Connaissance des concepts et de l'environnement du SOC

Durée: 2 Jours **Réf de cours: SOCF**

Résumé:

Cette formation permet aux participants d'acquérir les compétences ou connaissances nécessaires pour 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).

Public visé:

Cette formation s'adresse aux administrateurs Systèmes et réseaux.

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Expliquer le rôle, les principes, l'organisation, et le périmètre d'un SOC (Security Operation Center),
- Décrire l'actuelle approche de la sécurité du système d'information : du réseau aux « end-points »,
- Expliquer le rôle, les caractéristiques, et le fonctionnement général d'un outil de SIEM.

Pré-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)

Contenu:

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'évènements
- 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

Méthodes pédagogiques :

Support de cours remis aux participants

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.
• Modalités d'évaluation : le participant est invité à s'auto-évaluer par rapport aux objectifs énoncés.
• Chaque participant, à l'issue de la formation, répond à un questionnaire de satisfaction qui est 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 vous utilisez votre Compte Personnel de Formation pour financer votre inscription, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés.