SECOMEA

Security by design for cyber-physical systems

At Secomea, cybersecurity takes up a pivotal role. Everything we do follows internationally recognized industry best practices, and each stage of product development meets rigorous cybersecurity standards.

As a result, our products can be trusted to be secure from the moment they are deployed and after updates and new features are released.

The pillars of our cybersecurity strategy

NEVER TRUST, ALWAYS VERIFY

Zero Trust Model

Our solution is engineered with Zero-Trust principles at its core to prevent the risk of unauthorized entries through a robust focus on identity verification and access control.

MULTI-LAYERED APPROACH

Defense in Depth (DID)

Secomea's solution employs a combination of tiered protective measures to secure your organization's assets - from MFA to data encryption and network segmentation.

ICS NETWORK SEGMENTATION

Purdue Model (PERA)

Secomea's solution can be seamlessly integrated into your existing setup to define access boundaries and restrict communication down to each specific device's IP and port.

OUR SECURITY IS YOUR SECURITY

Secure development practices

Specification of security requirements

Minimum security requirements for the products' development and deployment are established. Threat analysis and risk assessment play important roles in identifying and classifying potential security risks. They involve defining trust boundaries for process, data, and control flow, including any communication to internal and external peripherals.

Secure by design

Our products are designed to implement the security principles of dependability, trustworthiness, and resilience. We ensure they are secure by design through the application of best practice principles such as defense in depth and threat modeling.

Security verification and validation testing

We verify the security of our products before deployment through validation testing that demonstrates the products' defense-in-depth strategy is effective. We apply a requirements-based testing approach to show that functional and security requirements have been correctly implemented.

THIRD-PARTY AUDIT ASSESSMENTS

Our security certifications

To show our formal commitment to securing our services, our system continually undergoes third-party security audits and assessments.

Through this significant investment, Secomea ensures the most advanced protection for its customers and demonstrates compliance with the following industry standards and best practices:

IEC 62443-4-1
on secure product development lifecycle requirements

This certification confirms that Secomea develops and maintains secure products by following a secure development lifecycle (SDL), including a secure-by-design development methodology, secure implementation, patch management, and product end-of-life.

IEC 62443-3-3
on system security requirements and security levels

This certification attests to Secomea's compliance with the technical control System Requirements (SRs) associated with the seven foundational requirements (FRs): Identification and authentication control (IAC), Use control (UC), System integrity (SI), Data confidentiality (DC), Restricted data flow (RDF), Timely response to events (TRE), and Resource availability (RA).

ISAE 3402
based on ISO 27002

Our organizational security measures are assessed and documented in a third-party ISAE 3402 report, which is the international standard providing assurance on an organization's adequate internal controls.

Our certification attests that our controls are consistent, complete, repeatable, and auditable and demonstrates to our customers that they are adequate to ensure the security of Secomea's services.

Secomea's controls have been reviewed based on the guidelines specified in ISO 27002 for organizational information security standards and information security management practices.

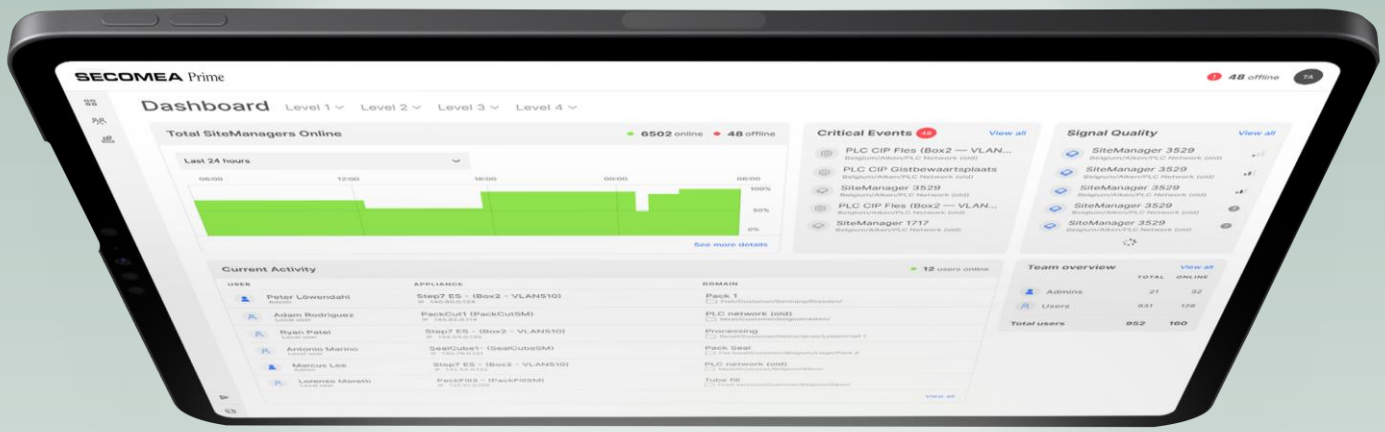
TRANSPARENCY AND ACCOUNTABILITY

Secomea is an official CVE Numbering Authority (CNA)

Secomea has been recognized by CISA as a CVE Numbering Authority (CNA), making it the first and, until recently, the only one in Denmark.

This means we are one of the few entities worldwide that can identify and name cybersecurity vulnerabilities. To this end, we have a Cybersecurity Advisory process in place through which our customers can report suspected security risks.

SECOMEA



SECOMEA Prime

Access, control, and protect your OT environments remotely with our purpose-built security features

Access

Grant access after approval of requests

In addition to scheduled and on-demand remote access, admins can enable access after approving user requests indicating the reason, timing, and duration of the remote access session.

Enable MFA and SSO

Users can only remotely access assets for which they have permission. Access is granted only after secure identity verification with Multi-Factor Authentication via SMS or Single Sign-On (Azure AD or Okta).

Scan transferred files for virus and malware

Files transferred remotely to or from an engineering station can be scanned for viruses or malware to assess and confirm their safety before downloading them.

Manage

Robust access governance

Establish role-based access control built on the least privilege principle. Set up hierarchy-based user roles and permissions individually or use the advanced grouping feature for bulk management of user access rights.

Real-time monitoring and audit logs

Maintain ongoing control and full transparency over your remote access sessions by checking the overview of current activities. All sessions are logged to keep track of who accessed which asset, when, and what they did.

Event alerts setup and automated actions

Configure alerts via email or SMS to be notified of specific events and set up actions automatically triggered by the occurrence of certain events.

Defend

Encryption and network segmentation

Connect your assets via AES 256bit encrypted tunnels based on TLS. Restrict connections down to each specific device's IP address and port, both remotely and on-site with I/O ports for physical control.

Protection against MitM attacks

Each Secomea's M2M server has a unique TLS certificate/key to which a Secomea's gateway binds the first time they connect (aka ToFu "Trust-on-first-use") and against which any subsequent connections are verified. Any change requires manual configuration.

Identify system vulnerabilities

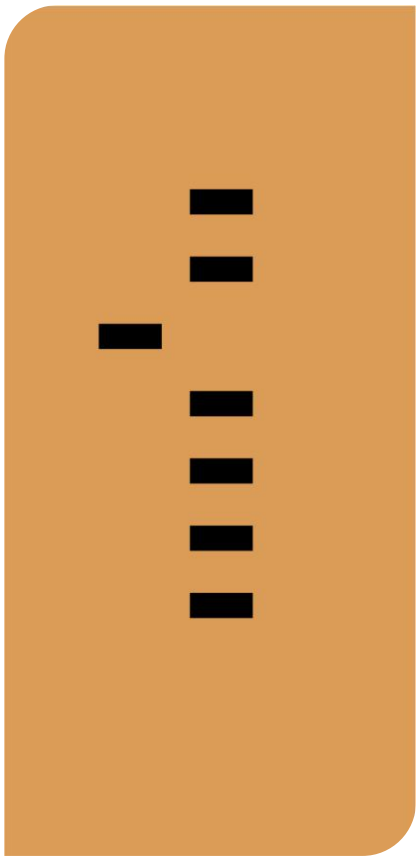
Easily check the security status of your remote access system in the Vulnerability Hub. Identify vulnerabilities due to outdated software and hardware to act promptly and keep everything current effortlessly.

TRANSPARENCY AND ACCOUNTABILITY

Supporting your compliance efforts

Secomea's cybersecurity capabilities can help you mitigate risks related to the use of IoT devices while assisting you in achieving your goals, such as optimizing the uptime of your IACS components and ensuring continuous delivery of essential services our society depends on.

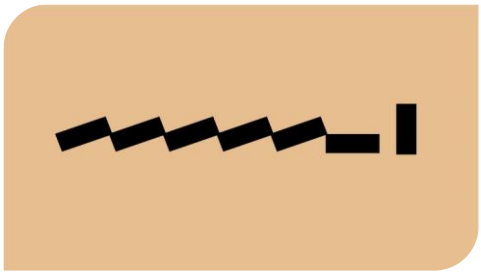
Prevention, operational readiness, and collaboration in cyber defense are key. All three aspects are covered when choosing Secomea as your supplier for secure remote access.



BEFORE

Predictive maintenance

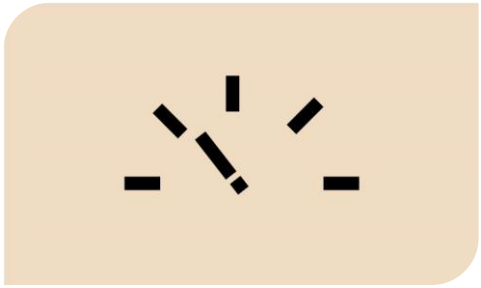
Stay ahead of system failures with predictive maintenance features. Identify potential issues before they escalate.



DURING

Crisis management

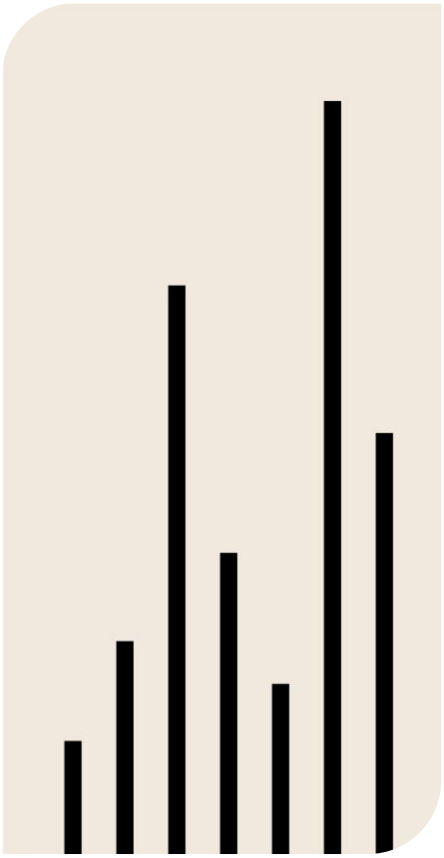
Isolate and contain threats in times of crisis. Whether through air gap or island mode configurations, you can effectively prevent the spread of disruptions.



DURING

Business continuity

Rely on real-time monitoring capabilities to detect vulnerabilities within your factories, including outdated machinery and connectivity issues.



AFTER

Forensic analysis

Review audit logs and session recordings to learn from past incidents and adjust your risk management strategies.

Simplify compliance governance

From physical safety to cybersecurity, from the **NIS2 legislation** to the **Cyber Resilience Act (CRA)** - we guide you as you navigate your regulatory environment, ensuring compliance without compromising efficiency.

Any questions? Reach out to us