Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow Enterprise Computing Solutions Ltd, Part 1st Floor, Suite 1D/1, Central House, Otley Road, Harrogate, HG3 1UG

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

Cortex XSIAM: Security Operations, Integration, and Automation

CODE:	LENGTH:	PRICE:
PAN_EDU-XSIAM-SOIA	24 Hours (3 days)	£2,295.00

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:
• Describe how endpoint agents, XDR collectors, NGFWs, and Broker VMs secure networks and devices.
• Query and analyze logs using XQL for data ingestion and detection.
• Configure Threat Intel Management features, automate workflows, and apply EDLs and indicator rules.

Scope

- Duration: 3 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 engineering roles, to use XSIAM.

The course reviews XSIAM intricacies, from fundamental components to advanced strategies and techniques, including skills needed to configure security integrations, develop automation workflows, manage indicators, and optimize dashboards for enhanced security operations.

Audience

SOC/CERT/CSIRT/XSIAM engineers and managers, MSSPs and service delivery partners/system integrators, internal and external professional-services consultants and sales engineers, SIEM and automation engineers.

Prerequisites

Participants should have a foundational understanding of cybersecurity principles and experience with network and endpoint security fundamentals.

Programme

0 - Course Overview
1 - Overview of Cortex XSIAM
2 - Software Components
3 - XQL
4 - Detection Engineering
5 - Integrations
6 - Automation
7 - Threat Intel Management
8 - Attack Surface Management

9 - UI Customizations

Session Dates

On request. Please Contact Us

Additional Information

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