Difenda Managed Detection & Response

FOR OPERATIONAL TECHNOLOGY (OT)

DIFENDA

Microsoft Partner
Microsoft

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

Member of
Microsoft Intelligent Security Association
Microsoft

Offer Overview

Difenda MDR for OT Onboarding

Includes everything in a standalone Microsoft Sentinel Implementation, plus implementation within the Difenda Shield platform and limited deployment support for Defender for IoT, if necessary.

Microsoft Sentinel Implementation

A one-time professional services engagement to have Microsoft Sentinel designed and implemented by one of Microsoft's most globally-trusted implementation partners.

Difenda MDR for OT Service

Difenda's world-class SecOps-as-a-Service offering, Managed Detection & Response, is an ongoing service whereby Difenda provides 24 x 7 threat detection and response services on customers' behalf, leveraging their Microsoft security tools including Microsoft Sentinel and Defender for IoT.

MDR
FOR OT

What's Included in Difenda MDR for OT?

Asset Discovery

Protection starts with visibility. Powered by Microsoft's Defender for IoT, our service leverages passive network capture technology to automatically discover assets and visualize OT/ICS networks and asset relationships, eliminating operational concerns typically associated with sensitive OT / ICS environments. This visibility is foundational to Difenda's ability to help customers secure their OT/ICS environments, but also supports operational planning and maintenance activities

Vulnerability Management

Once assets are discovered, our services capture OT/ICS environment communication, firmware, and other integral asset vulnerability related information. With this information, Difenda's C3 team can assess an OT/ICS environment overall risk posture and work with customers to develop proactive risk mitigation strategies.

Integrated IT and OT Threat Detection and Response

Core to Difenda's MDR services are the Microsoft Azure Sentinel and Defender suite of security products. In addition to providing customers with detection and response services within IT environments, customers can extend protection to OT/ICS environments through Defender for IoT services coupled with our MDR-OT service offering. By adding MDR-OT services to existing MDR for IT services, customers receive fully integrated 24x7x365 threat detection and response services, all delivered through the Difenda Shield. As with our IT MDR services, customers receive the following benefits by subscribing to our MDR-OT services:

- **Threat detection and response**
- **Threat hunting**
- **Threat intelligence**
- **SIEM platform and use case management**
- **Remote incident response services**

As part of our MDR services, customers can leverage both pre-defined and customer requested response playbooks covering both IT and OT environments. Our services are designed to consider key detection and response factors such as asset sensitivity / impact and maintenance schedules to protect critical production environments.

Difenda MDR for OT

Agentless network monitoring to safely gain a complete inventory of all your assets, with zero impact on infrastructure performance.

Attack Simulation

The ability to simulate attacks in an OT/ICS environment has traditionally been a time consuming, expensive and risky undertaking. Attack simulations are a key tactic to understand risk, ensure response readiness, and are increasingly becoming mandated by regulatory bodies. With Difenda's MDR-OT services and Microsoft Defender for IoT, attack simulation modelling can occur quickly and continuously be updated based on factors such as environment changes or emerging threats. Where required, Difenda can also develop simulated customer OT environments through partners such as IdeaWorks (https://www.mohawkcollege.ca/ideaworks), allowing for more real-life attack simulations.

Custom Protocol and Detection Development

Many organizations are running bespoke or legacy technologies within their OT/ICS environments, making asset discovery and threat detection incredibly challenging. Where required, Difenda's experts leverage Defender for IoT's Horizon development framework to develop custom protocol plugins, to ensure complete environment visibility. In addition, our Cyber Research and Response team uses several tactics to augment native Microsoft detection capabilities through our ATT&CK® driven development process.

Remote Incident Response

In the event of a serious breach, advanced response services may be needed. MDR customers can leverage an incident response retainer for additional assistance - which includes a discounted hourly rate and a guaranteed initial response time. These remote incident and forensic support services are delivered primarily by Difenda's own experienced Cyber Research & Response Team. For the rare circumstances where unique specialists need to be engaged, Difenda has established relationships with trusted firms and certified professionals.

DIFENDA www.difenda.com | info@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

Difenda Shield Implementation

While the Microsoft Sentinel deployment team begins their work, we are also busy preparing the Difenda Shield for you. For each new MDR customer, we design, configure, test, and document the Difenda Shield platform to meet special requirements gathered during project discovery phase.

Once implementation is complete, your onboarding team begins the transition to operations by providing your team hands-on training with the Difenda Shield and any supporting documentation.

Prepare

Successful projects follow a plan. Developed from years of experience, Difenda's delivery team guides new customers through a comprehensive checklist and an onboarding project manager is assigned to ensure everything is tracked and on schedule.

Build

Services in the Shield which leverage one or more Microsoft security technologies (e.g., Microsoft Sentinel) are designed and implemented by trained Difenda cybersecurity and IT professionals. During this phase Difenda also creates the new customer account in the Shield platform and configures it for each service selected.

Connect

Once the systems are built and the Shield is ready the first telemetry data can be sent. Log sources and vulnerability scanners are configured to begin transmission. Once an asset is transmitting event log data the Shield can begin protection immediately!

Verify

Difenda validates that each service is operating as designed with a formal quality assurance process which includes configuring monitoring to ensure the Difenda Shield is always protecting you, 24 x 7.

Fortify

A series of collaborating working sessions ensure every customer hits the ground running and gets the maximum value from the Shield services after transitioning from this onboarding phase to the ongoing operational phase. These sessions include documentation delivery and knowledge transfer sessions - ongoing operational meetings follow a mutually agreed upon cadence.

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

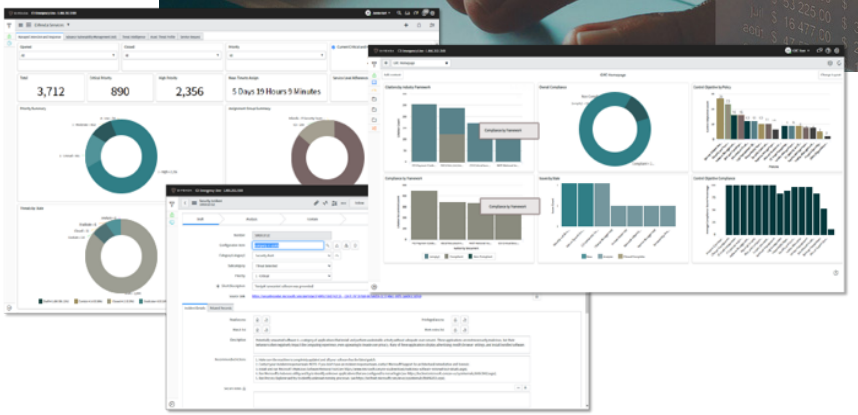
Coordinating complex security operations activities for Difenda's enterprise customers around the globe requires consistency and precision. At the heart of Difenda's operations is a Project Management Office (PMO) that keeps things running smoothly at all times.

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.

Difenda Shield Portal

The Difenda Shield delivers a clear and flexible customer experience through the Difenda Shield portal, our secure cloud-based SecOps service application. Key features of the portal include:



- **A convenient single pane of glass for all services in the Shield**
- **Asset discovery capabilities through for IT assets**
- **Real-time threat reports, including historical data for audit and compliance**
- **An integrated service request system for support and change requests**
- **Powerful and flexible dashboarding and reporting capabilities**

Why Difenda?

The crown jewel of your security operations stack needs to be set by experienced hands.

Decades of combined experience putting customer success first

It all started in 2008 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 and 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. Don't take our word for it; our staff and our facilities are highly decorated by third-party institutions.

Personnel Accreditation Highlights

- CISSP, GSEC, GCIH, PCI Professional
- OSCP, OSCE, CCFP, CEH, GCPT
- MS-500, AZ-500, MCSE, MCSA
- PMP, ITIL, Certified Scrum Master

Personnel Accreditation Highlights

- ISO 27001
- PCI DSS
- SOC 2 Type II

Operational Experience

Microsoft Sentinel is a security operations tool and so requires years of experience in the cyber-trenches to fully understand best practices and what pitfalls to avoid. Difenda's experience stems from its managed service division which provides cutting-edge Managed Detection & Response services leveraging Microsoft Sentinel.

Trusted by Microsoft

When Microsoft's largest and most-demanding customers need help deploying Azure Sentinel–anywhere in the world– Microsoft calls Difenda. A recent project success includes a complex implementation for a multinational corporation with 100,000+ endpoints.