Palo Alto Networks: Cortex XSIAM for Investigation and Analysis (XSIAM-IA)

Duración: 2 Días **Código del Curso: PAN-XSIAM-IA** **Método de Impartición: Curso Remoto (Virtual)**

Temario:

XSIAM is the industry's most comprehensive security incident and asset management platform, offering extensive coverage for securing and managing infrastructure, workloads, and applications cross multiple environments.
Throughout this course, you will explore the key features of Cortex XSIAM.
This course is designed to enable you to:
- Investigate incidents, 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 incident analysis.

This course is valued 20 PaloAlto training credits

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.

Dirigido a:

SOC/CERT/CSIRT/XSIAM analysts and managers, MSSPs and service delivery partners/system integrators, internal and external professional-services consultants and sales engineers, incident responders and threat hunters.

Objetivos:

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

Prerequisitos:

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

Exámenes y certificación

There is no online exit exam for this course, but there is a related certification: XSIAM Analyst

Contenido:

Course Modules

1- Introduction to Cortex XSIAM

2- Endpoints

3- XQL

4- Alerting and Detection

5- Threat Intel Management

6- Automation

7- Attack Surface Management

8- Incident Handling

9- Dashboards and Reports

Más información:

Para más información o para reservar tu plaza llámanos al (34) 91 425 06 60

info.cursos@globalknowledge.es

www.globalknowledge.com/es-es/

Global Knowledge Network Spain, C/ Retama 7, 6ª planta, 28045 Madrid