IBM QRadar SIEM Foundations

Référence : **IBMBQ104** Durée : **3 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• 1-Avoir des compétences en infrastructure informatique. • 2-Connaître les principes fondamentaux de la sécurité informatique. • 3-Connaissances de Linux, Windows, TCP/IP, Syslog. • 4-Avoir des connaissances de base en langue anglaise car le support de cours est en langue anglaise.

PROFIL DES STAGIAIRES

• Analystes de sécurité, les architectes techniques de sécurité, les administrateurs réseau et système utilisant QRadar SIEM.

OBJECTIFS

• Décrire l'architecture de QRadar et les flux de données. • Définir les sources de journaux, les protocoles et les détails des événements.. • Découvrir comment QRadar collecte et analyse les informations de flux réseau. • Utiliser l'application Use Case Manager. • Découvrir une variété d'applications QRadar, d'extensions de contenu et l'App Framework. • Analyser les infractions à l'aide de l'interface utilisateur QRadar et de l'application Analyst Workflow. • Rechercher, filtrer, regrouper et analyser les données de sécurité. • Utiliser l'AQL pour des recherches avancées. • Utiliser QRadar pour créer des rapports personnalisés. • Définir des rapports sophistiqués à l'aide de Pulse Dashboards.

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

Principes fondamentaux de IBM Security QRadar 7.4

Architecture QRadar

Vue d'ensemble de l'interface utilisateur QRadar

Source de logs QRadar

Flux QRadar et QRadar Network Insights

Moteur de règles personnalisées QRadar (CRE)

Application QRadar Use Case Manager

Actifs QRadar

Extensions QRadar

Travailler avec des infractions

Recherche, filtrage et AQL de QRadar

Rapports et tableaux de bord QRadar

Console d'administration QRadar

Des exercices détaillés sont fournis pour permettre aux participants de se familiariser avec le travail de routine d'un analyste de la sécurité informatique qui utilise la plateforme IBM QRadar SIEM. Les exercices couvrent les sujets suivants :

- L'architecture
- La présentation de l'interface utilisateur
- Les sources de journaux
- Les flux et QRadar Network Insights
- Le moteur de règles personnalisées (CRE)
- L'application Use Case Manager
- Les actifs
- L'App Framework
- Le travail avec les infractions
- La recherche, le filtrage et l'AQL
- Les rapports et les tableaux de bord
- Les tâches de l'administrateur QRadar

*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.*