OT System Cybersecurity Maturity

*60% of orgs are here (or before this step)**

*30% of orgs are here**

*10% of orgs are here**

Awareness
Recognize, commit to addressing the need for OT security

Visibility
Gain OT visibility via asset discovery, network mapping

"Oh Wow!"
Identify security blind spots, risks, governance gaps

Firefighting
Prioritize & address top blind spots, risks, governance gaps

Integration
Integrate & align OT with SOC/IT security program, tools, governance

Optimization
Harness OT security capabilities to drive operational resilience

Cybersecurity Assessment - Goals

- Should provide a non-invasive analysis of a customer's OT cybersecurity profile
- Should provide high-level view of a customer's cyber stance and provide direction to achieve cybersecurity objectives – such as following industry best practices or compliance with guidelines and standards including:
  - IEC-62443
  - NIST 800-82
  - NERC CIP
  - CFATS
  - ISO27001

Cybersecurity Assessment – Goals

During the Cyber Posture Assessment interviews, assessors conduct controls-related network discussions such as reviewing:

- ICS network architecture
- ICS components
- Cybersecurity procedures and policies
- Physical security procedures
- Cyber training levels of ICS personnel
- Documented incident response procedures
- Lifecycle management policies and procedures
- Role-based security practices

Cybersecurity Assessment - Use Cases

IT/OT/IoT Asset Discovery

- Gain detailed visibility into all IT, OT, and IoT managed & unmanaged assets to provide a strong foundation for effective OT asset management & cybersecurity

Lifecycle & Vulnerability Management

- Easily identify and manage the risks and vulnerabilities – such as missing critical patches, end-of-life indicators, and CVEs – affecting your managed and unmanaged assets
- See devices that are no longer supported, and effectively plan for obsolescence upgrades.

Cybersecurity Assessment - Use Cases

Audit & Compliance

- Easily, quickly, and effectively support audit requests and report compliance for your industrial network, resulting in greater confidence in your reporting, a reduced risk of failed audits, and stronger compliance and overall security posture.

M&A Due Diligence

- Conduct M&A due diligence on target companies' industrial networks more easily, quickly, and effectively, leading to a rapid fulfillment of M&A requirements and clear insight into operational risk posture — all while adhering to LOI specifications.

Cybersecurity Assessment - Use Cases

Incident Response

- Immediately arm responders with a full inventory and risk and vulnerability assessment of the compromised environment, thereby optimizing incident response efforts including impact assessments, scoping, and forensics for industrial networks.

Cybersecurity Assessment - Findings

Severity	Definition
Critical	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
Important	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.

Questions To Ask Yourself

- “Do you know all of the assets connected to your OT network?”
- “Can you tell me what your riskiest vulnerabilities are *right now?”*
- “When was the last time you did any sort of cybersecurity assessment?”
- “What vendors have access to your system? What is *their* cybersecurity policy?”

Schneider Electric's Global Cybersecurity Services Team

Global expertise and experience with Local Presence

6 regional hubs with Labs for engineering, testing, architecture replication, and solution development

17 district offices with field engineering hubs and consulting facilities.

50+ Cybersecurity Consultants with cross-industry certifications, experience, and expertise

150+ Field Service Engineers and technicians industry leading cybersecurity training

Life Is On Schneider Electric

Cybersecurity design & implementation portfolio

The solutions we design, and implement are flexible and customized to meet your specific needs and requirements. The most critical cybersecurity solution elements are defined in four categories.

Permit

Manage access to operations systems and information through network and physical controls.

- Authentication, Authorization, Accounting
- Multi-Factor Authentication
- Network Segmentation
- Secure Remote Access
- Physical Security

Protect

Implement specific controls as part of the operations systems for ongoing protection.

- Endpoint Protection, Anti-malware
- DLP, HIPS, Whitelisting
- Removeable Media Control
- Patch Management

Detect

Monitor the operating environment to detect and communicate threats.

- Security Information & Event Management (SIEM)
- Network Performance Monitoring
- Asset Identification
- Anomaly Detection
- Intrusion Detection

Respond

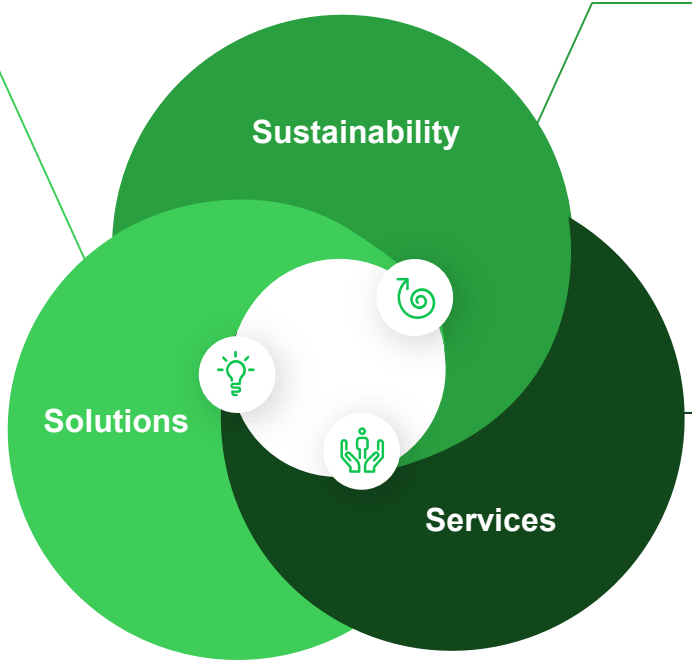
Develop procedures and systems to support rapid response to cyber incidents to contain and mitigate attacks.

- Backup / Disaster
- Recovery
- Forensics
- Incident Response

SE Cybersecurity Solutions & Services Capabilities

Platform

- **Central Cybersecurity Dashboards**
- Active Directory / User Management
- Endpoint Security
- **System Hardening**
- Configuration Management
- Security Data Enrichment (SIEM)
- **Secure Remote Access**
- Firewalls, Routers, and Switches
- Intrusion Detection/Prevention
- Network Segmentation
- Data Diodes
- **Anomaly Detection**
- **Automated Asset Inventory**
- Data Loss Prevention
- Endpoint Protection, AV, Whitelisting
- **Centralized Patch Management**
- Validated Patching & Updating
- Backup, Restore & Recovery
- Multi-Factor Authentication



Management

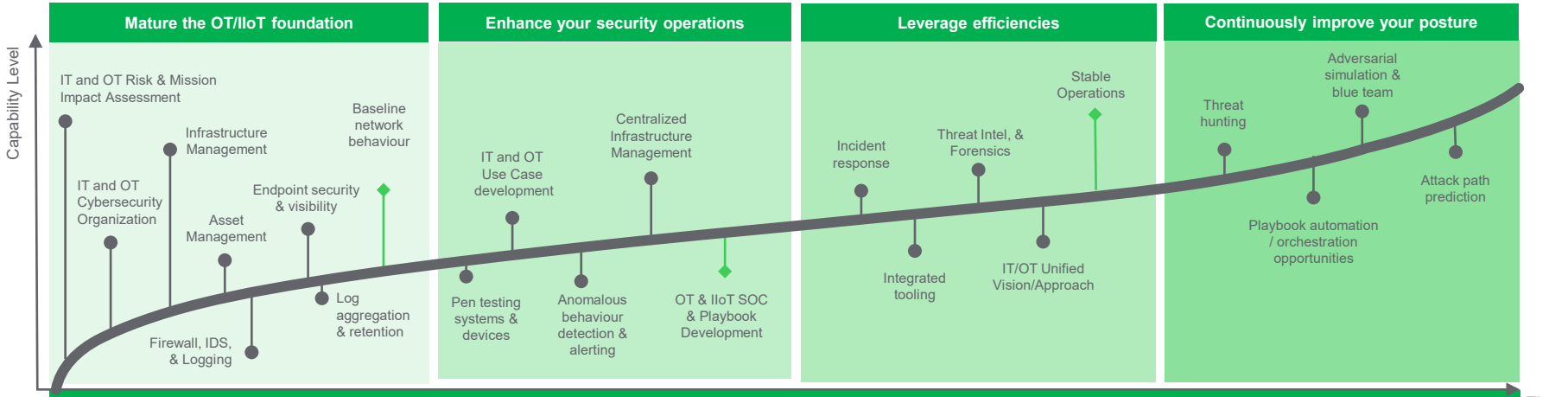
- **24x7 Managed Security Services**
- **Secure Patching & Updating**
- Secure Staging / FAT
- **Documentation Development/Mgmt.**
- Cybersecurity Lifecycle Management
- **Cybersecurity Role-Based Training**
- Incident Response & Recovery
- Network Scanning & Remediation
- **Cybersecurity Resiliency Planning**

Intelligence

- **Cybersecurity Risk Assessments**
- Product Operationalization
- **Virtual CISO Services**
- Compliance Gap Assessments
- Disaster Recovery Assessments
- **Secure Network Design**
- Professional Engineering Services
- **OT Cybersecurity Consulting**

IT and OT Cyber Platform Development Roadmap

Your path to a mature IT and OT Security Program requires solid foundations and increasingly sophisticated capabilities that allow organization to proactively monitor for and respond to threats across the global landscape. This process involves a multi-step, multi-tier approach that – when implemented, will position Vantage Group as the industry leader in IT and OT cyber defense capabilities.



Establish foundations
- Know & track what is connected to IT and OT
- Define IT and OT security perimeters & zones
- Define IT and OT visibility and pen testing
- Conduct baselines assessments
- Define security governance & training

Deploy programs
- Harden IT and OT Systems & Endpoints
- Deploy IT and OT Asset Management
- Operationalize Monitoring
- Deploy IT and OT Vulnerability & Patch Management Programs
- Deploy IT and OT BCP/DR programs

Expand programs
- Integrate IT and OT visibility into SOC
- Deploy OT/IIoT IR & OT/IIoT GRC Programs
- Pentest to validate IR processes
- Establish IT and OT Threat Hunting focus
- Develop & exercise IR playbooks

Mature programs
- Measure security value and ROI
- Exercise IR & determine pen testing effectiveness
- Threat modelling, simulations and predictive analytics

Success Story

“Next Level Cybersecurity as a Service” Platform

Global Data Center Company

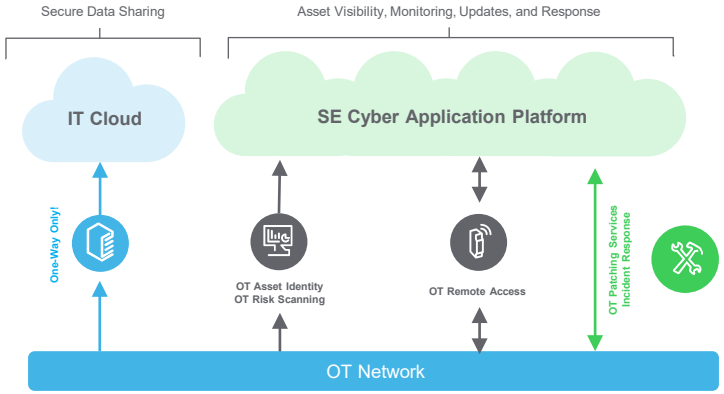
- ~90 Manufacturing Facilities, Central IT Organization

The Challenge

- Strong in Assessing and Access Controls, **struggle with “Protect, Detect, and Respond”**
- Multi-Vendor environment, many protocols, questionable OT network architecture
- No accurate way to view asset details or EOL status
- Poor authentication and logging of remote users
- Low data integrity from current OT tools
- Lack of trust leads to poor utilization of technology

The Challenge

- How do I share data with vendors securely?
- How do I execute patches without worrying about issues?
- How can I monitor threats and risks intelligently / centrally?
- How do I see all of my global assets and know their risks?



The Solution:

- Turn-Key Cybersecurity Management Platform with tool and user integration
- Curated, prioritized, and actionable alerts to keep the network safe w/ services follow-up
- Real time threat monitoring and asset identity of global OT infrastructure.
- SE Cyber Engineers provide monthly security hygiene reviews to Building, Power, and Automation teams

Get in touch **with our cybersecurity experts**

cybersecurity-services@se.com

Life Is On Schneider Electric

Life Is On | Schneider Electric