The advantages of Nexus Managed SOC

SOCs operate 24/7, which is crucial for the early detection of threats, as cyber crimials don't work 9-5.

Without SOC services, your company may lack the skills to timely detect and respond to threats, allowing cyber-criminals to remain hidden.

A SOC can significantly reduce attack dwell time, minimising financial impact from months (average attack dwell time is 43 days) to a matter of just minutes.

Decreased costs of breaches and operations

- Reducing the time a cyber attacker spends in your network helps minimise the impact and potential costs of a breach, including data loss, lawsuits, and damage to business reputation. The longer the attacker remains, the greater the potential damage to your company.
- Managing cybersecurity internally using in-house resources can be expensive and difficult. The scarcity of available and skilled cybersecurity professionals for hire makes filling these positions challenging.

Threat prevention

- SOCs go beyond incident detection; their analysis and threat hunting abilities prevent attacks, offering heightened visibility and control over security systems to stay ahead of potential threats and issues.
- SOC monitoring around the clock keeps the threat radar circulating, hunting out advanced TTPs (tactic, techniques & procedures) to malicious hosts, networks and cloud assets, before a breach occurs.

Improved threat management

- You may already have a variety of security solutions designed to prevent and detect threats. For maximum efficiency they must be centralised, standardised, correlated and monitored in real time, with resources available to analyse and respond to suspicious activities and incidents.
- Consolidating security functions in a SOC can save money.
- Incidents are often likely to span multiple entities, and this requires coordinated actions to reduce risk. A SOC perfectly meets all these requirements.
- With a Nexus Managed SOC in place, we'll be able to identify attacks faster and remedy them before they cause your business more damage.

Maintenance of regulatory compliance

- A SOC also helps your business to meet requirements that require security monitoring, vulnerability management and incident response function.
- Aids compliance with SOC 2, HIPAA and GDPR.

Enjoy peace of mind with these key features:

Comprehensive Monitoring

Monitor, search, alert and report on the 3 attack pillars: network, cloud and endpoint, with log data spanning:

- Windows, macOS & Linux security events
- Firewall & network device events
- Office 365 & Azure AD cloud events

Breach Detection

Detect adversaries that evade traditional cyber defenses such as Firewalls and AV. Identifies attacker TTPs and aligns with Mitre Att&ck, producing a forensic timeline of chronological events to deter the intruder before a breach occurs.

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 C2 servers

Plus, no hardware required!

As our managed SOC is cloud based, you don't need to worry about investing in, or maintaining, additional hardware.

nexus