+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 28/05/2024

S'inscrire

Formation IBM QRadar SIEM

4 jours (28 heures)

Présentation

Notre formation IBM QRadar SIEM vous enseignera la maîtrise d'un des logiciels SIEM les plus adoptés au monde. En effet, notre programme couvre l'ensemble des fonctionnalités de l'outil afin que vous puissiez efficacement analyser et traiter les attaques cybercriminelles.

Dans ce cours, vous apprendrez tout d'abord à comprendre la SIEM en profondeur et la place qu'occupe IBM QRadar SIEM au sein de votre environnement informatique. À travers une démonstration pratique, vous apprendrez à manipuler l'interface et à configurer vos alertes.

Vous découvrirez les bonnes pratiques d'usage, la gestion des rôles, des logs ou encore des flux de données. L'investigation et la surveillance avec IBM QRadar SIEM n'aura plus de secrets pour vous.

Comme pour toutes nos formations, nous vous présenterons la dernière version du logiciel : IBM QRadar 7.4.3.

Objectifs

- Comprendre l'importance d'un SIEM dans la cybersécurité et ses différentes fonctions
- Savoir installer et configurer QRadar
- Maîtriser l'intégration et la gestion des logs
- Utiliser les fonctionnalités avancées de QRadar

Public visé

- **Analystes Cybersécurité**
- Analystes SOC
- Chargé de cybersécurité
- Administrateur Système
- Administrateur Réseau

Pré-requis

Connaissances de base des réseaux et des systèmes.

Pré-requis matériel

Un accès à IBM QRadar SIEM.

Programme de notre formation IBM QRadar SIEM

INTRODUCTION AU SIEM

- Comprendre l'importance d'un SIEM
- Le rôle du SIEM dans la cybersécurité
- SIM vs SEM
- Directives et architecture d'un SIEM
- Présentation des capacités clés d'un SIEM :
  - Agrégation
  - Corrélation
  - Reporting
  - Stockage
  - Alertes
  - Automatisation

PRÉSENTATION DE QRADAR

- Les composants
- Les flux de données
- Prise en main de l'interface
- Les concepts fondamentaux de QRadar
- Les fonctionnalités principales de l'outil

GESTION ET ADMINISTRATION

- Installer QRadar
- Configuration
- Procédures de migration
- Mise à niveau
- Techniques de tuning pour optimiser les performances
- Stratégies de gestion des sauvegardes et de restauration des données
- Sécurité et gestion des accès utilisateurs
- Troubleshooting

LES LOGS ET LES FLUX

- Intégration des logs
- Normalisation des logs
- Gestion des évènements
- Méthodes pour analyser les événements liés à une attaque
- Configuration des sources de logs
- Préparation pour l'analyse des données
- Les outils de recherche
- Les outils de filtrage

SURVEILLANCE AVEC QRADAR

- Surveillance et interprétation des notifications de QRadar
- Comment utiliser les tableaux de bord
- Enquêter sur les anomalies détectées
- Configuration des notifications
- Les bonnes pratiques de surveillance
- Stratégies pour le suivi des changements d'actifs
- Détection des risques associés
- Pratiques recommandées pour la maintenance des informations relatives aux actifs

INVESTIGATION

- Techniques d'investigation des vulnérabilités
- Utilisation de la gestion des index et des données agrégées pour des recherches efficaces
- Introduction au langage de requête Ariel (AQL) pour des recherches avancées
- Analyse de cas réels
- Création de rapports d'investigation

CONSOLE D'ADMINISTRATION

- Utiliser la console d'administration
- Simulation d'attaques
- Analyse des processus avec Sysmon
- Bonnes pratiques pour la gestion des configurations et des paramètres de sécurité

OPÉRATIONS AVANCÉES

- Intégration de QRadar avec d'autres systèmes
- Gestion de types de sources de logs personnalisés
- Utiliser et configurer des collections de données de référence
- Créer des règles personnalisées
- Utilisation des extensions de QRadar
- Gestion des extensions
- Les bonnes pratiques pour la personnalisation de QRadar

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.

Organisme de formation enregistré sous le numéro 11 75 54743 75. Cet enregistrement ne vaut pas agrément de l’État.
© Ambient IT 2015-2024. Tous droits réservés. Paris, France - Suisse - Belgique - Luxembourg