DRAGOS

SOLUTION BRIEF

OT Tabletop Exercises

Structured workshops that help organizations anticipate, detect, and respond to real-world xOT cyber threats before an incident occurs.

OT Tabletop Exercises

Structured workshops that help organizations anticipate, detect, and respond to real-world xOT cyber threats before an incident occurs.

Overview

Dragos Tabletop Exercises (TTX) are structured workshops that help organizations anticipate, detect, and respond to real-world xOT cyber threats before an incident occurs. Grounded in Dragos threat intelligence, each engagement uses actual adversary TTPs, historical case studies, and industry-specific scenarios to evaluate incident response plans, identify gaps in detection and defense, and prioritize cybersecurity investments against the most critical assets.

TTX actively drills response capabilities, strengthens cross-team coordination, reduces adversary dwell time, and improves recovery readiness. The outcome is a clear understanding of where defenses stand today, and a prioritized roadmap to reduce operational and financial risk before a real attack tests them.

The Challenge

Plans That Have Never Met an Adversary

✕ Most OT incident response plans have never been evaluated against the adversaries most likely to target the organization. Teams do not know which threat scenarios put their most critical operations at risk, whether they collect the data needed to detect those scenarios, or how coordination holds up when a plan is activated under pressure. Those gaps stay invisible until a real incident exposes them.

How the Dragos TTX Works

✓ Past attacks and recent innovations in adversary toolkits targeting OT are the best basis for evaluating threat preparedness. By identifying your most critical assets in your operations and evaluating relevant threat scenarios against your architecture, you can identify weaknesses and investment priorities before an adversary does.

Dragos maintains a constantly updated repository of threat scenarios, historical case studies, and adversary TTPs built from our OT cyber threat intelligence, covering the electric, oil and gas, manufacturing, water, and transportation industries, as well as other xOT environments.

Six Threat Event Categories

Threat scenarios are organized into six categories, with customization available for your environment.

01 Ransomware

02 Targeted Disablement (OT Malware)

03 Unauthorized Operator Action

04 Third-Party Vendor & Supply Chain Compromise

05 Espionage & Reconnaissance

06 Hacktivism

Three Versions To Conduct a Cyber Drill and Evaluate Your Readiness

TTX starts with choosing threat scenarios and examining impacts, then organizing a drill around those scenarios. The drill emulates the scenario to challenge current incident response plans, practices, and capabilities. Dragos provides three versions of TTX:

Standard TTX

2–3 participants

Uses pre-developed scenarios from Dragos OT Cyber Threat Intelligence with minimal narrative injects. TTX workshops are run with 2-3 customer participants.

Custom TTX

3–4 participants

Starts with the scenarios above and develops additional narrative reflecting impact on the customer's unique asset types, vendors, personnel, partnerships, network architecture, and models. Expands participants (3-4) and can be further broadened in the SOW.

Executive TTX

Leadership & SMEs

Prepares top leadership to guide the incident response team during a serious incident. Leaders, stakeholders, and subject matter experts work through a simulation of an OT cybersecurity incident to understand response capabilities, business interdependencies, and decision-making processes, and to identify gaps in a low-impact environment.

Benefits

Test and Strengthen Your xOT Defenses

Evaluate cyber incident response processes and tools. Identify and correct gaps in your ICS cyber defenses to reduce operational and business risks.

Reduce Adversary Dwell Time

Gain greater awareness of the ICS threat landscape, improve readiness to combat targeted threats, and implement effective response procedures.

Reduce Operational and Financial Impacts

Implement efficient recovery procedures and strengthen internal communications between business units.

What You Can Expect

1

Threat Briefing Pack

A briefing of the threat scenarios, provided during the workshops with a strategic focus on detection, response, and recovery.

2

Key Prepared Materials

Facilitator Handbook, Exercise Agenda, Participant Manual, Facilitator Briefing Presentation (PDF version with ROE and Injects slides).

3

TTX Workshop

Dragos facilitates the exercise focusing on incident response and executive-level roles, responsibilities, authorities, and accountabilities (R2A2). The exercise tests the effectiveness of plan coordination with partners, capability and resource employment, communication flow, and actions taken upon plan activation.

4

After-Action Report (AAR) & Actionable Recommendations

Documents observations across each core capability, with a performance rating measured against expected performance, detailed findings, and prioritized recommendations for improving the Incident Response Plan.

Detect | Communicate | Activate | Respond

Contain | Document | Recover

About Dragos

Dragos delivers xOT cybersecurity for industrial and critical infrastructure, backed by a decade of frontline incident response experience. The Dragos Platform provides asset visibility, continuous monitoring, vulnerability management, and real-time threat detection, all powered by industry-leading intelligence. Dragos protects OT environments globally, including electric, oil and gas, manufacturing, water, and transportation.

Dragos is privately held and headquartered in Hanover, Maryland, operating globally across North America, EMEA, and APAC. Learn more about our technology, services, and threat intelligence offerings: request a demo or contact us.

Learn more: dragos.com