Secure Development Practices & Security Controls

NIS2 – Article 21.2 (d) supply chain security

Cyber supply chain risk management is mandated in NIS2, meaning organizations must assess and take into account the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures.

Secure Development Procedures

Secomea is certified for our compliance to IEC 62443-4-1, meaning we follow the requirements for Security Development Lifecycle Assurance (SDLA). The standard mandates security concerns to be proactively addressed at an early stage in the product lifecycle and thus ensures that security measures are built into the product.

Cybersecurity Practices

Secomea is using the following practices:

- **Specification of security requirements**
  Minimum security requirements for the development and deployment of the product are established. Threat analysis and risk assessment play important roles in identifying and classifying the potential security risks, and they involve the definition of trust boundaries for process, data, and control flow including any communication to internal and external peripherals.
- **Secure by design**
  The product is designed to implement the security principles of dependability, trustworthiness, and resilience. Securing the design through the application of best practice principles such as defense in depth and threat modelling. A thorough functionality and security verification of the model will be performed.
- **Security verification and validation testing**
  All security requirements for the product must be shown to have been met, and the product's defense in depth strategy shown to be effective when the product is deployed. A requirements-based testing approach is applied to show that functional and security requirements have been correctly implemented.

Secomea is continuously audited by the external security company performing risk analysis and assessment of the Secomea solution against the security levels of the international standards IEC 62443-3-3 and IEC 62443-4-2 for Industrial Automation Control Systems (IACS) components. The solution is also assessed against the IT baseline security protection requirements defined by the German federal office for information security (BSI).

Organizational Security

Our Organizational Security measures are documented in an ISAE3402 control report. We have auditors verifying that our control program is consistent, complete, repeatable, and auditable.

ISAE3402 is the international auditing standard for assurance reports on controls at service organizations. The report provides a description of the general information security controls related to Secomea's services to customers. The auditors have reviewed all the commonly accepted information security controls specified in ISO 27002:2017.

Cybersecurity advisory process

Secomea has the capability to identify and respond to vulnerabilities as well as work with customers to mitigate their risks using our defined cybersecurity advisory process. Our cyber advisory process includes an expected timeframe and conditions under which vulnerability information will be published.

Secomea is an official CVE Numbering Authority (CNA), and you can find our clearly defined and easily accessible intake mechanism to accept vulnerability information here: Cybersecurity Advisory - Secomea

Mitigating Cybersecurity Risks

Used together, Secomea's device cybersecurity capabilities and nontechnical supporting capabilities can help you mitigate cybersecurity risks related to the use of IoT devices while assisting you in achieving your goals – optimizing uptime of your IACS components and ensuring continuous delivery of the important services our society depends on.

Prevention, operational readiness, and collaboration in cyber defense are key. All three aspects can be covered when choosing Secomea as your supplier for secure remote access.