

Connaissance des concepts et de l'environnement du SOC

Formation Informatique / Bureautique / Sécurité



A l'issue de ce cours, vous serez en mesure de comprendre le rôle essentiel du SOC dans la sécurisation d'un système d'information, en appréhendant ses principes, son organisation, et son outil opérationnel (SIEM).

OBJECTIFS

- Connaître et comprendre le rôle, les principes, l'organisation, et le périmètre d'un SOC (Security Operation Center),
- Appréhender l'actuelle approche de la sécurité du système d'information : du réseau aux « end-points »,
- Connaître le rôle, les caractéristiques, et le fonctionnement général d'un outil de SIEM.

PUBLIC

- Administrateur Systèmes et réseaux

PRE-REQUIS

- Notions d'architecture logicielle Linux et Windows.
- Bonnes notions de réseau
- Connaissance basique des dispositifs de sécurité (Firewall, Proxy, Reverse Proxy, Antivirus...).
- Connaître le guide de l'hygiène informatique de l'ANSSI
- Avoir suivi le MOOC de l'ANSSI (secnumacademie.gouv.fr)

PROGRAMME

Introduction au SOC

- Définition et rôle du SOC dans le SI
- L'organisation du SOC et ses processus
- Panorama des menaces et évolutions
- La conformité
- Loi de programmation militaire et OIV
- Les journaux d'événements
- Les flux réseau
- Les indicateurs de compromission
- Les sources d'information

La sécurité actuelle du SI

- La sécurité périmétrique du S.I
- Sécurité des end points
- Sécurité industrielle
- Segmentation du réseau
- Cloud
- Shadow IT

Rôle et fonctionnement d'un SIEM

- Log management
- La corrélation
- L'importance de la gestion des actifs
- Concepts d'infraction de sécurité
- Les cas d'usage
- La gestion des vulnérabilités
- Implémentation de la PSSI
- Surveillance de la conformité
- Travaux intermédiaires : Accéder au site <https://www.securitylearningacademy.com/>
- Suivre les modules introductifs « QRadar »
- Lecture : Présentation du SOC d'AlertLogic <https://www.alertlogic.com/assets/files/InfoWorld-SOC-Article.pdf>

Horaires, Planning et Déroulement de cette formation

Horaires

- Formation de 9h00 (9h30 le premier jour) à 17h30.
- Deux pauses de 15 minutes le matin et l'après-midi.
- 1 heure de pause déjeuner

DEROULEMENT

- Les horaires de fin de journée sont adaptés en fonction des horaires des trains ou des avions des différents participants.



A retenir

Durée : **2 jours** soit 14h.
Réf. **SOCF**

☎ 01 42 93 52 72

Dates des sessions

Cette formation est également proposée en formule **INTRA-ENTREPRISE.**



Inclus dans cette formation



Coaching Après-COURS

Pendant 30 jours, votre formateur sera disponible pour vous aider. CERTyou s'engage dans la réalisation de vos objectifs.

100%
SATISFACTION
GARANTIE

Votre garantie 100% SATISFACTION

Notre engagement 100% satisfaction vous garantit la plus grande qualité de formation.

Connaissance des concepts et de l'environnement du SOC

Formation Informatique / Bureautique / Sécurité



- Une attestation de suivi de formation vous sera remise en fin de formation.
- Cette formation est organisée pour un maximum de 14 participants.

PROCHAINES FORMATIONS

[Réussir la Certification Gestion de Projet PMP du PMI](#)

[Réussir la Certification PRINCE2 Foundation](#)

[Réussir les Certifications PRINCE2 Foundation et PRINCE2 Practitioner](#)

[Réussir la Certification ITIL Foundation](#)

[Réussir la Certification Agile certifié SCRUM Master](#)

[Réussir les Certifications TOGAF Certified et TOGAF Foundation](#)

Retrouvez cette formation sur notre site :

[Connaissance des concepts et de l'environnement du SOC](#)