Next Generation Security Operations

Taming Cyber Security Complexity

With resourcing constrained, an IT team neither wants nor can afford to spend valuable time dealing with events that don't pose a threat to the organisation. Such events present a danger by masking the real threats and consequently taking too long to identify and contain a breach. A SIEM is an important tool in addressing this challenge. Tools alone don't alleviate the problem of time and resource being faced by organisations. Also, as security tools become increasingly advanced, they can become more challenging to manage.

Organisations need cost-effective future-focussed SIEM solutions without the worry of rising people and storage costs. They want technology that can adapt and expand as they do, and a supporting service that can ensure that technology is optimised, making them more efficient and more secure.

Sapphire's fully Managed SIEM service delivers the answer to these challenges.

How Sapphire can help you

Sapphire's Managed SIEM service delivers industry-leading Gartner® Magic Quadrant™, SIEM technology together with skilled implementation and operations from our dedicated cyber security experts, without the need to invest in SIEM infrastructure or recruit and retain in-house security analysts. Our service operates 24x7x365 service freeing up your team's time for more critical tasks whilst protecting your critical business operations and data.

You will benefit from the implementation of a scalable, cloud-native offering, providing advanced capabilities for log management and SIEM with limitless scale, on-premises or cloud, driven by our experts who understand the threats you face and how to defend against them.

Key Benefits

- Reduced time and resource burden
- Improved operational efficiencies in remediation, control and threat mitigation
- Customisable to your needs
- UK instance to remove data sovereignty concerns
- Faster, more accurate TDIR
- Stay compliant

Our Security Analysts will examine threat information to assess validity, severity and impact. We correlate this data against multiple premium threat intelligence feeds, commercial, open-source and government, providing context and deeper insight.

Contextualised threat data, combined with the experience of our analysts, our threat modelling and threat hunting methodology, reduces our mean time to respond. We improve operational efficiencies in remediation, control and threat mitigation above and beyond the technology by combining our expert analysts, engineering-first approach, threat intelligence lead methodologies and artificial intelligence to secure your business.

We operate a transparent service with all our automations and responses recorded and made available on our Services Dashboard. You also have transparency and clarity on your service costs, with both the management service and log storage

Utilise our skilled team to reduce your risk and exposure profile. Contact us today.

CONTACT US TO FIND OUT MORE

sapphire.net | 0845 58 27001

included in the fee, so you always know where you stand.

Enhance your SIEM with advanced UEBA

Are you concerned about malicious insider threats as well as the threat posed by internal weaknesses, human and technological? Having the ability to detect anomalies not only in the behaviour of the users in a corporate network but also the routers, servers, and endpoints in that network, is an important tool in your armoury.

The Advanced Security Analytics module works on top of the SIEM, providing further user and entity behaviour analytics, upgrading the ability to detect and respond to complex attacks. By analysing logs, enriching data with threat intelligence, and learning normal behaviour, it quickly pinpoints anomalies and assigns risk scores that help analysts prioritise response.

Summary

Standard Service

- Fully Managed UK Based SOC
- Cross-Platform Threat Detection
- System Monitoring (Incl. Windows, Linux, HP-UX, AIX)
- Cloud Infrastructure and SaaS Monitoring
- Network Infrastructure Monitoring
- End to End Case Management
- Statistical Analysis of Log Data
- Integrated Threat Intelligence Ecosystem
- Monthly Reporting
- Quarterly Review
- Robust SLA
- Customer Facing Dashboards
- Global Incident Response Included
- Dedicated Human Analyst Threat Hunting

Enhanced Service

All the above plus:

- Advanced Security Analytics (advanced UEBA)
- Anomaly Search

With Sapphire managing your SIEM service, you will benefit from a reduction in time and resource burden, improved Threat Detection and Incident Response (TDIR), achieve a better return on your investment, and meet your compliance requirements.

Utilise our skilled team to reduce your risk and exposure profile. Contact us today.

CONTACT US TO FIND OUT MORE

sapphire.net | 0845 58 27001