DIFENDA

DIFENDA MXDR FOR IT

POWERED BY MICROSOFT SENTINEL AND THE DEFENDER XDR PLATFORM

REAL BUSINESS VALUE:

MXDR is a comprehensive, cross function solution that addresses the complex security challenges businesses face today:

Cost & Focus:

MXDR is a well-defined, unhidden, controllable cost in your IT spend. Its value is in minimizing risk and eliminating hidden costs, allowing you to focus on your business and bottom line.

Less is More:

Consolidate your patchworked security stack into a single, comprehensive, effective platform. Unifying your security approach only enhances your ability to respond to threats quickly and reduce the risk of a security breach.

Risk-Based Prioritization:

The platform uses advanced analytics and artificial intelligence (AI) capabilities to analyze vast amounts of data in real-time. With data in-hand from assessments, continuous monitoring, and intelligence gathering, risk-focused decisions can be made quickly and effectively.

Organizational Fit:

The platform is designed to support existing, maturing cyber programs and reduce loads on internal teams. It is tailored to meet your specific needs and fill in whatever gaps or weaknesses your current approach to cyber security has. It is designed to scale as your business grows, automating routine security tasks and orchestrating response actions.

Effective Operationalization

Shift theory and conceptual plans into useable, repeatable, and measurable solutions that protect your business every minute of every day. Centralized management becomes possible as data from various sources is routed and processes by a single platform. This enhances

Iterative Innovation:

We collaborate with experts across the industry and validate all emerging trends. We are vigilant in defining and testing modern, innovative solutions to ensure they are effective in the real world. Once proven, we can implement and operationalize the solution quickly and effectively. Further, Microsoft's ongoing investment in research and development of the platform ensures you will stay ahead of emerging threats and security challenges.

DIFENDA'S MXDR PLATFORM - INDUSTRY LEADING AGILITY

As technology evolves, the battle against cyber threats has become increasingly complex and relentless. Enterprises are continuously facing evolving cyber risks that can compromise their sensitive data, disrupt operations, and tarnish their reputation. As cybercriminals become more sophisticated, organizations must adopt agile and comprehensive cybersecurity solutions to safeguard their assets effectively. The Difenda MXDR platform is the innovative security solution businesses need to address these challenges.

Difenda MXDR for IT is designed to integrate into your existing security stack, align with your security team, and immediately enhance their knowledge and effectiveness. We use a tailored, iterative process that allow customers to tune configurations, enhance controls, reduce alert volumes and gain effective control of their environments and infrastructure. Real-time insights are generated through our Difenda Shield Analytics platform, providing security leaders with the data points and dashboards required to drive their cyber strategy.

WHAT IS MXDR FOR IT?

In simple terms MXDR is a mixture of Microsoft security services & software, and Difenda's 24/7/365 Security Operations Service.
Specifically, MXDR is comprised of:

- ·Microsoft Sentinel
- ·Microsoft Defender XDR (Extended Detection and Response)
- ·Difenda Shield, our SecOps-as-a-Service platform
- ·Difenda AIRO: A Difenda developed automated triage and response engine

MODULAR BY DESIGN

The platform is architected for diverse, hybrid environments, that support monitoring all data sources, endpoints, networks, identities, cloud services and applications, to detect anomalous activities and security threats. It employs advanced analytics, machine learning algorithms, and threat intelligence feeds intended to identify suspicious behaviours indicative of cyberattacks or breaches.

Our services are designed to be modular, allowing customers to selectively license services depending on the nature of their environments and infrastructure. Customers can leverage some or all the following managed components:

- SIEM – Managed Microsoft Sentinel
- Microsoft Defender XDR, including Defender for:
  - Endpoint
  - Identity
  - Cloud
  - Office

THE DIFENDA APPROACH

Difenda experts will meet with your security teams and develop a plan based on what you have today and what you may need to fill in existing security gaps.
Our implementation methodology focuses on four specific actionable outcomes:

- **·Threat Profiling: Iterative contextualization of environmental threats.**
- **·Threat Detection: Rapid, 24x7 identification of threats.**
- **·Threat Hunting: Continuous search for new and emerging threats.**
- **·Threat Response: A combination of automated processes and human intervention for effective threat containment.**

In order to achieve this the following is included in each implementation:

- Microsoft Defender XDR Suite
- Microsoft Sentinel
- Microsoft Sentinel Log Source Integration
- Microsoft Sentinel Custom Development (Log Data Connectors, Analytic Rules, Playbooks, etc.)

Also included are the following services supplied by the Difenda Shield platform:

- 24x7x365 MXDR triage and response
- Difenda AIRO: Automated Triage and Response engine (SOAR)
- Difenda Shield Analytics Platform portal and real-time reporting
- Integrated Threat Intelligence, including advisories and bulletins
- Proactive Threat Hunting
- Ongoing Sentinel maintenance, including Log Data Connector, Analytic Rule, and Playbook development
- Remote Incident Response (RIR) retainer
- Dedicated Technical Account Manager (TAM)

ADVANCED TECHNOLOGY FOR SUPERIOR SECURITY: AIRO AND DIFENDA SHIELD

DIFENDA AIRO

DIFENDA SHIELD

AIRO (Automated Incident Response and Orchestration) is an advanced technology developed by Difenda, accessible to all of our Managed Service customers, such as those standing up MXDR. Specifically it integrates into your Microsoft Sentinel instance and works in collaboration with Azure automation services. It leverages threat enrichment, auto-triage, incident scoring, auto-response, and service synchronization to enhance incident response capabilities and streamline security operations. As you implement the MXDR platform and further refine capabilities, AIRO gains access to more information and resources. This additional data enables AIRO to continually improve its ability to detect threats, prioritize incidents, assign scores and respond quickly.

Our Difenda Shield platform is designed to provide customers with a streamlined 'SecOps-as-a-Service' platform comprised of our Cyber Command Center (ISO27001, SOC II Type 2 and PCI Certified) combined with highly automated and orchestrated processes based on proprietary integrations with Microsoft 365 services and other supporting industry-leading security technologies.

WHY DIFENDA

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.

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2023

Microsoft Intelligent Security Association

Microsoft Canada Impact Awards 2023 WINNER