

Cyber One Managed Extended Detection and Response (MXDR)

Quorum's Managed Security Service delivers intelligent security analytics and threat intelligence across the enterprise within one holistic, streamlined solution for alert detection, threat visibility, incident trends and vulnerabilities insight.



Cyber One provides single solution for monitoring the cyber security needs of organisations of all scales and maturity.

Managed Detection and Response services require a strategic combination of technology and human expertise that tightly focuses on detecting, analysing and responding to threats that have passed preventative tools. The key difference between Managed detection and response and other types of response and alert tools, is that it is a managed service, using technology, trends, AI and human expertise to review all potential attack surfaces. Undertaking a Managed Detection and Response operation internally is often out of grasp for clients requiring consistent attention and specialised skill sets such as threat hunting, analysis and incident response.

At Quorum, our values remain at the forefront of our work and Managed Detection and Response is an area of our Security Portfolio that utilises our best and brightest to deliver results for our clients. Our team of high achieving, awarded Cyber Security Analysts, Architects and Engineers, work to complement the huge amounts of data Cyber One processes, bringing a specialised level of knowledge, context and analysis that elevates the automated data analysis and provides leading insight into threat detection and response.

This dedication has been recognised at all levels we are the first partner in Australia to achieve the Microsoft verified Managed Extended Detection and Response (MXDR) solution status.

Cyber One unlocks holistic insights into the Azure and Microsoft 365 platforms and their associated security services. Discover highlighted trends, easily monitor risk areas, and regularly advise on how to bolster security posture through the further use of existing resources or complementary services.

Cyber One empowers organisations to proactively utilise security incident management capacities, including identifying vulnerabilities, security recommendations for monitored endpoints, and identity management across Microsoft 365 and Azure apps and resources by providing one solution that monitors the organisation's security needs.

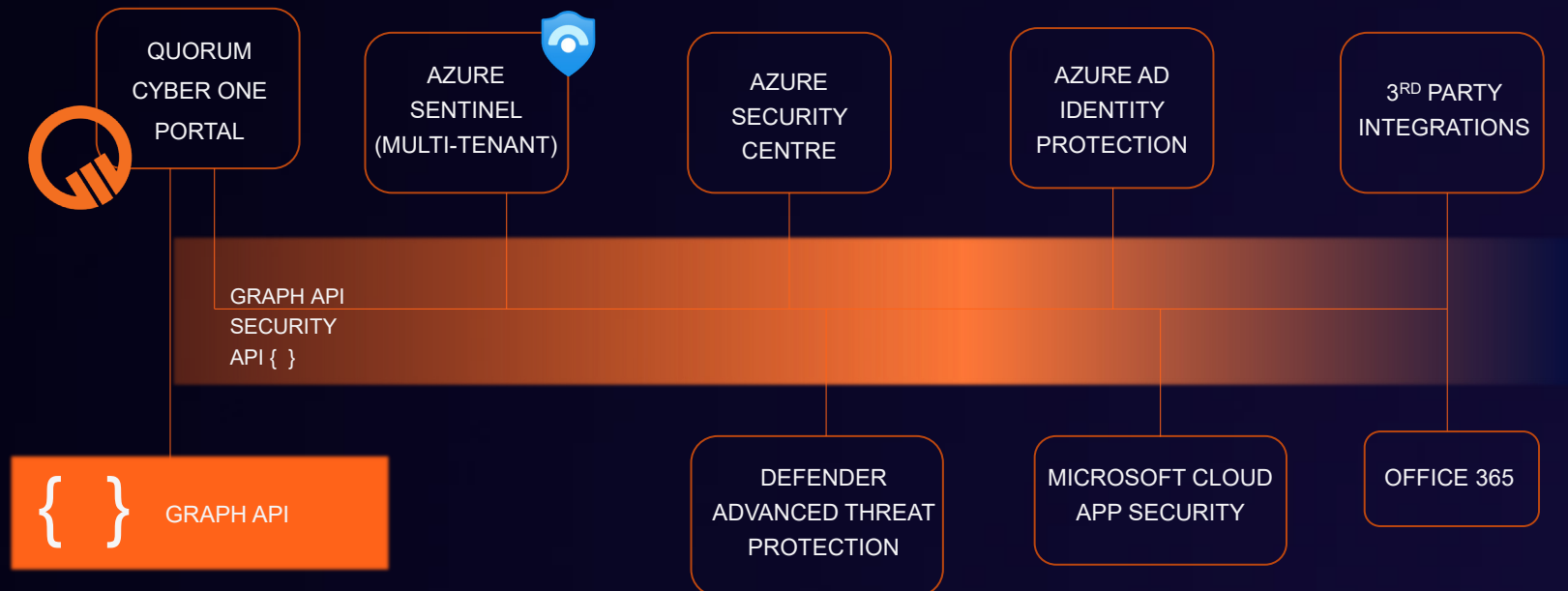
Microsoft Intelligent
Security Association



Cyber One provides one single solution for monitoring the cyber security needs of organisations of all scales and maturity. Its key benefits include:

- Security Service Delivery and Incident Management provided by the Quorum Managed Detection and Response Team
- A single pane of glass, allowing all important security data and the organisation's current security posture to be seen at a glance
- Reductions in the 'mean time to response' through the proactive notification of customers, and the Quorum team, of potential or identified risks (such as known or emerging vulnerabilities across applications, endpoints or Azure resources)
- Continuous improvement of the organisation's cyber security posture in order to reduce risk elements, balancing short-term improvements alongside long-term client objectives
- Compliance with industry framework regulations, such as ISO 27001
- Manage insider risk and increase security awareness training for all users

CYBER ONE INTEGRATION OVERVIEW





Microsoft
Solutions Partner
Security

Specialist
Threat Protection
Cloud Security
Identity and Access
Management
Information Protection and
Governance



Microsoft
Partner

2021 Partner of the Year Finalist
Security Award



Microsoft
Partner

2022 Partner of the Year Finalist
Security Award

Get in Touch

Phone
+61 (0)2 8966 1400

Email
sales@quorumsystems.com.au

Address
Level 6, 89 York Street Sydney, NSW, 2000

Microsoft Intelligent Security Association

