MANAGED THREAT DETECTION 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 advanced indicators of attack and compromise.
- **Decreased time-on-target:** Earlier discovery of threats reduces threat persistence and improves attack disruption

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.
- **Enhanced detection:** Experienced, skilled human analysis reduces false positives and enables threat prioritisation focussing efforts on meaningful events.

SERVICE DESCRIPTION

For organisations requiring near real-time interception and accurate identification of threats, our Managed Threat Detection service offering enhances our Hosted SIEM service by applying skilled SOC analysis on events to the automated analysis.

Human analysis serves to remove false-positives, improve detection accuracy, apply severity levels and threat prioritisation through custom alerting. This tier also includes the use of honey-tokens masquerading as legitimate users, file and directories to indicate potential attacks.

Customers will also get access to SecureData's Threat Advisory Services and collated vulnerability databases. This service does not include active Threat Hunting, Digital Forensics or Incident Response.

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
- Modification and customisation of standard log parsing rules. Custom log sources can be developed on request and might incur additional charges

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

Investigation, Triage and Response

- Alarm triage by skilled SOC Security Analysts

Alerting and Reporting

- Access to web-based console
- Access to pre-defined SIEM reports
- Compliance reporting against supported compliance frameworks.
- Communication of details of compliance violations
- Communication of triaged alert details
- Alert classification by skilled SOC Security Analyst
- Access to the SecureData portal with views of current alerts, alert incident trends and service performance

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 Threat Detection 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 Threat Detection service and strengthen your security posture, including Managed Firewall, Managed IDS/IPS, and Managed Vulnerability Scanning

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