

Cortex XDR : Security Operations and Integration

Réf. CORTEX-SOI · Palo Alto Networks · Cybersécurité

DURÉE 3 jours	NIVEAU Avancé	MODALITÉS Présentiel · Live · Intra	VOUCHER EXAMEN En option
-------------------------	-------------------------	---	------------------------------------

Présentation

Ce cours de 3 jours prépare les équipes SOC à mettre en œuvre Cortex XDR de bout en bout : déploiement des agents, politiques de prévention endpoint, intégration des sources de données et automatisation des réponses. Il met l'accent sur l'exploitation opérationnelle de la plateforme pour renforcer la posture de sécurité de l'organisation.

Objectifs pédagogiques

- Décrire l'architecture et les composants de Cortex XDR
- Déployer et configurer les agents et les politiques de prévention endpoint
- Intégrer les sources de données réseau, cloud et endpoint
- Configurer les règles d'exclusion, de restriction et de blocage
- Mettre en place la remédiation et la réponse aux incidents
- Administrer les profils, rôles et la gestion opérationnelle de la plateforme

Programme détaillé

1. Module 1 — Architecture et déploiement

- Composants Cortex XDR et data lake
- Déploiement des agents sur les endpoints
- Profils de prévention (exploit, malware)
- Gestion des politiques de sécurité

2. Module 2 — Intégration des données et prévention

- Intégration des sources réseau, cloud et logs
- Behavioral Threat Protection
- Règles d'exclusion et de restriction
- Gestion des exceptions

3. Module 3 — Réponse et administration

- Actions de remédiation sur endpoint
- Live Terminal et Host Insights
- Gestion des rôles et administration
- Bonnes pratiques d'exploitation SOC

Prérequis

Connaissances en sécurité des endpoints, concepts de SOC et administration système. Une expérience en détection et réponse aux menaces est recommandée.

Public visé

Analystes SOC, ingénieurs sécurité, administrateurs endpoint et équipes de réponse à incident.

Ce qui est inclus

- Support de cours officiel Palo Alto Networks Cortex
- Labs sur tenant Cortex XDR
- Attestation de fin de formation
- Accès à un formateur expert SOC
- Pauses & déjeuner

Certification

Formation non certifiante ; une attestation de fin de formation Advancia Training est délivrée à l'issue du cours.

1 150 DT HT / participant — tarif inter-entreprise · financement CNFCPP possible