ADVANCIA TRAINING

Performing CyberOps Using Cisco Security Technologies (CBRFIR)

Réf. CBRFIR · Cisco · Cybersécurité · **Formation certifiante**

DURÉE	NIVEAU	MODALITÉS	VOUCHER EXAMEN
5 jours	**Avancé**	**Présentiel · Live · Intra**	**Inclus**

Présentation

CBRFIR spécialise les professionnels de la cybersécurité dans la forensique numérique et la réponse à incident (DFIR). Vous apprenez à collecter et préserver les preuves, à analyser la mémoire, le disque et le réseau, et à conduire les phases de confinement et de remédiation, dans un parcours validant l'examen de concentration Cisco Certified CyberOps Professional.

Objectifs pédagogiques

- Appliquer les fondamentaux de la forensique numérique et de la réponse à incident
- Collecter et préserver les preuves numériques en respectant la chaîne de possession
- Réaliser l'analyse forensique de la mémoire, du disque et du réseau
- Conduire les phases de confinement, d'éradication et de récupération
- Analyser les artefacts d'attaque et les malwares
- Automatiser les tâches de forensique et d'IR avec les technologies Cisco

Programme détaillé

1. Module 1 — Fondamentaux forensiques et IR

- Cadres NIST et MITRE ATT&CK
- Types de preuves numériques
- Aspects légaux et réglementaires
- Chaîne de possession

2. Module 2 — Collecte et préservation des preuves

- Acquisition d'images disque et mémoire
- Live response
- Ordre de volatilité
- Intégrité et empreintes de hachage

3. Module 3 — Analyse forensique

- Forensique mémoire (ex. Volatility)
- Analyse disque et systèmes de fichiers
- Artefacts Windows et Linux
- Forensique réseau

4. Module 4 — Réponse à incident

- Détection et triage
- Confinement, éradication, récupération
- Analyse des malwares
- Renseignement sur les menaces

5. Module 5 — Automatisation et reporting

- Cisco Secure Endpoint et SecureX
- Scripts et playbooks
- Rédaction du rapport d'incident
- Leçons apprises

Prérequis

Maîtrise des fondamentaux CyberOps (CBROPS ou CBRCOR recommandé) et bonnes connaissances des systèmes d'exploitation et des réseaux.

Public visé

Analystes forensiques, membres d'équipes DFIR/CSIRT et analystes SOC de niveau 2 et 3.

Ce qui est inclus

- Support de cours officiel Cisco (Digital Learning)
- Travaux pratiques de forensique et de réponse à incident
- Voucher d'examen de certification 300-215
- Attestation de réussite Advancia Training
- Pauses-café, déjeuner et accès à un formateur expert certifié Cisco

Certification

Prépare à l'examen de concentration 300-215 CBRFIR (environ 90 minutes, QCM), l'un des examens du Cisco Certified CyberOps Professional. Advancia Training est centre d'examen agréé Pearson VUE : passez votre certification sur place.

1 900 DT HT / participant — tarif inter-entreprise · financement CNFCPP possible