Security solutions for critical infrastructure

SECTRA

Knowledge and passion

Times have changed

Modern society depends on operations in critical infrastructure being conducted securely and reliably; interruptions to operations can result in significant disruptions, giving rise to major financial and societal consequences.

Discussions around digitization have long been an important focus area for operations in critical infrastructure, such as energy and water supply, and for the process industry. Higher productivity, increased accessibility and efficiency gains have been a driving force in this journey. The result is a more connected IT and OT system, where tasks can be automated or carried out in a decentralized model. However, the focus is about to change—digitization has come a long way, and the new driving force for security is *the increasing rate of change.*

Increasing rate of change

Accelerated digitization, cloud-based control systems and implementation of security in a rapidly changing environment represent major challenges for operations in critical infrastructure. The driving forces underlying today's increasing rate of change can be seen in several different parts of society. A key one, of course, is the energy transition, where everyone has to do their part to use resources more efficiently. The electrification of the society is another major driving force. The energy transition and electrification are giving rise to a higher degree of automation, which is resulting in an increased need for cloud-based control systems. This in turn means that organizations need to manage the new and constantly changing security risks that this transition entails.

Operations need to adapt to this new way of working without increasing their risks or their exposure to security threats, which is also a challenge since the threat landscape is constantly changing due to the instability in the world. To respond to this increasing rate of change, there must be a holistic approach to security in all systems and all parts of the organization from square one.

The OT system is the heart of the organization, and it is important to find a good balance between a system's detective and preventive capabilities when it comes to cyberthreats and security risks. Thus, operations in critical infrastructure must have capabilities for detecting, protecting against and acting on all the risks their networks are exposed to. By doing this, operations can ensure continued function and deliveries to their customers and to society.

Seven capabilities for balanced security

A holistic approach to security is required to ensure continuous operations and delivery. Sectra has extensive experience in 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.

MITRE ATT&CK®

A well-established knowledge database based on real observations of cyberattacks.

Threat hunting

Proactive, human-centric searches for security risks and potential threats that may be disclosed in captured logs.

Incident response

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

Log monitoring and detection

Collects security-critical log events to obtain an overview of a security risk or an imminent or ongoing attack.

Risk and security assessment

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

Wire

An end-to-end encryption (E2EE) chat application for digital collaboration that supports both mobile and stationary devices.

Network monitoring and detection

Network traffic is identified and analyzed to minimize security-related threats and risks.

Minimize production downtime and loss of revenue

Network monitoring and detection

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

MITRE ATT&CK®

A knowledge base that can be used to develop threat models and methods to detect undesired activity in IT and OT systems. A monitoring service that applies the method can work proactively and identify known cyberattacks. This increases the chances of detecting any potential attack against the critical operations in time. In addition, applying MITRE as an integrated part of the monitoring solution for IT and OT increases security across the entire operation.

Threat hunting

This method is used in proactive security work and entails investigating saved log data based on the theory that deviations from normal behavior have taken place. This way, signs of any undetectable malicious activity in the critical systems and networks can be identified. Proactive security work is an important part of achieving balanced security across all operations and thereby reducing the risk of intrusion in critical systems.

Incident response

Protected locations in a 24/7 security operations center (SOC) analyze all the information gathered by the different detection capabilities. The traffic is first analyzed 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 reachable by phone. Sensitive information is protected using encrypted communication.

Log monitoring and detection

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

Risk and security assessment

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

Wire

A secure and easy-to-use app for digital collaboration that supports both mobile and stationary devices, with a user-friendly interface. The app features a high level of security through end-to-end encryption (E2EE) and uses session keys to encrypt the communication, thereby further reducing the level of vulnerability.

An experienced security service provider

Sectra is a leading security service provider of managed detection and response services (MDR) for critical security in energy, water supply and the process industry. We provide managed detection and response in close cooperation with our customers, adapted to their needs and resources.

Sectra is an innovative, dedicated partner for operations in critical infrastructure. In close cooperation with our customers, we can add capabilities that increase the security in critical systems. These different capabilities support a holistic security approach, which enables our customers to take advantage of the technological opportunities available today—without increasing their 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 with its 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 increasing rate of change.

The knowledge to meet expectations.
The passion to exceed them.

Sectra has 45 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 in areas such as energy and water distribution attain secure system development and balanced security in IT and OT systems. We believe this is best achieved jointly and in close cooperation with our customers.

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

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

This is a marketing material and may be changed at any time without prior notice. Sectra will not be held liable for any errors or misconceptions herein. © 2023 Sectra Communications AB