Cybersecurity Assessment Services

Understand your cybersecurity posture

A simplified and structured approach to review your key security controls

Completing a cybersecurity assessment is the first step in building a reliable and robust cybersecurity program and should be the starting point when applying cybersecurity requirements in an operational technology (OT) environment.

Our range of cybersecurity assessment services provide customers with an understanding of their cybersecurity posture by identifying gaps and key areas that need to be remediated. Additionally, our service provides recommendations and a roadmap to achieve your cybersecurity objectives.

Key benefits

- Helps you **focus on highest risk areas first** to prioritize effort.
- Focused recommendations help you **prioritize your cybersecurity budget.**
- Much of the service **can be delivered remotely, with results delivered quickly.**
- Clear report and **prioritized recommendations** simplify justification of resources.
- **Vendor agnostic** and can be administered across any infrastructure and industry.

se.com/cybersecurity

Life Is On | Schneider Electric

Understand your cybersecurity posture

The Schneider Electric cybersecurity assessment is a non-invasive high-level assessment performed by Schneider Electric's OT cybersecurity experts. Our cybersecurity assessment aligns to controls categories found with industry best practices and standards such as IEC 62443, NERC CIP, CFATS and ISO27001.

Service Elements

Our cybersecurity assessment service has two key elements:

- The assessment and report.
- Consulting services to discuss the results in depth and create a tangible roadmap for next steps.

Note: There are three levels of cybersecurity assessment that Schneider Electric performs. Our assessment options include:

1. **Core:** Cybersecurity assessment - A high level gap assessment.
2. **Enhanced:** A detailed risk assessment aligned to the control areas of IEC 62443.
   Optimized: A customized assessment that typically focuses on a deep dive of a high-risk environment, system or process.

1. Cybersecurity assessment

- Documentation review (e.g. network diagrams, current cybersecurity policies and program elements)
- Remote interviews with your key OT and cybersecurity stakeholders.
- Cybersecurity expert analysis identifying key risk areas, gaps and recommended steps for remediation.
- Deliverable: A report which gives a starting point to prioritize your future cybersecurity initiatives.

2. Expert consultation

- Our cybersecurity assessment includes a deep dive on the assessment results. Schneider Electric cybersecurity experts will provide detailed recommendations to provide step by step guidance for implementation.
- Here you will be able to ask our Schneider Electric cybersecurity experts questions and clarifications based on the assessment results.
- Our experts will outline a suggested time frame for implementation and a budget estimate.
- Deliverable: Workshop sessions that define a blueprint for cybersecurity and prioritize which areas to address first based on resources.

Prerequisites

To ensure a complete and actionable summary report, Schneider Electric must collect information about your OT systems prior to conducting interviews. The following information should be provided where available:

Data

- Information regarding current cybersecurity policies, cyber program objectives, applicable standards, existing cybersecurity tools and technologies.
- An OT network diagram showing ICS layers/ zones and labels displaying locations of critical assets on the network.

Personnel

- Identification of personnel most familiar with the OT network layout (OT / cyber knowledge).
- Stakeholders who can answer detailed technical questions regarding the OT equipment and assets used within the customer's network.

Cybersecurity assessment areas

Within the assessment our cybersecurity experts will conduct controls-related network discussions including a review of the following control areas:

- Network architecture
- ICS system components
- Cybersecurity policies and procedures
- Physical security procedures
- Cyber training levels of ICS personnel
- Documented incident response procedures
- Lifecycle management policies and procedures
- Access controls

Cybersecurity assessment report

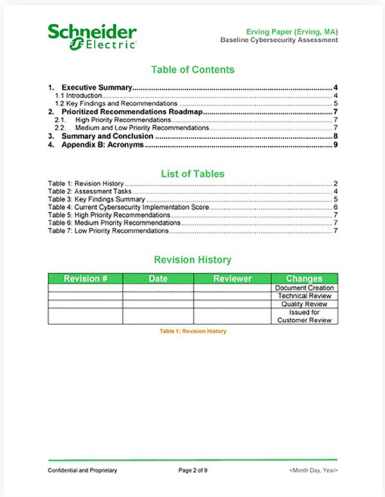
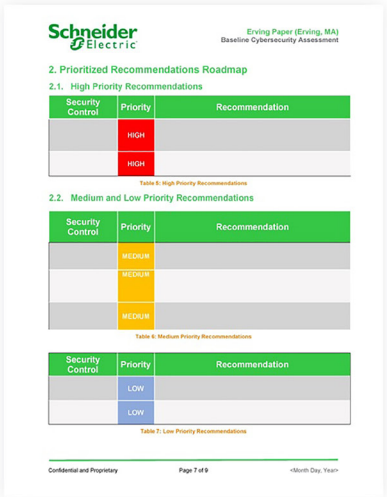

Schneider Electric
Erving Paper (Erving, MA)
Baseline Cybersecurity Assessment
Table of Contents
1. Executive Summary 4
1.1 Introduction 4
1.2 Key Findings and Recommendations 5
2. Prioritized Recommendations Roadmap 7
2.1. High Priority Recommendations 7
2.2 Medium and Low Priority Recommendations 7
3. Summary and Conclusion 8
4. Appendix B: Acronyms 9
List of Tables
Table 1: Revision History 2
Table 2: Assessment Tasks 4
Table 3: Key Findings Summary 5
Table 4: Current Cybersecurity Implementation Score 6
Table 5: High Priority Recommendations 7
Table 6: Medium Priority Recommendations 7
Table 7: Low Priority Recommendations 7
Revision History
Revision # | Date | Reviewer | Changes
Document Creation
Technical Review
Quality Review
Issued for Customer Review
Table 1: Revision History
Confidential and Proprietary
Page 2 of 9
<Month Day, Year>

Table of contents


Schneider Electric
Erving Paper (Erving, MA)
Baseline Cybersecurity Assessment
1.2 Key Findings and Recommendations
Table 3 lists key findings captured during the assessment.
Category | Finding
Asset Management
Control Systems Network Segmentation
Access Control
Physical Security
System Development and Maintenance
System Hardening
Logging and Auditing
Monitoring of OT Network
Information and Data Exchange
Training
Policies
Cybersecurity Management System
Incident Response and Disaster Recovery
Table 3: Key Findings Summary
Confidential and Proprietary
Page 5 of 9
<Month Day, Year>

Control Areas


Schneider Electric
Erving Paper (Erving, MA)
Baseline Cybersecurity Assessment
2. Prioritized Recommendations Roadmap
2.1. High Priority Recommendations
Security Control | Priority | Recommendation
HIGH
HIGH
Table 5: High Priority Recommendations
2.2. Medium and Low Priority Recommendations
Security Control | Priority | Recommendation
MEDIUM
MEDIUM
MEDIUM
Table 6: Medium Priority Recommendations
Security Control | Priority | Recommendation
LOW
LOW
Table 7: Low Priority Recommendations
Confidential and Proprietary
Page 7 of 9
<Month Day, Year>

Prioritized Recommendations

Experienced, capable and globally available

Schneider Electric's global team of cybersecurity experts understand the unique needs and challenges for OT systems and technologies. Our focus is on finding solutions that fit your unique requirements, regardless of the systems you use.

We work with leading cybersecurity product experts to bring the right solutions to your operation, ensuring that your people, processes, and technologies are protected.

Contact us today

Learn more about our cybersecurity assessment services and our full range of solutions that can support your needs for cybersecurity protection across all business types and industries.

cybersecurity-services@se.com

se.com/cybersecurity

Life Is On Schneider Electric

Schneider Electric Industries SAS
35, rue Joseph Monier - CS 30323
F92506 Rueil-Malmaison Cedex

998-21301259_GMA-US