

No. AJ-0001/22003

ASEAN-Japan Cybersecurity Capacity Building Centre  
15<sup>th</sup> Floor, The 9<sup>th</sup> Towers Grand Rama 9 (Tower B)  
33/4 Rama IX Road, Huai Khwang, Bangkok 10310

4<sup>th</sup> November 2022

### Invitation to Register for Technical Skill Training Related to Incident Response using a CTF Format


Dear Sir or Madam,

The ASEAN-Japan Cybersecurity Capacity Building Centre or AJCCBC (the Centre) under the Electronic Transactions Development Agency (“ETDA”), Ministry of Digital Economy and Society of Thailand is delighted to introduce you **“Technical skill training related to incident response using a CTF format”** that has been developed to strengthen cybersecurity workforces within ASEAN region. The course will be available on a self-learning platform from **10<sup>th</sup> January – 10<sup>th</sup> March 2023**. In this regard, the Centre would like to invite the participants from government sector and Critical Information Infrastructure (CII) to register for the training **by 7<sup>th</sup> December 2022**.

The Centre would appreciate if AMS participants could fill out the registration form by the indicated deadline. Details of Technical skill training related to incident response using a CTF format are provided in the enclosed General Information. Should you have any questions, please do not hesitate to contact [intl.cybersecyrity@ml.soumu.go.jp](mailto:intl.cybersecyrity@ml.soumu.go.jp). We look forward to welcoming AMS participants soon.

Please note that this registration is on a first come first served basis.

Yours faithfully,

  
Meetham  
Na Ranong

(Mr. Meetham Na Ranong)

Project Executive

ASEAN-Japan Cybersecurity Capacity Building Centre

# Technical skill training related to incident response using a CTF format

## ASEAN-JAPAN CYBERSECURITY CAPACITY BUILDING CENTRE (AJCCBC)

10<sup>th</sup> January – 10<sup>th</sup> March 2023

---

### GENERAL INFORMATION

#### 1. OVERVIEW

“Technical skill training related to incident response using a CTF format” aims at arming learners with technical skills related to incident response. The learners will gain knowledge of 4 cybersecurity areas, including log analysis, network analysis, malware analysis, and attack survey in a CTF\* format, which consists of 50 questions.

#### 2. Target Group

The target learners are officials in government or Critical Information Infrastructure (CII) in AMS who do not have much practical experience in cybersecurity but have basic knowledge of information, communication, networking, and cybersecurity.

#### 3. PREREQUISITE FOR TRAINEES

Necessary hardware and systems arrangement by trainees:

##### 1. Equipment Requirements:

Web browser: Major browser such as Internet Explorer, Microsoft Edge, Google Chrome

##### 2. Necessary knowledge:

- Basic cybersecurity knowledge on incident response.
- Basic knowledge and skills on Linux and related command.
- Good working knowledge of English.

\* Abbreviation for Capture the Flag: A quiz format in which participants use their security skills to search for hidden answers (flags) and submit their answers.



**MDES**  
Ministry of Digital Economy and Society



### 3. Recommended Tools to solve the CTF courses:

To solve the questions, it is recommended to download the tools to your devices.

The recommended tools are listed below:

- Wireshark: <https://www.wireshark.org/download.html>
- GitHub: <https://github.com/openwall/john>
- dtoPeek: <https://www.jetbrains.com/decompiler/>

### 4. REGISTRATION

Please use the following link or QR code to register. Please note that the seat of the training is on a first-come, first-served basis.

Technical skill training related to incident response using a CTF format



<https://forms.office.com/r/YyRULi9gRO>

Deadline: 7<sup>th</sup> December 2022

### 5. QUESTION ABOUT THE COURSE

If you have any question or need further information about the course, please contact [intl.cybersecyrit@ml.soumu.go.jp](mailto:intl.cybersecyrit@ml.soumu.go.jp).

\* Abbreviation for Capture the Flag: A quiz format in which participants use their security skills to search for hidden answers (flags) and submit their answers.