MANDIANT®
A FireEye® Company

Response Readiness Assessment

Engage Mandiant to assess your capabilities to detect, respond and contain advanced attacks and recommend how you can improve your defense posture to find and stop attackers faster.

DATA SHEET

SECURITY CONSULTING

WHAT YOU GET

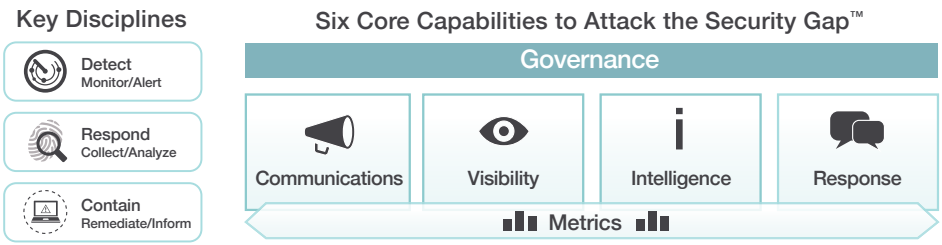
As part of the assessment you receive the following deliverables:

- **Independent assessment**
  Mandiant provides an independent assessment of your security monitoring and response capabilities.
- **Best practices overview**
  During the assessment we explain incident response best practices including how to structure your SOC workflow, integrate your SIEM with your IR processes and more.
- **Threat briefing**
  We provide an overview of the latest threats that Mandiant has seen and what can be done to protect against them.
- **Tabletop exercise**
  We run your team through a real-life exercise based on actual incidents Mandiant has responded to.
- **Prioritized recommendations**
  Our roadmap tells you what investments will yield the largest return and have the biggest impact on your security posture.

Overview

Mandiant responds to hundreds of computer security incidents every year. The Response Readiness Assessment draws on that experience to review your SOC and incident response capabilities against leading practices. We will help you determine where your program needs to go and how you can get there. Using a combination of discussions, document review, and a table-top exercise we'll create a detailed road map and specific recommendations.

Mandiant six core capability model



Our experts will review all aspects of your detection and response programs including your processes, technologies, and internal capabilities.

What we assess

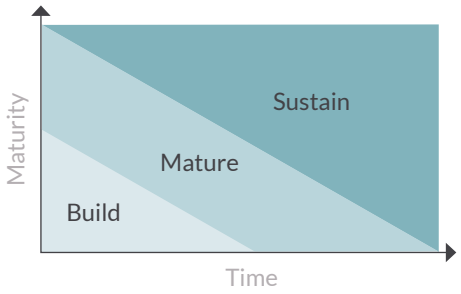
We provide you with a comprehensive survey of your existing security event monitoring, threat intelligence, and incident response capabilities and deliver specific, cost-effective recommendations for improvement. During the assessment Mandiant examines each area of your program to address some of the following questions:

- **Regulatory compliance:** Do your response strategies support applicable regulatory and legal requirements?
- **Organization:** Is your staff organized effectively and does your staff clearly understand their roles and responsibilities during an attack?
- **Training:** Does your staff have the training they need to respond effectively and efficiently when incidents arise?
- **Incident detection:** Does your organization have the mechanisms in place to rapidly detect an incident?
- **Processes:** Do you have a clear process for rapidly responding to potential data breaches?
- **Technology:** Does your organization have the necessary hardware and software to respond across your enterprise?

Whether you need to build a new program from scratch, enhance your existing processes or invest in technology we give you straightforward recommendations to improve your defense posture against real-world attacks.

Response readiness assessment capability maturity model

- Governance
- Visibility
- Communications
- Intelligence
- Response
- Metrics



A detailed report documents our findings and provides recommendations for improving your ability to find and stop advanced attackers.

Our approach

Over the course of the assessment, we baseline your current practices against our six core capability model. Then, we put your program to the test using real-life scenarios our consultants experience every day. Finally, we give you a roadmap with detailed recommendations for how to build, mature and sustain your security program.

Step 1: Assess your ability to detect, respond and contain threats

Mandiant experts collect and review your security operations, threat intelligence, and incident response program documentation to baseline your current practices against industry best practices. Detailed interviews of your staff help us understand processes that are unique to your program.

Step 2: Put your processes to the test with tabletop exercises

We work with you to customize a scenario that simulates an incident. Common scenarios include system compromise, internal leak of PII data, or an internal investigation of inappropriate use and threatening email. During the response, we assist and evaluate the effort from initial detection to resolution.

Step 3: Mandiant recommendations and roadmap

We provide you with a final report and presentation that blends our review of your procedures, your staff's insights, and our observations during the exercise. We focus on benchmarking your program against applicable legal or regulatory requirements and industry best practices, highlighting your program's strengths and opportunities for improvement.

CASE STUDY

Large manufacturer

- **Situation:** After Mandiant performed a detailed response and containment of an advanced targeted attack, the client wanted to improve their ability to deal with a similar attack in the future.
- **Result:** Mandiant's Response Readiness Assessment helped them build a plan to improve their security monitoring and incident response capabilities and justify the required investments.

Mandiant, a FireEye company, has driven threat actors out of the computer networks and endpoints of hundreds of clients across every major industry. We are the go-to organization for the Fortune 500 and government agencies that want to defend against and respond to critical security incidents of all kinds.

Mandiant, a FireEye Company | 703.683.3141 | 800.647.7020 | info@mandiant.com | www.mandiant.com | www.fireeye.com

MANDIANT
A FireEye® Company