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 XDR 3.2: Investigation and Response

CODE:	LENGTH:	PRICE:
PAN_EDU-262	2 day(s)	£1,495.00

Description

This instructor-led course teaches you how to use the Incidents pages of the Cortex XDR management console to investigate attacks.

It explains causality chains, detectors in the Analytics Engine, alerts versus logs, log stitching, and the concepts of causality and analytics.

You will learn how to analyze alerts using the Causality and Timeline Views and how to use advanced response actions, such as remediation suggestions, the EDL service, and remote script execution.

Multiple modules focus on how to leverage the collected data. You will create simple search queries in one module and XDR rules in another.
The course demonstrate how to use specialized investigation views to visualize artifact-related data, such as IP and Hash Views. Additionally, it provides an introduction to XDR Query Language (XQL).
The course concludes with Cortex XDR external-datacollection capabilities, including the use of Cortex XDR API to receive external alerts.

Objectives

Successful completion of this instructor-led course with hands-on lab activities should enable participants to:

- Investigate and manage incidents
- Describe the Cortex XDR causality and analytics concepts
- Analyse alerts using the Causality and Timeline Views
- Work with Cortex XDR Pro actions such as remote script execution
- Create and manage on-demand and scheduled search queries in the Query Center
- Create and manage the Cortex XDR rules BIOC and IOC
- Working with Cortex XDR assets and inventories
- Write XQL queries to search datasets and visualize the result sets
- Work with Cortex XDR’s external-data collection

Audience

- Cybersecurity analysts and engineers
- Security operations specialists

Prerequisites

Participants must have completed EDU-260 (Cortex XDR: Prevention and Deployment).

Programme

1 - Cortex XDR Incidents 2 - Causality and Analytics Concepts 3 - Causality Analysis of Alerts 4 - Advanced Response Actions 5 - Building Search Queries 6 - Building XDR Rules 7 - Cortex XDR Assets 8 - Introduction to XQL 9 - External Data Collection

Session Dates

Date	Location	Time Zone	Language	Type	Guaranteed	PRICE
10 Nov 2022	Virtual Classroom	GMT	English	Instructor Led Online		£1,495.00
10 Nov 2022	London - Dowgate Hill	GMT	English	Classroom		£1,495.00
09 Jan 2023	Virtual Classroom	GMT	English	Instructor Led Online		£1,495.00
09 Jan 2023	London - Dowgate Hill	GMT	English	Classroom		£1,495.00
16 Mar 2023	Virtual Classroom	GMT	English	Instructor Led Online		£1,495.00
16 Mar 2023	London - Dowgate Hill	GMT	English	Classroom		£1,495.00
30 May 2023	Virtual Classroom	BST	English	Instructor Led Online		£1,495.00
30 May 2023	London - Dowgate Hill	BST	English	Classroom		£1,495.00
27 Jul 2023	Virtual Classroom	BST	English	Instructor Led Online		£1,495.00
27 Jul 2023	London - Dowgate Hill	BST	English	Classroom		£1,495.00
14 Sep 2023	Virtual Classroom	BST	English	Instructor Led Online		£1,495.00
14 Sep 2023	London - Dowgate Hill	BST	English	Classroom		£1,495.00
23 Nov 2023	Virtual Classroom	GMT	English	Instructor Led Online		£1,495.00
23 Nov 2023	London - Dowgate Hill	GMT	English	Classroom		£1,495.00

Additional Information

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