How does a SOC protect your business?

Cyber attacks continue to grow in both frequency and sophistication, rising from 2.39 million to over 8.58 million incidents against UK businesses in 2024, as malicious actors seek to exploit any weakness they can find in a business's IT infrastructure. A Security Operations Centre (SOC/CSOC), manned by a team of experienced cyber security professionals, can act as a protective shield, hunting, detecting, and preventing security breaches before they cause lasting harm.

Statistics indicate that it takes the average business 21 days immediately to recover from a cyber attack, with lasting effects beyond this that can see repercussions for more than a year. Additionally, it is estimated that for more sophisticated targeted attacks that attackers could have access to up to 9 months before being detected. This not only highlights how attackers can linger within systems undetected before launching an attack, but also the importance for businesses of utilising a SOC to close this detection gap, not only delivering continuous security monitoring and swift incident response, but actively hunting out threats before they can cause harm to your business.

Why is a SOC valuable to your business?

Full Visibility of IT Assets

A key component of a SOC is to provide your business with an in-depth understanding of everything within it's digital environment. Every network device, application, operating system, and data repository is mapped, tracked and monitored. When a business owner has full clarity about the assets in use, lifting the vail on Shadow IT, decisions about security investments become more straightforward and more cost-effective, whilst reducing the possibility of vulnerabilities arising from overlooked, legacy, or unauthorised software/devices. This high-level visibility helps security analysts spot suspicious changes that may indicate an attempted intrusion, allowing them to react promptly and protect a business's most valuable resources.

Continuous Log Management

Our highly skilled SOC team rely on comprehensive logging to capture all security-relevant data from various sources, such as firewalls, servers, endpoints, and SaaS cloud platforms. These logs can be correlated in real time using specialist platforms like Security Information and Event Management (SIEM) systems and SaaS Alerts. Through advanced correlation rules, paired with artificial intelligence and machine learning algorithms, our SOC is able to easily and quickly identify abnormal behaviour across your network, or signs of an attack at an early stage. Additionally, maintaining this robust audit trail offers peace of mind to business owners, who can trust that every noteworthy system event is recorded in case forensic analysis is required. Effective log management reduces the risk of missing critical warning signs and helps maintain consistent vigilance over your digital estate.

Rapid Detection and Response

A SOC has the dual responsibility of both detecting potential intrusions and quickly responding to them to prevent large-scale damage. Our highly trained analysts use threat intelligence from numerous sources to determine whether flagged behaviour is benign or indicative of malicious activity. Should a confirmed threat by identified, our SOC team follows well-honed and trained procedures to contain and eradicate the threat, all while minimising disruptions to normal business operations, and often without any end user awareness until the incident response report. Prompt detection and action shrinks “dwell time,” meaning there is far less chance for attackers to steal sensitive data, seize control of key systems, or launch ransomware attacks.

Proactive Vulnerability Management

Our trained and highly skilled cyber security professionals apply continuous assessment methods to our clients to ensure that every device, system and software is regularly tested for potential weaknesses. Whether this be through continuous vulnerability scans or more in-depth penetration testing. By identifying vulnerabilities before they are exploited, it allows us to fix gaps early. It is *far* cheaper and less disruptive to fix an vulnerability as it is detected, rather than dealing with the aftermath of a breach.

Up-to-Date Threat Awareness

Cyber threats constantly evolving, with an estimated 560,000 new threats discovered globally every day, our SOC allows businesses benefit from having a trained and specialised team focused on staying current with the latest cyber security threats. Using threat intelligence feeds, community resources, and real-time data gathered from security devices, and much more, our SOC is able to monitor and constantly refine our defence strategies to counter emerging attacks 24/7/365 so that you don’t have to. This includes, malware and ransomware, phishing, targeted attacks and much more. By maintaining an awareness of up to date attacker tactics our SOC can quickly neutralise, or at least mitigate, their impact.

Compliance and Regulatory Confidence

Our SOC can also assist businesses to meet stringent regulatory requirements, such as Cyber Essentials Plus and ISO27001, by maintaining detailed logs, intrusion detection reports, and incident response timelines for audit and investigation. Many sectors, such as finance, healthcare, government, and businesses who have government contracts, must follow data protection laws and guidelines for both compliance and insurance purposes. These can be highly complex and failure to comply may lead to hefty fines and/or legal action. Our SOC incorporates these regulatory obligations into day-to-day processes and ongoing cyber defence strategies, making it simpler for a business owner to demonstrate compliance if a regulator or auditor requests evidence. Beyond avoiding penalties, there is an added trust factor with complying with these nationally, and internationally recognised standards. Clients, partners, and the public tend to have more confidence in a business that can show it has robust security processes in place, including continuous monitoring, a dedicated team and regular external penetration testing and audits from a certified team.

Round the Clock Security

Cyber criminals know when your business is most vulnerable to attack, often launching offensives outside of standard working hours, or through public holidays where attacks increase by an alarming 30%, aiming to exploit times when staff oversight is minimal. Our managed SOC ensures 24/7/365 coverage, which can be especially useful for businesses lacking the internal capacity to staff their own trained cyber security team at night or on weekends. This constant vigilance reassures business owners that someone is always watching for signs of cyber threats, whether that be mid-morning on a week day, or 3am Christmas morning (yes, this happened to someone who was not a client at the time but we were able to help) removing the need to worry about potential breaches going unseen for lengthy periods. Our round-the-clock SOC team defends your business's data and reputation by preventing threats even when you are not there.

How can TwentyFour secure your business from evolving threats?

Our SOC delivers a tailored and structured approach to defending against the latest cyber threats, helping business owners maintain safe and resilient operations 24/7/365. Whilst our services are tailored to your specific business, the goals remain the same: detect breaches as early as possible, respond effectively to prevent or minimise the threat, and constantly adapt as new threats emerge. A SOC is pivotal to that strategy, ensuring teams and technologies work cohesively to protect the core interests of the business and its stakeholders.