

Tabletop Exercise (TTX)



CPIRT will develop an agreed-upon scenario-based exercise where people with roles and responsibilities in an Incident Response plan participate in a virtual/room setting to validate the content of the plan by discussing their responsibilities and responses during an incident in order to identify improvement areas in the areas of the plan (processes/procedures/communications/responsibilities), evaluate technical implementations, and identify gaps in the IR Plan and relevant playbooks. CPIRT facilitators initiate the discussion by presenting a scenario and posing a set of questions based on the events in the scenario.

Aim: Validate the Incident Response Plan and playbooks relevant to the scenario and identify potential gaps and issues.

Deliverables: A written report of the observed TTX findings and their recommendations. Where valid and possible, the recommendations will be tied to the CIS Controls.

Methodology: gather exercise objectives, propose scenarios, validate, execute/facilitate, report

Benefits:

Enhanced Preparedness: A TTX provides an opportunity to test and validate an organisation's Incident Response (IR) plan and playbooks. By simulating a realistic scenario, participants can identify gaps and weaknesses in the plan, allowing for improvements to be made. This exercise helps to ensure that the organization is better prepared to respond effectively in the event of an actual incident.

Collaborative Learning: The exercise brings together individuals with different roles and responsibilities within the IR plan. By participating in discussions and sharing their perspectives, participants can learn from each other's experiences and knowledge. This collaborative learning environment fosters a better understanding of the overall incident response process and facilitates communication and coordination among team members.

Identification of Improvement Areas: Through the TTX, participants can evaluate the processes, procedures, communications, and responsibilities outlined in the IR plan. By discussing their roles and responses during the simulated incident, they can identify areas where the plan may be lacking or where improvements can be made. This exercise helps to refine the IR plan, ensuring it aligns with the organisation's needs and best practices.

Mitigation of Risks: By proactively conducting TTX's, organisations can identify potential gaps and issues in their IR plans and playbooks. By addressing these gaps and improving the plan, organisations can mitigate those risks potentially leading to incidents. Through the exercise, they can discover weaknesses, vulnerabilities, or potential bottlenecks that could impact their ability to respond swiftly and effectively. By addressing these concerns beforehand, organisations can reduce the impact of incidents and potentially avoid costly consequences.

*“Get **prepared BEFORE**
an incident occurs“*