MANAGED SIEM DATA SHEET

UNRESTRICTED

1. MANAGED SIEM

1.1 SERVICE DESCRIPTION

The Bulletproof Managed SIEM service provides 24/7 monitoring of your infrastructure, systems, network and applications for security events. By combining cutting-edge technology with human insight and ingenuity, it protects you from potential security incidents, with proactive alerts, incident response and reporting customised to suit your specific business, compliance and security objectives.

Bulletproof's SIEM service is delivered as a fully managed 'as a service' model, combining flexibility with ultra-resilient and secure in-house cloud hosting. Delivering a SaaS solution eliminates the need for expensive hardware appliances and their associated costs to be integrated into your infrastructure. This creates a drastically more cost-effective solution that also delivers increased power, flexibility and resilience than traditional SIEM deployments.

1.2 KEY FEATURES

The Bulletproof Managed SIEM service comes with advanced features as standard, including:

- **Integrated threat intelligence**
  Be on top of zero-day exploits, new attacks, and ransomware
- **Machine learning (AI modules)**
  Complex algorithms automatically detect behavioural changes
- **Active threat hunting**
  Real-time correlation across multiple sources for automatic detection
- **High-performance log management**
  A highly scalable log engine for limitless collection and storage
- **Powerful web portal**
  A central location to download pre-made and customised reports, as well as query live log data
- **Plug-in enhancements**
  Additional specific security options, including IPS, FIM/DLP, DDoS mitigation and more

Our service offering also includes the following:

- 24/7 support
- High-quality SLAs
- Incident response
- Regular reporting
- Quarterly service reviews
- Dedicated, reachable account manager

1.3 SIEM SOFTWARE PLATFORM

Our custom-built SIEM platform has been extensively developed in-house, engineered for maximum security and scalability. Delivered as a SaaS model means we can offer the service free from licensing and other third-party costs and restrictions. This results in a customised, flexible SIEM service that's tailored to your exact requirements.

Our ownership ethos extends through all layers of our organisation, including owning our own resilient UK data centres, private network infrastructure, and in-house UK Security Operations Centre (see 1.4 below). Bulletproof believes this end-to-end ownership drastically increases our security compared to competitors who use outsourced or overseas SOCs, who don't have their own data centres and network infrastructure.

Every aspect of our infrastructure is regularly scanned and penetration tested by our in-house cyber security specialists, and is certified to ISO 27001, 9001 and PCI DSS v3.2 standards.

1.4 IN-HOUSE SECURITY OEPRATIONS CENTRE

A key feature of Bulletproof is our in-house Security Operations Centre (SOC). Based entirely in the UK, it's the command centre of our cyber security operations and is staffed 24/7 by trained, experienced security professionals.

Our staff are:

- CREST approved
- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Offensive Security Certified Professional (OSCP)
- Tigerscheme Qualified Security Test Member (QSTM)
- Certified Ethical Hacker (CEH)
- ISO 27001 Implementer
- CCNA and CCNP Security
- Certified EU GDPR Practitioner

T: 01438 532 900 E: contact@bulletproof.co.uk W: www.bulletproof.co.uk