# Managed SIEM Service Description

SAPPHIRE™

25TH ANNIVERSARY

# Introduction

This Service Description details the Managed Security Information and Event Management (SIEM) service from Sapphire.

The information provided may change from time to time as new features and functionality are introduced.

## Contents

# Measuring Security Success

**Included are the key features that make up the components of our Managed Service; however, there are also additional benefits our Managed SIEM offer, designed to improve cyber-ops maturity and performance.**

## 01 A Reduction in Threat Dwell Time

Dwell Time is the duration a threat or threat actor has undetected access within a network or system until completely removed. Longer Dwell Times lead to greater exposure to threats being successful, increasing risk and cost. The Sapphire Security Operations Centre (SOC) measures the Dwell Time of discovered threats. More than just a metric, this represents a positive step towards a mature security posture.

## 02 Reduction in Mean Time to Detect (MTTD)

Faster detection of threats is a crucial target for our SOC. It improves operational availability for customers, and early detection can prevent exploitation and provide valuable insight into how and why a cyber incident has occurred. We monitor multiple indicators of compromise (IoC) and analyse events against numerous threat intelligence sources. This process helps eliminate false positives and offers valuable context.

Reducing MTTD greatly impacts the effectiveness of a threat or exploit. It can slow down lateral movement, make communication with command and control (C2) servers less likely, reducing exposure.

## 03 Mean Time to Respond (MTTR)

Our Security Analysts examine threat information to assess validity, severity and impact. We correlate this data against multiple premium threat intelligence feeds, providing context and deeper insight. Credible threats are reported to customers via cases, which contain both evidence and Analyst commentary, assisting with remediation.

Contextualised threat data, combined with the experience of our analysts, reduces our MTTR. We help to improve operational efficiencies in remediation, control and threat mitigation.

MTTD and MTTR are measured and reported based on an average of all cases raised over a reporting period. We measure Dwell Time from the timestamp of the earliest evidence detected to the point of case creation. These metrics help illustrate a continual improvement in cybersecurity operations.

**102%**

**Increase in ransomware**

CPR detects significant increase in first half of 2021, compared with same period in 2020.

**86%**

**Homeworking increases cyber-risk**

Carbon Black 2021 CISO survey reports detected attacks have increased due to homeworking.

# Service Offering

**Our managed services operate 24x7x365 from our UK-based Security Operations Centre (SOC) in Glasgow and our datacentre in Edinburgh. We have three service offerings depending on customer requirements, each offering greater levels of visibility and response.**

## Standard

Designed for organisations who need to meet compliance standards, with centralised log and event collection across critical points of their security and IT infrastructure. Log sources include security systems that generate security information across network and cloud infrastructures.

Data is processed, analysed and reported in line with our Service Level Agreement, offering improvements in Dwell Time, MTTD and MTTR metrics. Evidence and alerts are placed into context using threat intelligence and examined by our team of security analysts. Cases include evidence and clear guidance on remediation. Monthly reports contain rich findings, with analyst commentary, findings and recommendations.

## Premium

Building on the Standard service offering, Premium advances data collection to endpoint devices and critical servers, collecting user, file and application information. This adds significant detail to the information gathered, directly impacting the ability to detect, determine and identify threats in a much broader capacity.

User and Entity Behaviour Analysis (UEBA), artificial intelligence engines, contextualised threat intelligence, and advanced threat detection are applied, taking advantage of this richer data set.

Premium customers also benefit from access to a global incident response service, assisting with escalations from our SOC, should help be required with international investigations, take-down services or new and emerging threat actors and vectors.

## Premium+

The Premium+ service offers customers managed incident mitigation and remediation services. The SOC will respond with a range of actions to contain and mitigate identified threats within customer environments. This includes automated response services and manual responses, further reducing the MTTR.

The Premium+ service has an agreed set of corrective actions able to be performed. Customers moving to Premium+ will have previously been Premium customers, ensuring security events and operational activities required to resolve issues are fully understood before implementing responses.

# Service Matrix

| Features | Standard | Premium | Premium+ |
|---|---|---|---|
| Fully Managed UK Based SOC with DR | • | • | • |
| Cross-Platform Threat Detection | • | • | • |
| System Monitoring (Incl. Windows, Linux, HP-UX, AIX) | • | • | • |
| Cloud Infrastructure Monitoring | • | • | • |
| Log Data Collector | • | • | • |
| End to End Case Management | • | • | • |
| Statistical Analysis of Log Data | • | • | • |
| Integrated Threat Intelligence Ecosystem | • | • | • |
| Key User Monitoring | • | • | • |
| Quarterly Review | • | • | • |
| Monthly Reporting | • | • | • |
| Robust SLA | • | • | • |
| Customer Facing Dashboards | • | • | • |
| Host Monitoring† | | • | • |
| Systems Availability Monitoring† | | • | • |
| Process Monitor† | | • | • |
| File Integrity Monitoring† | | • | • |
| Windows Registry Monitoring† | | • | • |
| User Activity Monitor† | | • | • |
| Removable Media Detector† | | • | • |
| User and Entity Behaviour Analysis (UEBA)† | | • | • |
| Global Incident Response Integration | | • | • |
| Proactive Response and Incident Mitigation | | | • |
| Smart Response Automation | | | • |
| Dedicated Human Analyst Threat Hunting | | | • |
| Key Staff Monitoring and Threat Analysis†† | | | • |

† Additional Agent (Lite/Pro) license required or compatible EDR agent

†† Additional Cloud AI license required

# Features

## Fully Managed UK based SOC with DR

The Sapphire SOC and datacentre are entirely UK-based for all operational, processing and storage of data. Both our SOC and datacentre are built on a fully redundant and highly available architecture, ensuring zero data loss and continual service operation. Our Tier 4 datacentre  is compliant with ISO27001, Cyber Essentials+, PCI DSS, CSA Star, ISO14001 and ISO9001.

Our Analysts are certified with UK Government clearance at SC level, are UK police vetted (NPPV), and hold a range of Cyber Security, Analytics, and Threat Hunting certifications. In addition, Tier 1 Analysts have improvement programs for data and security analysis, certification and relevant vendor-based training.

## Cross-Platform Threat Detection
## System Monitoring
## Cloud Infrastructure Monitoring

Multiple log sources are combined to inform analysts undertaking threat inspection and hunting. Our service supports ingestion from over 350 pre-defined log sources, including on-premise, datacentre and cloud sources. Bespoke logs can also be parsed for inspection.

Directory related events such as user authentication, user creation, deletion and privilege escalation are monitored and reviewed, including Microsoft Active Directory. Analysts determine complex security events extracted from this correlated directory and cross-platform information.

> *"We've been using Sapphire's managed services for a year now. In that time, we have experienced a return on investment by saving time and freeing up our security team to focus their efforts on other areas of the business."*
>
> **- Steve Thornton, Infrastructure and Security, True Potential LLP**

## End to End Case Management

Detected threats are inspected for validity, checking their severity and impact. This process includes creating cases, gathering evidence from customer data, 3rd party threat intelligence feeds and analyst commentary. Cases can be escalated to senior analysts for further review if necessary. Case information is exported to customers where appropriate, providing recommendations and remediation actions.

[1] A Tier 4 datacentre is an enterprise class datacentre with redundant and dual-powered instances of servers, storage, network links and power cooling equipment.

### Statistical Analysis of Log Data
### Integrated Threat Intelligence Ecosystem

Our SIEM can ingest large volumes of data and analyse this for security event information. The automatic and manual analysis of security events provides a basis for our threat hunting and security investigations. In addition, statistical modelling enables faster detection of threat patterns across large data volumes. This process, enhanced by rich threat intelligence, provides context and is fully integrated into our SIEM technology platform.

### Key User Monitoring

Often specific individuals within a business will be identified by threat actors as targets for attack. These individuals may be public representatives of the organisation, have enhanced access to critical systems, or have the ability to make critical financial decisions. Enhanced auditing of key users can provide assurance whilst alerting our analysts to indicators of compromise at times of unusual or suspicious activity.

**25+**
Years of cyber security experience

**13+**
Managed Services Security Experts

**50+**
Cyber Security Consultants

### Quarterly Review
### Monthly Reporting
### Robust SLA

Our service is adaptable, changing the scope of devices, systems and users, based on customer requirements. Quarterly reviews ensure relevance and that value is maintained. In addition, we provide monthly reports detailing individual threats and management and board-level statistical analysis. Reports also include metrics such as Dwell Time, MTTD and MTTR, allowing measurement of continual improvement over the contract term.

The service is underpinned with a robust Service Level Agreement (SLA), detailing severity levels, response times and our engagement process. Sapphire can also provide technical consultancy, penetration testing, digital forensics and incident response based on client requirements.

### Customer Facing Dashboards

Clients can view security information via an authenticated HTTPS connection to a secure web environment. Dashboards illustrate current and historical security events and present this alongside regional, national and international data. Security trend information is included when available, giving deeper context to customer data.

Role-based access enables customers to access differing data views, segregating this into departmental based information such as Networks, Security and HR.

## Log Data Collector

The collection technology facilitates the aggregation of log data, security events and other machine data. Data Collectors can operate locally or remotely, are centrally maintained, simplifying deployment and management. Data Collectors can ingest logs from multiple sources and provide the interface to the Sapphire datacentre. All communication is fully encrypted and authenticated with compressed TLS, minimising bandwidth utilisation.

## Host Monitoring

**Systems Availability Monitoring**
**Process Monitor**
**File Integrity Monitoring**
**Windows Registry Monitoring**
**User Activity Monitor**
**Removable Media Detector**

Extending coverage to host-based monitoring provides further granular event detail on a user, application and data basis. This is achieved via light agents, delivering greater visibility into the activity occurring on endpoint devices and critical servers, including uptime and availability. The value of the service is further enhanced with this data, enabling deeper inspection and advanced analytics, thereby extending the visibility of security events.

File integrity monitoring is available, examining the creation, viewing, modification and deletion of files. Process and service activity monitoring enables detecting critical behaviour such as processes stopping or new or blacklisted processes starting. Registry monitoring detects additions, modifications, deletion and permission changes. Further features include network connection monitoring, user activity monitoring and data exfiltration activity via USB.

## User and Entity Behaviour Analysis (UEBA)

Focusing on user-based threats is a crucial method for combating a growing attack surface. UEBA can quickly and effectively detect, respond to, and mitigate known and unknown threats. Providing evidence-based starting points for investigation, it employs a combination of scenario analytics techniques, including statistical analysis, rate analysis, trend analysis, advanced correlation, and supervised and unsupervised machine learning (ML).

This variety of analytics enables enhanced detection of user-based threats, such as insider threat, account takeover, account privilege abuse, further reducing MTTD.

## Global Incident Response (IR) Integration

We provide a global incident response (IR) service to enhance our ability to support customers during critical attack or compromise. Where incidents occur beyond the area of scope for the customer (e.g. internationally), we can escalate to IR and assist clients with threat mitigation on a global basis. This can include root cause analysis, impact assessments, remediation planning and threat mitigation.

We integrate global threat intelligence data to our SOC, giving analysts an enriched view of existing, new and emerging threat actors and attack vectors on a minute by minute basis. Additionally, analysts benefit from understanding how threats detected within a local environment relate to global views.

At times of attack where assistance is needed, Sapphire can provide IR to Premium and Premium+ customers, which includes up to four hours of IR telephone consultancy per annum. If additional IR is required, customers can quickly purchase this on a case by case basis.

### Proactive Response and Incident Mitigation
### Smart Response Automation
### Dedicated Human Analyst Threat Hunting

The Sapphire SOC provides a range of mitigation responses to clients to ensure known and understood threats are quickly contained or eliminated via automated or manual response functions. Threats are validated continually, and we undertake a detailed investigation to ensure appropriate mitigation responses are applied. Cases may also include further recommendations on enhancements to customer security procedures and operations.

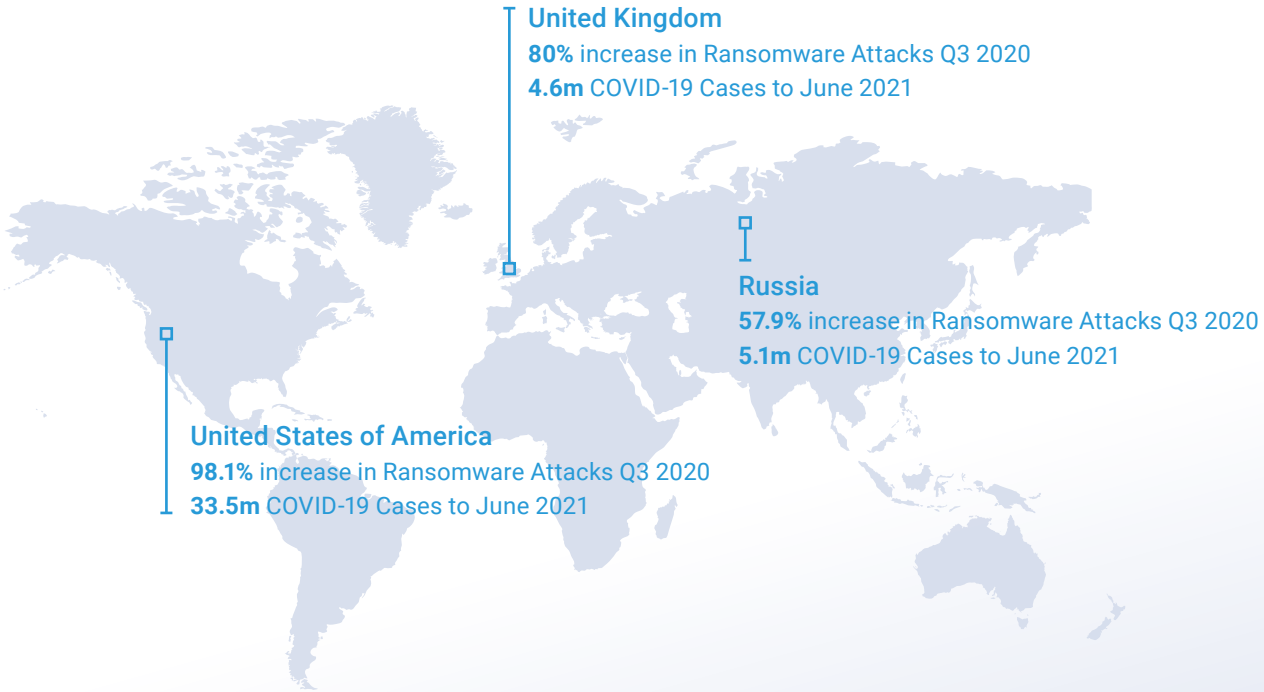
Threat hunting by senior analysts offers an additional perspective on the security of the overall customer environment. Our senior consultants have expertise in understanding a diverse range of threats, following trails of evidence to uncover potential and emerging areas of cyber-threat that may impact business.

### Key Staff Monitoring and Threat Analysis

When the activity of key staff requires deeper inspection, we can enable advanced intelligence to focus on these users to gain further insights. For example, we can detect insider threats, compromised accounts, administrator abuse and misuse, and other user-based threats. This is particularly suited for machine-assisted monitoring of high-risk users, such as IT, finance, and executive teams.

Our analysts have evidence-based starting points for threat hunting and data visualisations for machine-assisted qualification and investigation with these advanced analytics.

### 600% Global Increase in Cybercrime Due to COVID-19




Sources: Sapphire SOC, Check Point Software Technologies, Recorded Future, John Hopkins University.

# Get in touch

Sapphire has 25 years' experience mitigating cyber risk for some of the UK's largest organisations. For our clients, this means access to the best possible people, processes and technology, all continually augmented to match a highly fluid threat landscape.

Should you have any questions or need additional information then you can contact us via email info@sapphire.net or call 0845 5827001.

# Accreditations

We ensure our actions and activities are consistent and secure, taking environmental and employee responsibility seriously. Our company, SOC and data centre have achieved a range of accreditations, some of which are shown below.

bsi. ISO/IEC 27001 Information Security Management

bsi. ISO 14001 Environmental Management

CYBER ESSENTIALS PLUS

Crown Commercial Service *Supplier*

PCI DSS COMPLIANT

IASME® Consortium GOLD *Self-Certified* Company