Security Monitoring Service

Powered by CORTEX™ BY PALO ALTO NETWORKS

Ensure your business follows recognised industry good practices by leveraging leading next generation technology, certified security specialists and a fully sovereign UK SOC.

paloalto® NETWORKS

Net Consulting's Security Monitoring Service provides real time detect and alert capabilities. Based on Palo Alto's leading Cortex platform, the service is cloud-native and monitors networks, users and data to detect suspicious activity, security policy violations or data breaches. Improve your organisation's due diligence and legal and regulatory compliance with Security Monitoring from Net Consulting.

Machine Learning (ML) driven automation is used to manage the volume of events from your enterprise and provide a complete picture of each alert, stitching together disparate event data to reveal root cause and event timelines for analyst triage.

More unusual threats are assessed further by our specialist security analysts to provide additional context and support for customer incident response teams. Detected threats are alerted to your incident response team through pre-agreed contact paths.

Where threats are identified, these are notified as security incidents. Following the defined process, and our analysts provide initial next step recommendations. Our analyst team are then available to provide remote support to your incident management team.

Using experienced security specialists with detection processes aligned to Mitre's ATT&CK framework and a comprehensive threat database, the service stays current against the evolving threat landscape.

Our service combines industry leading (next generation) technology, certified security specialists and follows recognised industry good practices.

Features & Benefits

Features

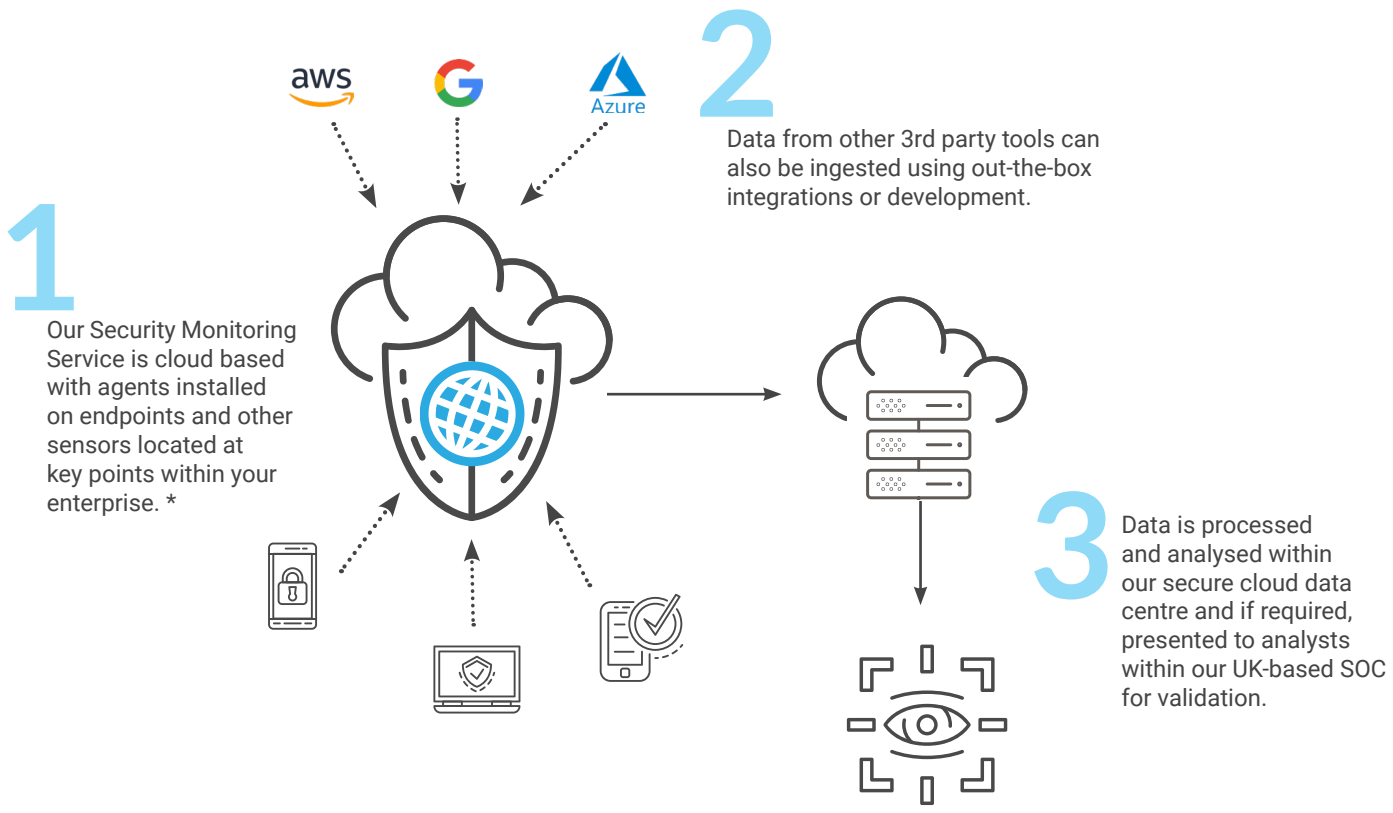
- Monitoring enriched with threat intelligence
- Proactive ML driven analysis to improve detection of advanced threats
- Built and operated to industry good practice
- Delivered from UK - based ISO 27001:2013 certified Security Operations Centre
- ITIL aligned service management processes
- Cloud native and turnkey solutions for rapid on-boarding
- Security cleared staff
- Event and incident data securely retained

Benefits

- Customer dashboards provide situational awareness, aids attack detection and improves time to detect
- Reduces probability of incident
- Minimises incident impact through quicker more informed response
- Supports compliance requirements
- Aids legal and forensic investigations
- Helps you manage compliance, legal and Incident costs

Service Delivery

Fully managed, self-service and virtual SOC/co-managed operating models are available.



*Subject to your change control, the service can be implemented in a matter of days and developed as more endpoints are added.

Service Levels, Reporting & Pricing

Service Levels

	Standard Package	Enhanced Package
Automated Detection, Alerting & Response	24 hrs/day, 365 days/year	24 hrs/day, 365 days/year
Analyst Response	Normal business hours	24 hrs/day, 7 days/week (on call)
Analyst Support	Normal business hours	24 hrs/day, 7 days/week (on call)
Service Desk	Normal business hours	Normal business hours

Reporting

Daily	Weekly	Monthly
Notification of significant activity i.e. high priority incidents created or updated.	Email summary of activity in period, incl: • Number of events processed • Number and type of incidents by category (malware, phishing etc) and priority. • Summary of incidents, responses and status • Identification of encrypted drives on endpoints • Summary status of endpoints and last contact	Email summary of service management activity expressed as point in time and monthly trending, incl: • Number of service fulfilment requests • RFCs received/in-progress in period and status • Service levels and key performance indicators – trending of key measures/ metrics over 12 month period • Annotated relevant contextual information • Summary of threat hunting/ digital investigations/other-ad-hoc investigations undertaken and status • Data storage volume consumed vs available including trending growth • Recommendations for improvement

Pricing

We offer a range of flexible pricing options dependent upon your preference. The services can be extended or augmented selecting options from the Service Catalogue.