MANAGED EXTENDED DETECTION AND RESPONSE FOR ENDPOINT

DIFENDA MXDR FOR EDR

DIFENDA

Member of
Microsoft Intelligent Security Association

Microsoft

Microsoft
Solutions Partner
Security

Specialist
Cloud Security
Threat Protection

MANAGED EXTENDED DETECTION AND RESPONSE FOR ENDPOINT

Proactive Threat Hunting and Incident Response

The days of set-and-forget security are behind us. To be effective against modern threats, a comprehensive security program must go beyond protection and monitoring capabilities. The ability to react quickly after the discovery of a potential breach is critical. Difenda's MXDR for EDR service includes proactive threat hunting and incident response services and is the best way to reduce attacker dwell time and the potential impact of a breach.

DIFENDA

www.difenda.com | sales@difenda.com | 1.866.252.2103

Member of Microsoft Intelligent Security Association

Microsoft

Microsoft Solutions Partner
Security
Specialist
Cloud Security
Threat Protection

A FORWARD-THINKING APPROACH TO ENDPOINT PROTECTION

Leverage Difenda's cybersecurity experts to strengthen your security posture. Powered by a combination of Microsoft's security solutions and the Difenda Shield platform, Difenda MXDR for EDR is an end-to-end process from receiving incidents to resolution. The model allows Difenda's C3 team to monitor and respond to cloud service, endpoint, backend infrastructure, user, and email threats using out-of-the-box Microsoft 365 Security services, Microsoft Sentinel analytics, and Difenda's proprietary capabilities.

Difenda MXDR for EDR Outcomes and Impact

- Complete design, deployment and management of EDR program
- Single endpoint solution maximizing Microsoft licensing capabilities
- Increased visibility and response capabilities
- Future-proofed platform to continuously tackle advancing technology
- Key operational support for busy IT teams
- Priority access to Difenda's Remote Incident Response services

DIFENDA

www.difenda.com | sales@difenda.com | 1.866.252.2103

Member of Microsoft Intelligent Security Association

Microsoft

Microsoft Solutions Partner
Security
Specialist
Cloud Security
Threat Protection

WHY DIFENDA?

The crown jewel of your security operations needs to be placed in experienced hands.

Decades of combined experience putting customer success first,
It all started with one mission:

Help our customers achieve success. Since then, we've leveraged our agile, innovative, and collaborative approach to create the powerful, modular cybersecurity suite Difenda Shield. We've also launched several advisory and offensive security services to drive awareness and meaningful outcomes across the people, processes, and technologies that drive the modern enterprise forward.

Certified and compliant with industry-leading standards

Trust, but verify – as the saying goes. Our staff and our facilities are highly decorated by third-party institutions. Difenda's personnel accreditation highlights include:

- CISSP, GSEC, GCIH, PCI Professional
- OSCP, OSCE, CCFP, CEH, GCPT
- MS-500, AZ-500, MCSE, MCSA
- PMP, ITIL, Certified Scrum Master
- ISO 27001
- PCI DSS
- SOC 2 Type II

Operational Experience

Microsoft Sentinel is a security operations tool that requires years of experience in the cyber-trenches to fully understand best practices and complexities to avoid. Difenda's experience stems from its managed service division which provides cutting-edge Managed Extended Detection & Response services leveraging Microsoft Sentinel.

Go-to partner for Microsoft Security integration and deployment

Difenda is the go-to Microsoft partner for XDR and the Defender suite of technology. Our experts work to integrate, mitigate and manage your security program with unique processes that leverage next-gen cloud technology to seamlessly reconcile, enhance, and manage assets in the Difenda Shield Portal.

DIFENDA

www.difenda.com | sales@difenda.com | 1.866.252.2103

Member of
Microsoft Intelligent Security Association
Microsoft

Microsoft Solutions Partner
Security
Specialist
Cloud Security
Threat Protection

5 KEY FUNCTIONS OF A SECURITY OPERATIONS PROGRAM

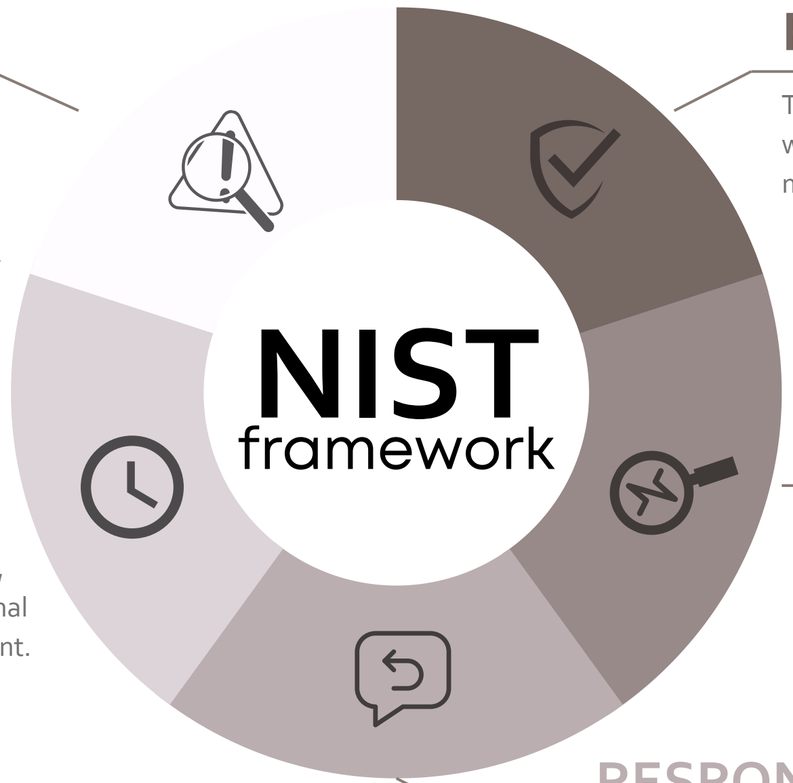
Industry-leading information security standards, such as the NIST Cybersecurity Framework, identify 5 key functions which must be present in a security operations program for it to be effective.

IDENTIFY

The ongoing process of developing a quantitative and qualitative understanding of the risks to an organization's people, assets, data, and capabilities prior to an incident.

PROTECT

The set of security controls which may partially or fully mitigate risks.



RECOVER

Timely restoration of the organization's people, assets, data, and capabilities to normal operation following an incident.

DETECT

The capability and process for timely discovery of an incident.

RESPOND

The capability and process for partially or fully limiting the impact of an incident.

DIFENDA MXDR FOR EDR IS COMPRISED OF SEVERAL COMPONENTS WHICH ARE ALIGNED TO THE NIST FRAMEWORK:

THREAT PROFILING

THREAT HUNTING

THREAT DEFENSE

THREAT RESPONSE
by Difenda Cyber Command Center (C3)

In addition to the above security operation capabilities, Difenda's MXDR for EDR offering provides forensic, audit, and compliance benefits. We reliably capture and securely retain all relevant security event information for future use.

DIFENDA

www.difenda.com | sales@difenda.com | 1.866.252.2103

Member of Microsoft Intelligent Security Association

Microsoft

Microsoft Solutions Partner
Security
Specialist
Cloud Security
Threat Protection

MAJOR CHALLENGES ORGANIZATIONS FACE WITH EFFECTIVE SECURITY OPERATIONS

Minimize the gap between speed of compromise and speed of detection with a strategically aligned security program encompassing your people, processes and technology.

PEOPLE

Hiring, training, and retaining qualified professionals during a growing global skills shortage.

PROCESS

Developing, implementing, managing, and aligning security operations to best practices.

TECHNOLOGY

Designing, building, configuring, and maintaining security infrastructure in an ever-changing technology landscape.

Managed Extended Detection & Response for Endpoint (MXDR for EDR) is a comprehensive solution offered by Difenda which addresses all three of these challenges across the entire organization to mitigate the potential impact of a breach. MXDR for EDR allows organizations of all types to benefit from a world-class security operations program, previously only available to banks and other large enterprises, without the major capital investment, resource constraints, and operational expenditures of building and running it "in-house."

DIFENDA

www.difenda.com | sales@difenda.com | 1.866.252.2103

Member of Microsoft Intelligent Security Association

Microsoft

Microsoft Solutions Partner
Security
Specialist
Cloud Security
Threat Protection

KEY FEATURES OF
DIFENDA MXDR FOR EDR

ASSET THREAT PROFILING

A thorough understanding of an organization's attack surface, critical infrastructure, sensitive data, and operational processes gives security operations staff the best chance to be successful by helping them to understand the customer's real business problems and risk, and also think like an adversary to prioritize their efforts accordingly. More intelligent threat detection capabilities and response playbooks are possible by categorizing endpoints.

INTELLIGENT THREAT DETECTION

A key part of any defense-in-depth strategy, workstations and servers must play an active part in detecting and containing possible threats, not just relying on conventional network-level protections like firewalls. 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 and contain attacks at machine-speed.

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

INTELLIGENT THREAT HUNTING

Difenda leverages security information and event management (SIEM) technologies, powered by Microsoft Sentinel, to collect, analyze and detect threats. Difenda's 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. As part of the ATT&CK driven development process, senior technical team members run attacks against simulated customer environments. Leveraging a 'Purple Team' approach to identify undetected threats, build detection use cases, and deploy updates to managed SIEM platforms.

Once threats are detected, Difenda's C3 experts rely on Difenda's security orchestration, automation, and response (SOAR) framework to quickly respond to threats in an automated manner. Difenda's SOAR framework is based on ServiceNow, Azure Automation, and Logic Apps services to support automated response activities.

In contrast to reactive security monitoring, threat hunting is the proactive process of systematically seeking out potential threats before an incident occurs. Difenda experts use a mix of manual and automated threat hunting techniques to form both ongoing and ad hoc, campaign-based hunting programs.

THREAT RESPONSE

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.

The Cyber Command Centre provides real-time service dashboards through the Difenda C3 portal and delivers regular operational debriefs as part of the standard MXDR for EDR offering.

A key differentiator of the Difenda MXDR for EDR service is that a remote incident response retainer is included as part of the core service. There is no monthly cost for the retainer. Customers pay only time and materials if the service is invoked.

The retainer provides customers access to the Difenda's remote incident response service, which includes a priority response time and a preferred hourly rate.

If invoked by the customer, Difenda will:

PROVIDE PRIORITY RESPONSE TO BREACHES OR POTENTIAL BREACHES; AND

ESTABLISH A CYBER INCIDENT COMMAND STRUCTURE:

In the event of a breach or potential breach, establish a Cyber Incident Command Structure which will consult with and advise the customer's Cybersecurity Incident Response Team (CSIRT) to resolve the breach in a manner that mitigates risk and liability to the customer; and

PROVIDE A DETAILED POST-INCIDENT DOCUMENT DESCRIBING:

- The actions taken by Difenda including the timing of those actions
- Results of the investigation
- Recommended next steps to prevent or mitigate the breach or potential breach from recurring

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

DIFENDA SHIELD FEATURES

Account Team

Ready to support you during your entire Difenda Shield journey, your assigned account team gets to know your team and your business.

Every Difenda Shield customer will have a:

Customer Success Manager (CSM) who works tirelessly to ensure Difenda's services always meet your business objectives

Technical Account Manager (TAM) that understands the technical and operational intricacies of your environment to provide the tailored guidance for your Difenda Shield services

Project Management Office

Coordinating complex security operations activities for Difenda's enterprise customers around the globe requires consistency and precision. At the heart of Difenda's operations is a Project Management Office (PMO) that keeps things running smoothly at all times.

Operational Cadence

From the very first kick-off meeting, Difenda stays in sync with customers through biweekly operational meetings for the duration of services. Difenda works with customers to set a mutually-agreeable cadence to meet regularly for planning, reporting, support, and escalations.

Difenda Shield Portal

The Difenda Shield delivers a clear and flexible customer experience through the Difenda Shield portal, our secure cloud-based SecOps service application. Key features of the portal include:

- A convenient single pane of glass for all services in the Shield
- Asset discovery capabilities through for IT assets
- Real-time threat reports, including historical data for audit and compliance
- An integrated service request system for support and change requests
- Powerful and flexible dashboarding and reporting capabilities

DIFENDA

www.difenda.com | sales@difenda.com | 1.866.252.2103

Member of Microsoft Intelligent Security Association

Microsoft

Microsoft Solutions Partner
Security
Specialist
Cloud Security
Threat Protection

WANT TO KNOW MORE ABOUT HOW YOU CAN ACHIEVE MAXIMUM SECURITY AND VISIBILITY WITH DIFENDA MXDR FOR EDR?

CHECK OUT OUR MXDR FOR EDR RESOURCES!

CASE STUDY: MXDR FOR EDR

How This Tourism Organization Built a Global Endpoint Protection Program with Difenda MXDR for EDR—increasing their visibility, building policy and deploying thousands of new assets.

READ IT NOW

MXDR FOR EDR—ONE PAGER

GET YOUR COPY!

MXDR FOR IT

Managed Extended Detection & Response For IT

Learn about MXDR For IT

DIFENDA

www.difenda.com | sales@difenda.com | 1.866.252.2103

Member of Microsoft Intelligent Security Association

Microsoft Solutions Partner
Security
Specialist
Cloud Security
Threat Protection

DIFENDA

Unparalleled Expertise, Microsoft Trusted

When it comes to choosing a security partner, you need a partner who is an expert in the field and who has earned the trust of Microsoft. At Difenda, we pride ourselves on our deep understanding of Microsoft security tools and our ability to help our customers optimize them for maximum protection.

As one of the original MSSPs to join the Microsoft Intelligent Security Association (MISA), we have a long-standing relationship with Microsoft that allows us to stay ahead of the curve on security threats. We are also one of only a handful of companies to receive the Microsoft Advanced Specialization in Threat Protection and Advanced Specialization in Cloud Security, which is a testament to our high level of expertise. When you partner with Difenda, you can be confident that you are getting unrivaled expertise and support from a team that is dedicated to helping you mitigate threats and reduce risk.

And we can put that expertise to work for you!

SPEAK TO A MICROSOFT SECURITY EXPERT TODAY

1.866.252.2103
sales@difenda.con