Fiche de formation
Techniques de réponse à incidents et d'analyse forensique dans le cadre du standard PCI-DSS

CONTACT POUR CETTE FORMATION

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

- Version 1.0
- 06/02/2024

Techniques de réponse à incidents et d'analyse forensique dans le cadre du standard PCI-DSS

Les objectifs pédagogiques

Ce programme de formation vise à former les équipes IT aux bonnes pratiques de réponse 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 délimiter le périmètre impacté, identifier le modus operandi des cyber criminels, 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, dans le respect des exigences du standard PCI-DSS.

01.

Sensibiliser les équipes IT aux bonnes pratiques de réponse à incident.

02.

Présenter les techniques couramment utilisées par les CERT pour délimiter le périmètre, identifier le mode opératoire et les TTP des attaquants.

03.

Détailler les bonnes pratiques à adopter pour collecter, analyser les preuves techniques permettant de comprendre la séquence des évènements et la KillChain dans le respect du standard PCI-DSS.

Techniques de réponse à incidents et d'analyse forensique dans le cadre du standard PCI-DSS

Informations pratiques

Public

- Équipe IT
- RSSI
- Équipe support
- Administrateur système
- Administrateur réseau

Prérequis

- Notions de base en informatique : réseau (protocoles, modèle OSI, etc.) et système (Linux ou Windows, gestion d'un serveur, etc.)

Évaluation des acquis

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

Modalités et délai d'accès

Le stagiaire 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 dans le cadre du standard PCI-DSS

La formation en présentiel ou distanciel

Programme

Introduction	Cycle de vie d'un incident	Rôle du CERT	Collecte de preuves	Analyse d'artefacts et timeline	Travail collaboratif	Synthèse des résultats
→ Contexte cybersécurité → Rappel du standard PCI-DSS et des exigences relatives à la réponse à incident → Rappel des notions de cycle de vie d'un incident → Bases du forensique	→ Phases du cycle → Focus sur la séquence E3R	→ Rôles et responsabilités des équipes de réponse aux incidents → Définition du périmètre d'intervention → 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 / malveillants et levée de doute → Création de la timeline → RETEX / Focus sur AWS	→ Travailler à plusieurs sur un même incident → Prise de note mutualisée → Partager le bon niveau d'informations (pivots / IOC) → S'organiser	→ Rédaction du rapport → Les recommandations → Retour d'expérience et leçons apprises → Respect du standard

Les plus de la formation

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

Tarifs et infos

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