SNOK™
Network Intrusion Detection System

SECURENOK®

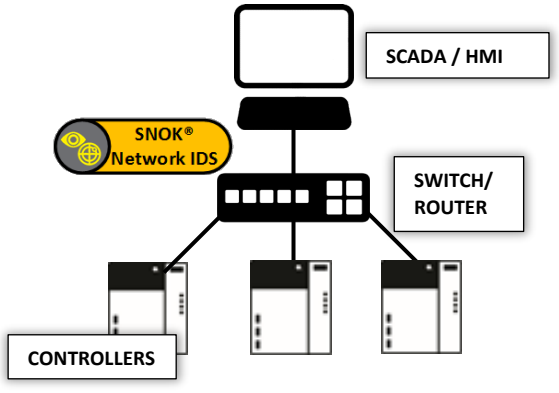
SNOK™

Cybersecurity monitoring for industrial infrastructure

SNOK™ Network Intrusion Detection System (IDS) is a network intrusion and anomaly behavior detection system made specifically for Industrial Automation and Control Systems (IACS).

Infrastructure such as the electric power grid, oil and gas installations, water utilities, transportation systems, manufacturing facilities and many more are increasingly vulnerable for cyber-attacks. SNOK™ obtains a full overview of the system you are defending and continuously monitors internal and external communications. SNOK™ detects viruses, malware and sophisticated attacks (Advanced Persistent Threats) and enables infrastructure owners to respond at an early stage.

The SNOK™ Network IDS can be placed at the perimeter of the network and strategic internal points to monitor the data traffic between critical components. This makes a SNOK™ Network IDS installation flexible and suitable to monitor networks in distributed and segmented infrastructures.



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

SNOK™ provides operators with insight into common blind spots such as controller networks. Many attacks enter the infrastructure from the inside and goes under the radar of perimeter protection such as firewalls.

Network Monitoring Agent	Total Alert Count	Initial Alert Timestamp	Last Alert Timestamp	Alert			
				Timestamp	Type	Description	Authorization Message
Trondheim Water Processing Filtration Plant	142	2019-06-28 09:19:15	2019-07-18 11:43:12	2019-06-28 09:19:15	Unexpected new connection	New protocol detected for this connection Protocol: CIP Source: 192.168.42.113 / 28:63:36:41:f8:8f : 102 Destination: 192.168.42.22 / 00:0c:29:ab:58:6c : 44818	N/A

SNOK™ uses anomaly detection to catch all types of intrusions, both malware and non-malware. SNOK™ Network IDS alerts the infrastructure operator in real time of security events such as:

- new device appearing on the network
- new connections between existing nodes
- new protocol usage
- unexpected traffic patterns

Upon detection of an alert, SNOK™ Network IDS provides information for the operator or analyst to localize and characterize the abnormal network behavior.

The SNOK™ Network IDS can be complemented by other products in the SNOK™ Cybersecurity Monitoring System family. The SNOK™ product family combines information from network and endpoint monitoring providing for early detection of attacks on your infrastructure.

SNOK™ - Real time monitoring, enables immediate response.

Built for Industry – SNOK™ unique abilities to uncover blind spots are achieved because SNOK™ is built for industry.

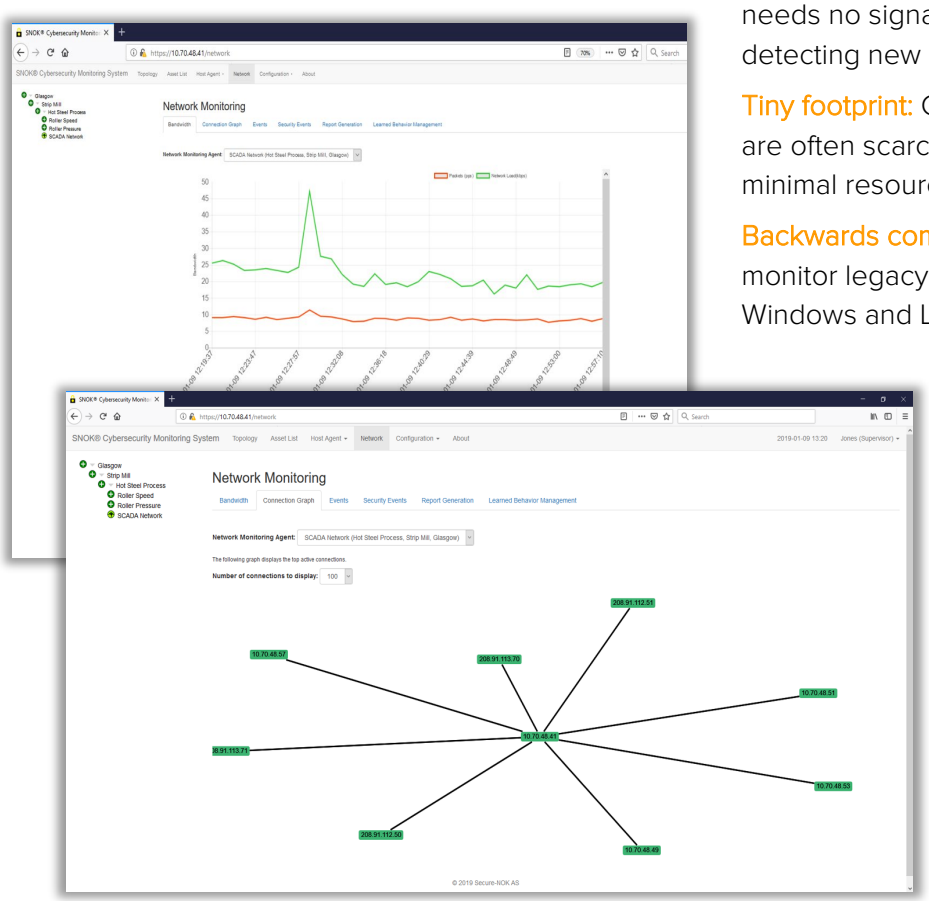
Non-intrusive: SNOK™ does not disturb the industrial process.

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 Automation and Control Systems. We provide solutions that detect cyber-attacks such as espionage, sabotage, malware and other harmful cybersecurity events in industrial installations.

The company was established in 2010 and is headquartered in Hamar, Norway with offices in Oslo and Stavanger. Secure-NOK™ is comprised of an international team with extensive experience in controls and automation systems cybersecurity.

SECURE-NOK™ AS
Grønnegata 142
2317, Hamar, Norway

secure@securenok.com
securenok.com

Real time monitoring, enables immediate response.