MXDR

Managed eXtended Detection and Response

Protect. Detect. Respond. Improve.

Managed monitoring, detection and response based on Microsoft Defender XDR and Microsoft Sentinel.

Gain visibility. Reduce risk. Strengthen defense.

Microsoft Defender XDR | Microsoft Sentinel | Microsoft Security | Best Practices

CUSTOMER PROBLEM

Smaller or less mature organizations need continuous expert oversight of critical Microsoft security alerts but may not be ready for a full advanced MXDR service.

Security teams need continuous detection and response across endpoint, identity, email, cloud apps and selected log sources, but lack enough resources to operate Microsoft security tools around the clock.

Advanced organizations need more than alert monitoring: they require extended visibility, proactive hunting, exposure-informed detections, response playbooks and transparent operational metrics.

HOW WE SOLVE IT

INNOVATE MXDR Micro provides focused monitoring, triage and guidance for high-priority Microsoft Defender XDR incidents, with optional Sentinel visibility for selected Microsoft sources. The service uses Microsoft Defender XDR, Defender for Endpoint, Entra ID Protection and standardized automated response runbooks.

INNOVATE MXDR Plus delivers managed monitoring, triage, investigation, tuning and response support using Microsoft Defender XDR and Microsoft Sentinel. The service includes detection engineering, automated playbooks with Logic Apps, reporting and continual improvement.

INNOVATE MXDR Advanced extends monitoring across Microsoft Defender XDR, Sentinel, cloud security, identity, selected third-party sources and threat intelligence. The service includes advanced hunting, detection engineering, SOAR automation, executive reporting, MITRE ATT&CK mapping, cost optimization and continuous service reviews.

YOUR OUTCOME

- Affordable entry point to managed detection and response
- Expert triage of critical Microsoft alerts
- Clear escalation and remediation guidance

- 24x7 Microsoft-native detection and response
- Reduced alert fatigue through expert triage and tuning
- Continuous improvement of detections and playbooks

- Extended coverage across Microsoft and selected third-party sources
- Proactive hunting and detection engineering
- Metrics-driven service improvement and executive visibility

SERVICE TIERS

MXDR MICRO

A lightweight Microsoft-native MXDR service for organizations that need expert monitoring without the complexity of a full SOC program.

INCLUDED

- Business hours monitoring
- Microsoft Defender XDR
- Critical alert triage
- Escalation support
- Standard runbooks
- Monthly reporting

KEY OUTCOMES

Affordable entry point | Expert alert validation | Guided remediation

MXDR PLUS — MOST POPULAR

A Microsoft-centric MXDR service that combines 24x7 monitoring, threat management and response orchestration across Defender and Sentinel.

INCLUDED

- 24x7 monitoring
- Microsoft Defender XDR
- Microsoft Sentinel
- Investigation & response support
- Detection tuning
- Logic Apps playbooks
- Monthly service reviews
- KPI reporting

KEY OUTCOMES

Reduced alert fatigue | Faster detection & response | Continuous improvement

MXDR ADVANCED

An advanced MXDR service for enterprises that need extended telemetry, proactive threat hunting and measurable cyber resilience.

INCLUDED

- Everything in Plus
- Threat hunting
- Detection engineering
- MITRE ATT&CK mapping
- Third-party telemetry
- SOAR optimization
- Executive reporting
- Cost optimization reviews
- Quarterly strategy reviews

KEY OUTCOMES

Proactive threat hunting | Extended visibility | Measurable cyber resilience

SERVICE COMPARISON MATRIX

CAPABILITY	MICRO	PLUS	ADVANCED
Defender XDR Monitoring	✓	✓	✓
Sentinel Monitoring	Limited	✓	✓
24x7 Coverage	—	✓	✓
Incident Investigation	Basic	✓	✓
Threat Hunting	—	—	✓
Detection Engineering	—	✓	✓
Third-Party Sources	—	—	✓
Executive Reporting	—	—	✓
MITRE Coverage Review	—	—	✓

MXDR OPERATING MODEL

WHAT YOU RECEIVE

SOC Portal Access | Incident Reports | Monthly Executive Report | Service Reviews | Threat Intelligence Insights | Detection Tuning | Hunting Reports (Advanced) | KPI Dashboards

INNOVATE
AXAITRA GROUP MEMBER

Member of Microsoft Intelligent Security Association

Microsoft Security | Microsoft Verified Managed XDR Solution

Let's start the conversation.

Contact us to turn security challenges into strategic opportunities through actionable insights and expert guidance

contact@innovate-security.ai
www.innovate-security.ai