ABOUT SECURE-NOK®

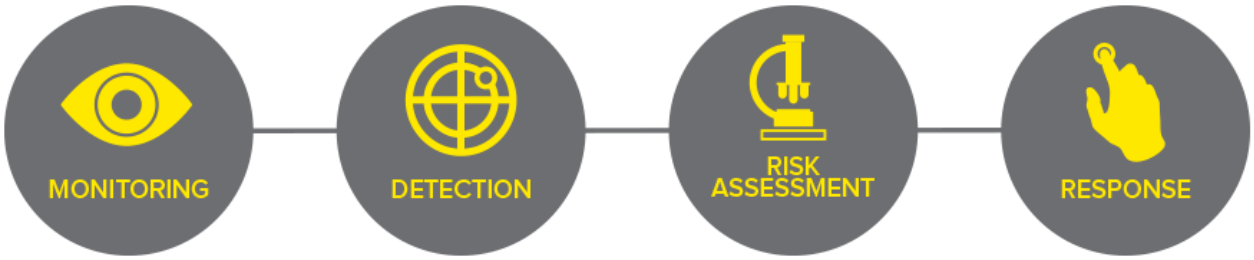
Secure-NOK® is a cybersecurity specialist company for Industrial Control Systems. The company was established in 2010 and has offices in Norway (Hamar) and in the U.S. (Houston, TX).

Secure-NOK® is comprised of an international team with extensive experience in controls and automation systems cybersecurity, including SCADA and embedded systems.

MISSION STATEMENT:

Secure-NOK® offers **SNOK®**, an easy-to-use state-of-the-art cybersecurity tool for high quality monitoring, detection and warning that is tailored for industrial controls systems. Through all of its products and services, **Secure-NOK®** enables decision makers to make well-informed security decisions based on accurate risk diagnostics, and provides knowledge and awareness of security risks and their consequences combined with holistic defense strategies and solutions.

Secure-NOK® provides solutions that detect and remove cyber-attacks such as espionage, sabotage, malware and other harmful cybersecurity events in energy & utility installations.



SECURENOK

SECURE-NOK® AS
Grønnegata 142
2317 Hamar, Norway

SECURE-NOK® LLC
3410 W Dallas St
Houston, TX 77019, U.S.
secure@securenok.com
securenok.com

Many Industrial Control Systems rely on outdated security models based on invalid assumptions.

Industrial Control Systems (commonly referred to as Operation Technology (OT) systems) play an integral part of modern society. These systems control the industrial process in sectors such as oil and gas, electrical power, manufacturing, water supply and other critical infrastructures whose reliable operation are vital for society as we know it.

Critical infrastructure has always been an attractive target for attackers and has traditionally been protected from intruders with physical barriers and monitoring and an "air-gap" from other computer systems to stay secure. Today's OT systems are however integrated with modern IT systems to an increasing degree, both through connections and transient equipment used in both environments. This makes modern industrial operations more efficient and safer but also exposed to the cyberthreats IT systems have been facing for decades.

Consequently, many industrial control systems rely on outdated security models based on invalid assumptions. At the same time, the frequency and sophistication of cyber-attacks against industrial control systems are increasing.

Stuxnet who targeted Iranian nuclear power plants is perhaps the most famous example of such attacks. Similar attacks have been reported in other industries. For instance, hackers targeted Ukrainian Power Utilities and brought down power to 225 000 customers in December 2015. In August 2008, an explosion of an oil pipeline near Refahiye, Turkey turned out to be caused by hackers. In addition to these high-profile attacks, Department of Homeland Security recorded more than 9 cyber-attacks per day in 2015 that targeted the energy industry and expect such attacks to become more frequent in the future.

SECURE-NOK® AS
Grønnegata 142
2317 Hamar, Norway

SECURE-NOK® LLC
3410 W Dallas St.
Houston, TX 77019, U.S.
secure@securenok.com
securenok.com

Faced with these challenges, it may seem natural to apply the methods used to secure IT systems to industrial control systems. While many approaches like use of network segmentation and firewalls should be utilized in securing both types of systems, other approaches will not work well. To be able to determine which methods to adopt, it is necessary to understand the differences in nature of the development and operations of the two different types of systems.

As an example, best practice for those responsible for the security of IT Operations is to make sure all parts of the system are properly patched at any given time. Further, an appropriate Incident Management and underlying Problem Management processes is an important part of the reliability of an IT system as a whole. All IT systems are maintained at regular intervals, this usually means that the system is taken down, although this is not always noticeable for the user. Usually the overhead created by security or maintenance applications cause no problems for the operation of the IT system.

The life cycle of an OT system is on the other hand very different. The system is designed to function in an extremely reliable fashion, often with strict timing constraints. Once in operation, many OT systems may run for several years without ever being updated. Many systems perform critical operations when interruptions are unacceptable. Introducing overhead or any security system that may slow down critical messages should be avoided without fully understanding its impact.

As IT and OT systems gradually melts into each other's domain, these differences still remain**. In protecting OT systems from the cyberthreats once associated with IT systems only, it must be done with the OT systems' basic constraints in mind.** The protection mechanisms must be carefully designed to accommodate OT systems, such as be non-intrusive and require minimal of the OT systems limited resources.

SECURE-NOK® AS
Grønnegata 142
2317 Hamar, Norway

SECURE-NOK® LLC
3410 W Dallas St.
Houston, TX 77019, U.S.
secure@securenok.com
securenok.com

SNOK®

To respond to challenges created by the integrated IT and OT systems, Secure-NOK® offers SNOK®, an easy-to-use, state-of-the-art tool for monitoring, detection, and early warning of cybersecurity events in industrial control systems.

SNOK® is designed according to OT-friendly principles:

- Non-intrusive – never slow down the industrial process or discard any messages.
- Minimal footprint – be lightweight on the control system as CPU power, memory etc. are scarce resources.
- Minimal maintenance – no need to update the system, no use of signature files that must be kept recent.
- Backwards compatible – industry systems may be old and contain elements that are no longer supported by the manufacturer but still needs cybersecurity protection.
- Quick and easy to install – short learning period to train the system.
- Able to detect both known and previously unknown attacks.

This allows SNOK® to be deployed deep inside OT systems, not just on its perimeters. The result is a system that can provide early warnings of cyberattacks whether they are coming from an outside hacker or from the inside through an infected USB stick, technician laptop or disgruntled employee. SNOK® will even pick up the subtle signs of early stage advanced persistent threat attacks not seen before.

SECURENOK

SECURE-NOK® AS
Grønnegata 142
2317 Hamar, Norway

SECURE-NOK® LLC
3410 W Dallas St.
Houston, TX 77019, U.S.
secure@securenok.com
securenok.com