Tutorial 3 – Tabletop/simulation exercise tutorial

Due date: 18 August 11.59pm

Weighting: 3%

a) In your own words, write no more than 500 words about the various stages in an incident response tabletop exercise (also known as a wargame or simulation)

This could include the stages of Planning and Preparation, Introduction, Exercise Execution, Debrief and Analysis, Follow-Up.

Was present at the in-person Deloitte tutorial on the 9th of August. This is what I remembered on how the simulation took place.

The **introduction** stage was where all participants were briefed on the exercise's purpose and goals for incident response. Deloitte conductors explained how the simulation (war games) is beneficial for testing, problem-solving, and decision-making skills, as well as assessing how well incident response procedures translate to real-world situations. The scenario that was presented was concerned with a "Theme Park Roller Coaster" speed that was safety-critical. They presented this current issue/threat at hand providing all groups with the necessary context to establish a clear timeline and understand the challenge they were about to face.

During the **exercise execution**, participants were prompted with further context as the situation developed, as well as questions and subsequent steps/actions the company's employees, engineers, and responders should take. This involved the conductors providing real-time events and providing supporting documentation/artifacts that reflected the evolving situation.

We were presented with the context of further developments and information such as employee access logs, SSH/IP logs, and system admin changes. We were then tasked with investigating irregularities based on supporting documentation that was provided for each question. This involved keeping track of access times, finding potential security hazards, and finding potential malicious actors in the logs. From here we could use problem-solving skills on what the best course of action was to take.

In group discussions, participants collaboratively decided on the best course of action to mitigate the threat at each stage. This process includes identifying the nature of the incident, containing the threat, and ensuring effective communication with stakeholders and the public. The exercise emphasizes the importance of collaboration, as the groups must investigate findings from the documentation and scenario to make informed decisions in real time.

Following each group discussion, a 'debrief and analysis' session takes place, where an open discussion among all groups, run by the conductors, allows for reflection on the decisions each group made. Each group presents their chosen action with the rationale behind it. The conductors then reviewed these actions, identifying the most effective response and providing justification for why it was considered the 'correct' choice. This analysis involved working through the list of possible answers/steps provided for the given scenario and explaining how one approach was deemed more appropriate given the circumstance at that point in time. This stage was crucial for learning as it highlighted real-world reasoning on why a strategy worked for that given situation, whether that was communication with the public/stakeholders or engineers rebooting the system, and identified what they would also do given different situations for the other risks that were possible answers. When we discussed and answered all stages of the incident response, we reached conclusions on how and why the threat took place, identified the malicious parties, mitigated the threats, and communicated with the public effectively.

b) Discuss some benefits of incident response tabletop/simulation Exercises

These are some of the benefits I took away from participating in the incident response simulation. I learned how to handle real incidents by participating in a team environment to practice response procedures. This allowed me to improve my communication and collaboration skills within a team in a safe controlled environment as well as helped me to use and improve my decision-making skills in a 'pressured' situation. By improving my communication, collaboration, and decision-making skills, I feel like I would be more confident in real-world scenarios.

You may answer the sections above using bullet points.

Specify whether you were present at the in person session on 9 August, or if you are completing this tutorial remotely. Students who were able to attend this session in person, please base your answers around the Deloitte session. Those who were not able to attend the session can answer from research alone.

Groupwork (where possible):	Discussion	1 point
Individual work:	Submission of document and reasoning 2 points	

Submissions will be marked individually and must be submitted by 18 August 11.59pm. This work should be in your own words. Any AI tools should only be used to brainstorm or edit. You must acknowledge any use of AI.