Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow ECS, Nidderdale House, Beckwith Knowle, Harrogate, HG3 1SA

Email: educationteam.ecs.uk@arrow.com
Phone: 0870 251 1000

Cortex XSIAM for Security Operations and Automation

CODE:	LENGTH:	PRICE:
PAN_EDU-270	32 Hours (4 days)	£2,995.00

Description

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

- Deploy, configure, and install XDR agents and configure Agent Groups and profiles
- Investigate incidents, examine assets and artifacts, and understand the causality chain
- Create correlation rules, use XQL to query logs, and analyze incidents using available tools and resources

Scope

- Duration: 4 days
- Format: Lecture and hands-on labs
- Platform support: Cortex

Objectives

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

Audience

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

Prerequisites

Participants must be familiar with enterprise product deployment, networking, and security concepts.

Programme

1. Introduction to Cortex XSIAM
2. Elements of Security Operations
3. Maturity Model
4. Agent Deployment and Configuration
5. Data Source Ingestion
6. Visibility
7. Data Model
8. Analytics
9. Alerting and Detecting
10. Attack Surface Management
11. Automation
12. Incident Handling / SOC

Session Dates

On request. Please Contact Us

Additional Information

This training is also available as onsite training. Please contact us to find out more.