CONDITION™ ZEBRA

Human-led, fully Tailored Services for Microsoft Security Solutions

- Open architecture-based MDR Platform
- Leverages existing endpoint/firewall investments
- AI/ML accelerated human-led threat hunting
- Hands-on keyboard-based incident response

Microsoft Defender for Endpoint | Microsoft Defender for Office 365 | Microsoft Sentinel

Managed Detection and Response (MDR) for Microsoft Defender

Detection
24x7 SOC powered managed services rendering 360-degree visibility and proactive threat hunting using super accurate threat intelligence.

Investigation
Highly precise, AI-driven investigation with expert-driven contextual analysis (covering IP stack, URL, and app reputation), root cause analysis, and triage.

Response
Open architecture platform that easily integrates with existing infrastructure with streamlined security workflows, 24x7 incident response, and expert-led remediation guidance.

Compliance
End-to-end compliance achievement through round-the-clock log collection, file integrity monitoring, and seamless vulnerability management.

Managed SIEM Services for Microsoft Sentinel

Design & Provisioning
We onboard log sources, provision usage reports, configure threat intel feed, and enable silent log monitoring on the SIEM platform.

Use Case Management
Effective identification and deployment of alert rules, configuration of playbooks & dashboards/ workbooks, creation of log parsers, and inclusion of additional log sources.

Detect, Respond, & Investigate
Detect anomalous activities quickly with super fast AI that monitors your environment 24x7. Automatically addressing threats letting experts handle the critical incident investigation.

Risk & Compliance Management
End-to-end compliance achievement through:- Effective identification & treatment of misconfigurations, and assessment of log sources & detection content against the MITRE ATT&CK Framework.

☎ +603-7665 2021 www.condition-zebra.com info@condition-zebra.com