DIFENDA

Member of Microsoft Intelligent Security Association

Microsoft

Microsoft Solutions Partner
Security
Specialist
Cloud Security
Threat Protection

MXDR FOR EDR

Difenda MXDR for EDR offers the latest in Microsoft's extended detection and response (XDR)—allowing all organizations to benefit from a world-class cybersecurity program that's built for scale, and integration-ready from day one.

Difenda is a globally accredited cybersecurity company that operates highly-certified cyber command centers. As one of Microsoft's top global implementation partners for Microsoft Sentinel and other Microsoft Security suite services, we provide 24/7/365 threat monitoring and response services that protect your cloud environment, network endpoints, and mission critical infrastructure.

WHAT WE OFFER

ASSET THREAT PROFILING

Better understand your threat profile and how it impacts your business.

Develop a deeper understanding of your attack surface, critical infrastructure, sensitive data, and operational processes. Get the best chance to be successful by identifying real business problems and risks. Get the tools to think like an adversary and strategically prioritize security efforts accordingly. Access expert threat detection capabilities and response playbooks are possible with increased capacity to categorize endpoints.

INTELLIGENT THREAT DETECTION

Utilize industry-leading threat intelligence to block & contain cyber attacks at machine-speed.

Difenda leverages industry leading Endpoint Protection Platform (EPP) technologies to prevent, contain, and remediate attacks from all threat vectors before, during, and after execution.

PRE-EXECUTION:
Detect threats, even zero-day attacks, using AI, replacing ineffective signature-based antivirus solutions.

ON-EXECUTION:
Behavioral AI observes complex activities, acting automatically to block & contain attacks at machine-speed.

POST-EXECUTION:
Rich forensic data collection supports organization-wide auto-immunity and endpoint-specific rollback capabilities.

EXPERT THREAT HUNTING

Combine manual and automated systems for expert threat hunting techniques.

Difenda leverages security information and event management (SIEM) technologies, powered by Microsoft Sentinel, to collect, analyze and detect threats. Difenda's MXDR for EDR service SIEM model is designed to support reliable, consistent, and cost-effective service delivery. Core to the MXDR for EDR service is Difenda's ATT&CK driven development methodology and automated response capabilities.

24/7 THREAT RESPONSE

Access 24/7/365 managed threat protection and an immediate defense strategy.

The Difenda Cyber Command Centre, is an advanced modern security operations center (SOC), is comprised of trained and experienced security personnel which are available 24/7/365 to manage threat response on behalf of Difenda's customers.

- Provide priority response to breaches / potential breaches
- Establish a cyber incident command structure
- Provide detailed post-incident document detailing

C3 strictly follows industry best practices for incident response and uses advanced tools to automate, monitor, record, and manage these processes.

See the difference a personalized approach to cybersecurity makes.

CONTACT A MICROSOFT SECURITY EXPERT TODAY: www.difenda.com | sales@difenda.com | 1-866-252-2103