Building a Secure Foundation for Converged IT/OT Systems

Who Am I

Leslie Forbes

- Tenable – Field Product Manager
- Anti Virus field – 9 years
- Systems Administration & Network Security
- Embedded Systems enumeration & analysis
- Laser control technology

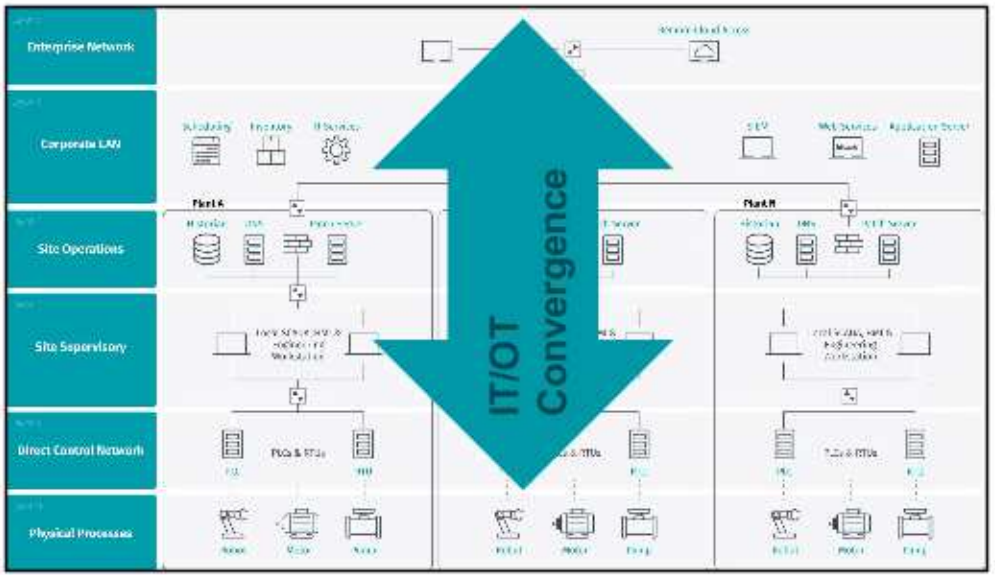
Topics

- Assume convergence
- Start with the basics
- Building blocks
- Q&A

What is in it for you?

- Better protected IT/OT systems
- Fewer security incidents to investigate
- Faster resolution of operational issues
- Improved IT/OT Security alignment

Assume IT/OT Convergence



tenable

OT is Under Attack

"23% have experienced a nation state attack."

"50% have experienced an attack against OT infrastructure that resulted in downtime."

"Only 20% have sufficient visibility into their attack surface."

Measuring OT Cyber Risks to the Business, February 2019, Ponemon Institute

tenable

OT Security Responsibility is Moving to IT

"By 2021, 70% of OT security will be managed directly by the CIO, CISO, or CSO departments, up from 35% today"[1]

"Due to a dearth of OT security skills, IT security teams are being asked to take ownership of OT security coordination, in many cases"[2]

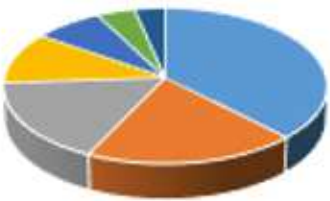
"Security teams in converging IT and OT organizations have limited visibility into OT assets; full inventories do not exist"[1]

1. Gartner: 2018 Strategic Roadmap for Integrated IT and OT Security, 3 May 2018
2. Gartner: Market Guide for Operation Technology Security, 2018, 30 July 2018

tenable

IT Tends to Set Policy, but OT Owns Controls

Who Sets Policy for Security of Control Systems?



- Chief Information Security Officer
- Other
- Unknown
- Chief Security Officer
- Chief Technology Officer
- Chief Operations Officer
- Corporate Risk Officer

Who is Responsible for Security Control Implementation around Control Systems?...

tenable

Adopt a Common Framework and Start with the Basics

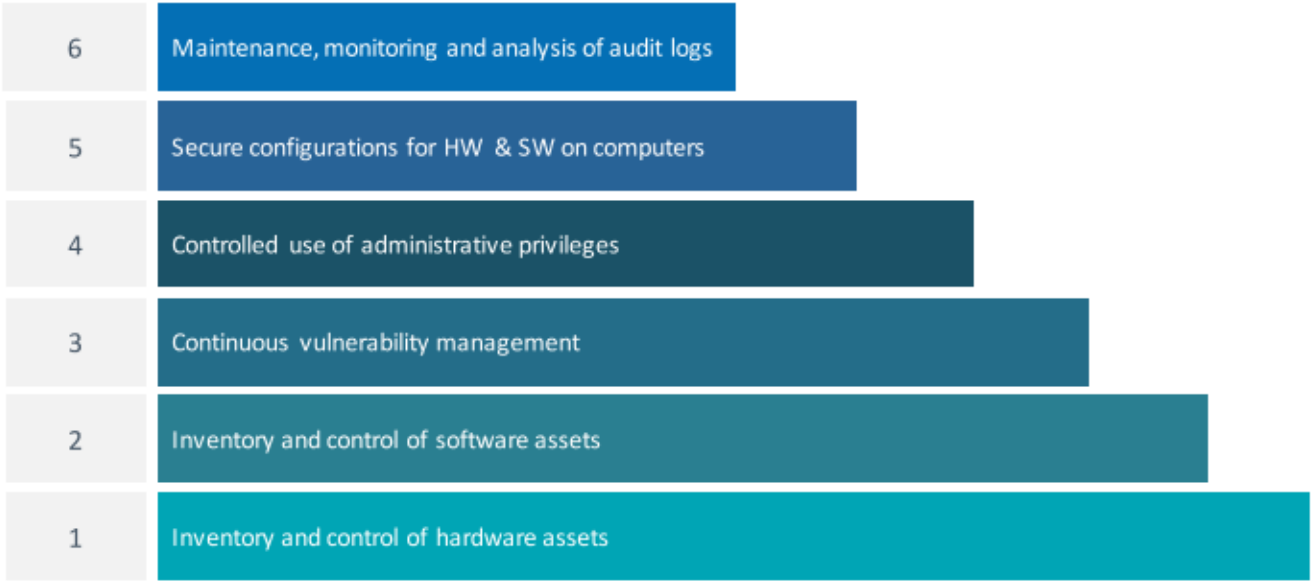
MANAGE CYBER RISK ACROSS THE IT/OT ATTACK SURFACE

Center for Internet Security: CIS Controls

Prioritized, well-vetted, and supported security actions to assess and improve security

tenable

Basic Controls



tenable

CIS Controls™

Implementation Guide for Industrial Security Controls

https://www.cisecurity.org/white-papers/cis-controls-implementation-guide-for-industrial-control-systems/

tenable

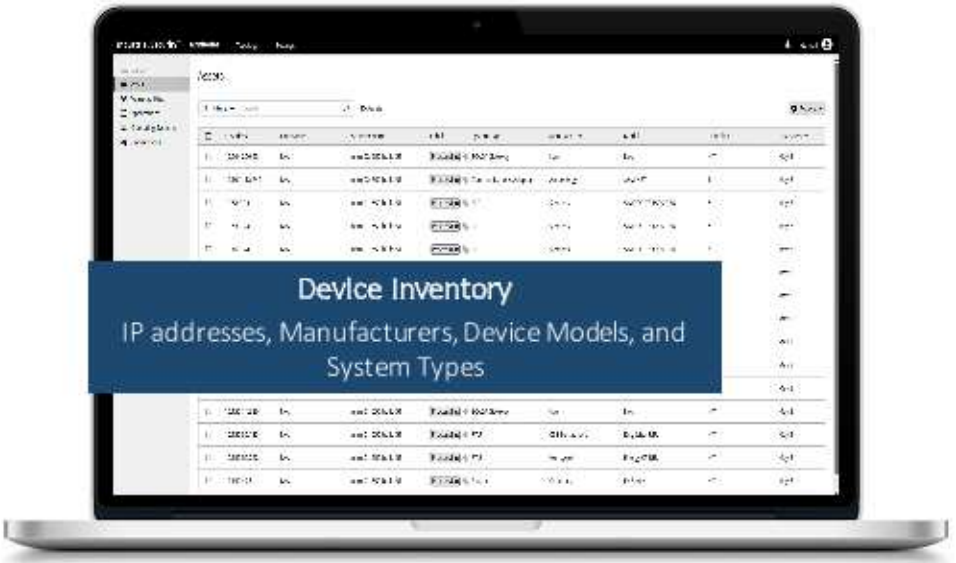
Inventory & Control of Hardware Assets

Selected Sub-Controls

- Utilize an active discovery tool
- Use a passive asset discovery tool
- Use DHCP logging to update asset inventory
- Address unauthorized assets

Selected ICS Considerations

- Passive methods to locate connected assets are preferred
- Follow approval processes for equipment modifications and acquisitions


Device Inventory
IP addresses, Manufacturers, Device Models, and System Types

tenable

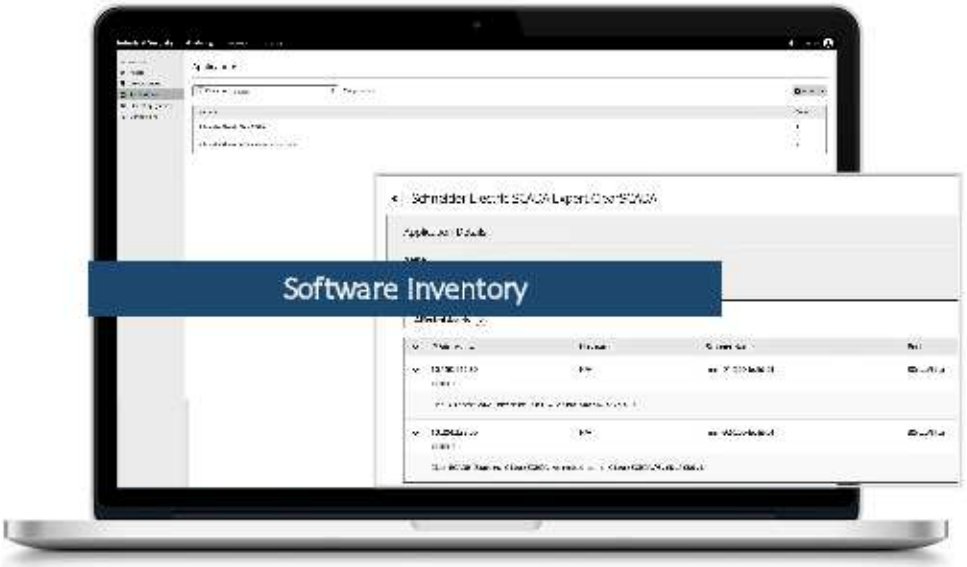
Inventory & Control of Software Assets

Selected Sub-Controls

- Maintain inventory of authorized software
- Ensure software is supported by vendor
- Utilize software inventory tools
- Address unapproved software
- Utilize application whitelisting

Selected ICS Considerations

- Large parts of ICS networks are comprised of devices too sensitive to scan
- Use application whitelisting only where feasible


Software Inventory

Continuous Vulnerability Management

Selected Sub-Controls

- Run automated vulnerability scanning tools
- Perform authenticated vulnerability scanning
- Deploy automated software patch management tools
- Utilize a risk rating

Selected ICS Considerations

- Scanning should only take place during planned maintenance or shutdowns
- Utilize an OEM vulnerability reporting service
- Utilize passive monitoring tools that correlate to known vulnerabilities


Vulnerabilities by Asset
See which assets are the most vulnerable

tenable

Controlled Use of Admin Privileges

Selected Sub-Controls

- Maintain an inventory of administrative accounts
- Change default passwords
- Use dedicated admin accounts
- Use dedicated workstations for all administration

Selected ICS Considerations

- When inventorying admin accounts, use automated tools only if known to not impact availability
- Use of dedicated machines or the use of isolation for admin machines may not apply

Secure Configurations for Computers

Selected Sub-Controls

- Establish security configurations
- Maintain secure images
- Implement automated configuration monitoring systems

Selected ICS Considerations

- Consider OEM and vendor recommendations
- Disable unused ports/services, change default accounts, update protocols, etc.
- All sub-controls apply

Maintenance, Monitoring… of Audit Logs

Selected Sub-Controls

- Utilize three synchronized time sources
- Activate audit logging
- Deploy SIEM or log analytic tools
- Regularly review logs

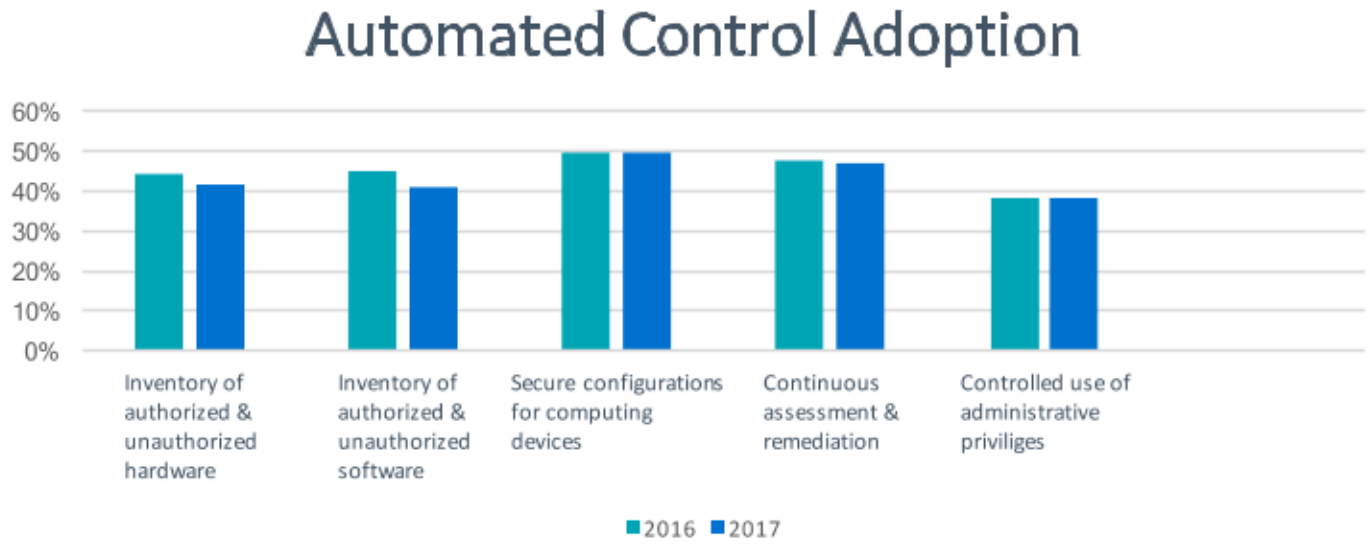
Selected ICS Considerations

- Gathering organizational information from logs may not apply
- Sub-controls related to aggregating and storing log data may not apply
- If use SIEM, ensure it supports ICS specific events

Common Control Foundation

Basic Controls	NIST CSF	NERC CIP v7
1. Inventory and control of hardware assets	ID.AM-1: Physical devices & systems are inventoried. ID.AM-3: Data flows are mapped PR.DS-3: Assets are formally managed	CIP-002-5.1 R1: BES cyber system categorization CIP-002-5.1 R2: BES cyber system categorization
2. Inventory and control of software assets	ID.AM-2:Software and applications are inventoried PR.DS-6: Integrity checking verifies software, etc.	CIP-010-2 R1: Configuration change management
3. Continuous vulnerability assessment	ID.RA-1: Vulnerabilities are identified & documented ID.RA-2: Threat & vulnerability information is received PR.IP-12: Vulnerability management plan is implemented DE.CM-8: Vulnerability scans are performed RS.MI-3: New vulnerabilities are mitigated or accepted	CIP-007-6 R2: Security patch management CIP-010-1 R3: Vulnerability assessments
4. Controlled use of administrative privileges	PR.AC-4: Access permissions are managed PR-AT-2: Privileged users understand responsibilities PR.MA-2: Remote maintenance prevents unauthorized access PR.PT-3: Access is controlled	CIP-004-6 R4: Access management program CIP-004-6 R5: Access revocation CIP-007-6 R4: Security event monitoring
5. Secure configurations for hardware	PR.IP-1: Baseline configurations are created and maintained	CIP-007-6 R2: Security patch management CIP-010-2 R2: Configuration monitoring
6. Log maintenance, analysis, and monitoring	PR.PT-1: Audit/log records are ... documented/reviewed DE.AE-3: Event data are collected & correlated DE.DP-1-5: Detection processes...	CIP-007-6 R4: Security event monitoring

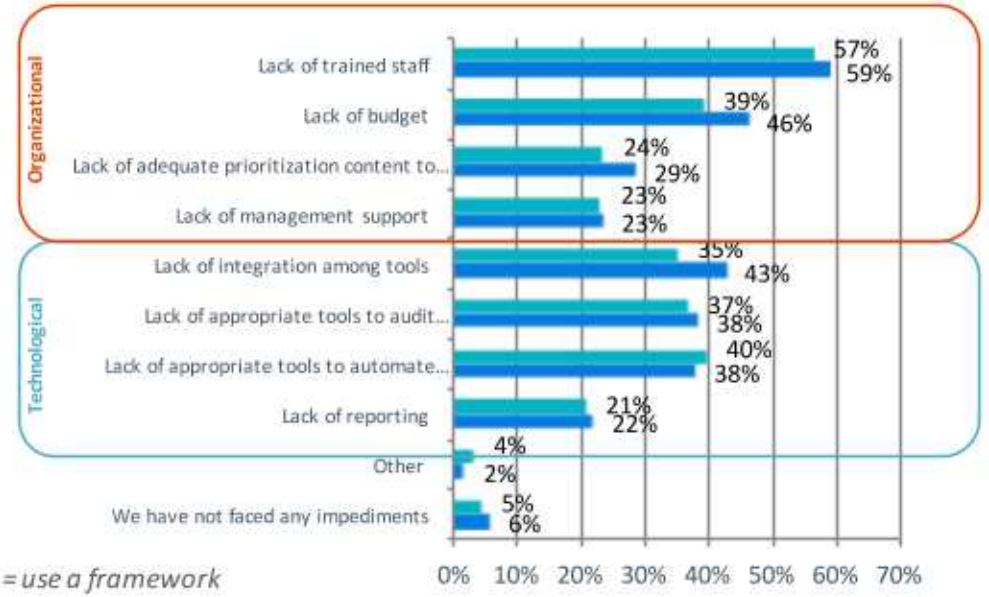
If you Need Improvement, you are not Alone



tenable

Implementation Impediments have Grown

What impediments have you encountered so far in implementing these cybersecurity frameworks?



tenable

Questions & Answers