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

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 — Défense du SI & Prévention des menaces

Section 1 : Introduction

- Chiffres clés et tendances cyber
- Rôle et définition d'un SOC
- Défense en profondeur
- Priorisation de la défense
- Cyber Kill Chain
- Métier d'Analyste SOC

Exercice 1 : Création d'un chemin d'attaque, défense et surveillance

Section 2 : Prévention des menaces

- Exploitation du Cyber Threat Intelligence (CTI)
- Principes du Threat Hunting
- Gestion des vulnérabilités

Jour 2 — Analyse Systèmes & Technologies SIEM

Section 3 : Analyse Systèmes

- Analyse Windows & Linux
- Sources de données externes : IPS/IDS, serveurs de fichiers, proxy, DNS, sandbox, mobiles

€ Tarifs

Prix public : 3925 €

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

Campus : Ensemble des sites

Rythme : 5 jours. 5 au 9 Octobre 2026
23 au 27 Novembre 2026

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

Distanciel possible : Oui

Prochaines sessions

Cliquez sur la date choisie pour vous inscrire :

- 16 / 06 / 2025
  : Ensemble des sites
  ✓ : Distanciel possible
  : 56 heures
  : 8 jours
- 22 / 09 / 2025
  : Ensemble des sites
  ✓ : Distanciel possible
  : 56 heures
  : 8 jours
- 17 / 11 / 2025
  : Ensemble des sites
  ✓ : Distanciel possible
  : 56 heures
  : 8 jours

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

- Analyse comportementale (UBA)
- Suite Sysinternals

Exercice 2 : Installation et configuration de Sysmon

Section 4 : Technologies SIEM

- Concepts SIEM & CIM
- Corrélation des données
- Découverte des solutions SIEM
- Suite ELK (Elastic)
- Beats (agents)
- Logstash

Exercice 3 : Installation et configuration des agents Beats

Jour 3 — Enrichissement des logs, Visualisation & Alerting

- Enrichissement de données
- Présentation ElasticSearch
- Présentation Kibana

Exercice 4 : Manipulation des filtres Grok

Exercice 5 : Visualisation dans Kibana

Section 5 : Optimisation de l'Alerting

- Introduction à l'alerting
- Contextualisation des alertes
- Principes de détection
- Optimisation avec SIGMA

Jour 4 — Alerting avancé & Mise en pratique

Matin : Alerting avancé

- Présentation d'Elastalert2
- Intégrations avancées
- Automatisation
- Playbooks
- Introduction aux solutions SOAR

Après-midi : Mise en pratique

Exercice 6 : Mise en place d'un système d'alerting complet

Jour 5 — Threat Émulation & Exercice final

Matin : Threat Émulation

- Principes et enjeux
- Importance des tests réguliers
- Méthodes et approches
- Analyse et documentation
- Plan d'action
- Présentation d'outils d'émulation

Après-midi : Exercice final

Exercice 7 : Mise en place d'une Threat Émulation

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

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

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