Managed Endpoint Detection & Response (M-EDR)

DIFENDA

Microsoft Partner
Microsoft

Gold Security
Gold Cloud Platform
Gold Application Development
Advanced Specialization - Threat Protection

Member of
Microsoft Intelligent Security Association
Microsoft

Managed Endpoint Detection and Response

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 Managed 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

Microsoft Partner
Microsoft
Gold Security
Gold Cloud Platform
Gold Application Development
Advanced Specialization - Threat Protection

Member of
Microsoft Intelligent Security Association
Microsoft

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.

These functional areas are:

IDENTIFY

An 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 partiallyor fully mitigate risks.

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.

RECOVER

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

Major Challenges Organizations Face with Effective Security Operations

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.

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

Process: Developing, implementing, monitoring, and managing security operations to best practices.

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

Managed Endpoint Detection & Response (M-EDR) is a comprehensive solution offered by Difenda which addresses all three of these challenges, in the first four of the five functional areas, across the entire organization. The M-EDR service 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 M-EDR is comprised of several components which are aligned to the NIST framework as follows:

Threat Profiling

Threat Hunting

Threat Defense

Threat Response
by Difenda Cyber Command Center (C3)

In addition to the above security operation capabilities, Difenda M-EDR offering provides forensic, audit, and compliance benefits by reliably capturing and securely retaining all relevant security event information for future use.

DIFENDA www.difenda.com | sales@difenda.com | 1-866-252-2103

M-EDR

Key Features of Difenda M-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 Defense

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 Defense

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 M-EDR service is Difenda's ATT&CK driven development methodology and automated response capabilities. As part of the ATT&CK driven development process, senior 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.

The Difenda Shield also draws real-time information from several open source and proprietary threat intelligence feeds to supplement our capability to recognize known-bad actors and suspiciously-behaving devices, users, and applications.

Threat hunting is the proactive process of systematically seeking out potential threats before an incident occurs. This is in contrast to the reactive process of security monitoring, where investigation begins after a potential incident has been detected. Difenda experts use a mix of manual and automated threat hunting techniques to form both ongoing and ad hoc, campaign-based hunting programs.

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

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.

A key differentiator of the Difenda M-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:

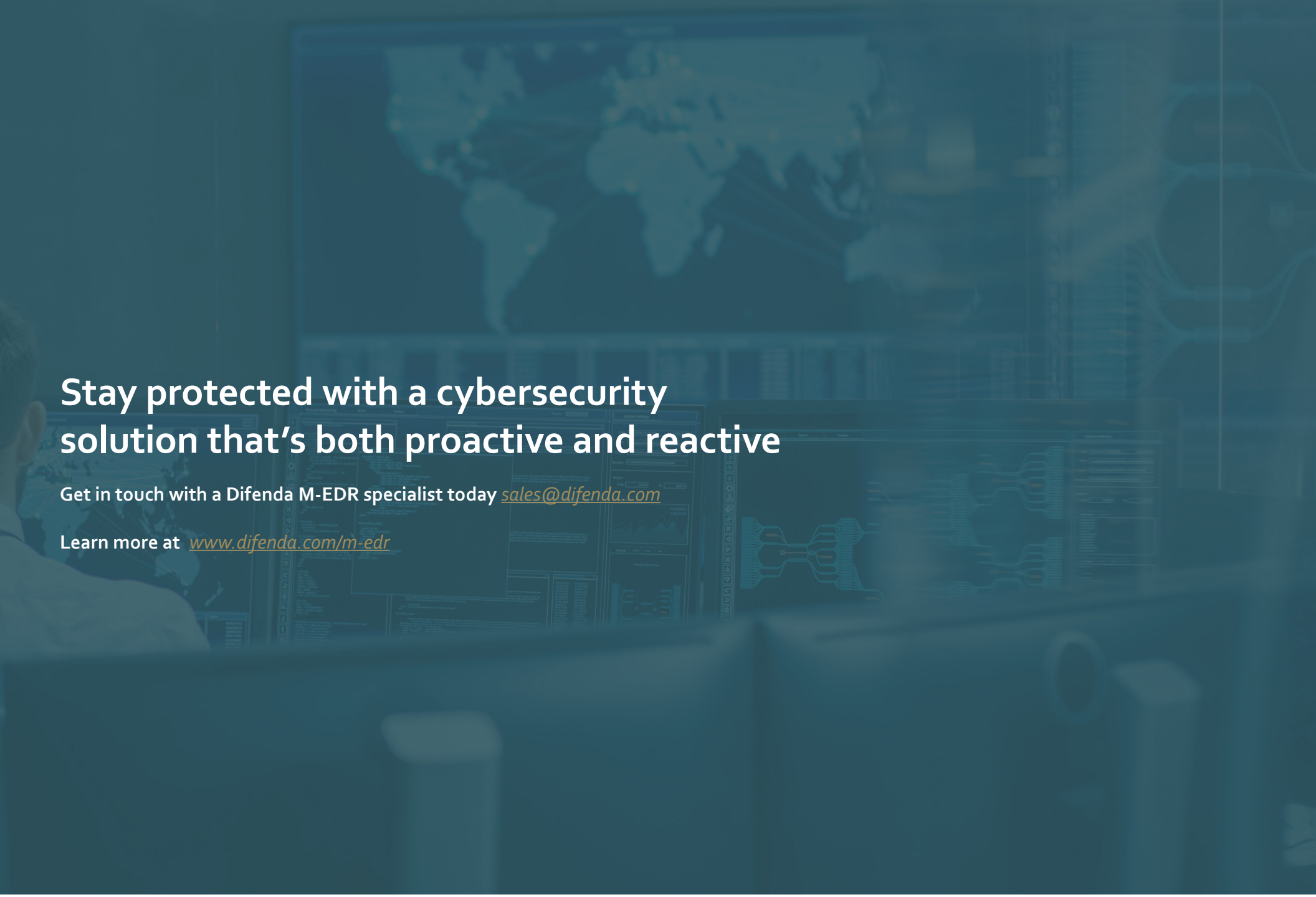
Provide priority response to breaches or potential breaches; and

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.



Stay protected with a cybersecurity solution that's both proactive and reactive

Get in touch with a Difenda M-EDR specialist today *sales@difenda.com*

Learn more at *www.difenda.com/m-edr*