# MDR for OT

*powered by Microsoft Defender for IoT*

With the rise of OT and ICS industries moving to leaner staffing models, and more automated processes, there is an increasing demand for connecting these previously air-gaped systems to the enterprise and even beyond. As technology continues to advance, greater connectivity has brought benefits in terms business and operations, but it has also raised concerns about cybersecurity.

## Growing cyber threats require a holistic defense strategy for operational technology

HOW WE DO IT

### 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.

### Vulnerability Management
Difenda's C3 team captures OT/ICS environment communication, firmware, and other integral asset vulnerability related information and assesses the environment overall risk posture and works with your team 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 your team with detection and response services within IT environments, you can extend protection to OT/ICS environments through Defender for IoT services coupled with our MDR-OT service offering. Your team receives fully integrated 24x7x365 protection, all delivered through the Difenda Shield including:

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

### Attack Simulation
With Difenda's MDR-OT services and Microsoft Defender for IoT, attack simulation modeling can occur quickly and continuously be updated based on factors such as environment changes or emerging threats.

### Custom Protocol and Detection Development
We leverage Defender for IoT's Horizon development framework to develop custom protocol plugins, to ensure complete environment visibility. Our Cyber Research and Response team uses tactics to extend native Microsoft detection capabilities through our ATT&CK® driven development process.

## KEY BENEFITS

- Turn-key agentless extended detection and response (XDR)

- Rapid deployment

- Works with diverse endpoints, IoT, OT, and industrial control system (ICS) devices

- Uses passive, agentless network monitoring to safely gain a complete inventory of all your assets, with zero impact on infrastructure performance

- Seamlessly integrates Difenda's IT MDR and MDR-OT services to provide customers with unified threat protection across the entire environment.

### IT and OT Playbooks
We offer both pre-defined and customer requested response playbooks covering both IT and OT environments.

## See The Difference A Personalized Approach To Cybersecurity Makes

CONTACT US TO REQUEST A DEMO:  www.difenda.com  |  info@difenda.com  |  1-866-252-2103