Analyste SOC

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

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.

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)

Chapitre 3 :
Les sources de données à monitorer
• Indicateur Windows (processus, firewall, etc.)
• Service WEB (serveur, WAF, activité)
• IDS/IPS

Code de formation : SOC

€ Tarifs

Prix public : 4299 €

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

Lieux & Horaires

Durée : 35 heures

Délai d'accès : Jusqu'a 8 jours avant le début de la formation, sous condition d'un dossier d'insciption complet

Prochaines sessions

Consultez-nous pour les prochaines sessions.

Informations non contractuelles - PDF généré le 12/11/2026

• 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, IoC
• Allez plus loin dans l'architecture ELK avec HELK

Jour 6 matin (cyber-entrainement)

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-entrainement)

TP 4 / Détecter une cyber attaque simple

Jour 7 matin (cyber-entrainement)

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

Informations non contractuelles - PDF généré le 12/11/2026

MODALITÉS

Modalités

Modalités : en présentiel, distanciel ou mixte . Toutes les formations sont en présentiel par défaut mais les salles sont équipées pour faire de l'hybride. – 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.
Validations des acquis : grille d'evalution des acquis établie par le formateur en fin de formation.

Informations non contractuelles - PDF généré le 12/11/2026