MANAGED HOSTED SIEM SERVICE

KEY BENEFITS

- **Improved productivity:** Cloud based and pro-actively managed market leading SIEM platform complemented with proprietary SecureData technology reduces management overhead, complexity and costs.
- **Reduced risk:** 24x7 intelligent automated analysis of events with risk-based scoring using over 700 identifiers.
- **Reduced costs:** Fully-fledged SIEM functionality without the costs of purchasing and maintaining self-managed on premise or cloud devices.

KEY SERVICE FEATURES

- **Increased visibility:** SLA-based alerting highlights potential abnormalities or indicators of attack.
- **Improved compliance:** Internal or regulatory compliance policies auditing requirements fulfilled thorough 365-day storage of logs
- **Holistic security approach:** Event collection across the estate's devices ensures improved threat detection over single-device detection
- **Ongoing detection improvement:** Tuning and retuning log collectors reduce false positives over time increasing ability to accurately detect anomalous events.
- **Track Record:** Benefit from SecureData's experience in both offensive and defensive security gained over 25 years.
- **Latest technology:** MTD platform is at the forefront of technology using the latest detection techniques including machine learning.

SERVICE DESCRIPTION

The service is a fully-managed cloud-based service where SecureData takes full responsibility for the deployment and integration of the service into the customer's environment. We maintain the service through ongoing fine-tuning of rules-bases and customised rule creation for enhanced threat detection.

Events are automatically correlated and analysed using an industry leading SIEM platform supplemented by open-source, commercial and SecureData proprietary toolsets for indicators of attack and compromise along each of the stages of the cyber kill-chain.

For organisations requiring log collection and storage, our service collects, classifies and aggregates events and archives these in our UK-based datacentres for up to 1 year. Historical data can be made available on request to aid the customer's investigations into incidents.

Alerts of suspicious activity are communicated via email for remediation by the customer. This service includes use of proprietary and commercial compromise databases to identify compromised passwords, sites and devices.

KEY TECHNICAL COMPONENTS

Log Collection and Storage

- Log and event collection by SecureData's Managed Threat Detection platform
- Log storage for 1 year
- Log and event correlation and aggregation with automated advanced attack analytics
- Retrieval of historical log data as requested
- Ongoing tuning of the log collection platform

Analytics

- Access to Threat Advisory Services and full vulnerability database
- Use of proprietary and commercial reputation lists to track communication with potentially malicious IP addresses
- Use of proprietary and commercial malware analysis databases to identify malware

Alerting and Reporting

- Access to web-based console
- Access to pre-defined SIEM reports
- Compliance reporting against supported compliance frameworks
- Communication details of any compliance violations

FOR MORE INFORMATION PLEASE CONTACT US
T: +44 (0)1622 723400 | E: info@secdata.com

WHY SECUREDATA

Cybersecurity specialists
SecureData specialises in cybersecurity services and solutions, with a 25-year track record of delivering managed services to some of the largest companies in the world.

Flexible delivery:
We take logs from your existing network infrastructure and security products, maximising and securing all your previous investments.

Extensive security insight
SecureData's Greater Intelligence platform processes over 50 billion events per month, giving us unparalleled access to current and emerging threats. SensePost, our elite consulting arm, is at the forefront of cybersecurity - providing insight into the criminal mindset. We use this information to ensure our Managed Hosted SIEM customers are as secure as they possibly can be.

Vendor insights
Our close partnerships with various vendors provides superior access to their technical experts and product roadmaps - keeping our SOC's knowledge ahead of the game.

Complementary services
We offer a broad range of services that can complement our Managed Hosted SIEM service and strengthen your security posture, including Managed Firewall, Managed IDS/IPS, Managed Vulnerability Scanning and Managed Compliance Monitoring.

ABOUT SECUREDATA

SecureData is a leading provider of cybersecurity services and solutions.

SecureData looks beyond point technologies to address cybersecurity as a whole. The company offers a comprehensive set of professional and managed security services across the entire attack continuum.

For over 25 years SecureData has been helping organisations assess risks, detect threats, protect assets and respond to breaches quickly and effectively ensuring essential IT infrastructure always remains secure and available.

SensePost, the consulting arm of SecureData includes some of the world's most preeminent cybersecurity experts. Trusted by both corporate and military organisations across multiple countries, SensePost helps organisations to protect IT infrastructure and stay ahead of evolving cybersecurity threats.

Operating across the UK, South Africa and the USA, SecureData has an enviable track record having delivered cybersecurity services for many business sectors including finance, insurance, retail, property, professional services, technology and government.

@SECUREDATAEUROPE @SECDATAEU WWW.SECDATA.COM

@SENSEPOST @SENSEPOST WWW.SENSEPOST.COM

SENSEPOST CONSULTANCY

FOR MORE INFORMATION PLEASE CONTACT US
T: +44 (0)1622 723400 | E: info@secdata.com