

P1 MANAGED SOC (SECURITY OPERATIONS CENTER)

Introducing Managed SOC (Security Operations Center) – Your Comprehensive Defence Against Cyber Threats

Managed SOC (Security Operations Center) is your ultimate shield against cyber threats, offering a layered approach to protect your business from various security risks. Perigon One's Managed SOC combines advanced technology with expert human analysis to keep your digital assets safe 24/7.



Key Differences:

- **Threat Detection:** While EDR alone can detect known malware and some advanced threats, Managed SOC enhances this capability with advanced threat intelligence and proactive threat hunting.
- **Threat Response:** Managed SOC provides human-led response and investigation, offering a higher level of expertise compared to automated responses provided by EDR alone.
- **Breach Detection:** Managed SOC goes beyond EDR by proactively hunting for indicators of compromise, providing a more comprehensive approach to breach detection.
- **SIEM Integration:** Managed SOC includes integrated seamless log monitoring, offering better visibility and threat detection capabilities compared to EDR alone.

Why You Need Managed SOC:

In today's ever-evolving threat landscape, traditional cybersecurity measures are no longer sufficient to defend against sophisticated attacks. Managed SOC offers a proactive and comprehensive solution to address the following business threats:

Business Threats	Endpoint Detection and Response (EDR) Alone	EDR Combined with SOC (Managed SOC)
Detection of Known Malware	✓	✓
Detection of Advanced Threats	Partially (limited to known patterns)	✓ (Leverages advanced threat intelligence and analysis)
Real-time Monitoring	✓	✓
24/7 Threat Response	✗ (Limited to automated response)	✓ (Human-led response and investigation)
Breach Detection	Partially (limited to known indicators)	✓ (Proactive hunting for indicators of compromise)
Detection of Insider Threats	✗ (May require additional solutions)	✓ (Monitors user behaviour and activity)
Response to Zero-day Attacks	✗ (Limited to known signatures)	✓ (Advanced threat detection capabilities)
SIEM Integration	✗ (Usually not included)	✓ (Integrated SIEMless log monitoring)
Cost Efficiency	✓ (Lower cost compared to SOC)	✗ (May require higher investment)
Security Expertise Requirement	✗ (Limited need for expertise)	✓ (Leverages expert SOC analysts)
Peace of Mind	✓	✓

Conclusion:

Managed SOC (Security Operations Center) offers a comprehensive and proactive solution to protect your business from cyber threats. By combining advanced technology with expert human analysis, Managed SOC provides peace of mind and ensures your digital assets are safeguarded against evolving threats. Upgrade your cybersecurity posture with Managed SOC by Perigon One.