Mandiant

Tabletop Exercise

Benefits

- Identify gaps between documented and expected responses in comparison to what actually happens.
- Recommendations based on real-world incident response best practices.
- Quick, efficient, non-invasive evaluation.

Evaluate your cyber incident response plan through scenario gameplay

Why Mandiant

Mandiant has been at the forefront of cybersecurity 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.

The Tabletop Exercise draws on this expertise to deliver custom scenario injects rooted in real-world experience and designed to address your key business and technical areas of risk.

Overview

The Tabletop Exercise evaluates your organization's cyber crisis processes, tools, and proficiency in responding to cyber attacks from both an executive strategic and technical incident response perspective. During each exercise, Mandiant consultants introduce multiple scenario injects based on real-world experience in a roundtable environment to observe the organization's simulated actions and decisions in response.

Approach

Before beginning a tabletop exercise, Mandiant experts first develop an understanding the client organization's threat profile, operational environment, and specific areas of concern. We conduct an on-site workshop with key individuals, and introduce evolving scenario injects based on attacker behavior, techniques, and tactics observed during our incident response work.

During the exercise, we observe gameplay to determine how simulated actions and decisions run concurrent to or diverge from the organization's documented plans and processes and the incident response best practices identified by Mandiant experts.

"Being able to respond efficiently and effectively to security incidents is critical to our business. The Tabletop Exercises were very valuable as they provided the means for the teams to validate decisions and engage in discussions."

— CISO, Global Technology Distribution Company

What you get

Executive Brief [PPT]

- An in-person overview of gameplay, specifically:
  - Participants' interaction with the incident response plan (IRP), communications plan(s) and escalation procedure(s)
  - Lessons learned
  - Strategic recommendations

Tabletop Exercise After-Action Report [PDF]

- Timeline of events
  - All injects
  - Stakeholder/participant responses
- Strategic cyber incident response analysis and recommendations for improvement related to gameplay, categorized by:
  - Detection
  - Response
  - Containment
  - Remediation

Tracks

We offer two Tabletop Exercise tracks: **technical incident response** and **executive crisis management**. Best practice calls for each track to be conducted annually — separately or as part of a coordinated exercise.

The Technical Incident Response track is ideal for security team management and staff looking to test their response process capabilities.

The Executive Crisis Management track is ideal for C-suite executives who want to test the effectiveness of their crisis response strategies.

After the workshop, we brief the organization in person and submit a written After-Action Report that includes a step-by-step summary of scenario inputs and responses.

TABLE 1. Service track comparison.

Service Track	Technical	Executive
Objective	Assess and analyze an organization's technical response capability to detect, respond to and contain an advanced threat.	Assess and analyze an organization's crisis management capabilities in the event of an advanced threat through the lens of the executive team.
Engagement timing	**Planning:** 1 week offsite **Scenario gameplay:** 1-2 days onsite **Final report:** 1 week	**Planning:** 1 week offsite **Scenario gameplay:** 1-2 days onsite **Final report:** 1 week
Target participants	• Cybersecurity incident response • team (CSIRT) • Security manager • Technical staff (such as those who work with network, server, email)	• Chief Information Security • Officer (CISO) • General C-suite executives • Public relations and corporate communications • General counsel
Focus areas	• When to isolate hosts on a network • When to re-image a system • How analysts should follow the defined IRP, communication plan, and escalation matrix • When and how to engage third party vendors	• When to pay extortion or ransom threats • Decision-making around the impact of containment tactics • Breach disclosure requirements to regulators and key stakeholders • Customer notification best practices • Media communication best practices
Delivery method	On-site scenario role play	On-site scenario role play