



ACCELERATE YOUR JOURNEY

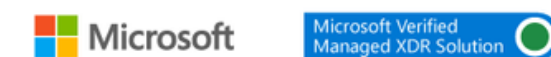
WITH MICROSOFT SENTINEL
PROFESSIONAL SERVICES

WHO WE ARE

As the winner of Microsoft Canada's Security Impact Award, Difenda stands as the most trusted provider of Microsoft Security services. Difenda accelerates, performs, and validates your Microsoft Security technology, meeting you wherever you are on your cybersecurity journey to maximize your outcomes.



Microsoft Intelligent
Security Association



ARE YOU LOOKING TO GAIN GREATER VISIBILITY TO GENERATE DEEPER INSIGHTS INTO YOUR SECURITY ENVIRONMENT?

YOUR JOURNEY STARTS HERE!

Accelerate your cybersecurity journey confidently with Difenda and Microsoft Sentinel, a cloud-native SIEM solution. Overcome security roadblocks by gaining enterprise-wide visibility into your security environment, maximizing your Microsoft Investment, and automating your defences. Get one step closer to a mature security posture by relieving overworked staff, bridging skill gaps, and ensuring seamless compliance.

Introducing Difenda: Your Trusted Microsoft Sentinel Partner



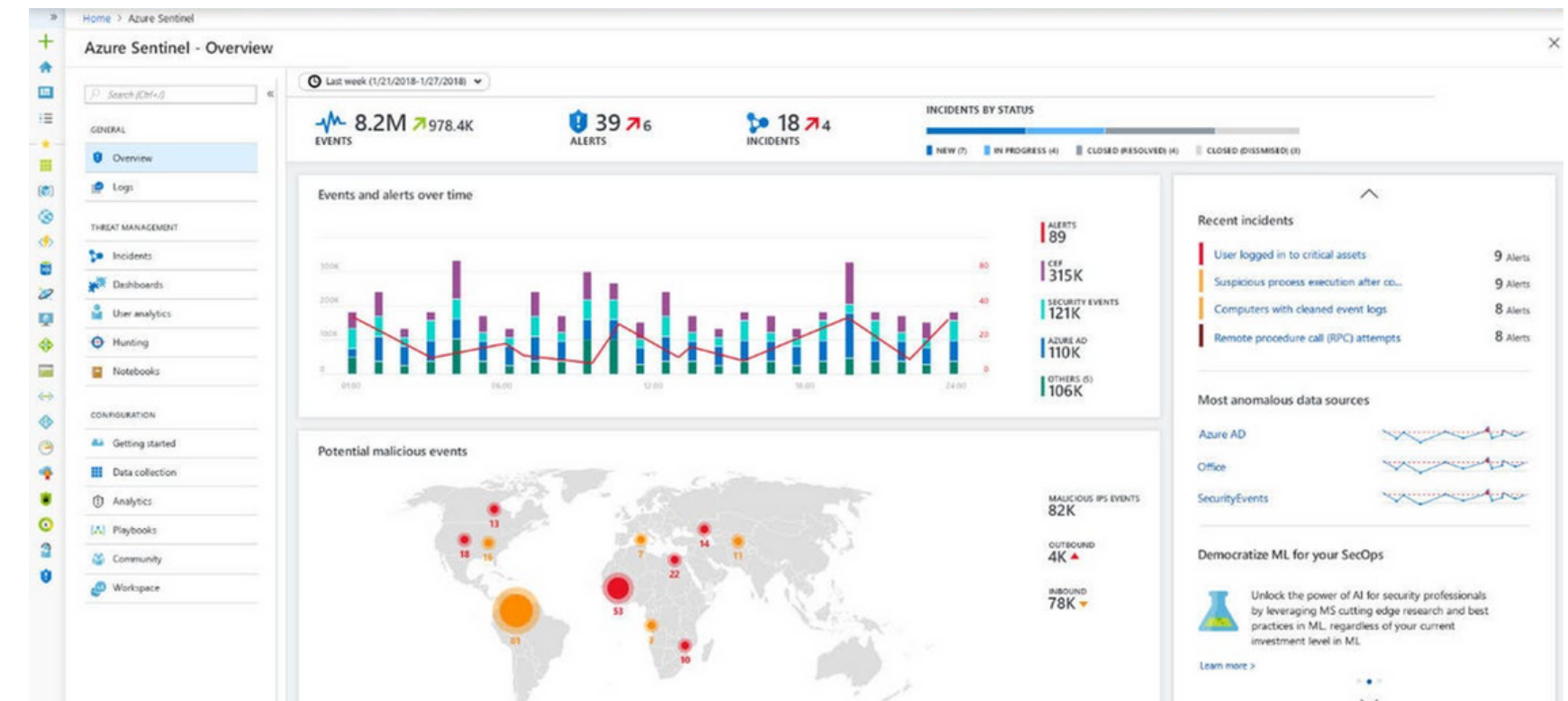
As the winner of Microsoft Canada's Security Impact Award, Difenda stands as the most trusted provider of Microsoft Security services. Only Difenda delivers true end-to-end security operations through professional and managed services focused on cybersecurity for where you are on your journey.

With Difenda's Microsoft Sentinel Professional Services, our Microsoft Security experts deploy Microsoft Sentinel within your designated Azure subscription, coupled with seamless configuration of native data connectors, analytic rules, and workbooks.

As experts in the field, we understand that each organization's security adventure is unique, which is why we kickstart the process by meticulously planning the implementation process. This ebook will help you understand how you can accelerate your security maturity and expand your horizons for what's possible with your Microsoft Security investment starting with Difenda.

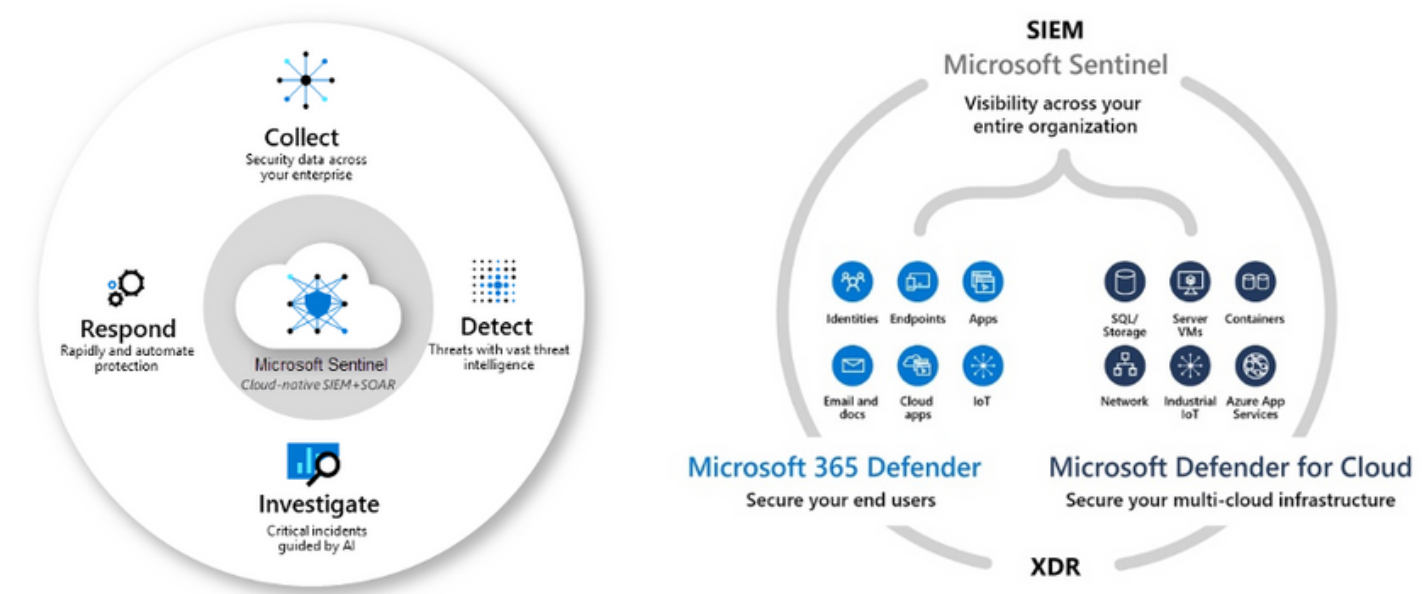
MICROSOFT SENTINEL OVERVIEW


Microsoft Sentinel is a cloud-native Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solution provided by Microsoft. It is designed to help organizations gain insights into their security posture, detect and respond to threats effectively, and provide a centralized platform for managing security incidents.



ENHANCE VISIBILITY

Microsoft Sentinel transcends the traditional boundaries of a cloud-first SIEM (Security Information and Event Management). Delivering a comprehensive suite of advanced capabilities, the platform provides the visibility and data needed to swiftly remediate threats and safeguard your digital landscape with unparalleled efficacy.



A man with a beard and glasses, wearing a white long-sleeved shirt, is sitting at a desk and working on a laptop. He is looking down at the screen. In the background, another person is visible, also working. The scene is set in a bright, modern office environment.

Let Difenda Be Your Guide: Embark On A 4-6 Week Journey to Microsoft Sentinel Design and Implementation

Looking to extend your security investment or are you unsure where to begin your Microsoft Security journey? With Difenda, Microsoft Sentinel Design and Implementation becomes a 5-step process!

1. Planning

As part of the pre-sales process, Difenda collaborates closely with you to understand both the technical and business requirements. By aligning these requirements, we clearly define the expected output for the engagement.

2. Customized Setup and Deployment

Difenda's experts will design, install, and configure Microsoft Sentinel based on the defined scope, ensuring you get the business outcomes you desire.

3. Quality Assurance and Performance Testing

After configuring the system, we take proactive measures to validate that all in-scope native log sources, associated analytic rules, and workbooks are functioning as designed.

4. Training And Knowledge Transfer

We provide collaborative virtual knowledge transfer and a technical overview workshop for your identified team members. Our aim is to ensure you have the necessary expertise to maximize the potential of Microsoft Sentinel.

5. Completed Sentinel Build Book

We will provide you with a comprehensive Build Book which will assist you in leveraging the newfound capabilities of your enhanced security solution.

WHY DIFENDA FOR SENTINEL DEPLOYMENT?



Difenda's Microsoft Sentinel Professional Services stand out by providing expert design and seamless implementation of the Microsoft Sentinel platform, harnessing the power of your native licensing capabilities. What sets us apart is our commitment to optimizing your investment through fine-tuning the configuration, ensuring you only pay for essential security log ingest. With Difenda, you gain a tailored and cost-effective solution, empowering your organization with unparalleled security and peace of mind.

FUEL YOUR JOURNEY



Enterprise-Wide
Visibility Into Your
Security Environment.



Save Time And
Resources With A
Centralized Platform.



Maximize Microsoft
Security ROI With
Out-Of-The-Box With
Sentinel Benefits.



Cut Costs By Ensuring
Efficient Payment For
Security Log Ingest.



Ensure Compliance
With Audit
Requirements.

TECHNICAL SCOPE

Configure, tune and validate:

Up to 5 native Microsoft data connectors	✓
Up to 5 out-of-the-box analytic rules	✓
Up to 3 out-of-the-box workbooks	✓
1 non-Microsoft log source using syslog integration	✓
1 custom analytic rule for in-scope log sources	✓
1 custom workbook with up to 3 elements	✓



Sample Use Case

Problem:

- Challenges in detecting potential security threats based on Indicators of Compromise (IoCs).

Solution:

- Difenda establishes a centralized log management system, aggregating and correlating data from various sources.
- With customized configurations, Difenda enabled real-time alerting for suspicious activities.

Case Study

Transform Your Cybersecurity Defense: Discover How Difenda's Microsoft Sentinel Professional Services Amplified Protection and Productivity For This IT Company!

[READ THE FULL STORY](#)



TACKLING ROADBLOCKS

Our mission is to provide the technology, expertise, and support needed to create a secure, resilient, and evolving security environment. Our security operations team creates custom cybersecurity services, powered exclusively by Microsoft's Security product platform for 24/7/365 coverage and relentlessly defends our clients against cyber risks and delivers business outcomes.

Overcome the most common challenges:

- Comprehensive requirements gathering
- Lack of visibility into your security environment
- Alignment of Sentinel design with industry requirements
- Overworked and under-skilled staff
- Meeting compliance and audit requirements
- Utilizing your Microsoft Investment to its fullest potential

Real People. Real Solutions.

CERTIFIED WHERE IT MATTERS MOST



HOW MICROSOFT SENTINEL ALIGNS WITH YOUR BUSINESS GOALS

Microsoft Sentinel is your bird's-eye view across the enterprise alleviating the stress of increasingly sophisticated attacks, increasing volumes of alerts, and long resolution time frames. Leveraging existing Microsoft licenses, organizations can maximize their investment and eliminate the need for custom configurations. With its scalability and flexibility, Sentinel caters to businesses of all sizes, empowering them to protect their valuable assets and sensitive data, ensuring a secure future and peace of mind.



The Advantages of Microsoft Sentinel for Existing Microsoft Security Customers

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.

FUNDING OPPORTUNITIES

You could be missing out on funding provided to some customers by our good friends at Microsoft!

[DOWNLOAD OUR GUIDE](#)

Maximize your security with
Difenda's **Managed SIEM**, powered
by Microsoft Sentinel.

TAKE THE NEXT STEP
TOWARD SECURITY
MATURITY



M-SIEM
Managed SIEM

SET UP MICROSOFT DEFENDER FOR FULL VISIBILITY

Expand the potential of your security resources with MXDR.



MXDR
Managed Extended
Detection and Response

Powered by:



Microsoft Sentinel + Microsoft
Defender for Endpoint

WE WANT TO BE A PART OF YOUR JOURNEY

Difenda is a Sec-Ops-As-A-Service company that takes a cybersecurity-first, Microsoft-only approach to solving today's toughest cybersecurity challenges. Our security operations team creates custom cybersecurity services, powered exclusively by Microsoft's Security product platform for 24/7/365 coverage. Only Difenda delivers true end-to-end security operations through professional and managed services focused on cybersecurity for where you are on your journey.

Difenda believes in delivering outcome-driven services that meet you right where you are on your cybersecurity journey. Our goal is to expand the horizons of what's possible in the cybersecurity space by mapping clients' outcomes as much as possible back to their current Microsoft Security tools, effectively enabling them to do more with their security investment.

As the winner of Microsoft Canada's Security Impact Award, Difenda stands as the most trusted provider of Microsoft Security services. We have a tenured history as one of the first MSSPs to join the Microsoft Intelligent Security Association (MISA). Our dedication to excellence is further exemplified by our status as a Microsoft Solutions Partner for Security and Microsoft MSSP. We have also earned MXDR verified solution status and hold Microsoft Specializations in Threat Protection and Cloud Security.

We want to put that expertise to work for you!

Take the Next Step Towards a Secure Future

1.866.252.2103 | sales@difenda.com

WWW.DIFENDA.COM

