DATA SHEET

CYBER SECURITY SERVICES

Cyber Security Operations Centre Services

Security Monitoring & Incident Alerting

The Cyber Security Operations Centre (CSOC) is a specialised unit to help your organisation prevent, detect and respond to a range of threats.

The CSOC provides monitoring and alerting for all of your systems and infrastructure - regardless of size, geography and manufacturer.

We enable you to reduce risk and increase your IT resilience.

The threat landscape is complicated and continuously changing. Knowing where to allocate your resources and how to mitigate business risk is a challenge that you needn't have to burden upon your IT department. It's not just an issue of finding the expertise to respond to threats and events when they happen - a huge amount of cost comes from needing to continuously monitor your estate and to implement the right solution to secure your business.

Your ultimate goal? Achieving peace of mind when it comes to your cyber security strategy, solutions and operations. As a highly accredited leading Cloud and Network provider in the UK we are a trusted safe haven in a world of hacks and data breaches. We understand what is needed to maintain your security.

The Cyber Security Operations Centre offers dedicated and skilled capability required to meet your security objectives. The CSOC is managed by a team of certified security analysts, engineers, architects and consultants. We help secure and protect what you value most 24 x 7, allowing you to focus on your core business services.

Monitoring and Alerting Services

Organisations can generate millions of security log alerts every day. The ability to interpret and respond to these alerts in real-time requires highly specialised expertise, which can be costly and resource-intensive to manage internally.

Historically, implementing security information and event management (SIEM) and other monitoring technologies can be complex and offers limited value without further investment in expensive analysts to interpret information into actionable advice.

We provide effective, responsive security monitoring for your whole cyber security estate - not just on the devices we supply.

The Correct Approach for Advanced Monitoring and Alerting Operations

There is an increasing need to monitor security events and understand your business risk. However, how do you continuously monitor incoming threats? How do you know when to respond? What infrastructure and configuration should you use to prevent risks? Augment your IT security effectively by engaging the experts. Our security-cleared personnel are experienced practitioners supported by a central and double-secured CSOC environment.

With our Network and Cyber Security expertise, we understand how to detect threats and vulnerabilities to protect your most valuable assets. We analyse signals 24 x 7 and raise actionable alerts to your attention helping to best remediate incidents. This keeps your data, systems and applications always available.

The CSOC monitoring and incident alerting service provides unified security management. Native data stays within your Network, while centralised controls and analysis provide a valuable managed service. This enables monitoring syslog streams and Network traffic across your infrastructure. Having the ability to detect activity on your network helps identify risk, mitigate threats, achieve compliance and improve your business and its cyber security operations.

How the Monitoring Service Works

The managed service consists of purpose built virtual devices for data collection 24 x 7. Events are monitored from end-user devices, servers, Network equipment, Firewalls and more. This data is then consolidated and analysed in a secure, Cloud-based, centralised platform. Here we apply technology-specific, custom-designed rules specific to your business.

Human analysis provides advanced security operations managed with a customer portal for incident identification and extensive reporting.

Security log monitoring, detection, analysis and alert management is simplified allowing for the detection of dormant threats and vulnerabilities in your Network.

24 x 7 Log monitoring and event management.

Customised rules engine.

CSOC human analysis and investigation.

FEATURES

- 24 x 7 real-time monitoring, analysis, alerting and reporting.
- Manual evaluation and investigation by certified security experts.
- Easy integration with existing solutions.
- Purpose-built system provides full and flexible security management.
- Categorise devices and assets with advanced business logic.
- Powerful processing of high volumes of data.
- Simple management platform presents reports and ticket investigation.
- Generate insight though analytics.
- Simple deployment, onboarding and management.

BENEFITS

- Monitor your whole security estate.
- Fast incident response.
- Reduced risk and increased cyber security.
- Integrate advanced technology and multi-layered solutions.
- Reduced 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.