Detect and respond to threats quicker with our Managed SIEM service

No network is totally secure. But the quicker you can spot a breach, the quicker you can deal with 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. We can design a SIEM solution that's right for your business. We'll tailor it to your needs, tap into the latest technology from our partners, and monitor it round-the-clock to protect your most important assets.

Protecting your data and monitoring your environment is vital

In today's digital world, your organisation is increasingly reliant on the networks and IT infrastructure that support it. If your networks or systems are breached by a cyber attack, then the time between incident occurrence and detection is vital. The quicker you identify a threat, the more likely you'll be able to contain it. You'll be better equipped to protect your organisation's most vital data, and avoid having sensitive information exposed on the internet or to the media.

A SIEM can help you understand what is happening in your IT estate, detect incidents in real time, and highlight malicious activities, 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 and contextual awareness needed to detect and respond to attacks and malicious behaviour.

A solution tailored for you

Our Managed SIEM is a fully managed threat detection service, monitoring and protecting your estate round-the-clock. It's tailored to meet your business objectives and regulatory compliance requirements.

With our Managed SIEM, you retain financial ownership over your platform, which can be hosted on your preferred cloud platform or in your own data centre. However, we'll be responsible for the deployment, configuration, and operation of the solution.

You'll benefit immediately from faster detection and response times, as well as valuable contextual detail and threat intelligence on each confirmed alert.

Key features

- integration and correlation of security and network logs and events including flow data.
- optional integration of vulnerability assessment data into SIEM tool.
- integrated threat intelligence feeds.
- detailed incident reporting.
- comprehensive alert status and on-demand compliance reporting capabilities.

With additional investment, you can leverage next generation features to customise the SIEM capability to meet your requirements:

- we use a combination of our Security Orchestration Automation and Response (SOAR) platform and specialist security analysts to review each alert. We then apply our experience and trusted threat intelligence to provide your security team with only the critical alerts you need to act on.
- reduce alert fatigue – Our SOAR capability filters out false positives and ensures you can focus on responding to genuine threats.

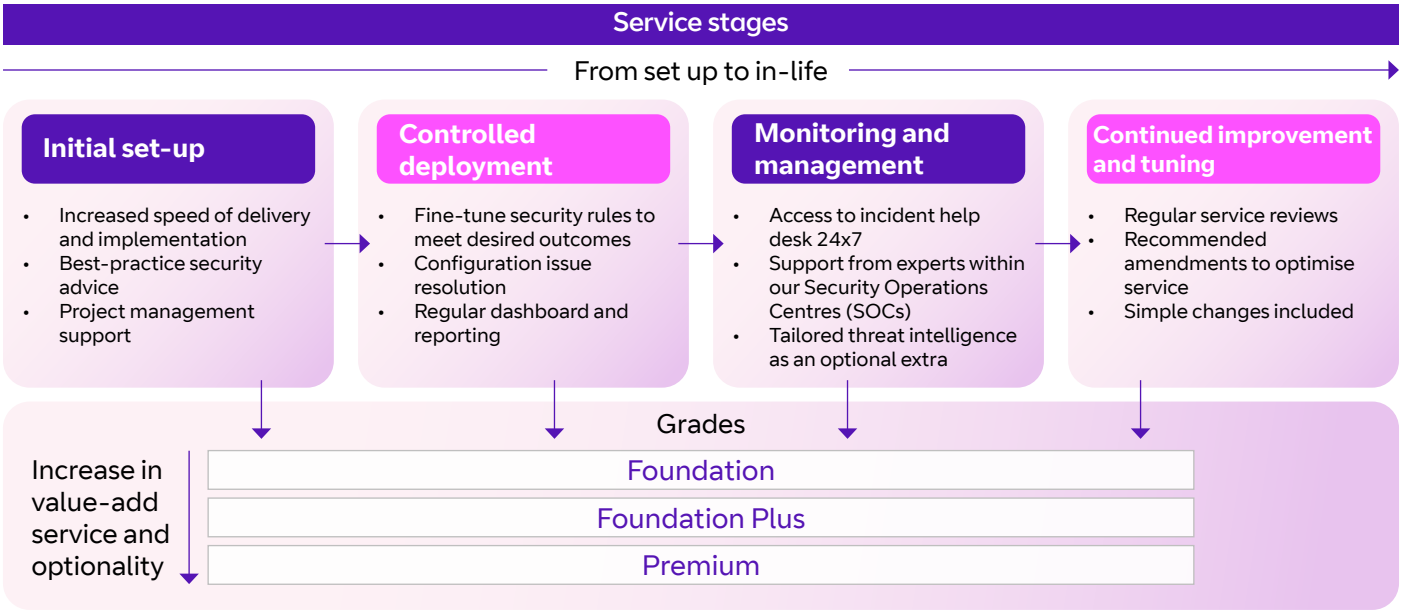
You'll also benefit from our visibility over other global security threats that we see across our wider networks.

Key advantages over DIY

- Our experts specialise in SIEM platform deployment and configuration, finding the best solution for you. SIEM appliances are proactively tested to further assure security, both on set up and following in-life changes.
- We can deploy complex solutions on your sites or in your preferred cloud hosting platform, anywhere in the world, with full project management and service commissioning.
- Our accredited security team will provide round-the-clock SIEM monitoring. Our management processes include in-life software updates and application patches.
- We've got IT support partners around the world to quickly replace faulty equipment and restore service in case of outages.
- Detailed reports can be accessed through a secure customer portal, providing information on system health and threat activity. These reports can be used to analyse user activity and provide hacking prevention assurance.
- We can even take over an existing SIEM system you have already deployed (subject to some basic checks) and provide you with all the benefits of a managed service.
- If you lack the internal expertise to be able to fully exploit and respond to the information and visibility that a SIEM solution provides, we can provide you access to our highly skilled Cyber Security Operations Centre (CySOC) analysts who will manage this on your behalf.

Choose the service level that's right for you

We offer three different service wraps – Foundation, Foundation Plus, and Premium – for you to choose from. Our standardised service stages ensure that your SIEM deployment follows global best practice from initial set up to in-life continuous improvement, helping you develop your cyber maturity.



Benefits to joining forces with us

Industry leading protection against new and dynamic threats

Our Managed SIEM solution is based on market-leading technology to protect your businesses and integrates with incident management solutions.

Proactive experts on hand

Our security specialists globally have expertise in the latest Technologies, and we have CySOCs split across geographical regions to monitor your SIEM round- the-clock, giving you the information you need to respond proactively.

Performance, scalability, and reliability

Our highly scalable service can meet the needs of all organisation sizes – from those with few sites and hundreds of devices, through to global organisations with many thousands of devices that need monitoring. Our experience in building resilient infrastructure ensures solution reliability with 24/7 software and hardware elements monitoring.

Take advantage of our global experience

We have years of experience protecting both ourselves and some of the largest global organisations from a myriad of security threats. This sort of protection is available for all our customers.

Professional services

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

Maintain ownership of your security policy

You remain in control of your security policy, and we'll help you define and implement it.

What could Managed SIEM do for you? Visit bt.com

Offices worldwide

JN: 1441114433 | May 2024