Mise en pratique du SIEM

Durée: 3 Jours **Réf de cours: SOCP** **Méthodes d'apprentissage: Classe à distance**

Résumé:

Cette formation est délivrée en synchrone à distance tout en garantissant l'accès à un environnement d'apprentissage complet!
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.

Public visé:

Administrateur Systèmes et réseaux, analystes de sécurité, les architectes techniques « sécurité », les gestionnaires d'infractions

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- 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

Pré-requis:

Connaissances des architectures logicielles Linux et Windows

Avoir suivi le module « Les outils de l'analyste SOC »

Test et certification

Contenu:

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

Méthodes pédagogiques :

Support de cours remis aux participants.
Pour le suivi de cette formation à distance depuis un site client équipé, il suffit d'avoir une bonne connexion internet, un casque avec micro et d'être dans un endroit au calme pour en profiter pleinement. Une fiche explicative est adressée en amont aux participants pour leur permettre de vérifier leur installation technique et de se familiariser avec la solution technologique utilisée.
L'accès à l'environnement d'apprentissage (support de cours officiel, labs), ainsi qu'aux feuilles d'émargement et d'évaluation est assuré.
En savoir plus : https://www.globalknowledge.com/fr-fr/solutions/methodes-d'apprentissage/classe-a-distance

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.