Palo Alto Networks Cortex XDR Investigation & Analysis (CXDRIA)

Duration: 2 Days **Course Code: PAN-CXDRIA** **Delivery Method: Virtual Learning**

Overview:

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 Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

Target Audience:

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.

Objectives:

- 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.

Prerequisites:

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

Content:

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

Further Information:

For More information, or to book your course, please call us on 00 20 (0) 2 2269 1982 or 16142

training@globalknowledge.com.eg

www.globalknowledge.com/en-eg/

Global Knowledge, 16 Moustafa Refaat St. Block 1137, Sheraton Buildings, Heliopolis, Cairo