

# SCC FOR HEALTHCARE



## PROTECT AND SECURE

## SIEM

**Securing patient and staff data has never been more important. With recent high-profile data breaches and changes to data protection regulations, healthcare organisations are under pressure to protect their IT infrastructure and business information. This is compounded by the difficulty of integrating and updating legacy systems, as well as a shortage of in-house security skills. In some instances, legacy security capabilities cannot meet growing threats, for example the disruption caused by the WannaCry attack in 2017.**

### **SECURITY INCIDENT AND EVENT MANAGEMENT (SIEM)**

Delivered from our UK-based security operations centre, we offer security solutions that will protect every aspect of an IT network and infrastructure. We can also help to reduce spend on security monitoring and risk management while offering the most resilient protection.

SIEM is an important piece of any organisation's security strategy, to monitor the whole network and all connected devices and proactively alert organisations of impending risk. In the fight against cyber crime, SCC can deliver a full SIEM service for healthcare organisations to protect their data, information, intellectual property, and valuable information assets.

Using IBM QRadar, the market-leading advanced analytics engine, SCC's managed SIEM service provides proactive security event monitoring and alerting. It collects data from multiple sources and compares it against a globally sourced catalogue of known threats.

SCC removes the overhead of retaining onsite security resources by having a dedicated team of specialists in our 24/7 Security Operation Centre (SOC). Our SOC complies with many government accreditations including ISO 27001:2013, GPG13 security compliance for PSN and PCI Compliance.



## Why Partner with SCC?

By partnering with SCC we can help healthcare organisations address cyber security issues by providing medical professionals with secure access to a compliant IT infrastructure that protects their data, network, applications, and devices from internal and external security breaches through a fully managed solution with 24/7 support.

We help to reduce spending on security monitoring and risk management, offering the most resilient protection available. Clinicians can have increased confidence that they are making decisions with correct, complete, and consistent data. Finance departments can have confidence that procedures are coded correctly and revenue streams from CCGs are correct and timely.

### KEY FEATURES

- Service intelligence built with internal SCC expertise, knowledge, and experience
- Centralised management, monitoring, and response from a dedicated cyber security team
- Managed security information and event monitoring
- Integration of a wide range of customer environment log sources
- Evolving service offering to maintain security position
- Service intelligence built with internal SCC expertise, knowledge, and experience
- 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

- Protects healthcare organisations' reputation and productivity
- Secures healthcare organisations' most valuable assets – confidential information and intellectual property
- Single solution for event and data flow log management
- Transforms the cyber security approach from reactive to proactive
- Reduction in the cost of security monitoring and risk management
- Delivered from a UK-based security operations centre
- Supports the healthcare organisation's security compliance strategy
- Removes the requirement for in-house skills.