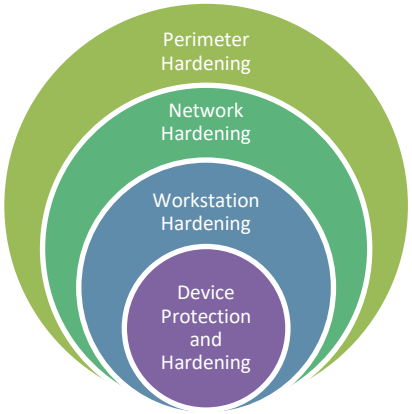
Read This First:
Recommended Cybersecurity Best Practices

Schneider Electric Is Focused on Cybersecurity

Schneider Electric adheres to a security by design approach to better secure our products, systems, and services. We continually evaluate cybersecurity threats to mitigate risk, reduce exploitable weaknesses, and defend against cyberattacks.

Recommended Cybersecurity Best Practices

To help keep your Schneider Electric products secure and protected, we recommend that you implement these cybersecurity best practices. Following these recommendations may help significantly reduce your company's cybersecurity risk.



Perimeter Hardening

Set up firewalls

Building a highly protected network that helps prevent outside access is the most critical line of defense against cyberattacks. We recommend that you follow these guidelines.

- Limit access to the networks on which Schneider Electric devices are placed.
- Always place Schneider Electric systems and devices behind firewalls and other security protection appliances that limit access to only authorized remote connections.
- Remove or secure devices that face the public internet to minimize exposure to attackers. Tools are available that will identify internet-accessible OT devices that are directly and insecurely exposed to the internet.
- Restrict external network connectivity to your systems and devices.
- Continually monitor for events that might indicate attempted unauthorized access.
- Limit access to internal networks where devices reside.

Network Hardening

Implement secure access controls

Reduce the pathways into and within your networks. Implement security protocols on existing pathways to make it more difficult for a threat to enter and move around your system. Isolate control and safety system networks and remote devices from your business network. Strong segmentation helps prevent an attacker that enters one part of the network from gaining access to other areas. Sanitize laptops and systems that were connected to any other network by fully updating software programs and using antivirus protection.

Disable unneeded / unused communication ports and protocols

PLC controllers and network interface modules generally support multiple communication protocols that are enabled by default. Disable ports and protocols that are not required for the application.

Use secure methods for remote access

Implement secure methods for remote users to access your network. Require all remote users to connect and authenticate through a single, managed interface before conducting software upgrades, maintenance, and other system support activities.

Create an asset inventory and network map

A detailed inventory of your assets and a map of your infrastructure can help increase awareness of components that may require patching and backup. We recommend that you follow these guidelines.

- Inventory all devices with an IP address, including their software and firmware versions.
- Include removable media and spare equipment.
- Identify all communication protocols used across the network.
- Catalog external connections to and from the OT networks, including vendor, third-party, and other remote access.

Set up measures for detecting compromises

Minimize the chances of compromise by monitoring and auditing system events 24/7. Use intrusion detection systems (IDSs), intrusion prevention systems (IPSs), antivirus software, and usage logs to help detect compromises in their earliest stages. Use a trusted time server such as NTP (Network Time Protocol) to synchronize the clocks for all devices in your network. This helps ensure that your logs provide accurate data about the time of any breach. Despite implementing these preventive measures, you may still experience compromises. Have a plan in place to quickly detect the issue and respond.

Workstation Hardening

Implement strong authentication and authorization controls

Change default passwords when new software is installed and regularly after that. (Do this now!)
This is particularly important for administrator accounts and control system devices. Eliminate the use of default passwords and disable default system accounts when possible. Use role-based access with multi-factor authentication to help prevent security breaches and provide a log of access activity. Add password security features, such as an account lockout that activates when too many incorrect passwords are entered and a requirement for strong passwords for all users.

Set up a blocklist to deny access to known suspicious or malicious entities

A blocklist (blacklist) filters incoming traffic and denies access to entities (such as domains, email addresses, or applications) that have been previously associated with malicious activity. It can help prevent known viruses, spyware, Trojans, worms, and other kinds of malware from accessing your system. Antivirus tools, spam filters, intrusion detection systems, and other security software commonly incorporate blocklists to help control access. One of the biggest advantages of a blocklist is its simplicity. Any entity not on the list is granted access, but anything that’s known or expected to be a threat is blocked. Most organizations use lists created by third parties, such as security service providers. In addition, you should create your own blocklist of users, IP addresses, applications, email addresses, domains, and anything else you want to keep off your system.

Use an allowlist to help keep your systems safe from unwanted software

Add allowlist (whitelist) software to your defenses so only entities that your system recognizes as authorized are granted access or privileges on your workstation. The allowlist works with your blocklist software to allow only known software to run. Using an allowlist increases your confidence that installed files and loaded executables have maintained their integrity and are authentic. This additional protection results in a higher degree of trust for the workstation by helping to prevent sophisticated attacks.

Encourage secure workstation habits

Everyone in your company can contribute to cybersecurity efforts by keeping their workstations as safe as possible. Scan any devices used to exchange data, such as external hard drives or USB drives, before using them in any node connected to the network. Remove unnecessary programs and services from workstations and store sensitive data on a server. Regularly back up data from hard drives. Finally, be sure everyone gets into the habit of locking their screens when they aren't in use.

Device Protection and Hardening

Install physical controls to help prevent unauthorized access

While this isn't just a cybersecurity issue, it's important to put physical controls in place so that no unauthorized person can access your equipment or devices. Keep all controllers in locked cabinets and limit access to any connected devices.

Track operating modes

Keep PLCs in RUN mode. If PLCs are not in RUN mode, confirm that an alarm informs the operators.

Check the documentation for product-specific information

Schneider Electric provides detailed information with every product. Review the product guides on the Schneider Electric website or that accompany your products to find cybersecurity recommendations and best practices directly related to your Schneider Electric products.

Plan for the Worst

Maintain current backups

The most effective way to recover from a malware attack is by backing up your systems and data frequently. Back up all critical resources off the network and keep a copy in a secure, tamperproof, or offline environment. Ensure that you have multiple backups over time, so you can restore from a version that predates any infection. Remember to test your backups regularly so you know they will work properly when you have to use them.

Prepare and test your recovery procedures

Develop a plan to recover from an attack when a system is malfunctioning, inoperable, or not working reliably. The plan should include disconnecting systems from the internet if they can still run reliably, setting up compensating controls for systems that must stay connected, and limiting functionality to reduce risk and attack surface area. Also include the steps required for manual operations in case the system becomes unavailable. Assign responsibilities for restoring the network and devices quickly when it is safe to do so. Be sure to test your plan before you have to use it.

Hold exercises to test your incident response plan

When an incident occurs and tensions are high, having confidence in a tested incident response plan can minimize your risk and exposure. Hold incident response walkthroughs and invite executives, IT and OT managers, public affairs, and legal. Review key decisions points and specify who will make the decisions at each time. Include scenarios for systems that are malfunctioning, inoperable, or not working reliably due to external interference. Confirm that applicable equipment is never left in program mode, where is it vulnerable to unauthorized updates. Review your support contracts and government services for response and recovery.

Minimize Your Risk

Apply patches and updates

Most vendors work diligently to develop and distribute patches or mitigations for identified vulnerabilities. Even after patches and updates are released, many systems remain vulnerable because organizations are either unaware of or choose not to implement these fixes. Effective patching can stop a large number of attacks, so implement a monitoring system to be sure you always apply the latest patches and updates for operating systems, antivirus tools, and any other software.

Be aware of vulnerabilities

Schneider Electric regularly posts security notifications with information on vulnerabilities and patches that it receives from entities such as the U.S. Department of Homeland Security's ICS-CERT, Computer Emergency Readiness Teams (CERTs) from various countries, cybersecurity ISACs (Information Sharing and Analysis Centers) around the world, and cybersecurity firms. These updates are designed to fix known vulnerabilities and are encouraged for any Internet-connectable device. You can also subscribe to our newsletter to receive security notifications.

Train your employees

Provide cybersecurity training to all your employees to help keep your organization secure. Explain phishing emails, infected attachments, malicious websites, and other methods that attack them directly. Require contractors or managed services vendors to complete the equivalent cybersecurity training.

For More Information and Assistance from Schneider Electric

For details and assistance on protecting your installation, contact your local Schneider Electric Cybersecurity Services organization or see Cybersecurity Services on the Schneider Electric website.

To view posted security notifications:
https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp

To subscribe to our security newsletter:
https://www.se.com/ww/en/work/support/cybersecurity/notification-contact.jsp

For Cybersecurity Services:
https://www.se.com/us/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

For Additional Information on Cybersecurity Best Practices

Quick Start Guide: An Overview of the ISA/IEC 62443 Series of Standards
International Society of Automation (ISA) Global Cybersecurity Alliance (ISAGCA)

Cybersecurity Advisory: NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems, Alert (AA20-205A), July 2020
US Department of Homeland Security, Cybersecurity & Infrastructure Security Agency (CISA)

Cybersecurity Best Practices
Center for Internet Security

e-Guide: Building a Cybersecurity Strategy for the Digital Economy

Cybersecurity by Design: Building a Company Culture to Strengthen a Digital Business

Document # 20765160 – June 2022
Document download: https://www.se.com/us/en/download/document/7EN52-0390/