Course : Palo Alto Networks - Cortex™ XDR 3.6: Investigation and Response (EDU-262)

Official course, preparation for Palo Alto Networks exams

Practical course - 2d - 14h00 - Ref. PA5
Price : 1790 € E.T.

NEW

With the training, you'll learn how to investigate attacks via Cortex XDR's incident pages. You'll see causal chains, alerts, logs, log stitching and the Causality and Chronology views. You'll use advanced response actions (remediation, EDL, remote scripting), create simple search queries, XDR rules and explore specialized views (IP, Hash). An introduction to the XQL language and integrations via the Cortex XDR API is also included.

Teaching objectives

At the end of the training, the participant will be able to:

- Investigating and managing incidents
- Describe Cortex XDR's concepts of causality and analysis
- Analyze alerts with Causality and Chronology views
- Use Cortex XDR Pro actions such as remote script execution
- Create and manage on-demand or scheduled search queries in the Query Center
- Create and manage Cortex XDR BIOC and IOC rules
- Working with Cortex XDR assets and inventories
- Write XQL queries to interrogate data sets and visualize results
- Using Cortex XDR external data collection

Intended audience

Cybersecurity analysts and engineers, security operations specialists.

Prerequisites

Completion of EDU-260 (Cortex XDR: Prevention and Deployment).

PARTICIPANTS

Cybersecurity analysts and engineers, security operations specialists.

PREREQUISITES

Completion of EDU-260 (Cortex XDR: Prevention and Deployment).

TRAINER QUALIFICATIONS

The experts who lead the training courses are specialists in the subjects covered. They are approved by the publisher and certified for the course. They have also been validated by our teaching teams in terms of both professional knowledge and teaching skills for each course they teach. They have at least three to ten years of experience in their field and hold or have held positions of responsibility in companies.

ASSESSMENT TERMS

Assessment of targeted skills prior to training.
Assessment by the participant, at the end of the training course, of the skills acquired during the training course.
Validation by the trainer of the participant's learning outcomes, specifying the tools used: multiple-choice questions, role-playing exercises, etc.
At the end of each training course, ITTCERT provides participants with a course evaluation questionnaire, which is then analysed by our teaching teams. Participants also complete an official evaluation of the publisher.
An attendance sheet for each half-day of attendance is provided at the end of the training course, along with a certificate of completion if the participant has attended the entire session.

TEACHING AIDS AND TECHNICAL RESOURCES

The teaching resources used are the publisher's official materials and practical exercises.

Practical details

Teaching methods

Training in French. Official course material in digital format and in English. Good understanding of written English.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training course.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you have specific accessibility requirements? Contact Ms FOSSE, disability advisor, at the following address: psh-accueil@orsys.fr so that we can assess your request and its feasibility.

Course schedule

1. **Module 1: Cortex XDR incidents**
2. **Module 2: Concepts of causality and analytics**
3. **Module 3: Causal analysis of alerts**
4. **Module 4: Advanced response actions**
5. **Module 5: Creating search queries**
6. **Module 6: Creating XDR rules**
7. **Module 7: Cortex XDR assets**
8. **Module 8 : Introduction à XQL**
9. **Module 9: External data collection**

Options

Certification : 260 € HT

Cette formation est recommandée dans le cadre du parcours de préparation aux certifications suivantes : Security Operations Professional, XDR Engineer.
Comment passer votre examen ?

The certification option comes in the form of a voucher or invitation that will allow you to take the exam at the end of the training course.

Dates and locations

REMOTE CLASS
2026 : 24 Mar., 16 June, 29 Sep., 8 Dec.

PARIS LA DÉFENSE
2026 : 24 Mar., 26 Mar., 8 Dec.