

CyberOne –Managed Security

Organisations across the globe are facing advanced, sophisticated, and often targeted attacks. Just as companies seek outside expertise for legal and financial matters, they should now be looking for experts in cyber security and dataprivacy.

Why do you need Managed Security Service?

See and stop threats before they cause harm, with managed security for a modern digital world. Obtain a bird's-eye view of cybersecurity across the enterprise with data insights and monitoring with visualisations. The Cloud Collective team put the cloud and large-scale intelligence to work leveraging decades of Microsoft security experience.

- Make your threat detection and response smarter and faster with Artificial Intelligence (AI)
- Eliminate security infrastructure setup and maintenance
- Elastically scale to meet your security needs – while reducing IT costs

Our Process

We install and configure components from the Microsoft Cybersecurity Reference Architecture to provide maximum coverage and effectiveness. Leveraging AI, Azure Sentinel deployed in the customer's environment and integrated with our Australian-based Security Centre, enables a "single pane of glass" for Quorum and Internal Security Teams to look for threats. When a threat is detected we will notify you of the incident and execute our customised automation. Our key goal is to reduce "mean time to detect" and "mean time to resolve"

- 1 Identify & define scope for Managed Security Service
- 2 Enable and on-board onto Managed Azure Sentinel quickly and efficiently
- 3 Collect data across users, devices, applications, and infrastructure, both on-premise and in cloud
- 4 Detect previously uncovered threats and minimise false positives using analytics and unparalleled threat intelligence from Microsoft
- 5 Investigate threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft
- 6 Respond to incidents rapidly with built-in orchestration and automation of common tasks
- 7 Notify you of any security incidents and give advice on the next steps for remediation

What is Managed Security?

Leveraging key components of the Microsoft Cybersecurity Reference Architecture and Azure Sentinel a scalable, cloud-native, Security Information Event Management (SIEM) and Security Orchestration Automated Response (SOAR) solution. Cloud Collective Managed Security Service delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response. Our Managed Security Service lets the Cloud Collective be your Managed Security Service Provider (or to bolster your current team) allowing your Internal IT team to focus on delivering value to your business rather than monitoring the company's security posture and alerts.

What do you get?

Cloud Managed Security Incident Event Management system based on Azure Sentinel including:

- Continuous detection
- Monthly report containing any security alerts and events
- 24x7 notification of P1 security incidents
- 100% Australian owned and operated security centre

Cost

Two functional tiers available.

TIER 1 Essentials

- End to End Managed Cybersecurity Detection
- Limited Incident Handling
- Automated Response
- Risk Exposure Scoring
- Vulnerability Reporting

TIER 2 Elite

- End to End Managed Cybersecurity Detection
- Incident Handling
- Automated Response
- Risk Exposure Scoring
- Risk Mitigation
- Vulnerability Reporting and Remediation
- Advanced Threat Hunting

Pricing available on request.

Part of the CLOUD collective

antares

icomm

quorum



go far
go together