ADVANCIA TRAINING

IBM Security QRadar SIEM Foundations

Réf. BQ105G · IBM · Cybersécurité

DURÉE	NIVEAU	MODALITÉS	VOUCHER EXAMEN
3 jours	**Fondamental**	**Présentiel · Live · Intra**	**En option**

Présentation

IBM Security QRadar est l'une des plateformes SIEM les plus déployées pour la détection et l'investigation des menaces en temps réel. Cette formation fondamentale initie les analystes à la navigation dans la console, à l'analyse des offenses et à l'exploitation des flux d'événements et de réseau. Elle constitue le socle indispensable pour opérer efficacement au sein d'un SOC.

Objectifs pédagogiques

- Naviguer dans la console QRadar et ses différents onglets
- Analyser et investiguer les offenses de sécurité
- Exploiter les activités de logs (Log Activity) et réseau (Network Activity)
- Comprendre le rôle des sources de logs, des flows et des assets
- Construire des recherches et filtres pour l'investigation
- Générer des rapports de sécurité à partir des données collectées

Programme détaillé

1. Module 1 — Introduction à QRadar SIEM

- Rôle d'un SIEM et principes de QRadar
- Architecture : collecteurs, processeurs et console
- Navigation dans l'interface et les tableaux de bord
- Notions d'événements, de flows et de magnitude

2. Module 2 — Investigation des offenses et des activités

- Comprendre la création et le cycle de vie d'une offense
- Analyse d'une offense : source, cible et contexte
- Exploration de Log Activity et Network Activity
- Recherches, filtres et regroupements de données

3. Module 3 — Assets, règles et reporting

- Gestion des assets et enrichissement du contexte
- Introduction aux règles de corrélation et building blocks
- Sources de logs et intégration des équipements
- Création et planification de rapports de sécurité

Prérequis

Connaissances de base en administration système, en réseaux TCP/IP et en concepts de sécurité informatique. Aucune expérience préalable de QRadar n'est requise.

Public visé

Analystes SOC débutants, administrateurs sécurité, ingénieurs systèmes et réseaux impliqués dans la supervision de sécurité.

Ce qui est inclus

- Support de cours officiel IBM
- Travaux pratiques d'investigation sur console QRadar
- Attestation de fin de formation Advancia Training
- Pauses et déjeuners inclus
- Accompagnement par un formateur expert cybersécurité IBM

Certification

Formation non certifiante ; une attestation de fin de formation Advancia Training est délivrée à l'issue du parcours.

1 150 DT HT / participant — tarif inter-entreprise · financement CNFCPP possible