



Managed Security Operations Centre

24x7 Threat Monitoring

Cyber criminals could be sneaking into your network, snatching data, or plotting ransomware attacks. With our world class 24/7 Managed Security Operations Centre on guard, we'll catch and halt most attacks before any harm is done.

Comprehensive Managed Detection & Response



Endpoint Security

Protect your endpoints with Windows and MacOS event log monitoring, advanced breach detection of malicious files and processes, threat hunting, intrusion detection, 3rd party next-gen AV integrations and more.



Network Security

Gain new levels of network protection with firewall and edge device log monitoring integrated with real time threat reputation, DNS information and malicious connection alerts.



Cloud Security

Secure the cloud with Microsoft 365 security event log monitoring, Azure AD monitoring, Microsoft 365 malicious logins and 365 risk detection.

24x7 Managed SOC Powered by Cybersecurity Experts

Nexus Managed SOC is a managed detection and response service that leverages the threat monitoring platform to detect malicious and suspicious activity across three critical attack vectors: endpoint, network and cloud. Our team of cybersecurity experts hunt, triage and work with you when actionable threats are discovered. Services include:

- **Continuous Monitoring** – Around-the-clock protection with real-time advanced threat detection
- **Breach Detection** – We catch sophisticated and advanced threats that bypass traditional AV and perimeter security solutions
- **Threat Hunting** – An elite cybersecurity team proactively hunts for malicious activities so you can focus on other pressing matters
- **No Hardware Requirements** – Patent-pending cloud-based technology eliminates the need for costly and complex on-premise hardware

Managed Security Operations Centre

24x7 Threat Monitoring

Managed SOC – Key Features

We save you time and money by leveraging your existing tools and cybersecurity investments across endpoints, network and cloud. This allows you to focus on what matters most – your business.



SIEMless Log Monitoring

Monitor, search, alert and report on endpoint, network and cloud threat vectors, including key log data from Windows and MacOS, firewalls, networked devices, Microsoft 365 & Azure AD – all without requiring an additional SIEM or SIEM hardware.



Threat Intelligence and Hunting

Real-time threat intelligence monitoring, linked with extra intelligence fed from premium partners, gives our SOC analysts the largest global repository of threat indicators to hunt down attackers and find advanced threats in your systems.



Breach Detection

Detect adversaries that evade traditional cyber defenses. We identify attacker tactics, techniques and procedures, aligning to MITRE ATT&CK. This allows our SOC analysts to detect indicators of compromise before damage is done.



Intrusion Monitoring

Real-time monitoring of malicious and suspicious activity, identifying indicators such as connections to terrorist nations, unauthorized TCP/UDP services, backdoor connections to command and control servers, lateral movements and privilege escalation.



Next-Generation Malware

Use your preferred malware prevention or leverage our command and control application for Microsoft Defender, backed up with a secondary line of defense using our malicious detection of files, tools, processes and more.



Service Desk Triage

Our dedicated team employs advanced tools and methodologies in the initial assessment, allowing us to promptly categorise and address security events, bolstering the overall resilience of your organisation's cybersecurity posture.



Seamless Integrations

Our managed SOC solution integrates with popular cybersecurity products, meaning we have greater visibility across your existing tools, including:

- AV/AM monitoring with Bitdefender, Cylance, Deep Instinct, SentinelOne, Sophos, Webroot, Windows Defender
- Firewall Analyzer & Monitoring with Barracuda, Cisco Meraki, Fortinet, Juniper, pfSense, SonicWall, Ubiquiti, Untangle, WatchGuard
- Email and DNS Monitoring with Barracuda, DNSFilter, IRONSCALES, Microsoft 365

And much more!