Cortex XDR Investigation and Response

Scope

- Level: Advanced
- Duration: 2 days
- Format: Lecture and hands-on labs
- Platform support: Cortex XDR Pro per Endpoint

Prerequisites

Participants must have completed (Cortex XDR: Prevention and

Deployment).

Course Modules

1 – Introduction to Cortex XDR Incidents

2 – Working with Causality and Analytics Concepts

3 – Using Causality Analysis of Alerts

4 – Working with Advanced Response Actions

5 – Working with Building Search Queries

6 - Building XDR Rules

7 – Using Cortex XDR Assets

8 - Introduction to XQL

9 -Using External Data Collection