Details about the workshop.

1. Program details/contents

Incident Handling and Management: Tools, Techniques, Response and Procedures

This training is specially conducted to equip participants with the intermediate knowledge in incident handling, forensic analysis and cyber defense. Participants will be exposed to the security environment through practitioners' experience sharing, case studies and hands on exercises by doing relevant analysis with the related tools. For digital forensics, the module will enhance the participants' capability in identifying digital evidence for the targeted incident. Participants will be exposed to the Standard of Procedure (SOP) in handling and conducting the forensics analysis and also the way they should present the all analysis findings to the stakeholders. Cyber defense strategies will also be included as to mitigate operational risks.

2. Workshop plan (with time duration)

Module 1 (2 hours):

- Security Incident and Handling
- Incident Handling: Objective, Importance, Definition
- Incidents: Classification, Response Level, Priorities
- Standard Procedures (Steps) Involved in Incident Handling
- Digital Forensics, First Responder Procedures, Forensic Analysis and Digital Forensics Report Writing

Module 2 (1 hour):

- Cyber Defense Strategies in Mitigating Operational Risks

Module 3 (1 1/2 hours hands-on):

- Real Sample Incidents and Case Study
- Log analysis

Module 4 (1 1/2 hours hands-on):

- Real Sample Incidents and Case Study
- Analyzing malware samples