securenok®

WHITE PAPER

Protecting PCS 7 Distributed Control Systems Against Cyberattacks

PREPARED BY:
SECURENOK® AS

See more. Fear less.

Navigating Cybersecurity Challenges in Manufacturing

Industrial control systems such as Siemens PCS 7 are at the heart of critical operations across industries. From oil and gas, energy and chemicals to manufacturing, food production and water infrastructure.

As industrial environments become more connected, the cyber threat is also evolving. Recent warnings from CISA and other authorities demonstrate that attackers are increasingly targeting industrial controllers directly, making visibility and detection inside the OT environment more important than ever.

This whitepaper looks at the cybersecurity challenges associated with Siemens PCS 7 and S7 controllers, and explains how the SNOK® Cybersecurity Monitoring Platform, including network, endpoint and direct PLC threat detection, can provide additional layers of protection for critical industrial operations.

Tonje Rønneberg Skei
Chief Executive Officer

securenok®

Distributed control systems are at the heart of modern industry and critical infrastructure.

Distributed Control Systems (DCS) are computerized systems used to control and automate industrial processes. They are deployed across a wide range of industries and critical infrastructure, including oil and gas, energy production, chemicals, manufacturing, food and beverage, pharmaceuticals, water and wastewater, district heating and other process industries.

DCSs are particularly important in complex and large-scale processing facilities where reliability, availability and safety are critical. In these environments, disruption of the control system can have consequences far beyond loss of IT services, potentially affecting production, equipment, safety and the physical process itself.

The Siemens SIMATIC PCS 7 is one of the most widely deployed distributed control systems and has been used in industrial facilities around the world for decades. PCS 7 continues to be used both in existing installations and in new industrial projects.

Because of the critical processes controlled by these systems, protecting PCS 7 environments against cyberattacks is essential.

Today's threat situation and regulatory response.

Owners and operators of industrial facilities and critical infrastructure must increasingly assume that their OT environments may become targets of cyberattacks.

Threat actors range from sophisticated and well-funded nation-state groups to organized cybercriminals, hacktivists and other actors making use of increasingly accessible cyber capabilities.

A successful attack against an industrial control system can result in loss of production, disruption of essential services, manipulation of industrial processes or, in the worst case, consequences for safety and the surrounding environment.

At the same time, the tools available to attackers continue to evolve. Capabilities that once required significant specialist knowledge are increasingly automated and made accessible through commercial attack tools, stolen credentials, malware ecosystems and, more recently, artificial intelligence.

This development has also resulted in significantly stronger regulatory requirements for operators of critical infrastructure.

In the European Union, the original Network and Information Security Directive (NIS1) established common cybersecurity requirements for operators of essential services. It has since been replaced in the EU by the more comprehensive NIS2 Directive, which expands the number of sectors and organizations covered and introduces stronger requirements for cybersecurity risk management, incident reporting, supply-chain security and management accountability.

In Norway, the Digital Security Act (Digitalsikkerhetsloven) and associated regulation entered into force on 1 October 2025, implementing NIS1 into Norwegian law.

The legislation introduces fundamental cybersecurity requirements for organizations providing services that are particularly important to society, including organizations within energy, transport, healthcare, water supply, banking, financial market infrastructure and digital infrastructure.

Organizations covered by the legislation are required to implement appropriate and proportionate technical and organizational security measures based on their risk exposure and to report serious digital security incidents.

Norwegian authorities are also preparing the implementation of NIS2 and the CER Directive, which will expand the scope further and strengthen cybersecurity and resilience requirements for critical and important organizations.

securenok®

How to secure OT systems such as PCS 7?

Industrial automation and control systems are commonly referred to as Operational Technology (OT).

At a fundamental level, securing OT follows many of the same cybersecurity principles as securing other digital systems. Systems must be identified, protected and monitored, and organizations must be prepared to respond to and recover from cyber incidents.

These principles are reflected in frameworks such as the NIST Cybersecurity Framework.

However, OT systems such as Siemens PCS 7 also require a tailored approach.

Security technology, processes and procedures must be designed around the specific characteristics of the industrial environment. Equally important, security measures must coexist with the operational environment and must not interfere with or disrupt the industrial process.

The core automation systems in many PCS 7 environments have traditionally been based on Siemens SIMATIC S7 Programmable Logic Controllers (PLCs), including the widely installed S7-300 and S7-400 families.

PLCs are dependable industrial devices designed to execute automation tasks continuously and reliably.

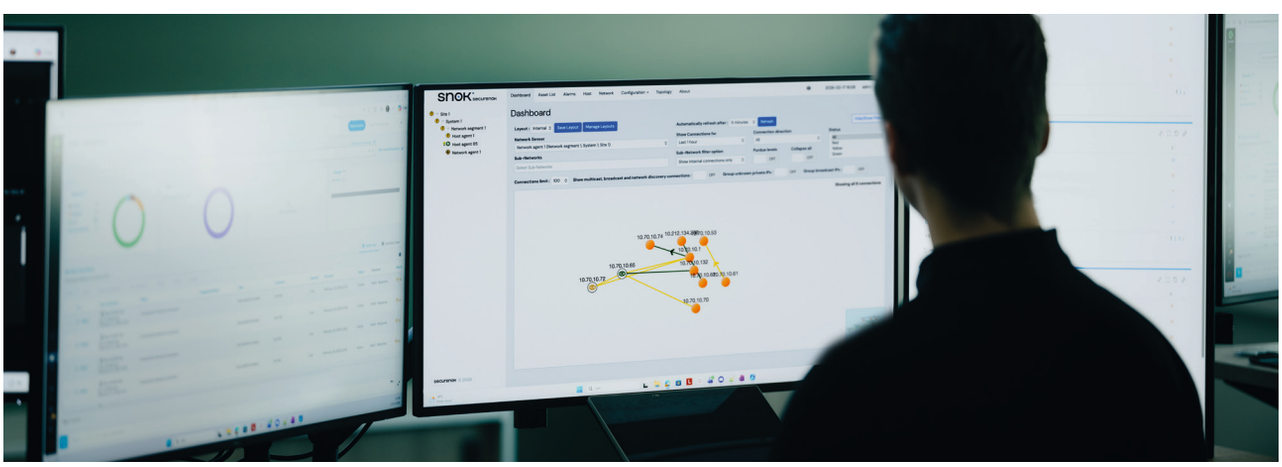
However, many industrial controllers and industrial protocols were originally designed to operate inside trusted and isolated environments. Strong authentication, encryption and other modern security mechanisms were therefore not always fundamental design requirements.

This creates an important cybersecurity challenge when these systems become increasingly interconnected. For this reason, protecting PLC environments should follow a defense-in-depth approach.

This philosophy is reflected in industrial cybersecurity standards and frameworks such as IEC 62443 and the NIST Cybersecurity Framework.

Defense in depth means establishing several independent layers of security around critical systems. The objective is not to assume that one security barrier will stop every attacker. Instead, several layers should work together to prevent attacks where possible and detect malicious activity if preventative controls are bypassed.

An industrial facility should therefore never rely solely on a firewall. Protection should also include segmentation, access control, system hardening, monitoring, detection and response capabilities throughout the OT environment.



The Securenok SNOK solution is tailored to monitor OT systems

The SNOK Cybersecurity Monitoring Platform from Securenok is specifically designed for industrial and OT environments.

SNOK combines several monitoring technologies and sensor types to provide visibility into different layers of the OT environment. This enables organizations to monitor network communication, critical endpoints and industrial controllers and supports a defense-in-depth cybersecurity strategy.

securenok®

SNOK Network Intrusion Detection System

The SNOK Network Intrusion Detection System (NIDS) uses passive sensors to monitor network communication passing through industrial network infrastructure.

Sensors are typically connected to network equipment using port mirroring or SPAN functionality and do not interfere with the industrial traffic itself.

The network sensor learns the normal communication patterns of the OT environment and can identify unauthorized or abnormal activity.

Examples include:

- Asset inventory showing devices communicating through monitored network infrastructure
- Unknown devices or IP addresses appearing on the network
- Changes in protocol usage or communication patterns
- New communication attempts towards PLCs
- Communication to or from external addresses
- Deviations from established network behavior

Deploying sensors at appropriate locations across the OT environment increases visibility and reduces potential monitoring blind spots.

SNOK Endpoint Monitoring

The SNOK Endpoint Monitoring module uses lightweight host sensors installed on Windows and Linux systems within the OT environment.

Typical examples include:

- Engineering workstations
- Operator stations
- HMIs
- Servers
- Other systems with access to industrial controllers

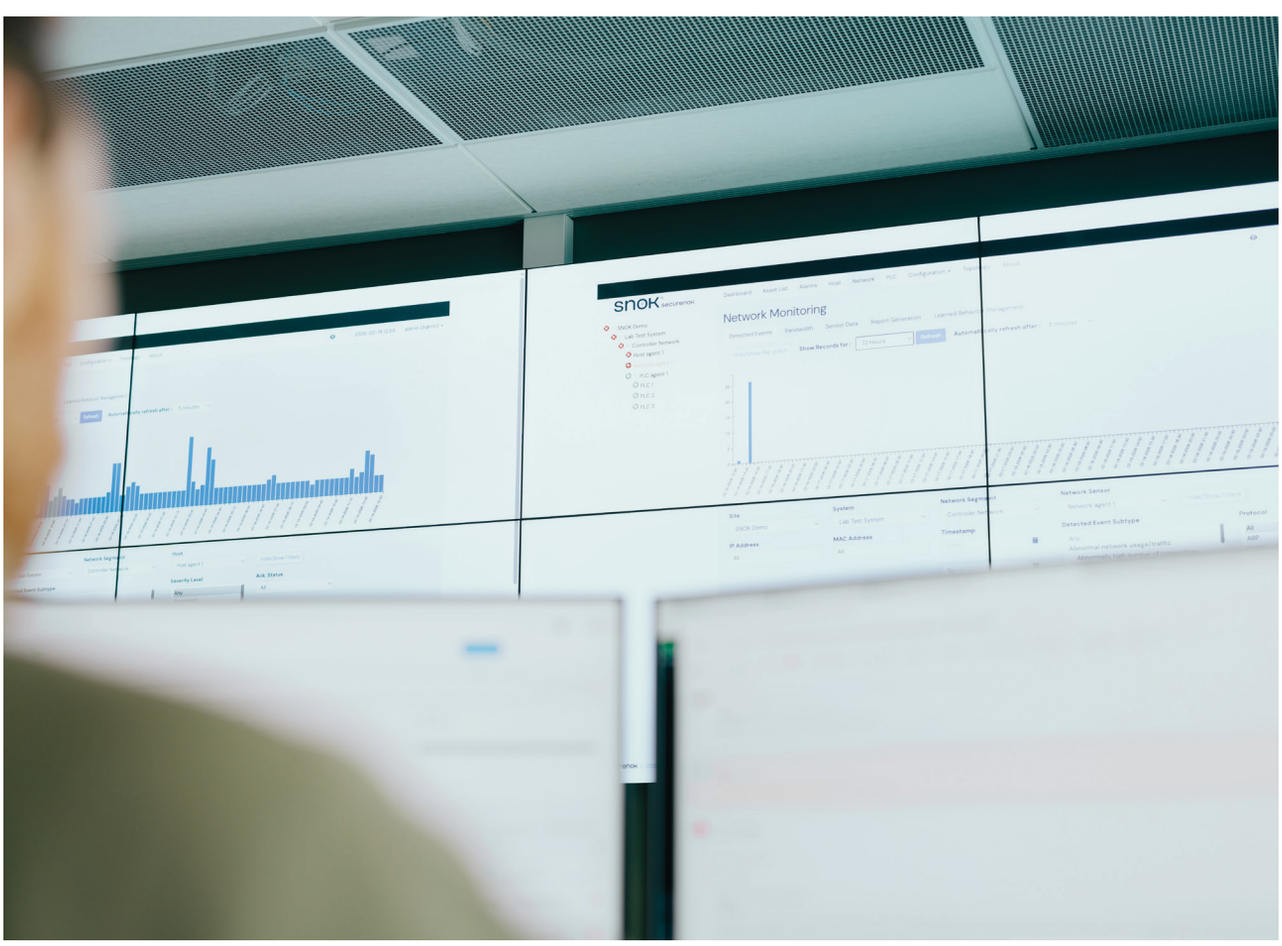
These systems are critical because they often have legitimate access to PLCs and other automation equipment.

They can therefore also become attractive targets for attackers attempting to gain deeper access to the industrial process.

SNOK Endpoint Monitoring can detect events including:

- New processes being started
- Signed or unsigned software execution
- USB device insertion
- Changes to endpoint firewall configuration
- Unexpected changes in system resource utilization
- Changes in network communication
- New or failed user logins

The sensors are designed to be lightweight and non-intrusive and can support both modern and selected legacy operating systems commonly found in industrial environments.



securenok®

SNOK PLC Threat Detection

The SNOK PLC Threat Detection module provides direct monitoring of Siemens S7 controllers, including S7-300 and S7-400 PLCs.

Securenok developed this capability already in 2016, based on the recognition that network monitoring alone cannot always determine whether the logic or configuration inside an industrial controller has been changed.

Today, this technology has moved well beyond the development stage.

SNOK PLC Threat Detection is deployed in active industrial installations, including oil and gas assets, where direct visibility into the condition and behavior of critical controllers forms an additional layer of OT cybersecurity monitoring.

The solution is also offered through multiple SecureNOK partners as part of broader OT monitoring and cybersecurity solutions, enabling asset owners to integrate direct PLC monitoring into their existing security architecture and operational security services.

The PLC sensor runs on separate hardware and communicates with the controller using the PLC's native communication mechanisms to retrieve security-relevant information.

The SNOK PLC Threat Detection module analyzes this information to identify changes that may indicate that a controller has been altered, reconfigured or manipulated.

Examples include:

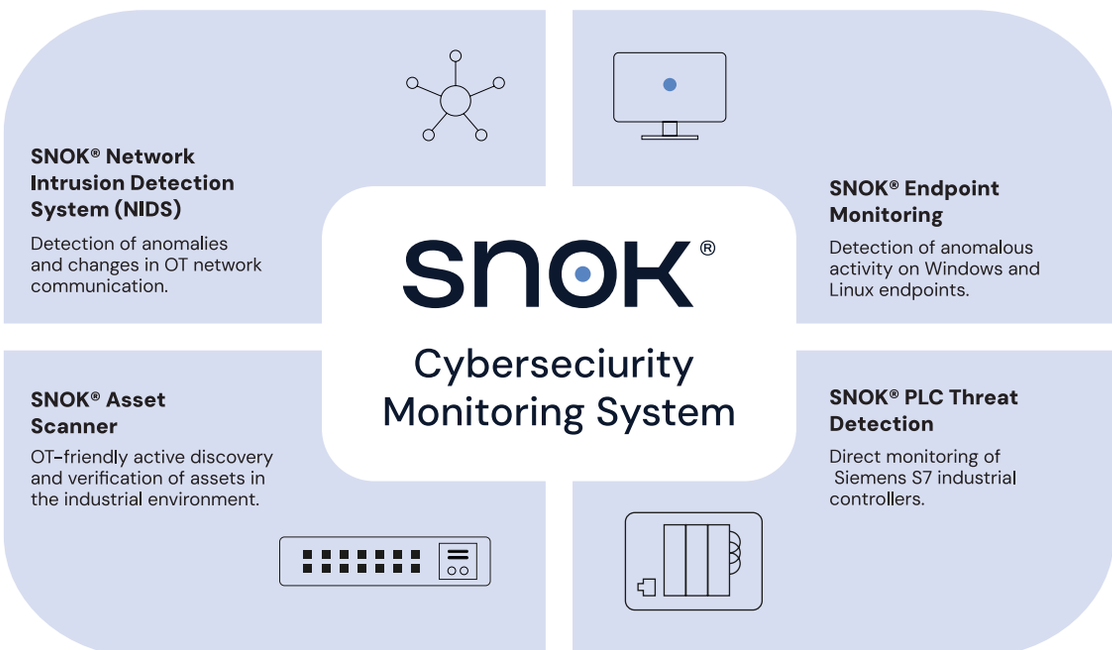
- Changes to PLC properties
- Runtime changes
- Changes to PLC memory blocks
- Changes associated with PLC reprogramming

The purpose is to provide visibility at the controller level itself.

This becomes particularly important in situations where an attacker has already bypassed network security controls or is using legitimate engineering tools, credentials or communication paths to interact with the PLC.

SNOK Product Modules

The different SNOK monitoring technologies complement each other:



SNOK Product Modules.

Together, these technologies provide visibility across several layers of an OT system.

Tuning SNOK to monitor local conditions for each OT environment

Network, endpoint and PLC sensor data is analyzed by the SNOK detection platform.

Anomalies and security-relevant events identified by the sensors can generate detected events and, when appropriate, alarms. SNOK's security analysis combines behavioral baselining with configurable detection rules.

During the baseline period, the system observes the characteristic behavior of the monitored environment. Subsequent deviations from this established behavior can then be identified and assessed.

The configurable ruleset allows organizations to distinguish expected operational variations from activities that violate security policy or require further investigation.

This makes it possible to adapt monitoring to the characteristics of each individual OT environment and its different operational areas.

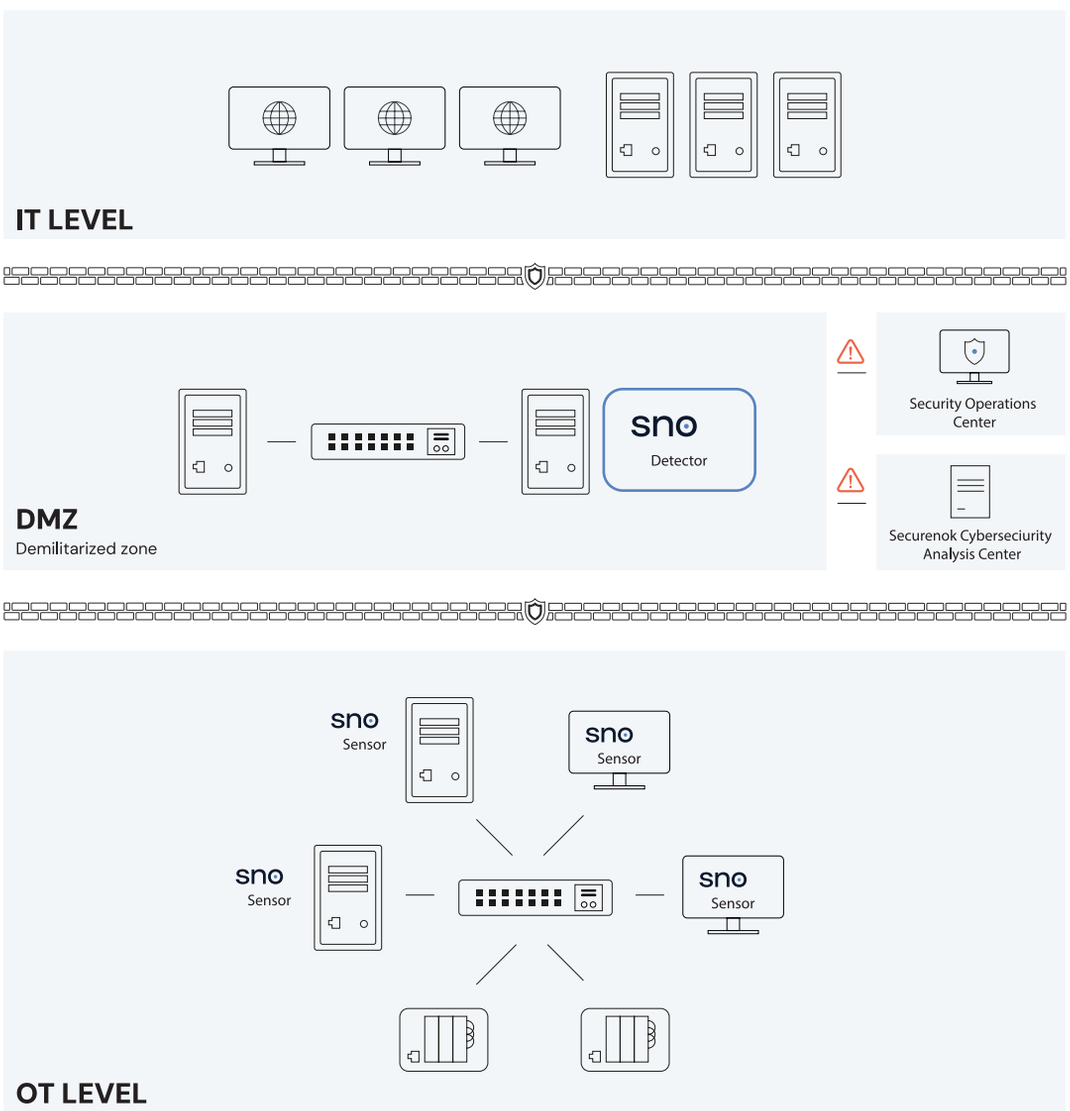
Handling of alarms

SNOK alarms can be handled in several ways.

The user interface is designed to support operational and technical personnel responsible for industrial systems. Many organizations also operate centralized Security Operations Centers (SOCs), either internally or through managed security service providers.

SNOK alarms and security events can be integrated with commonly used SOC and SIEM platforms. SecureNOK and its partners can also support customers in analyzing and responding to cybersecurity events originating from OT environments.

This allows information from industrial systems to become part of the organization's broader cybersecurity monitoring and incident response capability while retaining the OT-specific context required to understand what an event means for the physical process.



Flexible deployment options

The SNOK modules can be deployed independently or combined depending on the architecture and cybersecurity requirements of each industrial environment.

This provides flexibility when monitoring PCS 7 systems in both existing industrial installations and new projects. Passive network monitoring is an effective way of observing communication to and from industrial controllers. However, many existing industrial networks contain switches or network architectures that do not provide the port mirroring capabilities required for broad network monitoring.

Replacing or upgrading this infrastructure across a large industrial facility can require significant investment and operational effort. In such environments, the SNOK PLC Threat Detection module can monitor supported PLCs directly without depending on mirrored network traffic. Endpoint monitoring can similarly provide additional visibility from engineering workstations, HMIs and other systems inside the OT network.

Combining these approaches allows monitoring to be adapted to the actual architecture of the industrial installation rather than requiring major changes to the control system solely for cybersecurity purposes.

securenok®

OT cyberattack scenarios - and how they can be detected by SNOK

OT systems are generally better isolated from the public internet than conventional IT environments. However, isolation alone does not eliminate cyber risk.

Attackers can reach industrial environments through several paths, including:

- Internet-facing services elsewhere in the organization
- Remote access solutions
- Vendor and maintenance connections
- Compromised engineering systems
- Stolen credentials
- Supply-chain compromises
- Malicious or compromised insiders

If attackers bypass the organization's initial security controls, they will often attempt to move laterally through the infrastructure toward systems that provide access to the OT environment.

During this process, network monitoring can identify unexpected communication, new devices, new protocols or unusual interaction with industrial assets. Individual events may sometimes resemble legitimate engineering or maintenance activity. However, an actual intrusion will often create a sequence of anomalies that together reveal abnormal behavior. This can provide security personnel with an opportunity to investigate before the attacker reaches the most critical systems.

One way of gaining control of an industrial process is to compromise systems that already have authorized access to the controllers.

These may include:

- Engineering stations
- HMIs
- Operator stations
- Maintenance systems
- Other authorized OT endpoints

An attacker compromising one of these systems may be able to use legitimate industrial software and credentials to interact with controllers.

SNOK Endpoint Monitoring can identify activity such as:

- New users logging in
- New programs being installed or executed
- Unexpected processes
- Changes in network communication
- USB devices being connected
- Other deviations from the system's normal behavior

These signals can provide early indications that a trusted OT endpoint is being misused.

The PLC represents one of the most critical points in an industrial control system because it directly executes the logic controlling the physical process. The objective should always be to detect an attacker before they reach this level. However, defense in depth requires organizations to assume that this may not always be possible.

An attacker could compromise an authorized engineering workstation. Vendor credentials could be stolen. Remote maintenance infrastructure could be abused. A malicious insider could have direct access to automation equipment. A sophisticated attacker may also deliberately use legitimate protocols and engineering functionality in an attempt to avoid conventional security controls.

In these situations, monitoring the PLC itself provides an important additional layer of detection. The SNOK PLC sensor monitors security-relevant information directly from supported Siemens S7 controllers and can detect changes that may indicate manipulation or reprogramming.

This means that even if an attacker has successfully passed through earlier security barriers, activity affecting the industrial controller itself can still generate a warning.

securenok®

Defense in depth requires visibility

No individual cybersecurity technology can guarantee that an attacker will never gain access to an industrial environment. Firewalls can be bypassed, credentials can be compromised, authorized systems can become infected, remote access can be abused or insiders may already have access.

The principle of defense in depth therefore requires multiple layers of prevention and detection. Critical functions should be surrounded by several security barriers, and those barriers must themselves be monitored.

The objective is to detect an intrusion early enough for operators and security personnel to respond before critical industrial assets are manipulated and before the physical process is affected. The SNOK Cybersecurity Monitoring Platform provides several complementary sensor technologies that can be deployed according to the architecture of the individual industrial environment.

By combining visibility from the network, endpoints and industrial controllers themselves, organizations can reduce blind spots and gain additional opportunities to identify malicious activity before an attacker achieves the intended impact.

Tor Ommund Ljosland
Chief Sales Officer

Epost: tol@securenok.com
Tlf: +47 41 40 67 70

Adil Lakrimi
Senior Sales Executive

Epost: adl@securenok.com
Tlf: +47 95 23 22 26

See more. Fear less.