Exclusive Operations Centre

Managed Security Solutions by Exclusive Networks

Comprehensive Cybersecurity from Exclusive Operations Centre (XOC)

Our team of highly skilled security experts uses advanced systems and tools to protect organizations from cyber attacks. Our SOC teams monitor and analyze security data in real-time to detect and respond to threats, ensuring continuous protection. Cyberattacks are a constant threat to businesses of all sizes. A SOC provides 24/7 monitoring and defense, preventing significant financial and reputational damage by addressing threats in real time.

Why SOC Services from Exclusive Networks?

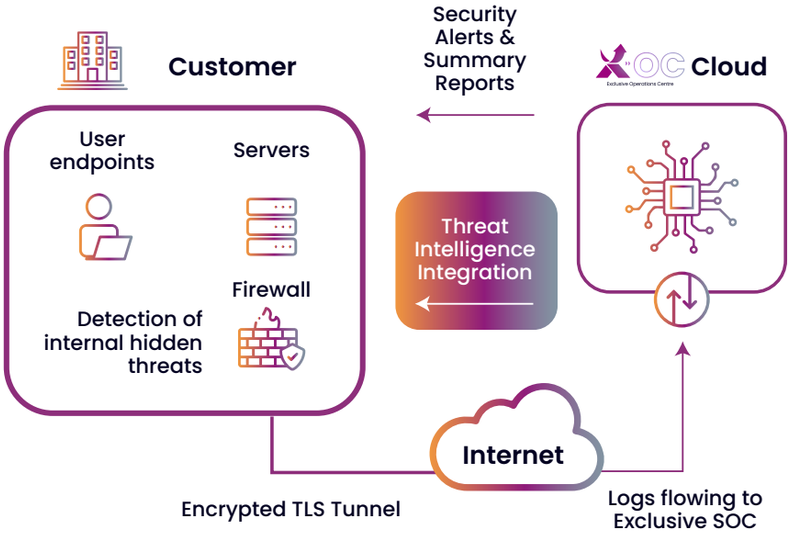
- **Cost-Effective:** Our SOC services are offered at a fraction of the cost of setting up and running an in-house security team, making top-tier security accessible to SMBs.
- **Flexible and Scalable:** If you don't have enough threats to justify an in-house team or don't want the hassle of managing one, we offer comprehensive protection without the high costs.
- **Advanced Detection:** Utilizing cutting-edge tools and AI, we identify threats missed by traditional measures.
- **Comprehensive Reporting:** Monthly and on-demand reports give complete visibility into your security status.
- **Global Expertise:** With over 150 SOC analysts across 7 locations, we ensure 24/7 global coverage with local expertise.
- **Proven Track Record:** Trusted by numerous clients, our SOC services effectively reduce risks and mitigate threats.

Our SOC Solutions for SMBs:

Small and medium-sized businesses are increasingly targeted by cyber attackers. Exclusive Networks offers tailored SOC solutions to help SMBs enhance their defenses and mitigate risks effectively. Here's why you should choose us:

- **Critical Events Fundamentals:** Ingests security event logs, applies real-time Threat Intelligence, and detects hidden threats. Includes a Cybersecurity Services Portal, email alerts, monthly reports, and 3-month log archiving. Includes 5 of the most popular security use cases (see table on the following page).

- **Critical Events Advanced:** Builds upon the fundamentals with integrated Threat Intelligence for automatic threat blocking. Includes 8 of the most popular security use cases (see table on the following page).



For Larger Enterprises:

- **Managed Detection & Response (MDR):** Comprehensive 24/7 incident response and multi-source event log analysis, covering EDR, MS AD, SIEM, and Cloud. This service eliminates the need for an in-house security team by providing extensive incident response, investigation, analysis, threat hunting, and mitigation.

- **Palo Alto Managed SOCaaS:** Full management, monitoring, alerting, reporting, automation, use case management, and security incident response for a Palo Alto security estate. Ideal for enterprises that need to outsource comprehensive SOC services to a third party.

	All Core Vendors			Palo Alto
	Critical Events Fundamentals	Critical Events Advanced	Managed Detection & Response (MDR)*	Palo Alto Managed SOCaaS
Technology Profile	Firewalls with up to 2.2Gbps protected throughout each Firewall-only based services	Firewalls with up to 2.2Gbps protected throughout each Firewall-only based services	Firewalls, Endpoints Security, MS Active Directory, SIEM, Cloud Security No limit on protected throughout	Full suite of Palo Alto Strata, Cortex & Prisma solutions No limit on protected throughout
Cybersecurity Services Portal	✓	✓	✓	✓
Alerts	✓	✓	✓	✓
Reports	✓	✓	✓	✓
Archiving	✓	✓	✓	✓
Integrated Threat Intelligence	✗	✓	✓	✓
24 x 7 Security Incident Response	✗	✗	✓	✓
Multiple Event Sources (Endpoint, MS AD, Customer SIEM, Cloud etc.)	✗	✗	✓	✓
Included Use Cases				
Malware Activity	✓	✓	✓	✓
Users Accessing Deep Web Resources	✓	✓	✓	✓
Corporate Credentials Exposed Externally	✓	✓	✓	✓
Microsoft Windows Attacked Assets	✓	✓	✓	✓
Applications Usage Visibility	✓	✓	✓	✓
Suspicious DNS Activity	✗	✓	✓	✓
Suspicious SMTP Activity	✗	✓	✓	✓
Data Exfiltration	✗	✓	✓	✓
User Behaviour Analytics on Active Directory (ADUBA)	✗	✗	✓	✓
DGA Malware Detection	✗	✗	✓	✓
Anomalous Users in Active Directory	✗	✗	✓	✓
Brute Force Login Attempts	✗	✗	✓	✓
Anomalous Logging Activity	✗	✗	✓	✓
Connections to Suspicious Destination Countries	✗	✗	✓	✓
Custom Use-Cases	✗	✗	✓	✓
Security Management				
24 x 7 policy and configuration change management	✗	✗	✗	✓
Policy sanitisation and security validation	✗	✗	✗	✓
Device configuration and topology report	✗	✗	✗	✓
Daily configuration backup	✗	✗	✗	✓
Firmware updates and testing	✗	✗	✗	✓
24 x 7 device availability monitoring	✗	✗	✗	✓
24 x 7 Technical Assistance Centre (TAC)	✗	✗	✗	✓
Compliance & best practice validation	✗	✗	✗	✓

*Managed Detection & Response (MDR) is highly customizable, offering a wide range of custom use cases. For tailored solutions or inquiries about MDR, please reach out to us.

Please contact our XOC team at serviceadvisory@exclusive-networks.com or contact your local sales representative.