SOC365

Cyber Defence with Teeth

HedgehogSecurity

Delivering Peace of Mind

Defend your data.

Everywhere

Full-spectrum security that keeps your data safe across all touchpoints no matter where you operate.

Do you need to:

- Sleep well?
- Defeat cyber-attacks?
- Prove effective defences?
- Monitor systems 24 hours a day?
- Build and maintain trust in your business?.

SOC365 Secures your Operation

Organisations, industries, and critical national infrastructure are becoming increasingly interconnected - with many processes now relying on digital technologies and real-time data exchange.

This digital transformation has coincided with a rise in sophisticated cyber-attacks - and whether the intention is disruption, the theft of strategic data or operational damage; the severe economic and societal repercussions have never been greater.

To mitigate and manage these risks, the implementation of effective cyber defence is necessary.

That is what we do. Cyber Defence.

Why SOC365?

Faster detection and quicker response.

AI supporting humans for instant Cyber Defence.

Staffed 24 hours a day, 365 days a year

Comprehensive support from local and regional specialists

Unparalleled SOC proficiency, with long term experience in safety, security and working with sensitive data

Proven security monitoring expertise for critical assets in IT and OT environments

AI supported since 2018 with our own internal AI defender

Attack Disruption and deception networks as part of the service

Ensuring sustainable security for a competitive advantage

Detect Defend Disrupt

We Detect

We detect through:

1. EDR/XDR Agents for Windows, Linux, Mac, HPUX, Oracle, Solaris
2. Virtual and Physical Appliances for Syslog, raw IP
3. Cloud based syslog collectors

And these are monitored 24x7x365 by our defenders and our first line AI system. We also monitor existing systems such as Microsoft Sentinal, CrowdStrike and others.

We Defend

We use automation and defenders' skills to defend systems from attacks, letting you know the state of defence in real time. From automatic isolation of systems to network communication interruption and process elimination, we work tirelessly to defend systems and networks.

We Disrupt

When an attack cannot be defended in less than 20 minutes, we disrupt the attackers with takedown notices, abuse reports, tarpits and honeypots. To the limits of law, we will fight back, removing the attacker's ability to communicate.

SOC365

Hedgehog Managed Security Services

Whether it is simply a managed SIEM or a fully managed SOC service, we have the tools and solutions to assist.

What is Included	Managed SIEM	Managed SOC
Fully hosted remotely delivered cloud SIEM	✓	✓
Cloud SIEM tuning and maintenance 24/7	✓	✓
AI monitoring service	✗	✓
24/7 Level 2/3 SOC Analysts	✗	✓
24/7 Threat Hunting	✗	✓
24/7 Threat Containment	✗	✓
24/7 Incident Response	✗	✓
Unlimited remote incident support	✗	✓
Dedicated customer portal	✓	✓
XDR licenses	✓	✓
Vulnerability Scanning	✗	✓
Threat Intelligence	✗	✓
Cyber Security Maturity Assessment	✗	✓
Security reviews of 3rd party security vendors	✗	✓

SOC365

Attacks Managed

Hedgehog Security's SOCs operate 24/7, 365 days a year; and are run by a team of cyber experts with extensive experience in both fully outsourced and hybrid service models.

Our teams follow a comprehensive "continuous maturity improvement" process that helps to keep cyber resilience up-to-date and in line with the cyber threats of tomorrow.

We deliver protective security monitoring for IT, OT and maritime platforms to the government, defence, aeronautics, space, energy, transportation, shipping, manufacturing, banking and finance industries.

From design to service

We can either design, build and run a new SOC tailored to your infrastructure, or alternatively optimise your existing SOC to enhance your security posture.

Lifetime service delivery

We work with you in partnership to constantly update and optimise the SOC service to meet your specific needs and advancing threats.

Cyber-on-Demand

For security needs that evolve over time, we offer a flexible framework contract that delivers cyber security services as and when they are needed.

Incident response recovery

In the event of a serious attack, we can provide CSIRT (Computer Security Incident Response Team) experts to undertake forensic analysis and support remediation activities.

Advanced custom rules & detections

We quickly address our customer's risks with immediate implementation of the best use cases from the continuously-updated library of custom rules and detections.

Advanced threat hunting

We apply the very latest global threat intelligence from a range of open and closed sources, to detect the most advanced attacks - including those that target your specific environment.

Consulting & Professional Services

We can help you to build the basis for a SOC project or for continuous improvements to your cyber resilience. Our experts have a proven track record of delivering security within both the public and private sectors.

Full environment coverage

Our SOC services can cover your entire enterprise, from IT to OT and cloud services, providing a complete overview of your security posture. Services can be provided from either our premises or your own site.

Protecting Assets & Networks

Integration of Hedgehog and Partner Security products like Network, Data and Endpoint Security from Wazuh and Sentinel from Microsoft.

We are passionate about Cyber Defence

SOC365 by Hedgehog Security brings fanatical cyber defence to businesses and organisations of all sizes.

We work tirelessly to be more Hedgehog, to keep the pricks on the outside.

To find out how we can help you, contact one of our defenders today.

Hedgehog Security Ltd.
International House
Mosley Street, Manchester

https://hedgehogsecurity.co.uk
+44 3333 444 256

SOC365