Moon VM

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 VM

1 protection

Included in this SOC

- Vulnerability Management (VM)
- 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 VM the right SOC for me?

Tailored to your specific needs, our Moon Vulnerability Management service reinforces your existing estate and extends the value of your security investments to deliver robust protection. Our leading defensive technology SOC service is configured 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 vulnerability management, we stay one step ahead of attacks by hardening your organisational defences.

- **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 VM benefits

- Rapid remote deployment of monitoring and protection software through cloud management.
- Key Risk Indicator and security maturity improvements delivered within 2 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.
- Flexibility to evolve your service using our 'Roll Out Roll In' SOC protections.

In depth: Moon VM protections

Technology

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

- **Vulnerability Scanners virtual appliance**
  - Flags vulnerabilities in your networks, cloud systems and internet facing perimeter, including unknown systems and shadow IT.
  - OWASP Web Application Scanning and Compliance Scanning (includes PCI DSS, SoX, NIST, CIS and many more).
  - Logs emerging threats via a threat intelligence feed.
- **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

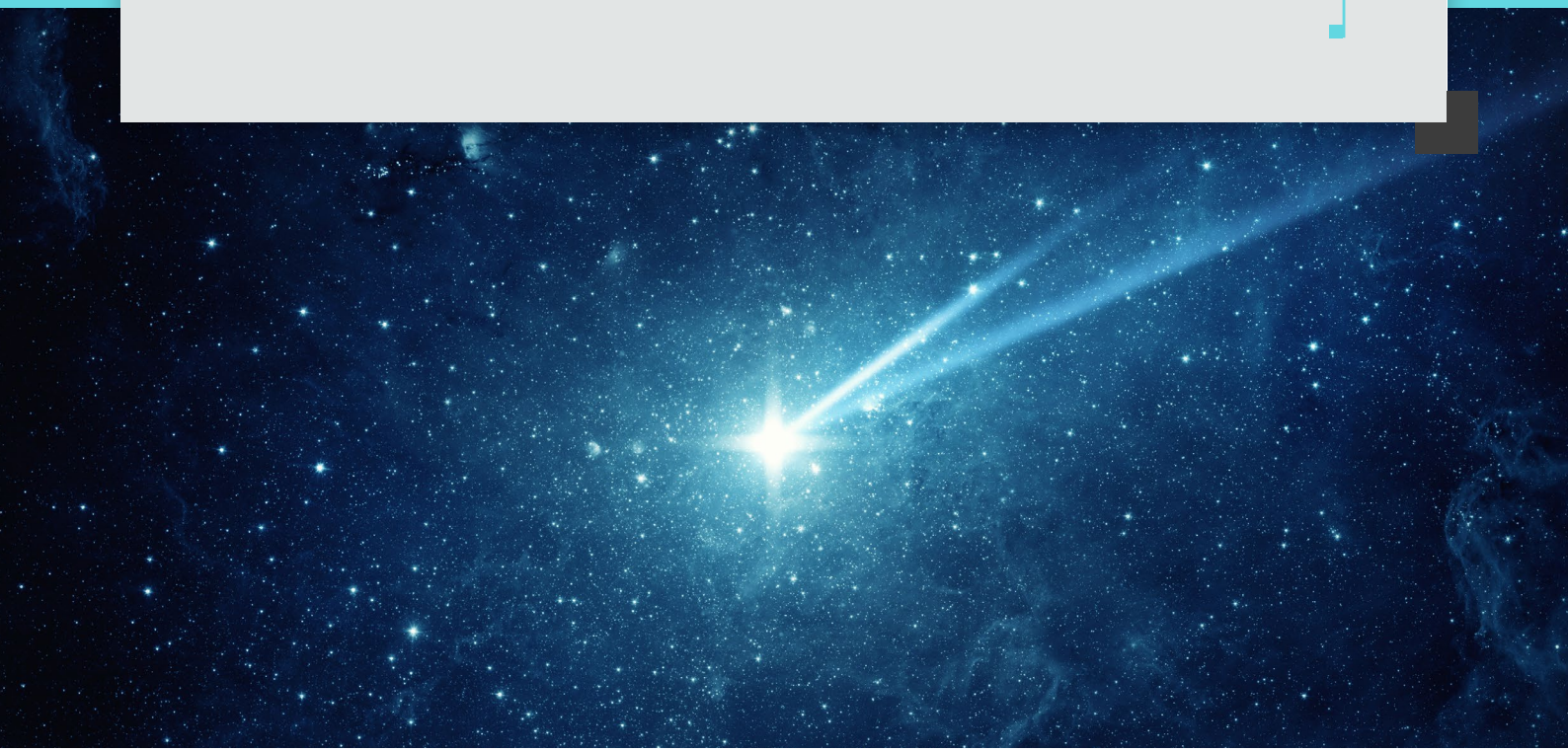
Humans are critical to interpreting and acting on technology's advice, which is why they're a huge part of what we do for you. Your Moon SOC team includes:

- **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.
- **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: VM

What is it?

Vulnerability Management (VM) enables your organisation to identify security weaknesses before they become a problem. Our always-on virtual scanners monitor your networks, cloud systems and internet facing perimeter to identify potential risks, flagging them to our SOC team who can then take further action.

Why do I need it?

VM helps you take control of your IT and cloud networks, bolstering them to the highest industry standards. Network and host discovery identify any systems connected to your network that you might not be aware of, such as legacy systems or shadow IT. You can then take control of these assets or decide to decommission them – lowering your overall risk while improving your level of security maturity.

Many cyber-attacks publicised in the media have been due to unpatched or poorly configured systems. VM is a key baseline security measure which increases your organisation's resilience to cyber-attacks.

VM management

- **Policy management** – We customise and maintain your vulnerability scan policies to meet your organisation's needs. Our experienced team set up automated scanning schedules, reducing operational overhead on your business systems and networks.
- **Fully managed service** – Our SOC analysts provide scanning reports on agreed schedules and will also trigger ad-hoc scans as requested, or if our threat intelligence uncovers a new critical vulnerability on your networks.

Additional VM service features

- **Compliance scanning** – Includes OWASP Web Application Scanning and Compliance Scanning (includes PCI DSS, SoX, NIST, CIS and many more).
- **Threat Intelligence feed** – Discloses new vulnerabilities and emerging threats.
- **Optional vulnerability scanning agents** – Provides real-time scanning and continuous host-based scanning, useful for vulnerability management of mobile endpoints.

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.

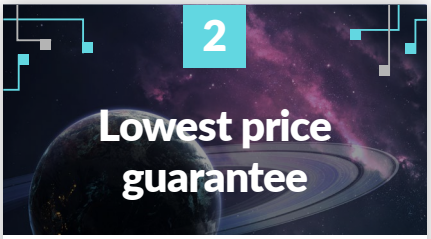
Reporting

- **Key Risk Indicator reports (KRI)** – Weekly or monthly KRI reports provide a full picture of your VM 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 other incident management platforms.

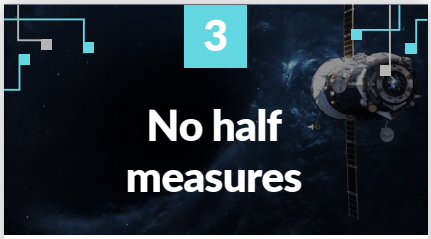
Our customer pledge

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

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.



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.



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