Cybersecurity, Product Security and Data Protection at Schneider Electric

Protecting communities and building trust with critical infrastructure in a growing threat environment

July 2023

Executive summary

Schneider Electric provides energy and digital automation solutions for efficiency and sustainability by integrating world-leading energy technologies, real-time automation, software, and services into integrated solutions. In doing so, Schneider Electric serves customers and partners in homes, buildings, industries, and critical infrastructure worldwide.[1]

This white paper provides an overview of Schneider Electric's vision and discipline for cybersecurity, product security and data protection. It describes key components of the company's security posture, including initiatives to bolster resilience and create Trust in the context of a growing attack surface, evolving regulations and customer expectations.

[1] Schneider Electric products and systems are used in over one million buildings worldwide, including 40,000 water & wastewater treatment installations, 40% of the world's hospitals, 10 of the world's top electric utilities, and 10 of the world's largest airports.

Introduction

Schneider Electric is the global leader in the digital transformation of energy management and industrial automation, integrating world-leading process and energy technologies for homes, buildings, data centers, critical infrastructure, and industries.

With a digital footprint that spans the globe, the company's risk landscape is constantly evolving and requires ongoing protection against cybersecurity threats and attacks. Therefore cybersecurity, product security and data protection are integral to Schneider Electric's business strategy and the digital transformation journeys of its customers.

The company believes that no single entity can achieve effective cybersecurity alone. When one organization is targeted by a cyberattack, the consequences can be far-reaching, leaving others equally vulnerable. With cyber threats evolving at an unprecedented pace, it is vital that all work together to mitigate risk and safeguard collective interests.

Trust is a core driver of Schneider Electric's security posture

Schneider Electric is committed to doing business responsibly, earning and sustaining Trust by creating safe, secure, and resilient digital ecosystems for its customers. The Trust Charter,[2] which embodies the company's Code of Conduct, is the framework for how Trust underscores all interactions and relationships with the communities it serves.

Schneider Electric recognizes that the security of its offerings and its ability to safeguard its customers' data while complying with regulations is key to building sustainable relationships. To reach the highest level of trustworthiness, the company continuously enhances its security posture through five core pillars:

1. Cybersecurity fundamentals and awareness.
2. An enterprise-wide, risk-based approach.
3. Cyber defense, threat intelligence and incident response and recovery.
4. Supply chain and installed-base security.
5. Customer and authority relationship and expectations.

By diligently implementing these pillars throughout everyday operations, Schneider Electric aims to continuously build resilience and nurture Trust, while mitigating risks over its digital and operational landscapes.

[2] "Trust Charter, Schneider Electric's Code of Conduct", March 2023, https://www.se.com/ww/en/download/document/SchneiderElectric_TrustCharter/

Pillar 1: Enforcing Digital, Operational and Physical Security Fundamentals

a. Establishing a cyber culture focusing on people

Schneider Electric encourages an open and transparent culture where employees are encouraged to self-report any possible issue, such as intrusion, errors, or vulnerabilities. The company encourages a “see something, say something” culture to quickly detect exposures and breaches.

Protecting critical infrastructure and ensuring operational continuity is everyone’s responsibility, from C-level (with tone from the top) to shop floor (with a leader in charge of cybersecurity in each plant). Schneider Electric recognizes that people empowerment is needed to complement the best tools and processes to effectively combat threats.

Special attention is brought to:

- **Fostering a culture of awareness through training.** Every employee, including new hires, undergoes mandatory annual training to learn about the company's policies and secure behaviors. The training materials are updated regularly to keep pace with evolving threats, tactics, techniques, and regulations. To foster a security culture, practical exercises like Cyber Month, Trust Week, and regular phishing campaigns are conducted to enhance employee awareness and preparedness.
- **Cultivating a pool of cyber-talent.** To address today's complex threat landscape, the company leverages its external attractivity and internal resources, searching for and attracting motivated people within the industry. In line with its Diversity, Equity & Inclusion and Multi-Hub principles, it identifies technical, operational and leadership skills to elevate competencies within the organization.
- **Building a community.** Schneider Electric aims to create a borderless cybersecurity, product security, and data protection community to develop cooperation and emulation. Having this sense of purpose allows to “act as owners”.

b. Addressing digital, operational & physical security fundamentals

Protection of computer systems, networks, and access to sites are fundamental lines of defense. By implementing digital and physical security measures, the company can prevent intrusions.

- **Securing the company’s physical sites.** Global site protection rules establish secure access to sites and data. Site managers instill a safety culture by conducting a yearly risk assessment tailored to their location, while all employees are expected to "act like owners", each with a role to play. Schneider Electric’s most critical R&D centers, industrial sites, and customer-staging facilities are scrutinized regularly and must meet stringent requirements within the company’s proprietary maturity model.
- **Securing identities and monitoring assets.** Schneider Electric regulates access to its systems and assets with a centralized Identity and Access Management (IAM) solution. Access is role-based and follows the Principle of Least Privilege (PoLP).

Single-Sign-On (SSO) with Multi-Factor Authentication (MFA) is enforced for increased security, while administrative and technical controls scrutinize the security posture of devices connecting to the company's environment. Secure remote access connections are provided for employees and contractors, and access is revoked on the last day of employment.

- **Securing networks.** The company implements various controls and measures to protect its networks and endpoints, such as using reference architectures, installing security patches, segmenting networks, and managing digital assets with encryption and Endpoint Detection Response (EDR) solutions. In addition, it employs host-based intrusion detection and prevention capabilities on high-risk assets, along with mobile device management and Mobile Threat Defense (MTD) applications, to provide comprehensive protection for its mobile devices. Specific policies, security controls, alerts, training, and procedures for privileged accounts are implemented to secure access to the most critical assets.

  To monitor its operational technology environment, Schneider Electric partners with Claroty[3] for real-time network flow monitoring and live tracking of devices from initial deployment to obsolescence while notifying when to patch.

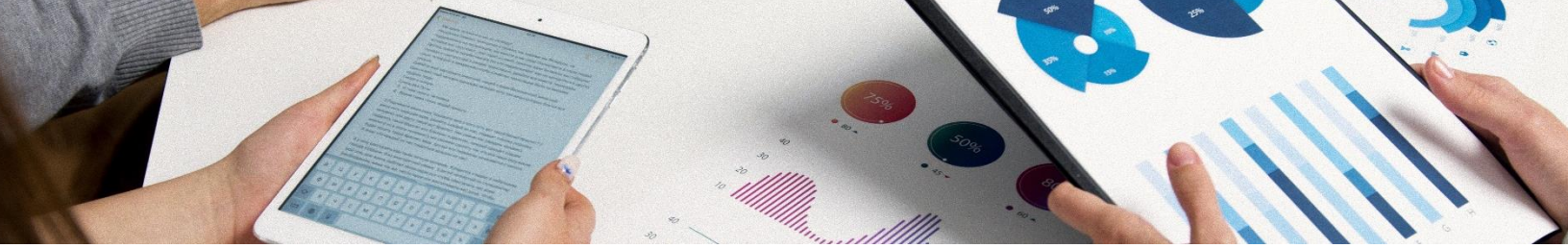
c. Continuously challenging cybersecurity posture

As the threat landscape continues to evolve, Schneider Electric constantly challenges itself to improve its posture by:

- **Monitoring its cybersecurity posture with cyber-rating agencies.** These services enable continuous benchmarking of performance against peers and monitors in real time the exposed digital footprint of the company.[4] This methodology is deployed with subsidiaries to encourage and sustain acceptable levels of maturity across the extended enterprise. Scoring allows stakeholders to speak a common language when addressing cybersecurity maturity and performance with customers, partners, peers, and authorities.
- **Assessing security capabilities with audits.** By scrutinizing each risk scenario, the company examines its systems for any vulnerabilities. These practices facilitate discussions with customers and authorities to establish a shared approach to cybersecurity and enhance the security of the company's supply chain.
  - Third-party entities conduct regular audits, certifications, and vulnerability testing, which apply to products, systems, sites, and services.
  - Internal audits are periodically conducted to check the posture of the company with respect to physical security, digital security, and data protection.
- **Reporting cybersecurity risks to Executives and the Board of Directors:**
  - Monthly updates and metric reports on security practices are shared at the highest level of the company (including factory and distribution centers' performance).
  - The Board of Directors is updated annually at the Digital and Audit Committee on cybersecurity strategy, maturity, and practices.

[3] "Claroty and Schneider Electric Collaborate to Enhance Industrial Cybersecurity", June 2022, https://www.se.com/us/en/about-us/newsroom/news/press-releases/claroty-and-schneider-electric-collaborate-to-enhance-industrial-cybersecurity-629f212112d98c056d1c8026

[4] https://www.se.com/ww/en/about-us/cybersecurity-data-protection/



Pillar 2: Taking an Enterprise-Wide Risk-Based Approach

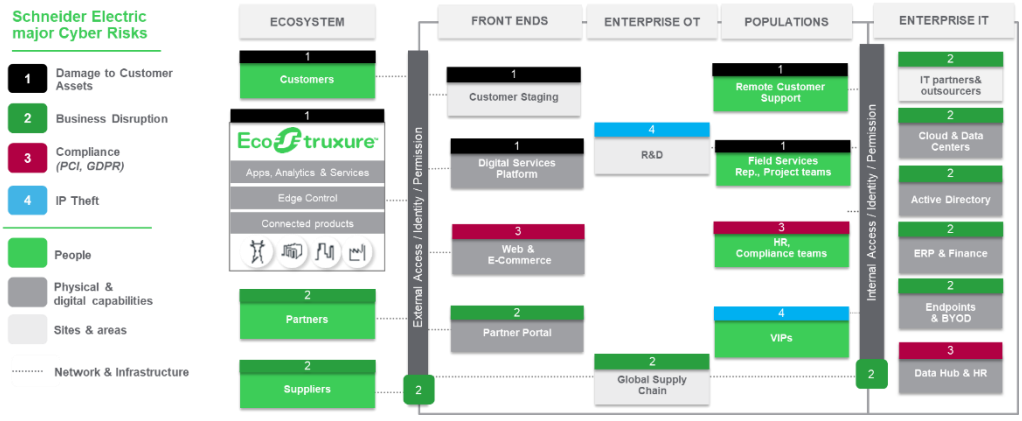
Schneider Electric's cybersecurity, product security and data protection strategy requires a company-wide, end-to-end, risk-informed approach. The company aims to protect its digital and operational landscapes through a risk-informed Enterprise Risk Management (ERM) framework.[5]

a. Mapping cyber risk across the extended enterprise

Schneider Electric analyzes risks across its extended digital and operational landscapes as seen in Figure 1, in order to determine how to mitigate the corresponding risks.

Figure 1

Schneider Electric's end-to-end digital and operational landscapes



As a result, the company uses a companywide Cyber Risk Register[6] to segment these risks into four categories:

1. Damage to customer's assets and operations.
2. Disruption of company's operations.
3. Non-compliance with global and local regulations.
4. Voluntary and involuntary loss, leakage, or exposure of Intellectual Property (IP).

This Register translates cybersecurity risks into business and operational risks with quantified potential financial exposure,[7] and risk accountability up to the C-suite. Our approach leverages the National Institute of Standards and Technology (NIST) Cybersecurity Framework[8] to increase the company's overall level of cyber resilience. It helps promote a shared understanding of the critical business risks, facilitates investment in risk mitigation initiatives, and fosters collaboration throughout the enterprise.

The company has a central body that governs its security portfolio and coordinates a community of security practitioners across various businesses and territories.

[5] "2022 Annual Report: Introduction by Chief Governance Officer & Secretary General, Hervé Coureil, https://flipbook.se.com/catalog/ww/en/41123-Schneider-Annual-Report-2022-EN/#page/296

[6] It is a widespread utility among many cybersecurity professionals that allow practitioners to track and measure risks in one place.

[7] Known as EML – Estimated Maximum Loss

[8] NIST is a non-regulatory agency of the United States Department of Commerce https://www.nist.gov/cyberframework

Security leaders are held responsible for managing risks within their domains (functions, regions, site); they have shared ownership of the risks, allowing the company to manage them where they originate.

The risk management process leverages the Three Lines of Defense Model to ensure end-to-end accountability with operational teams (that act upon their risks by implementing mitigation controls), security leaders (overseeing the execution of risk mitigation) and independent assurance (internal or external audits) to review and evaluate the implementation of risk management and ensure effectiveness of mitigation.

This risk-centric methodology also applies to Schneider Electric's subsidiaries.[9]

b. Mitigating risks and measuring the level of defense

Schneider Electric has security policies in place that dictate secure behaviors and practices to be followed throughout the company. The company's overarching General Information Security Policy and all supporting cybersecurity, product security and data protection policies comply with widely recognized standards such as the ISO/IEC 27000-series,[10] the NIST Cybersecurity Framework as well as ISA/IEC 62443.[11] These policies apply to all employees and contractors with access to our IT assets and systems, and are communicated regularly through various channels, such as newsletters and mandatory online training. The company updates these policies annually to reflect a changing threat landscape, evolving regulations and industry practices.

To ensure the resilience of its operations, the company has differentiated protection to some systems including but not limited to Active Directory, e-commerce platform, or certain partner portals. Compromise of these "Crown Jewels" could hamper the company's operations and impact its customers. Each asset must be breach-resistant to detect and respond to an attack. This means that such an asset is subject to administrative and technical controls, regular auditing, quarterly vulnerability scans, and periodic penetration testing. These assets must be breach-ready, and so, disaster and recovery plans are reviewed, approved, and tested every year as a mandatory recurrent control. Crown Jewels also have strict data protection requirements, with appropriate controls in place for:

1. Access (principle of "least privilege", securing admin workstations)
2. Storage (encrypting at rest and systematic backups, tested restore)
3. Protection (application patching, OS, and database hardening)
4. Data flow and consumption (data interaction monitoring, inventory of connectors & API)

Special attention is brought to sensitive audiences. In addition to the general annual learning path, these populations are offered supplemental, role-based cybersecurity training:

- Admins, HR, R&D and Executives must be aware of risks associated with dealing with sensitive data.
- Customer-facing employees must take additional customized training to ensure vigilance when it comes to cybersecurity with customers and their data.

[9] "Security Principles for Subsidiaries Policy", September 2022, https://download.schneider-electric.com/files?p_Doc_Ref=SE-Security-Non-Integrated-Co

[10] ISO/IEC 27001 Standard

[11] ISA/IEC 62443 Series of standards

- Shopfloor workers in all plants follow dedicated training on behaviors to limit the risks associated with their work. A local cyber expert is accountable for implementing the right behavior.

A culture maturity scheme is deployed on above-mentioned populations to understand what gaps must be addressed to raise the level of secure behavior readiness.

Schneider Electric believes that an adaptation of Zero Trust is as critical to operational environments as it is to digital systems. As an illustration, the company implements Zero Trust on infrastructure through Cyber Assurance Principles:

1. Continuous Verification: leverage data to verify systems, devices, and users
2. Least-Privilege Access: provide secure access to only what is necessary
3. Logical Segmentation: isolate and limit the impact of security threats
4. Supply-Chain Risk Awareness: collaborate with suppliers and customers
5. Scaling With Automation: automate defenses to reduce manual tasks
6. Proactive Detection: adopt a breach mindset to proactively detect threats
7. Business Resilience: learn from incidents to improve contingency strategies

These principles embody a risk-centric approach[12] which will continue to evolve as Schneider Electric matures its controls and capabilities.

c. Managing compliance while tackling new challenges

In line with its digital transformation, the company must:

- **Seek compliance with leading standards.** Overall enforcement is supported by internal audits and certifications by external authorities based on the NIST SP 800-53[13] and ISO/IEC 27001 frameworks.
- **Comply with data protection laws**, such as, but not limited to the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) and the Personal Information Protection Law (PIPL).
- **Safeguard privacy and protect data.** Its data risk management framework covers data quality, retention, regulatory requirements, and the proper use of data for machine learning and AI. Schneider Electric adopted the Data Capability Assessment Model[14] (DCAM), tailored to the industry and its operational profile.
- **Secure customer payment information.** Schneider Electric's compliance with the Payment Card Industry Data Security Standard[15] (PCI-DSS) requirements protects sensitive customer payment information. The company expects its vendors to maintain PCI-DSS compliance for their environments to support Schneider Electric's e-commerce strategy and platforms.

d. Embracing AI opportunities and challenges

With the evolutions of Artificial Intelligence (AI), including the arrival of Large Language Models like ChatGPT, the company puts security guardrails on the use cases developed.

[12] "From IT to OT: Extending Zero Trust Principles for Greater Resiliency", October 2022, https://cybertechaccord.org/from-it-to-ot-extending-zero-trust-principles-for-greater-resiliency/

[13] "NIST SP 800-53: Security and Privacy Controls for Information Systems and Organizations", September 2020, https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

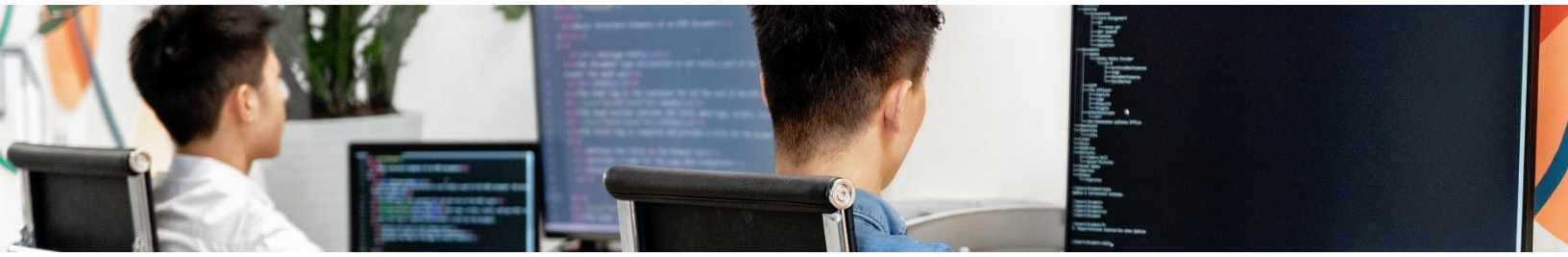
[14] Data Management Capability Assessment Model (DCAM) Framework

[15] PCI DSS Documentation

This includes conducting risk assessments during the ideation phase, performing standard security controls such as identity and access management, vulnerability assessments as well as specific controls to prevent data exposure or poisoning.

Dedicated communication and training raise employees' awareness on risks on how to use these technologies safely. A dedicated governance for AI is established and digital certification ensures the right level of security is in place.

The company recognizes the potential for innovative technologies to enhance its cyber initiatives and is exploring ways to leverage them, such as by detecting threats from behavioral analytics, enabling real-time monitoring and containment. However, as it does so, it is equally mindful of ethical considerations, ensuring that every application is assessed and challenged on grounds of social responsibility, sustainability, and human-centricity to avoid misuse in accordance with our Data Risks Management principles.[16]



Pillar 3: Raising the bar on Cyber Defense, Threat Intelligence, and Incident or Crisis Response

Schneider Electric endeavors to power an "always-on" world, even in the context of an unpredictable future.

a. Utilizing Threat Intelligence

Schneider Electric has established a capability that provides strategic, operational, and tactical threat intelligence to its security and business functions. This intelligence helps bolster cyber defense and drive product development by providing insight into threat actors targeting Schneider Electric while keeping a watchful eye on emerging threats and new technologies.

The company leverages threat intelligence platforms to collect information geared towards the safety and security of its customers, the continuity of its own operations and the protection of IP. Enhanced monitoring and deep analysis allow for the identification of potential cyber threats and incidents, while coordination with National Security Agencies on intelligence and information sharing help the company to address Nation States' Advanced Persistent Threats (APTs).

Recognizing that attackers are trying to take advantage of privileged internal assets, Schneider Electric monitors for anomalous data movement and abnormal behavior to ensure the integrity and security of its systems, products, and networks. The company can trigger Incident Response on weak signals.

b. Detecting incidents, responding & remediating

Schneider Electric is ready for and prepares to respond to operational disruption, such as being a vector of attacks for its customers, compliance issues, IP theft, exposure, or leakage.

[16] "Trust Charter, Schneider Electric's Code of Conduct", March 2023, https://www.se.com/ww/en/download/document/SchneiderElectric_TrustCharter/

- **Developing incident response plans.** The response to an incident must follow a predetermined, tested, and repeatable protocol to contain the event and protect the company, customer assets, and operations. Schneider Electric's incident response plans define management and response activities, including assigning roles and responsibilities, escalation requirements, and specific technical, administrative, and procedural activities. The company's Security Operations Center (SOC) operates 24/7/365 and is staffed with security analysts who leverage Security Incident and Event Management (SIEM) platforms to aggregate and correlate logs from diverse sources.
- **Detecting Incidents.** The company's digital and operational landscapes, external attack surface and media (including Dark Web, social media, and hackers' forums) are constantly monitored to obtain the most up-to-date threat intelligence and Indicators of Compromise (IoC).
- **Responding to incidents.** Teams are in place to respond to incidents if and when they occur, with incident owners and handlers close to the field. Incidents are categorized according to risks laid out in the Risk Register.
- **Learning from incidents.** Post-incident analysis is consistently conducted, using a global root cause analysis methodology to document the factors that led to the event and associated corrective actions. Electronic or physical evidence is preserved which may be required to support potential litigation or prosecution. A debriefing is organized at the senior leadership level which allows the company to improve its security controls and policies, reinforce its resilience, and inform its approach to risk.
- **Exercising on crisis and incidents.** The company regularly conducts exercises simulating substantial operational, customer, or media events. These crisis simulations, based on its Cyber Risk Register, aim to be as close to reality as possible and often involve a large group of players (beyond the security teams), the company's customers and/or third-party organizations such as National Security Agencies. Simulations help test breach resistance and readiness, and train teams involved in the crises along the Cyber Kill Chain.[17]

c. Improving resilience and recovery

To protect against a sudden adverse event that could affect its operations, the company has created a plan, for which mission-critical business functions are designed to continue operations during and after a disaster/crisis.

Factories, staging areas, and R&D labs, as well as critical applications, have risk mitigation processes in place, such as site fail-over to an alternate facility and Supplier Business Continuity Plan activation. The company has also implemented a contingency plan that prepares its internal and customer-facing digital systems for response and recovery from a disaster thanks to proper planning and infrastructure investment.

Additionally, regular testing protocols help to validate that plans are sound and address potential gaps.

[17] The Lockheed Martin Cyber Kill Chain® is a series of steps that trace the stages of a cyberattack from the early reconnaissance stages to the exfiltration of data

Pillar 4: Building Trust along the Supply Chain, and with the Installed Base

To mitigate the risks from design to maintenance and build Trust along its supply chain, Schneider Electric leverages practices prescribed in standards such as ISA/IEC 62443 and ISO/IEC 27001. The company also pushes for responsible interactions between actors within the supply chain.

a. Managing risks with suppliers

Schneider Electric mandates that its suppliers meet high standards in cybersecurity and privacy, as per the Third-Party Security Principles.[18] The company requires them to extend these guidelines to their own suppliers and service providers. These security expectations are included in the onboarding process and Schneider Electric assesses suppliers' cybersecurity maturity to verify compliance with the company's requirements before engagement.

Suppliers are segmented based on current and future business strategy, their value proposition, and risk exposure (data shared, product security, digital and physical access levels). Critical suppliers are treated as partners and undergo C-level cyber discussions, internal digital certification, and controlled assessments based on industry-standard frameworks. Cyber scoring capabilities are used to continuously monitor suppliers for potential cyber events and provide alerts to prevent supply chain disruptions.

Supplier agreements require Suppliers to notify Schneider Electric when an incident occurs and cooperate to mitigate risk.

b. Implementing security practices for products and software

Schneider Electric strives to design and make products cyber-secure by design, while aiming to create secure building blocks that will shape the future of secure products. The company seeks to:

- **Provide a secure IoT-enabled architecture.** As a manufacturer, Schneider Electric embeds security throughout EcoStruxure™,[19] its vendor-neutral, IoT-enabled architecture and platform, which includes a tailored stack of connected products, edge control solutions, software, cloud-based applications, analytics, and services. EcoStruxure employs cybersecurity industry-leading practices from the devices up to the hosted applications, and spans six domains of expertise, representing the convergence of digital and operational technologies.

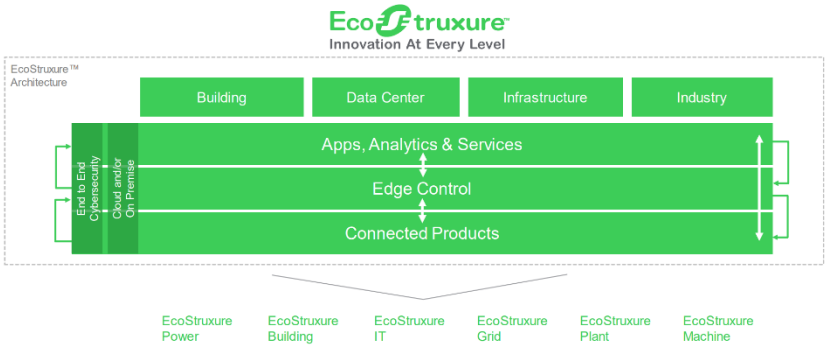


Figure 2

Schneider Electric's EcoStruxure™ architecture

[18] "Schneider Electric Third-Party Security Principles", September 2022, https://www.se.com/id/en/download/document/3rd_party_cyber_09112020AR0/

[19] EcoStruxure Solutions Overview

- **Implement Secure Lifecycle Management.** Schneider Electric recognizes the need to have cybersecurity measures fit-for-purpose throughout the entire lifecycle of the product, from development to retirement. This discipline includes end-to-end security across all software and system development lifecycles, certified to the ISA/IEC 62443-4-1 Secure Development Lifecycle standard, to which Schneider Electric has contributed for over a decade.
- **Conduct pen tests, final security reviews and digital certification.** The company enhances the security validation of its technology leveraging its CREST-accredited penetration testing lab[20] and by engaging external partners. All applications, products, or systems undergo a formal security review, with EcoStruxure™ cloud offers undergoing an additional digital certification process. This brings a consistent and disciplined approach to embedding security into the company's products and maintaining external certifications.
- **Oversee the security of its industrial environment.** One cyber leader per site monitors alerts, vulnerabilities, and supports incident response. On top of this governance, hygiene is assured globally, in plants and distributions centers (including OT asset inventory, IT/OT firewalls and Secure Remote Access, endpoint protection on all PCs and real-time monitoring). From 2022 onwards, every new production line is ISA/IEC 62443-3-3 and ISA/IEC 62443-2-4 Security Level 2 compliant.
- **Manage product vulnerabilities.** Schneider Electric's vulnerability management process, based on ISO/IEC 29147[21] and ISO/IEC 30111,[22] tracks and fixes vulnerabilities with the assistance of its Corporate Product Cyber Emergency Response Team (CPCERT). The company's teams continuously detect, mitigate, and remediate vulnerabilities for products in the market as they are discovered. Schneider Electric aims to work collaboratively with Researchers, Country Cyber Emergency Response Teams (CCERTs) and asset end-users through the Cybersecurity Support Portal[23] to ensure that accurate vulnerability mitigation and remediation information is responsibly disclosed. In cases of critical vulnerabilities, the incident management protocol can be activated to expedite resolution.
- **Declare Software Bill of Materials (SBOM).** Schneider Electric collaborates with industry-leading organizations and implements stringent verification processes, including thorough documentation and regular updates, to provide customers with accurate SBOMs.
- **Protect IP and Source Code.** Schneider Electric protects its portfolio of IP, preventing accidental loss, source code exfiltration and tampering through:
    - Legal frameworks such as patents, licenses, and escrow agreements
    - Administrative controls including non-disclosures, and specific addendums
    - Security measures including access control and code integrity regarding third-party and open-source code. Source code is categorized to determine the level of protection needed, such as localization and code sharing, in accordance with its Source Code Security principles.[24] Each control has explicit objectives to be met, with evidence that project teams must deliver.

[20] "Schneider Electric Global Security Labs become CREST Accredited", February 2021, https://www.crest-approved.org/schneider-electrics-global-security-labs-receive-crest-pen-test-accreditation/

[21] "ISO/IEC 29147", October 2018, https://www.iso.org/standard/72311.html

[22] "ISO/IEC 30111", October 2019, https://www.iso.org/standard/72311.html

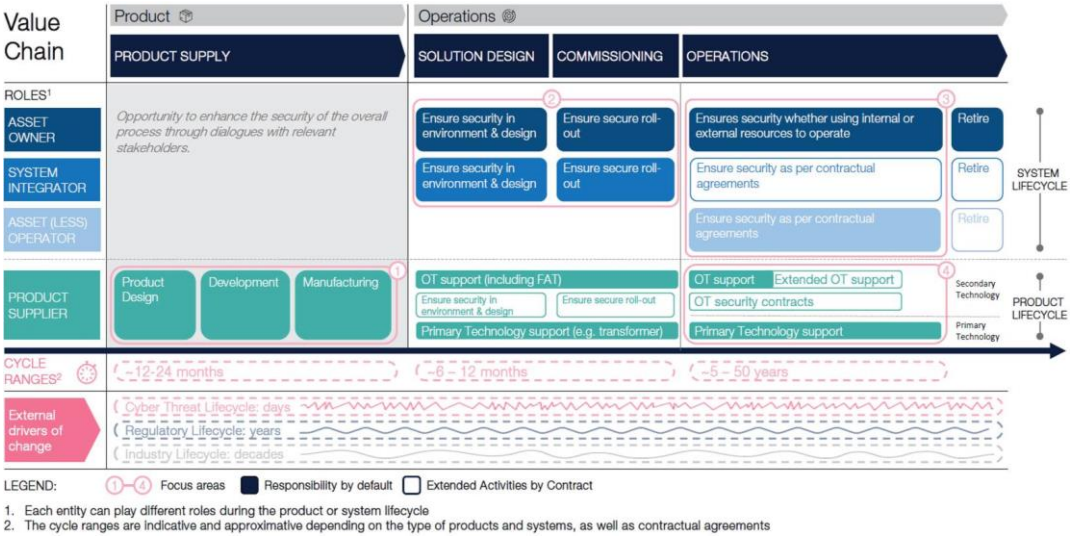
[23] Schneider Electric Cybersecurity Support portal

[24] "Schneider Electric Source Code Security Principles", September 2022, https://www.se.com/id/en/download/document/source-code-security-principle/

- **Safeguarding security in customer environments.** To meet customer expectations, Field Service Representatives (FSRs) must follow consistent and sound security measures and be certified with a "Cyber Badge".[25] This certification demonstrates they have undergone training on secure operation principles consistent with industry-leading cybersecurity standards such as the NIST, ISA/IEC 62443-2-4 and ISO/IEC 27000-series, and possess up-to-date equipment and software to carry out their work on a customer site.

Figure 3

Focus areas per role throughout the value chain[26]



c. Helping customers secure their installed base

Schneider Electric understands patching is an important process and works with its customers to perform patching on the products installed in their environment, so to not become targets.

The company has built an operational technology threat intelligence capability supporting risk identification and qualification within a customer's install base. It seeks to proactively detect and engage with customers to inform and qualify risks, improving visibility, thereby enhancing risk management for both parties. This collaborative approach enables the company to learn from identified exposures and secure the development of future digital architectures.

To better support its customers in protecting their operational environments, Schneider Electric offers customized Solutions and Services.[27] Cybersecurity experts collaborate with them in designing and implementing comprehensive defense strategies that specifically target their security challenges for new and existing installations, regardless of the system vendors involved.

[25] "Cyber Badge Principles", April 2022, https://www.se.com/id/en/download/document/Cyber-Badge-Policy/

[26] "Cyber Resilience in the Electricity Ecosystem: Securing the Value Chain", November 2020, https://www.weforum.org/whitepapers/cyber-resilience-in-the-electricity-ecosystem-securing-the-value-chain/

[27] Schneider Electric Cybersecurity Services

Pillar 5: Meeting Customer and Authority Expectations

The recent wave of large-scale cyber-attacks shows how essential it is to bring the international community together to protect peace and security in the digital space.[28]

a. Cooperating with the ecosystem to share knowledge, insights, and practices

Schneider Electric firmly believes that partnering with others is key to building a more resilient security posture for the broader industry. Through collaboration, we can collectively stay ahead of evolving threats, learn from others' practices, and collaborate on innovative solutions that can benefit customers and society as a whole.

Schneider Electric works closely with cross-industry organizations and is a founding member of the ISA Global Cybersecurity Alliance, a member of both the Paris Call and the Cybersecurity Coalition. As a signatory of the Cybersecurity Tech Accord, the company works closely with its partners to address supply chain security concerns. It actively contributes to the World Economic Forum through the Global Future Council on Cybersecurity, the Oil and Gas, Electricity and Manufacturing Groups to help strengthen resilience across the industry by leveraging collective intelligence and expertise.

Schneider Electric also supports a wide range of partnerships with universities, private institutions, think tanks, NGOs and government agencies to strengthen innovation and improve security integration into its products and solutions.

For example, the company is an active member of Cybersecurity at MIT Sloan (CAMS) and collaborates with Commissariat de l'Energie Atomique (CEA) research.

b. Working with authorities and national agencies

Schneider Electric actively contributes to the development of cybersecurity policies, regulations, and standards in its major regions of operation. The company is involved in over 26 globally recognized standards organizations in the U.S., Europe, and Asia Pacific, actively contributing to advance the interests of its customers and industry. For example, Schneider Electric partners with the World Economic Forum to establish a common reference point for driving more regulatory consistency globally. [29]

The company often volunteers as an early adopter to drive the evolution of its processes and products. For example, Schneider Electric was the first equipment manufacturer to provide hardware and software components for identifying and mitigating cybersecurity vulnerabilities in the energy supply chain through the U.S. Department of Energy CyTRICS program.[30]

c. Engaging with customers

Schneider Electric receives requests from customers regarding its posture on cybersecurity, product security and data protection. A Trust Center service helps provide responses in a timely manner. To enhance Trust with its customers and critical infrastructure clients, Schneider Electric promotes dialogue for transparent communication regarding information-sharing, security framework, certifications, and posture.

---

[28] "Paris Call", December 2018, https://pariscall.international/en/

[29] Cyber Resilience in the Electricity Industry, July 2020

[30] DOE CESER Partners with Schneider Electric, September 2020

Conclusion

At Schneider Electric, cybersecurity, product security and data protection are crucial business imperatives, especially as the company serves critical infrastructure. Security of the operational landscape, sovereignty of data, and survivability of systems are crucial for societal security and stability.

The company is committed to doing business responsibly and with integrity, earning and sustaining Trust in its products, systems, and services. Mitigating risks stemming from developing threats is the result of continuous dialogue and cooperation with governments, suppliers, and customers, growing resilience through collaboration.