Engage. Explore. Empower.

Connecting Visionaries in Radiation Safety, Science and Industry

MIRION Connect 24

Annual Users' Conference

July 29 - August 2 | Omni Dallas Hotel, Dallas, TX

MIRION TECHNOLOGIES

Cybersecurity Audits, Compliance Areas, and What to Check for, Audit Q&A

July 31, 2024

MIRION TECHNOLOGIES

Agenda

- Inspection Data Requests
- Violations or Findings
- Cybersecurity Audits & Compliance Areas
  - What are the Violations and Findings
  - Where do we need to look
  - What is the Mitigation to avoid being the “Lucky Few”
  - What are some Tips to avoid them
  - What are some of the Tripping points that cause them
- The Risk – Vulnerable and Exposed vs Vulnerable but not Exposed
- Audit Q&A

Inspection Data Requests

Inspection Data Requests

Provide this information by MM/DD/YYYY

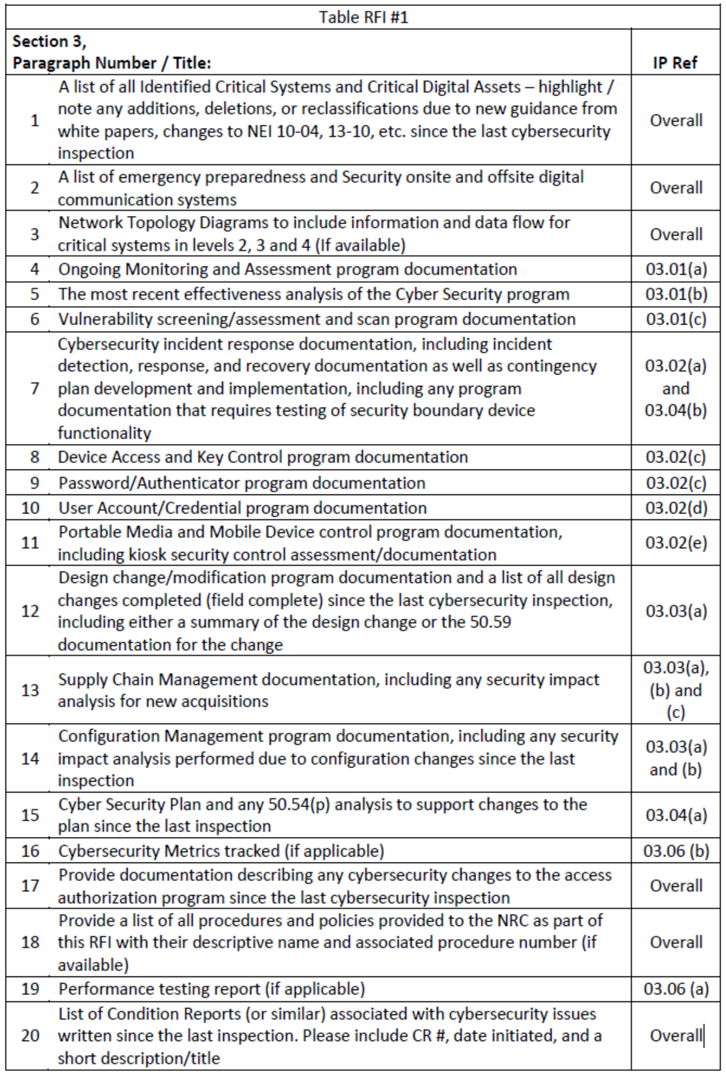


Table RFI #1

	Section 3, Paragraph Number / Title:	IP Ref
1	A list of all Identified Critical Systems and Critical Digital Assets – highlight / note any additions, deletions, or reclassifications due to new guidance from white papers, changes to NEI 10-04, 13-10, etc. since the last cybersecurity inspection	Overall
2	A list of emergency preparedness and Security onsite and offsite digital communication systems	Overall
3	Network Topology Diagrams to include information and data flow for critical systems in levels 2, 3 and 4 (If available)	Overall
4	Ongoing Monitoring and Assessment program documentation	03.01(a)
5	The most recent effectiveness analysis of the Cyber Security program	03.01(b)
6	Vulnerability screening/assessment and scan program documentation	03.01(c)
7	Cybersecurity incident response documentation, including incident detection, response, and recovery documentation as well as contingency plan development and implementation, including any program documentation that requires testing of security boundary device functionality	03.02(a) and 03.04(b)
8	Device Access and Key Control program documentation	03.02(c)
9	Password/Authenticator program documentation	03.02(c)
10	User Account/Credential program documentation	03.02(d)
11	Portable Media and Mobile Device control program documentation, including kiosk security control assessment/documentation	03.02(e)
12	Design change/modification program documentation and a list of all design changes completed (field complete) since the last cybersecurity inspection, including either a summary of the design change or the 50.59 documentation for the change	03.03(a)
13	Supply Chain Management documentation, including any security impact analysis for new acquisitions	03.03(a), (b) and (c)
14	Configuration Management program documentation, including any security impact analysis performed due to configuration changes since the last inspection	03.03(a) and (b)
15	Cyber Security Plan and any 50.54(p) analysis to support changes to the plan since the last inspection	03.04(a)
16	Cybersecurity Metrics tracked (if applicable)	03.06 (b)
17	Provide documentation describing any cybersecurity changes to the access authorization program since the last cybersecurity inspection	Overall
18	Provide a list of all procedures and policies provided to the NRC as part of this RFI with their descriptive name and associated procedure number (if available)	Overall
19	Performance testing report (if applicable)	03.06 (a)
20	List of Condition Reports (or similar) associated with cybersecurity issues written since the last inspection. Please include CR #, date initiated, and a short description/title	Overall

Provide this information one month later

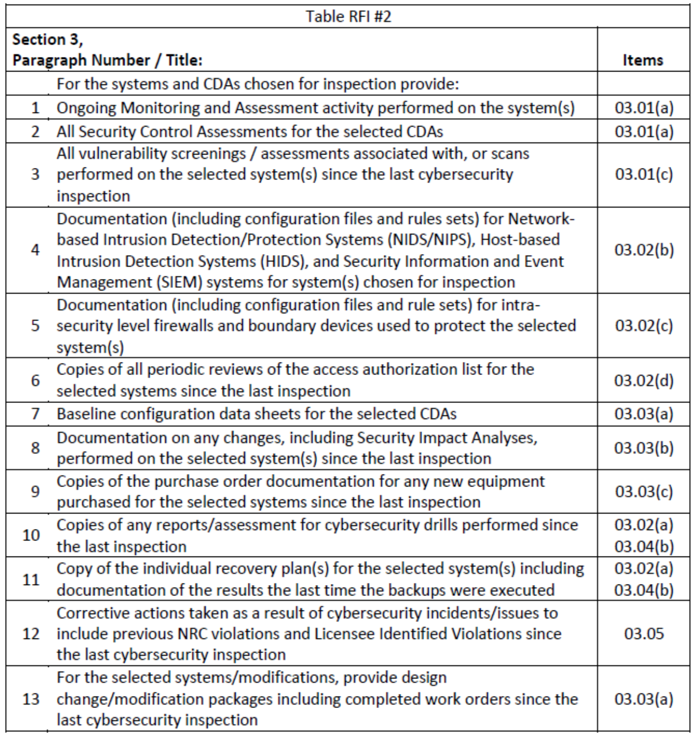


Table RFI #2

	Section 3, Paragraph Number / Title:	Items
	For the systems and CDAs chosen for inspection provide:	
1	Ongoing Monitoring and Assessment activity performed on the system(s)	03.01(a)
2	All Security Control Assessments for the selected CDAs	03.01(a)
3	All vulnerability screenings / assessments associated with, or scans performed on the selected system(s) since the last cybersecurity inspection	03.01(c)
4	Documentation (including configuration files and rules sets) for Network-based Intrusion Detection/Protection Systems (NIDS/NIPS), Host-based Intrusion Detection Systems (HIDS), and Security Information and Event Management (SIEM) systems for system(s) chosen for inspection	03.02(b)
5	Documentation (including configuration files and rule sets) for intra-security level firewalls and boundary devices used to protect the selected system(s)	03.02(c)
6	Copies of all periodic reviews of the access authorization list for the selected systems since the last inspection	03.02(d)
7	Baseline configuration data sheets for the selected CDAs	03.03(a)
8	Documentation on any changes, including Security Impact Analyses, performed on the selected system(s) since the last inspection	03.03(b)
9	Copies of the purchase order documentation for any new equipment purchased for the selected systems since the last inspection	03.03(c)

10	Copies of any reports/assessment for cybersecurity drills performed since the last inspection	03.02(a)
		03.04(b)

11	Copy of the individual recovery plan(s) for the selected system(s) including documentation of the results the last time the backups were executed	03.02(a)
		03.04(b)

12	Corrective actions taken as a result of cybersecurity incidents/issues to include previous NRC violations and Licensee Identified Violations since the last cybersecurity inspection	03.05
13	For the selected systems/modifications, provide design change/modification packages including completed work orders since the last cybersecurity inspection	03.03(a)

Provide for 1st week on-site

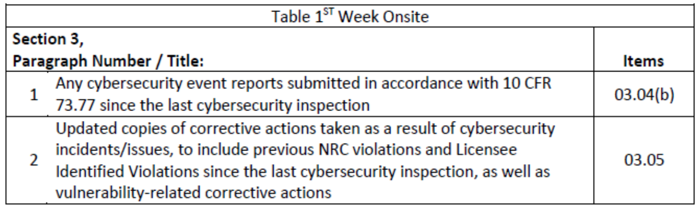


Table 1ST Week Onsite

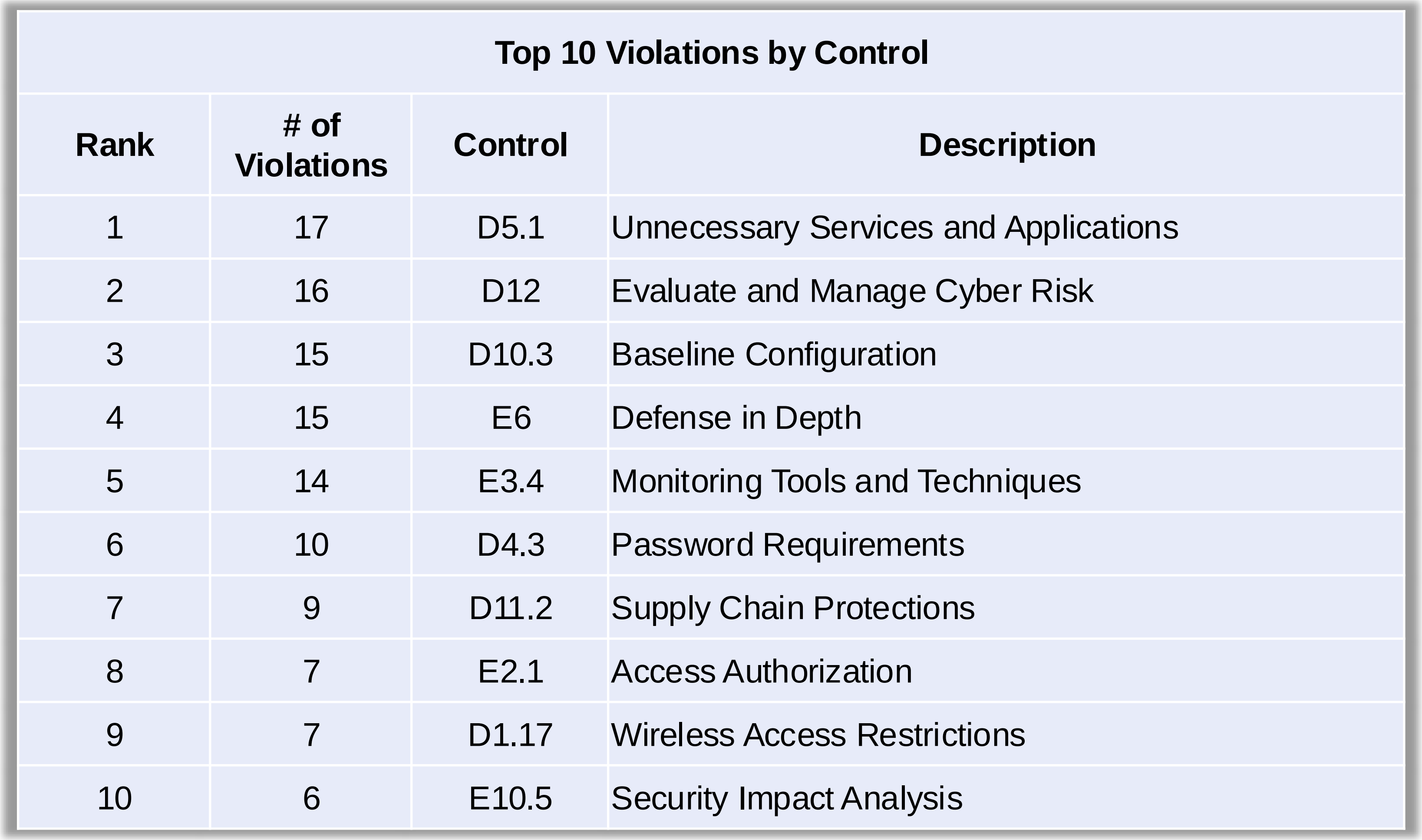
	Section 3, Paragraph Number / Title:	Items
1	Any cybersecurity event reports submitted in accordance with 10 CFR 73.77 since the last cybersecurity inspection	03.04(b)
2	Updated copies of corrective actions taken as a result of cybersecurity incidents/issues, to include previous NRC violations and Licensee Identified Violations since the last cybersecurity inspection, as well as vulnerability-related corrective actions	03.05

Most Common Violations or Findings

Most Common Violations or Findings

Top 10 Violations by Control

- 2022-2023 data per 2024 NEI Cyber Workshop
- What drives the number of violations includes
  - How detailed and accurate the program documentation is
  - How well it's followed
  - How repeatable the results are
  - How well the individuals doing the work understand it



Top 10 Violations by Control			
Rank	# of Violations	Control	Description
1	17	D5.1	Unnecessary Services and Applications
2	16	D12	Evaluate and Manage Cyber Risk
3	15	D10.3	Baseline Configuration
4	15	E6	Defense in Depth
5	14	E3.4	Monitoring Tools and Techniques
6	10	D4.3	Password Requirements
7	9	D11.2	Supply Chain Protections
8	7	E2.1	Access Authorization
9	7	D1.17	Wireless Access Restrictions
10	6	E10.5	Security Impact Analysis

Cybersecurity Audits & Compliance Areas

Most Common Violations or Findings

Unnecessary Services and Applications

CAUSE

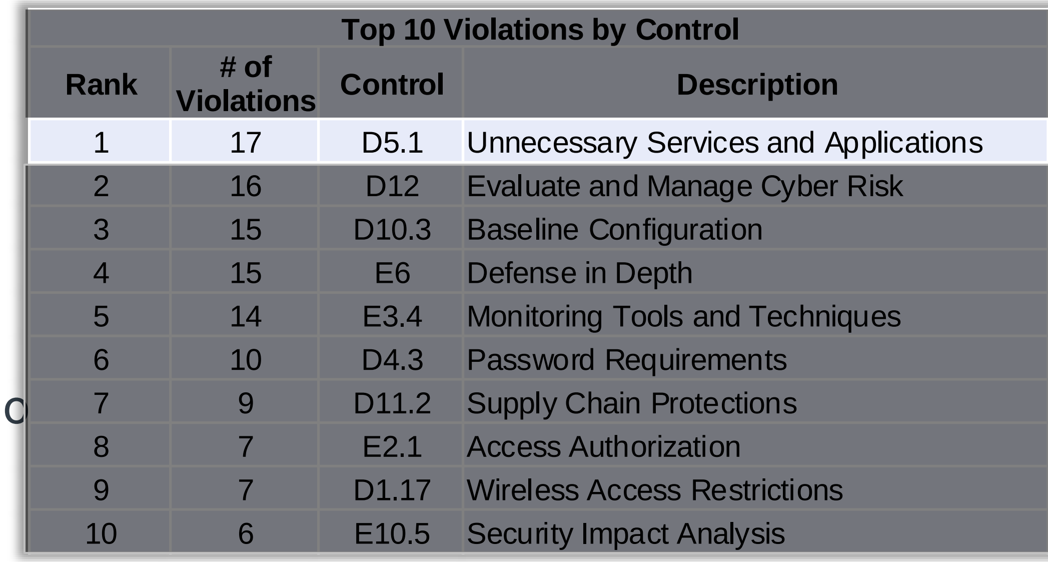
- Enabled Services and Features not needed during operation or maintenance
- Installed & Portable applications not used during operation or maintenance
- Enabled Application Options for functions not used during operatio or maintenance

WHERE

- Workstations, Servers, switches, encoders, terminal servers, Biometrics, Mercury, any device with a login

MITIGATION

- Document on a per device basis detailing why it’s enabled or installed
- Regular Verification of state
- Have a consistent approach

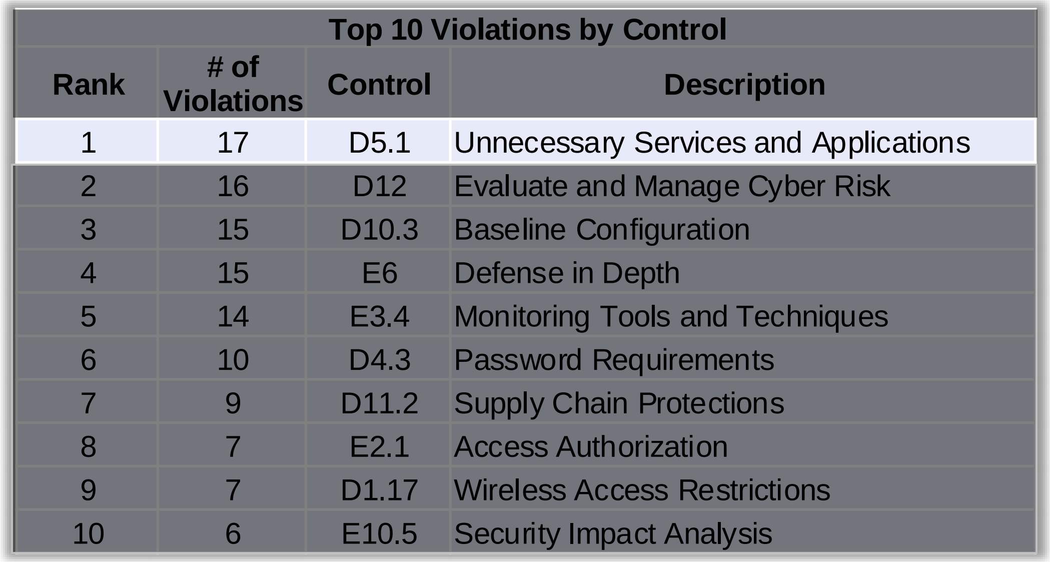


Top 10 Violations by Control

Rank	# of Violations	Control	Description
1	17	D5.1	Unnecessary Services and Applications
2	16	D12	Evaluate and Manage Cyber Risk
3	15	D10.3	Baseline Configuration
4	15	E6	Defense in Depth
5	14	E3.4	Monitoring Tools and Techniques
6	10	D4.3	Password Requirements
7	9	D11.2	Supply Chain Protections
8	7	E2.1	Access Authorization
9	7	D1.17	Wireless Access Restrictions
10	6	E10.5	Security Impact Analysis

Most Common Violations or Findings

Unnecessary Services and Applications



Top 10 Violations by Control			
Rank	# of Violations	Control	Description
1	17	D5.1	Unnecessary Services and Applications
2	16	D12	Evaluate and Manage Cyber Risk
3	15	D10.3	Baseline Configuration
4	15	E6	Defense in Depth
5	14	E3.4	Monitoring Tools and Techniques
6	10	D4.3	Password Requirements
7	9	D11.2	Supply Chain Protections
8	7	E2.1	Access Authorization
9	7	D1.17	Wireless Access Restrictions
10	6	E10.5	Security Impact Analysis

TIPS

- Automate these checks (CBA Tool, EZ-Audit, Powershell/scripts). It saves time, more frequent, more accurate, and provides repeatable results

TRIPS

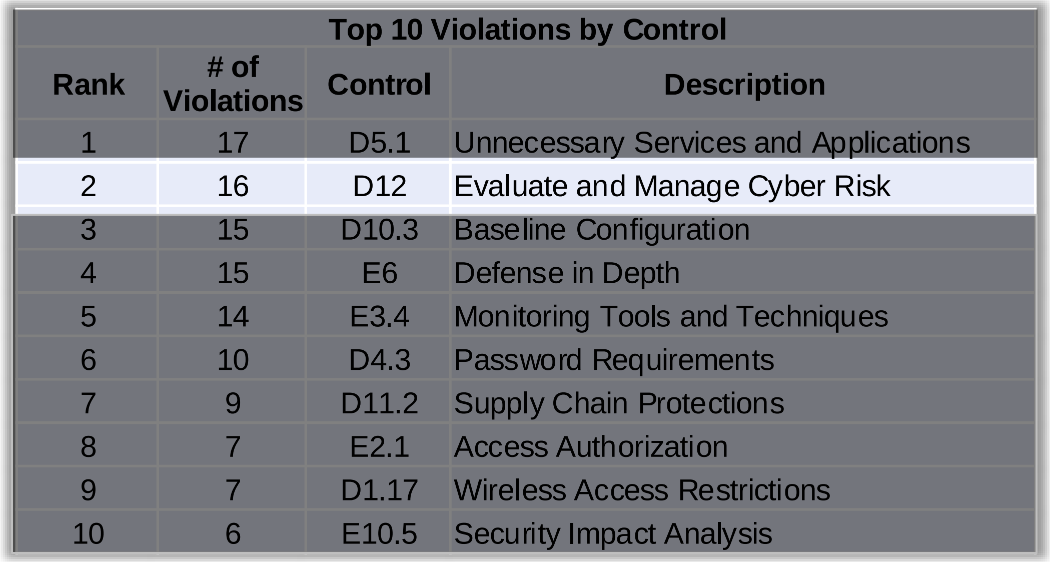
- Restoring a backup or rolling back a policy/configuration can revert back to an undocumented state
- Troubleshooting cleanup – often times tools are installed or services are enabled during troubleshooting and the excitement or complexity of the fix may leave you in an undocumented state
- Hardware replacements / RMA – That new hardware is from a different time and place. It could have different firmware or factory default settings that no one even realized. Review your documentation to verify its state
- Windows (and other vendor) updates can change the state of a service and will change the version of files and applications on your system. In some cases your can reapply the change but in some cases you may just need to update your documentation

What We're Doing

- Refreshing our Disabled Services GPO's
- A lot of CBA Tool development
  - Refining Windows 10 and Server 2019 rules
  - Developing Windows 11 and Server 2022 rules
- Automated Deployment efforts

Most Common Violations or Findings

Evaluate and Manage Cyber Risk



Top 10 Violations by Control			
Rank	# of Violations	Control	Description
1	17	D5.1	Unnecessary Services and Applications
2	16	D12	Evaluate and Manage Cyber Risk
3	15	D10.3	Baseline Configuration
4	15	E6	Defense in Depth
5	14	E3.4	Monitoring Tools and Techniques
6	10	D4.3	Password Requirements
7	9	D11.2	Supply Chain Protections
8	7	E2.1	Access Authorization
9	7	D1.17	Wireless Access Restrictions
10	6	E10.5	Security Impact Analysis

CAUSE

- Not monitoring software and hardware vulnerabilities
- Not upgrading and updating software
- Not maintaining cyber controls
- Not regularly validating controls
- Not understanding your interdependencies

WHERE

- Workstations, Servers, switches, encoders, terminal servers, Biometrics, Mercury, any device with a login

MITIGATION

- Review CVEs and Manufacturer product notifications
- Perform your **Risk = Hazard x Exposure x Vulnerability** analysis – more later

Most Common Violations or Findings

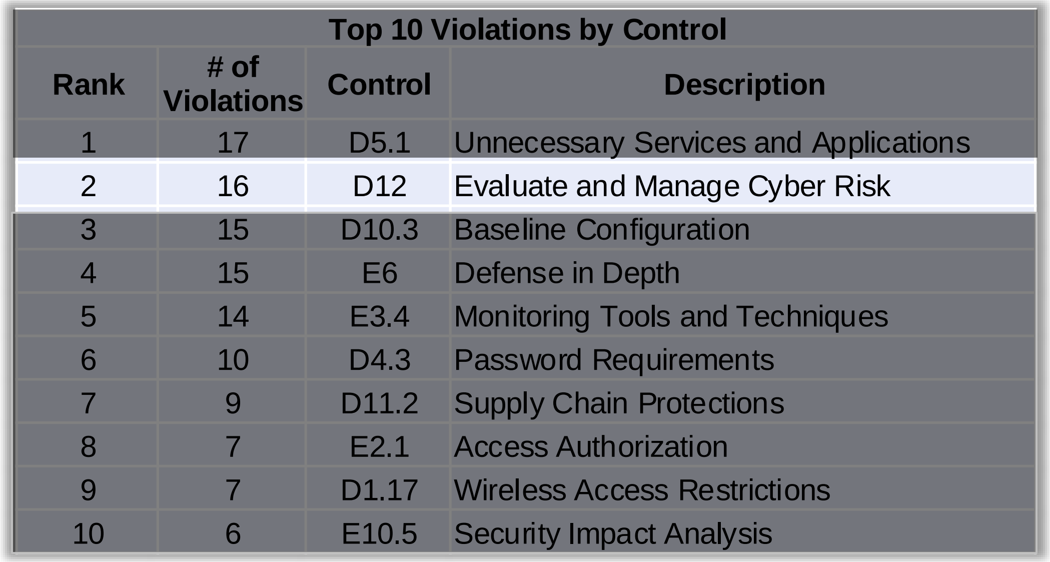
Evaluate and Manage Cyber Risk

TIPS

- Better understand the system and components
- Monitor software versions and CVE postings for that software
  - Nessus credentialed scans will give you a list of every software version you have and if it has a vulnerability
  - Read new version Release Notes from your vendors
- Documenting your Data flows, mitigating controls, interdependencies
  - Nessus port scans findings

TRIPS

- A decision is made not to upgrade something because of fear alone
- Incorrectly quantifying a risk because you misunderstanding the hazard, exposure, or vulnerability
- Unknown hazards / exposures / vulnerabilities
  - Update Nessus!



Top 10 Violations by Control			
Rank	# of Violations	Control	Description
1	17	D5.1	Unnecessary Services and Applications
2	16	D12	Evaluate and Manage Cyber Risk
3	15	D10.3	Baseline Configuration
4	15	E6	Defense in Depth
5	14	E3.4	Monitoring Tools and Techniques
6	10	D4.3	Password Requirements
7	9	D11.2	Supply Chain Protections
8	7	E2.1	Access Authorization
9	7	D1.17	Wireless Access Restrictions
10	6	E10.5	Security Impact Analysis

What We're Doing

- Expanding our documentation for services and features
- Working to improve our hardening stance and documentation
- Expanded/improved our System Subsystem Design Document (SSDD)

Most Common Violations or Findings

Baseline Configuration

CAUSE

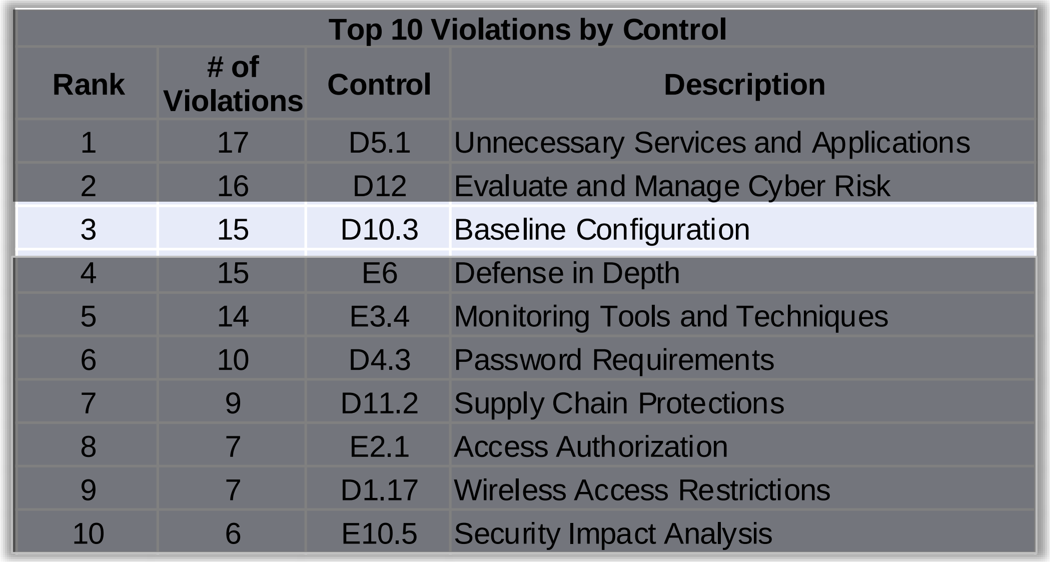
- Changes can be how a program is configured, what version of executables are being used, or what hardware is installed. Unknowns in any of these is a loss of configuration management
- Software is upgraded, patch is applied, software is reconfigured. Dip switches are changed

WHERE

- Workstations, Servers, switches, encoders, terminal servers, Biometrics, Mercury, any device with a login

MITIGATION

- Document everything!!!
  - File versions, firmware versions, hardware versions
  - Switch positions, dip switch settings,
  - Application settings, services settings, registry settings, config file settings



Top 10 Violations by Control

Rank	# of Violations	Control	Description
1	17	D5.1	Unnecessary Services and Applications
2	16	D12	Evaluate and Manage Cyber Risk
3	15	D10.3	Baseline Configuration
4	15	E6	Defense in Depth
5	14	E3.4	Monitoring Tools and Techniques
6	10	D4.3	Password Requirements
7	9	D11.2	Supply Chain Protections
8	7	E2.1	Access Authorization
9	7	D1.17	Wireless Access Restrictions
10	6	E10.5	Security Impact Analysis

Most Common Violations or Findings

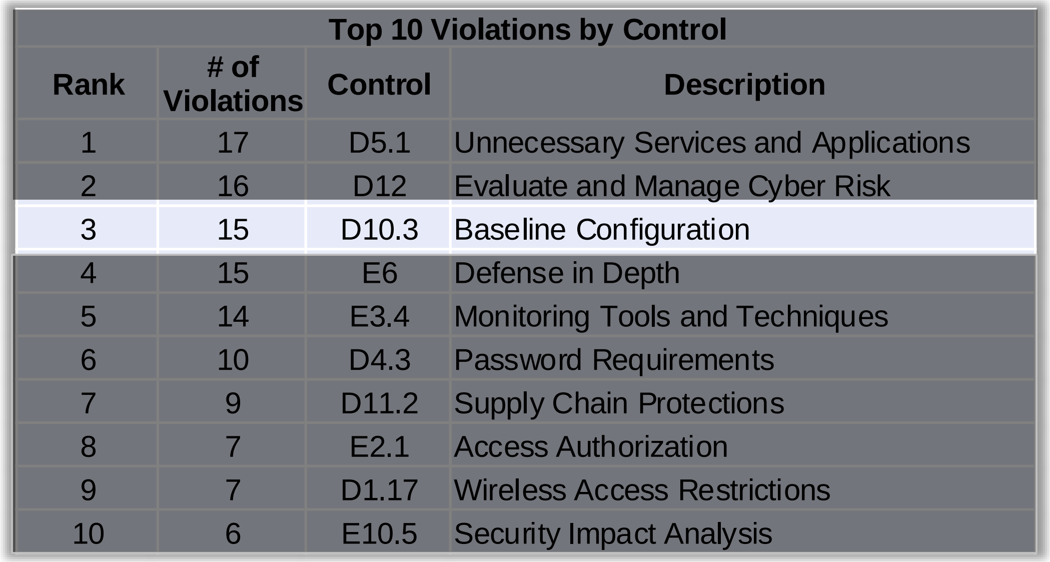
Baseline Configuration

TIPS

- Automate these checks (CBA Tool, EZ-Audit, Powershell/scripts). It saves time, more frequent, more accurate, and provides repeatable results.
- Review application interfaces to ensure you have documentation detailing every setting.
- Practice restoring devices on a Maintenance or Training system to help vet out processes and documentation.

TRIPS

- Changes made during Troubleshooting or investigation that don't get reversed to their original state.
- Changes made during Upgrades. Some updates or newer versions of software could change settings
- Restoring a device to a previous back from before a change was made
- Hardware based settings differ on RMA'd Motherboards or other hardware. Be sure to reapply/revalidate bios or lifecycle controller settings after hardware replacement



Top 10 Violations by Control			
Rank	# of Violations	Control	Description
1	17	D5.1	Unnecessary Services and Applications
2	16	D12	Evaluate and Manage Cyber Risk
3	15	D10.3	Baseline Configuration
4	15	E6	Defense in Depth
5	14	E3.4	Monitoring Tools and Techniques
6	10	D4.3	Password Requirements
7	9	D11.2	Supply Chain Protections
8	7	E2.1	Access Authorization
9	7	D1.17	Wireless Access Restrictions
10	6	E10.5	Security Impact Analysis

What We're Doing

- Expanding our documentation for services and features
- Expanding the CBA Tool gather and validation checks
- Development of Cyber based Preliminary and Detailed Design packages/deliverables

Most Common Violations or Findings

Defense in Depth

CAUSE

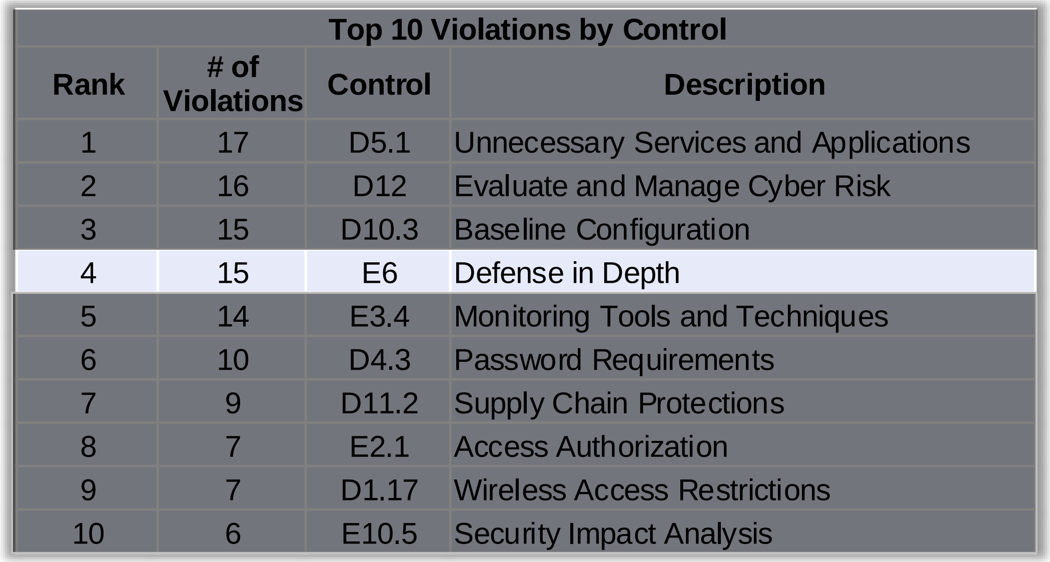
- Components or controls do not have layered protections or controls

WHERE

- Any components within the system

MITIGATION

- Regular validation of cyber controls
- Analysis of attack vectors to ensure multiple layers or protection exist for each attack



Top 10 Violations by Control			
Rank	# of Violations	Control	Description
1	17	D5.1	Unnecessary Services and Applications
2	16	D12	Evaluate and Manage Cyber Risk
3	15	D10.3	Baseline Configuration
4	15	E6	Defense in Depth
5	14	E3.4	Monitoring Tools and Techniques
6	10	D4.3	Password Requirements
7	9	D11.2	Supply Chain Protections
8	7	E2.1	Access Authorization
9	7	D1.17	Wireless Access Restrictions
10	6	E10.5	Security Impact Analysis

Most Common Violations or Findings

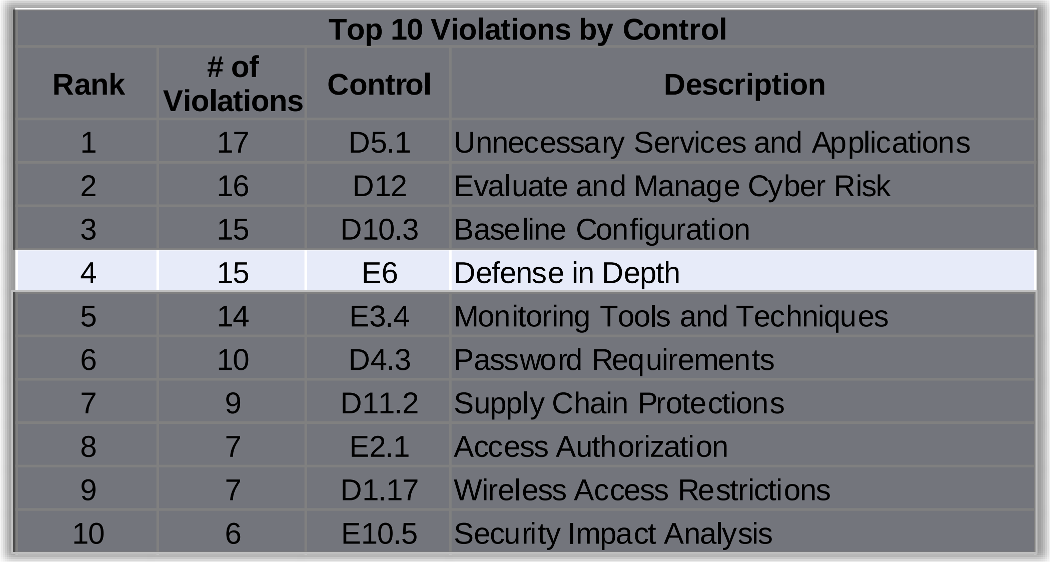
Defense in Depth

TIPS

- Don't forget Physical protection when evaluating digital assets
- Consider hardware capabilities when evaluating risk. Slower, less powerful devices, even if compromised, may not be able to affect the overall system dramatically enough to affect overall functionality.
- VLAN and other component segregation utilizing Access control Lists can mitigate the affects of a compromised device within the overall system.

TRIPS

- Temporarily disabled controls
- Legacy hardware retired in place, and still powered
- Last minute changes during transition or troubleshooting
- Additions to the system after initial installation



Top 10 Violations by Control			
Rank	# of Violations	Control	Description
1	17	D5.1	Unnecessary Services and Applications
2	16	D12	Evaluate and Manage Cyber Risk
3	15	D10.3	Baseline Configuration
4	15	E6	Defense in Depth
5	14	E3.4	Monitoring Tools and Techniques
6	10	D4.3	Password Requirements
7	9	D11.2	Supply Chain Protections
8	7	E2.1	Access Authorization
9	7	D1.17	Wireless Access Restrictions
10	6	E10.5	Security Impact Analysis

What We're Doing

- Designing systems with multiple levels of protection
- Only enabling communications between devices that need to communicate with each other.
- Following best practices during configuration and hardening.

Most Common Violations or Findings

Monitoring Tools and Techniques

CAUSE

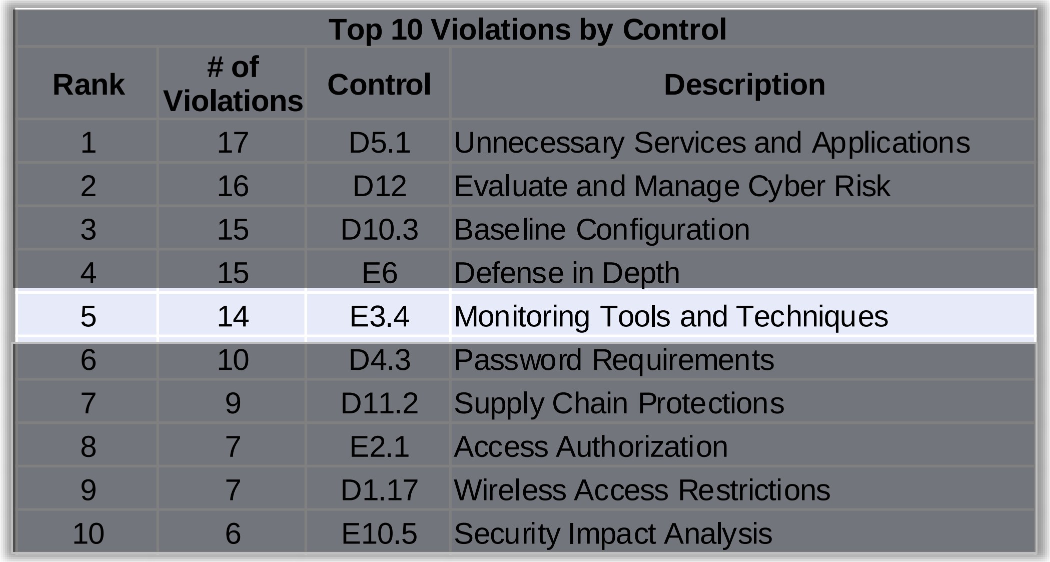
- Devices are not monitored to ensure they are functioning as designed/expected.
- Troubleshooting tools are not present on the system
- Tools are present on the system but their use is not documented to a degree that warrants their presence.

WHERE

- Workstations, Servers, Storage repositories

MITIGATION

- Documentation of all diagnostic tools and how/when they are to be used on the system.



Top 10 Violations by Control

Rank	# of Violations	Control	Description
1	17	D5.1	Unnecessary Services and Applications
2	16	D12	Evaluate and Manage Cyber Risk
3	15	D10.3	Baseline Configuration
4	15	E6	Defense in Depth
5	14	E3.4	Monitoring Tools and Techniques
6	10	D4.3	Password Requirements
7	9	D11.2	Supply Chain Protections
8	7	E2.1	Access Authorization
9	7	D1.17	Wireless Access Restrictions
10	6	E10.5	Security Impact Analysis

Most Common Violations or Findings

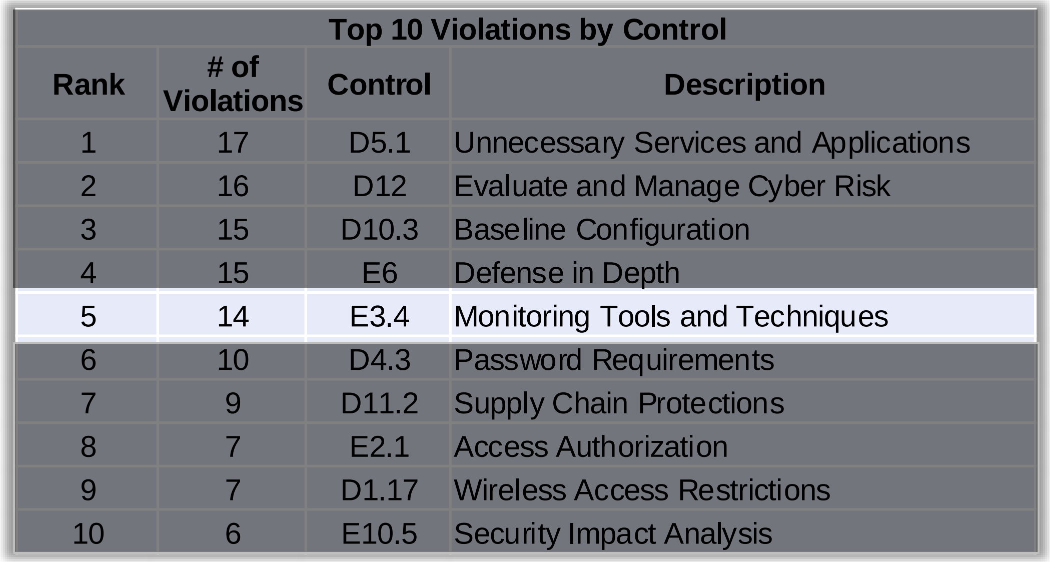
Monitoring Tools and Techniques

TIPS

- Document any Monitoring or diagnostic tools that is installed on the system

TRIPS

- Leaving undocumented monitoring tools on the system.
- Installing temporary tools or diagnostic programs on the system without updating documentation or removing the tools/apps afterwards
- “portable” applications or programs are placed on a system but will not show up as “Installed” through traditional scanning



Top 10 Violations by Control

Rank	# of Violations	Control	Description
1	17	D5.1	Unnecessary Services and Applications
2	16	D12	Evaluate and Manage Cyber Risk
3	15	D10.3	Baseline Configuration
4	15	E6	Defense in Depth
5	14	E3.4	Monitoring Tools and Techniques
6	10	D4.3	Password Requirements
7	9	D11.2	Supply Chain Protections
8	7	E2.1	Access Authorization
9	7	D1.17	Wireless Access Restrictions
10	6	E10.5	Security Impact Analysis

What We’re Doing

- Improving Documentation

Most Common Violations or Findings

Password Requirements

CAUSE

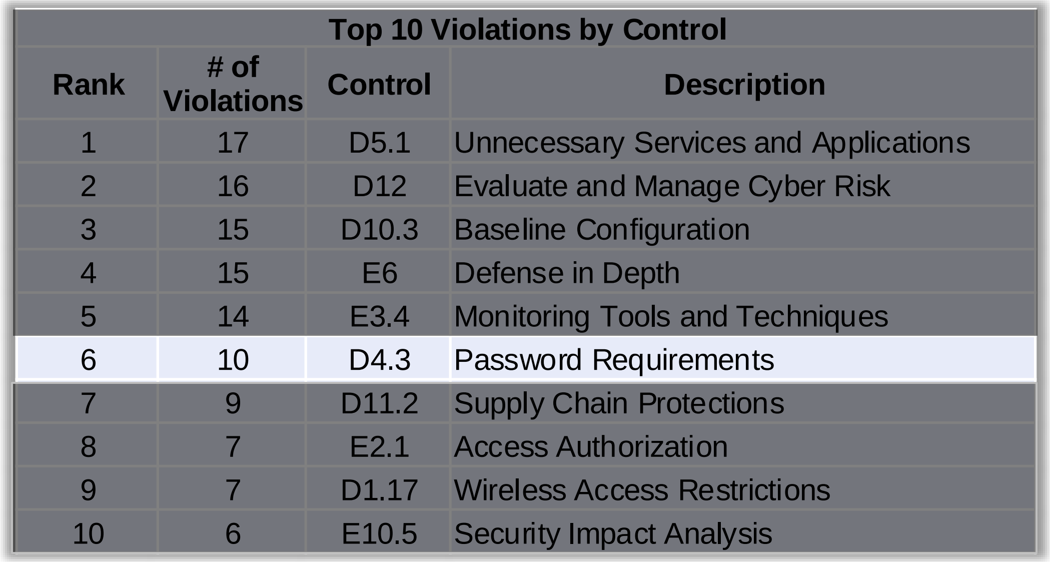
- Passwords not being changed at required intervals
- Accounts being classified incorrectly as not needing Password changes

WHERE

- Workstations, Servers, switches, encoders, terminal servers, Biometrics, Mercury, any device with a login

MITIGATION

- Classify all accounts as user accounts or service accounts.
  - Any account a user would log into should be changed at some interval.
  - Any account the system uses but users do not log into are service accounts and would not require a regular password change
- Enable Password complexity and length restrictions where technically feasible



Top 10 Violations by Control

Rank	# of Violations	Control	Description
1	17	D5.1	Unnecessary Services and Applications
2	16	D12	Evaluate and Manage Cyber Risk
3	15	D10.3	Baseline Configuration
4	15	E6	Defense in Depth
5	14	E3.4	Monitoring Tools and Techniques
6	10	D4.3	Password Requirements
7	9	D11.2	Supply Chain Protections
8	7	E2.1	Access Authorization
9	7	D1.17	Wireless Access Restrictions
10	6	E10.5	Security Impact Analysis

Most Common Violations or Findings

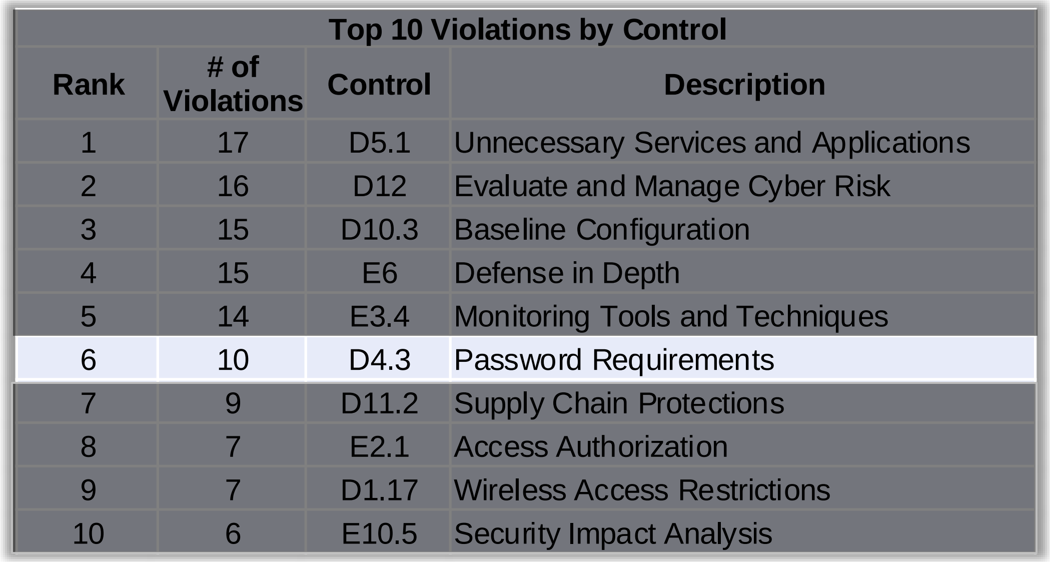
Password Requirements

TIPS

- Some firmware or software updates will add password length or functional capabilities. Re-evaluate each component after an update.

TRIPS

- Not changing passwords per procedure
- Not documenting accounts that should not have their password changed
- Not documenting passwords correctly after a change
- Restoring a system after changing a password and not changing the password again to match documentation



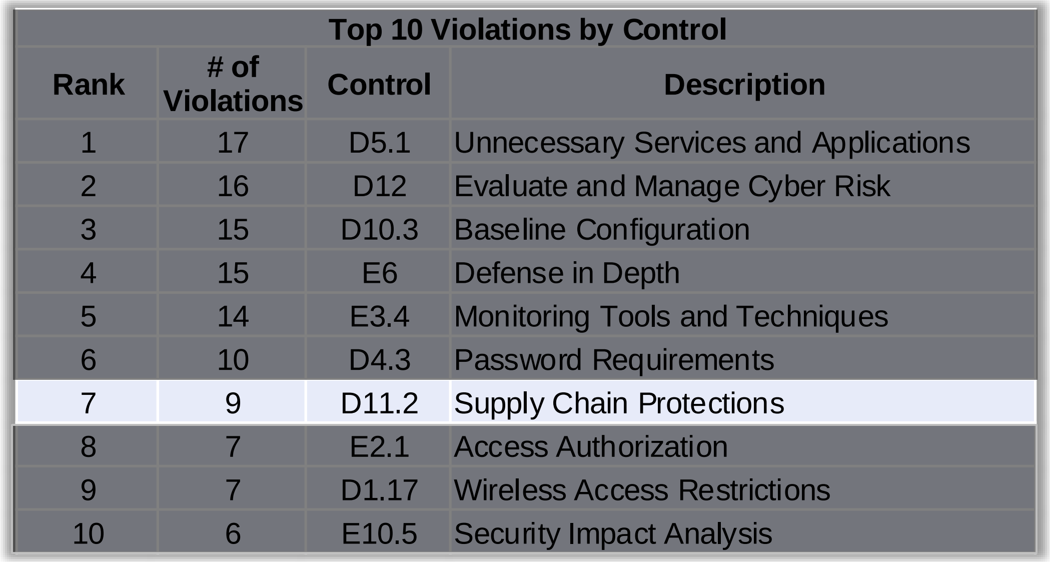
Top 10 Violations by Control			
Rank	**# of Violations**	**Control**	**Description**
1	17	D5.1	Unnecessary Services and Applications
2	16	D12	Evaluate and Manage Cyber Risk
3	15	D10.3	Baseline Configuration
4	15	E6	Defense in Depth
5	14	E3.4	Monitoring Tools and Techniques
6	10	D4.3	Password Requirements
7	9	D11.2	Supply Chain Protections
8	7	E2.1	Access Authorization
9	7	D1.17	Wireless Access Restrictions
10	6	E10.5	Security Impact Analysis

What We're Doing

- Improving Documentation
- Implementing Password vaults

Most Common Violations or Findings

Supply Chain Protections



Top 10 Violations by Control			
Rank	# of Violations	Control	Description
1	17	D5.1	Unnecessary Services and Applications
2	16	D12	Evaluate and Manage Cyber Risk
3	15	D10.3	Baseline Configuration
4	15	E6	Defense in Depth
5	14	E3.4	Monitoring Tools and Techniques
6	10	D4.3	Password Requirements
7	9	D11.2	Supply Chain Protections
8	7	E2.1	Access Authorization
9	7	D1.17	Wireless Access Restrictions
10	6	E10.5	Security Impact Analysis

CAUSE

- Bad Signature updates (Old Mcafee, Symantec)
- Malware from the Solarwinds' Orion update in 2020
- Corrupt system file within CrowdStrike weeks ago

WHERE

- Everything we buy
- Software, Upgrades, and Patches provided by Manufacturers

MITIGATION

- Use Trusted Vendors and monitor them
  - Recent issues/news
  - QA programs focused on vendors using good practices
- Validate the software through hash checks or fingerprints for vendor provided content
- Validate functionality on a maintenance system before installing on production

Most Common Violations or Findings

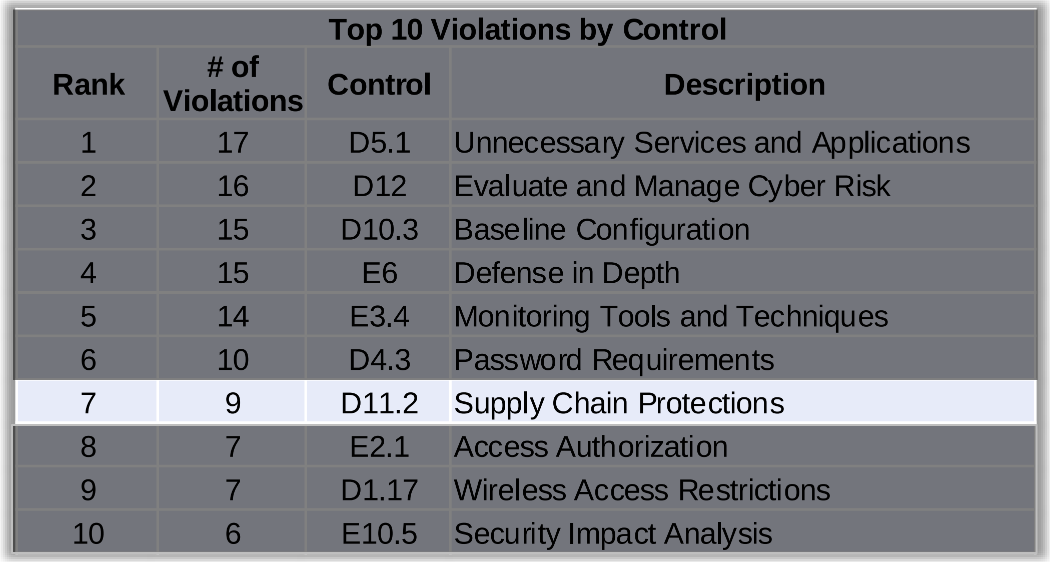
Supply Chain Protections

TIPS

- Verify your MD5 and SHA checksums on all downloaded files
- Don’t install content updates until they are tested with some burn-in time

TRIPS

- Downloading files from untrusted websites
- Using/running files without verifying their Hash
- In some cases the act of moving files through the scanning



Top 10 Violations by Control			
Rank	# of Violations	Control	Description
1	17	D5.1	Unnecessary Services and Applications
2	16	D12	Evaluate and Manage Cyber Risk
3	15	D10.3	Baseline Configuration
4	15	E6	Defense in Depth
5	14	E3.4	Monitoring Tools and Techniques
6	10	D4.3	Password Requirements
7	9	D11.2	Supply Chain Protections
8	7	E2.1	Access Authorization
9	7	D1.17	Wireless Access Restrictions
10	6	E10.5	Security Impact Analysis

What We’re Doing

- Using vendors that follow good practices
- All updates or upgrades provided by Mirion will include checksums to validate

Most Common Violations or Findings

Access Authorization

CAUSE

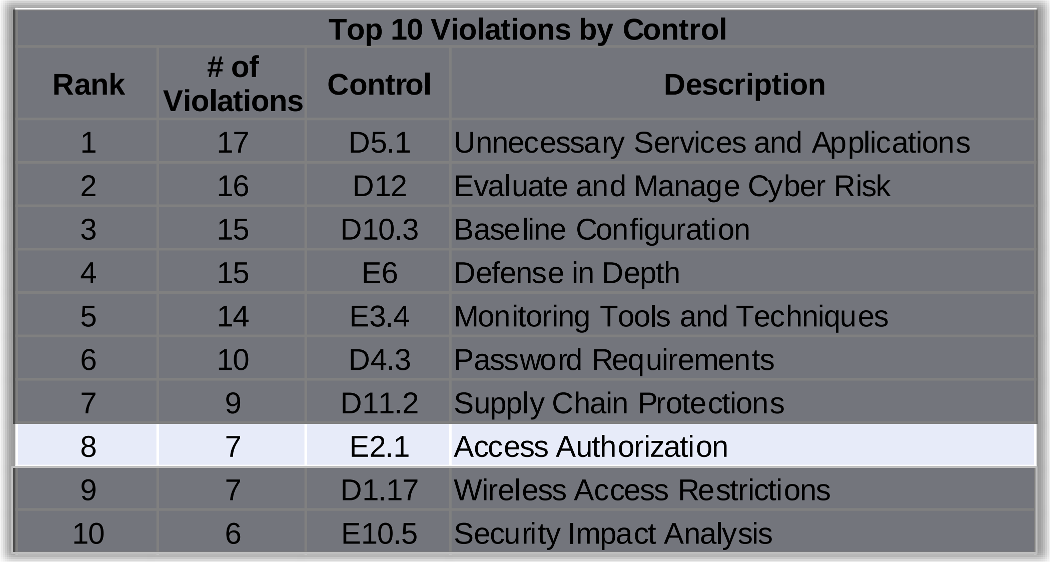
- Violations in access

WHERE

- Procedures
- Training

MITIGATION

- Documentation and training of access policies and procedures



Top 10 Violations by Control			
Rank	**# of Violations**	**Control**	**Description**
1	17	D5.1	Unnecessary Services and Applications
2	16	D12	Evaluate and Manage Cyber Risk
3	15	D10.3	Baseline Configuration
4	15	E6	Defense in Depth
5	14	E3.4	Monitoring Tools and Techniques
6	10	D4.3	Password Requirements
7	9	D11.2	Supply Chain Protections
8	7	E2.1	Access Authorization
9	7	D1.17	Wireless Access Restrictions
10	6	E10.5	Security Impact Analysis

Most Common Violations or Findings

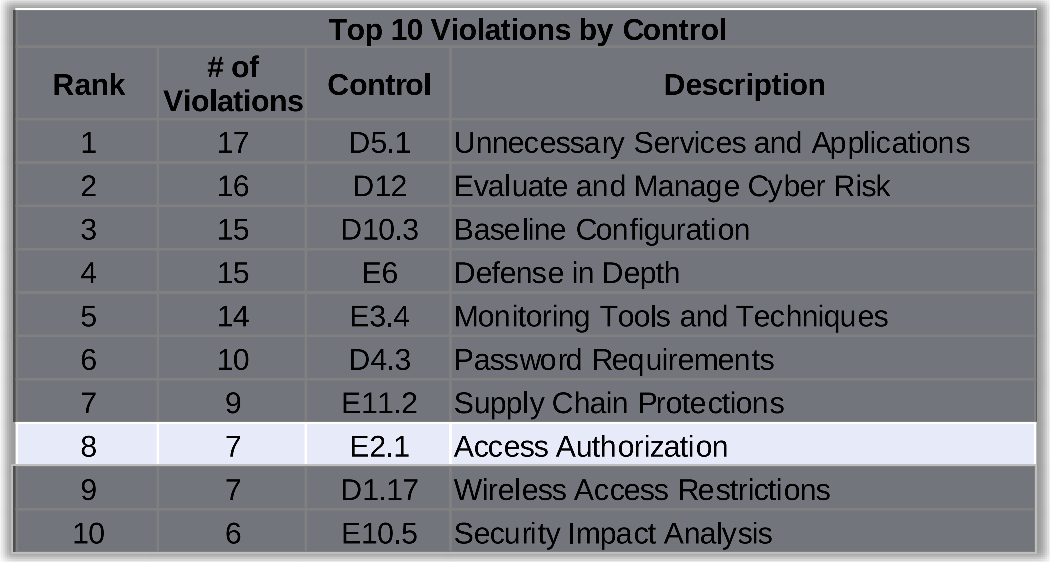
Access Authorization

TIPS

- Know your procedures
- Trust but verify

TRIPS

- Assumptions



Top 10 Violations by Control			
Rank	# of Violations	Control	Description
1	17	D5.1	Unnecessary Services and Applications
2	16	D12	Evaluate and Manage Cyber Risk
3	15	D10.3	Baseline Configuration
4	15	E6	Defense in Depth
5	14	E3.4	Monitoring Tools and Techniques
6	10	D4.3	Password Requirements
7	9	E11.2	Supply Chain Protections
8	7	E2.1	Access Authorization
9	7	D1.17	Wireless Access Restrictions
10	6	E10.5	Security Impact Analysis

What We're Doing

- Testing new versions of HID/Mercury hardware to ensure new versions of Mercury hardware works as expected

Most Common Violations or Findings

Wireless Access Restrictions

CAUSE

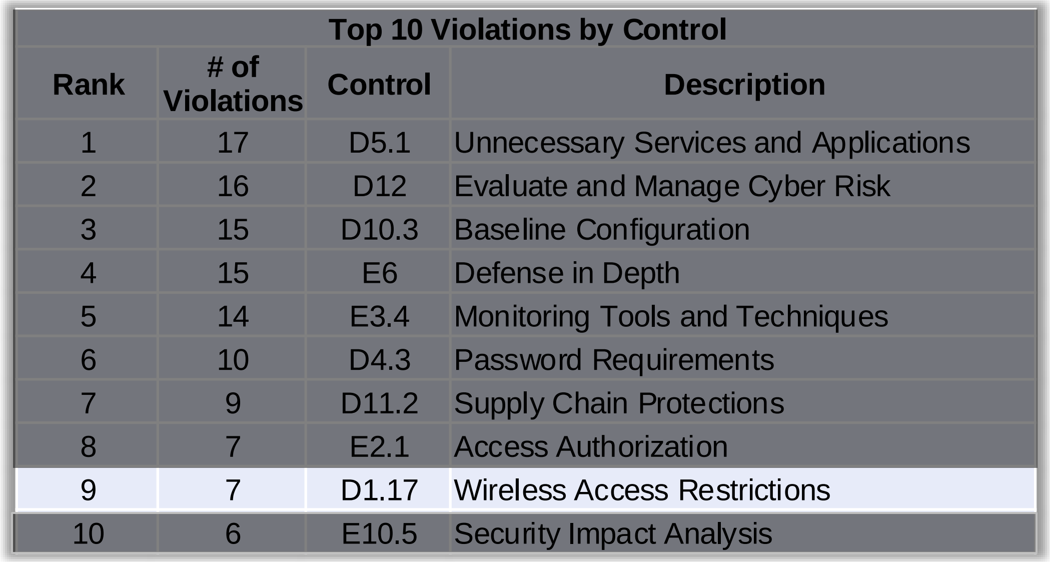
- Using wireless technology without proper protections

WHERE

- With Critical Digital Assets

MITIGATION

- Avoid when possible
- Updated guidance from NEI 08/09 rev 7, once ratified, will describe acceptable use and necessary protections for wireless use



Top 10 Violations by Control			
Rank	**# of Violations**	**Control**	**Description**
1	17	D5.1	Unnecessary Services and Applications
2	16	D12	Evaluate and Manage Cyber Risk
3	15	D10.3	Baseline Configuration
4	15	E6	Defense in Depth
5	14	E3.4	Monitoring Tools and Techniques
6	10	D4.3	Password Requirements
7	9	D11.2	Supply Chain Protections
8	7	E2.1	Access Authorization
9	7	D1.17	Wireless Access Restrictions
10	6	E10.5	Security Impact Analysis

What We're Doing

- Monitoring NEI 08/09 Rev 7 development
- Road mapping out the use of what wireless solutions where it makes sense and where

Most Common Violations or Findings

Security Impact Analysis

CAUSE

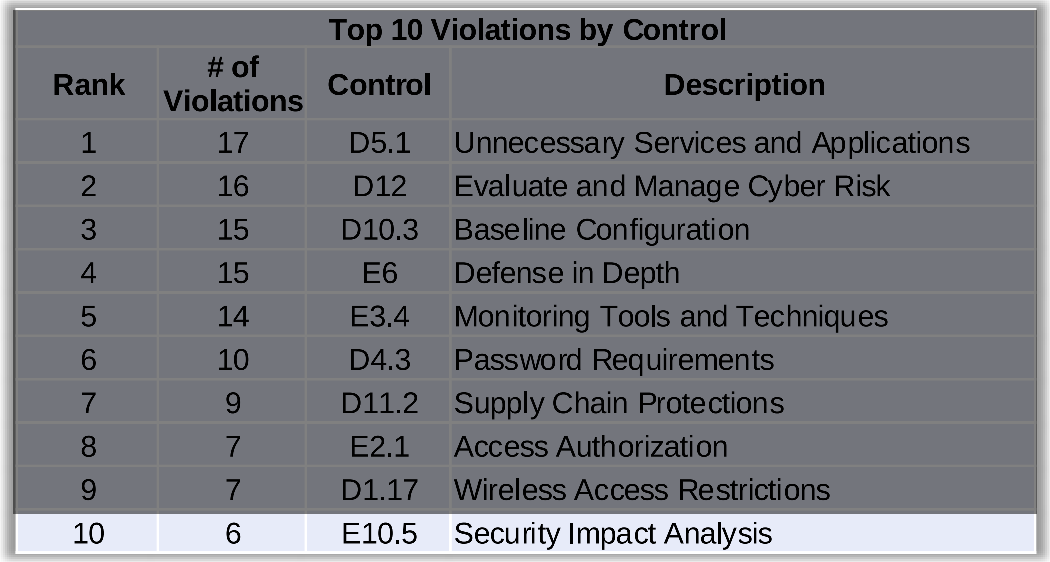
- A system or component failing
- A cyber control being disabled
- No support contracts in place
- Not maintaining hardware/software licensing

WHERE

- Subscription based services/components (VMWare/Trellix/etc)
- Equipment retired in place but still on
- EOL but required hardware/software

MITIGATION

- Maintain subscriptions, licenses, and support contracts
- Update software and hardware when EOL/EOS is identfied
- Spares on hand



Top 10 Violations by Control			
Rank	# of Violations	Control	Description
1	17	D5.1	Unnecessary Services and Applications
2	16	D12	Evaluate and Manage Cyber Risk
3	15	D10.3	Baseline Configuration
4	15	E6	Defense in Depth
5	14	E3.4	Monitoring Tools and Techniques
6	10	D4.3	Password Requirements
7	9	D11.2	Supply Chain Protections
8	7	E2.1	Access Authorization
9	7	D1.17	Wireless Access Restrictions
10	6	E10.5	Security Impact Analysis

Most Common Violations or Findings

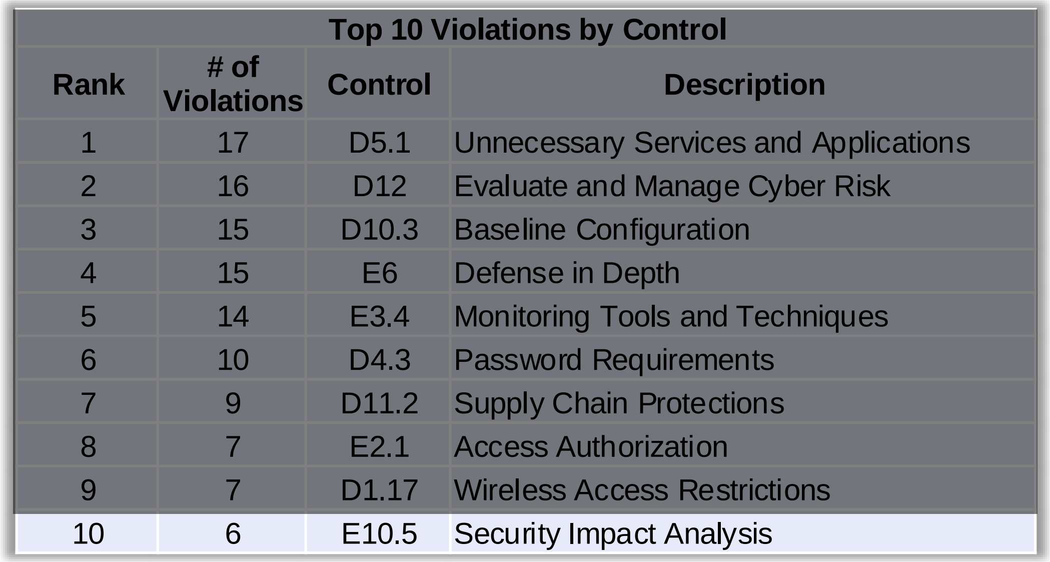
Security Impact Analysis

TIPS

- Document and monitor your license, subscription, and support contract end dates
- Be proactive with training
- Continue to develop your Risk and Impact plans to account for the unique and change landscape of technology and vendor/manufacturer practices
- Buy support in longer term agreements

TRIPS

- Not being aware of when equipment or software may be going end of life or end of support
- Not knowing when a vendors or manufacturer changes their licensing or renewal procedures
- Not having updated contact or support number before they are needed



Top 10 Violations by Control

Rank	# of Violations	Control	Description
1	17	D5.1	Unnecessary Services and Applications
2	16	D12	Evaluate and Manage Cyber Risk
3	15	D10.3	Baseline Configuration
4	15	E6	Defense in Depth
5	14	E3.4	Monitoring Tools and Techniques
6	10	D4.3	Password Requirements
7	9	D11.2	Supply Chain Protections
8	7	E2.1	Access Authorization
9	7	D1.17	Wireless Access Restrictions
10	6	E10.5	Security Impact Analysis

What We're Doing

- Life Cycle Management contracts
- Maintains some spare equipment

The Risk

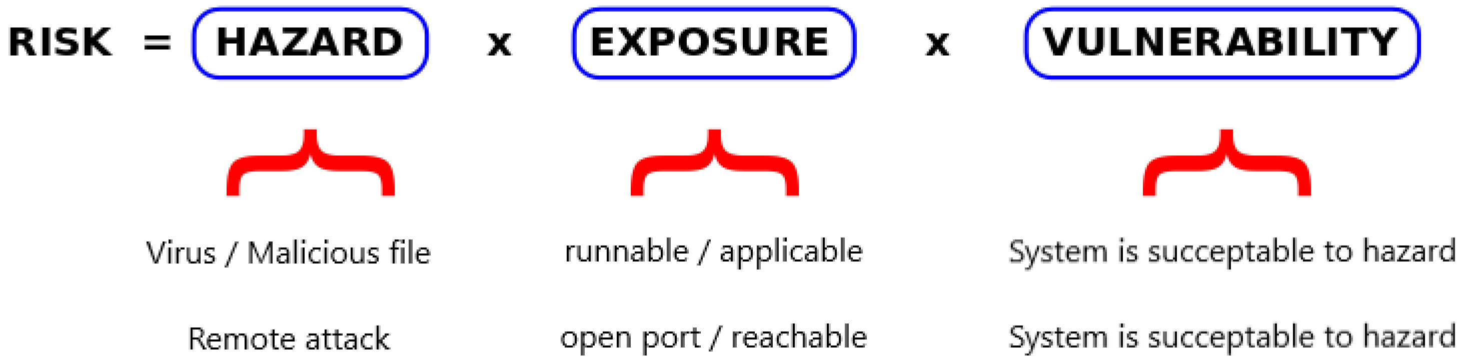
Vulnerable and Exposed vs Vulnerable but not Exposed

Vulnerable and Exposed vs Vulnerable but not Exposed

Risk is a value

If you think of it as simple math

- Zero risk is the goal



RISK = HAZARD x EXPOSURE x VULNERABILITY

HAZARD	EXPOSURE	VULNERABILITY
Virus / Malicious file	runnable / applicable	System is succeptable to hazard
Remote attack	open port / reachable	System is succeptable to hazard

MIRION TECHNOLOGIES

Audit Q&A