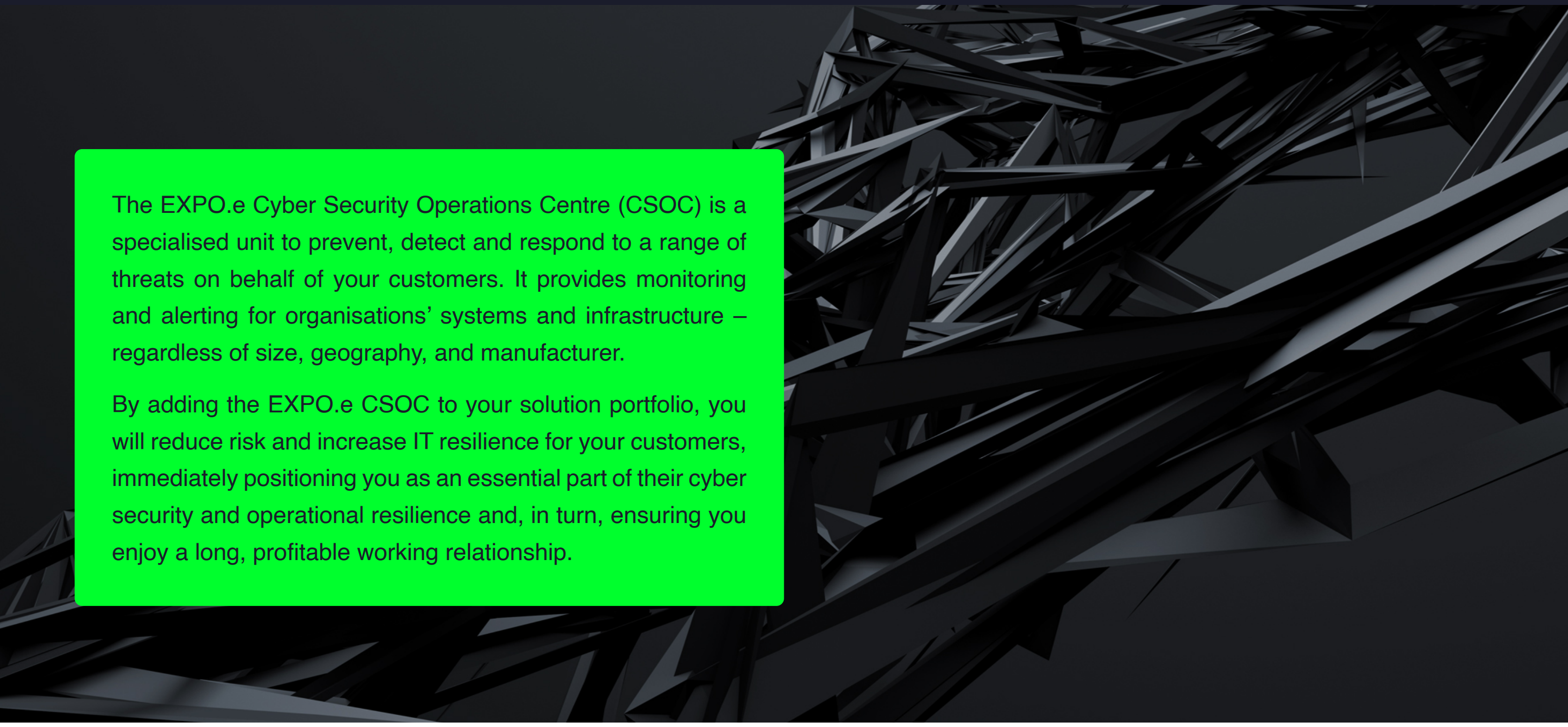
DATA SHEET

# Cyber Security Operations Centre Services

Security Monitoring & Incident Alerting



The EXPO.e Cyber Security Operations Centre (CSOC) is a specialised unit to prevent, detect and respond to a range of threats on behalf of your customers. It provides monitoring and alerting for organisations' systems and infrastructure – regardless of size, geography, and manufacturer.

By adding the EXPO.e CSOC to your solution portfolio, you will reduce risk and increase IT resilience for your customers, immediately positioning you as an essential part of their cyber security and operational resilience and, in turn, ensuring you enjoy a long, profitable working relationship.

The threat landscape is complicated and continuously changing. Knowing where to allocate resources and how to mitigate business risk is an ongoing challenge for IT departments. 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 the entire estate and implement the right solutions. All customers want peace of mind when it comes to their 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 increasingly complex hacks and data breaches. We understand what is needed to maintain the highest level of security, and the importance of being able to provide your customers with complete peace of mind.

The EXPO.e Cyber Security Operations Centre offers dedicated and skilled capability required to meet your security objectives. EXPO.e's team of certified security analysts, engineers, architects and consultants work 24x7 to secure and protect your customers' critical systems, freeing them to work with you to enhance their 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.

**EXPO.e** provides effective, responsive security monitoring for your customers' entire cyber security estates – not just on the devices we supply.

## THE CORRECT APPROACH FOR ADVANCED MONITORING AND ALERTING OPERATIONS

As an EXPO.e Channel Partner, you can bring in the experts to augment your customers' cyber security. Our security-cleared personnel are experienced practitioners supported by a central and double-secured CSOC environment, significantly streamlining the process of making this leading-edge standard of cyber security part of your solution portfolio.

EXPO.e's CSOC monitoring and incident alerting service provides unified security management. Native data stays within the network, while centralised controls and analysis provide a valuable managed service. This enables monitoring syslog streams and network traffic across the customer's infrastructure, helping to identify risk, mitigate threats, and maintain compliance.

With more than twenty years of network and cyber security expertise, we understand how to detect threats and vulnerabilities to protect your customers most valuable assets. We analyse signals 24x7 and raise actionable alerts to best remediate incidents, ensuring data, systems and applications are always available, without any additional input required from your teams or customers.

## HOW IT WORKS

This fully managed service is built on virtual devices designed for ongoing data collection. 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, tailored to each customer.

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 the network.

## 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.

bsi. ISO 9001 Quality Management | ISO 27001 Information Security Management | ISO/IEC 20000-1 Information Technology Service Management | CSA STAR Cloud Security | ISO 22301 Business Continuity Management | ISO 50001 Energy Management | ISO 14001 Environmental Management | BS 10012 Data Protection | ISO 27017 Security Controls for Cloud Services