

## WHAT IS A MANAGED SOC?

As cyber adversaries continue to use more sophisticated forms of attack, protecting an organisation's digital infrastructure is becoming increasingly difficult to manage. Organisations are looking for more effective security solutions, such as managed security operations centres (SOC), to protect their operations.

*But what is a SOC, how does a managed SOC work and what are the benefits?*

A SOC brings together security information and event management (SIEM) technology with a team of security experts that oversee and manage processes to continually monitor a network, actively search for threats and respond to any incidents.

However, investing in an in-house SOC can be costly, both in terms of the associated setup and maintenance costs, as well as the workforce and expertise required to manage it effectively.

It's no surprise, then, that more and more businesses are turning to managed security service providers (MSSP) that offer SOC-as-a-Service to handle all aspects of managing the security operations of their networks.

## HOW DOES IT WORK?

A SOC comprises a security team of analysts and engineers who are trained to identify, analyse and respond to cyber security threats, while continually working to prevent attacks. They do so by using a combination of technology and robust processes to monitor network vulnerabilities in real time. Security experts at the MSSP work as an extension of your security and/or IT team providing 24/7 monitoring of your security position and keep abreast of new and emerging threats.

A SOC will act against attacks by implementing the following processes:

- Identify areas of weaknesses by simulating real-world attacks
- Detect any threats or attacks as they occur in real time
- Protect systems from threats through 24/7 monitoring
- Respond to attacks to minimise duration, impact and cost of a breach
- Recover systems, restore data and restart network.

## THE BENEFITS OF A MANAGED SOC

Opting for a managed SOC takes the stress out of having to manage your cyber security in-house. There are numerous other benefits of implementing a managed SOC, including:

1. **Quicker deployment:** Utilising an MSSP's investment in the latest SIEM technology, processes and security experts allows you to deploy a SOC within your organisation much more quickly than building it inhouse.
2. **Reduce costs:** A managed service is typically offered at a monthly cost that is predictable and much more affordable. Therefore, there are no capital costs when investing in a managed SOC and the overall costs are much lower than managing your network security in-house.
3. **Meet compliance requirements:** Use a managed SOC to produce daily auditable reports and threat analysis outlines, required for frameworks and regulated industries, including PCI DSS and ISO 27001.
4. **Round-the-clock security:** With a managed SOC, a dedicated team of experts can run the SOC at its most effective 24/7, as well as offering security expertise and incident response to detected security breaches.
5. **Access to security experts:** You can avoid having to deploy resource away from servicing the business or hiring security analysts with a managed SOC and gain immediate access to experts with specialist skills to manage your security effectively.