Training sheet - Incident response and forensics analysis techniques

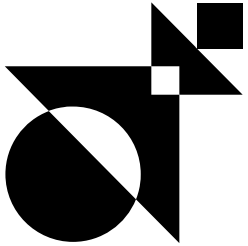
CONTACT FOR THIS TRAINING

Miora RAHARINIRINA
Almond Institute coordinator
almond.institute@almond.eu
+33 7 64 42 71 56

- Version 1.0
- 22/07/2024

Incident response and forensics analysis techniques

Course overview



This training program is designed to train IT teams to the best incident response practices once a security incident has been detected. This course presents the state-of-the-art techniques commonly used by CERT analysts to delimit the impacted perimeter, identify the cyber criminals' modus operandi, the killchain and the Tactics, Techniques and Procedures (TTPs and tools). It details the best practices to be adopted for collecting evidence, analyzing system, network or malicious code artifacts to identify indicators of compromise, traces of attacks, evidence of exfiltration, persistence mechanisms installed, etc. in compliance with PCI-DSS requirements.

01. Understanding the challenges of forensic science

02. Identifying forensic challenges

03. Investigating a cyber attack

04. Collecting evidence

05. Analyze artifacts

06. Understanding KillChain

07. Present results and sequence of events

08. Write a report with a timeline and summary

09. Prepare a list of suitable recommendations

10. Taking a step back from the crisis

→ READ MORE

Incident response and forensic analysis techniques

Useful informations

Who should attend?

- IT Team
- CISO
- Support team
- System administrator
- Network administrator
- Security Analyst (SOC/CSIRT)

Entry requirements

- Computer basics: network (protocols, OSI model, etc.) and system (Linux or Windows, server management, etc.).
- Knowledge of log analysis (Event ID, network logs, AV)

Method of assessment

Production of a final online questionnaire covering all the concepts learned.

How and when to access

The participant is considered registered when:

- The prerequisites and needs are identified and validated
- The training agreement is signed

Registration requests can be sent up to 10 working days before the start of the training.

To go further

This training course is a preparation for the following training course:

- Advanced system forensics techniques
- Crisis and major incident management

Accessibility

Whether you are recognized as having a disability or not, making our training accessible to everyone is part of our commitment. If you need compensation or adaptation for the content, the supports, the "venue", the material used, the schedules, the rhythm, **we are at your disposal**.

Incident response and forensic analysis techniques

Almond INSTITUTE

Face-to-face and distance learning

Course curriculum

Introduction	Role of CERT	Evidence collection	Artifacts Analysis	Timeline and Collaborative Work	Crisis management	Summary of results
→ Cybersecurity context → Some figures around cybercrime → Reminder of the concepts of DICT → History of forensics from start to digital	→ Phases of an incident lifecycle → Focus on the E3R sequence → Roles and responsibilities of incident response teams → First aid gestures → Definition of the scope of intervention (+scoping) → Setting Goals	→ Choice of elements → Chain of custody (hash, copy) → Online vs. offline collection → Disk copy (software vs hardware) → Backups	→ Parsing → Processing → Identification of suspicious elements → Memory Analysis → FileSystem Analysis → Artifact analysis → Network communication analysis → Malware	→ Creation of the timeline → Working together on the same incident → Shared note-taking → Share the right level of information (pivots / IOCs) → Get organized	→ The main principles → Logistics → Mistakes not to make → Long time → Communication → Authorities → RETEX Ransomware	→ Writing of the investigation report → Recommendations → Feedback and lessons learned → Respect of the evidence → Anonymized reports

Training benefits

- → Training provided by a defensive security expert
- → Operational recommendations
- → Practical tools
- → Real-life case studies

Prices and informations

- → **Duration:** 21 hours (3 days)
- → **Price:** Contact us
- → **Financing :** OPCO support