

SOC (Security Operation Center) – Les fondamentaux

5 jours (35 heures)

Initiation

Présentiel ou classe à distance

à partir de

3 925 € HT par personne (TVA en vigueur) **Repas inclus en présentiel**

Contenu mis à jour le 30/09/2026. Document téléchargé le 07/10/2026.

Objectifs

A l'issue de cette formation, vous serez capable de :

- Décrire l'état de l'art du SOC (Security Operation Center)
- Organiser les tâches du quotidien dans un SOC
- Organiser et monitorer la collecte et l'analyse de données du SOC
- Répondre aux besoins des enjeux liés à la cybersécurité et des menaces par le métier d'analyste SOC
- Déployer et maintenir un SIEM.

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

Responsables de la Sécurité des Systèmes d'Information (RSSI), Directeurs des Systèmes d'Information, administrateurs systèmes et/ou réseaux, pentesters, consultants en sécurité de l'information et étudiants en sécurité informatique.

Prérequis

Avoir des connaissances générales en sécurité offensive et défensive, telles que les techniques de hacking, les modes opératoires adverses, des notions sur les systèmes d'exploitation et les mécanismes de durcissement associés.

Programme

1 Pendant votre formation

SOC (Security Operation Center) – Les fondamentaux

Jour 1

Etat de l'art du SOC (Security Operation Center)

- La place du SOC dans la sécurité des systèmes d'information
- Les rôles et les constituants
- Les différents types
- Les avantages et les contraintes
- Les données collectées et le playbook
- Le modèle de gouvernance des SOC
- Les différents métiers présents dans un SOC
- Les prérequis et le rôle d'un analyste
 - Techniques
 - Soft skills
 - Rôles
 - Modèles
- Les référentiels
 - MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)
 - MITRE DeTT&CT (Detection and Tactical Threat Countermeasure)
 - MITRE CAR
 - MITRE Shield
 - CKC (Cyber Kill Chain) de Lockheed Martin
 - The Diamond Model of Intrusion Analysis
 - NIST CSF (Cybersecurity Framework)
 - Purdue Model for ICS Security
- Les langages et protocoles
 - STIX (Structured Threat Information eXpression)
 - AXII (Trusted Automated Exchange of Intelligence Information)
 - Sigma
- Les plateformes d'échanges
 - AlienVault OTX (Open Threat Exchange)
 - MISP (Malware Information Sharing Platform)
 - ThreatConnect
 - Anomali ThreatStream

- TruSTAR

Exemples de travaux pratiques (à titre indicatif)

- Utilisation du framework ATT&CK pour modéliser les enjeux de sécurité du SI de la salle de formation
- Création de la liste des principaux scénarii d'attaque et propositions de contre-mesures

Focus sur l'analyste SOC

- Les tâches au quotidien
- L'analyse et le traitement des alertes
- La révision de l'état de sécurité
- L'identification et le reporting
- Le Threat Hunting

Exemples de travaux pratiques (à titre indicatif)

- Utilisation de l'outil Sysmon
- Utilisation d'outils d'Inforensic
- Création de règles de surveillance des élévations de privilèges
- Analyse d'IoC fournis par le formateur pour déterminer s'il s'agit d'une attaque

Les sources de données à monitorer et points de vigilance

- Les systèmes d'exploitation
- Processus, Firewall, journal d'événements...
- Les antivirus et dispositifs de End Point Protection (EDR et XDR)
- La gestion des comptes utilisateurs et l'utilisation de privilèges
- Les outils comportementaux (UEBA)
- Le rôle et le positionnement des IPS et des IDS
- Le rôle et le positionnement des proxies et gateways de sécurité
- Les serveurs d'application
- Le cas des services Web (Serveur, WAF, activité...)
- Les outils de gestion des vulnérabilités

Exemples de travaux pratiques (à titre indicatif)

- Installation d'un H-IPS et paramétrage de la réaction aux incidents et des remontées d'alertes
- Installation d'un H-IDS et paramétrage de la réaction aux incidents et des remontées d'alertes

Jour 2

Les sources de données à monitorer et points de vigilance – Suite

- La sécurité de la connectique Ethernet
- La sécurité des couches basses du modèle OSI
- Les services d'infrastructure DHCP et DNS
- La connexion et périphériques externes (USB, Wi-Fi, 4G...)
- La prévention de la perte de données (DLP)

- Le traitement du Whitelisting
- La sécurité des emails et de la messagerie

Exemples de travaux pratiques (à titre indicatif)

- Paramétrage d'un Firewall pour protéger le système d'un rogue DNS
- Création d'un script de protection contre les ARP Cache Poisoning
- Création d'un script d'inspection et de détection d'attaque par ARP Cache Poisoning
- Installation d'un N-IDS et paramétrage de la réaction aux incidents et des remontées d'alertes
- Analyse des données sensibles exposées et exploitation

Tour d'horizon des SIEM (Security information and event management)

- Le positionnement et le rôle d'un SIEM
- Le principe de fonctionnement et principaux composants
- Les objectifs
- Les étapes de mise en place d'un SIEM
- Les solutions communautaires et commerciales existantes

Exemples de travaux pratiques (à titre indicatif)

- Installation d'un serveur Web et d'un IPS ou d'un IDS avec paramétrage de la redirection des logs vers le syslog
- Mise en place d'un SIEM pointant sur le syslog
- Attaque et observation des remontées d'alertes

Jour 3

Introduction à Elastic Stack

- Présentation de la suite Elastic (Elastic NV, Logstash, Kibana et Beats)
- Le fonctionnement d'Elastic NV
- Les agents de collecte de données Beats et Sysmon
- La syntaxe Lucene
- Les alertes avec ElastAlert et Sigma
- Découverte de Logstash
- Découverte d'Elastic NV
- Découverte de Kibana

Exemples de travaux pratiques (à titre indicatif)

- Mise en place d'ELK et paramétrage de la remontée de logs
- Création d'alertes et d'alarmes
- Utilisation d'ElastAlert et Sigma

Prise en main de Logstash

- Fonctionnement de Logstash
- Configuration de Logstash pour l'intégration de données
- Création de pipelines de données : filtres, plugins et patterns

- Gestion des erreurs et monitoring de performance de Logstash

Exemples de travaux pratiques (à titre indicatif)

- Installation et paramétrage de Logstash pour remonter des logs systèmes et applicatifs

Jour 4

Exploration de Kibana

- Création de dashboards et visualisations (graphiques, tableaux, cartes)
- Utilisation de Kibana pour l'exploration de données en temps réel
- Fonctionnalités avancées : Canvas, Machine Learning et alertes
- Aller plus loin dans l'architecture ELK avec HELK

Exemples de travaux pratiques (à titre indicatif)

- Création d'un dashboard
- Création d'un filtre
- Ajout de règles de détection des IoC

Sécurité et optimisation de la performance

- Techniques de sécurisation d'Elastic Stack
- Surveillance et tuning des performances
- Best practices pour le déploiement en production

Exemples de travaux pratiques (à titre indicatif)

- Sécurisation du serveur ELK
- Création d'un script de suivi des performances

Jour 5

Reportings

- Les différents reporting de l'analyste
- Les rapports
 - D'alertes et de sécurité (attaques et violations de sécurité)
 - D'analyse d'incidents
 - De vulnérabilités
 - De gestion des correctifs
 - De tendances et de menaces
 - D'audits de conformité
- Les règles pour auditer son système d'information

Exemples de travaux pratiques (à titre indicatif)

- Préparation des KPI avec Kibana
- Création d'un rapport des attaques interceptées et évaluation de leurs impacts

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

Nous contacter pour en savoir plus →

Modalités pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2I, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

* nous consulter pour la faisabilité en distanciel

** ratio variable selon le cours suivi

Accessibilité aux personnes en situation de handicap

Détails de la session

Du 14 décembre 2026 au 18 décembre 2026 (5 jours / 35 heures)

Metz

Du 14 décembre 2026 au 18 décembre 2026

Metz

- 14 décembre 2026 ----- 9h00 – 15h00
- 15 décembre 2026 ----- 9h00 – 15h00
- 16 décembre 2026 ----- 9h00 – 15h00
- 17 décembre 2026 ----- 9h00 – 15h00
- 18 décembre 2026 ----- 9h00 – 15h00