Security in critical infrastructure

SECTRA

Knowledge and passion

The “new normal”

Modern society depends on the operations of critical infrastructure being conducted securely and reliably; interruptions to operations can result in significant disruptions, with major financial and societal consequences as a result.

Increased digitalization in critical infrastructure has resulted in IT and OT systems becoming increasingly complex, as well as internal and external networks being linked together. This development has enabled improved efficiency, increased accessibility and greater customer value, but has also increased vulnerability. External threats and internal risks are continually changing, which will be the “new normal” for a long time ahead.

Balanced security over time

– security for constantly evolving operations

Balanced security over time means being able to manage risks so as to handle and carry out digitalization projects without increasing risk and threat scenarios in operations. In the new digital reality, both infrastructure and digital services are evoling at a rapid pace. This means that operations in critical infrastructure (e.g. energy and water supply, and process industry) are faced with the challenge of strengthening their capabilities for detecting, protecting against and acting on all the risks their networks are exposed to.

Moreover, the use of cloud solutions and digital ecosystems increases the attack surface for cyberthreats while the attacks are becoming smarter and exploit human behaviour to gain access to sensitive information. Risk management therefore needs to confront the continual change in external threats and internal risks that the new normal entails.

That is why achieving balanced security over time requires operations to act on risks instead of acting on attacks or the consequences of an incident. By detecting and identifying threats and risks in time before they have caused real damage, operations can achieve balanced security over time, thus ensuring continued function and deliveries.

Seven capabilities for a balanced security

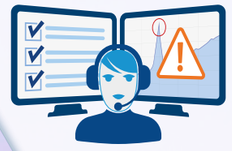
A holistic approach to security is required to ensure continuous operations and delivery. Sectra has an extensive experience within Managed Detection and Response, and offers seven different capabilities that can help your operations achieve a balanced security level over time, thereby reducing the risk of external threats and internal risks.

Network monitoring & detection

Network traffic is identified and analysed to minimise securityrelated threats and risks.

Incident response

Sectra's security analysts react and act in the event of deviations and incidents.



Log monitoring and detection

Collects securitycritical log events to obtain a picture of an imminent or ongoing attack.

Physical detection

Analyses video streams in real time and reports all suspicious activity.

Risk and security assesment

Identifies risks and lists actionable recommendations to help you mitigate them.

Behaviour monitoring

Creates expanded security awareness, thereby reducing the risk of human error.

Mobile workplace

Increases possibilities for managing sensitive or classified information during mobile work.

Minimize production downtime and loss of revenue

Network monitoring & detection

Industrial control system (ICS) network traffic will be identified and analysed to minimise risks that could constitute a threat against maintaining continuity in operations. This capability detects deviations in the networks by using a monitoring service that reacts proactively to potential threats and risks. Therefore, measures can be taken before the deviations can lead to serious consequences.

Log monitoring and detection

Security-critical log events are collected from various critical systems in operations (e.g. from IT/OT networks, switches, firewalls and servers). All information on security-critical events—supicious login attempts, for example—are grouped, and a picture of a potential threat or incident in progress can be rapidly obtained by correlating data from many different sources.

Risk and security assessment

Find the strengths and weaknesses in your organization's ability to detect, manage and protect against security related risks through both technical and organizational assessments. Identifying risks that may affect the ability to deliver critical services, and lists actionable recommendations to help you mitigate the risks.

Behaviour and policy compliance monitoring

Creates expanded security awareness for users, and staff are continually trained in managing information security. Security culture is thus improved and the risk of human error leading to serous consequences for operations decreases. Moreover, the system can easily detect malicious insiders as well as external threats that exploit internal resources.

Incident response

Protected locations in a 24/7 security operations centre (SOC) analyse all the information gathered by the different decetcion capabilitites. The traffic is first analysed in advanced systems, then Sectra's security analysts take over in the event of an incident to dig deeper and deal with the incident so that operations can quickly return to normal. Sectra's team of analysts and incident responders are always available by telephone.

Physical detection

The system notes deviations from normal movement patterns, and alarms are sent if movements or abnormal sounds occur in an area designated as prohibited. The system is also equipped with sensors that can identify suspicious sounds. Video streams are analysed in real time using artificial intelligence, and all suspicious activity is reported directly to the operations.

Mobile workplace

In pace with increased digitalisation, employees are becoming more mobile and need to work remotely. That is why the need for tools that can manage the sensitive or classified tasks of the operations is increasing. Sectra Mobile Workplace offers a total solution with a secure mobile VPN. Moreover, the solution is equipped with Sectra Tiger/R smartphone encryption that enables secure speech and text.

An experienced managed security service provider

Sectra is a leading managed security service provider (MSSP) for critical security in energy and water supply, and the process industry. We provide Managed Detection and Response in close partnership with our customers, adapted to their needs and resources.

Sectra is an innovative, dedicated partner for operations in critical infrastructure. In close partnership with our customers, we can add capability that increases operational reliability that thereby supports the work in providing security-critical services without interruption. With seven capabilities, all of which enable a holistic security solution, customers can make use of the technological opportunities available today without increasing exposure to threats or risks.

All the capabilities are supported by a team of Sectra security experts and security analysts, who are available around the clock for advice and support. Sectra works closely together with our customers to design a balanced security approach over time, adapted to the risk level and risk appetite of the operations. Together with our customers, we will face the new normal.

THE KNOWLEDGE TO MEET EXPECTATIONS. THE PASSION TO EXCEED THEM.

Sectra has more than 40 years of experience in developing security solutions for organizations such as defense ministries, government authorities, and other critical functions of society. Through our services we help actors within for example energy and water distribution in attaining sustained, value-based security, supporting them in the digital transformation.

Sectra is a public company founded in 1978. Our head office is located in Linköping, Sweden and business is conducted through operations in Sweden, the Netherlands, Finland and the US.

Sectra Communications AB • communications@sectra.com • communications.sectra.com

SECTRA

Knowledge and passion