Présentiel/distanciel

SOC Security Manager

Cofinancé par l'Union européenne

Objectifs pédagogiques

- Identifier et comprendre les enjeux de la sécurité des systèmes d'information et des menaces actuelles
- Maîtriser l'utilisation des Security Information and Event Management (SIEM) pour la détection des incidents de sécurité
- Développer des compétences en matière de stratégie de détection et de traitement des alertes de sécurité
- Acquérir des connaissances approfondies en Threat Hunting, OSINT, et Cyber Threat Intelligence pour anticiper et contrer les menaces
- Analyser et réagir efficacement à des scénarios de compromission, comme les attaques par APT et ransomware

Prérequis

- Avoir une bonne connaissance des systèmes d'information et des réseaux
- Posséder des bases en matière de sécurité informatique
- Avoir de l'expérience dans l'administration système ou réseau est un plus, mais pas obligatoire

Public concerné

Cette formation est idéale pour les professionnels IT souhaitant se spécialiser dans la sécurité des systèmes d'information, notamment :

- Les responsables sécurité des systèmes d'information (RSSI)
- Les analystes de sécurité
- Les membres d'une équipe SOC
- Les administrateurs systèmes et réseaux souhaitant se spécialiser dans la sécurité

Présentiel/distanciel

Programme détaillé

Cofinancé par l'Union européenne

Jour 1 : Introduction (7 heures)

- La Sécurité des Systèmes d'Information
- Les menaces sur un Système d'Information : enjeux de la supervision
- Qu'est-ce qu'un Security Operation Center (SOC) ?
- Les missions du SOC
- Les bénéfices d'un SOC
- Les différentes organisations d'un SOC

Jour 2 : La détection des incidents de sécurité (7 heures)

- Présentation des Security Information and Event Management (SIEM)
- Définitions des évènements, alertes et incidents de sécurité
- Les sources d'information dans un SOC
- Format des journaux d'évènements et normalisation
- Exemples de journaux d'évènements

Jour 3 : La stratégie de détection et de traitement des alertes (7 heures)

- Exemple d'attaque et cas d'usage
- Règles SIGMA
- Le principe de positivité
- Analyser les incidents de sécurité
- Reconnaître les phases d'une attaque
- Supervision circonstancielle

Jour 4 : Comprendre les menaces et les acteurs : Threat Hunting, OSINT et CTI (7 heures)

- Cyber Threat Intelligence (CTI)
- Threat Intel Platform (TIP)
- Modèle Diamant
- Tactics-Techniques-Procedures
- STIX / TAXII
- Définition des Indicateurs de Compromission et l'importance du contexte
- Méthodologie des attaques
- Méthode d'investigation Threat Hunting

Jour 5 : Cas d'une compromission (7 heures)

- Scénario 1 (APT)
- Scénario 2 (Ransomware)

Présentiel/distanciel

Cofinancé par l'Union européenne

Délais d'accès à la formation

Les inscriptions sont possibles jusqu'à 48 heures avant le début de la formation.
Dans le cas d'une formation financée par le CPF, ENI Service est tenu de respecter un délai minimum obligatoire de 11 jours ouvrés entre la date d'envoi de sa proposition et la date de début de la formation.

Modalités et moyens pédagogiques, techniques et d'encadrement

Formation avec un formateur, qui peut être suivie selon l'une des 3 modalités ci-dessous :
1 Dans la salle de cours en présence du formateur.
2 Dans l'une de nos salles de cours immersives, avec le formateur présent physiquement à distance. Les salles immersives sont équipées d'un système de visio-conférence HD et complétées par des outils pédagogiques qui garantissent le même niveau de qualité.
3 Depuis votre domicile ou votre entreprise. Vous rejoignez un environnement de formation en ligne, à l'aide de votre ordinateur, tout en étant éloigné physiquement du formateur et des autres participants. Vous êtes en totale immersion avec le groupe et participez à la formation dans les mêmes conditions que le présentiel. Pour plus d'informations : Le téléprésentiel notre solution de formation à distance.

Le nombre de stagiaires peut varier de 1 à 12 personnes (5 à 6 personnes en moyenne), ce qui facilite le suivi permanent et la proximité avec chaque stagiaire.
Chaque stagiaire dispose d'un poste de travail adapté aux besoins de la formation, d'un support de cours et/ou un manuel de référence au format numérique ou papier.
Pour une meilleure assimilation, le formateur alterne tout au long de la journée les exposés théoriques, les démonstrations et la mise en pratique au travers d'exercices et de cas concrets réalisés seul ou en groupe.

Modalités d'évaluation des acquis

En début et en fin de formation, les stagiaires réalisent une auto-évaluation de leurs connaissances et compétences en lien avec les objectifs de la formation. L'écart entre les deux évaluations permet ainsi de mesurer leurs acquis.
En complément, pour les stagiaires qui le souhaitent, certaines formations peuvent être validées officiellement par un examen de certification.
Les candidats à la certification doivent produire un travail personnel important en vue de se présenter au passage de l'examen, le seul suivi de la formation ne constitue pas un élément suffisant pour garantir un bon résultat et/ou l'obtention de la certification.
Pour certaines formations certifiantes (ex : ITIL, DPO, ...), le passage de l'examen de certification est inclus et réalisé en fin de formation. Les candidats sont alors préparés par le formateur au passage de l'examen tout au long de la formation.

Moyens de suivi d'exécution et appréciation des résultats

Feuille de présence, émargée par demi-journée par chaque stagiaire et le formateur.
Evaluation qualitative de fin de formation, qui est ensuite analysée par l'équipe pédagogique ENI.
Attestation de fin de formation, remise au stagiaire en main propre ou par courrier électronique.

Qualification du formateur

La formation est animée par un professionnel de l'informatique et de la pédagogie, dont les compétences techniques, professionnelles et pédagogiques ont été validées par des certifications et/ou testées et approuvées par les éditeurs et/ou notre équipe pédagogique.
Il est en veille technologique permanente et possède plusieurs années d'expérience sur les produits, technologies et méthodes enseignés.
Il est présent auprès des stagiaires pendant toute la durée de la formation.

Accessibilité de la formation

ENI Service s'engage en faveur de l'accessibilité pour les personnes en situation de handicap (PSH). Toutes nos formations sont ainsi accessibles aux PSH. Pour en savoir plus, nous vous invitons à consulter la page "Accueil des personnes en situation de handicap" de notre site internet.