Superior security and data protection across all your environments every time

AUCloud Security Operations Centre as a Service (SOCaaS) provides confidence that your data is continuously monitored and protected by a rapid response capability.

Powered by an industry-leading combination of security technology and highly skilled analysts, AUCloud's SOCaaS delivers more than your traditional SOC capability.

AUCloud SOCaaS provides continuous monitoring of your data to detect, prevent, investigate and respond rapidly, to cyber threats.

Monitoring, rapid detection and confident response capability

Continuous Protective Monitoring

Continuous monitoring of your environment ensures potential threats are quickly identified - before they become incidents.

Incident detection and response

Using the Cumulo platform, logs can be collated and triaged and suspicious activity prioritised to ensure resources are appropriately and efficiently targeted.

Expert analysts and playbooks

Tailored playbooks provide a recommended course of action for specific threats enabling rapid response when it's needed.

Complementary 'add-ons' for additional capability

Complement the Cumulo monitoring platform with virtual and/or physical appliances that perform network packet capture, SNORT, and BRO to provide additional information and context.

Transparency and audit capability

Honesty and transparency is key to success which is why customers can view and audit every action and decision made by our SOC analysts.

AUCloud SOC Service levels

AUCloud SOCaaS provides service flexibility that meets your needs.

SOCaaS service levels can be tailored to meet your specific data monitoring, protection and response requirements. Additionally, if you have sensitive data or high value assets, our consumption based service approach allows you to easily increase your monitoring requirements to meet the higher level protection needs of those resources.

Features	Baseline	Enhanced	Premium
Security alert generation	24x7 automated	24x7 automated	24x7 automated
SOC coverage	Office hours	Office hours	24x7
Response and resolution priority	Lowest	Moderate	Highest

Features

- 24/7 security monitoring, triage, alerts, analysis and incident response
- Evergreen solution with regular updates
- Multiple delivery models: on-premise, public cloud and hybrid cloud
- Continually updated threat intelligence and risk modelling, consumed from open source and commercial feeds
- Traffic analysis, deep packet Inspections, IDS, vulnerability scanning, blacklist monitoring
- Distributed and federated architecture, multi domain and multi classification incident response, dedicated cyber case management and generated playbooks
- Mobile and remote workforce monitoring - geo alerting, location reputation checking, identification of compromised home networks
- Accommodates OFFICIAL or PROTECTED requirements

Benefits

- Reduced cost of monitoring with increased coverage
- Triage and analysis services identify threats before they become incidents
- Near real time alerting and incident response
- Situational awareness allows confident response decisions
- Speed of delivery - can be rapidly integrated into your environment
- A single holistic view of risks and threats across the enterprise, including private and public cloud infrastructure
- End-to-end business security confidence with essential security audit assurance
- Centralised integrated security knowledge repository with enhanced anomaly detection
- The ability to proactively manage threats and avoid incidents, ensures the operational continuity of your IT systems
- Ability to maximise existing IT investment in security

AUCloud SOCaaS technology partners:

e2e assure

Next Steps

1. Contact our sales team at sales@australiacloud.com.au or 1800 282 5683
2. Talk to us about your business and how AUCloud SOCaaS can enable your data protection strategy