Security & Information Assurance

Do you have a strategy for monitoring and responding effectively to threats? Delivered from our UK based security operations centre, we can help reduce your spend on security monitoring and risk management.

Our service offers you an intelligence-led approach to protecting your information, intellectual property and most valuable assets. We provide security support, regulatory compliance and alerts for your IT infrastructure to help you mitigate the risk of attack.

We monitor your network providing detailed analysis and alerts against a globally sourced catalogue of known and emerging security threats so you can anticipate and respond. Our service is powered by IBM QRadar, rated by international analysts as one of the world's best security analytics platforms.

KEY FEATURES

- Managed security information and event monitoring (SIEM)
- Integration of a wide range of customer environment log sources
- Proactive security alerts
- Detailed event correlation and automatic prioritisation
- End to end service reporting and SLAs
- Expert security operations centre
- IBM X-Force integrated global threat intelligence

KEY BENEFITS

- Single solution for event and data flow log management
- Reduces the cost of security monitoring and risk management
- Built on market leading IBM QRadar platform
- Delivered from a UK based security operations centre
- Assists with GDPR compliance
- Removes complexity of managing hybrid cloud services

Integrate multiple log sources for security analysis

24/7 Proactive security event monitoring

Fast response times to security events

Expert security operations centre

Help internal compliance and regulatory bodies

Why Us?

- Service intelligence built with internal SCC expertise, knowledge and experience
- Centralised management, monitoring and response from a dedicated cyber security team
- Evolving service offering to maintain security posture
- Enhanced features to come around vulnerability and risk management against the SIEM output providing greater intelligence

Service Offering

The Cyber Security Intelligence Service is available to customers with the following service options:

Feature	Standard	Managed
Log Correlation/Normalisation 24/7	Yes	Yes
Event/Alert Triage	Optional	Yes
Detailed Reporting	Yes	Yes
Remediation Recommendations	Optional	Yes
QRadar Standard Log Sources	Yes	Yes
Bespoke/Non-standard Log Sources	Optional	Optional
Compliance Policy Implementation	Optional	Optional
Service Management	Yes	Yes
8/5 Security Operations Centre	Yes	-
24/7 Security Operations Centre	-	Yes
Proactive Log Analysis	-	Yes
IBM X-Force Integration	Yes	Yes
Powered by Watson	Yes	Yes
Emergency Support (P1)	Optional	Yes

TECHNOLOGIES MONITORED

- Servers: Windows, Linux, IBM
- Platforms: Azure, Office 365, SharePoint
- Authentication: Active Directory, RSA
- Services: Exchange, end point protection (AV, encryption, IDS, IPS etc)
- Network: Cisco, Huawei
- WLAN: Fortinet, Cisco, Huawei
- Network Defence: Checkpoint, Cisco, Fortinet, Juniper, Tipping Point, Citrix (firewalls, load balancers, IDS, IPS, remote access etc)

OFFICE MANAGEMENT

- Average 100 a week that become incidents for management
- Average 1 per month that become major incidents
- 1000's that become records for trend analysis, information building