Cyber Security Operations Centre (CSOC)

24/7 Monitoring and Alerting

[COMPANY NAME]'s Cyber Security Operations Centre (CSOC) is dedicated to helping your organisation prevent, detect, and respond to a wide range of threats, providing comprehensive monitoring and alerting services for all systems and infrastructure.

The cyber threat landscape is constantly evolving, making it challenging to allocate resources effectively and respond to threats and events, while continuously monitoring your environment and implementing the right security solutions can be costly.

Your ultimate goal is to achieve peace of mind when it comes to your cyber security, so our CSOC is managed by [COMPANY NAME]’s own certified analysts, engineers, architects, and consultants, allowing you to focus on your core business services.

Monitoring and Alerting

Organisations generate millions of security log alerts daily. Interpreting and responding to these requires highly specialized expertise, which can be challenging to manage internally. Historically, implementing security information and event management (SIEM) and other monitoring technologies has been complex and expensive.

[COMPANY NAME] provides effective and responsive security monitoring for your entire cyber security environment, not just the devices we supply. We understand the correct approach for advanced monitoring and alerting operations to continuously monitor incoming threats, know when to respond, and determine the appropriate steps to prevent risks.

We analyse signals 24/7 and raise actionable alerts, helping you remediate incidents effectively. This ensures your data, systems, and applications are always available.

The CSOC monitoring and incident alerting service offers unified security management, where native data stays within your network. This enables monitoring syslog streams and network traffic across your infrastructure, identifying risks, mitigating threats, and maintaining compliance.

How it works

Our managed service includes purpose-built virtual devices for 24/7 data collection, monitoring events from end-user devices, servers, network equipment, firewalls, and more. This data is consolidated and analysed in a secure, Cloud-based platform, for which we apply technology-specific rules, custom-designed for your business.

Human analysis drives advanced security operations, managed through a highly intuitive customer portal for incident identification and reporting. Security log monitoring, detection, analysis, and alert management are simplified, enabling the detection of dormant threats and vulnerabilities in your network.

Features

* 24/7 real-time monitoring, analysis, alerting, and reporting.
* Manual evaluation and investigation by certified security experts.
* Easy integration with existing solutions.
* Purpose-built system for comprehensive and flexible security management.
* Categorisation of devices and assets using advanced business logic.
* Powerful processing of high volumes of data.
* Simple management platform presenting reports and facilitating ticket investigation.
* Generate insights through analytics.
* Easy deployment, onboarding, and management.

Benefits

* Monitor your entire security environment.
* Rapid incident response.
* Reduced risk and increased cyber security.
* Integration of advanced technology and multi-layered solutions.
* Decreased capital expenditure.
* Simplified operating model with increased automation.
* Accountability and support from certified cyber security analysts.
* Analytics and full visibility.
* Manage and report on compliance.