Palo Alto Cortex XSIAM : SOC autonome et intégration sécurité réseau

Lien : https://innov-systems.com/formation/palo-alto-cortex-xsiam-soc-autonome-et-integration-securite-reseau

DURÉE
5 jours (35h)

RÉFÉRENCE
SI62

CATÉGORIE
Palo Alto Networks

Innov Systems

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Comprendre l’architecture de Cortex XSIAM
- Maîtriser les concepts de SOC autonome
- Centraliser et analyser les données de sécurité
- Automatiser la détection et la réponse aux incidents
- Intégrer la sécurité réseau dans le SOC
- Réduire les temps de détection et de réponse
- Utiliser l’IA pour améliorer la cybersécurité
- Corréler des événements multi-sources
- Mettre en place des playbooks automatisés
- Améliorer la visibilité globale de la sécurité
- Optimiser les opérations SOC
- Étudier des cas concrets de SOC moderne

POUR QUI ?

- SOC analysts
- Ingénieurs cybersécurité
- Security architects
- DevSecOps engineers
- Administrateurs sécurité
- Responsables SOC
- CTO et RSSI
- Consultants en cybersécurité
- Ingénieurs réseau et sécurité
- Threat hunters
- Data engineers sécurité
- Toute personne impliquée dans les opérations de cybersécurité

Innov Systems

Programme détaillé

1 / Introduction à Cortex XSIAM

- Concept de SOC autonome (Security Operations Center)
- Positionnement de Cortex XSIAM dans l'écosystème Palo Alto
- Évolution des SOC traditionnels vers l'automatisation

2 / Architecture de Cortex XSIAM

- Data lake de sécurité unifié
- Corrélation automatisée des événements
- Orchestration des workflows SOC

3 / Collecte et ingestion des données de sécurité

- Sources réseau, endpoint, cloud et identité
- Normalisation des logs
- Centralisation des événements de sécurité

4 / Détection avancée des menaces

- Détection basée sur l'IA et le machine learning
- Corrélation d'incidents multi-sources
- Réduction des faux positifs

5 / Automatisation des réponses (SOAR)

- Playbooks automatisés
- Réponse aux incidents en temps réel
- Réduction du temps de réaction (MTTR)

Innov Systems

6 / Intégration avec la sécurité réseau

- Intégration avec firewalls et solutions réseau
- Corrélation trafic réseau et événements SOC
- Visibilité bout en bout

7 / Threat Intelligence et enrichissement des données

- Sources de threat intelligence
- Enrichissement contextuel des alertes
- Priorisation des menaces

8 / Monitoring et observabilité SOC

- Dashboards et KPIs SOC
- Suivi des incidents en temps réel
- Analyse des tendances de sécurité

9 / Gouvernance et optimisation SOC

- Gestion des politiques de sécurité
- Optimisation des workflows SOC
- Conformité et audit

10 / Études de cas et SOC autonome

- Transformation d’un SOC traditionnel
- Automatisation complète des opérations
- Bonnes pratiques d’implémentation

Innov Systems

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

23 au 27 Nov. 2026	Distanciel
04 au 08 Jan. 2027	Présentiel - Casablanca
01 au 05 Mars 2027	Présentiel - Casablanca
26 au 30 Avr. 2027	Présentiel - Casablanca
21 au 25 Juin 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés