

Cortex XDR : Investigation and Analysis

Réf. CORTEX-IA · Palo Alto Networks · Cybersécurité

DURÉE 2 jours	NIVEAU Avancé	MODALITÉS Présentiel · Live · Intra	VOUCHER EXAMEN En option
-------------------------	-------------------------	---	------------------------------------

Présentation

Ce cours avancé de 2 jours forme les analystes à investiguer les incidents détectés par Cortex XDR : analyse des alertes, reconstitution de la chaîne d'attaque et chasse proactive aux menaces. Il approfondit les capacités d'analyse causale et le langage de requête XQL pour accélérer la détection et la remédiation.

Objectifs pédagogiques

- Analyser les alertes et incidents dans la console Cortex XDR
- Reconstituer la chaîne d'attaque via l'analyse causale (Causality)
- Mener des investigations sur les endpoints et le réseau
- Rédiger des requêtes de recherche avec XQL (XDR Query Language)
- Conduire des campagnes de threat hunting proactif
- Documenter les incidents et les indicateurs de compromission (IOC)

Programme détaillé

1. Module 1 — Analyse des alertes et incidents

- Cycle de vie des incidents
- Tableau de bord et triage
- Analyse causale (Causality View)
- Scoring et priorisation des alertes

2. Module 2 — Investigation approfondie

- Investigation endpoint et réseau
- Artefacts et indicateurs de compromission
- Timeline et corrélation d'événements
- Cas pratiques d'incident

3. Module 3 — Threat hunting et XQL

- Introduction à XQL et aux datasets
- Requêtes de recherche avancées
- Chasse aux menaces proactive
- Reporting et documentation

Prérequis

Avoir suivi le cours Cortex XDR : Security Operations and Integration (EDU-260) ou disposer d'une expérience équivalente d'exploitation de Cortex XDR.

Public visé

Analystes SOC de niveau 2/3, threat hunters, analystes de réponse à incident et ingénieurs sécurité.

Ce qui est inclus

- Support de cours officiel Palo Alto Networks
- Labs d'investigation guidés
- Attestation de fin de formation
- Accès à un formateur expert threat hunting
- Pauses & déjeuner

Certification

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

750 DT HT / participant — tarif inter-entreprise · financement CNFCCP possible