Analyste SOC niveau avancé

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Domaine : Cybersécurité - sécurité informatique

Filière : Sécurité défensive

Rubrique : SOC (Security Operations Center)

Éligible au CPF : Oui
Code CPF : 36399

Action collective : Non

PRÉSENTATION

Objectifs & compétences

A l'issue de la formation, le stagiaire sera capable d'assurer les fonctions d'analyste d'un Security Operations Center (SOC), principalement la détection et l'analyse des intrusions, l'anticipation et la mise en place des protections nécessaires.

Public visé

Techniciens et administrateurs Systèmes et Réseaux, responsables informatiques, consultants en sécurité, ingénieurs, responsables techniques, architectes réseaux, chefs de projets…

Pré-requis

Connaître le guide sécurité de l'ANSSI, avoir des connaissances en réseau, avoir suivi le parcours introductif à la cybersécurité ou posséder des connaissances équivalentes. Avoir suivi le cours Analyste SOC1

PROGRAMME

Jour 1 matin & après-midi (Threat hunting) Approfondissement

Chapitre 1 :
Les sources de données à monitorer
• Indicateur Windows (processus, firewall, etc.)
• Service WEB (serveur, WAF, activité)
• IDS/IPS
• EDR, XDR
• USB
• DHCP, DNS
• Antivirus, EPP
• DLP, whitelist
• Email
Atelier pratique : cas d'usage et ligne de défense, mise en place du monitoring

Jour 2 matin & après-midi (analyse, Logstash, Elastic search) Approfondissement

Chapitre 2 :
Logstash (ETL)
• Fonctionnement de Logstash
• Les fichiers input & output
• Enrichissement : Les filtres Groks et sources externes
Atelier pratique : Configuration de Logstash

Jour 3 matin (gestion des incidents)

Chapitre 3 :
Réponse à incident
• État de l'art de la réponse à incident (CSIRT, CERT, FIRST, CERT-FR)
• Les différents métiers du CSIRT

Code de formation : SOC2

€ Tarifs

Prix public : 2100 €

Tarif & financement :
Nous vous accompagnons pour trouver la meilleure solution de financement parmi les suivantes :

- **Le plan de développement des compétences** de votre entreprise : rapprochez-vous de votre service RH.
- **Le dispositif FNE-Formation**.
- **L'OPCO** (opérateurs de compétences) de votre entreprise.
- **Pôle Emploi** sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.
- **CPF** -MonCompteFormation

Contactez nous pour plus d'information

Lieux & Horaires

Durée : 21 heures

Délai d'accès :
Jusqu'à 8 jours avant le début de la formation

Prochaines sessions

Consultez-nous pour les prochaines sessions.

• Quelle méthode, quel framework pour un CSIRT
• PRIS (Prestataires de réponse aux incidents de sécurité) de l'ANSSI
• Communication avec le CSIRT • Alerter le CSIRT lors d'une détection
• Comment le CSIRT procède lors d'une crise et une réponse à incident

Jour 3 après-midi (Conclusion)

Chapitre 4 :
conclusion
• Échange des différents travaux, rapport des stagiaires lors de la formation
• Points positifs, points négatifs
• Quelle conclusion pour la méthodologie d'un analyse SOC

MODALITÉS

Modalités

Modalités : en présentiel, distanciel ou mixte – Horaires de 9H à 12H30 et de 14H à 17H30 soit 7H – Intra et Inter entreprise
Pédagogie : essentiellement participative et ludique, centrée sur l'expérience, l'immersion et la mise en pratique. Alternance d'apports théoriques et d'outils pratiques.
Ressources techniques et pédagogiques : Support de formation au format PDF ou PPT Ordinateur, vidéoprojecteur, Tableau blanc, Visioconférence : Cisco Webex / Teams / Zoom
Pendant la formation : mises en situation, autodiagnostics, travail individuel ou en sous-groupe sur des cas réels

Méthode

Fin de formation : entretien individuel
Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation
Assiduité : certificat de réalisation (validation des acquis)