Analyste SOC, le métier

Cours Pratique de 2 jours - 14h
Réf : ASH - Prix 2024 : 1 660CHF HT

Ce cours très pratique présente le concept de SOC ainsi que l'ensemble des outils nécessaires en tant qu'analyste SOC.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

Comprendre les concepts et l'environnement d'un SOC

Utiliser les outils d'analyse

LE PROGRAMME

dernière mise à jour : 09/2023

1) Le SOC (Security Operations Center)

- Qu'est-ce qu'un SOC ?
- À quoi sert-il ? Pourquoi de plus en plus d'entreprises l'utilisent ?
- Les fonctions du SOC : logging, monitoring, reporting audit et sécurité, analyses post-incidents.
- Les bénéfices d'un SOC.
- Les solutions pour un SOC.
- Le SIM (Security Information Management).
- Le SIEM (Security Information and Event Management).
- Le SEM (Security Event Management).
- Exemple d'une stratégie de monitoring.

2) Le métier de l'analyste SOC

- En quoi consiste le métier de l'analyste SOC ?
- Quelles sont ses compétences ?
- Monitorer et trier les alertes et les événements.
- Savoir prioriser les alertes.

LES DATES

CLASSE À DISTANCE
2024 : 13 mai, 27 mai, 24 juin, 09 sept., 18 nov.

PARTICIPANTS

Techniciens et administrateurs système et réseau.

PRÉREQUIS

Bonnes connaissances en réseau et sécurité. Connaître le guide d'hygiène sécurité de l'ANSSI. Avoir suivi le parcours introductif à la cybersécurité.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…
Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.