Formation Mise en pratique du SIEM

N° ACTIVITÉ : 11 92 18558 92 | TÉLÉPHONE : 01 85 77 07 07 | E-MAIL : inscription@hubformation.com

Cette formation permet aux participants d'acquérir les compétences et connaissances nécessaires, grâce à des mises en situation réelles, de comprendre pourquoi et comment utiliser les différents outils, méthodologies, et services externes dont vous disposerez, en tant qu'analyste, au sein d'un SOC.

Référence	SOCP
Durée	3 jours (21h)
Tarif	2 250 €HT
Repas	60 €HT(en option)

SESSIONS PROGRAMMÉES

A DISTANCE (FRA)

du 3 au 5 novembre 2025

VOIR TOUTES LES DATES

Objectifs

| Expliquer la chaîne méthodologique d'usage des principaux outils à la disposition d'un analyste SOC
| Tester la conception de propositions de remédiation
| Identifier les perspectives d'évolution des outils de SIEM
| Expliquer l'ensemble des services et organisations spécialisés en matière de cyber sécurité

Public

| administrateurs systèmes et réseaux, analystes de sécurité, les architectes techniques « sécurité » et les gestionnaires d'infractions

Prérequis

| Connaissances des architectures logicielles Linux et Windows Avoir suivi le module « Les outils de l'analyste SOC »

Programme de la formation

Mises en situation
| Le cas « Target », 110 Millions d'enregistrements dérobés : analyse d'une attaque de points de vente en plein Black Friday.
| Discussion ouverte et travail collectif : propositions d'amélioration pour donner suite à l'analyse du cas Target.
| Présentation par les étudiants d'un cas de hack et analyse collective.

Le SIEM, extensions et perspectives ?
| La réponse à incident
| L'analyse de binaires / L'étude forensique
| Les procédures itératives d'amélioration continue
| Le Threat Hunting
| Le rôle de L'ANSSI, du SANS Institute, les CERTs/CSIRTs
| L'écosystème des CERTs et des CSIRTs privés, commerciaux et publics
| Les métiers de la cyber sécurité, les certifications reconnues

Préparation et passage de la certification Analyste QRadar
| Rappel des notions et références utiles
| Examen blanc
| Passage de la certification

Méthode pédagogique

Chaque participant travaille sur un poste informatique qui lui est dédié. Un support de cours lui est remis soit en début soit en fin de cours. La théorie est complétée

par des cas pratiques ou exercices corrigés et discutés avec le formateur. Le formateur projette une présentation pour animer la formation et reste disponible pour répondre à toutes les questions.

Méthode d'évaluation

Tout au long de la formation, les exercices et mises en situation permettent de valider et contrôler les acquis du stagiaire. En fin de formation, le stagiaire complète un QCM d'auto-évaluation.

Suivre cette formation à distance

Voici les prérequis techniques pour pouvoir suivre le cours à distance :

| Un ordinateur avec webcam, micro, haut-parleur et un navigateur (de préférence Chrome ou Firefox). Un casque n'est pas nécessaire suivant l'environnement.
| Une connexion Internet de type ADSL ou supérieure. Attention, une connexion Internet ne permettant pas, par exemple, de recevoir la télévision par Internet, ne sera pas suffisante, cela engendrera des déconnexions intempestives du stagiaire et dérangera toute la classe.
| Privilégier une connexion filaire plutôt que le Wifi.
| Avoir accès au poste depuis lequel vous suivrez le cours à distance au moins 2 jours avant la formation pour effectuer les tests de connexion préalables.
| Votre numéro de téléphone portable (pour l'envoi du mot de passe d'accès aux supports de cours et pour une messagerie instantanée autre que celle intégrée à la classe virtuelle).
| Selon la formation, une configuration spécifique de votre machine peut être attendue, merci de nous contacter.
| Pour les formations incluant le passage d'une certification la dernière journée, un voucher vous est fourni pour passer l'examen en ligne.
| Pour les formations logiciel (Adobe, Microsoft Office...), il est nécessaire d'avoir le logiciel installé sur votre machine, nous ne fournissons pas de licence ou de version test.
| Horaires identiques au présentiel.

Accessibilité

Les sessions de formation se déroulent sur des sites différents selon les villes ou les dates, merci de nous contacter pour vérifier l'accessibilité aux personnes à mobilité réduite.
Pour tout besoin spécifique (vue, audition...), veuillez nous contacter au 01 85 77 07 07.