

Incident Response Tabletop Exercise

|  |  |
| --- | --- |
| **Exercise title** |  |
| **Exercise date/time/location** |  |
| **Scope** | Describe the scope of the incident response tabletop exercise. |
| **Purpose** | To uncover <company's> preparedness against <attack scenario> due to <attack vector>. |
| **Objectives** | List objectives of the exercise. For example:1. Assess <company's> ability to detect <attack vector>.
2. Assess <company’s> ability to respond to <attack>.
3. Assess <company’s> ability to analyze <attack vector>.
4. Assess <company’s> ability to mitigate/eliminate malware.
5. Evaluate <company's> communication capabilities during a <attack scenario>.
 |
| **Attack vector** | List initial attack vector. |
| **Incident scenario** | List incident scenario. |
| **Team members** | List participants, including but not limited to exercise facilitator, exercise moderator, exercise scribe and responders. |
| **Discussion questions** | Include discussion questions based on the attack vector and attack scenario based on the steps in the incident response lifecycle:* Preparation
* Detection
* Analysis
* Containment
* Eradication
* Recovery
* Post-incident activity
* Other questions
 |
| **Notes** | List notes taken during the exercise. |
| **Post-exercise recommendations and review** | Include any post-exercise activities or recommendations. For example, summarize how the tabletop exercise can be improved and how the incident response plan can be adjusted or improved. |