AMTRA
S O L U T I O N S

AMTRA MANAGED EXTENDED DETECTION & RESPONSE (MXDR)

Proactively Stop Threats Before They Impact Your Business

AMTRA Managed Extended Detection and Response (XDR) minimizes the gap between speed of compromise and speed of detection with proactive threat hunting and incident response services. Utilizing machine learning and analytics, AMTRA MXDR correlates activity, normalizes information and identifies threats across your entire network so you can get back to what really matters.

WHAT'S INCLUDED

Threat Profiling
Gain an understanding of your attack surface, critical infrastructure, sensitive data, and operational processes with full visibility into your threat landscape.

Threat Response
Contain threats faster with 24/7/365 managed threat response services designed to rapidly contain endpoint, user, and email-based threats to mitigate potential breaches.

Threat Defense
Leverage AMTRA MXDR and Microsoft 365 Security services, to prevent, detect, contain, and remediate attacks from threat vectors before, during, and after execution.
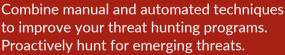
Threat Intelligence
Access industry-leading threat intelligence to improve detection and provide proactive threat bulletins. Stay current on industry trends from our leading security experts.

Threat Hunting
Combine manual and automated techniques to improve your threat hunting programs. Proactively hunt for emerging threats.

Dashboard & Reporting
AMTRA MXDR offers comprehensive dashboards and real-time reporting to maximize visibility & support security decisions.

HOW DOES IT WORK

AMTRA's MXDR is powered by a combination of Microsoft's security solutions and the AMTRA security platform. The model allows AMTRA's security team to monitor and respond to cloud service, endpoint, backend infrastructure, user, and email threats using Microsoft 365 Security services, Microsoft Sentinel analytics, and AMTRA's proprietary capabilities. Our MXDR solution is also compatible with Azure Active Directory (Azure AD), Microsoft Defender for Cloud Apps, and Microsoft Purview Information Protection.