TABLETOP-IN-A-BOX

Thank you for downloading our tabletop-in-a-box. Use these instructions and the materials provided to conduct a tabletop exercise with your team and test your incident response plan and preparedness.

NEED AN EXAMPLE OF A TABLETOP EXERCISE IN ACTION?

Watch the live tabletop session we hosted during hack_it 2020 for some inspiration.

BEST PRACTICES TO KEEP IN MIND

Players should use existing plans, policies, procedures, and resources to guide their responses.

Discussions should focus on key actions, activities and decisions that each Player would perform given the specific scenario conditions.

Players should first discuss the actions stipulated by the scenario but are welcome to engage in "what if" discussions of alternative scenario conditions.

There is no "hidden agenda" nor are there any trick questions.

WHAT IS A TABLETOP EXERCISE?

A tabletop exercise is a preparedness activity designed to test your organization's incident response protocols, tools and proficiency in reacting to cybersecurity threats. The exercise takes participants through the process of dealing with a simulated incident scenario that can then highlight gaps in incident response planning.

TABLETOP EXERCISE GOALS

The purpose of a tabletop exercise is to validate your existing incident response plan and identify its strengths and weaknesses before an actual incident occurs. These exercises are designed to be a learning tool and facilitate open discussion.

HOW TO CONDUCT YOUR TABLETOP EXERCISE

First, you must designate roles. Most effective tabletop exercises are led by an individual Facilitator who will lead the gameplay for the Players.

FACILITATOR

The Facilitator will guide the Players through the scenario and is responsible for ensuring that discussions remain focused on the exercise objectives. They are also responsible for making sure everyone is included in the conversation and has the opportunity to participate.

PLAYERS

Players have an active role in discussing their preparedness, response and recovery activities during the exercise. Players should discuss or initiate actions based on the simulated exercise scenario and corresponding questions.

Once all roles have been assigned, the Players will then randomly split into two teams: the 'Business Leads' and the 'Technical Leads'. As Players go through the exercise, they should challenge themselves to think about how they would respond based on the team they've been assigned.

HUNTRESS

The Facilitator will then go through the Tabletop Exercise (in PowerPoint format), present the scenario, take the Players through the exercise questions and facilitate the discussion. At certain points, 'Injects' and 'Discussion Points' will show up to either present a new piece of information, take the discussion in a new direction or expand the discussion in some way.

Upon completion of the exercise, all participants should regroup for a debrief and evaluation. You can use the instructions below to facilitate your debrief discussion.

DEBRIEF AND EVALUATION

A debrief should be held immediately following the exercise. The purpose of the debrief is to come together to collect all participants' observations and feedback and evaluate both the exercise and your team's incident response preparedness.

WANT TO CONTINUE YOUR INCIDENT RESPONSE EDUCATION?

Here are some materials that can help:

Pre-Incident Checklist
Incident Response Checklist

If you have any questions or feedback on how to improve this exercise, please reach out to **marketing@huntresslabs.com.**

DEBRIEF DISCUSSION QUESTIONS

As a group, discuss the following questions:

- Was the exercise scenario realistic for your organization, processes and current security posture?
- Did communications and processes flow as expected throughout the exercise? If not, why and where were the gaps?
- What other plans, policies, or procedures would players implement to respond to the incident described in the exercise scenario?
- On a scale of 1–5 (with 5 being the best), how would you rate your team on how well you handled and responded to the incident described in the exercise scenario?
- Do you have any recommendations for improvements or areas that require follow-up?
- Is everyone sufficiently familiar with the incident response plan established by your organization?
- What parties and persons should be involved throughout a cyber-related incident? Are roles and responsibilities clearly defined? Are there other teams or persons in the organization who should be included?
- What actions do all participants plan to take in order to address any outstanding issues?