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. 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 cyberattack, then the time from when the incident occurred to when it's detected is vital. The shorter this time, the more likely you'll 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.

A Security Incident and Event Management System (SIEM) can help you understand what is happening in your IT estate, detect incidents in near 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 that you need to detect and respond to attacks and malicious behaviour.

A solution tailored for you

Managed SIEM is a fully managed Threat Detection service, monitoring and protecting your estate 24x7x365, tailored to meet your business objectives and regulatory compliance requirements.

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

You'll benefit immediately from faster detection and response times coupled with 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, such as:

- Big data platform integration with the SIEM platform
- User Entity Behaviour Analytics module integrated into SIEM
- Security Orchestration and Automation Response (SOAR) platform integration to further automate your incident response.

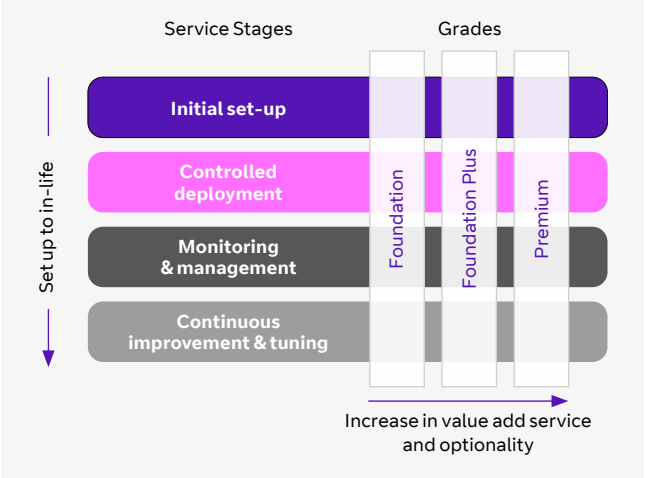
You can also benefit from our visibility of other global security threats that we see across our wider networks.

Key advantages over DIY

- Our experts specialise in the deployment and configuration of SIEM platforms and will implement 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 proactively monitor your SIEM 24x7x365. Our management processes include in-life software updates and application patches.
- Our IT support partners can provide onsite attendance around the world to replace faulty equipment and restore service within hours.
- 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 assurance of hacking prevention.
- 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 our 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, then we can provide you access to our highly skilled cyber SOC 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 setup to in-life continuous improvement, helping you to develop your cyber maturity.



Description of your needs	
Foundation	Customers with limited or no security staff who need an automated, industry standard approach to security managed services. Using best practice standard templates, reporting and service support with an automated customer portal.
Foundation Plus	Customers who have developed their security maturity and who require industry or scenario-specific templates and use cases. They wish to improve their existing security operations by working with us to outsource general CySOC capabilities and provide security best practice guidance.
Premium	Customers who require bespoke, customisable security managed services and wish to establish a security partnership with us where our CySOC services become an integral part of the customer's IT Service Management and Security Operations with high levels of hands-on interaction.

Benefits to joining forces with BT

Industry-leading protection against new and dynamic threats

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

Proactive experts on hand

Our 3000+ security specialists have expertise in the latest technologies. Based in our global Cyber Security Operation Centres, they monitor your SIEM around 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 sizes of organisation – from a few sites and hundreds of devices though to global organisations with many thousands of devices that need monitoring. Our experience in building resilient infrastructures will ensure the reliability of your solution, with 24x7 monitoring of all software and hardware elements.

Take advantage of our global experience

We have many years of experience protecting both ourselves and the largest global organisations from a myriad of security threats, all of which will be available to you.

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 the performance of your solution.

Use case library

We have an extensive library of use cases that can easily be deployed in your Managed SIEM solution.

Maintain ownership of your security policy

You remain in control of your security policy, with help from us to define and implement it.

What could Managed SIEM do for you?

- **Website:** www.btireland.com
- **Telephone:** 1800 924 929
- **Email:** clientservices-ire@bt.com
- **Outside ROI:** +353 1432 4680

Offices worldwide.