SNOK™
PLC Threat Detection

SECURENOK®

SNOK™

Keeping an eye on your PLCs

SNOK™ PLC Threat Detection continuously monitors PLCs for signs of cyber-attacks. PLC and their networks have traditionally not been designed to be secure, security strategy has mainly relied on air gapping the PLC environment from other networks and cyber based infrastructure.

Today PLCs are however integrated with modern IT systems to an increasing degree, both through connections and transient equipment used in both environments. Tools such as shodan.io make sure any PLC that accidently is made Internet reachable is instantly exposed to potential perpetrators.

SNOK™ alert immediately about events such as PLC property changes or memory changes. These may be caused by attempts to re-program or change configurations of a PLC. SNOK™ PLC Threat Detection will detect such events regardless if the PLC is manipulated over the network or unauthorized tampering on site.

PLC	Total Alert Count	Initial Alert Timestamp	Last Alert Timestamp	Alert			
				Timestamp	Type	Description	Authorization
Trondheim Water Processing Filtration Plant Water Quality Ph Monitor	1	01/23/2019 13:24:49	01/23/2019 13:24:49	01/23/2019 13:24:49	PLC property alarm	PLC protection status has changed PLC protection status, PLC IP:192.168.42.113 Selector protection level: Unknown Parameter protection level: No password CPU protection level: Access Grant Selector position: RUN-P Startup switch: Unknown	Authorize
Trondheim Water Processing Filtration Plant Water Quality Ph Monitor	1	01/23/2019 13:24:42	01/23/2019 13:24:42	01/23/2019 13:24:42	PLC property alarm	PLC operating mode has changed PLC CPU status, PLC IP:192.168.42.113 PLC status: RUN	Authorize

SNOK™ is installed either as an appliance in the PLC network or as a Virtual Machine on available hardware in the network. This provides visibility and insight into the core of PLC infrastructures:

- Immediate event alerts with automated indication of cyber-criticality
- Visibility to current configuration and configuration changes
- Production of change event logs

SNOK™ monitors PLC status.

Combined with other products in the SNOK™ Cybersecurity Monitoring System family, the environment surrounding PLCs can be monitored as well, reducing blind spots in the infrastructure and detecting abnormal attempts to communicate with PLCs.

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. By that we mean:

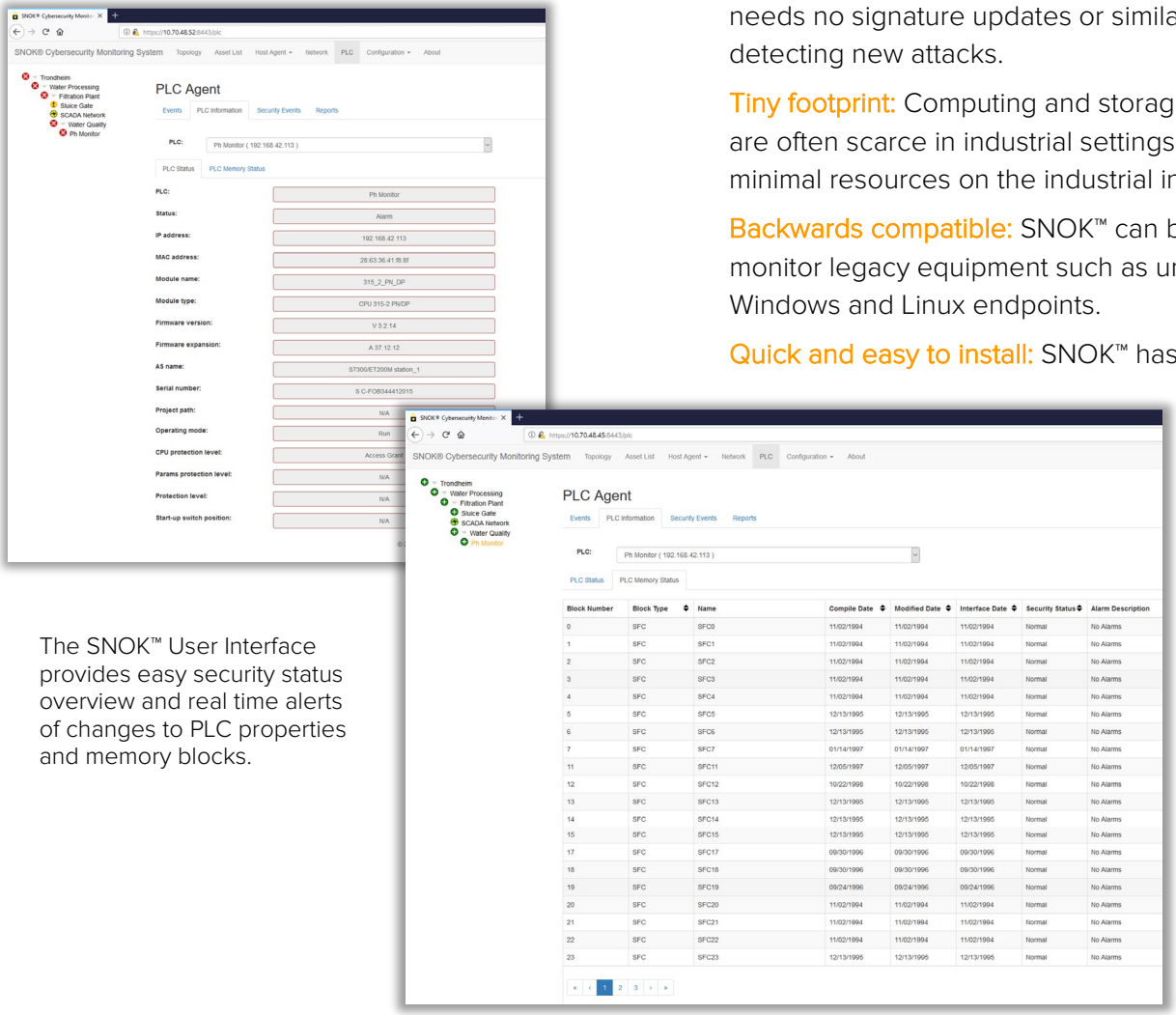
Non-intrusive: SNOK™ does not disturb the industrial process.

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 easy security status overview and real time alerts of changes to PLC properties and memory blocks.

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.