CIRRO

Cloud Security Operations (Managed SOC)

Service Name *3*
Service description 3
Managed SOC service levels 3
Service level guidance 4
Our of Hours Wrap Around Service 4

Service Name

Service description

Cirro provides a managed Security Operations Centre (SOC) service delivering continuous monitoring, detection, and response for cloud environments. The service is designed to help public sector organisations identify security threats quickly, reduce incident impact, and maintain clear operational accountability.

The Managed SOC operates 24×7×365 and integrates with supported cloud platforms, security tooling, and log sources. Services include event monitoring, alert triage, investigation, incident response coordination, and operational security reporting. All security activities are delivered as an ongoing operational service rather than advisory consultancy.

Our SOC works closely with cloud operations teams to ensure security incidents are handled in line with agreed processes, escalation paths, and service levels. Where required, the service supports containment and remediation actions within the customer environment, subject to agreed access and change controls.

The service is delivered by Cirro´s partner Innovate under their ISO/IEC 27001-certified information security management system and aligned to Cyber Essentials Plus controls. Operational security auditing and control validation are included as part of live service delivery. The service does not include certification audits, penetration testing, or standalone security consultancy.

Managed SOC service levels

Feature	SOC Core	SOC Enhanced	SOC Advanced
Security monitoring hours	24×7×365	24×7×365	24×7×365
Log and event monitoring	✓	✓	✓
Alert triage and prioritisation	✓	✓	✓
Security incident notification	✓	✓	✓
Incident investigation depth	Basic	Detailed	Advanced
Incident response coordination	✓	✓	✓
Containment and remediation support	–	✓	✓
Operational security auditing	–	✓	✓
Threat intelligence integration	–	✓	✓
Proactive threat hunting	–	–	✓
Custom detection use cases	–	–	✓
Security reporting and reviews	Standard	Enhanced	Advanced
Dedicated security contact	–	Optional	✓

Service level guidance

- SOC Core is suited to organisations requiring continuous monitoring and alerting with clear visibility of security incidents.
- SOC Enhanced adds deeper investigation, operational auditing, and supported response actions.
- SOC Advanced provides the highest level of security maturity, including proactive threat hunting and advanced detection capabilities.

Our of Hours Wrap Around Service

Security threats are ever present, and incidents do respect business hours. Some customers, particularly smaller organisations do not have sufficient resources to cover 24by7 every day of the year.

Cirro can offer an out of hours SOC service which will maintain monitoring and incident response out of hours allowing customers to protect themselves cost effectively.