CERT-PH
NATIONAL COMPUTER EMERGENCY RESPONSE TEAM
DICT

Cyber Incident Drill 2021

Frequently Asked Questions

q1. Who should attend the CERT-PH Cyber Incident Drill?

a1. Anyone under the specified CII sector can be part of the event, even without prior knowledge on cyber threats and attacks. However, it is highly recommended that participating teams are composed of at least one member who has technical functions such as computer and/or network support that handles information/computer security related incidents in their respective organization..

q2. Is there a limit to the number of participants per team?

a2. Yes, we strictly limit three (3) personnel/participants at most per each participating team.

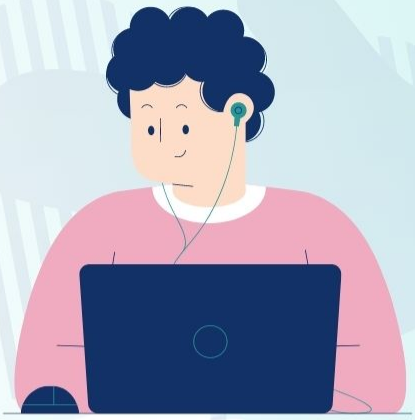
q3. Do we need 3 participants to accomplish the whole drill exercises?

a3. No, at least one (1) dedicated participant can join and complete the drill. We do not limit the number of members per organization who can assist the team in solving the drill scenarios and injects. However, only three (3) officially designated members will have access to the drill platform provided by CERT-PH.

q4. Does the registration limit only one team per organization?

a4. No, there is no limit to the number of teams that can register per organization. However, as stated in q3, there is a limit of three (3) participants per team.

q5. What is the minimum system requirement to accomplish the drill scenarios?



a5. A windows or unix system that have the following system components:

- Processor: 2 Ghz
- RAM: 4 Gb
- Internet Connection: At least 5 Mbps of internet connection

q6. Are there any specific applications/software that you would like to recommend for us to install in the computers we're going to use for the drill?

a6. Tools and platforms will be helpful in solving the challenges:

- For Windows based operating system users:
  - Source Code Editor (e.g Notepad++, Sublime Text)
  - Open-source/free/license spreadsheet for reading CSV files
  - File text scanner / extractor
  - Online IP geolocation checker
  - Online mail blacklist checker
- For Unix based operating system users:
  - Terminal basic commands
    - cat
    - uniq
    - strings
    - grep
    - awk
    - file
  - Password cracking tool
  - Online IP geolocation checker
  - Online mail blacklist checker

CERT-PH
NATIONAL COMPUTER EMERGENCY RESPONSE TEAM
DICT

Cyber Incident Drill 2021

In addition to this, CERT-PH does not require the use of Virtual Machine (VM)s for the conduct of the dril. However, even though this is only a scenario-based activity, CERT-PH recommends to adopt incident response best practices such as conducting investigation on a separate environment from your organization's network, e.g., VMs or computers that are on an isolated network.

CERT-PH
NATIONAL COMPUTER EMERGENCY RESPONSE TEAM

DICT

Cyber Incident Drill 2021

q8. Is it mandatory to install Discord in our Desktop/Laptop?

a8. No, participants may also use the Discord mobile application as an alternative.

q7. Who can we contact if there are problems and/or issues encountered during the drill?

a7. Private Discord channels will be used for CERT-PH to accommodate the participants regarding their questions and inquiries.

q9. Can we allow non-registered participants to join the pre-drill and actual drill event?

a9. No, we will not accommodate additional participants past the registration deadline as this may disrupt the event flow. Participants are required to attend the pre-drill (technical briefing) as necessary technical details about the conduct of the actual drill will be discuss the facilitators.

q10. What if I cannot join the Pre-Drill (Technical Briefing) activity?

a10. Your team must have at least one (1) dedicated member to participate in the pre-drill who can relay the information discussed during the pre-drill activity to the entire team.

The attendance form must still be accomplished either by you or your teammate.