SOLUTION BRIEF

Test Your OT Cyber-Incident Playbooks with FortiGuard Tabletop Exercises

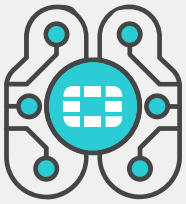
Tabletop Exercises for Operational Technology: Electric Grids, Water and Sewer Systems, Pipelines, and More

Executive Summary

Imagine a professional sports team going into a playoff game without practice or a teenager barreling onto a busy highway before taking any driver's training. Like these scenarios, running your organization's operations without understanding how your operational technology (OT) security posture and processes have evolved as your network and personnel have changed can lead to unpleasant surprises—at inopportune times, such as during a cyber incident.

FortiGuard Tabletop Exercises (TTXs) enable security teams to test plans and processes before a potential cyber incident occurs. TTXs enable you to test what to do—whom to call, when to call, and using what criteria—based on the circumstances, such as what has happened and which devices are impacted. Against the backdrop of change, TTXs provide your teams with real-world scenarios to evaluate their understanding of processes and playbooks, and to test their communication efficacy. You will gain visibility into quantifiable gaps and recommended actions for fixing them.

By understanding the feasibility and effectiveness of your organization's processes, your security team can catch the "gotchas" before you're under an actual cyberattack. Using the exercise outcomes allows you to make informed decisions about how to improve your readiness. TTXs are an important part of security hygiene best practices, particularly given that people, processes, and threats are constantly evolving.



50% of organizations reported experiencing one or more cybersecurity incidents. And attackers continue to use phishing, malware, and increasingly AI-powered tactics to exploit operational vulnerabilities.[1]

OT Networks Exposed to Cyber Risks

While OT is less visible than IT at most organizations, and certainly in the public consciousness, it is no less important to the economy and everyday lives. After all, OT systems control the critical infrastructure that everyone depends on, including the electrical grid, water and sewer systems, fuel pipelines, power plants, and transportation networks. It is also essential for the manufacture and distribution of all types of goods.

As IT and OT networks converge, organizations expose their traditionally isolated OT networks to new cyber risks. Cybercriminals continue to launch malware attacks, such as CrashOverride/Industroyer, Triton, and VPNFilter, targeting vulnerable OT systems.

A study examining 1 million OT devices revealed that 40% of organizations have at least one asset exposed to the internet without proper security. Additionally, around 31% were found to have internet-facing assets with known exploited vulnerabilities.[2]

Are We Prepared for a Cyberattack?

Regardless of the specific number of attacks, variants, or threat actors that pose risks to your organization, the prevalence of these attacks and their potential impact can be significant.

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 the security team or the broader enterprise teams 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 when an attack occurs.

"These exercises shouldn't just mark off compliance checkboxes. Instead, they must serve as proactive, high return on investment (ROI) security investments that improve operational resilience, safety, and response readiness. Best of all, they are applicable across all critical infrastructure sectors."[3]

The FortiGuard 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. They 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 assist the team in identifying security gaps in their posture or processes. Guiding participants verbally through the scenarios, facilitators help the company's participants work together, using the provided intelligence from investigations, to determine a course of action for each.

Facilitators raise questions about each scenario and encourage discussion and interaction across the team. This more relaxed environment—utilizing scenarios from actual cyber incidents—provides participants with the opportunity to assess their abilities when they're not under pressure and need to respond to a real incident.

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
- Encourage more effective communication among 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 first-hand 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 the actions that 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 and engaging way to assess an organization's processes, communications, and plans, and ultimately, your collective ability to respond to a cyber incident.

At the close of the exercises, TTXs help you and your team 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 a subscription service that allows you to select 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 the option to choose from several services that can include:

- Incident response readiness assessment
- Incident response playbook development
- Tabletop exercises (incident response playbook testing)
- Offensive services such as penetration testing and red teaming
- Digital forensics and incident response (with a one-hour service-level objective)

Additional hours may be purchased as needed. Fortinet also offers the FortiGuard Incident Readiness Subscription Service Lite, which includes 10 initial service points (40 hours) and a 24-hour service-level objective.

Strengthen Your Security Posture with TTXs

Regardless of the latest threats or changes in your enterprise, TTXs provide security leaders with an understanding of the efficacy of their current incident response playbook. Security leaders gain visibility into quantifiable gaps and get suggested actions 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 gained can inform your security design to withstand and evolve with the changes to your enterprise and in the threat landscape, helping you better prepare for “game day” or when the “rubber hits the road.”

To learn more about FortiGuard Tabletop Exercises or to schedule your next TTX, contact FortiGuard Labs.

[1] Key Findings from the Fortinet 2025 Operational Technology Security Report, Fortinet, July 9, 2025, https://www.fortinet.com/blog/business-and-technology/key-findings-from-the-fortinet-2025-operational-technology-security-report.

[2] Robert Lemos, Industrial System Cyberattacks Surge as OT Stays Vulnerable, Dark Reading, February 25, 2025, https://www.darkreading.com/cyber-risk/industrial-system-cyberattacks-surge-ot-vulnerable.

[3] Dean Parsons, ICS/OT-Specific Tabletop Exercises Matter More Now, SANS, August 5, 2025, https://www.sans.org/blog/ics-ot-specific-tabletop-exercises-matter-now.

October 28, 2025 7:13 PM / MKTG-2289-0-0-EN