



DATA SHEET

Managed Defense—Nights and Weekends

Off-Hours Managed Detection and Response



HIGHLIGHTS

- **Frontline Experience:** Managed Defense analysts use the same tools, techniques and procedures that are used by FireEye Mandiant consultants in the field.
- **Enhance Existing Capabilities:** Augment your existing security team with Managed Defense expertise to enhance existing capabilities.
- **Cost Effective:** Attain 24x7 SOC coverage without having to recruit, train, and retain additional Infosec talent.
- **Fully Transparent:** Automated reporting and portal access provide visibility into alert disposition and trending.
- **Managed Defense Consultants:** Security experts are your main point of contact.
- **FireEye Expertise:** Access to malware and forensic analysts.

As an organization grows and becomes more frequently targeted, it develops a greater need for a dedicated 24x7 security operations center. Companies that have focused on establishing and improving their SOCs have made headway against the never-ending battle with attackers.

Complexities and costs increase as more SOC capabilities and shift coverage are added. It's also difficult and costly to recruit, train and retain security experts to maintain continuous coverage at all times.

You need a trusted partner to continue to monitor your network after hours with an analyst-driven approach that leverages the latest threat intelligence cultivated from frontline experience.

You need FireEye Mandiant Managed Defense—Nights and Weekends.

Analyst Driven Detection and Response

Managed Defense—Nights and Weekends is a managed detection and response service that provides after-hours support and fills gaps in your 24x7 SOC capabilities. By leveraging FireEye Mandiant frontline expertise, along with industry-leading threat intelligence and technology, it augments your security team with advanced detection and investigation capabilities that reveal even the most sophisticated attacker.

Managed Defense analysts partner with your security operations center to provide in-depth review of attacker activity along with customized response recommendations, delivering the context needed to take definitive action.

How It Works

Managed Defense—Nights and Weekends picks up where your team clocks out and 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 and investigate threats.

You are notified immediately when evidence of compromise has led to an investigation. You can track the status of this investigation via a secure portal while our analysts continue to work the incident to completion.

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.

WHY MANAGED DEFENSE

- **Experience**
Draw on the experience of Mandiant incident response teams, who spend 200,000+ hours per year on the most impactful breaches
- **Faster Detection**
Median time to investigate and respond with Managed Defense is 67 minutes
- **Cost effective**
Development and maintenance of in-house capabilities can take a lot of time, money and resources
- **Intelligence**
Access to nation-state grade intelligence collection supported by 150+ intelligence analysts
- **Powerful Defense**
Proprietary technology stack incorporates FireEye technology and intelligence
 - 150 million FireEye product detections
 - 22 million Managed Defense alerts ingested
 - 170 thousand Analyst Investigations
 - 91% of high priority threats resolved without Rapid Response
 - 98% of Rapid Response incidents resolved without full incident response

Table 1. Comparison of Managed Defense offerings.

	Managed Defense	Managed Defense—Nights and Weekends
Emerging Threat Detection	✓	✓
Managed Defense Consultant	✓	✓
Managed Hunting	✓	
Onboarding Required	✓	✓
Appliance Health Monitoring	✓	✓
Incident Scoping/Rapid Response	✓	✓
Remediation Recommendations	✓	✓
Alert Monitoring and Validation	24x7	Off hours support (nights, weekends, holidays)
Access to Security Experts	✓	✓

Why FireEye Mandiant

FireEye 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.

To learn more about FireEye, visit: www.FireEye.com

FireEye, Inc.

601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

©2019 FireEye, Inc. All rights reserved. FireEye is a registered trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. MD-EXT-DS-US-EN-000194-02

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.

