

Analyste SOC (Security Operations Center)

INFORMATIONS GÉNÉRALES

Type de formation : Formation continue

Éligible au CPF : Non

Domaine : Cybersécurité - sécurité informatique

Action collective : Non

Filière : Sécurité défensive

Rubrique : SOC (Security Operations Center)

Code de formation : SOC12

€ Tarifs

Prix public : 6399 €

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.

France Travail: sous réserve de l'acceptation de votre dossier par votre conseiller Pôle Emploi.

CPF -MonCompteFormation

Contactez nous pour plus d'information : contact@aston-institut.com

PRÉSENTATION

Objectifs & compétences

- Connaître l'organisation d'un SOC
- Comprendre le métier d'analyste SOC
- Appréhender les outils utilisés par les analystes SOC
- Identifier les principales problématiques à travers des cas d'usage
- Apprendre à détecter des intrusions
- Savoir gérer différents incidents
- Optimiser la sécurité d'un système d'information

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.

📍 Lieux & Horaires

Campus : Ensemble des sites

Durée : 56 heures

Délai d'accès :

Jusqu'à 8 jours avant le début de la formation

Distanciel possible : Oui

PROGRAMME

Jour 1 matin - SOC et métier d'analyste

Chapitre 1 :

Etat de l'art du Security Operation Center

- Définition du SOC
 - Les avantages, l'évolution du SOC
 - Les services intégrés au SOC, les données collectées, playbook
 - Le modèle de gouvernance du SOC (approche SSI, type de SOC, CERT, CSIRT)
 - PDIS de l'ANSSI (Prestataires de détection d'incidents de sécurité)
 - Pré requis et rôles d'un analyste SOC (techniques, soft skills, rôles, modèles)
 - Les référentiels (ATT&CK, DeTT&CT, Sigma, MISP)
- Démonstration 1 - utilisation du framework ATT & CK via Navigator (attaque et défense)

Jour 1 après-midi (découverte & mise en place du SIEM)

Chapitre 2 :

Focus sur l'analyste SOC

- Quel travail au quotidien
 - Triage des alertes
 - Révision et état de sécurité
 - Identification et rapport
 - Threat hunting
- Démonstration 2- utilisation de l'outil SYSMON

Jour 2 matin & après-midi (Threat hunting)

📅 Prochaines sessions

Cliquez sur la date choisie pour vous inscrire :

■ 25 / 11 / 2024

📍 : Ensemble des sites

✓ : Distanciel possible

🕒 : 56 heures

📅 : 8 jours

Chapitre 3 :

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

Exercice 1 / cas d'usage et ligne de défense

Jour 3 matin (analyse, Logstash, Elastic search)**Chapitre 4 :**

Tour d'horizon du SIEM

- Contexte du SIEM
- Solution existante
- Principe de fonctionnement d'un SIEM
- Les objectifs d'un SIEM
- Solution de SIEM

Jour 3 après-midi (analyse, Logstash, Elastic search)**Chapitre 5 :**

Présentation de la suite Elastic

- Les agents BEATS, sysmon
- Découverte de Logstash
- Découverte de Elasticsearch
- Découverte de Kibana

TP 1 / mise en place d'ELK et première remontée de log

Jour 4 matin & après-midi (analyse, Logstash, Elastic search)**Chapitre 6 :**

Logstash (ETL)

- Fonctionnement de Logstash
- Les fichiers input & output
- Enrichissement : Les filtres Groks et sources externes

Jour 5 matin (analyse, Logstash, Elastic search)**Chapitre 7 :**

ElasticSearch

- Terminologie
- Syntax Lucene
- Alerte avec ElasticAlert et Sigma

TP 2 / création d'alertes, alarmes

Démonstration 3 / utilisation d'Elastalert et Sigmac

Jour 5 après-midi (Kibana)**Chapitre 8 :**

Kibana

- Recherche d'événements
 - Visualisation des données
- Démonstration 4 / création d'un filtre sur Kibana
- Ajout de règles de détection, loC
 - Allez plus loin dans l'architecture ELK avec HELK

Jour 6 matin (cyber-entraînement)**Chapitre 9 :**

Mise en situation

- A travers des outils ESD Academy, l'analyste SOC est en situation et doit identifier plusieurs scénarios d'attaque lancés par le formateur
- TP 3 / Configurer un SIEM et l'exploiter

Jour 6 après-midi (cyber-entraînement)

TP 4 / Détecter une cyber attaque simple

Jour 7 matin (cyber-entraînement)

TP 5 / Détecter un cyber complexe (APT MITRE ATTACK)

Jour 7 après-midi (rapport)**Chapitre 10 :**

Rapport

- L'analyste SOC doit rapporter les attaques détecter et identifier les menaces, impacts, vérifier si son système d'information est touché.

TP 6 / Créer un rapport des attaques interceptées et évaluer l'impact

Jour 8 matin (initiation à la gestion des incidents)**Chapitre 11 :**

Réponse à incident

- État de l'art de la réponse à incident (CSIRT, CERT, FIRST, CERT-FR)
- Les différents métiers du CSIRT
- 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 8 après-midi (Conclusion)**Chapitre 12 :**

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**

Jusqu'à 8 jours avant le début de la formation, sous condition d'un dossier d'inscription complet

Méthode

Fin de formation : entretien individuel.

Satisfaction des participants : questionnaire de satisfaction réalisé en fin de formation.

Assiduité : certificat de réalisation.

Validations des acquis : grille d'évaluation des acquis établie par le formateur en fin de formation.