



Response Readiness Assessment

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



WHAT YOU GET

- **Independent assessment:** An independent assessment of your security monitoring and response capabilities.
- **Best practices overview:** A focus on IR best practices such as how to structure your SOC, enhance security monitoring and integrate threat intelligence.
- **Tabletop exercise:** A real-time cyber exercise scenario that is based on actual incidents Mandiant consultants have responded to in the field.
- **Prioritized recommendations:** A customized roadmap that highlights the investments that will have the most significant impact on IR.

The Mandiant Difference

Mandiant, a FireEye company, has over 14 years of experience at the forefront of cyber security and cyber threat intelligence. Our incident responders have been on the frontlines of the world's 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.

Overview

The Mandiant Response Readiness Assessment evaluates an organization's incident response (IR) function, which includes their security operations center (SOC) and IR capabilities, against leading practices and identifies improvement opportunities.

Using a combination of team discussions, internal document review and tabletop exercises, Mandiant consultants conduct a comprehensive survey of your existing cyber security event monitoring, threat intelligence and incident response capabilities to deliver a detailed roadmap and specific, cost-effective improvement recommendations.

Whether you need to build a new incident response function from scratch, enhance your existing processes, or invest in supporting technology, Mandiant provides proven practices to improve your defense posture against persistent and sophisticated real-world attacks.

Our Approach

First, Mandiant consultants compare your current practices against the Mandiant Six Core Capabilities Model that addresses the incident response function:

Governance

Serves as a foundation for an effective IR function that advances the organization's principal objectives.

Threat Intelligence

Uses attacker intelligence to understand and detect threat actor tools, tactics and procedures (TTPs).

Visibility

Represents the people, processes and technology that detect threats across the organization's business architecture.

Response

Represents how the organization verifies and categorizes incidents, evaluates their severity and determines proper response actions.

Communications

Represents the IR communication processes to important internal and external stakeholders.

Metrics

Signifies the measurement and development strategies needed to maintain and improve the IR function.

METRICS



Cyber Traffic Visibility



Stakeholder Communications



Local and Global Threat Intelligence



Incident Response Readiness

GOVERNANCE



Next, Mandiant experts test your program using common real-life scenarios they have experienced. Finally, they develop a customized roadmap with detailed recommendations on how to build, mature and sustain an enhanced cyber security program for your organization.

What we Assess

Mandiant experts use our proven approach to examine each area of your cyber security program:



Compliance

Do your response strategies support applicable regulatory and legal requirements?



Organization

Is your staff well organized and do they clearly understand their crisis roles and responsibilities?



Training

Is your team trained to respond effectively and efficiently when incidents arise?



Detection

Does your organization have the mechanisms in place to rapidly detect an incident?



Processes

Do you have a clear process in place for quickly responding to potential data breaches?



Technology

Does your enterprise's installed hardware and software facilitate successful incident response?

Our Process

Step 1

Assess your ability to detect, respond and contain threats

Mandiant consultants review your SOC and IR documentation, and compare your current processes against industry best practices to establish your baseline performance. They also conduct detailed staff interviews to better understand SOC and IR processes that are unique to your organization.

Step 2

Test your processes with tabletop exercises

Incident scenarios (i.e., system compromise, unauthorized access of personally identifiable information (PII), policy violations, inappropriate emails) are simulated to evaluate your organization's response processes from incident detection to closure.

Step 3

Adopt recommendations and custom roadmap

The observations identified during documentation review, staff interviews, and the tabletop exercise will be used to develop the final report and presentation. Your organization will be benchmarked against legal and regulatory requirements, and industry best practices. The RRA will highlight your organization's SOC and IR strengths, and identify improvement opportunities.

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

© 2018 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. DS.RRA.US-EN-042018

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 has over 6,600 customers across 67 countries, including more than 45 percent of the Forbes Global 2000.

