

## Palo Alto Networks: Cortex XDR Security Operations and Integration

**Durée: 3 Jours**    **Réf de cours: PAN-CXDRSOI**    **Méthodes d'apprentissage: Classe à distance**

### Résumé:

Gain hands-on expertise in security operations, incident investigation, and system optimization to effectively protect modern environments. This 3-day instructor-led course provides in-depth training on Cortex XDR, Palo Alto Networks' powerful extended detection and response platform. You will gain hands-on expertise in security operations, incident investigation, and system optimization to effectively protect modern environments.

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

Classe à Distance - site Client

Cette formation peut être suivie à distance en synchrone depuis n'importe quel site pourvu d'une connexion internet (2 Mb/s en symétrique recommandés). Le programme (théorie et pratique) suit le même déroulé pédagogique qu'en présentiel. La solution technologique adoptée permet aux apprenants à distance de suivre les présentations faites au tableau, de voir et d'entendre l'instructeur et les participants en temps réel, mais également d'échanger avec eux.

### Public visé:

- SOC/CERT/CSIRT/XDR engineers and managers
- MSSPs and service delivery partners/system integrators
- Security consultants and sales engineers.

### Objectifs pédagogiques:

- Describe the role of Cortex XDR components, including endpoint agents, XDR collectors, NGFWs, and Broker VMs, in securing networks and devices.
- Utilize XQL to query and analyze logs for effective data ingestion and threat detection.
- Design and implement workflows to streamline security operations.
- Apply External Dynamic Lists and indicator rules to enforce security policies.

### Pré-requis:

- Attendees should possess a solid understanding of cybersecurity principles, including network and endpoint security concepts.

### Test et certification

- [Palo Alto Networks Certified XDR Engineer](#)

### Contenu:

Course Modules	3 - Integrations	7 - System Optimization
0 - Course Overview	4 - XQL	8 - Dashboards and Reports
1 - Overview of Cortex XDR	5 - Detection Engineering	9 – Email Security
2 - Software Components	6 – Platform Automation	

---

## Méthodes pédagogiques :

### **Palo Alto Networks Education:**

The technical curriculum developed by Palo Alto Networks and delivered by Palo Alto Networks Authorized Training Partners helps provide the knowledge and expertise you need to protect our digital way of life. Our trusted certifications validate your knowledge of the Palo Alto Networks product portfolio and your ability to help prevent successful cyberattack

---

## Autres moyens pédagogiques et de suivi:

- Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
- Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
- En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

### Délais d'inscription :

- Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
- Votre place sera confirmée à la réception d'un devis ou ""booking form"" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
- Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via [moncompteformation.gouv.fr](http://moncompteformation.gouv.fr).

### Accueil des bénéficiaires :

- En cas de handicap : plus d'info sur [globalknowledge.fr/handicap](http://globalknowledge.fr/handicap)
- Le Règlement intérieur est disponible sur [globalknowledge.fr/reglement](http://globalknowledge.fr/reglement)