IBM QRadar SIEM Advanced Topics

Référence : **IBMBQ204G** Durée : **2 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• 1-Avoir des connaissances sur les sujets suivants : • 1.1-Infrastructure informatique. • 1.2-Fondamentaux de la sécurité informatique. • 1.3-Linux. • 1.4-Windows. • 1.5-Mise en réseau TCP/IP. • 1.6-Syslog. • 1.7-Compétences de base pour IBM QRadar Security Intelligence Platform (au moins les compétences enseignées dans le cours IBM QRadar SIEM Foundations - BQ104). • 2-Avoir des connaissances de base en langue anglaise car le support de cours est en langue anglaise.

PROFIL DES STAGIAIRES

• Administrateurs et analystes de la sécurité.

OBJECTIFS

• Découvrir comment créer des sources de journal personnalisées. • Découvrir comment travailler avec des collections de données de référence et des règles personnalisées. • Utiliser les données X-Force et l'application Threat Intelligence. • Utiliser l'application Use Case Manager. • Apprendre à utiliser UBA et QRadar Advisor. • Découvrir l'accordage. • Explorer les scripts d'action personnalisés. • Discuter de l'intégration avec IBM SOAR.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Qradar

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Sources de journal personnalisées

Collectes de données de référence et règles personnalisées

BM X-Force Threat Intelligence dans QRadar

Analyse du comportement des utilisateurs et Advisor avec Watson

Réglage

Scripts d'action personnalisés

Intégration IBM SOAR

*Notre **référent handicap** se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.*