BT Cloud SIEM

Datasheet

Providing the core intelligence to protect your business from constantly evolving threats

You probably have a number of security solutions in place – each solving an individual problem and generating vast quantities of data. A Managed Cloud Security Incident and Event Management (SIEM) system can help you understand what is happening on your networks by pulling all of this data together in real time, enabling you to detect and highlight malicious activity, threats and attempted hacks before they become an issue.

The digital landscape is a dangerous one and it's evolving. Hacktivists, criminals, rogue nation states, malicious and accidental insiders – the threats and attackers facing your business are diverse and skilled. You also need to be prepared as data protection regulations are tightened. As more and more smart devices get connected you need to protect your extended network effectively, while keeping up with the almost 12 million new variants of malware discovered every month. And if your networks or systems are breached by a cyberattack, then the time between the incident occurring and it's detection is vital. Not only do you need to protect your extended network effectively as more and more smart devices get connected. You need to keep up with nearly 12 million new variants of malware discovered every month, and if your networks or systems are breached by a cyberattack, then 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 and protect your organisation's most vital data. But with vast quantities of security data at your fingertips, can you make sense of it all?

Understanding the challenge

A Managed Cloud SIEM can help you understand what is happening in your IT estate, detect incidents in near real time and highlight malicious activities, threats and 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. And even if you have successfully deployed a SIEM solution, reducing the signal-to-noise ratio and extracting actionable intelligence is harder than it sounds. By using BT's Cloud SIEM you'll benefit immediately from faster detection and response times, coupled with valuable contextual detail and threat intelligence on each confirmed alert. We take responsibility for detecting potential high-impact attacks and provide the skills and expertise needed to effectively run, tune and monitor the service – freeing up your people to concentrate on other high value workstreams.

Centralised monitoring and extensive coverage:

- **No initial capital investment** – with a subscription-based (OPEX) 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 scarce and expensive cyber-security experts yourself
- **Round the clock support** – our accredited security team will proactively monitor your SIEM 24/7. Our management processes include in-life software updates and application patches
- **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 gives you, we can provide expert security guidance on how to respond to incidents and to continually enhance your security environment.

Focus on key alerts without overwhelming your security team

Powered by IBM QRadar, currently rated as the industry leader in the Enterprise SIEM space, our cloud-based service monitors log feeds from your networks and generates alerts for any potential incidents on a near real-time basis.

Through advanced correlation technology, intelligence gathering and analysis our Cyber Security Operations Centre (CySOC) analysts can prioritise tasks and focus on critical alerts. The comprehensive reporting capabilities of Cloud SIEM also provide you with near real time visibility of your security status, and the ability to generate on-demand compliance reports with your risk posture, people and processes. At its core, Cloud SIEM is a monitoring and detection service, which combines continuous monitoring, threat detection and collaborative threat intelligence to help detect cyber-attacks of all types. From zero-day exploits to privilege escalation, ransomware and more. We'll deliver these capabilities through a global network of SOCs providing service to our customers 24/7.

Features	Managed Service 1	Managed Service 2	Managed Service 3
Custom use cases and rules	3	15	30
Platform monitoring and maintenance	✓	✓	✓
Onboarding and rule setup	✓	✓	✓
Missing log source monitoring	✓	✓	✓
Cloud log retention and management (<92 days)	✓	✓	✓
Event Correlation	✓	✓	✓
Event/alert management	✓	✓	✓
Trend reporting	✓	✓	✓
Case registration	✓	✓	✓
Incident management and co-ordination	X	✓	✓
Best practice security guidance	X	✓	✓
Root cause analysis/post-incident support	X	X	✓
Backdated IoC hunting	X	X	✓

Security Improvement action plan creation	X	X	✓
Available Options (additional charges apply)	Managed Service 1	Managed Service 2	Managed Service 3
Vulnerability scan data integration	X	Option	Option
Traffic flow analysis	X	X	Option
3rd party ticketing system integration	X	X	Option
Cloud log retention and management (>92 days)	X	Option	Option

Why choose BT?

Continuous monitoring

Our security team has extensive experience of supporting many large customer environments and you'll be able to tap into their skills and expertise. You'll also get contextualised and actionable information that is ready to use. Our global SOCs monitor 24/7 with pre-defined escalation playbooks for incident response.

Meet your audit and compliance needs

With a single platform you get a consolidated view of your estate aligned with industry standards to help meet compliance standards. We keep security event logs on your behalf for up to 92 days (with longer storage available for an additional charge) so you have a full audit trail.

Flexible usage-based pricing

As a subscription-based, on-demand solution you can scale up and down to meet your needs.

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

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.

October 2021