Moon MDR

Dedicated defences that protect your biggest vulnerabilities

Technology advises, humans decide

Part of our Security Operations Centre (SOC) solutions, our specialist protections are a dedicated service that secures against specific risks to your business universe. Using a powerful combination of human and machine, our highly-skilled and experienced team harness information gathered by state-of-the-art tools, and enhance it with expert intelligence, analysis and action. This powerful blend enables us to deliver optimum results – identifying and solving security challenges with speed and efficiency.

With our Moon protections you can realise enterprise-grade defences that secure your business round the clock for a competitive price point that's a fraction of the cost of recruiting your own resource.

Moon MDR

1 protection

Included in this SOC

- Managed Detention and Response (MDR)
- Threat Intelligence (GTIN)
- I3 – Incident Management Portal

Experts on watch

Our managed services provide peace of mind, with a dedicated SOC team on watch 24 hours a day, 365 days a year. A handpicked selection of security analysts, threat intelligence specialists and cyber security engineers combine their expertise to interpret technology insights and action defensive measures on your behalf.

Is Moon MDR the right SOC for me?

Tailored to your specific needs, our Moon MDR service reinforces your existing estate and extends the value of your security investments to deliver robust protection. Our leading defensive SOC service is designed to strengthen your defences in three important ways:

- **Proactive defence** – Prevention is better than cure. Our cyber threat intelligence system provides advanced warning of cyber threats targeting your organisation or sector. Coupled with MDR technology, we stay one step ahead of attacks by hardening your organisational defences.
- **Reactive defence: automated** – The first wall of defence. Industry-leading security tools protect your users and systems in real-time by automatically blocking network and malware threats, and preventing data theft and exfiltration attempts.
- **Reactive defence: incident response playbooks** – Enhanced threat response. Going one step further than automated tools alone, our analysts interpret insight from threat hunting technology to seek out indicators of compromise in your networks and trigger best-practice incident response processes.

In depth: Moon MDR benefits

- Rapid remote deployment of monitoring and protection software through cloud management.
- Key Risk Indicator and security maturity improvements delivered within 4 weeks of SOC deployment.
- Protect key data, intellectual property and client data from theft and accidental leakage.
- Harden networks and systems to common network intrusion attacks and malware.
- Detect targeted and sophisticated network attacks.
- Help protect against zero-day malware.
- Reduce employee overhead and improve speed of response through automated defence and remediation.
- Flexibility to evolve your service using our ‘Roll Out Roll In’ SOC protections.

In depth: Moon MDR protections

Technology

Technology plays a vital role in protecting your IT. Your Moon SOC service is underpinned by state-of-the-art security:

- **MDR software agents and cloud management portal**
  - Protects against advanced malware and network threats through risk-based alerting.
  - Reveals threat actors who already have a foothold on your network.
  - Detects zero-day risks and advanced persistent threats.
- **I3 Security Incident Management Portal**
  - Tracks security alerts and incidents through a centralised portal.
  - Contains security run books tailored to your needs.
  - Shows you the ‘metrics that matter’ through live security posture and risk indicator dashboards.
- **Global Threat Intelligence Network (GTIN)**
  - Uses a database of current threats, campaigns, botnets and malicious websites to seek out indicators of compromise.

People

Humans are critical to interpreting and acting on technology's advice, which is why they're a huge part of what we do for you. Your Moon SOC team includes:

- **Security Analyst:** Your eyes and ears. Monitors, analyses and investigates your IT estate 24x7.
- **Security Engineer:** Ensures your systems seamlessly integrate with ours so everything works as it should.
- **Security Assurance Consultant:** Answers the difficult questions and provides valuable guidance that supports your decisions.
- **Security Delivery Manager:** Oversees every element of your service from internal response process to coordination of different teams.
- **Threat Intelligence Specialist:** Looks beyond your perimeter to seek and stop cyber threats before they cause harm.

Process

We dot the I's and cross the T's by ensuring best-practice processes are meticulously followed during the deployment of our managed security services:

- **On-going tuning of alert and defensive rule sets:**
  Ensures your security stays matched to your organisation as it evolves.
- **Early warning threat intelligence:**
  Shows you how to best-protect your business before an attack strikes.
- **Active threat hunting:**
  Detects sophisticated attackers and advanced persistent threats.
- **Monthly Key Risk Indicator reporting:**
  Summarises the risks we've uncovered and prevented, benchmarked against key performance indicators.
- **Incident orchestration:**
  Resolves and remediates incidents through collaboration with your in-house teams.

Protection overview: MDR

What is it?

MDR (Managed Detection and Response) delivers real-time detection and prevention of advanced network threats and malware. Using a combination of machine learning, signature detection and threat intelligence, MDR will identify anomalous activity on endpoint systems and will automatically block and quarantine high risk events. Low risk events are also flagged to the SOC team for further investigation.

Why do I need it?

MDR goes beyond even the best of anti-virus products. Rather than defending only against known threats, MDR allows a SOC team to actively hunt for zero-day cyber attacks and Advanced Persistent Threats. MDR is the ideal technology for organisations who are concerned about advanced threats and malware - it ensures that attackers can't gain a foothold on your networks and keeps your business off hackers' radar.

MDR management

- **Management of alert and defensive rules** – We continuously tune alert rulesets in response to your business needs and the threat landscape. Automated incident response playbooks mean defensive action is triggered as soon as threats are detected.
- **Active threat hunting** – Ongoing threat hunting combines machine intelligence with skilled human analysis and decision-making.
- **Advanced incident analytics** - Includes malware sandboxing and analysis of zero-day malware threats.
- **Cyber threat intelligence** - We monitor the internet and hacker forums for indicators of compromise, leaked data, targeted campaigns and fraudulent web domains – so we're always a step ahead.

Additional MDR service features

- **Lightweight MDR agent** - Protects servers and cloud workloads, and can be rapidly deployed to desktops and laptops.
- **Control endpoint connectivity** – including access Bluetooth and USB devices
- **Defensive play books** – Can either be automated or support a 1-click response.
- **Threat Hunter toolkit** - Supports MITRE ATT&CK tactics, techniques, and procedures.

SOC management

- **Alert use-cases** – Starting with a baseline security alerting ruleset, we evolve this over time to implement new alerts as required.
- **Fully managed service** – Our SOC analysts monitor your security alerts 24/7 and can supply ad-hoc reporting upon request.
- **Evolving service** – We continually adapt our monitoring and alerting methods to match the ever-changing threat landscape. Our SOC team are up-to-date with the latest threat trends and keep watch for new techniques, tactics and procedures being deployed by cyber attackers.
- **Scalable Capacity** – We can flex your SOC service capacity to match your security needs.

Reporting

- **Key Risk Indicator reports (KRI)** – Weekly or monthly KRI reports provide a full picture of your MDR service. These highlight the most important risks, whilst providing insight into recent threats and the steps taken to defend against them.
- **Key Performance Indicators (KPI)** – We benchmark our performance by tracking incident response and resolution times.
- **I3 access** – All customers have access to our I3 incident management portal, granting real-time visibility into how our analysts are investigating and responding to security incidents.
- **Flexible alert notifications** – When our analysts identify a threat, they'll notify you via your chosen method – through email, in the I3 portal, by telephone or through integrations with incident management platforms.

Our customer pledge

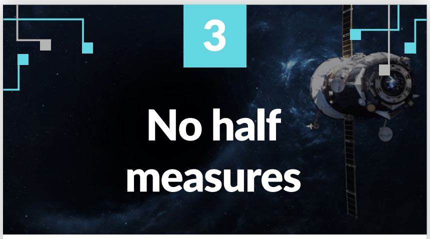
We want you to be completely satisfied with your SOC service – our promise to you:

1 1-month pilot free of charge

Put us to the test and let us run your 24x7 Security Operations for free for the first month. You can benchmark our performance against pre-agreed success criteria – and if you're not convinced after the pilot, it won't cost you a penny.

2 Lowest price guarantee

Our mission is to make high-quality, tailored managed security services affordable to the mid-market – and we stand by our word. If you find another provider who can offer a like-for-like SOC service for lower cost, we will refund the difference.



3 No half measures

When you take part in our pilot you can expect the full Zepko service, not a trimmed down version. We'll run a full 24x7 SOC operation, providing access to our specialist SOC team, process models and procedures, at the same level as our existing customers.

Take the next step

Found the right protection for you? Get in touch with us to start your 1-month pilot or for more information about our services.

+44 (0) 845 074 0790 | **info@zepko.com**

Get in touch

:zepko