IBM QRadar SIEM, les fondamentaux

Cours Pratique de 3 jours - 21h
Réf : IBF - Prix 2024 : 2 390CHF HT

QRadar est un outil de corrélation d'événements permettant de collecter et trier les informations pertinentes générées par les différents dispositifs de sécurité. Ce cours permettra de configurer l'application, analyser le flux des données et générer les rapports en fonction des alertes pré-paramétrées.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Collecter, analyser et générer des rapports sur les données avec QRadar

Enrichir les données opérationnelles à l'aide de recherches et de flux

Créer des alertes en temps réel

Générer des rapports

LE PROGRAMME

dernière mise à jour : 02/2019

1) Le SIEM

- Qu'est qu'un SIEM (Security Information Event Management) ?
- Pourquoi faut-il corréler les événements ?
- Les outils SIEM du marché.

2) L'architecture et l'interface de QRadar

- Présentation et positionnement de l'outil QRadar.
- Comment configurer QRadar SIEM pour collecter des données.
- Apprendre à détecter les activités suspectes.
- L'architecture et les composantes de QRadar SIEM et du flux de données.
- L'interface utilisateur de QRadar.

Travaux pratiques : Prise en main de l'interface de QRadar.

3) Analyse et recherche d'actions suspectes

- Enquêter sur les attaques suspectes.
- Chercher les violations de politiques de sécurité.
- Rechercher, filtrer, grouper et analyser les données de sécurité.
- Analyser les événements et les flux.
- Enquêter sur profils d'actifs.

Travaux pratiques : Mise en place d'une recherche d'attaques ou de violations de politiques de sécurité. Créer des alertes en temps réel.

4) Gestion des règles et des index

- Pourquoi la hiérarchie du réseau.
- Déterminer comment les règles examinent les données entrantes et créent des infractions.
- Comment utiliser les index et la gestion de données agrégées.

Travaux pratiques : Examiner les données entrantes et créer des infractions. Utilisation des règles et des index.

PARTICIPANTS

Administrateurs systèmes et réseaux.

PRÉREQUIS

Connaissances de base des réseaux et des systèmes.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

5) Les dashboards
- La gestion des dashboards.
- Les différents éléments d'un dashboard.
- Comment se déplacer entre les dashboards ?
- Personnaliser les dashboards et leurs éléments.

Travaux pratiques : Personnalisation des dashboards.

6) Les rapports
- Présentation des rapports.
- Les paramètres généraux.
- Les différents objets d'un rapport et leurs paramètres.
- Créer des rapports personnalisés.

Travaux pratiques : Création et utilisation de rapports.

7) Les filtres et la recherche avancée
- Les filtres disponibles et utilisables rapidement.
- Utiliser des filtres pour effectuer une recherche.
- Utilisation du langage AQL (Ariel Query Language) pour des recherches avancées.

Travaux pratiques : Mise en place des filtres et utilisation des recherches avancées.

LES DATES

CLASSE À DISTANCE
2024 : 09 sept., 18 déc.