IBM GUARDIUM

Lien : https://innov-systems.com/formation/ibm-guardium

DURÉE
10 jours (70h)

RÉFÉRENCE
OS437

CATÉGORIE
Infosphere, Biginsights, Guardium

OBJECTIFS DE LA FORMATION

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

- Maîtriser l'architecture et les composants de la solution IBM Security Guardium
- Être capable d'installer, de configurer et d'administrer une infrastructure Guardium complète
- Savoir déployer et gérer les agents S-TAP sur différents systèmes d'exploitation et bases de données
- Développer et implémenter des politiques de sécurité robustes pour l'audit, l'alerte et le blocage
- Utiliser les modules de Vulnerability Assessment et de Classification pour renforcer la posture de sécurité
- Créer des rapports personnalisés et automatiser les tâches d'audit pour répondre aux exigences de conformité
- Gérer le cycle de vie des incidents de sécurité, de la détection à la remédiation, via les outils Guardium
- Intégrer Guardium dans un écosystème de sécurité plus large, notamment avec les SIEM
- Dépanner efficacement les problèmes courants et appliquer les bonnes pratiques pour optimiser la solution

Innov Systems

POUR QUI ?

- Administrateurs de bases de données (DBA) souhaitant sécuriser leurs environnements
- Ingénieurs et analystes en cybersécurité (SOC/SecOps) responsables de la surveillance des données
- Architectes de sécurité chargés de concevoir et de mettre en œuvre des solutions de protection des données
- Auditeurs IT et responsables de la conformité (Compliance Officers) ayant besoin de valider les contrôles de sécurité
- Administrateurs système et infrastructure responsables du déploiement et de la maintenance de la solution

Innov Systems

Programme détaillé

1 / Introduction à IBM Guardium et à la Sécurité des Données (DAM)

- Comprendre les concepts de la sécurité des données (DAM/DAPM - Data Activity Monitoring / Data Access Protection and Monitoring)
- Présentation de la suite IBM Security Guardium et de son positionnement sur le marché
- Discussion sur les cas d'usage principaux : conformité (RGPD, PCI-DSS), détection des menaces et audit

2 / Architecture de la solution Guardium

- Description des composants clés : Collecteurs, Agrégateurs et Central Manager (CM)
- Comprendre les flux de données et de configuration entre les différents composants
- Différencier les modes d'inspection du trafic : S-TAP, K-TAP, et inspection réseau

3 / Installation et Configuration Initiale de l'Appliance

- Procédure d'installation d'une appliance virtuelle Guardium (Collecteur/CM)
- Configuration initiale post-installation : réseau, fuseau horaire, mots de passe
- Utilisation de la console de gestion (CLI) et de l'interface graphique (GUI) pour les paramétrages de base

4 / Déploiement et Gestion des Agents (S-TAP)

- Installation et configuration d'un agent S-TAP sur un serveur de base de données (Windows/Linux)
- Gestion du cycle de vie des S-TAP depuis le Central Manager
- Validation du bon fonctionnement et du flux de données entre le S-TAP et le Collecteur

5 / Configuration des Sources de Données

- Ajout et configuration de sources de données pour les bases de données (Oracle, SQL Server, MySQL)

Innov Systems

- Paramétrage des mécanismes d'inspection spécifiques à chaque type de SGBD
- Gestion des groupes de sources de données pour simplifier l'application des politiques

6 / Création de Politiques de Sécurité (Policy Builder)

- Introduction au Policy Builder et à la logique des règles (critères, actions)
- Création d'une politique de sécurité simple pour auditer l'accès des comptes à privilèges
- Installation et activation d'une politique sur les collecteurs

7 / Politiques de Sécurité Avancées et Corrélation

- Utilisation de règles de corrélation pour déclencher des alertes complexes (ex: attaque par force brute)
- Configuration d'actions d'alerte en temps réel (e-mail, SNMP, Syslog)
- Mise en place de politiques de blocage pour empêcher les requêtes SQL non autorisées

8 / Reporting et Audit

- Exploration des rapports prédéfinis pour la conformité et l'audit
- Création de rapports personnalisés avec le Query Builder pour répondre à des besoins spécifiques
- Automatisation de la génération et de la distribution des rapports

9 / Évaluation des Vulnérabilités (Vulnerability Assessment)

- Configuration et exécution de scans d'évaluation des vulnérabilités sur les bases de données
- Analyse des résultats et des recommandations pour corriger les failles de sécurité
- Intégration des tests de vulnérabilité dans les processus de sécurité récurrents

10 / Découverte et Classification des Données Sensibles

- Configuration d'un processus de classification pour identifier les données sensibles (ex: numéros de carte de crédit, données personnelles)
- Utilisation des résultats de classification pour affiner les politiques de sécurité

Inov Systems

- Création de rapports de classification pour les auditeurs et les responsables de la conformité

11 / Gestion des Alertes et Workflow Automation

- Configuration du portail d'investigation des incidents et des alertes
- Création de processus de workflow pour l'assignation et le traitement des incidents (Todo list)
- Intégration avec les systèmes de ticketing pour l'automatisation de la gestion des cas

12 / Administration et Maintenance de la Plateforme Guardium

- Gestion des sauvegardes et des restaurations des appliances Guardium
- Procédure de mise à jour (patching) des composants de la solution
- Surveillance de la santé du système (monitoring du buffer, des performances, de l'espace disque)

13 / Fonctionnalités Avancées et Intégrations

- Introduction à la surveillance de l'activité des fichiers (FAM - File Activity Monitoring)
- Intégration de Guardium avec un SIEM (ex: IBM QRadar) via Syslog ou LEEF
- Utilisation des API Guardium pour l'automatisation et l'intégration avec des outils tiers

14 / Dépannage (Troubleshooting) et Bonnes Pratiques

- Analyse des problèmes courants : S-TAP non connecté, données manquantes, alertes non générées
- Utilisation des outils de diagnostic CLI (support must_gather)
- Revue des bonnes pratiques pour l'optimisation des performances et la scalabilité de l'architecture
- Administrateurs de bases de données (DBA) souhaitant sécuriser leurs environnements
- Ingénieurs et analystes en cybersécurité (SOC/SecOps) responsables de la surveillance des données
- Architectes de sécurité chargés de concevoir et de mettre en œuvre des solutions de protection des données
- Auditeurs IT et responsables de la conformité (Compliance Officers) ayant besoin de valider les contrôles de sécurité

Inov Systems

- Administrateurs système et infrastructure responsables du déploiement et de la maintenance de la solution

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

Prochaines dates programmées

30 Nov. au 11 Déc. 2026	Présentiel - Casablanca
12 au 25 Jan. 2027	Présentiel - Casablanca
08 au 19 Mars 2027	Présentiel - Casablanca
03 au 14 Mai 2027	Présentiel - Casablanca
28 Juin au 09 Juil. 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