MANAGED SECURITY INFORMATION AND EVENT MANAGEMENT

DIFENDA M-SIEM

DIFENDA

Member of
Microsoft Intelligent Security Association
Microsoft

Microsoft
Solutions Partner
Security
Specialist
Cloud Security
Threat Protection

MANAGED SECURITY INFORMATION AND EVENT MANAGEMENT

✓ COMBINE MANUAL AND AUTOMATED THREAT DETECTION TECHNIQUES TO IMPROVE SECURITY POSTURE

The days of set-and-forget security are behind us. Difenda leverages security information and event management (SIEM) technologies, powered by Microsoft Sentinel, to collect, analyze and detect threats. Difenda M-SIEM service model is designed to support reliable, consistent, and cost-effective service deliver.

THE STATE OF SIEM SECURITY

CYBERCRIME. INCREASING COMPLEX ATTACKS. GROWING THREAT LANDSCAPE. SHORTAGE OF SECURITY PROFESSIONALS.

These all represent clear and present dangers to your customers' networks, businesses, and personally identifiable information. The days of set-and-forget security are behind us.

In its early days, SIEM was shaped by new compliance drivers that dominated the 90's and early 2000's. In more recent years, SIEM has evolved to handle the convergence of platforms while accelerating threat detection against sophisticated ransomware and malware.

The security landscape had increased dramatically with the proliferation of connected devices, cloud adoption and a growing remote workforce. Cybercriminals have taken this opportunity to increase and improve their attack methodology.

Today, M-SIEM represents an evolution of log management that provides security teams with more information from the security environment. The challenge is finding a solution that casts a wider net with more scalability, visibility and automation.

OVERCOME TODAYS MOST COMMON CHALLENGES

25 incidents are reviewed by the average analyst every day.

66% of security professionals believe there aren't enough qualified analysts to handle the increasing volume of security threats.

67% of security leaders feel overwhelmed by the security landscape.

WHAT'S INCLUDED

- ✓ Threat Profiling
- ✓ Threat Hunting
- ✓ Threat Defense
- ✓ Log Management

COMPREHENSIVE MANAGED THREAT PROTECTION

Leverage Difenda's cybersecurity experts to strengthen your security posture. Improve the security of your business' computer network with real-time automation, monitoring, logging and event alerts. Powered by a combination of Microsoft's security solutions and the Difenda Shield platform, Difenda M-SIEM is an end-to-end process for threat management.

Difenda M-SIEM Outcomes and Impact

- Customized infrastructure and threat intelligence
- Streamline people, processes and technology
- Increased visibility and response capabilities
- Future-proofed platform to continuously tackle advancing technology
- Hybrid security environment promoting further cloud adoption
- Meet complex operational requirements with ease

COMPLIANCE

If you're operating in a highly regulated sector, like the public sector, healthcare, or finance, you need to be aware of the existing compliance laws that are applicable to your specific industry. Difenda M-SIEM helps you comply with the security standards and regulations that apply to your industry, to avoid costly fines and penalties.

Most regulations and standards require companies to log all events and review them in a timely manner, so they can take appropriate actions if needed.

By leveraging SIEM Software, your security team is able to track events concerning your company's information security, such as potential data breaches, helping you to react faster.

Even though most of the regulations do not explicitly mandate the use of SIEM software for achieving compliance, SIEM happens to be one of the most effective solutions to cover the security requirements of multiple regulations at once.

Easily comply with the most common compliance frameworks

HIPAA
PCI-DSS
GDPR

To be compliant with most regulations applicable to your organization, Difenda helps:

- Track business critical events
- Evaluate the risk of a data breach event for any of your processes
- Based on the risk level, define which of your events are considered the highest threats
- Keep records of the security events: what happened, exact timing, how was it handled, etc

Why Microsoft Sentinel

MORE THAN JUST A CLOUD FIRST SIEM

Microsoft Sentinel is best for businesses wanting to take their cybersecurity to the next level with enriched investigation and detection with AI.

Designed with automation, integration, extensibility, and ease-of-use in mind and the only cloud-native SIEM / SOAR solution has just put enterprise-grade SOC operations capabilities within reach of organizations of any size.

Microsoft Sentinel provides a bird's-eye view across security networks, alleviating the stress of increasingly sophisticated attacks, alert fatigue, and time-consuming investigations.

MICROSOFT IS INVESTING $20 BILLION ON CYBERSECURITY OVER THE NEXT FIVE YEARS

Do More With Less

Collect

Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.

Detect

Detect previously undetected threats using Microsoft's analytics and threat intelligence.

Investigate

Investigate threats with artificial intelligence, and hunt for suspicious activities at scale.

Automate

Respond to incidents rapidly with built-in orchestration and automation processes.

Microsoft Intelligent Security Association

Microsoft

Microsoft Verified Managed XDR Solution

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.

Go-to partner for Microsoft Sentinel

Difenda is a design partner and Microsoft's top global implementation partner for Sentinel. 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.

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.

CERTIFIED WHERE IT MATTERS MOST

- Microsoft CERTIFIED – INFORMATION PROTECTION ADMINISTRATOR – ASSOCIATE
- Microsoft CERTIFIED – IDENTITY AND ACCESS ADMINISTRATOR – ASSOCIATE
- Microsoft CERTIFIED – SECURITY OPERATIONS ANALYST – ASSOCIATE
- Microsoft CERTIFIED – AZURE SECURITY ENGINEER – ASSOCIATE
- Microsoft CERTIFIED – AZURE ADMINISTRATOR – ASSOCIATE
- Microsoft CERTIFIED – DEVOPS ENGINEER – EXPERT
- Microsoft 365 CERTIFIED – SECURITY ADMINISTRATOR – ASSOCIATE

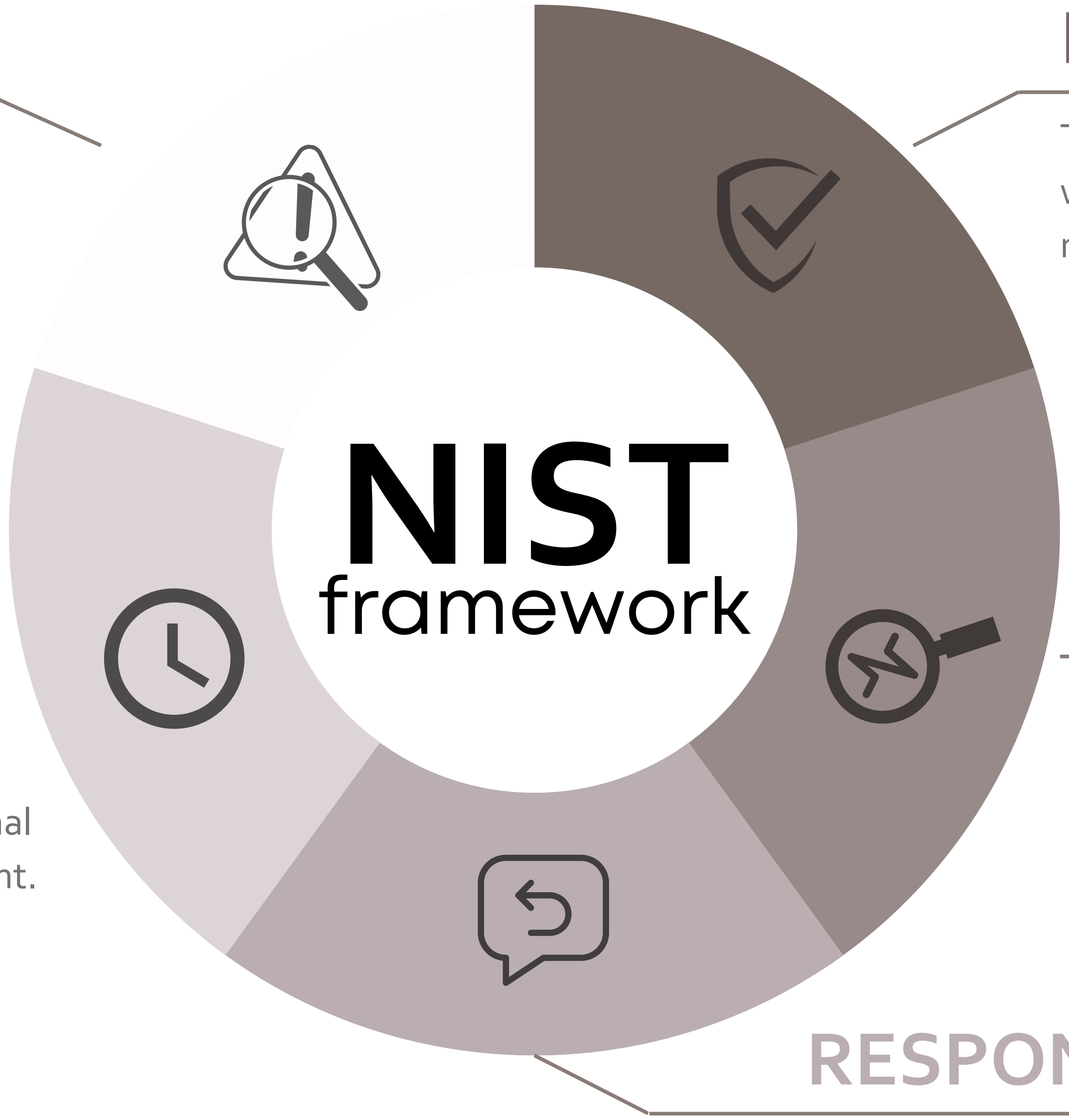
bsi. ISO/IEC 27001 Information Security Management

PCI DSS COMPLIANT

AICPA SOC

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.

DETECT

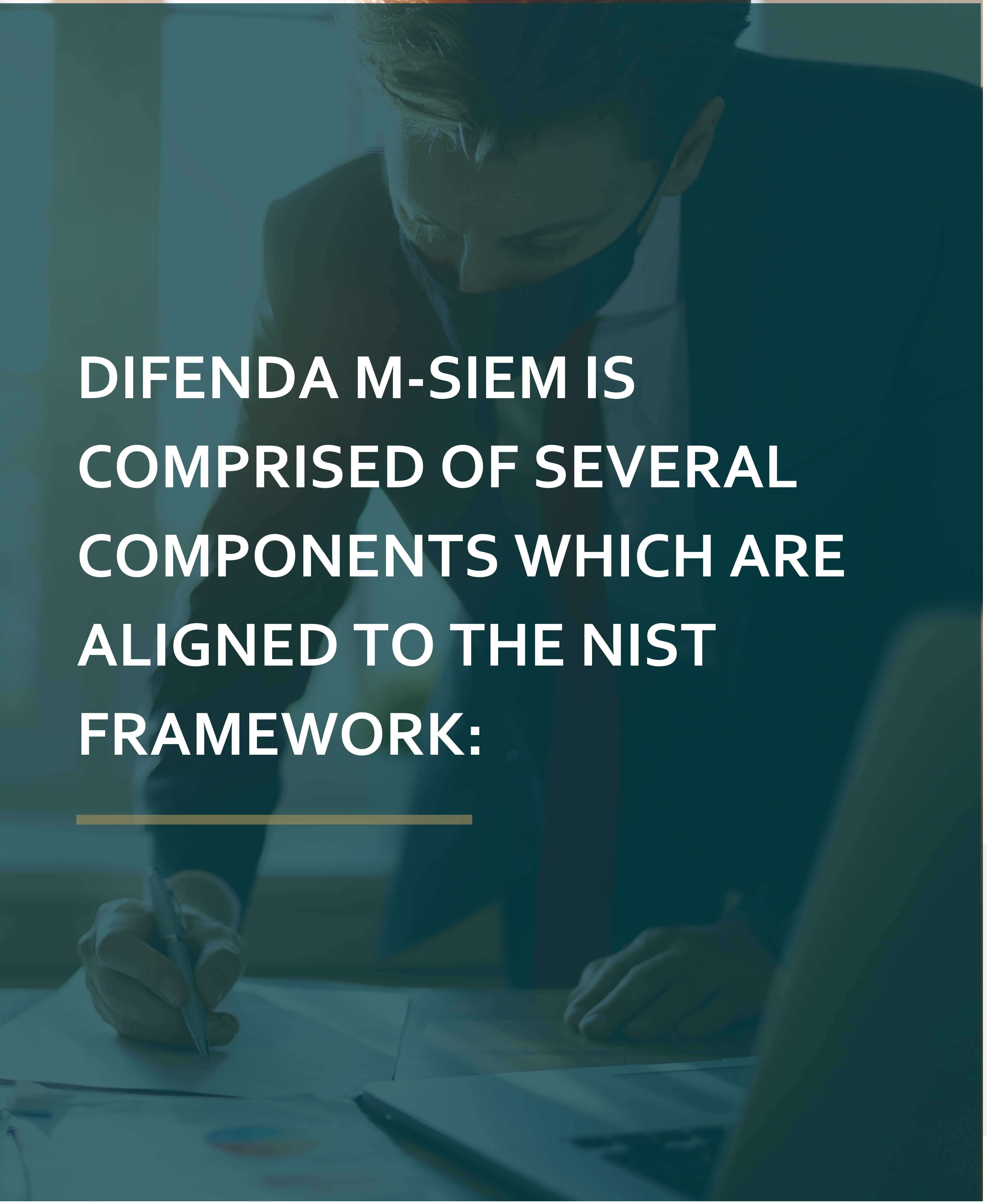
The capability and process for timely discovery of an incident.

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 M-SIEM IS COMPRISED OF SEVERAL COMPONENTS WHICH ARE ALIGNED TO THE NIST FRAMEWORK:

THREAT PROFILING

THREAT HUNTING

THREAT DEFENSE

LOG MANAGEMENT
by Difenda Cyber Command Center (C3)

In addition to the above security operation capabilities, Difenda M-SIEM provides forensic, audit, and compliance benefits. We reliably capture and securely retain all relevant security event information for future use.

DON'T SPEND WEEKS WITHOUT KNOWING AN ATTACK IS IN PROGRESS

BENEFITS OF M-SIEM

- Improved security data: SIEMs aggregate and normalize your security data, improving the potential for it to be analyzed and used in incident response workflows. The SIEM can then store normalized security data for extended analytics and reporting. This not only increases visibility but may also help with compliance.
- Increased visibility: SIEM systems mitigate the risk of threat actors hiding in dark spaces within your network because they are collecting security event data from everywhere in the network. It then works to analyze this data, effectively highlighting those dark spaces.
- Improved compliance: SIEM will help you meet demanding compliance requirements. It does this by improving your security posture and helping monitor your organizational environment.
- Fewer false positive alerts: Almost 50% of your security alerts are just “noise”. Machine learning technology can reduce the amount of time your team is spending on false positives, by only highlighting legitimate threats.
- Dedicated Support: With SIEM as a service, your account is assigned a dedicated account team to ensure your valued outcomes are always in focus.

STREAMLINE PEOPLE, PROCESSES AND TECHNOLOGY

Managed Security information and Event Management is a comprehensive solution offered by Difenda which addresses challenges across the entire organization to mitigate the potential impact of a breach. M-SIEM 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."

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.

KEY FEATURES OF DIFENDA M-SIEM

ASSET THREAT PROFILING

Develop a thorough understanding of your organization’s attack surface, critical infrastructure, sensitive data, and operational processes. This gives security operations staff the best chance to be successful by helping them to understand the customer’s real business problems and risk. Difenda helps you think like an adversary to prioritize 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

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.

THE DIFENDA DIFFERENCE

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.

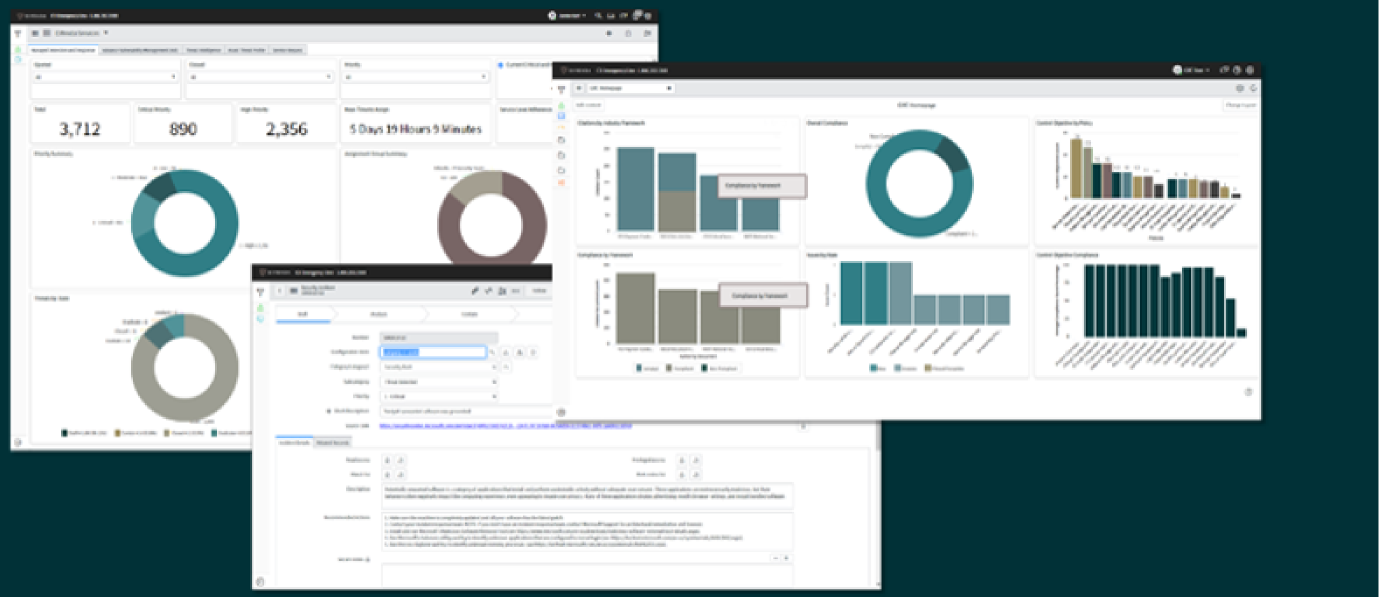
Operational Cadence

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.

THE DIFENDA SHIELD PORTAL

The Difenda Shield Portal is a powerful web-based platform where you can interact with various aspects of threats, make changes to requests, and gain enhanced visibility into your cybersecurity solutions. Our Difenda Shield Dashboards Allow You To:

✓ Collect daily trend data
✓ Provide a summary of key information to improve
✓ decision making
Enable end-user dashboard parameter selection



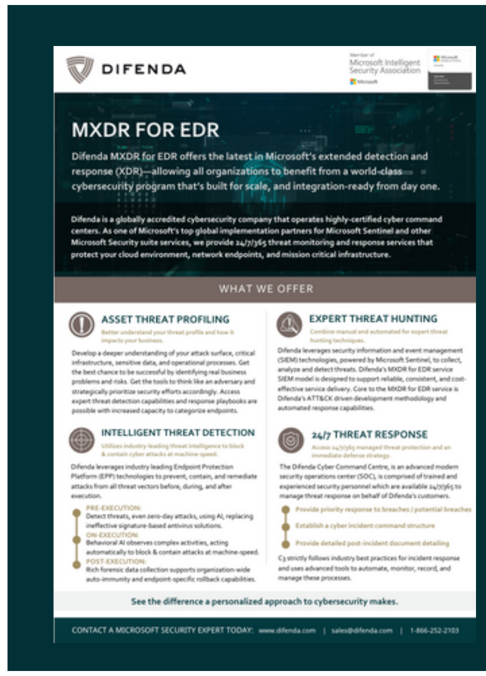
DISCOVER MORE ABOUT WHAT YOU CAN ACHIEVE MAXIMUM SECURITY AND VISIBILITY WITH DIFENDA M-SIEM.

CHECK OUT OUR M-SIEM RESOURCES!

CASE STUDY: M-SIEM

How this firm eliminates operational challenges from legacy security stack with Difenda M-SIEM

READ IT NOW



DIFENDA

Member of Microsoft Intelligent Security Association

Microsoft

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

Utilizes 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 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

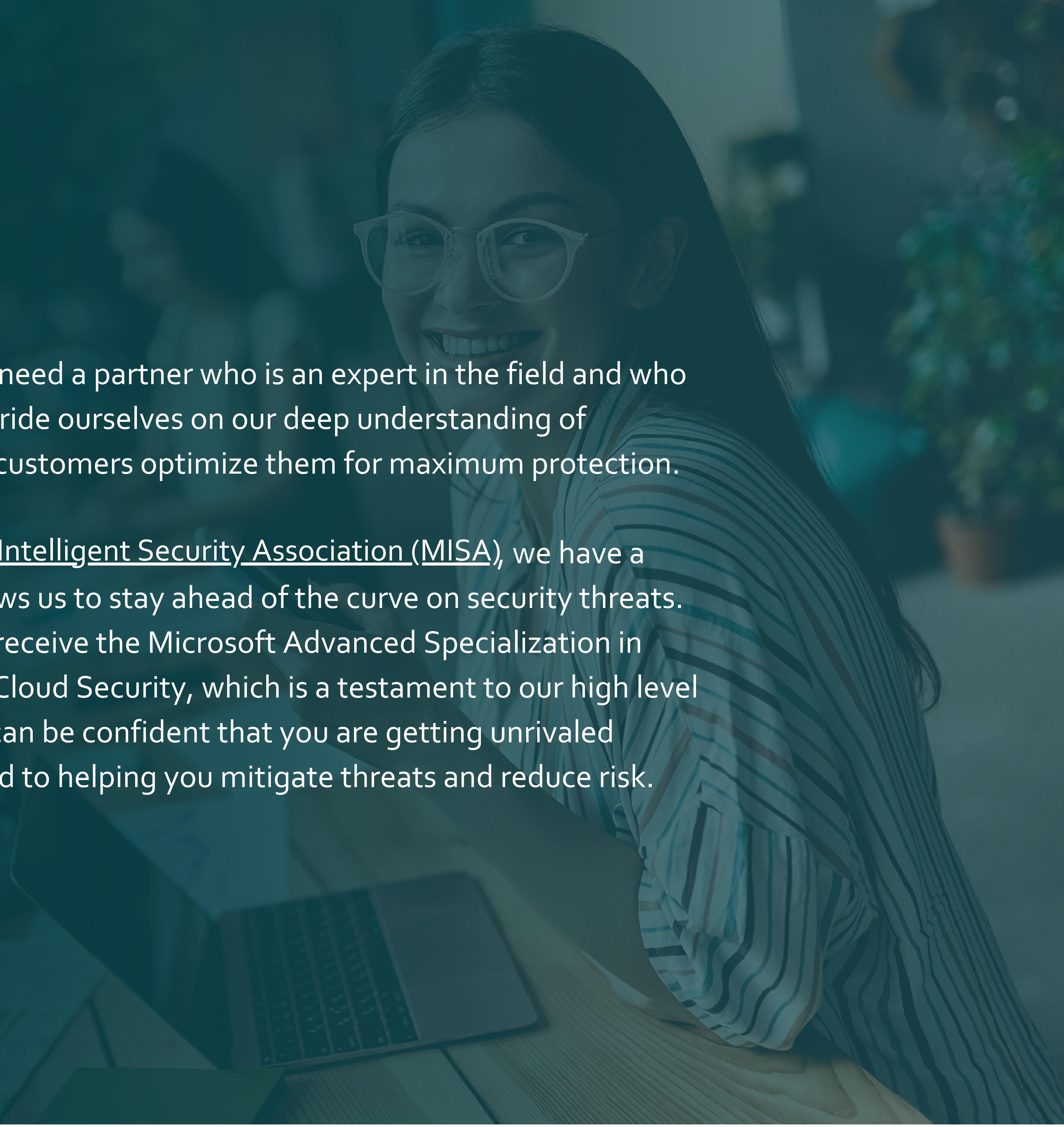
M-SIEM—ONE PAGER

GET YOUR COPY!

MXDR FOR IT

Managed Extended Detection & Response For IT

Learn about MXDR For IT



DIFENDA

Cybersecurity First, Microsoft Only.

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 SECURITY EXPERT TODAY

1.866.252.2103
sales@difenda.com

Microsoft Intelligent
Security Association

Microsoft

Microsoft Verified
Managed XDR Solution

Microsoft
Solutions Partner
Security

Specialist
Cloud Security
Threat Protection