Security Operations Centre (SOC)

Service Description for G-Cloud 15

zenzero

Document Purpose

This is document serves as a high-level description of our Security Operations Centre (SOC), and the supporting Managed Detection and Response Service.

The aim is to describe, in simple terms, the service, the deliverables of the service and the associated benefits. This is described in a non-technical and vendor agnostic way.

More detail can be provided when engaging with our team so that we can understand your specific requirements.

For more information:

- Please visit: IT Support, Security, Data and AI Solutions | Zenzero
- Phone: 0333 3209 900
- Email: Hello@Zenzero.co.uk

Scope of Service

Introduction

A Security Operations Centre (SOC) is a centralised command post where a team of cybersecurity professionals, including analysts, engineers, and managers, continuously monitors, detects, and responds to threats. Our SOC is the centralised hub for your security. The primary mission of our SOC is to limit damage by catching cyberattacks that bypass traditional defences.. We achieve this through a number of key methods including:

- **Continuous Monitoring (UK based 24/7/365):** Our UK based SOC monitors every corner of our clients' IT estates, including servers, endpoints (laptops/mobile), cloud environments, and networks, to detect suspicious activity in real time.
- **Threat Detection & Triage:** Using tools like SIEM (Security Information and Event Management), our SOC filters through millions of data logs to identify genuine threats while discarding "false positives."
- **Incident Response:** When an attack is confirmed, our SOC acts quickly and decisively. We isolate affected systems, revoke compromised user accounts, and remove malicious files to prevent the threat from spreading.
- **Vulnerability Management:** The team proactively identifies weaknesses (unpatched software or misconfigurations) and works with to fix them before attackers can exploit them.
- **Threat Intelligence:** Our SOC stays ahead by tracking global trends, new malware strains, and current attacker tactics to fortify the organisation's defences pre-emptively. This is build upon our large vendor databases of cyber information, and leading information from our Digital Forensics and Incident Response Team.
- **Compliance:** Our SOC can help you meet your compliance aims, including Cyber Essentials Plus, ISO27001, and more.

We support this with our managed Managed Detection and Response service, that provides a highly tailored solution based on industry leading technologies, coupled with relevant threat intelligence information and a 24/7 continuous monitoring service of all managed endpoints. This MDR service quickly detects threats that have bypassed existing defences and security controls and conducts rapid containment and remediation.

Customers' critical assets (workstations, laptops, servers, virtual machines, mobile devices etc.) are monitored in real-time and when a threat is observed, Zenzero will inform the customer (based on the severity of the threat) and take the necessary actions to isolate and perform remediation where necessary. Support is provided across the various product tiers covering features such as NGAV, Anti-Spam, Anti-Spyware, Device and Application Control, Host Web Filtering, EDR, to name a few. Zenzero's managed service builds on all the

product tier offerings, providing a comprehensive managed endpoint security service for the customer. Key products in our MDR service include the following products:

- **Fortinet FortiEDR:** FortiEDR provides robust protection both before and after an infection. We leverage its machine-learning NGAV engine for pre-infection prevention and its unique real-time, post-infection protection to defuse active threats even on an already compromised device.
- **Microsoft Defender for Endpoint P2:** Ideally suited to organisations heavily invested in the Microsoft ecosystem, we manage its full suite of capabilities, including risk-based vulnerability management and attack surface reduction rules. The native integration with Microsoft Entra ID and Defender for Cloud Apps enables an extended detection and response strategy.
- **SentinelOne:** Renowned for its AI-powered, signature-less detection capabilities we manage its autonomous agent, which can identify and stop both known and unknown threats, including sophisticated zero-day attacks, without relying on traditional signature updates.

Service Features

SOC Service Features

We operate a fully UK-based 24/7 SOC, that can offer your organisation support 24/7/365. This team is further supported by our Digital Forensics teams, located across the UK, Dubai and Australia, allowing us to operate a true follow-the-sun model for continuous expertise and rapid response if desired. On top of this team of experts, we can offer our clients a list of proprietary advantages to our SOC services.

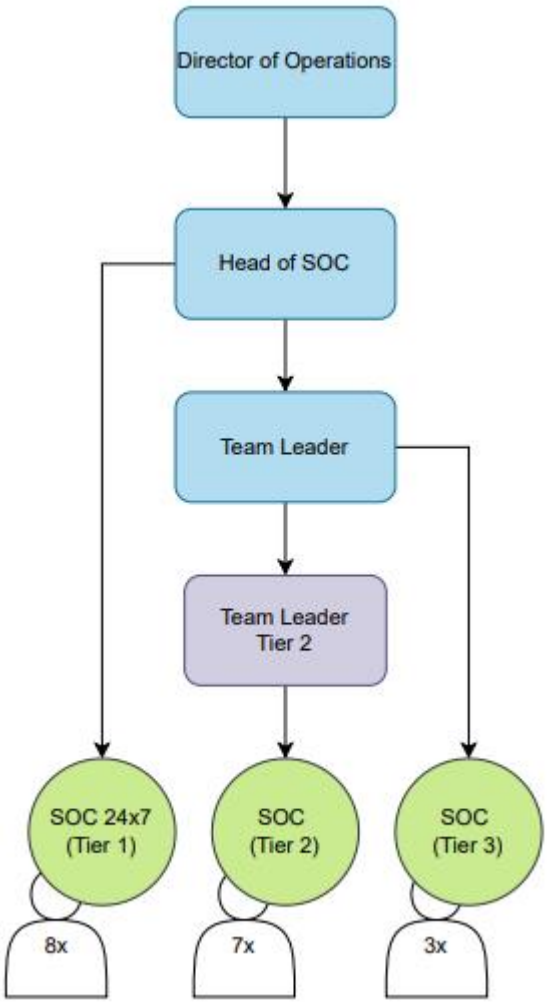
- **RealTime Risk Platform:** Our proprietary RealTime Risk Platform is widely used by customers as a dynamic cyber risk register, providing continuous, data driven visibility into their security posture and enabling clear prioritisation of remediation activities. It underpins our continuous improvement approach, supporting monthly advocate meetings where we jointly review emerging risks, progress against agreed actions, and mitigation timelines. This ensures all parties remain aligned, accountable, and focused on reducing risk in a measurable and collaborative way.
- **Zensec XDR Platform:** We deliver our own enhanced XDR solution, offering a broader and more robust suite of capabilities than standard Microsoft Defender XDR. This includes deeper correlation with known IP databases, advanced detection logic, and greater contextual visibility across the environment.
- **Embedded DFIR Expertise:** Our Digital Forensics and Incident Response (DFIR) team directly informs and strengthens our security operations. We continuously integrate DFIR findings, threat intelligence, and behavioural insights into our monitoring, detection, and response workflows

All of our SOC clients are supported by a security advocate. The Zensec Security Advocate is designated as your service owner and risk manager. They will ensure that the items alerts and recommendations presented within the Real-Time Risk Portal are clearly explained, correctly prioritised and translated into tangible improvements in your security posture as part of a proactive risk management agenda.

The Zensec Security Advocate is a multi-faceted role, combining technical expertise with strategic business alignment. Their responsibilities include:

- **Strategic Advisor:** The Advocate works closely with your team to develop and refine your long-term security strategy. They help you interpret the trends in your Zensec Risk Score, identify systemic weaknesses, and build a prioritised roadmap for remediation and improvement.
- **Threat Briefings:** The Security Advocate provides proactive, tailored threat intelligence briefings, identifying the emerging threats, vulnerabilities, and attacker tactics that are most relevant to your industry and technology stack.
- **Incident Escalation Point:** For critical security incidents, your Advocate is your central point of contact. They assist in triage of the incident, assessing its potential business impact, and act as the seamless liaison to our 24/7 Cyber Security Incident Response Team (CSIRT) for digital forensics and recovery efforts if required.

The basic structure of our SOC is included below, so that you can understand how resources are distributed, and how escalation is conducted.



MDR Service Features

Our SOC will be supported at all stages with our MDR Response Service, that will feed information into the SOC as a strategic hub for our cyber security, and provide comprehensive monitoring and incident response capabilities. Leveraging advanced threat detection technologies and expert security analysts, we monitor user endpoints 24/7 to quickly identify and eliminate potential threats. Our service improves overall security posture, mitigates risks, and minimises the impact of cyberattacks. This means in practice that we will undertake:

- Management of the Endpoint platform and endpoint clients/agents including setup, configuration, and ongoing maintenance and upgrades.
- Monitoring and triage of alerts, filtration and elimination of false positives and notification
- of alerts of interest to the customer, under 24x7 SLA. Notified alerts will be enriched with environmental context, criticality assignment, and remediation recommendations.
- Weekly and/or monthly alert summary reporting.
- Remediation of threats discovered, ensuring all endpoints are safe to use with minimal interaction from the customer.
- Adhering to strict response and resolution SLAs ensuring the customer's endpoints are and remain protected at all times.
- Technical support for NGAV, Anti-Spam, Anti-Spyware, Device and Application control features.

Threat Hunting

Our MDR service includes Threat Hunting as a standard feature. This ensures that automated threat detection via the EDR and SIEM mechanisms outlined is augmented with proactive, human-led threat hunting to unearth threats that may have managed to bypass all existing threat prevention and detection mechanisms. We conduct Threat Hunting at three different levels.

- We have constant proactive threat hunting, that is completed by our SOC, that seeks threats within your estate. This is an iterative process, with knowledge built over time to establish a baseline, and catch any deviations from this.
- In the case of an alert, we conduct reactive Threat Hunting. This will see our tier three SOC staff review the estate, and seek any threats, using intelligence from the triggered alert to drive their hunt
- In the case of a suspected breach, we will conduct a Threat Hunt focused on that breach, and seeking out information regarding it. This occurs in the case of a suspected breach; if a breach is confirmed then we will engage our Incident Response Plan.

Incident Management

In the case of an incident, we have strong, incident management processes built into our MDR service. This sees us take an incident through a process of triage, investigation, response and reporting. This process in underpinned by our SOC team, our SOAR and SIEM products, that combine alerts into a single case for ease of handling during the incident lifecycle

- **Triage:** Alerts are checked and triaged, The principle is to look at alerts and eliminate false positives by analysing traffic surrounding each alert
- **Incident Analysis:** When a True Positive is confirmed, our SOC team will focus on analysing the incident, confirming that a response is necessary, and then planning response to achieve our SLAs.
- **Incident Response:** Zenzero will respond to analysed incidents to contain and mitigate the threat as soon as possible, including out of hours if necessary.

Alongside this process, we will escalate to the customer in the case of an incident. We will ensure to include all relevant details, and will track our actions within our SOAR platform to ensue that all case details, actions and case activity are tracked.

The end result of the combination of our SOC, a dedicated Security Advocate, and our MDR solutions is a stronger, more resilient cyber security service that you can rely on. Threat Hunting, strong processes for incident resolution and a strong interlink between our MDR service, SOC staff, and our SIEM allows for a joined up approach that tackles cyber security threats proactively rather than just reactively, constantly seeking and eliminating weaknesses and threats to your security set up.

Service Level Agreements

Our standard agreed service levels are included in the table below:

Incident Priority	Business Impact	Target Response	Business Hours
Critical – P1	Very high impact in all business areas, extreme impact on users and disruption is excessive. Possibility of a security breach. Major incident. Possible financial implications, loss of company or user data at risk. Possible ICO implications or Pii / Pfi data loss possible	1 Hour	24/7

Incident Priority	Business Impact	Target Response	Business Hours
Standard – P2	Medium impact, security alarm has been triggered and is not a false positive. There is a medium risk to the business.	4 Hours	Working Day 9-5
Low – P3	The risk to the business from the security alarm is low or minimal.	Next Business Day	Working Day 9-5

Next steps

Speak with a member of our team to build a SOC service that works for you using the phone number and email address above. Or you can use our website to book a consultation.

Pricing

Please find below our pricing for our SOC service, and our MDR service. Our SOC service is charged on a basis of per asset per month. Our MDR service is charged out per user per month.

SOC Service	Cost		
Standing Charge	£250		
SIEM (Per Computer Asset)*	£39.50		
SIEM (Per Network Asset)*	£275.30		
MDR Service	**0 -250**	**250 -1000**	**1000+**
MDR (Sentinel)*	£7.90	£7.43	£6.98
MDR (FortiEDR or Sentinel One)*	£10.10	£9.49	£8.92