Improve threat detection and response with Cloud Security and Information Event Management (SIEM)

Now you can easily detect and mitigate threats to your organisation, without the expense of running an in-house system, using cloud-native SIEM-as-a-service.

Today's interconnected digital landscape is fertile ground for cyber criminals. Hacktivists, ransomware crews, nation state threat actors, and malicious and accidental insiders – the threats facing your business are many and varied.

The devil is in the detail

Most organisations already have plenty of security solutions in place, all generating vast quantities of data. Indicators of compromise are hiding in these logs – the difficulty is how to make them visible to your security team.

A SIEM system can pull all this data together to understand what's happening in real-time to your networks, and to detect and highlight threats and attempted hacks before they become an issue.

Sizing and deploying a SIEM however, is a complex task. If you get it wrong, you could end up with an expensive asset that fails to provide necessary insight and situational awareness. And even if you have successfully deployed the solution, identifying critical alerts, and reducing false positives is harder than it sounds.

Introducing Cloud SIEM from BT

Cloud SIEM is a cyber threat detection and response service which collects logs and events from your estate. It then correlates these events with external threat intelligence to provide actionable alerts.

By using our Security Cloud SIEM, you'll benefit immediately from faster detection and response times, coupled with the valuable contextual detail on each confirmed alert.

We'll take responsibility for detecting potential high-impact attacks on your infrastructure, providing the skills and expertise needed to effectively run, tune, and monitor the service – freeing up your team to concentrate on high value strategic work.

Centralised monitoring and expert analysis

- No initial capital investment – with a subscription (OpEx) based pricing model for predictable costs.
- Rapid, low-risk deployment – using our multi-tenanted architecture hosted in AWS provides immediate value.
- Lower staff costs – no need to hire, train, and retain expensive cyber security experts yourself.
- Round-the-clock support – our accredited security team will proactively monitor your SIEM 24/7, 365 days a year.
- Detailed reporting – access system health and threat activity reports through our secure customer portal.
- Full visibility – a 'single pane of glass' view covers all in-scope security infrastructure.

If you don't have the in-house experts to fully exploit the information and visibility that a SIEM solution creates, we can provide expert security guidance on how to respond to incidents and to continually enhance your security environment.

Focus on the key alerts without overwhelming your security team

We monitor your network in real-time, filtering out routine and false alerts to provide only the information needed to protect your business.

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.

In addition, you get real-time visibility of your security status with comprehensive reporting capabilities available in Cloud SIEM. You can also generate on-demand compliance reports.

Our solution ensures we detect attacks on your organisation as they happen, allowing you to deal with them before they cause significant damage.

Feature	Foundation	Foundation Plus	Premium
Standard use cases and policies	✓	✓	✓
Custom use cases and rules*	3	15	30
Platform health monitoring and maintenance	✓	✓	✓
Onboarding rule setup	✓	✓	✓
Cloud log retention and management	✓	✓	✓
Event correlation	✓	✓	✓
Event / alert management	✓	✓	✓
Trend reporting	✓	✓	✓
Case registration	✓	✓	✓

Feature	Foundation	Foundation Plus	Premium
Incident management and coordination	✗	✓	✓
Best practice security guidance	✗	✓	✓
Mitigation planning	✗	✗	✓
Root cause analysis post-incident support	✗	✗	✓
Security improvement action plan	✗	✗	✓

Options (additional charges apply)	Foundation	Foundation Plus	Premium
Vulnerability scan data integration	✗	Option	Option
Third party ticketing system integration	✗	Option	Option

*** rule usage dependent on appropriate log sources being available**

Why work with us?

- Continuous monitoring – our global Security Operations Centres (SOCs) monitor your estate round-the-clock with pre-defined playbooks for incident response.
- Expert analysts and proven processes – our security team has extensive experience in supporting large customer environments. You'll also get ready-to-use contextualised and actionable information.
- Reduce alert fatigue – our SOAR capability filters out false positives and ensures you can focus on responding to genuine threats.
- Meet your audit and compliance needs – with a single platform, you'll get a consolidated view of your estate, which is aligned with industry standards. We retain your event logs for a period of time, so you have a full audit trail.
- Flexible usage-based pricing – we offer a subscription-based, on-demand solution that can be scaled up and down to meet your needs.
- Partnerships that work – our solution is created by combining our managed service wrap with one of the industry's top technology partners for SIEM.

What could Cloud SIEM do for you? Visit bt.com/security

Offices worldwide

JN: 1441114433 | May 2024