

IBM QRadar SIEM Advanced Topics

Réf. BQ205G · IBM · Cybersécurité

DURÉE 2 jours	NIVEAU Avancé	MODALITÉS Présentiel · Live · Intra	VOUCHER EXAMEN En option
-------------------------	-------------------------	---	------------------------------------

Présentation

Une plateforme SIEM ne délivre sa pleine valeur qu'avec des règles finement réglées et des recherches puissantes. Cette formation avancée approfondit la personnalisation de QRadar : règles et building blocks, reference sets, propriétés personnalisées et langage de requête AQL. Elle permet aux analystes confirmés d'améliorer la précision de détection et de réduire les faux positifs.

Objectifs pédagogiques

- Concevoir des règles de corrélation et des building blocks personnalisés
- Créer et exploiter des reference sets et reference data
- Définir des propriétés d'événements personnalisées (custom properties)
- Rédiger des recherches avancées avec le langage AQL
- Optimiser et régler les règles pour réduire les faux positifs
- Construire des tableaux de bord et rapports avancés

Programme détaillé

1. Module 1 — Règles de corrélation avancées

- Structure des règles, tests et building blocks
- Règles d'événements, de flows, communes et offenses
- Reference sets, reference maps et enrichissement
- Chaînage de règles et scénarios de détection

2. Module 2 — Propriétés personnalisées et recherches AQL

- Création de custom properties par expression régulière
- Introduction au langage de requête Ariel (AQL)
- Recherches avancées, agrégations et fonctions
- Exploitation des données pour l'investigation approfondie

3. Module 3 — Tuning, tableaux de bord et reporting

- Analyse et réduction des faux positifs
- Optimisation et priorisation des règles
- Construction de tableaux de bord personnalisés
- Rapports avancés et indicateurs pour le SOC

Prérequis

Maîtrise des fondamentaux de QRadar (formation BQ105G ou équivalent) et expérience de l'investigation d'offenses.
Bonnes connaissances en cybersécurité et en réseaux.

Public visé

Analystes SOC confirmés, ingénieurs SIEM, administrateurs et référents QRadar.

Ce qui est inclus

- Support de cours officiel IBM
- Ateliers avancés de règles, AQL et tuning sur 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.

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