MANDIANT

DATASHEET

MANAGED DEFENSE FOR OT

Specialized expertise, technology and frontline intelligence

HIGHLIGHTS

- **Full team of OT experts.** Over eight years serving OT-specific customers with decades of cyber security and engineering experience.
- **Real-time visibility.** Customizable Helix dashboards enhance communication, reporting and collaboration between the IT/OT security teams and individual site engineers.
- **Market-leading threat intelligence.** Security analysts from multiple Mandiant groups apply the latest and real-time machine, victim and adversary intelligence to locate and detail threats in your environment faster.
- **Comprehensive hunting.** Analysts proactively hunt for hidden attackers and threat activity using FireEye technology, analytical expertise and intelligence.
- **Investigation and response.** Analysts thoroughly investigate critical threats, providing detailed answers to effectively respond.
- **OT security analysts.** Direct collaboration with a Mandiant OT security expert during high priority incidents.
- **24x7 Alert Coverage.** SOCs in the United States (Virginia and California), Ireland, and Singapore.

As operational technology (OT) devices have become more connected, they have also become more exposed and subject to additional vulnerabilities. Unfortunately, many users do not focus on securing OT data and systems.

Technology alone does not fully protect against a determined attacker or accidental misuse. Finding IT talent with OT expertise or OT talent with advanced cyber response experience to secure OT assets can be a daunting task. You need a trusted partner to monitor your network around the clock with a pro-active, analyst-driven approach leveraging the latest threat intelligence cultivated from experience.

You need Mandiant Managed Defense for OT.

Intelligence-led detection and response

Managed Defense for OT is a managed detection and response (MDR) service that leverages the full power of Mandiant and leading OT tool providers, combining industry-recognized cyber security expertise, FireEye technology and unparalleled knowledge of attackers to help minimize the impact of a breach.

Managed Defense for OT helps you amplify your security team with OT expertise. This service is continuously fueled by the industry's largest global cyber threat intelligence capability that harnesses machine, campaign, adversary and victim intelligence gained on the frontlines of the world's most consequential cyber attacks. This frontline intelligence and expertise drives detection and guides our analysts' hunting and investigation activities to provide enterprise-wide visibility and proactively identify and respond to hidden threats.

How it works

Managed Defense uses our proprietary technology stack to provide real-time visibility across the enterprise, including ICS and cloud infrastructure.

Managed Defense analysts leverage adversary, victim and machine-based threat intelligence to detect, investigate and proactively hunt for known and previously undetected threats.

When signs of compromise are confirmed, you are notified immediately and can review the latest findings via a secure portal while our analysts continue to investigate the incident.

You also receive a detailed summary report that provides threat context along with remediation recommendations to form an effective response and help prevent attackers from completing their mission.

TABLE 1. Comparison of Managed Defense offerings.

	Managed Defense (Managed Detection and Response)	Managed Defense for OT (OT / ICS Expertise)
Emerging Threat Detection	✓	✓
Adversary Hunting at Scale	✓	+OT Hunting
Managed Hunting	✓	✓
Onboarding Required	✓	✓
Appliance Health Monitoring	✓	✓
Incident Scoping/Rapid Response	✓	✓
Remediation Recommendations	✓	✓
Alert Monitoring and Validation	24x7	24x7
Access to Analysts	✓	+Access to OT Security Experts
Asset/Vulnerability Inventory[2]	✓	✓

Managed Defense for OT Tiers

Foundational Security Coverage

- FireEye Network Security at the IT/OT border/perimeter
- FireEye Helix
- FireEye Endpoint Security deployed where possible

Full Situational Awareness

- FireEye Network Security at the IT/OT border/perimeter
- FireEye Helix
- FireEye Endpoint Security agents where possible
- 3rd Party Tech - OT Asset Inventory
- OT Jumpstart

Options/add-ons: Cyber-physical intelligence subscription, Waterfall data diode, full Managed Defense

Why Mandiant

Mandiant has been at the forefront of cyber security and cyber threat intelligence since 2004. Our incident responders are on the frontlines of the most complex breaches worldwide. We have a deep understanding of both existing and emerging threat actors, as well as their rapidly changing tools, tactics and procedures.

WHY MANAGED DEFENSE

- **Escalation threats and risks between IT and OT.** Understand clearly when risks in the operational or corporate environment can impact one another
- **Annual security posture review.** Understand your environment better through a periodic, third-party assessment of your risks and threats
- **Intelligence.** Access to nation-state grade intelligence collection supported by 150+ intelligence analysts
- **Rollup of security events and risks within the environment.** Maintain the situational awareness needed to ensure safe and orderly operations
- **Custom FireEye Helix dashboards.** Tailor real-time views of the OT environment to enhance communications between IT and OT security teams as well operational employees and engineers
- **Monthly asset and vulnerability reporting.*** Locate weak points in the OT network and determine whether they can be patched or remediated

*requires 3rd party technology.

Learn more at **www.mandiant.com/managed**

Mandiant
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300
833.3MANDIANT (362.6342)
info@mandiant.com

About Mandiant
Since 2004, Mandiant has been a trusted security leader to organizations that can't afford to fail. Today Mandiant delivers decades of frontline insights at scale through easy-to-deploy and consume SaaS solutions for provable and transformative cyber defense.