

Your Cyber INSURANCE



IBM QRadar SIEM Foundations – 3Jours

Jours	Module	Unités
Jour 1	Introduction & Fondations	- Unit 0 : Présentation générale — concepts fondamentaux de QRadar, rôles, architecture de la plateforme. - Unit 1 : Architecture de QRadar — flux de données, collecte des logs/événements, comment QRadar traite l'information. - Unit 2 : Interface utilisateur (UI) — prise en main de l'interface, navigation, vues, menus. - Unit 3 : Configuration des sources de logs — définition des log sources, protocoles, format des événements / données à collecter.
Jour 2	Flux réseau, règles & gestion des ressources	- Unit 4 : Flux réseau & Network Insights — collecte et analyse des flux réseau (network flows), visibilité réseau. - Unit 5 : Moteur de règles personnalisées (Custom Rule Engine, CRE) — création et gestion des règles de détection, logique déclenchée sur événements/flux. - Unit 6 : Application Use Case Manager — gestion des cas d'usage (use cases), scénarios de sécurité, gestion des incidents. - Unit 7 : Gestion des assets / entités — définition et administration des assets, corrélation des logs/flux avec assets.
Jour 3	Analyse, reporting, administration	- Unit 8 : Extensions & apps supplémentaires — découverte des apps, extensions, modules additionnels disponibles dans QRadar. - Unit 9 : Gestion des « Offenses » — analyser les alertes/incidents, workflows d'analyste, visualisation des offenses. - Unit 10 : Recherche, filtrage, AQL — utiliser les fonctions de recherche, filtres, requêtes avancées (AQL) pour explorer les données. - Unit 11 : Reporting & Dashboards — création de rapports, tableaux de bord personnalisés, visualisation des données agrégées. - Unit 12 : Console d'administration — tâches d'admin, gestion de la configuration, maintenance, gestion des utilisateurs, paramètres