Palo Alto Networks Cortex XDR : Maîtriser le Déploiement et la Sécurisation avec Cortex XDR

Lien : https://innov-systems.com/formation/palo-alto-networks-cortex-xdr-matriser-le-deploiement-et-la-securisation-avec-cortex-xdr

DURÉE	RÉFÉRENCE	CATÉGORIE
4 jours (28h)	**SEC274**	**Fortinet**

OBJECTIFS DE LA FORMATION

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

- Comprendre en profondeur l’architecture et les composants clés de Cortex XDR
- Savoir installer, configurer et administrer efficacement la console de gestion Cortex XDR
- Déployer et ajuster les politiques de prévention, de détection et de réponse aux incidents
- Analyser et corriger les incidents de sécurité à partir des alertes et rapports Cortex XDR
- Optimiser la performance et la fiabilité des agents XDR dans des environnements complexes

POUR QUI ?

- Administrateurs systèmes et réseaux responsables de la sécurité des postes et serveurs
- Ingénieurs cybersécurité en charge du déploiement et de l’exploitation d’une solution EDR/XDR
- Responsables SOC (Security Operations Center) souhaitant renforcer la maîtrise opérationnelle de Cortex XDR
- Chefs d’équipes techniques assurant la supervision et la remédiation des menaces avancées

Programme détaillé

1 / INTRODUCTION À CORTEX XDR

- Positionnement de Cortex XDR dans l'écosystème Palo Alto Networks
- Concepts XDR, EDR et corrélation multi-source
- Avantages de l'approche unifiée de détection et de réponse

2 / ARCHITECTURE ET COMPOSANTS

- Présentation de la plateforme et des flux de données
- Rôles des agents, de la console et des connecteurs
- Communication et intégration avec les autres produits Palo Alto (Cortex Data Lake, NGFW)

3 / INTERFACE D'ADMINISTRATION

- Présentation de la console de gestion
- Navigation, tableaux de bord et rapports par défaut
- Personnalisation des vues et filtres d'analyse

4 / PREMIÈRE CONFIGURATION

- Initialisation de la console et configuration réseau de base
- Création d'administrateurs et gestion des rôles
- Paramètres régionaux, licences et configuration du Data Lake

5 / DÉPLOIEMENT DES AGENTS CORTEX XDR

- Préparation et méthodes d'installation (manuelle, scriptée, GPO, MDM)
- Bonnes pratiques de déploiement à grande échelle
- Vérification de l'état et de la communication des agents

6 / PROFILS ET POLITIQUES DE PROTECTION

- Configuration des profils de sécurité
- Application des politiques selon les groupes d’utilisateurs ou d’appareils
- Gestion des mises à jour, signatures et moteurs de détection

7 / PROTECTION CONTRE LES LOGICIELS MALVEILLANTS ET LES EXPLOITS

- Mécanismes de détection comportementale et signatures
- Configuration des modules anti-malware et anti-exploit
- Étude de cas : prévention d’une attaque par ransomware

8 / ANALYSE DES ALERTES ET INVESTIGATIONS

- Typologie des alertes Cortex XDR
- Méthodologie d’investigation pas à pas
- Corrélation d’événements et recherche avancée

9 / RÉPONSE ET REMÉDIATION

- Actions automatiques et manuelles : isolation, suppression, restauration
- Orchestration des réponses via playbooks et intégrations tierces
- Mise en œuvre de stratégies de réponse rapides dans un environnement SOC

10 / GESTION DES EXCLUSIONS ET EXCEPTIONS

- Définir et appliquer des exceptions aux politiques
- Gestion des faux positifs et optimisation continue
- Audit et traçabilité des modifications

11 / SUPERVISION ET RAPPORTING

- Exploitation des tableaux de bord analytiques
- Création de rapports personnalisés et alertes programmées

- Suivi de la conformité et indicateurs de performance

12 / DÉPANNAGE ET MAINTENANCE

- Diagnostic des erreurs fréquentes sur les agents et la console
- Méthodes de résolution des problèmes de communication et d’intégration
- Sauvegarde, mise à jour et bonnes pratiques de maintenance

13 / BROKER VM ET INTÉGRATIONS AVANCÉES

- Rôle et configuration de la Broker VM
- Connexion à d’autres outils de sécurité (SIEM, firewalls, cloud)
- Automatisation du déploiement et intégration continue

14 / CAS PRATIQUES ET ÉVALUATION FINALE

- Études de cas réels de détection et remédiation
- Atelier de configuration complète d’un environnement Cortex XDR
- Synthèse des bonnes pratiques et validation des acquis

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

28 au 31 Juil. 2026	Présentiel - Casablanca
22 au 25 Sep. 2026	Distanciel
17 au 20 Nov. 2026	Distanciel

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