DATASHEET

Threat Baselines & Tabletop Exercises

Threat Baselines and Tabletop Exercises enhance an organization's ability to anticipate, detect, and respond to cyber threats through structured workshops. These services simulate real-world OT security incidents – threat scenarios – that provide intelligence-driven threat models to prioritize cybersecurity investments and reduce operational risks. Drills and exercises can help refine response strategies, identify weak points in plans, improve cross-team coordination, and better prepare organizations for incidents.

Through documentation reviews and staff interviews, Dragos provides tactical and strategic recommendations to enhance the security of critical industrial control systems (ICS). While each review is tailored to the context of your organization, the process includes key modules designed to identify security gaps and deliver actionable insights

Past attacks and recent innovations in adversary toolkits targeting OT are the best approach to evaluating your threat preparedness. By identifying your most critical "crown jewel" assets in operations and evaluating those threat scenarios against your architecture, you can start to identify weaknesses and investment priorities.

Dragos leverages our industry leading OT cyber threat intelligence to maintain a repository of threat scenarios, historical case studies, and adversary TTPs relevant to electric, oil and gas, water and wastewater, transportation, building management systems, data centers, mining, and manufacturing across many segments.

Example scenarios are: Ransomware, IT/OT Trust Abuse, Insider Threat, Trusted Vendor Compromise, XENOTIME, Building Automation, HMI Hijacking, and Generator, with customization available.

BENEFITS

Test And Strengthen Your ICS 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

- Get greater awareness of the ICS threat landscape.
- Improve readiness to combat targeted threats.
- Implement effective response procedures.

Reduce Operational And Financial Impacts

- Implement efficient recovery procedures.
- Strengthen internal communications between various business units.

Threat Baselines: Using Threat Scenarios to Identify Potential Impacts

The Threat Baseline is a structured workshop designed to help organizations identify and prioritize OT-specific cyber threats. Using real-world intelligence and industry threat models, it assesses security risks, detection capabilities, and incident response readiness. The workshop provides actionable recommendations to improve operationalization of intelligence, optimize security investments, and enhance overall threat preparedness.

Deliverable	Description
Threat Briefing Pack	A briefing of the current threat landscape and the chosen threat scenarios will be provided during the workshops with a strategic focus on detection, response, and recovery.
Workshop	Collaborative sessions to transfer knowledge of the current threat landscape and the chosen scenarios. Detailed analysis of the scenarios is provided leveraging adversary, TTPs, the ICS Cyber Kill Chain, case studies, etc. The outcome is the identification of data collection requirements needed for detection & response for the chosen scenarios.
Threat Baseline Report	Prioritized list of recommendations derived from the workshop. Data collection requirements needed for the detection and response of each threat scenario.

Tabletop Exercises: Conduct a Cyber Drill to Evaluate Your Planning

A tabletop exercise (TTX) starts with the approach outlined in the threat baselines – choosing threat scenarios and looking at impacts. It then goes to the next level of organizing a drill around those scenarios. The drill emulates the scenario to challenge the current incident response plans, practices, and capabilities. Dragos provides two versions of TTX:

- **Standard TTX:** leverages pre-developed scenarios from Dragos OT Cyber Threat Intel with minimal narrative injects. TTX workshops are run with 2-3 customer participants.
- **Custom TTX:** Starts with scenarios above and develops additional narrative that include impact on customers unique asset types, vendors, personnel, partnerships, network architecture, and models. Expands participants (3-4) and can be further broadened in SOW.

Deliverable	Description
Threat Briefing Pack	A briefing of the threat scenarios will be provided during the workshops with a strategic focus on detection, response, and recovery.
Key Prepared Materials	Facilitator Handbook, Exercise Agenda, Participant Manual, Facilitator Briefing – Presentation (PDF version with just ROE and Injects slides).
Tabletop Exercise Workshop	Dragos facilitates the exercise focusing on the Incident Response & executive level roles, responsibilities, authorities, & accountabilities (R2A2). The Exercise tests effectiveness of coordination of the plans with partners, capability and resource employment, communication flow, and actions taken upon plan activation.
Post-Exercise Report & Actionable Recommendations	Provides an evaluation of each key step Detect, Activate, Respond, Contain, Communicate, Document, Recover. It evaluates performance in the TTX against expected performance, providing detailed findings and prioritized recommendations for improving the Incident Response Plan.

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East. Learn more about our technology, services, and threat intelligence offerings: **request a demo** or **contact us**.