DATA SHEET

Response Readiness Assessment

Assess your ability to detect, respond to, and contain advanced cyber attacks

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 tactics, techniques and procedures (TTPs).

Overview

Whether you need to build a new incident response function from scratch, enhance your existing processes or invest in supporting technology, Mandiant can help improve your defense posture against persistent and sophisticated real-world attacks. The FireEye Mandiant Response Readiness Assessment evaluates an organization's cyber defense capability, which typically includes their security operations center (SOC) and incident response (IR) functions. The assessment is led by Mandiant consultants who leverage industry best practices and firsthand experience in responding to intrusions across different geographies and industry verticals. After the assessment, Mandiant consultants deliver a report with a detailed roadmap and prioritized improvement recommendations.

Most organizations, even those that have invested heavily in cyber defense, may retain some uncertainty about their ability to properly identify, accurately assess and appropriately respond to targeted threats. Using lessons learned from responding to a range of threats, such as commodity malware, ransomware, cyber crime and nation-state APT attacks, Mandiant consultants evaluate your organization's ability to manage threats specific to your organization and provide the guidance you need to realize practical and meaningful improvements.

Our Approach

Mandiant consultants use a combination of documentation review, analysis of logging configurations, deep-dive workshops, tabletop exercises and simulated threat detection controls testing to rigorously review and validate your organization's cyber defense capability against Mandiant's six core response readiness competencies:

- **Governance.** The foundation for an effective cyber defense capability that supports the overall business mission.
- **Communications.** The communication processes involving internal and external stakeholders before, during, and after an incident.
- **Visibility:** The people, processes, and technology that detect threats across the organization's infrastructure.
- **Threat Intelligence.** Attacker intelligence used to understand and identify threat actor tools, tactics and procedures (TTPs) in support of detection and response efforts.
- **Response.** How the organization verifies and categorizes incidents, evaluates their severity and determines proper response actions.
- **Metrics.** The measurement and development strategies needed to maintain and improve cyber defense capability over time.

After the assessment, Mandiant consultants deliver a detailed report with prioritized recommendations for improving your cyber defense capability.

Tiered Model: Organizations differ in size, maturity and end goals. The Response Readiness Assessment is tailored to your organization's needs. Core competencies are reviewed and augmented with various support activities.

Table 1. Response Readiness Assessment Tiers.

Tiers and assessment components	TIER I Assess	TIER II Assess Exercise	TIER III Assess Exercise Technically validate
Typical Duration (weeks)	4	5	6
Documentation Review	X	X	X
Six Core Response Readiness Competencies Workshops	X	X	X
Logging Configuration Review	X	X	X
Detailed Response Readiness Assessment Report	X	X	X
Technical Briefing (report walkthrough)	X	X	X
Executive Briefing (customized PowerPoint)		X	X
Incident Response Team Skills Matrix Exercise		X	X
Organization's Response Readiness Capability and Industry Comparison		X	X
Response Readiness Improvement Roadmap		X	X
Industry Threat Insights		X	X
Technical Tabletop Exercise		X	X
Executive Tabletop Exercise			X
Simulated Threat Detection Controls Testing (powered by FireEye Verodin)			X

Assessment Schedule

Depending on the tier, the assessment comprises four to six phases and typically takes between four and six weeks to complete.

Documentation Review (1 week)

An offsite review of relevant cyber defense documentation such as incident response plans, playbooks, communications plans and crisis management plans.

Onsite Workshops and Skills Matrix Exercise (1 week)

Onsite workshop that covers each of the core response readiness competencies in collaboration with your stakeholders, as well as a skills matrix exercise with the incident response team (up to seven workshops in total).

Logging Configuration Review (0.5 weeks)

A review of critical log samples to validate configurations for effective threat detection and response.

Tabletop Exercises (0.5 weeks)

Discussion-based tabletop exercises with your technical and executive stakeholders to assess the end-to-end incident response process (up to two exercises).

Simulated Threat Detection Controls Testing (1 week)

Simulated attacks conducted in your network in a safe and controlled way to assess the effectiveness of threat detection controls.

Reporting and Debrief (2 weeks)

A report that details prioritized tactical and strategic recommendations, as well as an actionable roadmap, for improving the organization's cyber defense capability.

DELIVERABLES

After the assessment, Mandiant consultants deliver a report that includes:

- An assessment of your organization's current cyber defense capability
- Detailed recommendations to consider as you build or improve on your cyber defense capability.
- Technical briefing
- An actionable roadmap of recommended initiatives for improvement (for Tier II and Tier III)
- Executive briefing (for Tier II and Tier III)

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

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.

FIREEYE™