Palo Alto Networks Cortex XDR Investigation & Analysis (CXDRIA)

Durée: 2 Jours **Réf de cours: PAN-CXDRIA** **Méthodes d'apprentissage: Classe à distance**

Résumé:

Gain hands-on expertise in endpoint management, case management, forensic analysis and platform automation
XDR is the industry's most powerful extended detection and response platform. You will gain hands-on expertise in endpoint management, case management, forensic analysis and platform automation. Throughout this course, you will explore the key features of Cortex XDR.
This course is designed to enable you to:
- Investigate cases, analyze key assets and artifacts, and interpret the causality chain.
- Query and analyze logs using XQL to extract meaningful insights.
- Utilize advanced tools and resources for comprehensive case analysis

Virtual and Classroom learning - V&C Select™

V&C Select™ is a simple concept and a flexible approach to delivery. You can 'select' a course from our public schedule and attend in person or as a virtual delegate. Virtual delegates do not travel to this course, we will send you all the information you need before the start of the course and you can test the logins.

Public visé:

This course is for a wide range of security professionals, including SOC, CERT, CSIRT, and XDR analysts, managers, incident responders, and threat hunters. It is also well-suited for professional-services consultants, sales engineers, and service delivery partners.

Objectifs pédagogiques:

- The course is designed to enable cybersecurity professionals, particularly those in SOC/CERT/CSIRT and Security Analysts roles, to use XDR.
- The course reviews XDR intricacies, from fundamental components to advanced strategies and techniques, including skills needed to navigate case management, platform automation, and orchestrate cybersecurity excellence.

Pré-requis:

Participants should have a foundational understanding of cybersecurity principles and experience with analyzing incidents and using security tools for investigation.

Contenu:

Module 1: Introduction to Cortex XDR

Module 2: Endpoints

Module 3: XQL

Module 4: Alerting and Detection

Module 5: Vulnerability ; Forensics

Module 6: Platform Automation

Module 7: Case Management

Module 8: Dashboards ; Reports

Autres moyens pédagogiques et de suivi: