Formation : Palo Alto Networks - Cortex XDR: Investigation and Analysis

Cours officiel, préparation aux examens Palo Alto Networks

Cours pratique - 2j - 14h00 - Réf. PA5
Prix : 1790 € H.T.

NEW

Avec cette formation, vous découvrirez Cortex XDR, une plateforme avancée de détection et de réponse étendues. Vous développerez des compétences pratiques en gestion des endpoints, analyse d'incidents, investigation et exploitation des journaux avec XQL, ainsi qu'en utilisation d'outils avancés pour analyser efficacement les cas.

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Mener des investigations XDR en analysant cas, actifs, artefacts et chaînes de causalité
- Interroger et analyser les journaux avec XQL pour produire des analyses pertinentes
- Exploiter les outils et ressources avancés pour une analyse complète des incidents
- Maîtriser la gestion des cas et l'automatisation de la plateforme XDR
- Appliquer des stratégies et techniques avancées XDR en contexte SOC/CERT/CSIRT

Public concerné

Professionnels de la sécurité : analystes SOC, CERT, CSIRT, XDR, managers, responders incident, threat hunters, ainsi que consultants, ingénieurs commerciaux et partenaires delivery.

Prérequis

Avoir des bases en cybersécurité, une expérience en analyse d'incidents et en outils de sécurité, ainsi qu'une bonne compréhension de l'anglais écrit.

PARTICIPANTS

Professionnels de la sécurité : analystes SOC, CERT, CSIRT, XDR, managers, responders incident, threat hunters, ainsi que consultants, ingénieurs commerciaux et partenaires delivery.

PRÉREQUIS

Avoir des bases en cybersécurité, une expérience en analyse d'incidents et en outils de sécurité, ainsi qu'une bonne compréhension de l'anglais écrit.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils sont agréés par l'éditeur et sont certifiés sur le cours. Ils ont aussi été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum trois à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Évaluation des compétences visées en amont de la formation.
Évaluation par le participant, à l'issue de la formation, des compétences acquises durant la formation.
Validation par le formateur des acquis du participant en précisant les outils utilisés : QCM, mises en situation...
À l'issue de chaque formation, ITTCERT fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques. Les participants réalisent aussi une évaluation officielle de l'éditeur.
Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

Méthodes et moyens pédagogiques

Méthodes pédagogiques

Animation de la formation en français. Support de cours officiel au format numérique et en anglais.

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Programme de la formation

1. **Module 1 : Introduction à Cortex XDR**
2. **Module 2 : Endpoints**
3. **Module 3 : XQL**
4. **Module 4 : Alertes et détection**
5. **Module 5 : Vulnérabilités et analyse forensique**
6. **Module 6 : Automatisation de la plateforme**
7. **Module 7 : Gestion des incidents**
8. **Module 8 : Tableaux de bord et rapports**

Options

Certification : 260 € HT

Cette formation est recommandée pour préparer la certification Palo Alto Networks Certified XDR Analyst.
Comment passer votre examen ?

L'option de certification se présente sous la forme d'un voucher ou d'une convocation qui vous permettra de passer l'examen à l'issue de la formation.

Dates et lieux

CLASSE À DISTANCE
2026 : 24 mars, 16 juin, 29 sep., 8 déc.

PARIS LA DÉFENSE
2026 : 24 mars, 26 mars, 8 déc.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Les ressources pédagogiques utilisées sont les supports et les travaux pratiques officiels de l'éditeur.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.