Sectra
Managed detection & response

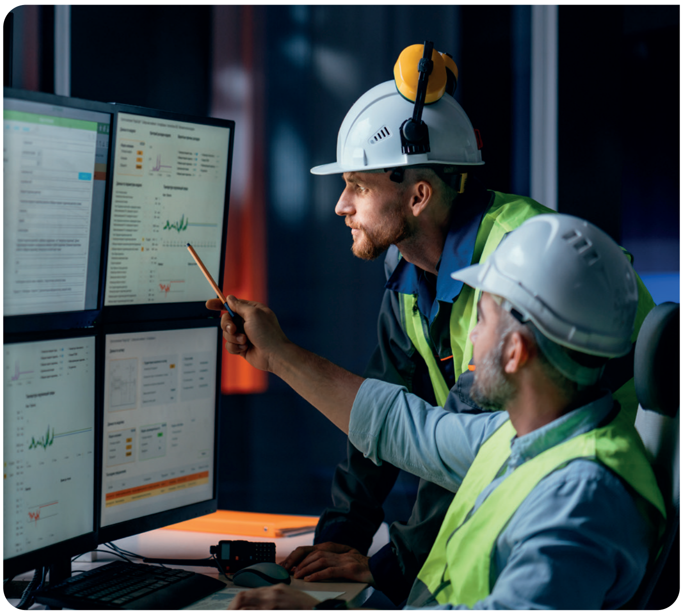
When safeguarding operational technology (OT) environments, a standard approach simply won't suffice. That's where Sectra's OT-focused Security Operations Center (SOC) steps in. Sectra has over 45 years of experience in cybersecurity and has been delivering detection and response services to critical infrastructure in Sweden since 2016. Sectra understands the unique challenges of OT environments and is a trusted managed security service provider, providing behavior-based monitoring for the most critical network assets.

A service that grows with the client over time

More and more organizations are converging their IT systems with previously isolated OT systems in need of increased efficiency, leading to new types of threats. With a service tailored for real-time requirements, Sectra offers managed detection and response, ensuring the most critical operational processes remain uninterrupted. Sectra cooperates closely with its clients to build balanced security over time, ensuring organizations grow sustainably in an increasingly connected world. In other words, OT security monitoring isn't just a service, it's a collaboration model designed to empower the client's total security capability.

Sectra SOC enables security risk management

Identifying and managing security risks is a fundamental aspect of any operation, but many organizations face the same challenge when monitoring their critical systems. There's not enough time or competence to identify and act on risk-reducing measures without having to pour resources into it. Sectra's monitoring service has all the expertise and tools necessary to identify and help clients mitigate the most critical security risks. With active threat intelligence, threat hunting sessions and detection capabilities based on the MITRE ATT&CK® Framework, Sectra creates visibility in our clients' OT environments that is kept up to date against current threat scenarios.

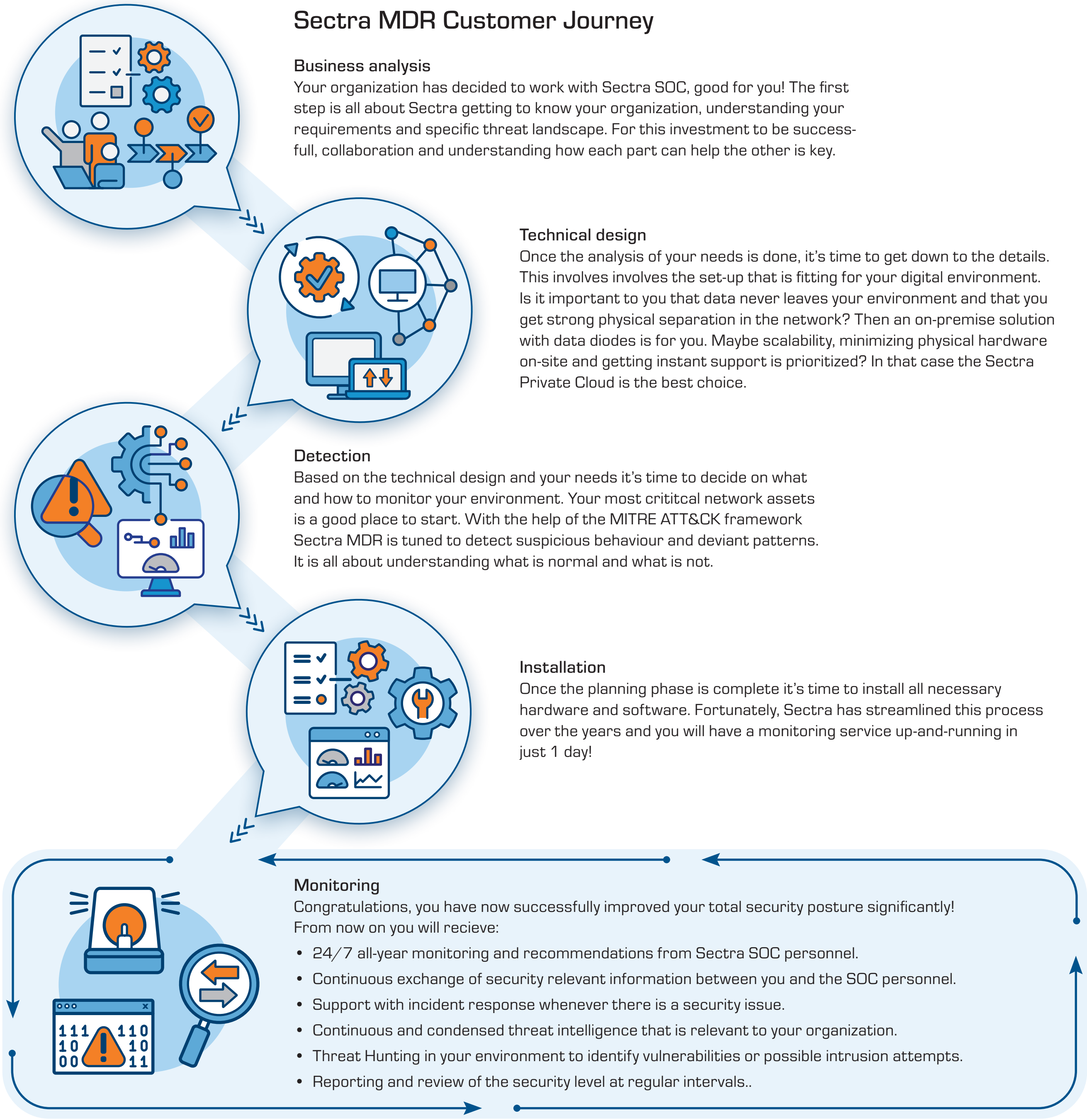


Advantages with monitoring from Sectra

- Collaboration and partnership. Integration with the client's existing security capabilities, creating a unified force against potential threats.
- Incident management expertise. A dedicated team that rapidly responds to any incidents, minimizing the impact on business operations.
- Risk identification and management. Utilizing behavior-based detection and threat intelligence, Sectra SOC actively identifies and mitigates vulnerabilities before they can be exploited.
- Non-intrusive detection of critical network assets within, and adjacent to, the OT environment.
- 1-day deployment with prebuilt data integrations that deliver higher visibility from day one.
- 24/7, all-year monitoring by Sectra SOC.

The NIS2 Directive

A primary goal of the EU NIS2 Directive is to ensure the availability of critical societal functions. Sectra MDR provides mature detection and response, a core component of meeting regulatory requirements for critical infrastructure. It also forms the basis for other security measures and helps to quickly detect issues so they can be dealt with promptly, ensuring uninterrupted deliveries to society.



Sectra MDR Customer Journey

Business analysis

Your organization has decided to work with Sectra SOC, good for you! The first step is all about Sectra getting to know your organization, understanding your requirements and specific threat landscape. For this investment to be successful, collaboration and understanding how each part can help the other is key.

Technical design

Once the analysis of your needs is done, it's time to get down to the details. This involves involves the set-up that is fitting for your digital environment. Is it important to you that data never leaves your environment and that you get strong physical separation in the network? Then an on-premise solution with data diodes is for you. Maybe scalability, minimizing physical hardware on-site and getting instant support is prioritized? In that case the Sectra Private Cloud is the best choice.

Detection

Based on the technical design and your needs it's time to decide on what and how to monitor your environment. Your most crititcal network assets is a good place to start. With the help of the MITRE ATT&CK framework Sectra MDR is tuned to detect suspicious behaviour and deviant patterns. It is all about understanding what is normal and what is not.

Installation

Once the planning phase is complete it's time to install all necessary hardware and software. Fortunately, Sectra has streamlined this process over the years and you will have a monitoring service up-and-running in just 1 day!

Monitoring

Congratulations, you have now successfully improved your total security posture significantly!
From now on you will recieve:

- 24/7 all-year monitoring and recommendations from Sectra SOC personnel.
- Continuous exchange of security relevant information between you and the SOC personnel.
- Support with incident response whenever there is a security issue.
- Continuous and condensed threat intelligence that is relevant to your organization.
- Threat Hunting in your environment to identify vulnerabilities or possible intrusion attempts.
- Reporting and review of the security level at regular intervals..

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.

SECTRA

Knowledge and passion