Detection technologies for critical infrastructure

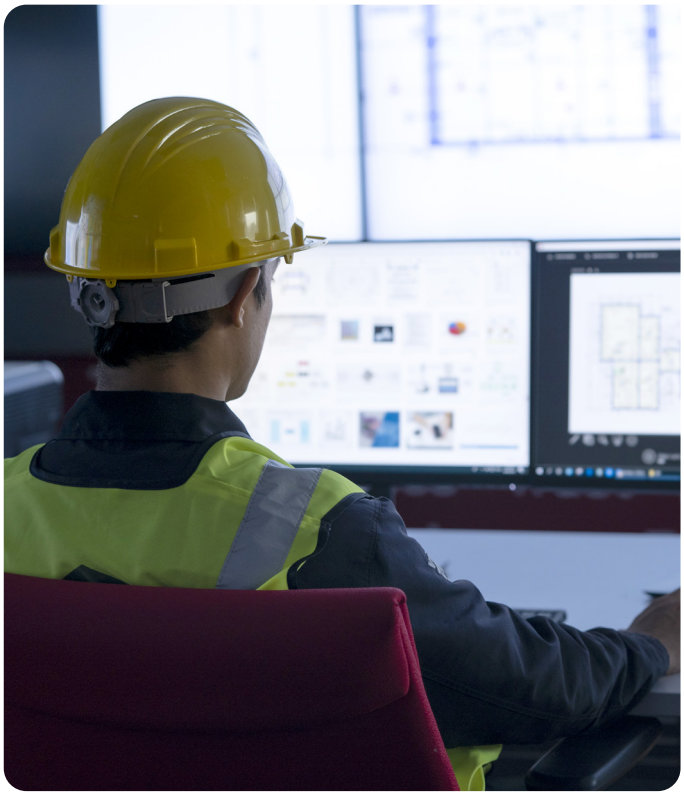
By detecting and identifying threats and risks in time and acting on them instead of reacting to attacks or the consequences of an incident, operations can ensure business continuity and delivery. Network and log monitoring are two key detection technologies that detect potential malicious activities in critical networks and enable an adaptive security approach.

A service that grows over time together with the customer

Through a highly secure architecture, Sectra can monitor networks and systems simultaneously while maintaining a strong separation between the monitored systems. The monitoring service is continuously adapted to the customer's network infrastructures, architectures and assets as well as the growth of the operations' business and services. This is done to maintain a low risk level over time and to have a service that grows together with the needs and ability of the customer's operations.

Log and network monitoring enables visibility

The service enables high visibility within critical networks, detects system configuration changes, undesirable application and user behaviors at endpoints, and is highly focused on the MITRE ATT&CK® framework, which is essential for detecting any kind of technique that an adversary may use inside the network to perform or prepare for an attack. Operations face a common challenge in regard to monitoring their critical systems: there is not enough time, competence or access to the right tools to get value out of the information they receive. Sectra's monitoring service has all the prerequisites needed when it comes to expertise and tools to detect and act on abnormal behaviors.



Advantages with monitoring from Sectra

The monitoring system normalizes data from both log sources and network intrusion detection sensors, which increases context awareness and thereby efficiency in threat hunting and incident response. Five key advantages:

- Strong separation between the customer's environment and the monitoring system by using data diodes.
- Unifies logs from multiple sources in one place for correlation of abnormal activities.
- Quick deployment with prebuilt data integrations that deliver higher visibility from day one.
- The detection rules are mapped directly to MITRE ATT&CK®, leveraging a knowledge base of adversary tactics and techniques based on real-world observations.
- Uses network-based signatures to detect and enrich known threats in real time while also enabling detection of historic breaches with an indexed and searchable history of network traffic.

Technical specification

High assurance separation	• Data diodes provide strong separation between customer network and monitoring cluster • Supplier-independent diode technology
Log sources	• Windows event logs • Linux audit logs • Firewalls, IPS, IDS (Including but not limited to Sectra's network IDS) • Servers, switches • Integrations with custom log sources
Log cluster	• Log cluster and its data installed as an on-premise solution • Detection engine uses customized rules, threat intel feeds and machine learning • Log cluster supports installation in cloud environment
Metrics	*Log cluster* • 1 Gb/s maximum peak data flow over network diode • 1.8 TB of available and searchable live data * • Long-term storage of searchable archived historical data *Network IDS* • Four simultaneous network connections per sensor * • Up to 2 Gbit/s aggregated network traffic per sensor (without signatures) * • Up to 1.5-1.7 Gbit/s with signatures per sensor * • Signatures with over 37,000 rules in over 40 categories • New signatures updated daily
Security	• Encryption at rest • Hardened in accordance with the CIS-CAT benchmarks, a set of internationally recognized secure configuration guidelines • Dual independent encryption tunnels for remote access • Tempered detection • High assurance of event delivery with back pressure support and continuous event delay monitoring

** extendable according to customer requirements*

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

SECTRA

Knowledge and passion