QRadar EDR: Foundations

Durée: 2 Jours **Réf de cours: BQ505G** **Méthodes d'apprentissage: Classe à distance**

Résumé:

Dans ce cours, vous découvrez l'architecture IBM Security® QRadar® EDR et comment positionner le produit dans le paysage des solutions de sécurité de votre entreprise. Vous apprendrez à installer QRadar EDR Hive dans votre entreprise et les agents EDR sur vos équipements. Vous pourrez passer en revue l'interface utilisateur et la façon de naviguer dans le tableau de bord EDR tout en enquêtant sur les menaces reçues..
Ce cours s'applique à la version 3.12 de la solution QRadar EDR sur site.
Mis à jour 18/12/2024

Classe à Distance - site Client

Cette formation peut être suivie à distance en synchrone depuis n'importe quel site pourvu d'une connexion internet (2 Mb/s en symétrique recommandés). Le programme (théorie et pratique) suit le même déroulé pédagogique qu'en présentiel. La solution technologique adoptée permet aux apprenants à distance de suivre les présentations faites au tableau, de voir et d'entendre l'instructeur et les participants en temps réel, mais également d'échanger avec eux.

Public visé:

Ce cours est destiné en priorité aux : Administrateur Security operations center (SOC) Analyste SOCAnalyste Cyber sécurité Responsable du traitement des incidents Managed Service Security Provider (MSSP)

Objectifs pédagogiques:

- Dans ce cours, vous apprendrez à effectuer les opérations suivantes :
- Naviguer dans le tableau de bord QRadar EDR
- Décrire l'architecture de QRadar EDR
- Installer QRadar EDR Hive sur site et configurer l'installation initiale
- Déployer l'agent QRadar EDR sur vos équipements.
- Enquêter sur les menaces sur les équipements
- Gérer les équipements
- Comprendre les alertes et les tendances et y répondre
- Agir sur les attaques par malware comportemental et ransomware
- Configurer les notifications et le protocole de transfert de courrier simple
- Configurer les redirections d'alertes
- Définir des politiques
- Gérer les fichiers téléchargés et mis en quarantaine à partir de périphériques
- Configurer les utilisateurs, les groupes et les clients
- Configurer Hive-Cloud Score
- Créer des applications
- Surveiller les logs d'audit

Pré-requis:

Contenu:

Introduction à l'utilisation du tableau de bord

Aperçu du tableau de bord

Architecture de QRadar EDR

Installation de QRadar EDR sur site

Téléchargement, installation et mise à jour de l'agent QRadar EDR

Protéger vos équipements

Enquêter sur les menaces affectant les terminaux

Gestion des équipements

Comprendre les alertes et les tendances et y répondre

Agir sur les attaques de ransomware et de logiciels malveillants comportementaux

Recherche de menaces sur les terminaux à l'aide d'un exercice QRadar EDR

Administrer votre environnement

Configuration des notifications et du protocole SMTP (Simple Mail Transfer Protocol)

Configuration des alertes de transfert

Définition des politiques

Gestion des fichiers téléchargés et mis en quarantaine à partir de vos équipements

Configuration des utilisateurs, des groupes et des clients

Configuration de Hive-Cloud Score

Création d'applications

Surveillance des logs d'audit

Méthodes pédagogiques :

Un support de cours officiel sera fourni 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.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera 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 cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement