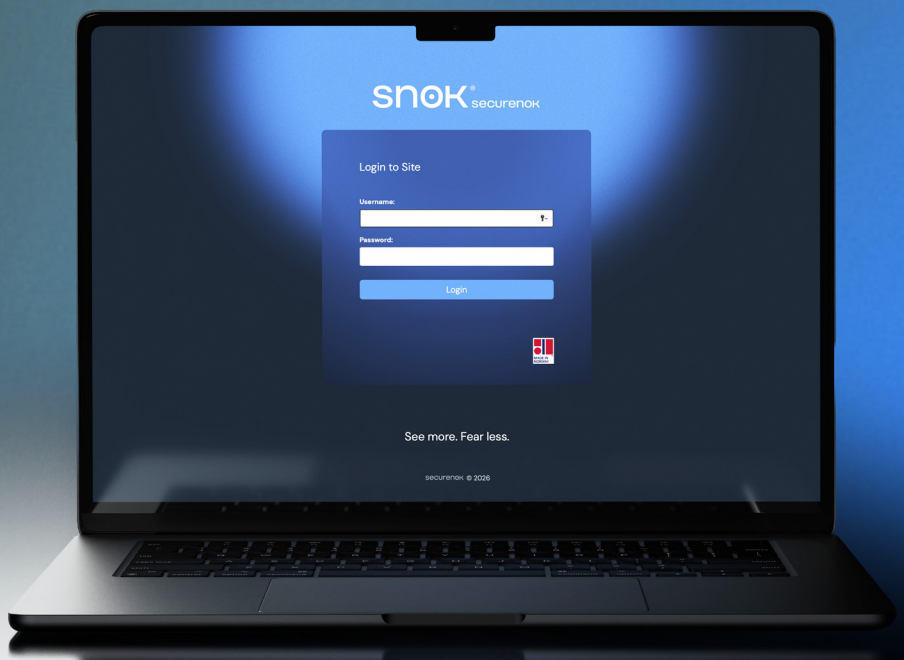
PRODUCT BROCHURE

SNOK® Cybersecurity Monitoring System



See more. Fear less.

securenok®

"At Securenok, we believe industrial organisations need to see what is happening in their OT environments and detect unwanted activity before it affects operations."

Industrial operations depend on systems that were not always designed for today's connected threat landscape.

SNOK® was developed specifically for industrial environments – providing continuous visibility and early warning while respecting the operational requirements of critical systems.



Tonje Rønneberg Skei
Chief Executive Officer

Continuous visibility and early warning for industrial OT environments.

The SNOK® Cybersecurity Monitoring System provides early warning of cyberattacks and unwanted changes in Industrial Automation and Control Systems (IACS), often referred to as Operational Technology (OT).

SNOK® combines information from industrial network traffic, critical Windows and Linux endpoints and industrial controllers. Sensor information is collected and analysed in the SNOK® Platform to establish normal behaviour, identify deviations and provide operators and security teams with actionable security insight.

Through a single web-based user interface, users can monitor discovered assets, network communication, security events and alarms without losing sight of the operational context.

- Real-time situational awareness across the monitored OT environment
- Continuously updated asset and communication overview
- Behaviour-based detection of suspicious or abnormal activity
- Early warning of cyber threats and unwanted changes
- Monitoring data and operational visibility can remain within the customer's secured environment

- Actionable security insights
- Compliance with IEC 62443 and NIS2



- Early detection of cyber threats
- On-premise deployment, full data control

CYBER ESSENTIALS CERTIFIED PLUS

MADE IN NORWAY

SNOK® combines network, endpoint and controller-level monitoring to reduce blind spots.

SNOK® Network Sensor

Passively monitors traffic from industrial switches and routers to identify assets, communication patterns and anomalous network behaviour.

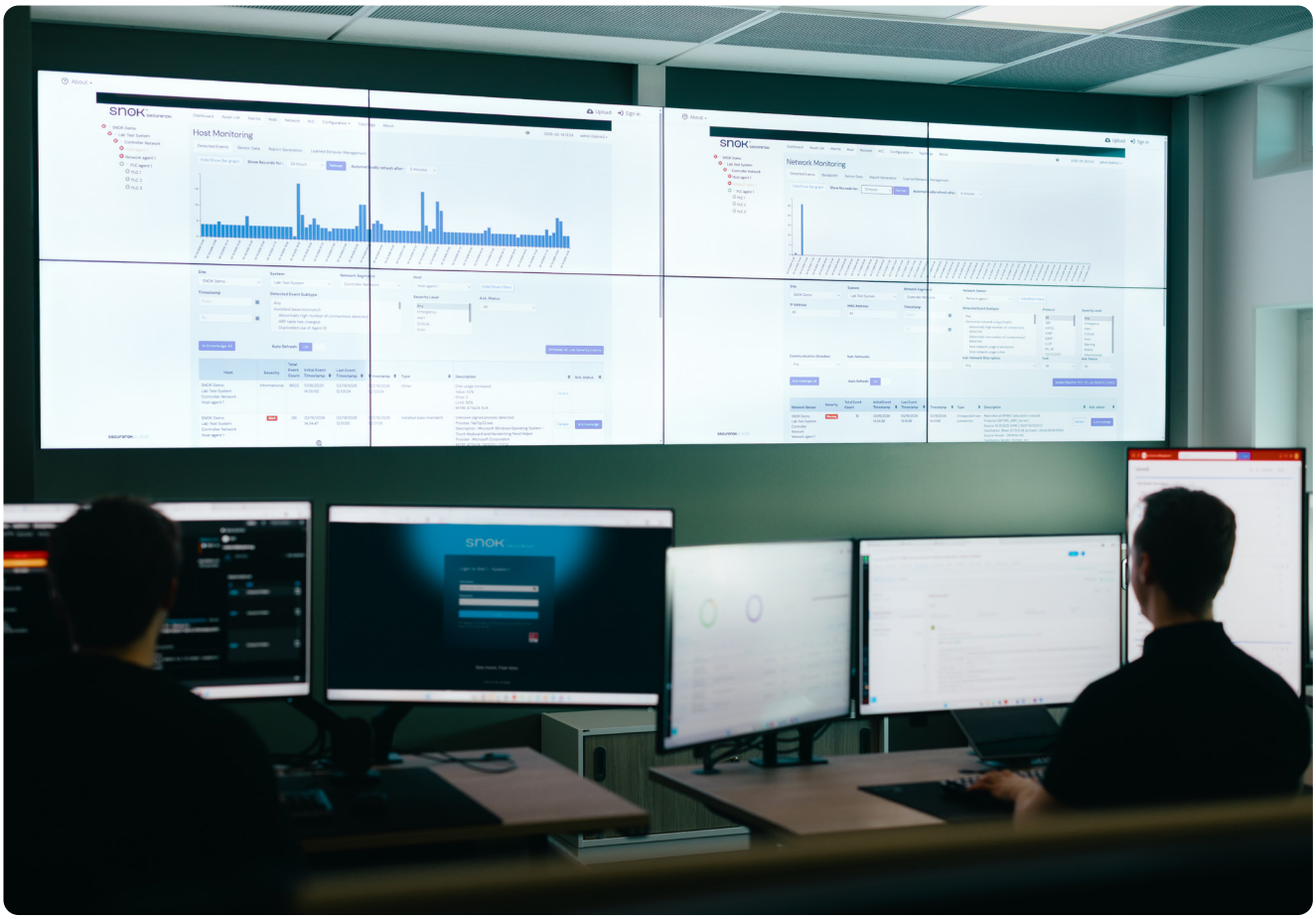
SNOK® Endpoint Sensor

Installed on Windows and Linux endpoints to monitor processes, system behaviour and security-relevant changes directly on critical hosts.

SNOK® PLC Sensor

Uses industrial protocols to collect information from supported PLCs and detect changes that may indicatereprogramming or unauthorized manipulation.

A SNOK® installation can consist of one or many sensors of any type. This makes it possible to adapt visibility to the architecture, criticality and risk profile of each industrial environment.



SNOK® Network Sensor

Passive network visibility without disturbing industrial operations.

The SNOK® Network Sensor collects network information from mirrored traffic on industrial switches and routers. It is designed to observe communication without actively interfering with the industrial process.

By monitoring traffic over time, SNOK® builds an understanding of the assets present in the network, how they communicate and what normal network behaviour looks like.

- New equipment communicating in the network
- Changes in traffic between existing equipment and computers
- Unexpected or new communication paths
- Exposure to insecure networks and new remote connections
- Asset and communication information for investigation and risk assessment

"It is often impossible to keep OT environments fully up to date with security patches. Continuous monitoring with sufficient visibility is therefore essential to detect and respond early to intruders who have managed to bypass perimeter controls and gained access."



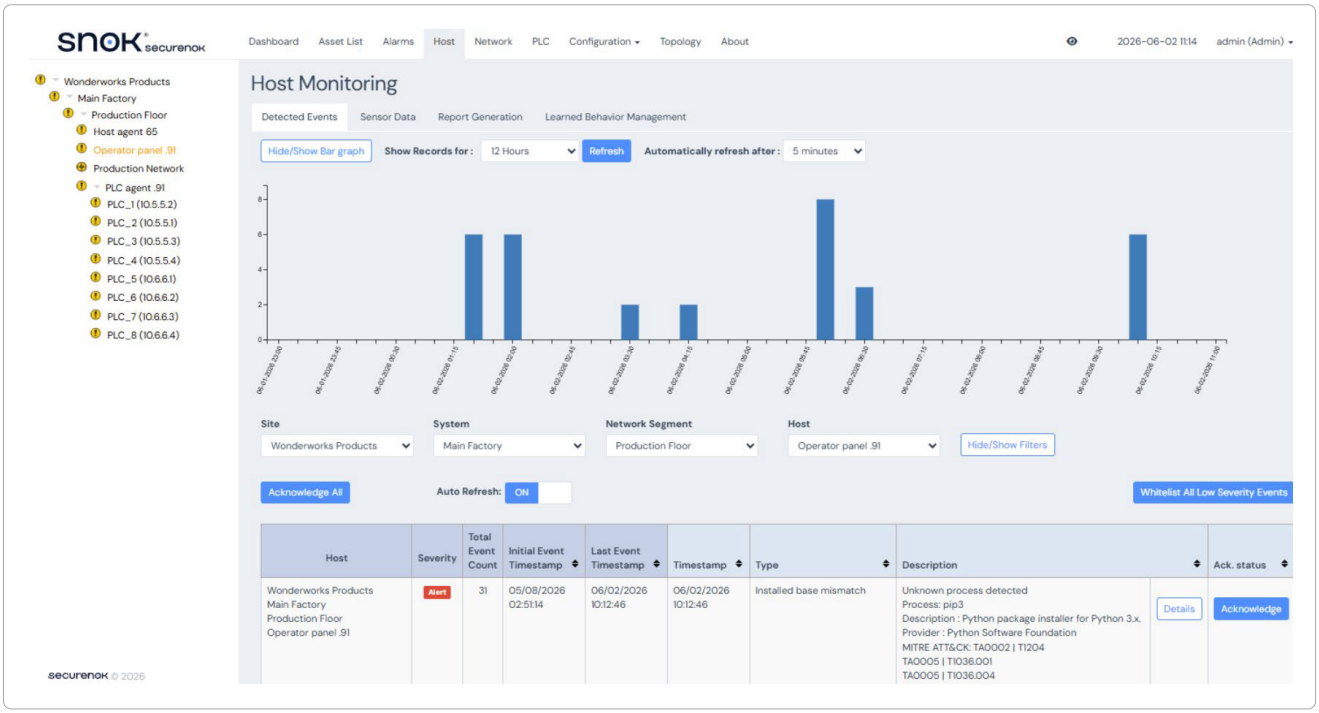
Nina Hesby Tvedt
Chief Technology Officer

SNOK® Endpoint Sensor

Host and PLC Sensors add visibility where network monitoring alone may not be enough.

SNOK® Endpoint Sensor are installed on Windows and Linux endpoints in the OT environment and monitor behaviour directly on the system. They supplement network visibility with information from critical HMIs, SCADA workstations, historians, servers and other industrial endpoints.

- New processes detected on the endpoint
- USB devices inserted
- Anomalies in endpoint resource usage
- Operating system and security configuration information
- Process and application behaviour relevant to security investigations



SNOK® PLC Sensor

SNOK® PLC Threat Detection provides deeper insight into supported industrial controllers. For Siemens S7 environments, the sensor can collect status information and detect changes such as PLC property, configuration or memory changes.

- Attempts to reprogram or change PLC configuration
- Changes that may occur over the network or through local/on-site manipulation
- Additional controller information for asset and security analysis



Firewalls are essential. But permitted traffic is not necessarily safe traffic.

Firewalls are a fundamental part of OT security. They control which communication is allowed between networks and security zones. However, important activity can also take place within the same OT network, behind the firewall, or through communication that the firewall is configured to permit.

SNOK® complements existing security controls by continuously monitoring network communication, critical endpoints and supported industrial controllers. This provides visibility into changes and abnormal behaviour that perimeter security alone may not detect.



SNOK® does not replace your firewall.
It adds visibility behind it.

- A new or unauthorized device starts communicating inside the OT environment
- Known assets begin communicating differently over permitted network paths
- A new process starts or a USB device is inserted on a critical Windows/Linux endpoint
- A supported PLC is reprogrammed or its configuration changes

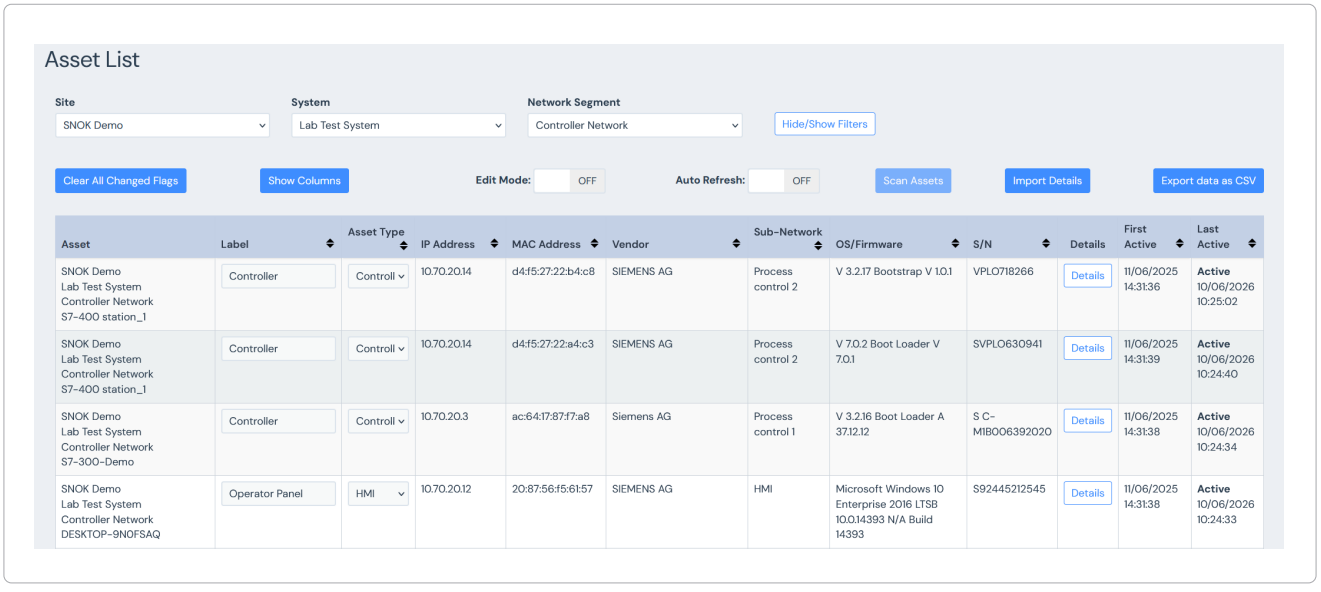


Know what is connected, how assets communicate and where unexpected activity occurs.

Effective OT security starts with knowing what is connected, how assets behave and how they communicate. SNOK® combines asset information with continuous monitoring of network activity, providing context for anomaly detection, vulnerability assessment, threat investigation and risk management.

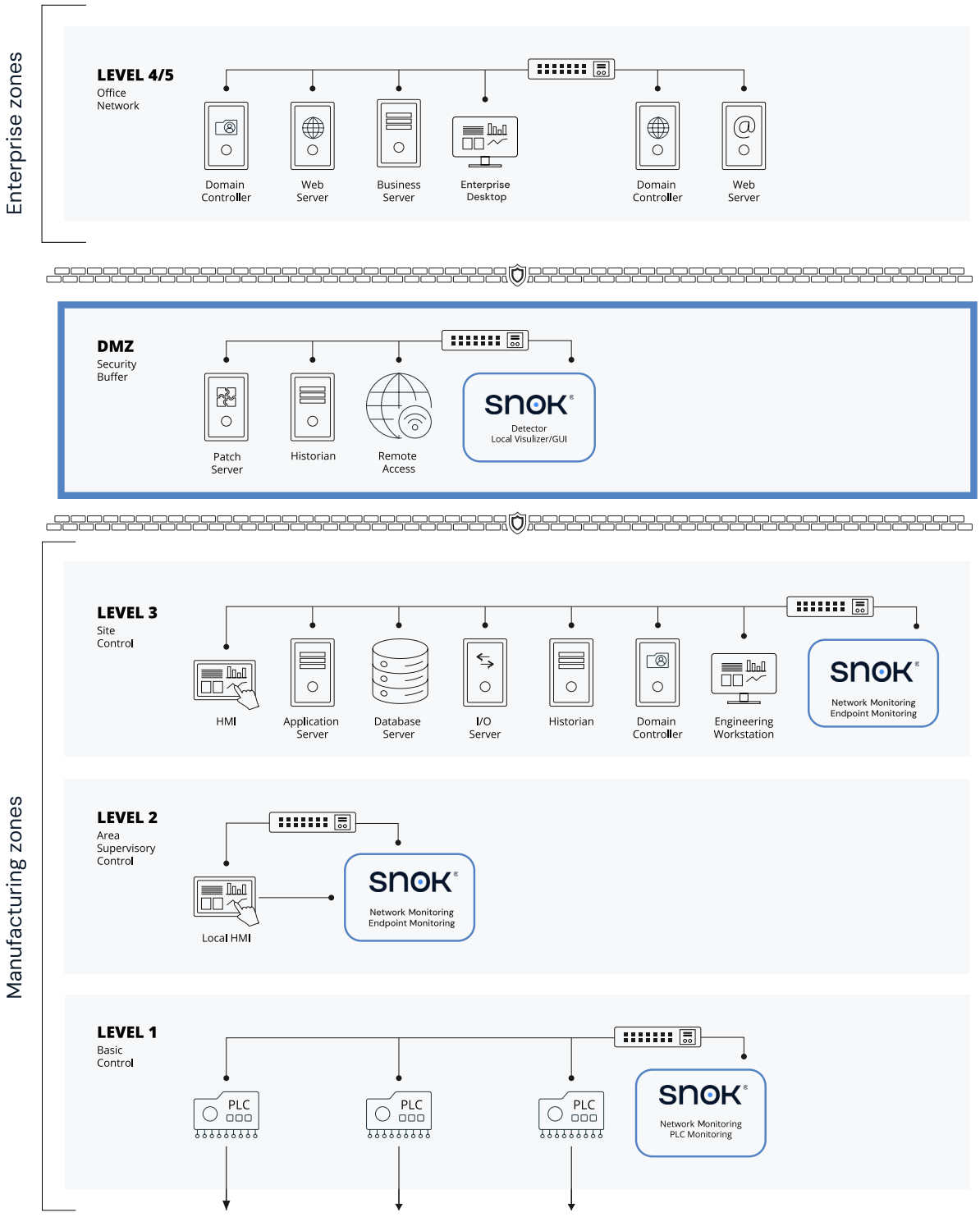
Asset discovery and communication insight:

- Build an asset inventory primarily through passive monitoring of network traffic
- Identify communication relationships and changes over time
- Display available information such as IP and MAC address, vendor, hostname, asset/node type, subnet, operating system or firmware, and observation timestamps
- Enrich asset information using Endpoint sensor and PLC Sensors
- Optionally use low-impact active scanning where appropriate and operational risk has been considered
- Export information for external assessment and security processes



Flexible deployment in industrial environments

Deploy SNOK® where visibility is needed – from network zones to critical endpoints and controllers. SNOK® can be deployed using physical or virtual components and scaled from a single monitored network to environments with multiple sensors and industrial zones.



Use SNOK® as an OT visibility and detection layer within existing security operations.

Alarms and detected events from the SNOK® Platform can be integrated with third-party systems such as SIEM and SOAR platforms.

SNOK® supports streaming of alarms and events using Webhook or Syslog and provides a REST API that can be used to retrieve alarms, events and other platform information.

This allows customers and security partners to combine OT-specific monitoring from SNOK® with established SOC processes, workflows and response capabilities.

CORTEX XSOAR BY PALO ALTO NETWORKS

servicenow

splunk>

Microsoft Sentinel



Public Use Case

From OT visibility to continuous security monitoring

IVAR started with a SNOK® Health Check and continued with SNOK for ongoing OT monitoring.

IVAR

Customer profile

- Owned by 12 municipalities in Rogaland
- Supplies over 360,000 residents
- 8 water treatment facilities

"With a health check based on the SNOK® technology, we gained a full overview of what is actually happening in the OT network. It gave us both increased operational security and a concrete tool for meeting new regulatory requirements."



Svein Roar Aas
IT Security Advisor – IVAR IKS

Following the Health Check, IVAR chose to buy and implement the SNOK® Cybersecurity Monitoring System in its process facilities. SNOK® is used for continuous OT monitoring, and security events are connected to SOC services for ongoing monitoring and follow-up.

Customer journey

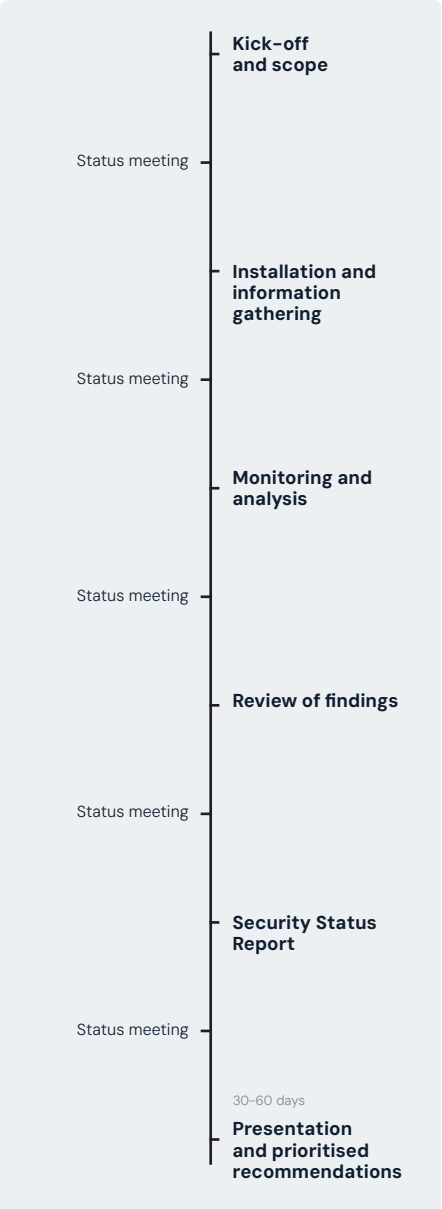
- SNOK® Health Check used to establish visibility into assets, communication and security weaknesses
- Security Status Report with prioritized short- and long-term actions
- SNOK® selected for continuous monitoring and implemented in the process facilities
- Security events connected to SOC services for ongoing monitoring and follow-up
- A scalable foundation for extending OT monitoring across additional facilities

OT Health Check

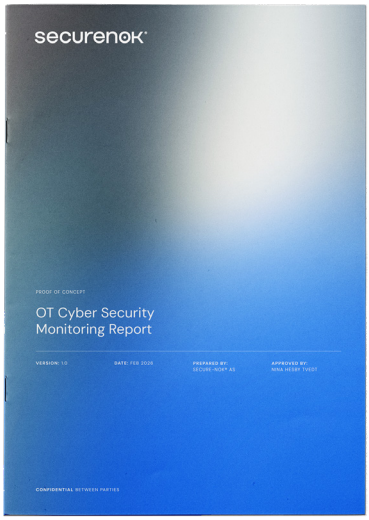
A fast, fact-based starting point for OT security.

A SNOK® Health Check is a practical assessment of the security status of an OT environment. The SNOK® Platform is connected to the selected network and monitors traffic over an agreed period, providing insight into what is actually connected and communicating and where security efforts should be prioritised.

The platform can be installed **without planned production shutdown**. Network data can be stored and analysed **locally within the customer's environment,** with **access controlled** by the customer.



- Asset and communication overview
- Identified weaknesses and unwanted behaviour
- Prioritised recommendations
- Input to risk assessments, IEC 62443 / regulatory work and OT security planning
- Recommended setup for continuous monitoring



See more. Fear less.

securenok®

SECURENOK® AS | Luramyrveien 29, 4313 SANDNES, NORWAY, **www.securenok.com**

CYBER ESSENTIALS CERTIFIED PLUS

MADE IN NORWAY