Our vision is to help you build, implement and maintain an ongoing programme to reduce cyber risk in a way that's right for your business. Our managed SIEM service is part of a range of services we've developed to help you succeed in an ever-changing landscape.

What is the Managed SIEM service?

Our SIEM (Security Information and Event Management) service is designed to reduce cyber risk by monitoring for, and detecting, security threats – enabling you to respond quickly, with guidance from our Cyber Analysts. Our platform also retains all the logs you need for audit and forensic investigation purposes, and supports compliance with regulations and standards such as GDPR.

How does it work?

The service is delivered using our managed SIEM platform, which collects, normalises and stores millions of logs from multiple sources across your IT, cloud and SaaS environments. The advanced platform uses continuously updated threat intelligence and provides endpoint intrusion detection, user activity monitoring, event correlation and log management to identify and prioritise threats. Cloud, on-premise and hybrid deployment options are also available.

KEY FACTS

- ***Comprehensive*** – integration with Check Point's Incident Response Service
- ***Reassuring*** – continuously updated advanced threat analytics
- ***Reliable*** – highly accurate incident detection
- ***Seamless*** – cloud, on-premise and hybrid deployment options
- ***Compliant*** – ISO 27001 and Cyber Essentials Plus accredited

What are the benefits?

Continually monitors threats, so you don't have to

Using the millions of logs and data about users, assets and vulnerabilities collected from your IT environment, our platform applies machine learning and advanced behavioural analytics to quickly detect and validate threats. This not only enables faster incident response, but also frees up your team to focus on achieving your business's key objectives.

Eliminates time wasted on false threats

We can help you understand exactly which response actions need to be taken and when. By continuously tuning and calibrating our SIEM and SOAR (Security Orchestration, Automation and Response) platforms to your specific environment, we identify and remove false positives and ensure only genuine threats are reported to you via highly accurate alerts.

Makes complex security issues easy to understand

We offer an easy-to-use dashboard of key metrics and real-time information, along with detailed written reports drafted by our expert analysts on a monthly basis. The reports set out key recommendations for improving your cyber security in a way that's simple to understand – and we provide service review workshops by WebEx, to talk you through it all.

Reduces the expense of cyber security

Our SIEM platform is fully managed by our dedicated team of security analysts, providing you with market-leading technology and expertise, without the need to build a costly in-house capability. The team is based in Marlow, in the UK, and operates on a 24/7/365 basis to give you the support you need, when you need it.

Minimises downtime and disruption

Our service fully integrates with Check Point's Incident Response Service. This is available around the clock to contain any threats, minimise financial and reputational loss, and reduce downtime. We have a 30-minute remote support response SLA, ensuring the IRT (Incident Response Team) can quickly deal with incidents to minimise disruption.

WHY SOFTCAT

- Fully managed security monitoring service – save time and money
- Expert guidance on threat response – reduce the impact of incidents
- Easy-to-understand reporting – simplify complex issues and findings
- Workshop-led service reviews – know where to make improvements
- Around the clock support – strengthen your cyber resilience