

Providing the core intelligence to protect your business

No network is totally secure. But the quicker you can spot a breach, the quicker you can snuff out the threat. A Security Incident and Event Management System (SIEM) can help you understand what is happening in real time on your network before anything causes a problem. At BT we can design a SIEM solution that's right for your business. We'll tailor to just how you need, tap into the latest technology from our partners and monitor it round the clock to protect your most important assets.

Your network and IT infrastructure are vital to the success of your business. No doubt you keep them protected – with firewalls, intrusion prevention systems, email scanners, anti-virus systems and other controls – but no network can be made totally secure. Hackers and criminals know the value of your data and use increasingly sophisticated means to gain access to your networks and data.

If your network or IT is breached, the time from when the attack occurred to when it is detected is vital. The shorter this time the more likely you are to be able to contain the incident, protect your organisation's most vital data and avoid having sensitive information exposed on the internet or to the media.

Providing insight into your network

A Security Incident and Event Management System (SIEM) can help you understand what is happening real time on your networks, detect and highlight malicious activity, threats and attempted hacks before they become an issue.

Sizing and deploying a SIEM, however, is a complex task. Get it wrong and you could end up with an expensive asset that fails to provide the insight and situational awareness as to what is happening in your networks and IT infrastructure that you need to detect and respond to hacks and malicious behaviour.

At BT we can design a solution that is right for you. We can tailor our support to whatever you need, wherever you do business. Our security experts will monitor your SIEM around the clock and give you detailed reports on your system's health and performance. We will manage software upgrades and patching, proactively respond to faults and ensure your SIEM is operational 24x7, leaving your or BT analysts free to focus on responding to the events the SIEM detects and flags.

Protect yourself – and your most important assets – with the best

- get a **better insight** into your network
- enjoy a **fully tailored** solution
- have a **dedicated team** of security experts and constantly evolving technology
- access the **latest technology** – with SIEM solutions from leading vendors including McAfee, IBM QRadar and LogRhythm

A complete solution, tailored for you

Our managed SIEM service provides a number of advantages over and above a typical in-house or DIY implementation. Our experts specialise in the deployment and configuration of SIEM platforms. We proactively test SIEM appliances, both on set-up and following in-life changes, as further assurance of security.

We can deploy complex solutions on your sites anywhere in the world, with full project management and service commissioning. Our accredited security team will proactively monitor your SIEM 24x7x365, while our management processes include in-life software updates and application patches.

Our IT support partners provide onsite attendance around the world, to replace faulty equipment and restore service within hours. You can access detailed reports through a secure customer portal, providing information on system health and threat activity. These reports can be used to analyse user activity and provide assurance of hacking prevention.

We can even take over an existing SIEM system you have already deployed (subject to some basic checks) and bring the benefits of our managed service. And if you lack the internal expertise to be able to fully exploit and respond to the information and visibility that a SIEM solution provides, then our Cyber Core Service gives you access to our highly skilled cyber SOC analysts to manage this on your behalf.

	Foundation	Foundation Plus	Premium
Description of your needs	Limited or no security staff. IT support staff have difficulty responding to large case volumes	Robust IT service management but limited security capability	Looking to embed outsourced SOC resources as an integral part of the IT Service Management & Security Operations
Continuous improvement & tuning	Six month review of service effectiveness with change management fees	Quarterly review of service effectiveness with agreed changes	Monthly reviews with dedicated in-life service optimisation lead
Monitoring & management	Health monitoring, threat visibility, reactive P1 response, automatic P3 fix	Proactive P1 joint actionable intelligence & restoration, enhanced P1/P2 reporting	Customer-defined P1/P2, guaranteed fix on P1
Controlled deployment	48 hour window to confirm inputs	30-day joint data validation and rules optimisation. 90-day SIEM joint data validation and rules optimisation	30-day joint data validation and rules optimisation. 90-day SIEM joint data validation and rules optimisation. Rules employing tailored intelligence sources
Initial set-up	BT best-practice policy	Industry best-practice policy, joint decision	Customer-specific enhanced policies

Why choose BT?

Industry-leading protection against new and dynamic threats

We work with market leading vendors. The solution is based on a choice of technologies to protect your business: McAfee, IBM and LogRhythm.

Experts on hand

Reduce the need to recruit and retain specialist IT staff. Our 2,500+ security specialists have expertise in the latest technologies and provide 24x7x365 cover.

Scalability

Our highly scalable service can meet the needs of all sizes of organisation – from those organisations with a few sites and hundreds of devices though to global organisations with many thousands of devices that need monitoring.

Proactive monitoring

From our 14 Global Security Operations Centres we provide a centralised monitoring of your SIEM, giving you the information you need to respond proactively.

Maintain ownership of your security policy

You remain in control of your security policy, while we help you to define it, ensuring it is expertly implemented and maintained.

Professional services

We can provide you with technical consultants on an “as needed” basis, complementing your organisation’s in-house skills and providing analysis and design expertise which will optimise the performance of your solution.

What could Managed SIEM do for you?

Visit bt.com/globalservices

Offices worldwide.

The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract. © British Telecommunications plc 2019. Registered office: 81 Newgate Street, London EC1A 7AJ. Registered in England No: 1800000.

Issued: January 2019

