Operationalize Microsoft Sentinel

Whether you’re deploying it from scratch, finishing a partial deployment, or just giving your existing environment a tune-up, Difenda can assist you with optimizing Microsoft Sentinel throughout your security journey. Difenda takes a Microsoft only approach to cybersecurity which allows for our experts to focus on creating the outcomes you desire.
More Than Just a Cloud-First SIEM

SIEM technologies have been slowly and consistently improving since first introduced, but Microsoft Sentinel represents the first major leap forward in years. Designed with scale, automation, integration, extensibility, and ease-of-use in mind, the only cloud-native SIEM / SOAR solution has just put enterprise-grade SOC operations capabilities within reach of organizations of any size.

Organizations that invest in other components of the Microsoft Security platform, such as Microsoft Defender, can now leverage Microsoft Sentinel at a fraction of the total cost of ownership compared to other best-in-class SIEM products because of free / discounted fees and operational sustainability through automation.
Microsoft Sentinel in Action

Difenda is a trusted Microsoft partner and a part of an invitation-only incubator within Microsoft, giving us private preview access to products and allowing us to give feedback directly to Microsoft development teams to further enhance their solutions' capabilities.

After many successful engagements globally, Microsoft has come to trust Difenda with its largest and most complex customer projects.
Solving Customer Challenges

Rolling out any solution which requires deploying software across the environment can pose significant operational and technical challenges. These are further complicated by the potential for serious consequences for an incomplete or failed deployment.

Some of the most common challenges our customers have faced include:

- Incomplete requirements gathering
- Designs not in alignment with requirements
- Stalled / incomplete rollout
- Overworked and under-skilled information staff not motivated to adapt
- Staff lacking product experience and training
- Missing or unaware of integration or features
- Lack of automation capabilities
- Uncertainty of program efficacy

Organizations can reduce these risks and ensure the smoothest possible transition with guidance from experts who have been there and done that.

Our Microsoft Certifications:

www.difenda.com | sales@difenda.com | 1.866.252.2103
Customers working with Difenda can expect:

- Rapid Implementation
- Proven Experience
- Global Scalability
- Trusted by Microsoft

Microsoft Sentinel Outcome and Impact:

- Increase enterprise-wide visibility and response capabilities
- Address operational capability gaps in your current program
- Best-practice design and deployment
- Increase team productivity with log source integration and optimization
- Future-proofed platform to continuously tackle advancing technology
- Increased ROI by greatly reducing operating costs
Common activities of a Microsoft Sentinel professional services engagement include:

**Preparation**
- Requirements discovery and documentation
- Environment discovery and documentation
- Initial resource and schedule planning

**Design**
- Environment and requirements analysis
- Development, documentation, review, and approval of technical design

**Deployment**
- Azure tenant creation, if necessary
- Log source onboarding using Microsoft tools (e.g., SCCM, Intune, GPO)

**Configuration**
- Enabling and configuration of product capabilities (e.g., Analytics, Workbooks, hunting queries, UEBA, Jupyter Notebooks, threat intelligence, automations)
- Tuning to Difenda recommendations, Microsoft best practices, and industry standards

Bolster Your Security, Not Your Workload
Maximize your security with Difenda’s Managed SIEM, powered by Microsoft Sentinel.

Step up to Microsoft Defender get

GET FULL VISIBILITY

Faster detection and response starts now with Difenda MXDR.

Powered by: Microsoft Sentinel + Microsoft Defender for Endpoint

Development and Integrations
- Creation and customization of dashboards and reports
- Custom detection, including threat hunt queries and Analytics Rules
- Development of response automations
- Integration support with Microsoft Security tools and beyond!
  - Azure Active Directory
  - Microsoft Defender for Cloud
  - Microsoft Defender for Cloud Apps
  - Microsoft Defender for Endpoint
  - Microsoft Defender for Identity
  - Microsoft Defender for IoT
  - Microsoft Defender for Office 365
  - Microsoft Defender for Servers
  - Microsoft Information Protection
  - DLP
  - CASB
  - CMDB
  - IAM / PAM
  - Other SIEM / SOAR solutions
  - Threat intelligence feeds
  - Vulnerability Scanners

Enablement
- Product, project, process, and design documentation
- Knowledge transfer sessions
- Project management services
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 WITH A SECURITY EXPERT

1.866.252.2103
sales@difenda.com