

MDR SOC

Managed Detection & Response – Security Operations Centre

Always-on threat visibility, detection, and response for your organisation



24/7

Always-On SOC Protection

99.9%

Threat Detection Accuracy

<15 Min

Mean Time to Respond

WHAT IS MDR SOC?

Cyber threats don't keep business hours – and neither do we. **AUZA MDR SOC** is a fully managed, round-the-clock Security Operations Centre combining elite human analysts with AI-powered automation to detect, investigate, and neutralise threats before they impact your business. We provide complete threat visibility across endpoints, cloud, networks, and SaaS – so your team stays focused on growth, not incidents.

MDR SOC COMPONENT

1 24/7 Threat Monitoring

Continuous surveillance across endpoints, cloud, and networks — real-time alerting with round-the-clock analyst oversight.

2 Incident Response

Rapid triage and containment of active threats. Analysts investigate, prioritise, and coordinate remediation to minimise dwell time.

3 Advanced Threat Intelligence

Curated global feeds for emerging threats. Indicators of compromise operationalised in real time across your environment.

4 Proactive Threat Hunting

Identifying hidden threats before they escalate using human-led investigation and AI-driven behavioural analytics.

5 EDR / SIEM Management

End-to-end log collection, event correlation, and compliance reporting — reducing alert fatigue and ensuring audit-ready visibility.

6 Endpoint Detection & Response

Behavioural analysis and automated isolation of compromised endpoints, stopping lateral movement and minimising blast radius.

FROM DEPLOYMENT TO DEFENSE IN THREE STEPS

1 Onboard & Integrate

Deploy lightweight agents, connect log sources, and integrate with Microsoft 365 and Azure. Fully operational in as little as 72 hours – no rip-and-replace required.

2 Detect & Investigate

AI-driven correlation surfaces high-fidelity alerts. Tier 2 & 3 analysts investigate every confirmed threat, eliminating noise and providing full attack context.

3 Contain, Report & Strengthen

Guided response playbooks enable rapid containment. Monthly threat reports and quarterly reviews continuously harden your security posture over time.

WHY AUZA MDR SOC? BECAUSE THREATS DON'T WAIT - AND NEITHER DO WE.

Microsoft-Aligned Stack

Built on Microsoft Sentinel, Defender XDR & Azure — maximizing your existing investment with native SIEM/XDR integration.

Rapid Time-to-Value

Fully operational within 72 hours. Pre-built detection rules and connectors eliminate lengthy deployment cycles.

Human + AI Analyst Fusion

Elite Tier 2 & 3 SOC analysts augmented by machine learning — reducing false positives by up to 80%.

Compliance Ready Reporting

Pre-built dashboards aligned to MAS TRM, ISO 27001, and Singapore PDPA requirements.

Seamless Integration

Connects with Microsoft 365, Azure, Splunk, CrowdStrike, Palo Alto, and 100+ log sources.

Dedicated Incident Commander

A named security advisor coordinates response, stakeholder comms, and post-incident reviews.

GET STARTED - CONTACT US!

[Request a Demo](#) | [Get a Free Assessment](#) | [Contact Our Team](#)



Your Partner in Security, From Strategy to Execution

EMAIL
sales@auza.cc

WEBSITE
WWW.AUZA.CC