Managed Security Information & Event Management (M-SIEM)

DIFENDA

Microsoft Partner
Microsoft

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

Member of
Microsoft Intelligent Security Association
Microsoft

Managed Security Information & Event Management

Comprehensive managed threat detection

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.

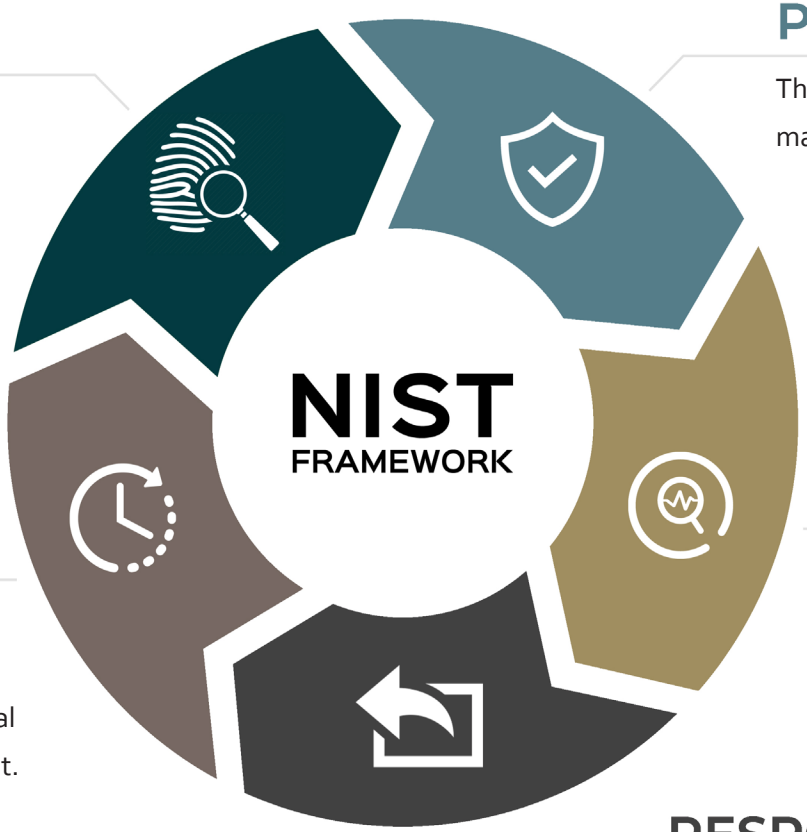
These functional areas are:

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.

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

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 Security Information & Event Management (M-SIEM) is a comprehensive managed threat detection solution offered by Difenda which addresses all three of these challenges, in the first three of the five functional areas, across the entire organization. The M-SIEM 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."

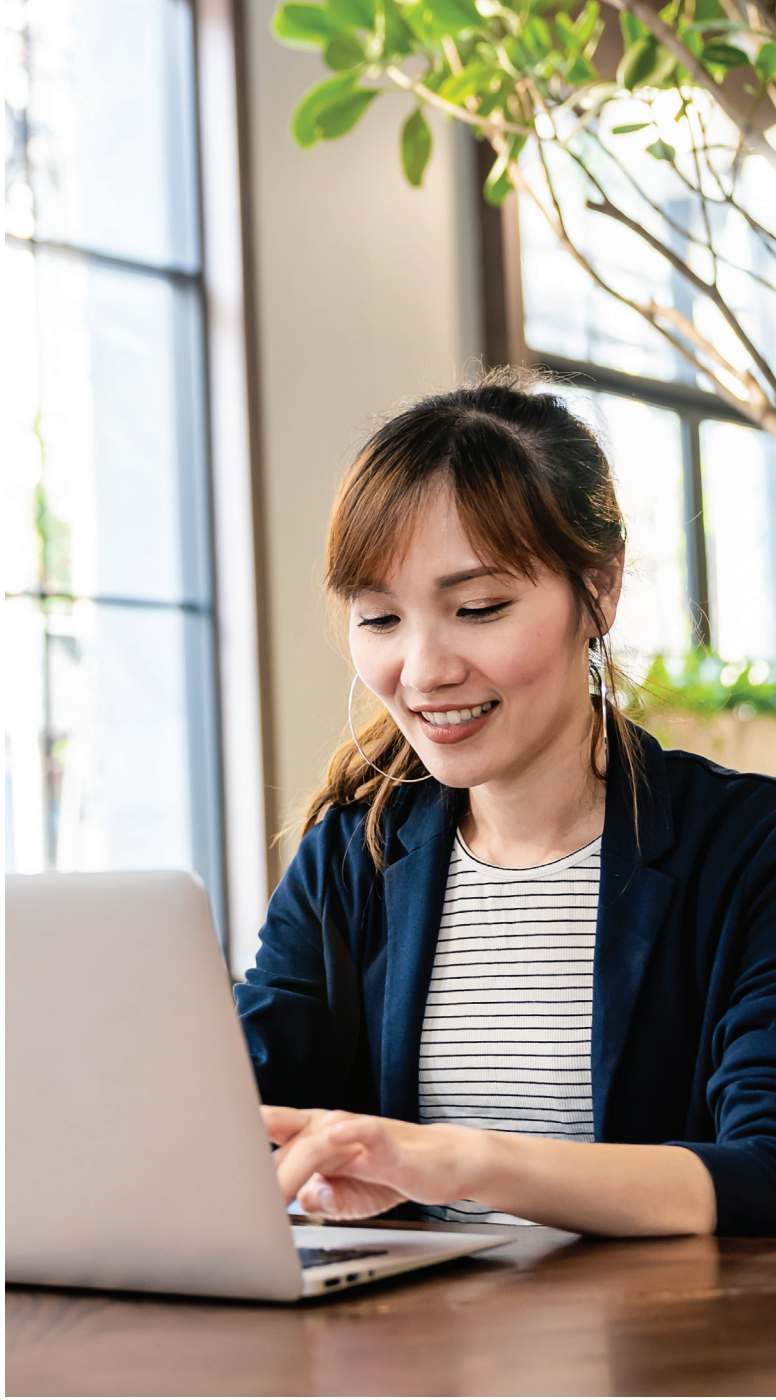
Difenda M-SIEM is comprised of several components which are aligned to the NIST framework as follows:

Threat Profiling

Threat Defense

Threat Hunting

In addition to the above security operation capabilities, Difenda M-SIEM 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

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

Member of
Microsoft Intelligent Security Association
Microsoft

Key Features of Difenda M-SIEM

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.

Threat Detection

As part of M-SIEM, Difenda configures, monitors, optimizes, and manages Microsoft Sentinel's threat detection capabilities. Key components of threat detection include:

Analytics Rules:

- Microsoft Sentinel out-of-the-box Analytics Rules
- Difenda's proprietary shared use case library
- Custom Analytics Rules, as requested by customers
- Additional detection resources from the Microsoft development community

Machine Learning:

- Microsoft Sentinel Fusion
- User and Entity Behavioral Analytics

Threat Hunting

Difenda leverages security information and event management (SIEM) technologies, powered by Microsoft Sentinel, to collect, analyze and detect threats. Difenda's M-SIEM service SIEM model is designed to support reliable, consistent, and cost-effective service delivery.

Core to the M-SIEM service is Difenda's ATT&CK driven development methodology. 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 (SOAR) framework and industry standards (i.e., NIST 800-61) to investigate, document, and communicate threats in a consistent. Difenda's SOAR framework is based on ServiceNow, Azure Automation, and Logic Apps services.

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-be-having 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-SIEM offering.

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

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

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

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