Cortex XDR: Investigation and Response (EDU-262)

Durée: 2 Jours **Réf de cours: PAN-EDU-262** **Version: 3.6** **Méthodes d'apprentissage: Virtual Learning**

Résumé:

This instructor-led course teaches you how to use the Incidents pages of the Cortex XDR management console to investigate attacks. It explains causality chains, detectors in the Analytics Engine, alerts versus logs, log stitching, and the concepts of causality and analytics.
You will learn how to analyze alerts using the Causality and Timeline Views and how to use advanced response actions, such as remediation suggestions, the EDL service, and remote script execution.
Multiple modules focus on how to leverage the collected data. You will create simple search queries in one module and XDR rules in another. The course demonstrate how to use specialized investigation views to visualize artifact-related data, such as IP and Hash Views. Additionally, it provides an introduction to XDR Query Language (XQL). The course concludes with Cortex XDR external-data-collection capabilities, including the use of Cortex XDR API to receive external alerts.

Public visé:

Cybersecurity analysts and engineersSecurity operations specialists

Objectifs pédagogiques:

- Successful completion of this instructor-led course with hands-on lab activities should enable participants to:
- Investigate and manage incidents
- Describe the Cortex XDR causality and analytics concepts
- Analyze alerts using the Causality and Timeline Views
- Work with Cortex XDR Pro actions such as remote script execution
- Create and manage on-demand and scheduled search queries in the Query Center
- Create and manage the Cortex XDR rules BIOC and IOC
- Working with Cortex XDR assets and inventories
- Write XQL queries to search datasets and visualize the result sets
- Work with Cortex XDRs external-data collection

Pré-requis:

Participants must have completed EDU-260 (Cortex XDR: Prevention and Deployment).

- PAN-EDU-260 - Cortex XDR 3.2:Prevention and Deployment (EDU-260)

Contenu:

Course Modules

1 - Cortex XDR Incidents

2 - Causality and Analytics Concepts

3 - Causality Analysis of Alerts

4 - Advanced Response Actions

5 - Building Search Queries

6 - Building XDR Rules

7 - Cortex XDR Assets

8 - Introduction to XQL

9 - External Data Collection

Méthodes pédagogiques :

Palo Alto Networks Education
The technical curriculum developed and authorized by Palo Alto Networks and delivered by Palo Alto Networks Authorized Training Partners helps provide the knowledge and expertise that prepare you to protect our digital way of life. Our trusted certifications validate your knowledge of the Palo Alto Networks product portfolio and your ability to help prevent successful cyberattacks, safely enable applications, and automate effective responses to security events.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement