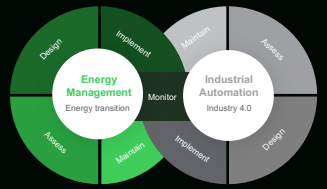
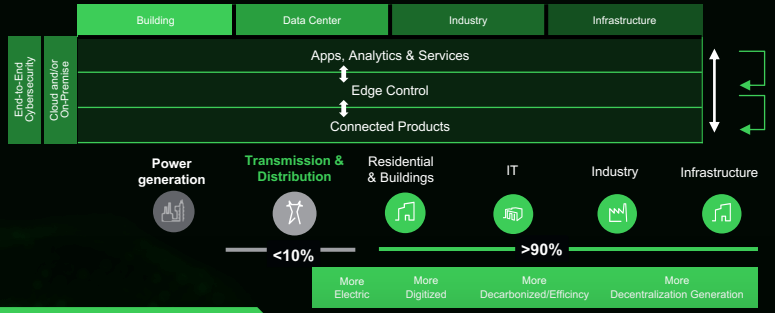

DIGITAL
Critical Infrastructure Protection (CIP)
Advanced Cybersecurity Solutions & Services
se.com/cybersecurity-services
Property of Schneider Electric
Life Is On
Schneider Electric

EcoStructure: end-to-end cybersecurity



EcoStruxure™
Innovation At Every Level



Addressing cybersecurity challenges on multiple levels

Cybersecurity solutions for operational lifecycle
Consulting, integration and managed security services

Technology partnerships
Situational awareness, compliance, change management, big data security

System deployment
Secure delivery of project and services during product or system deployment

End-to-End Cybersecurity

Cybersecurity by design
Secure products, solutions, software

Team certifications

ISA · CISSP · CISM · CISA · IEC · Security+ · GPEN · 27001 · GICSP · NERC · CEH · LPT · CHFI · EXPERT

Cybersecurity strategy and approach

1. Provide customers with operational technology (OT) cybersecurity solutions and services to meet their business goals and security objectives, comply with international and local cybersecurity frameworks and standards, and deliver continuous monitoring of cybersecurity performance within OT.
2. Provide solutions and services to protect OT network infrastructures and enable convergence with IT platforms to ensure protection against cyber threats.
3. Sustainability is at the heart of our strategy and operations, Schneider Electric is consistent in offering new OT cybersecurity solutions and integrate best-in-class technologies, creating a world class partner for operational stability and digitalization.

Assessments & Posture visibility
Identify security blind spots, risks, and governance gaps.

Cyber Program Development
Prioritize & create a unique blueprint for addressing your risks.

Cybersecurity Workshops
Recognize, commit to addressing OT security

Secure Lifecycle

Design & Implementation
Architect a unique package of security controls and services to maximize protection.

Optimization
Continually review, tune, and train to drive resilience enterprise wide.

Operate and Maintain
Align OT with SOC/IT security program, tools, governance.

Strengthening your cybersecurity

1

Strong cybersecurity is a business requirement.

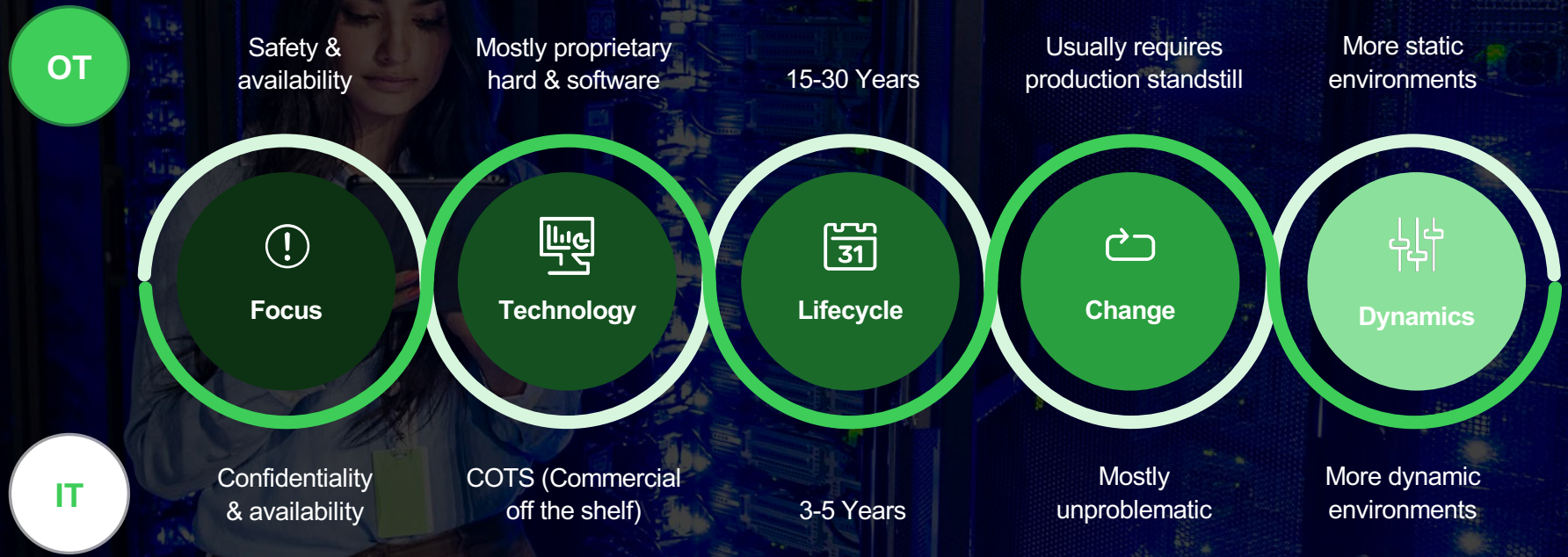
2

Secure data collection and transmission is critical when harnessing the benefits of IoT.

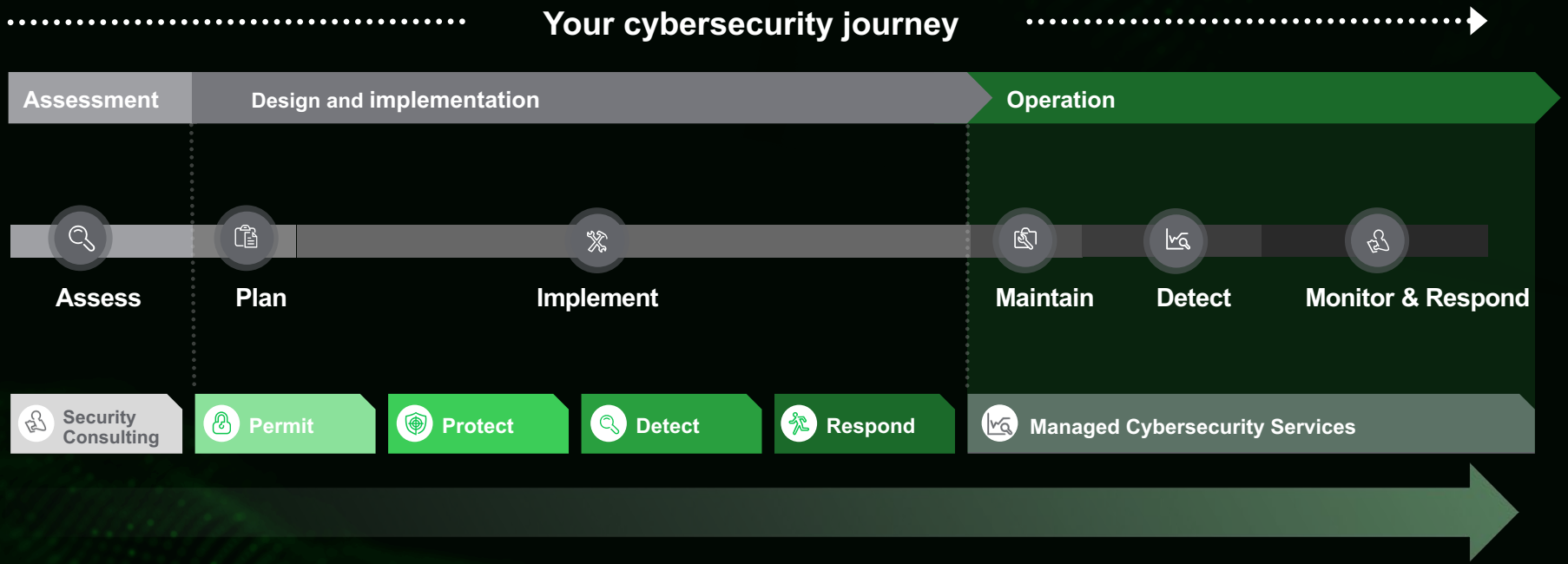
3

Schneider Electric is committed to supporting your digital transformation.

Operational Technology (OT) cybersecurity



Your cybersecurity journey



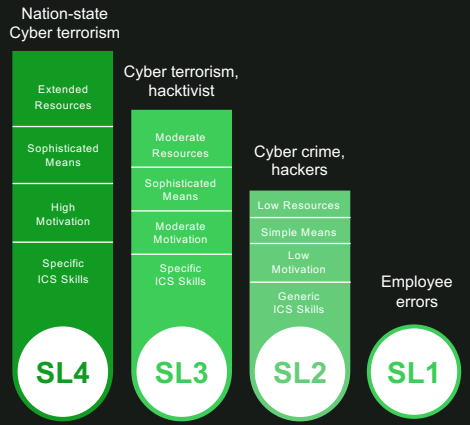
IEC 62443: The cybersecurity language Security Level (SL)

IEC 62443 is an international series of standards that addresses cybersecurity for operational technology in automation and control systems

These seven FRs are the foundation for system (and components) capability security levels

FR 1 – IAC Identification and Authentication Control	FR 2 – UC Use Control	FR 3 – SI System Integrity	FR 4 – DC Data Confidentiality	FR 5 – RDF Restricted Data Flow	FR 2 – TRE Timely Response to Events	FR 7 – RA Resource Availability
Identify and authenticate all users (humans, software processes and devices) before allowing them to access the system	Enforce the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the system and monitor the use of these privileges	Ensure the integrity of the system to prevent unauthorized manipulation	Ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure	Segment the control system via zones and conduits to limit the unnecessary flow of data	Respond to security violations by notifying the proper authority, reporting needed evidence of the violations and taking timely corrective action when incidents are discovered	Ensure the availability of the system against the degradation or denial of essential services

Security levels within IEC62443



IEC62443-2-4

Compliance

Requires 24/7 network monitoring

ZTA: Delivers an integrated security model

Zero Trust architecture

Design principles

- Assume breach
- Never trust, always verify
- Verify explicitly

Policy, Decision, Enforcement Point (PDEP) requirements

- Authentication
- Authorization
- Encryption
- Audit
- Inspection

Cybersecurity compliance implementation

GAP assessment

Conduct gap-assessments against local regulatory authority cybersecurity controls frameworks.

Review and improve

- Review and improve existing cybersecurity programs
- Controls review with the local regulatory authority
- Cybersecurity framework review

Secure architecture

Secure network design and architecture deep-dive.

Policy & roadmap

Develop a cybersecurity policy roadmap and procedures for the local regulatory authority compliance requirements.

Schneider Electric offering

- Determine the current security posture.
- Comply with the local regulatory authority regulations.
- Establish a roadmap for compliance.
- Protect IT/OT systems and network infrastructure against threats.

Cybersecurity solutions and services portfolio

Supporting partners

Security Consulting – Design & Implementation – Monitoring – Maintenance – Training

Services

Capability
Standard Gap Assessments
Cybersecurity Risk Assessments
Secure Network Design
System Hardening
Incident Response Planning
Penetration Testing*
Cybersecurity Training*
Documentation & Policy Development*

* Custom/Specialized

Solutions (Aligned to IEC 62443)

	Capability
SL1	Active Directory/User Management
SL1	Backup and Recovery
SL1	Endpoint Protection
SL1	Patch Management
SL1	Network Segmentation/Firewalls
SL1	Secure Remote Access
SL2	Anomaly Detection
SL2	Intrusion Detection/Prevention
SL2	Log Management
SL3	Automated Asset Inventory
SL3	Multifactor Authentication

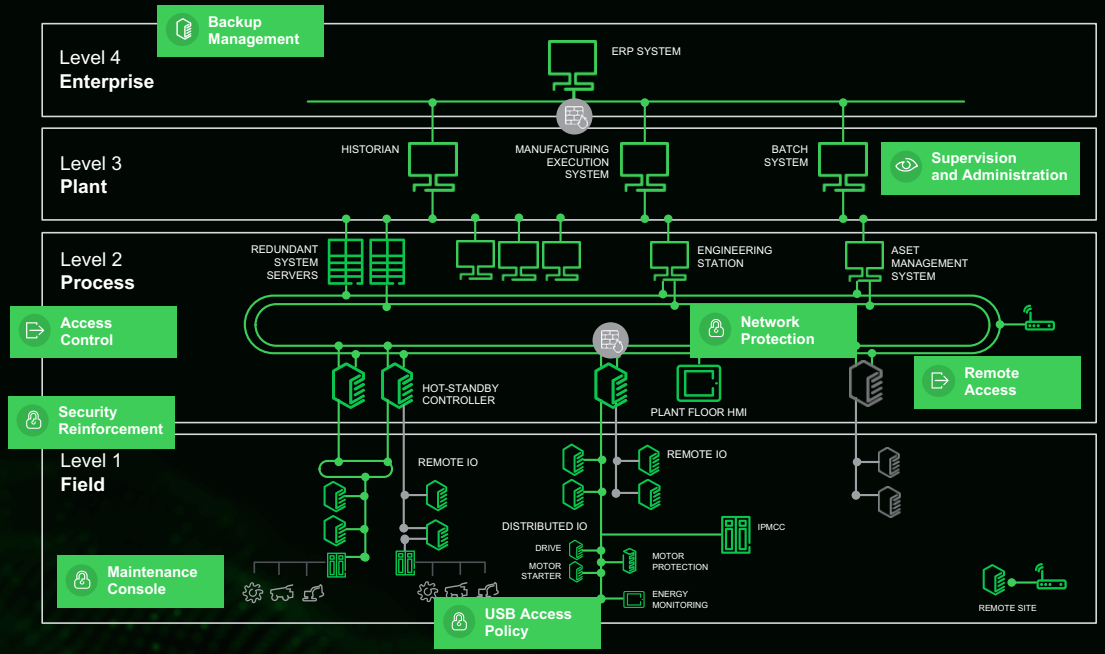
Supporting technology

Capability
Network Performance Monitoring
Removal Media Control
Application Control (Whitelisting)
Security Data Enrichment (SIEM)
Security Orchestration, Automation, and Response (SOAR)*

Sustainability (Recurring)

Capability
24x7 Managed Detection & Response (MDR)*
Security Device Management (SDM)
Incident Response & Recovery*

Cybersecurity solution - design



Reference architecture

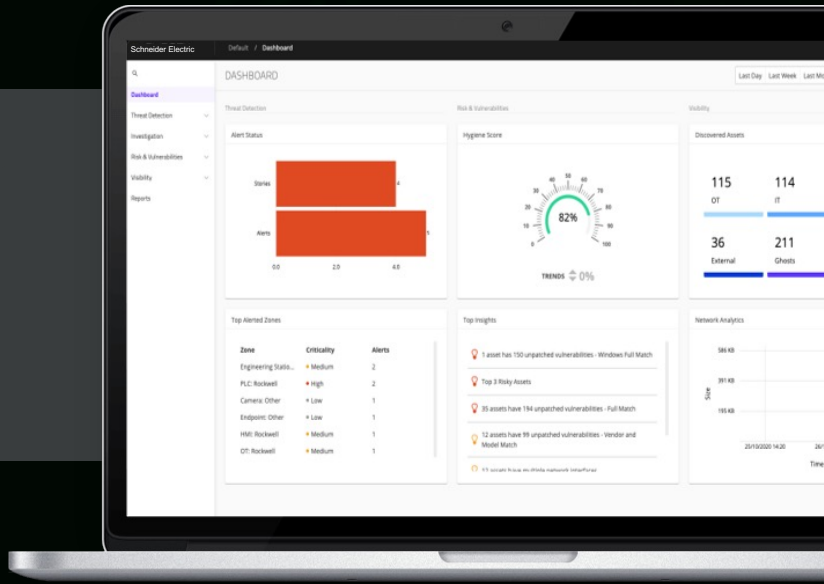
- New project/Existing system to be upgraded
- Selection of solutions compatible with the operation of your system (solutions tested and validated by Schneider)

CAP: Cybersecurity Application Platform

Security simplified by Schneider Electric

Schneider Electric's offering provides comprehensive asset inventory, secure remote access, and threat detection for buildings

- Automated, vendor agnostic inventory of all known and unknown facility assets
- Risk and vulnerability management
- Continuous threat monitoring for suspicious behavior



Simplifies security

Reduces risk

Minimizes effort

15 cybersecurity fundamentals for critical infrastructure

Recommended Cybersecurity Controls

Secure Architecture Architectures that support visibility, log collection, asset identification, segmentation, industrial DMZs, process-communication enforcement.

Assets Visibility
Automated Asset Discovery and inventory, Anomalies Detection, Vulnerabilities Management. Implementation of Threat intelligence platform.

Operational Visibility
Security Operations Center (SOC) or Managed Security Services (MSS) capabilities for Visibility and improved security intelligence. Effective use of AI/ML for situational awareness and Prediction/detection of customizable threats.

High Availability
Hyper-converged Infrastructure, Redundant networks, Segmentation & Micro-segmentation, Zero Trust Architecture (PDEP), Whitelisting and Secure Architecture by Design.

Incident Response
Operations-informed Incident Response Plan with focused system integrity and recovery capabilities during an attack. Exercises designed to reinforce risk scenarios and use cases tailored to the ICS environment.

Secure Remote Access
Identification and inventory of all remote access points and allowed destination environments, on-demand access and MFA where possible, jump host environments to provide control and monitor points within secure segment.

Managed Security Services overview

Cybersecurity simplified

Schneider Electric's 24x7 Managed Security Service offers contextualized vulnerability management, threat monitoring, incident response support, and customer-relevant threat intelligence.

Core Service Outcomes

- 24x7 Security Coverage
- IT-OT Security Synergy
- Consistently meet compliance
- Have a trusted advisor in your back pocket

Immediately improve security posture

Accelerate time to value

Reduce mean time to detect & respond

	Core
Assets Management	Asset Inventory and Visibility
Vulnerability & Risk Management	Vulnerability Assessment
Threat and Incident Management	Threat Detection and response
Cybersecurity control Management	Cyber devices Health Monitoring
Compliance Management	Regulation Compliance Reporting
CS Performance Management	KPI and Reporting

Security Platform Maintenance and technical support

Our proven track record

Global industrial cybersecurity facts and figures

Number of customers
180+

Number of projects
1100+

Countries of operation
25+

Global cyber experts
174

Cyber certifications
25+

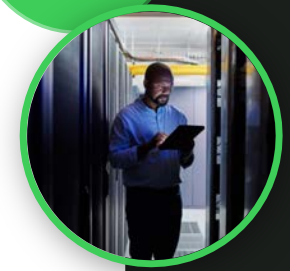
Industry segments
14+

Schneider Electric - cybersecurity skills profile

The Schneider Electric Cybersecurity Solutions and Services Group is a collaboration of control systems and cybersecurity professionals who are industry and vendor certified from globally recognized organizations.

We have an experienced and certified global team helping our customers achieve their cybersecurity objectives and goals.

Our team have assessed, designed and implemented some of the largest and most sophisticated network security infrastructures, regionally and globally.



- ISA/IEC62443 CS Design Specialist ISA/IEC62443
- CS Maintenance Specialist
- ISA/IEC62443 CS Risk Assessment Specialist
- ISA/IEC62443 CS Fundamentals Specialist
- Global Industrial Cybersecurity Professional (GICSP)
- Certified Information Security System Professional (CISSP)
- Certified Information System Auditor (CISA)
- Certified in Risk and Information Systems Control (CRISC)
- ISO 27001 Lead Auditor
- Certified SCADA Security Architect
- CompTIA A+ and Security+
- Certificate Holder (ISA/CDS)
- Computer Hacking Forensic Investigator
- Certified Computer Forensics Examiner
- Certified Ethical Hacker (CEH)
- Microsoft Certified Database Administrator
- Microsoft Certified Professional
- Microsoft Certified Solutions Associate
- Microsoft Certified System Administrator
- Microsoft Certified System Engineer
- Microsoft Certified Technology Specialist SQL
- Microsoft Certified System Engineer Microsoft
- Certified Technology Specialist SQL Cisco
- Certified Design Associate (CCDA) Cisco
- Certified Network Administrator (CCNA) Cisco
- Certified Network Professional (CCNP) Cisco
- Certified Internetwork Expert (CCIE) Fortinet
- Certified Network Security Professional
- Palo Alto Accredited Configuration Engineer
- Tenable Certified Nessus Auditor
- Tripwire Certified Professional
- VMWare Certified Professional
- ITIL Version 3 Foundations

Why Schneider?

- Vendor-agnostic solution capabilities
- End-to-end security with innovation and interoperability at every level
- Ability to implement cybersecurity solutions across varying operating environments
- Flexible security solutions to ensure maximum value and efficiency
- Understand & apply IT cybersecurity solutions within OT context and perspective
- Customize controls based on customers' requirements

Life Is On Schneider Electric

se.com/cybersecurity-services

Life Is On Schneider Electric