

品項名稱:

FireEye MD 防禦管理監控平台

產品介紹:

光靠技術無法完全抵禦堅定，持久和隱秘的攻擊攻擊者。人類的專業知識可以補充技術以提供靈活性，獨創性和專注力-特別是針對高級多階段攻擊，以及與響應相關的活動。但是透由尋找/僱用/培訓和聘請安全專家。

商品特色:

託管防禦使用我們的專有技術堆疊來提供實時整個企業的可見性，包括 ICS 和雲基礎架構。管理國際分析師利用對手及受害者和基於機器的威脅檢測和調查威脅的情報。當有妥協證據導致您遭受損失時，會立即通知您。調查您可以通過安全門戶跟踪此類調查的狀態同時我們的分析人員繼續努力使事件完成。您還將收到一份詳細的摘要報告，其中提供了有關威脅的上下文以及與補救建議，以形成有效的應對和幫助阻止攻擊者完成任務。

DATA SHEET

Managed Defense

Managed detection and response (MDR) backed by the full power of Mandiant Solutions



HIGHLIGHTS

- **Market-Leading Threat Intelligence:** Security analysts from multiple FireEye and Mandiant Solutions teams apply the latest and real-time machine, victim and adversary intelligence to locate and detail threats in your environment faster.
- **Alert Prioritization:** Identify the most critical alerts to provide focus to those that must be responded to immediately.
- **Comprehensive Hunting:** Analysts proactively hunt for hidden attackers and threat activity using extant technology alongside Mandiant analytical expertise and intelligence.
- **Security experts:** Liaise with a primary point of contact who facilitates additional support such as analysis of malware samples, in-depth forensic analysis or on-site incident response.
- **24x7 Coverage:** SOCs in the United States (Virginia), Ireland and Singapore provide 24x7 coverage.

Technology alone cannot fully protect against a determined, persistent, stealthy attacker. Human expertise can complement technology to offer flexibility, ingenuity and focus—especially against advanced, multi-stage attacks, and for response-related activity. But it is difficult and costly to find, hire, train and retain security experts.

Security teams need a trusted partner to monitor their network around the clock with a proactive, analyst-driven approach that uses the latest threat intelligence from frontline experience.

Mandiant Managed Defense is a managed detection and response (MDR) service that combines industry-recognized cyber security expertise, Mandiant technology and unparalleled knowledge of attackers to help minimize the impact of a breach.

Intelligence-Led Detection and Response

Managed Defense 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 reveal even the most sophisticated attacker. Security analysts provide a comprehensive assessment of attacker activity along with customized response recommendations, delivering the context needed to understand threats, assess risk and take definitive action.

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 and investigate threats.

You are notified immediately when evidence of compromise has led to an investigation. You can track the status of such investigations 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.

Additional Managed Defense Options

In addition to the 24/7 service, several other versions of Managed Defense are available for your specific needs:

Managed Defense for FireEye Endpoint Security

Augment your security team to accelerate detection and investigation activities across all endpoints. Managed Defense consultants partner with your team and leverage FireEye Endpoint Security to handle detections against known threats, advanced detections that require behavioral analytics and full forensic acquisitions from a compromised endpoint.

Managed Defense—Nights and Weekends

Gain continuous access to managed detection and response expertise with off-hours (evenings, weekends, holiday) support. Ideal for the organization seeking to expand their internal security operations center visibility to 24x7 without incurring the overhead of recruiting, training and retaining additional teams.

Managed Defense for Operational Technology (OT)

Deploy a managed detection and response (MDR) service that leverages the full power of Mandiant Solutions and leading OT tool providers. Specifically tailored for the OT environment, Managed Defense for OT uses the proprietary FireEye technology stack to provide real-time visibility across the enterprise, including ICS and cloud infrastructure.

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

- **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 Mandiant Threat 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

To learn more about Mandiant Solutions, visit: www.FireEye.com/mandiant

FireEye, Inc.

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

©2020 FireEye, Inc. All rights reserved. FireEye and Mandiant are registered trademarks 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-000115-03

About Mandiant Solutions

Mandiant Solutions brings together the world's leading threat intelligence and frontline expertise with continuous security validation to arm organizations with the tools needed to increase security effectiveness and reduce business risk.

