Fiche de formation
Techniques de réponse à incidents et d'analyse forensique

CONTACT POUR CETTE FORMATION

Miora RAHARINIRINA
Chargée de mission formation
almond.institute@almond.eu
07 64 42 71 56

- Version 1.0
- 26/06/2024

Techniques de réponse à incidents et d'analyse forensique

Les objectifs pédagogiques

Ce programme de formation vise à former les équipes IT aux bonnes pratiques de réponse à incident et d'investigation, une fois un incident de sécurité détecté. Ce module présente les techniques à l'état de l'art, couramment utilisées par les analystes CERT pour collecter les preuves, délimiter le périmètre impacté, identifier le modus operandi des cybercriminels, la chaine d'attaque et les Tactiques, Techniques et Procédures (TTP et outils). Il détaille les bonnes pratiques à adopter pour collecter les preuves, analyser les artefacts systèmes, réseaux ou de codes malveillants pour identifier les indicateurs de compromission, les traces d'attaques, preuves d'exfiltration, mécanismes de persistances installés, etc.

01. Comprendre les enjeux de la criminalistique

02. Identifier les challenges du forensique

03. Investiguer après une cyberattaque

04. Collecter des preuves

05. Analyser des artefacts

06. Comprendre la KillChain

07. Présenter ses résultats et la séquence des évènements

08. Rédiger un rapport avec une timeline et un résumé

09. Préparer une liste de recommandations adaptées

10. Prendre du recul sur la crise

Techniques de réponse à incidents et d'analyse forensique

Informations pratiques

Public

- Équipes IT
- RSSI
- Équipes support
- Administrateurs système
- Administrateurs réseau
- Analystes sécurité

Prérequis

- Notions de base en informatique : réseau (protocoles, modèle OSI, etc.) et système (Linux ou Windows, gestion d'un serveur, etc.)
- Connaissance en analyse de logs (Event ID, journaux réseau, AV)

Évaluation des acquis

Réalisation d'un questionnaire en ligne final recouvrant l'ensemble des notions apprises.

Modalités et délai d'accès

L'apprenant est considéré inscrit lorsque :

- Les prérequis et besoins sont identifiés et validés
- La convention de formation est signée

Les demandes d'inscription peuvent être envoyées jusqu'à 10 jours ouvrés avant le début de la formation.

Accessibilité

Que vous soyez reconnu en situation de handicap ou pas, rendre notre formation accessible à toutes et à tous fait partie de notre engagement.

Si vous avez besoin d'une compensation ou adaptation pour le contenu, les supports, le « lieu », le matériel utilisé, les horaires, le rythme, **nous sommes à votre écoute.**

Techniques de réponse à incidents et d'analyse forensique

La formation en présentiel ou distanciel

Programme

Introduction	Rôle du CERT	Collecte de preuves	Analyse d'artefacts	Timeline et Travail collaboratif	Gestion de crise	Synthèse des résultats
→ Contexte cybersécurité → Quelques chiffres autour du cybercrime → Rappel des notions de DICT → Histoire du forensique jusqu'au digital	→ Phases du cycle de vie d'un incident → Focus sur la séquence E3R → Rôles et responsabilités des équipes de réponse aux incidents → Gestes de 1^{iers} secours → Définition du périmètre d'intervention (+scoping) → Définition des objectifs	→ Choix des éléments → Chain of custody (hash, copie) → Collecte onligne vs collecte offline → Copie de disques (software vs hardware) → Les backups	→ Parsing → Processing → Identification d'éléments suspects → Analyse Mémoire → Analyse FileSystem → Analyse artefacts → Analyse com' réseau → Malwares	→ Création de la timeline → Travailler à plusieurs sur un même incident → Prise de note mutualisée → Partager le bon niveau d'informations (pivots / IOC) → S'organiser	→ Les grands principes → La logistique → Les erreurs à ne pas commettre → Temps long → Communication → Autorités → RETEX Ransomware	→ Rédaction du rapport d'investigation → Les recommandations → Retour d'expérience et leçons apprises → Respect de la preuve → Rapports anonymisés

Les plus de la formation

- Formation dispensée par un expert en sécurité défensive
- Recommandations opérationnelles
- Compatible exigences PCI-DSS
- Outils pratiques
- Études de cas réels

Tarifs et infos

- **Durée :** 21 heures (3 jours)
- **Tarif :** contactez-nous
- **Financement :** Prise en charge OPCO