SOLUTION BRIEF

Test Your Cyber-Incident Playbooks with FortiGuard Tabletop Exercises

Executive Summary

Imagine a team going into a playoff game without practice, or a teenager thrust onto a busy highway before taking any driver training courses. Like these scenarios, operating without any knowledge of how your security posture and processes have changed as the organization's network and personnel have evolved leads to surprises at an inopportune time: during an actual cyber incident.

FortiGuard Tabletop Exercises (TTXs) help security teams test their plans and processes outside of a cyber incident. Tabletops let you test what to do—who to call, when to call, and according to what criteria—based on the circumstances, such as what happened and which devices are impacted. Against the backdrop of change, TTXs provide teams with real-world scenarios to evaluate their processes and playbooks and test their communications efficacy. Security leaders gain visibility into quantifiable gaps and recommended actions for fixing them. By understanding the feasibility and effectiveness of their processes, teams can catch the "gotchas" before they're under fire from an actual cyberattack. Using the exercise outcomes, security leaders can make informed decisions about how to improve their readiness. TTXs are an important part of security hygiene best practices, particularly given that people, processes, and threat types are constantly evolving.

"... a tabletop exercise can identify potential gaps and ensure the right process is in place to mitigate and recover from a potential attack."[1]

Are We Prepared for a Cyberattack?

Regardless of the specific number of attacks, variants, or threat actors that pose a risk to your organization, the prevalence of these attacks and their potential impact can be significant. Nearly half of executives surveyed feel their security has not "kept up with digital transformation."[2]

Enterprises are dynamic, living entities with employee turnover, skillset shortages, and technology changes. This means that your security posture is not static, and therefore your playbook should not be either.

TTXs are one of several readiness tools that help companies identify and validate current working practices, procedures, and policies to detect and respond to an attack. These discussion-led exercises can engage just the security team or the broader enterprise teams who are typically engaged during an actual attack. They provide a forum for constructive discussion in each scenario in which operational plans and processes are reviewed among the exercise participants. The outcome is to enable everyone, not just security leaders, to understand where the group can make improvements in their plans so that they're adequately prepared if and when an attack occurs.

The TTX Process

TTXs are conducted by the FortiGuard Incident Response and Readiness team and are based on real-world experience and scenarios to which they've responded.

The TTXs consist of discussion-based exercises that test an organization's playbooks, processes, and communications in detecting and responding to a cyber incident. Using a series of scenarios based on real-world attacks mitigated by the FortiGuard Incident Response team, facilitators test the organization's incident response plan and help to identify security gaps in the organization's security posture or processes. Guiding participants verbally through the scenarios, facilitators help the company's participants to work together, with the provided intelligence from investigations, to determine a course of action for each. They ask questions about each scenario and encourage discussion and interaction across the team. This more relaxed environment—while using scenarios from actual cyber incidents—gives participants the opportunity to assess their abilities while they're not under pressure and responding to a real incident.

"Being entirely honest with oneself is a good exercise."
– Sigmund Freud

The key objectives of the exercise are to:

- Identify and validate current working practices, procedures, and policies
- Identify strengths, weaknesses, and gaps
- Build knowledge and relationships among team members
- Foster more effective communication between teams
- Initiate conversation on how to be better prepared for similar challenges

There are no winners or losers at the end of these exercises. Instead, teams walk away with helpful firsthand insight into their overall state of readiness when it comes to detecting and responding to cyber incidents.

By the end of each testing scenario, each stakeholder should have a stronger understanding of what actions should be taken, and by whom. At the end of the TTX, participants receive a final report that includes recommendations to ensure the organization has a clear and concise incident response action plan.

TTX Outcomes and Service Options

Change is a constant in every organization. Similarly, so is the threat landscape. TTXs provide an active, engaged way to assess an organization's processes, communications, and plans, and ultimately their collective ability to respond to a cyber incident.

At the close of the exercises, TTXs help leaders and their teams answer these questions:

- What worked well?
- How could we improve?
- What changes or updates to plans, policies, and procedures need to be implemented?

FortiGuard TTX benefits include:

- Team building
- Team response efficacy
- Opportunities for security gap correction
- Communication improvements
- Incident response plan efficacy

For a more comprehensive approach to incident preparedness, FortiGuard offers the choice of standalone TTXs or the option of a subscription service that allows you to choose from a full suite of proactive and incident response services. The FortiGuard Incident Readiness Subscription Service offers security leaders the ability to better prepare, rapidly respond, and take effective actions at every step. The service is a one-year subscription that provides options from a number of proactive, preparedness services that can include:

- Incident readiness assessment
- Incident response playbook development
- Tabletop exercise (incident response playbook testing)
- Digital forensics and incident response (with a one-hour service-level objective)

Additional hours may be purchased as needed.

Strengthen Your Security Posture with TTXs

Regardless of the latest threats or changes in your enterprise, TTXs can provide you with an understanding of the efficacy of your current incident response playbook. Security leaders gain visibility to quantifiable gaps and get suggestions for closing those gaps, ultimately leading to a clear and concise incident response plan. Regardless of which service option you choose, the experience and knowledge you gain can inform empowered actions to bolster your enterprise to better prepare for "game day."

[1] Chuck Brooks, "Alarming Cyber Statistics For Mid-Year 2022 That You Need To Know," Forbes, June 3, 2022.

[2] ThoughtLab, "Cybersecurity Solutions for a Riskier World," accessed July 29, 2022.

December 15, 2022 3:19 PM

1857922-0-0-EN