QRadar SOAR: Foundations

Durée: 2 Jours **Réf de cours: BQ405G** **Méthodes d'apprentissage: Classe à distance**

Résumé:

Dans ce cours, vous découvrirez l'architecture IBM Security® QRadar® SOAR et comment positionner le produit dans la conception de l'architecture de sécurité de votre entreprise.
Vous pourrez acquérir une expérience pratique de l'interface SOAR, en enquêtant et en gérant les cas et les utilisateurs avec le module SOAR Breach Response, les playbooks et l'intégration du courrier électronique.
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:Administrateurs Security operations center (SOC) Analystes SOCAnalystes Cyber sécuritéResponsables du traitement des incidentsManaged Service Security Provider (MSSP)

Objectifs pédagogiques:

- Dans ce cours, vous aborderez les sujets suivants :
- Modèles architecturaux QRadar SOAR
- Installer le produit et configurer la licence et l'accès
- Examiner la console SOAR
- Gérer les alertes
- Utiliser le concept d'artefacts
- Utiliser les capacités de traitement des enquêtes
- Intégrer le système de messagerie électronique pour les utilisateurs et la gestion des dossiers
- Se concentrer sur le module Breach Response
- Acquérir une expérience pratique de la plateforme SOAR
- Concevoir des playbooks
- Intégrer les solutions IBM et tierces à SOAR

Pré-requis:

Contenu:

Premiers pas	Utiliser le concept d'artefacts	Playbooks et intégrations
Décrire les modèles architecturaux	Gestion des cas et intégration des courriels	Acquérir une expérience pratique de la plateforme SOAR
Installer le produit et configurer la licence et l'accès	Utiliser les capacités de gestion des dossiers	Concevoir des playbooks
Examiner la console SOAR	Intégrer le système de messagerie électronique pour les utilisateurs et la gestion des dossiers	Intégrer des solutions IBM et tierces à SOAR
Gérer les cas et utiliser le module complémentaire Breach Response	Se concentrer sur le module Breach Response	

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