MANAGED THREAT DETECTION
MANAGED THREAT HUNTING
MANAGED ADVANCED THREAT HUNTING

SERVICE DESCRIPTION

In response to the realisation that not all attacks can be prevented, organisations with mature risk assessment and mitigation policies are investing in methods of detecting and hunting the threats that have bypassed traditional defences and penetrated their networks.

Accurately detecting threats requires more than simply collecting device logs or reviewing SIEM entries. Multiple contributing factors need to be considered:

- events and behaviours need to be correlated across an organisation's entire estate
- vulnerability data and emerging threats need to be considered
- the broader threat environment needs to be factored in using targeted threat intelligence
- behaviour analytics that do not rely on signatures to detect sophisticated attacks need to be applied
- expert review determining whether suspicious events and behaviour represent an Indicator of Attack or Compromise is required
- threat hunting needs to be an ongoing exercise constantly assessing the behaviour of the network for anomalies

Using our proprietary Managed Threat Detection platform to apply context and substance to collected data through commercial technology, open-source & proprietary software and human resources, our service rapidly and accurately focusses in on the handful of indicators that reveal an attacker's presence.

KEY BENEFITS & DELIVERABLES

- **Enhanced Security & Visibility:** Constant vigilence of security events rapidly identifies anomolous behaviour
- **Analyst Led Detection:** Experienced, skilled human analysis reduces false positives and enables threat prioritisation focussing efforts on meaningful events (Threat Hunting Only)
- **Reduced risk:**24x7x365 analysis of events with risk-based scoring using over 700 advanced indicators of attack and compromise
- **Minimised Time-On-Target:** Earlier discovery reduces threat persistence and improves attack disruption
- **Ongoing Detection Enhancement:** Tuning and retuning log collectors reduce false positives over time increasing ability to accurately detect anomalous events.
- **Improved productivity:** Cloud based and proactively managed market -leading SIEM platform complemented with proprietary SecureData technology reduces management overhead, complexity and costs.
- **Reduced costs:** Fully-fledged SIEM functionality without the costs of purchasing and maintaining self-managed on premise or cloud devices
- **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 compliance reporting

KEY SERVICE COMPONENTS

- Log & event collection by SecureData's Managed Threat Detection platform
- Log storage for 1 year with retrieval of historical log data as requested
- Log and event correlation and aggregation with automated advanced attack analytics
- Modification and customisation of standard log parsing rules. Custom log sources can be developed on request at additional cost
- Access to SecureData's Threat Advisory Services and risk-scored CVE vulnerability database
- Use of proprietary & commercial reputation lists to track communication with potentially malicious IP addresses
- Use of proprietary & commercial malware analysis databases to identify malware
- Use of proprietary & commercial compromise databases to identify compromised passwords, sites and devices (Threat Hunting Services Only)
- Alarm triage by skilled SOC Security Analysts
- Investigation of alarms in context for potential attacks or compromises on an ongoing basis (Threat Hunting Services Only)
- Retrieval and interpretation of historical log data as required (Threat Hunting Services Only)
- Ongoing access to designated security consultant (Advanced Threat Hunting Only)
- Access to the SecureData portal with views of current alerts, alert/incident trends & service performance
- Access to pre-defined reports
- Monthly annotated management reporting with information on alerts & incidents with commentary and trend information (Threat Hunting Services Only)
- Monthly review meeting with Security Consultant to examine & interpret alerts, attacks & compromises highlighting noteworthy trends (Advanced Threat Hunting Only)
- Compliance reporting against supported compliance frameworks
- Communication of:
  - o details of compliance violations
  - o triaged alert details
  - o full details of potential attacks or compromises
- Alert classification by skilled SOC Security Analyst

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.

Outstanding expertise
Our Managed Firewall service is delivered by our UK-based SOC - delivering immediate, 24x7x365 access to specialists who deal with device health incidents, requested and recommended changes, security optimisation and help ensure continuous availability.

Extensive security insight
SecureData's Threat Intelligence platform processes over 30 billion security 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 mind-set. We use this information to ensure our Managed Firewall customers are as secure as they possibly can be.

Vendor insights
Our close partnership with Check Point, Fortinet, Cisco and Palo Alto Networks 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 complement our Managed Firewall service and strengthen your security posture, including Managed IDS/IPS, Managed Threat Detection, 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

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