IBM QRadar SIEM : fondamentaux

Lien : https://innov-systems.com/formation/ibm-qradar-siem-fondamentaux-

DURÉE	RÉFÉRENCE	CATÉGORIE
4 jours (28h)	**SEC251**	**IBM**

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Savoir configurer IBM QRadar SIEM
- Savoir analyser le flux des données et générer les rapports

POUR QUI ?

- Administrateurs systèmes ou réseaux

Innov Systems

Programme détaillé

1 / Introduction à IBM QRadar

- Définition d’un SIEM
- Le fonctionnement d'un SIEM
- Les objectifs d'un SIEM et de la corrélation des données
- Panorama des outils SIEM du marché
- Présentation de QRadar
- Positionnement de l’outil QRadar

2 / Architecture de QRadar

- Configuration de QRadar SIEM pour collecter des données
- Détection des activités suspectes
- Architecture des composants IBM QRadar SIEM et flux de données
- Utilisation de l'interface utilisateur QRadar SIEM

3 / Analyser et rechercher des actions suspectes

- Enquêter sur une infraction déclenchée par des événements
- Enquêter sur les événements d'une infraction
- Utiliser les profils d'actifs pour enquêter sur des infractions
- Enquêter sur une infraction déclenchée par des flux
- Enquêter sur profils d'actifs

4 / Gérer des règles et des index

- Utilisation de la hiérarchie du réseau
- Index et gestion de données agrégées

Innov Systems

5 / Utiliser QRadar SIEM Dashboard

- Gestion des dashboards
- Les différents éléments d’un dashboard
- Se déplacer entre les dashboards
- Personnalisation des dashboards et leurs éléments

6 / Créer des rapports

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

7 / Utiliser les filtres et la recherche avancée

- Les filtres disponibles et utilisables rapidement
- Utilisation des filtres pour effectuer une recherche
- Utilisation d'Ariel Query Language (AQL) pour les recherches avancées

8 / Analyser une attaque à grande échelle dans le monde réel

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Inov Systems

Prochaines dates programmées

12 au 15 Jan. 2027	Présentiel - Casablanca
09 au 12 Mars 2027	Présentiel - Casablanca
04 au 07 Mai 2027	Présentiel - Casablanca
29 Juin au 02 Juil. 2027	Présentiel - Casablanca
31 Août au 03 Sep. 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés

Innov Systems