IBM QRadar SIEM Foundations

Durée: 3 Jours **Réf de cours: BQ104G** **Méthodes d'apprentissage: Classe à distance**

Résumé:

IBM Security QRadar offre une visibilité approfondie de l'activité des réseaux, des terminaux, des utilisateurs et des applications. Il assure la collecte, la normalisation, la corrélation et le stockage sécurisé des événements, des flux, des actifs et des vulnérabilités. Les attaques suspectes et les violations de politiques sont mises en évidence comme des infractions. Dans cette formation, vous découvrez l'architecture de la solution, comment naviguer dans l'interface utilisateur et comment enquêter sur les infractions. Vous recherchez et analysez les informations à partir desquelles QRadar a conclu à une activité suspecte. Des exercices pratiques renforcent les compétences acquises.
L'environnement de labs pour cette formation utilise la plateforme IBM QRadar SIEM 7.4.

Public visé:

Cette formation est conçue pour les analystes de sécurité, les architectes techniques de sécurité, les administrateurs réseau et système utilisant QRadar SIEM.

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- 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

Pré-requis:

- Infrastructure informatique
- Principes fondamentaux de la sécurité informatique
- Linux
- Windows
- Mise en réseau TCP/IP
- Syslog

Contenu:

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

Méthodes pédagogiques :

Support de cours officiel IBM est remis aux participants

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• Modalités d'évaluation : le participant est invité à s'auto-évaluer par rapport aux objectifs énoncés.
• Chaque participant, à l'issue de la formation, répond à un questionnaire de satisfaction qui est ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

•Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
•Votre place sera confirmée à la réception d'un devis ou ""booking form"" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
•Attention, si vous utilisez votre Compte Personnel de Formation pour financer votre inscription, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés.