ManageEngine
Log360

STEPS TO CONDUCT AN EFFECTIVE

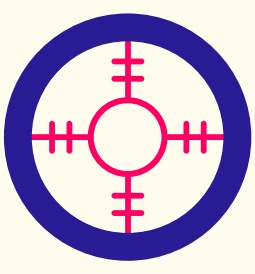
CYBERWAR GAME FOR A CISO

01 CHOOSE THE OBJECTIVE OF THE GAME

What do you want to achieve through the game? Have clear objectives. Here are a few examples:

- To determine the MTTD and MTTR of attacks
- To review the effectiveness of security controls
- To preempt the worst-case scenario in terms of an attack
- To train the defense team to be better prepared
- To assess the overall security posture and maturity

02 DECIDE THE SCOPE FOR THE GAME



What theme are you going to choose for the game, and how elaborate is it going to be? To determine this:

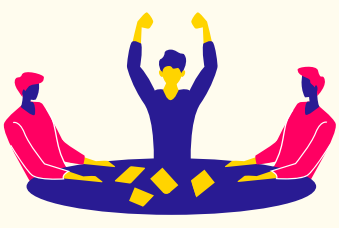
- Choose an attack that your organization is vulnerable to.
- Decide the number of days the game is going to run, who's going to participate, and the extent and range of the attack.

03 CHOOSE THE ORGANIZER OF THE GAME

Who is going to organize and conduct the game?

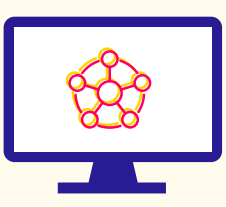
- Decide whether it's going to be outsourced or organized internally.
- If you outsource, you need to decide if you're going to do it partially or completely.
- Determine the facilitator, either yourself or an external war-game expert.

04 DECIDE THE MODE OF THE GAME

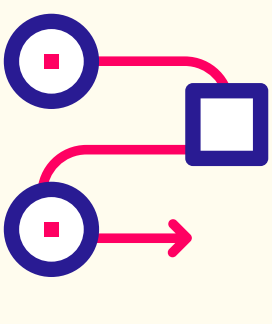


Are you going to conduct it virtually or offline?

- Decide if the game is going to be a discussion-based tabletop exercise or a simulation-based exercise.
- If it's the latter, create simulations of your organization's business and security architecture in a test environment to make your experience realistic.



05 HAVE MILESTONES FOR ATTACK AND DEFENSE TEAMS



What are the criteria for assigning points and deciding the winner?

- Set milestones for the attack and defense teams based on the objective you chose.
- Once achieved, provide feedback and assign points.
- Do this until all milestones have been achieved and declare the winner.

06 INTERPRET GAME INSIGHTS

How will you interpret the insights inferred from the game?

- Review the game again once it's complete, and inform participants on what they did right along with where they went wrong.
- Based on your inferences, inform security teams in detail about where potential security vulnerabilities exist and how they can be overcome.
- Update your security guidelines and protocols accordingly, and train your team repeatedly so they respond to attacks instinctively.

To learn more **Visit this page**