TABLETOP EXERCISE

EVALUATE YOUR ORGANIZATION’S ABILITY TO EFFECTIVELY EXECUTE YOUR CYBER INCIDENT RESPONSE PLAN THROUGH SCENARIO GAMEPLAY

WHY MANDIANT

Mandiant has over 10 years of near-daily interaction with organized, persistent attackers and threat groups around the world, logging thousands of hours annually working with organizations of all sizes to remediate security breaches, identify vulnerabilities that targeted attackers exploit and provide guidance on closing security gaps. 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 the 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

Mandiant begins by understanding the organization’s threat profile, operational environment and specific areas of concern. We conduct an onsite workshop with key individuals, introducing 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 process and/or Mandiant’s incident response best practices.

“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, engage in discussions”

- CISO, Global Technology Distribution company

BENEFITS

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

How prepared are you to execute your cyber security incident response plan?
Following the workshop, we share our observations with the organization in an initial in-person briefing, followed by a written Exercise After-Action Report with a step-by-step summary of scenario inputs and responses according to each step of the preparedness cycle: Detection, Response, Containment and Remediation.

Tabletop exercise process

Step 1: Planning stage — Scenario & Inject development — 1 week

Step 2: Tabletop workshop — Introduce scenarios with evolving injects to evaluate response — 1-2 days onsite

Step 3: Report Development and Delivery — 1 week

Report sample

For more information on Mandiant consulting services, visit: www.FireEye.com/Mandiant.html

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