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

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

## 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 any knowledge of how your operational technology (OT) security posture and processes have changed as your network and personnel have evolved can lead to nasty surprises—at inopportune times like during a cyber incident.

FortiGuard Tabletop Exercises (TTXs) help security teams test plans and processes before a cyber incident. TTXs let you test what to do—whom to call, when to call, and using what criteria—based on the circumstances such as what happened and which devices are impacted. Against the backdrop of change, TTXs provide your teams with real-world scenarios to evaluate your understanding of processes and playbooks and to test your 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.

## OT Networks Exposed to New 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. And it is 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 have already launched new malware attacks—such as CrashOverride/Industroyer, Triton, and VPNFilter—targeting vulnerable OT systems.

In early 2022, the Russian invasion of Ukraine and related geopolitical events placed another spotlight on OT security. In April 2022, the U.S. Cybersecurity and Infrastructure Security Agency (CISA), along with its counterparts in Australia, Canada, New Zealand, and the United Kingdom, warned that Russian state-sponsored actors had stepped up their efforts in response to damaging sanctions imposed by the West. The agencies urged those responsible for critical infrastructure networks to “prepare for and mitigate potential cyber threats—including destructive malware, ransomware, DDoS attacks, and cyber espionage—by hardening their cyber defenses and performing due diligence in identifying indicators of malicious activity.”[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.

Enterprises are dynamic, living entities with employee turnover, skillset shortages, and technology changes. This means that your security posture is not static, and therefore nor is your playbook. When considering the biggest cybersecurity challenges executives face, nearly half of executives surveyed in 1,200 companies globally feel their security has not "kept up with digital transformation."[3]

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.

**Industrial control system (ICS) incident response tabletops provide a high return on investment in several important areas. Regularly conducted incident response tabletop exercises are part of a mature ICS security program that can identify weak points in security efforts and enable proactive defense to address this range of threats.[4]**

## 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 to work together with 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—while using scenarios from actual cyber incidents—gives participants 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 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, 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 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 the option to choose 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)

Note: Additional hours may be purchased as needed.

## 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 to 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."

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

[2] Alert (AA22-110A), "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure," CISA, April 20, 2022, revised May 9, 2022.

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

[4] Dean Parsons, "Top 5 Incident Response Tabletops and How to Run Them," SANS, June 16, 2021.

FORTINET

www.fortinet.com



January 24, 2023 4:13 PM

1887120-0-0-EN