SNOK™
Network Intrusion Detection System
Industrial Automation and Control Systems (IACS) in infrastructure such as the electric power grid, oil and gas installations, water utilities, transportation systems, manufacturing facilities and many more are today integrated with IT systems to an increasing degree. Digitalization and automation are making industrial operations more efficient and safer. However, this also means exposure to cyber-attacks similar to those IT systems have been facing for decades.

Perpetrators can launch attacks on IACS both through network connections and transient equipment used in both environments. A preferred method of targeting industrial infrastructure, is to first compromise trusted insiders to bypass perimeter defense mechanisms. For most ICAS this is the only layer of cyber defense protecting industrial infrastructure. Consequences of cyber-attacks on industrial networks can be production loss and sometimes accidents and massive destruction.

SNOK™ Network Intrusion Detection System (IDS) is a network intrusion and anomaly behavior detection system made specifically for industrial controls systems. SNOK™ continuously monitors internal and external communications of a control system. It detects viruses, malware and sophisticated attacks (Advanced Persistent Threats) at an early stage, including those that are undetectable by conventional security tools.

The SNOK™ Network IDS can be placed at the perimeter of the network, or at strategic internal points to monitor the data traffic between critical components. The infrastructure owner is alerted in real time of security events such as:

- new device appearing on the network
- new connections between existing nodes
- anomalies in traffic patterns

The SNOK™ solution is installed in the industrial network monitoring from the inside.

The SNOK™ Network IDS can be complemented by other products in the SNOK™ Cybersecurity Monitoring System family to provide the best coverage. The SNOK™ product family combines information from network and endpoint monitoring thereby reducing blind spots in your infrastructure.
Industrial Automation and Control Systems (IACS) in infrastructure such as the electric power grid, oil and gas installations, water utilities, transportation systems, manufacturing facilities and many more are today integrated with IT systems to an increasing degree. Digitalization and automation are making industrial operations more efficient and safer. However, this also means exposure to cyber-attacks similar to those IT systems have been facing for decades.

Perpetrators can launch attacks on IACS both through network connections and transient equipment used in both environments. A preferred method of targeting industrial infrastructure, is to first compromise trusted insiders to bypass perimeter defense mechanisms. For most ICAS this is the only layer of cyber defense protecting industrial infrastructure. Consequences of cyber-attacks on industrial networks can be production loss and sometimes accidents and massive destruction.

SNOK™ Network Intrusion Detection System (IDS) is a network intrusion and anomaly behavior detection system made specifically for industrial controls systems. SNOK™ continuously monitors internal and external communications of a control system. It detects viruses, malware and sophisticated attacks (Advanced Persistent Threats) at an early stage, including those that are undetectable by conventional security tools.

The SNOK™ Network IDS can be placed at the perimeter of the network, or at strategic internal points to monitor the data traffic between critical components. The infrastructure owner is alerted in real time of security events such as:

- New device appearing on the network
- New connections between existing nodes
- Anomalies in traffic patterns

The SNOK™ Network IDS can be complemented by other products in the SNOK™ Cybersecurity Monitoring System family to provide the best coverage. The SNOK™ product family combines information from network and endpoint monitoring thereby reducing blind spots in your infrastructure.

Early attack detection – SNOK™ will detect attacks at an early stage because it monitors your blind spots for subtle traces of attacks.

Beyond signatures – More than 50% of attacks are non-malware related – these are not detectable using traditional signature detection. SNOK™ on the other hand uses anomaly detection. This means it will detect all types of intrusions, catching both known malware, malware seen never before and non-malware attacks.

Built for Industry – SNOK™ unique abilities to uncover blind spots are achieved because SNOK™ is built for industry. By that we mean:

**Non-intrusive**: SNOK™ does not disturb the industrial process.

**No maintenance required**: SNOK™ knows the fundamentals of a cyberattack. Once installed it needs no signature updates or similar to keep detecting new attacks.

**Tiny footprint**: Computing and storage resources are often scarce in industrial settings. SNOK™ uses minimal resources on the industrial infrastructure.

**Backwards compatible**: SNOK™ can be used to monitor legacy equipment such as unsupported Windows and Linux endpoints.

**Quick and easy to install**: SNOK™ has a simple installation process and requires only a short learning period to train the system.

The SNOK™ User Interface provides real time situational awareness.
ABOUT Secure-NOK™

Secure-NOK™ is a cybersecurity specialist company for Industrial Control Systems that provides solutions that detect and remove cyber-attacks such as espionage, sabotage, malware and other harmful cybersecurity events in industrial installations.

The company was established in 2010 and has offices in Norway (Hamar) and in the U.S. (Houston, TX). Secure-NOK™ is comprised of an international team with extensive experience in controls and automation systems cybersecurity, including SCADA and embedded systems.

Secure-NOK™ AS
Gronnegata 142
2317 Hamar, Norway

Secure-NOK™
3410 W Dallas St.
Houston, TX 77019, U.S.

secure@securenok.com
securenok.com

© 2018, Secure-NOK™. All rights reserved.
The information contained herein is the intellectual property of Secure-NOK™.