow for flexibility and adaptability and provide greater incremental value as the business and security program evolve.



Accomplishments....

Knowledge Gained

- Knowledge of organizational security pressure and the drivers behind it
- Insight into stakeholder goals and obligations
- Defined security risk tolerance information
- Comprehensive knowledge of security current state and initiatives required to achieve security objectives

Processes Optimized

- Detailed security program assessment
- Prioritized security roadmap for next ~3 years
 - A roadmap that is relevant and realistic for your organization
- Guidance for streamlined communication of security information
- Processes for continuous improvement tracking and integration of new security initiatives

Deliverables Completed

- Information Security Pressure Analysis Tool
- Information Security Requirements Gathering Tool
- Information Security Program Gap Analysis Tool
- Information Security Strategy Communication Deck



Next Steps....

- Work the Initiatives
- Re-assess



Questions & Answers



Thank You!



Artifact Slide

- Example spreadsheet used for the VDSS security strategy project.



Microsoft Excel
Worksheet



Exceptions in Depth

John Craft

Deputy Commonwealth Information Security Officer

March 6, 2019





Security

- Good security
 - Proactive
 - Common defense in depth
 - Culture of security
- Bad security
 - Reactive
 - Siloed
 - Silent



What is an exception?

A deviation from an established rule, policy, standard, or baseline.





Acknowledgement of Risk

Also a formal acknowledgement of risk by the Agency Head

- Code of Virginia § 2.2-603(F) states: “the director of every agency and department in the executive branch of state government, including those appointed by their respective boards or the Board of Education, shall be responsible for securing the electronic data held by his agency or department and shall comply with the requirements of the Commonwealth's information technology security and risk-management program as set forth in § [2.2-2009](#).”
- Submission of an exception request stipulates that the Agency Head understands and accepts responsibility for the risks incurred in the environment.



Why must the CISO approve?

- Risk must often be assessed from an enterprise perspective
- More complete knowledge of available enterprise controls
- Evaluation against the established enterprise risk threshold



Common exception drivers

- Technical limitations
- Regulatory or legal requirements
- Business needs
- Personnel / staffing limitations
- Contractual requirement
- Budgetary limitation*
 - Rarely an acceptable justification



Common Exception Request Examples

- End-of-Life (EOL) software
- Inability to accept patches
- Deviation from security baseline
- Unable to maintain exclusive control of encryption keys for hosted services
- Password strength limitation
- Session lock expiration



What is expected?

- Business need / Justification
- Scope and extent
- Compensating controls
- Identification of risks and residual risks
- Specific duration – not to exceed one year
- Agency Head approval



Templates

- VITA CSRM has templates for many of the common exception requests
- A blank template is located at:

http://www.vita.virginia.gov/uploadedfiles/VITA_Main_Public/Library/PSGs/Word_versions/Blank_Exception_form.doc



Blank Template

COV **Information** Security Policy & Standard Exception Request Form
Agency Name: _____ Contact for Additional Information: _____

Policy/Standard requirement to which an exception is requested: _____

Note: This request is for an exception(s) to a component of the Commonwealth policy and/or standard(s) and approval of this request does not in any way address the feasibility of operational implementation. You are encouraged to check with your technical support staff prior to submitting this request.

1. Provide the **Business or Technical Justification:**

2. Describe the scope including quantification and requested duration (not to exceed one (1) year):

3. Describe all associated risks:

4. Identify the controls to mitigate the risks:

5. Identify all **residual** risks:

I have evaluated the business issues associated with this request and I accept any and all associated risks as being reasonable under the circumstances.

Printed name Agency Head

Signature

Date



Justification

- The business or technical need driving the request. This well defined and includes applicable artifacts, such as:
 - Work requests
 - VCCC / helpdesk tickets
 - Project plans
 - Vendor documentation
- Cost is rarely considered a compelling justification



Things to think about before you start

- What resources do my at-risk systems have access to?
- What is the privilege context of the system or account?
- What is the comprehensive risk before controls?
- What controls will be the most effective?
- Where do controls best fit into my architecture?
- What risks do the controls not address?



Scope and duration

- Exception should document details:
 - Number of systems impacted
 - Applications impacted
 - Accounts impacted
 - Data sensitivity classification
- Duration should be specified
 - Not to exceed one year
 - Exception should be remediated before expiration; if not, an extension or new request should be submitted



Compensating Controls

- Controls implemented to satisfy the requirements of approved security standards, policies, and baselines when those requirements cannot be met.
- Compensation controls should:
 - Be commensurate with the risk of not adhering to the original requirement;
 - Meet the intent of the original requirement; and
 - Provide similar defense as the original requirement.



Risks

- Identify risks associated with the requested security exception
- Compensating controls should be matched to identified risks
- Residual risks are those risks not completely mitigated by compensating controls
 - Compensating controls rarely completely mitigate risk



Common compensating controls

- Application control (WWLS)
 - End-of-support software
 - Shared systems
- Host-based Intrusion Prevention System (HIPS)
 - End-of-support frameworks (.NET) associated with approved processes
 - Unsupported transactional systems (databases)



Common compensating controls

- Managed firewall
 - End-of-support software / systems
 - Shared systems
 - Systems that cannot have other technical controls installed
- Enhanced logging and monitoring
- Enhanced physical security
- Enhanced scanning operations



Submission requirements

- Submission must come from the Agency Head or the Agency ISO
- Submission must be explicitly approved by the Agency Head
 - This can be via email
 - If approved by delegate, must provide proof of official DOA



Pending Archer Update

- CSRM is currently developing an exception workflow to allow agency ISOs to directly enter exception requests into Archer
 - ISO initiation
 - Automated expiration notification
 - Still requires explicit agency head documented approval



Demo

Archer Demo



Thank you for attending!

Questions?



Virginia Information Technologies Agency

Upcoming Events





Work group convening

- The April 2018 OSIG Performance Audit on Cybersecurity made a recommendation to study the adoption of NIST SP 800-37 to assess risk and test controls.
- If you are interested in participating in a work group to review the recommendation, please email [Ed Miller](mailto:Ed.Miller@vita.virginia.gov)



2019 COV Security Conference

2019 Security Conference Registration and Call for Papers

Registration for the 2019 Commonwealth of Virginia (COV) Information Security Conference is now open. The 2019 conference will be held April 11-12 at the Altria Theater in Richmond.

Conference and registration information can be found on the link below.

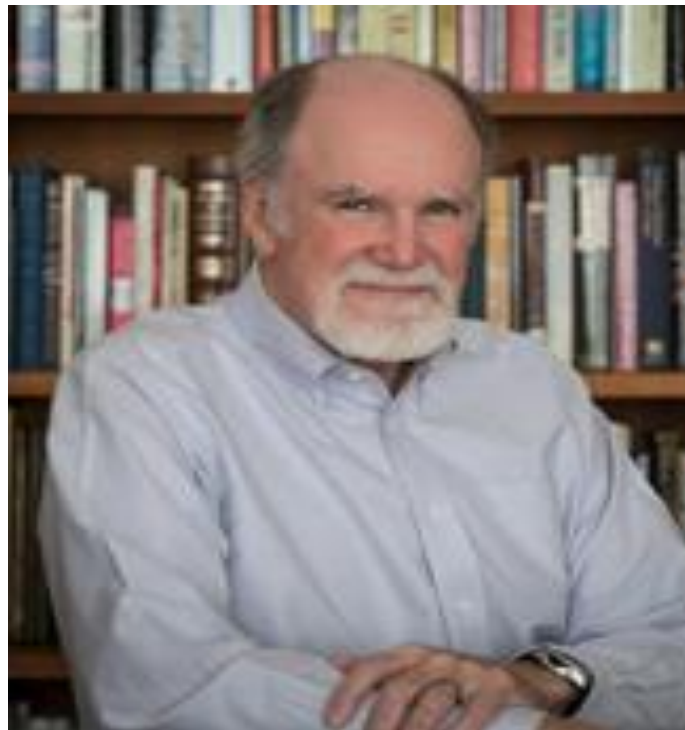
<https://www.vita.virginia.gov/commonwealth-security/cov-is-council/cov-information-security-conference/>

For all other conference questions:
[***covsecurityconference@vita.virginia.gov***](mailto:covsecurityconference@vita.virginia.gov)

Note: There will be a VITA ISO track. All new ISO's are encouraged to attend.

Keynote Speaker – Day One

Steve Uzzell – Internationally renowned
photographer and inspirational speaker



Keynote Speaker – Day Two

Jake Kouns – CISO Risk Base Security





Lunchtime Keynote Speaker – Day Two

Renee P. Wynn, NASA Chief Information Officer





SANS FOR508 - Advanced Digital Forensics and Incident Response Course – Richmond, VA

Date: March 6 - April 17, 2019

Location: ePlus

4101 Cox Road

Glen Allen, VA

Instructor: Andrew Skatoff

Cost: \$5,620

For more information:

<https://www.sans.org/mentor/class/for508-richmond-06mar2019-andrew-skatoff>



Virginia Cybersecurity Partnership

VCSP Member Meeting - Data Science and Cybersecurity

Date: March 12, 2019

Time: 10 a.m. - 2 p.m.

Cost: Free Event Category: Members Only

Location: University of Virginia – Zehmer Hall

104 Midmont Ln
Charlottesville, VA 22903



IS Orientation

The next IS Orientation will be held on March 28 from 1-3 p.m. in room 1221 (CESC).



Future ISOAG

April 3 , 2019 @ CESC 1-4 p.m.

**Speakers: Dr. Michaela Iorga, NIST
Bob Auton, VITA**

ISOAG meets the first Wednesday of each month in 2019

Adjourn

THANK YOU FOR ATTENDING

