securenok®

WHITE PAPER

# Cybersecurity in the Food Industry

**PREPARED BY:**
SECURENOK® AS

See more. Fear less.

# Navigating Cybersecurity Challenges in the Food Industry

Digitalization and increased automation have made food production more efficient – but also more vulnerable. When IT and OT converge, new security challenges with corresponding consequences emerge: From production halts and loss of recipes to regulatory sanctions and reputational damage.
With stricter requirements in EU directives (such as NIS2) and standards like ISO27001 and IEC 62443, the food industry must make cybersecurity an integrated part of daily operations.

This document provides insights into the threat landscape and shows how the SNOK® Cybersecurity Monitoring System can contribute to a more secure and stable production.

**Tonje Rønneberg Skei**
Chief Executive Officer

securenok®

# Possible consequenses from Insufficient Cybersecurity

Even minor incidents in the water sector can have major consequences, affecting public health, safety, and trust alike:

**Production downtime**

In an industry with perishable goods and tight margins, even short interruptions can cause major losses, product discards, and distribution delays.

**Loss of trade secrets**

Recipes, process parameters, and production methods are valuable intellectual property. Attacks that exfiltrate such data can weaken competitiveness long-term.

**Reputational damage**

Customers expect safe and reliable products. A security incident compromising food safety or customer data can quickly erode trust in the brand.

**Regulatory consequences**

New requirements like NIS2 impose reporting duties and risk management obligations. Non-compliance can result in fines or loss of licenses.

# Why Cyberattacks Occur?

Food production environments typically operate with a hybrid of legacy and modern OT/IT technologies. Many OT technologies were developed in times when systems were more isolated from the internet. The result is a complex, fragmented security situation where threats may slip past existing defenses.

**Lack of built-in security**
Many control systems and machines cannot handle traditional security measures like updates or antivirus without compromising stability.

**Weak network segmentation**
Attacks can spread freely between IT and OT networks without proper separation and control.

**Limited visibility and monitoring**
PLCs, HMIs, and sensors are often not covered by regular IT security monitoring, creating blind spots that attackers can exploit.

**IT personell and Security Operations Centre (SOC) often lack OT expertise**
Traditional IT security centers often lack tools, processes, or personnel to understand OT environments and their specific needs.

securenok®

# Mandatory Security System

Cybersecurity in the food industry is no longer optional – it is an obligation. The sector is classified as important under the EU`s NIS2 directive, with clear requirements for how production environments should be secured.

## NIS2

**New regulation with real consequences**
NIS2 came into force in the EU in October 2024 and is expected to be implemented into national legislation during 2025.

- Mandatory reporting of serious incidents within 24 hours.
- Documented risk management and technical security controls.
- Security incident response plans including detection, response, recovery.
- Clear leadership accountability.

Violations of the rules may result in fines, audits, and loss of licenses — and in severe cases, personal liability for company management.

## IEC 62443

**Industry-standard for OT security**
This is the most widely recognized global standard for OT security. It divides production systems into security zones, and defines clear requirements for:

- Network architecture and segmentation
- Access control and authentication
- Continuous monitoring and logging
- Security updates and lifecycle management

For food producers, IEC 62443 provides a framework tailored to the production environment's strict requirements for uptime and stability.

## ISO 27001

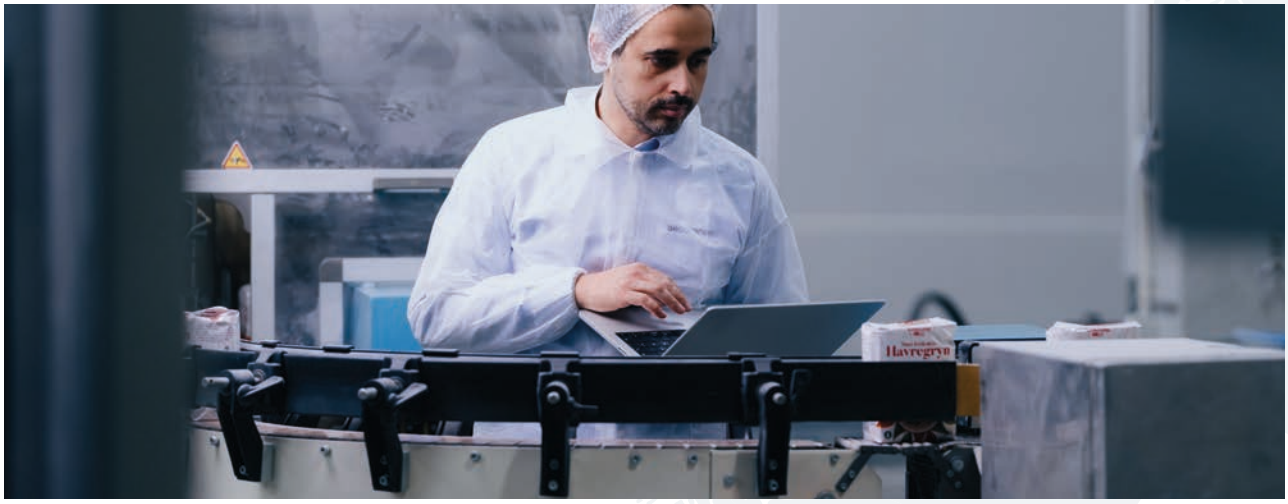
**Convergence of IT and OT**
Many food manufacturing organizations use ISO 27001 when implementing IT security. OT systems that control important processes must be included in the organization's risk management and their Information Security Management System (ISMS).


## The Consequence

Food producers must establish a structured, documented, and continuous approach to cybersecurity. Ad hoc measures or isolated fixes are no longer sufficient. A well-functioning monitoring system like SNOK® helps meet all three regulatory frameworks simultaneously — by ensuring visibility, incident handling, and proper documentation.

securenok®

# Customer Case Study




## Customer profile

- Global food manufacturer
- 20+ facilities worldwide
- 1,000+ employees

## Challenge

The customer had asked several IT security providers to also cover OT security but found it challenging to find the right solutions and expertise. They assumed that there were security gaps in their OT environments but did not have the overview. The customer needed to gain control over all facilities and ensure that there were no blind spots or unknown security gaps. The customer also wanted 24/7 monitoring of OT, which their current SOC managed service provider did not offer as part of their SOC services.

## Solution

**SNOK® Network Sensors**
Monitors the traffic in the OT environment to detect unauthorized activity early and prevent damage

**SNOK® Endpoint Sensors**
Strategically placed endpoint sensors on PCs in the OT environment. Reduces blind spots and enables effective monitoring of critical parts of the OT environment with low visibility to other systems.

**Secure-NOK Analysis Services**
- Analysis services, as basis for decisionmaking, data assessment, security meetings, etc. from the Secure-NOK analysis center.
- Weekly security event review.
- Integration and establishment of OT SOC with third-party SOC provider.

"Cybersecurity is no longer just an IT concern – it is critical to continuity, competitiveness, and trust."

securenok®

# SNOK® – A System Tailored for OT in the Food Industry

**SNOK® Cybersecurity Monitoring System offers real-time insight, alerts, and safety. Built to work in challenging OT environments, it operates without disrupting production.**

### Network sensors

Passive monitoring of normal traffic with anomaly detection.

### Endpoint sensors

Patented technology compatible with both modern and legacy Windows/Linux systems.

### API integrations

Supports integration with tools used by internal/external SOCs (e.g., SIEM).

### Benefits

- Actionable security insight
- Early detection of cyber threats
- Compliance with IEC 62443 / NIS2
- Operational continuity

Actionable security insights

Compliance with IEC 62443 and NIS2

Early detection of cyber threats

Continuity of production

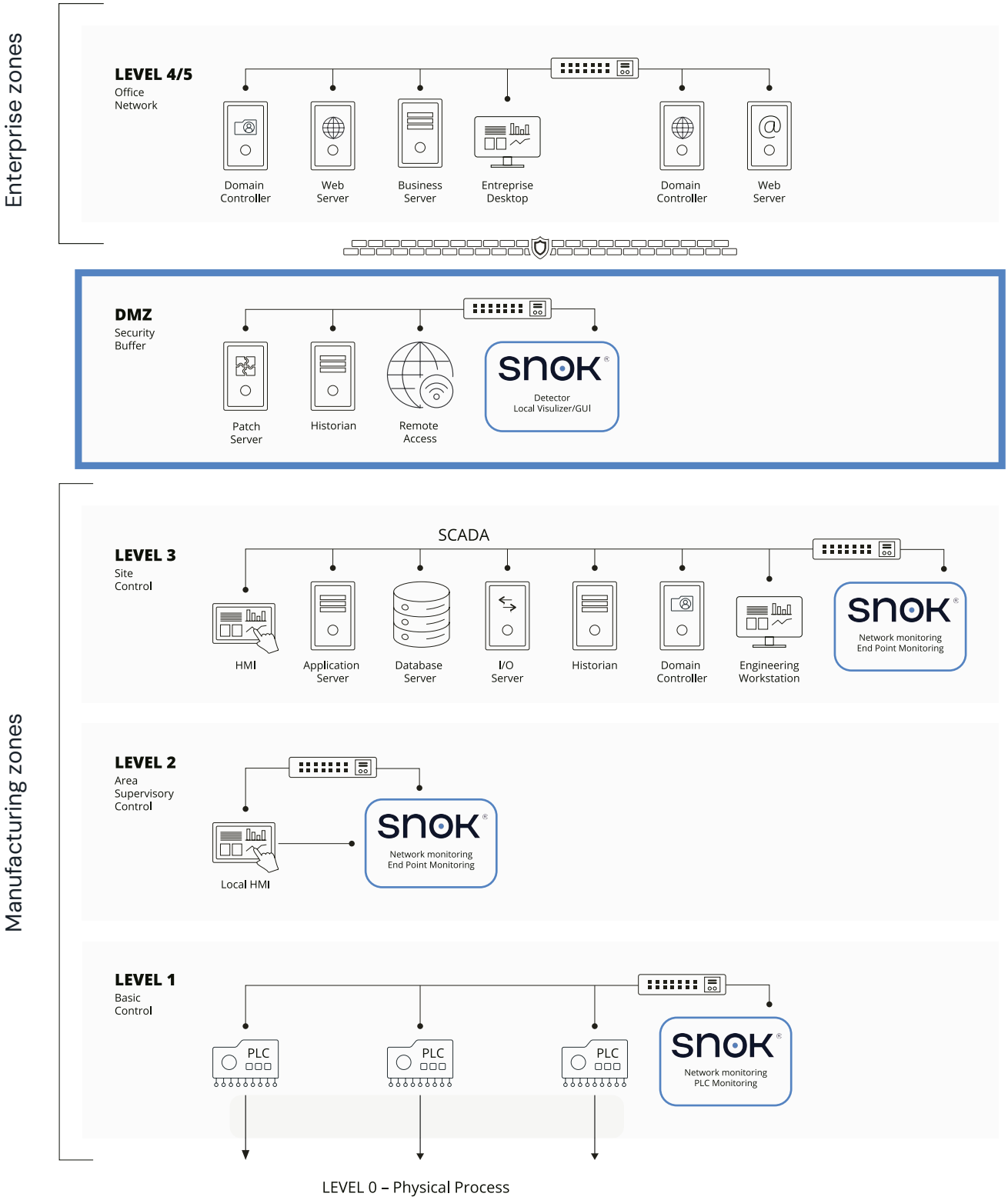
snok®

CYBER ESSENTIALS CERTIFIED PLUS

MADE IN NORWAY

# Implementing SNOK®

Implementation includes installing sensors in the network and on endpoints, and integrating alerting capabilities into the customer's event management workflows in the Operations Control Center or Security Operations Center.



securenok®

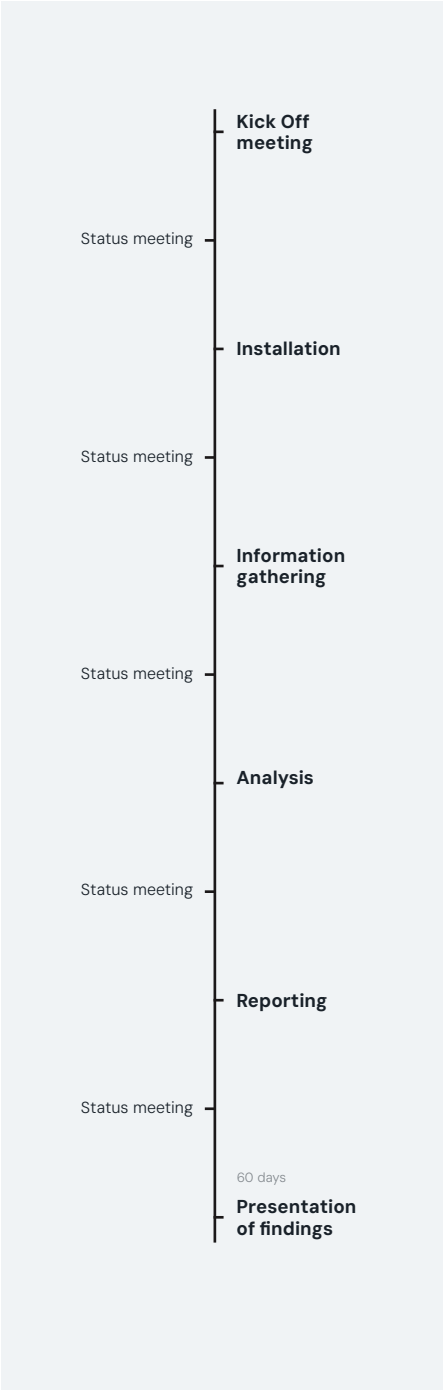
# Best Practices for Safer Food Production

**Security is not just about technology—it requires good processes and proper organization.**

• Segmentation: Separate IT and OT environments to limit the impact of potential attacks.
• Real-Time Monitoring: Use sensors to monitor networks and critical devices.
• Secure Endpoints: Remove unnecessary software and restrict network access on all devices.
• Response Preparedness: Develop and regularly test an incident response plan.
• Appropriate Expertise: Collaborate with OT specialists, not just IT security vendors.

By combining these measures, food producers can reduce risk and increase resilience against attacks.

# Implementation and timeline for security status with Securenok




**Visibility**

Full insight into OT assets and traffic

**Risk**

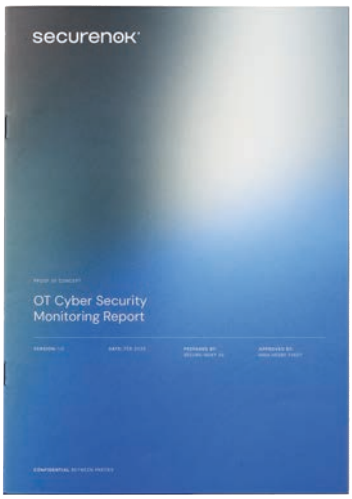
Uncovers weaknesses and unwanted behavior

**Actions**

Concrete, prioritized recommendations

**Fixed price**

60-day SNOK license and report included



securenok®

# Would you like an assessment of your company's security status or a non-binding consultation?

We offer a security status assessment and practical advice to strengthen your preparedness, tailored to municipalities and inter-municipal companies.


**Tor Ommund Ljosland**
Chief Sales Officer

**Epost:**
tol@securenok.com

**Tlf:**
+47 41 40 67 70

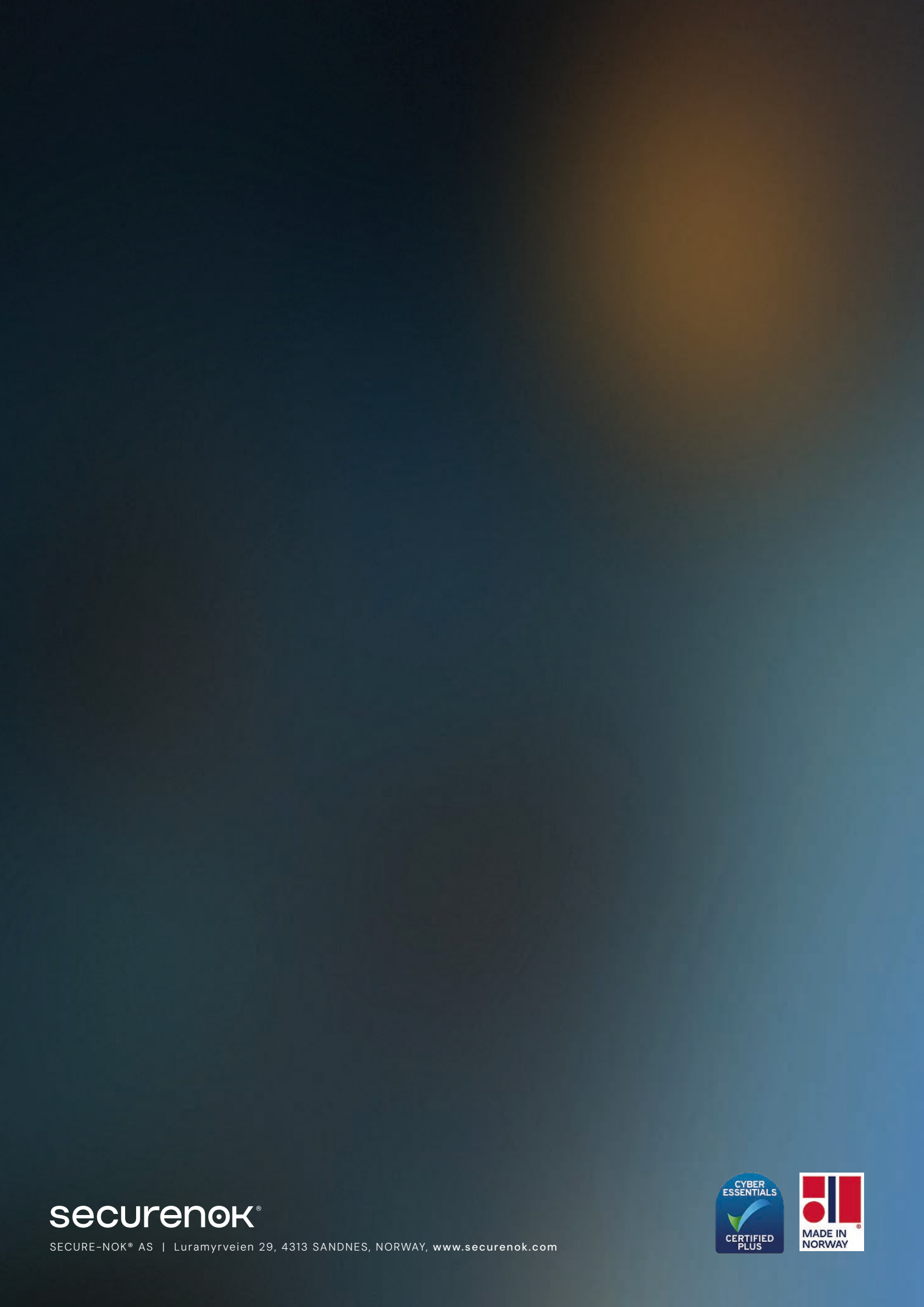


**Adil Lakrimi**
Senior Sales Executive

**Epost:**
adl@securenok.com

**Tlf:**
+47 95 23 22 26

See more. Fear less.



securenok®

SECURE-NOK® AS | Luramyrveien 29, 4313 SANDNES, NORWAY, **www.securenok.com**

CYBER ESSENTIALS CERTIFIED PLUS

MADE IN NORWAY