White paper

Building today's SOC

Balancing risk, resources and reality

verizon business

In an era of relentless cyber threats, a security operations centre (SOC) serves as an organisation's cybersecurity command centre—monitoring alerts, detecting incidents and directing threat responses in real time.

Developing the right cybersecurity capability is about balancing risk tolerance with available resources and expertise. Before choosing an approach—whether in-house, hybrid or a fully outsourced model—it's necessary for organisations to assess their critical assets, risk tolerance, compliance requirements and budget.

An in-house SOC offers complete control over operations and security measures. It also requires a significant upfront investment, along with ongoing costs for staffing and technology to maintain and enhance protection and risk mitigation.

A managed SOC service provides on-demand access to expert analysts, who have global threat perspective and 24/7 "eyes on glass." This gives organisations access to existing capability, expertise, technology and scalability—without the complexity, time and cost of building an internal team.

Many organisations choose a hybrid approach, freeing internal resources for higher-order tasks and decision-making, while a partner takes on the core day-to-day operational tasks.

Building an in-house SOC requires technology, people and processes

Technology is a critical pillar of any cyber defence strategy. Security tools such as security information and event management (SIEM), security orchestration, automation and response (SOAR) and endpoint detection and response (EDR) work together to identify, investigate and mitigate threats.

With cloud services now pervasive across most technology ecosystems, SOCs must monitor misconfigurations, application programmable interface (API) vulnerabilities and unauthorised access across hybrid and dynamic environments. A zero trust approach to monitoring activities means verifying every user, device and application to mitigate the risk of unauthorised access to sensitive systems and data. A modern SOC's objective is real-time detection of anomalies and automated threat containment before breaches escalate.

Increasingly, attackers are using artificial intelligence (AI) to automate attacks, accelerating vulnerability discovery, phishing customisation and malware obfuscation at scale. To counter this, SOCs can employ AI and machine learning to more quickly detect anomalies, automate triage and employ predictive analytics. These tools can help to filter out noise for analysts, allowing them to focus on priority threats.

SOCs must adapt to emerging threats that extend beyond traditional malware. Deepfake phishing and AI-generated voice fraud are making social engineering attacks harder to detect, making continuous monitoring essential.

A modern SOC needs to stay ahead of these trends, integrating comprehensive threat intelligence feeds, AI-driven analytics and real-time behavioural monitoring to identify new attack methods before they cause damage.

People: The human element

On the front lines, SOC analysts and proactive threat hunters act as first responders, triaging alerts and filtering out false positives. More complex cases are escalated for in-depth analysis, threat containment and coordinated response efforts.

SOC analysts study attack tactics, discover anomalies and aim to uncover patterns that can bypass traditional security controls.

These skills are in high demand, requiring expertise in real-time incident response, attack methodologies and threat intelligence.

Many organisations are addressing the chronic shortage of cybersecurity professionals by upskilling existing IT staff. However, this process takes time—potentially leaving a gap in protection and increasing the risk of cyberattacks during the transition.

Organisations also need to consider adequate levels of skills and resources required to deliver 24/7 security monitoring and that response capabilities need to be adequately protected outside of business hours.

Processes: IT ops, threat detection and playbooks

In general, processes are the glue that binds technology with people. For example, IT operations processes dictate acceptable risk levels by setting boundaries and workflows. They also help to enforce accountability and ensure security teams apply updates and patches, while escalating alerts according to policy.

Threat detection processes should be dynamic and continuously refined to keep up with new threats. If they aren't regularly reviewed and maintained, then visibility of potential and known risks will reduce over time.

Finally, clear playbooks are essential to properly investigate and manage security alerts. Process improvement requires dedicated resourcing to ensure effectiveness and relevance to the changing threats and vulnerabilities.

Taking an outsourced approach

Outsourcing SOC functions to a partner can help reduce costs, scale security operations and provide access to top-tier expertise. Instead of managing a full in-house team, organisations gain 24/7 monitoring, automation and expert threat intelligence—operating as an integrated security team rather than a passive service. This can directly reduce the cost and impact incurred by the business and its customers from a cyberattack.

However, not all SOC providers offer the same capabilities. Managed security services providers (MSSPs) focus on log monitoring, vulnerability scanning and compliance-driven security. MSSPs help provide reports and monitoring that can meet regulatory requirements, but they typically lack real-time threat hunting and active response capabilities.

Managed detection and response (MDR) providers can help fill gaps for those without dedicated in-house response teams.

Hybrid co-managed SOCs

Hybrid co-managed SOCs allow organisations to retain control over critical security functions while outsourcing 24/7 monitoring, intelligence and automation. This provides flexibility, keeping high-risk operations in-house while using specialist expertise for threat detection and incident response.

When selecting a SOC partner, factors such as industry expertise, response times, compliance capabilities and AI-driven threat intelligence should be carefully assessed. The right partner aligns with an organisation's security needs, integrates effectively with internal teams and provides the necessary coverage to detect and respond to threats in real time.

Organisations should assess whether their chosen SOC partner provides flexibility and transparency in how they integrate process and technology for an effective and adaptive hybrid SOC.

Key considerations: cost, expertise and risk

An in-house SOC, built specifically for an organisation's strategy and operational requirements, risk exposure and regulatory obligations, provides better control over security operations and data.

Maintaining an in-house SOC requires ongoing investment in both technology and cybersecurity talent. Organisations need to continuously update advanced security tools while also recruiting, training and retaining skilled professionals in a highly competitive job market.

Engaging a SOC partner offers an alternative by providing a range of services that can be customised for responsive incident management. A SOC partner can also be integrated with an organisation's IT and security capabilities with a dedicated team that can become deeply embedded in the organisation's infrastructure and culture. This approach delivers an always-on, tailored security presence.

While in-house teams can offer strong threat intelligence, scalability and a deep understanding of the organisation's environment, building and maintaining such a team requires significant investment and time. During this ramp-up, gaps in coverage may increase cyber risk. On the other hand, outsourced SOC providers can offer immediate scale and specialised expertise, but may lack the institutional knowledge and on-site presence of an internal team. When evaluating any SOC approach—internal, external or hybrid—key considerations include cultural alignment, familiarity with existing security tools, regulatory compliance and the organisation's appetite for operational flexibility.

Whether in-house or outsourced, a SOC needs to align with both regulatory and industry-specific security requirements. These regulatory requirements necessitate an organisation conduct continuous monitoring, audits and proactive security governance to maintain compliance.

Building a SOC is not a one-time project—it is a living, evolving operation that requires constant monitoring, maintenance and adaptation. This adaptability is driven by the everchanging and escalating cyber threat landscape, as well as responding to changing business needs to be responsive and cost-effective.

Without sustained investment in the latest technologies, expertise and security strategies, even the most advanced SOC can quickly become outdated and less effective.

Learn more

To learn more about selecting the best approach for your security operations centre requirements, contact your Verizon Business Account Representative. Email apaccontactus@verizon.com. Or visit verizon.com/business/en-au/contact-us/.