

Managed Security Services for SMB - PARAMOUNT CYBER DEFENSE CENTER (CDC)

AI-Driven SOC-as-a-Service Powered by Microsoft Sentinel



The Triple Challenge:



Compliance Pressure



Talent Shortage



Advanced Cyber Threats

Organisations across Australia and New Zealand face increasing cybersecurity pressure. Advanced threat actors, AI-driven attacks, and growing regulatory requirements are making security operations significantly more complex.

At the same time, organisations struggle with cybersecurity talent shortages, alert fatigue, and fragmented visibility across security tools.

Paramount Sentinel SOC addresses these challenges by delivering a 24x7 AI-assisted Cyber Defense Center powered by Microsoft Sentinel and Microsoft Defender XDR, providing continuous threat detection, automated response, and compliance aligned security monitoring.

Rising cyber threats in Australia and New Zealand are addressed by Paramount Sentinel SOC with 24x7 AI-powered security.

Introduction

Organisations today face three major cybersecurity challenges:

Increasing regulatory pressure – frameworks such as Essential Eight, SOCI Act, and APRA CPS 234 require continuous monitoring and evidence of security controls.

Cybersecurity talent shortages – organizations struggle to recruit and retain skilled SOC analysts.

Advanced cyber threats – attackers now leverage automation, AI, and sophisticated attack techniques.

Introducing Paramount Sentinel SOC – A Microsoft Sentinel Powered Cyber Defense Center

Paramount Computer Systems delivers a 24x7 Cyber Defense Center (CDC) built on Microsoft Sentinel, Defender XDR, and Security Copilot, providing organizations across ANZ with advanced threat detection, automated response, and compliance-aligned security operations.

Our SOC services provide expert-led security monitoring, threat intelligence integration, and automated incident response that strengthens your security posture while supporting regulatory compliance.



How We Address Today's Security Challenges

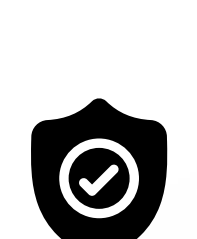
Your Challenge	One Solution - What we do	Your Strategic Benefit - What You Gain
Talent Shortage & 24/7 SOC Coverage	Paramount deploys a full SOC capability including L1, L2, and L3 analysts, threat hunters, and Microsoft security specialists, operating through our Cyber Defense Center.	Organizations gain 24x7 monitoring, investigation, and response capability without the cost and complexity of building an internal SOC team.
Alert Fatigue & Security Noise	Advanced Sentinel analytics, UEBA, and AI-assisted triage prioritize critical threats and eliminate false positives.	Security teams focus only on high-risk incidents, significantly reducing investigation time and analyst burnout.
Fragmented Security Visibility	Microsoft Sentinel integrates telemetry across identity, endpoint, cloud, SaaS, and network environments to provide unified monitoring.	Organizations gain centralized visibility and situational awareness, closing the security gaps attackers exploit.
Advanced & AI-Driven Threats	Integration with Microsoft Security Copilot (where applicable)++ and Threat Intelligence feeds enables rapid detection and response at machine speed.	Threats are detected and contained before they escalate into major incidents.
Compliance & Audit Pressure	Sentinel continuously collects logs, alerts, and incident data aligned to regulatory frameworks.	Organizations maintain audit-ready evidence of monitoring, detection, and incident response capabilities.
Optimizing Microsoft Security Investment	Paramount fine-tunes Microsoft Sentinel and Defender deployments to optimize detection coverage and reduce data ingestion costs.	Customers maximize security ROI and operational efficiency while strengthening cyber resilience.

Built for Australia's Cybersecurity Frameworks



Essential Eight – Continuous Control Monitoring

Paramount Sentinel SOC continuously monitors the effectiveness of Essential Eight security controls. The SOC detects threats such as MFA bypass attempts, exploitation of unpatched vulnerabilities, privilege escalation, suspicious application execution, and backup tampering. This ensures Essential Eight controls are actively enforced.



SOCI Act – Critical Infrastructure Protection

Organizations regulated under the Security of Critical Infrastructure (SOC) Act must maintain strong monitoring and incident reporting capabilities. Paramount SOC enables continuous monitoring of critical infrastructure assets, behavioral analytics, CIRMP risk visibility, and rapid cyber incident detection.



APRA CPS 234 & CPS 230 Compliance

Financial institutions must demonstrate strong information security monitoring and response capabilities. Paramount Sentinel SOC enables continuous monitoring, rapid threat investigation, structured incident timelines, and operational risk visibility aligned with APRA standards.



Integration with Australian Threat Intelligence

Our SOC integrates intelligence from Microsoft Defender Threat Intelligence, ACSC advisories, ASD threat intelligence feeds, and STIX/TAXII integrations ensuring detection aligns with Australia's evolving threat landscape.

What is included in the offer:



24x7 monitoring from remote SOC (up to 10GB/day ingestion and up to 300 users)



SIEM onboarding and integration



SIEM administration and use case management



Breach & Attack Simulation (one test)



Dark web monitoring (one sweep)



Vulnerability management (twice annually)

How much: **AUD 14 per user per month with a minimal 12-month contract.**

Additional Cybersecurity Services from Paramount



Risk & Governance

Third party risk management
Compliance advisory



Security Testing

Penetration testing



Incident Preparedness

Incident response retainer

Conclusion

Cyber threats are evolving rapidly. Organizations need a modern security operations capability that combines human expertise, AI-driven analytics, and continuous monitoring.

Paramount Sentinel SOC provides a Microsoft-powered Cyber Defense Center (CDC) that strengthens cyber resilience while supporting ANZ's regulatory requirements.

Focus on your business while we defend your environment 24x7.



Why Paramount?

- Microsoft Security specialists with deep Sentinel expertise
- Proven SOC operating model supporting global customers
- Integration with the Microsoft Security ecosystem (Defender, Sentinel, Entra)
- Compliance-aligned monitoring for ANZ regulatory frameworks
- AI-assisted SOC operations using Microsoft Security Copilot
- Paramount is a member of the Microsoft Intelligent Security Association (MISA) and a Managed XDR partner - the highest level of accreditation within the Microsoft security ecosystem.
- CREST certified MSOC from Paramount



Contact Us

Neeti Rodrigues

neeti.r@paramountassure.com +61 432 036 056

Udeesh Millathe

Udeesh.m@paramountassure.com +61 402 909 718