SCC FOR CENTRAL GOVERNMENT

SCC We make IT work

PROTECT AND SECURE

SIEM

With increased regulation and the need for GDPR compliance, the protection of citizens' data is of the utmost importance, together with inter-agency collaboration, and improving cyber defences. With recent high-profile data breaches and changes to data protection regulations, Central Government departments and agencies are under pressure to protect their IT infrastructure and business information.

As cyber attacks become more sophisticated it is imperative that confidential data is kept safe, and that the most effective strategy for monitoring and responding to threats is already in place.

INTRODUCING SECURITY INCIDENT AND EVENT MANAGEMENT (SIEM)

Delivered from our UK-based security operations centre, we offer security solutions that protect every aspect of an organisation's IT network and infrastructure. We can also help to reduce spend on security monitoring and risk management, while offering organisations 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 Central Government departments and agencies to protect their data, information, intellectual property, and most valuable information assets.

Using IBM QRadar, which is a market-leading advanced analytics engine, SCC's managed SIEM service provides 24/7 proactive security event monitoring and alerting. It collects data from multiple sources and compares it against a globally sourced catalogue of known threats.

We remove 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 government accreditations including ISO 27001:2013, GPG13 security compliance for PSN, and PCI Compliance.

Why Partner with SCC?

SCC offers security solutions that protect every aspect of an organisation's IT network and infrastructure. Solutions work seamlessly together to protect against and halt the spread of viruses, malware, and ransomware attacks. We help to reduce spending on security monitoring and risk management and help to protect staff and citizens with secure access to a compliant IT infrastructure that protects data, network, applications, and devices from internal and external security breaches.

KEY FEATURES

- Service intelligence built with 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
- Proactive security alerts
- Detailed event correlation and automatic prioritisation
- End to end service reporting and Service Level Agreements (SLAs)
- Expert security operations centre
- IBM X-Force integrated global threat intelligence.

KEY BENEFITS

- Protects the reputation and productivity of Central Government departments and agencies
- Secures organisations' most valuable assets – confidential information and intellectual property
- Offers a 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 organisation's security compliance strategy
- Removes the requirement for in-house skills.

scc We make IT work

CONTACT
publicsector@scc.com