Schneider Electric
Product & Offer Security

As the threat of cyber security attacks and product exploitation in today's digital world increases rapidly, so does our customers need for more secure products. Our products and solutions are being used for operating critical infrastructure such as buildings, traffic systems, power plants, gas and oil production and manufacturing plants. Schneider recognizes the importance of having an active and aggressively managed cyber security function. Thus, Schneider is responding to these potential risks by incorporating security protections and processes as it develops and deploys products, services and solutions. As a company we understand the regulatory and compliance requirements our customers demand. That is why we are taking the initiative to deploy Secure Development Lifecycle (SDL) practices in our products and offerings. SDL is a development process that helps build more secure offerings and addresses security compliance requirements.

The following is a list of some of our security practices by stage:

Train:
We continually train our employees to design, develop, test and deploy more secure offerings.

Requirements:
By researching and writing detailed security requirements, we enumerate the cyber security features and customer security requirements to be included in the product development.

Design:
Security architecture documents are produced that follow industry accepted design patterns to develop the security features required by our customer. These documents are reviewed and threat models are created to identify, quantify, and address the potential security risks.

Develop:
Implementation follows the detailed design, and is guided by documentation for best practices and coding standards. We use a variety of security tools as part of the development process including static, binary and dynamic analysis of the code.

Verify:
Security testing on the product implementation is performed from the perspective of the threat model and robustness. Regulatory requirements as well as the deployment strategy are included as part of the test cases.

Release:
Security documentation that defines how to more securely install, commission, maintain, manage and decommission the product or solutions is developed. Security artifacts are reviewed according to the Requirements Phase plan and to the security level that was targeted.

Deploy:
The project team or deployment leader preps the field on how to sell the offer, how to respond via Tech Support to secure offer inquiries, and how to install and optimize the security features. Our services team can provide help for customers to install, manage, and upgrade our products and solutions.

Respond:
Schneider Electric has a Corporate Product Cyber Emergency Response Team (CPCERT) that manages vulnerabilities and supports our customers in the event of a cyber incident.

Schneider Electric is well aware of the geopolitical and technical challenges brought on by the consideration of cyber security for Critical Infrastructure. We are organizing our company to help respond to that challenge with updated processes, technical solutions, support for our customers, and education to our employees on the importance of our role in helping to protect Critical Infrastructure and society as a whole.