

SOAR – Orchestration, automatisation et réponse aux incidents de sécurité informatique

3 jours (21 heures)

Perfectionnement

Présentiel ou classe à distance

à partir de

2 730 € HT par personne (TVA en vigueur) Repas inclus en présentiel

Contenu mis à jour le 25/09/2026. Document téléchargé le 07/10/2026.

Objectifs

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

- Définir les concepts, l'architecture et les cas d'usage d'un socle SOAR moderne
- Mettre en place un processus de réponse aux incidents aligné sur NIST SP 800-61r3 et le NIST CSF 2.0
- Concevoir, implémenter et tester des playbooks d'orchestration et d'automatisation pour différents types d'incidents
- Intégrer SIEM, EDR, IDS / IPS, CTI et outillage ITSM / DevOps au sein d'une plateforme SOAR
- Mesurer et améliorer la performance opérationnelle (MTTD, MTTR, qualité des playbooks et couverture MITRE ATT&CK)
- Gouverner et faire évoluer un programme SOAR (gouvernance, risques, conformité et amélioration continue).

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

À qui s'adresse cette formation ?

Ingénieurs et analystes SOC (N1-N3), membres de CSIRT / CERT, ingénieurs sécurité / architectes sécurité en charge des solutions SIEM / SOAR, responsables sécurité opérationnelle et responsables Blue Team, ainsi que les ingénieurs systèmes / réseaux impliqués dans la réponse aux incidents.

Prérequis

Avoir une bonne connaissance des concepts de base en sécurité des systèmes et des réseaux ainsi qu'une expérience pratique des logs, SIEM ou EDR / XDR en environnement de production. Avoir une bonne compréhension des processus SOC / CERT / CSIRT et des principaux types d'incidents. Etre à l'aise avec les scripts (Python, PowerShell ou équivalent) et les API REST est un plus.

Programme

1 Pendant votre formation

SOAR – Orchestration, automatisation et réponse aux incidents de sécurité informatique

Jour 1 – Matin

Contexte, enjeux et fondamentaux

- Enjeux actuels de la réponse aux incidents
 - Explosion du volume d'alertes et fatigue des analystes
 - Pression réglementaire, exigences de temps de réponse et reporting
 - Rôle des SOC, CSIRT, CERT et des opérations IT
- Définitions et périmètre SOAR
 - Security Orchestration, Automation and Response : définitions clés
 - Différences et complémentarité avec SIEM, XDR et UEBA
 - Principales capacités d'une plateforme SOAR moderne
- Composants et architecture d'une solution SOAR
 - Connecteurs, intégrations et API de l'écosystème sécurité / IT
 - Moteur de workflows et moteur de règles
 - Gestion des cas, des incidents et des artefacts
- Cas d'usage typiques
 - Tri automatique des alertes SIEM et déduplication
 - Réponse automatisée aux IOC simples (IP, domaine et hash)
 - Enrichissement automatisé par CTI et sources externes

Cadres de référence : NIST, MITRE ATT&CK et CTI

- NIST SP 800-61r3 et NIST CSF 2.0
 - Fonctions Identify, Protect, Detect, Respond et Recover appliquées à l'Incident Response
 - Recommandations clés et considérations de Rev 3

- MITRE ATT&CK et automatisation
 - Rappels sur les tactiques, techniques et procédures
 - Utilisation d'ATT&CK pour cartographier playbooks et détections
- Rôle de la Cyber Threat Intelligence
 - Types de CTI, formats d'échange (IOC, rapports et flux)
 - Intégration de la CTI dans les workflows SOAR

Jour 1 – Après-midi

Architecture détaillée et intégrations SOAR

- Intégration avec SIEM / XDR
 - Normalisation et corrélation des alertes
 - Envoi d'alertes, gestion des incidents et synchronisation d'état
- Intégration avec EDR, firewalls, proxy et IAM
 - Actions automatisables fréquentes : blocage, quarantaine, reset...
 - Points de contrôle, limites et garde-fous
- Intégration avec ITSM / ticketing et outils collaboratifs
 - Création et mise à jour automatique de tickets
 - Notifications, escalades et communication durant l'incident

Exemples de travaux pratiques (à titre indicatif)

- Découverte d'une plateforme SOAR et de ses connecteurs
- Parcours guidé d'une interface SOAR (connecteurs, cas et playbooks)
- Configuration de base d'un connecteur SIEM

Jour 2 – Matin

Modélisation des processus de réponse aux incidents

- Typologie des incidents et priorisation
 - Phishing, malware, ransomware, compromission d'accout, insider...
 - Critères de sévérité, impact, probabilité et criticité des actifs
- De la procédure manuelle au playbook automatisé
 - Identification des tâches répétitives et standardisables
 - Définition des points de décision et scénarios d'escalade
- Patterns de playbooks
 - Playbooks d'enrichissement et de tri d'alertes
 - Playbooks de containment et de remédiation automatisés
 - Playbooks de communication, notification et reporting

Exemples de travaux pratiques (à titre indicatif)

- Cartographier un processus end-to-end pour un use case (phishing et malware)
- Traduire ce processus en étapes de playbook (pseudo-workflow)

Conception de playbooks SOAR

- Structure interne d'un playbook
 - Déclencheurs (triggers) : alertes, tickets et événements API
 - Actions, conditions, boucles et timers
- Gestion des données et des artefacts
 - Manipulation des champs d'alerte, artefacts et entités (IP, users, hosts)
 - Journalisation des actions, traçabilité et horodatage
- Gestion des erreurs et des exceptions
 - Timeouts, échecs d'API et indisponibilité de composants
 - Stratégies de repli et reprise sur erreur

Exemples de travaux pratiques (à titre indicatif)

- Implémenter un playbook de tri et enrichissement d'alerte (IOC check, CTI, WHOIS et sandbox)
- Tester sur un jeu de données / alertes de démonstration

Jour 2 – Après-midi

Automatisation avancée : scripts, API, conditions

- Utilisation d'API REST dans les workflows
 - Appels API vers CTI, SIEM, EDR et systèmes internes
 - Gestion des tokens, authentification et pagination
- Scripts custom pour enrichir les playbooks
 - Scripts Python / PowerShell simples pour manipuler des données
 - Bonnes pratiques de versioning et de réutilisation
- Conditions avancées et logique métier
 - Seuils, agrégations et corrélation de multiples événements
 - Intégration de règles spécifiques métier / conformité

Exemples de travaux pratiques (à titre indicatif)

- Playbook avancé avec logique conditionnelle
- Etendre un playbook pour inclure plusieurs scénarios d'issue (auto-remédiation, semi-auto et manuel)
- Ajout d'un script custom pour un enrichissement spécifique

Jour 3 – Matin

Cas d'usage concrets SOAR

- Playbooks type pour phishing
 - Analyse automatique des emails, liens et pièces jointes

- Interaction avec la messagerie (quarantaine, retract et bannissement)
- Playbooks pour compromission d'endpoint / malware
 - Isolation automatique d'un poste, blocage d'IOC et déclenchement de scan EDR
 - Collecte automatisée d'artefacts (journaux, mémoire et fichiers)
- Playbooks pour incident d'identité / IAM
 - Réinitialisation de mot de passe, suspension de compte et MFA reset
 - Notifications aux propriétaires d'applications et aux managers

Exemples de travaux pratiques (à titre indicatif)

- *Construire un playbook complet pour un scénario (phishing ciblé, ransomware sur un serveur...)*
- *Test sur plusieurs jeux d'alertes et ajustement des conditions*

Jour 3 – Après-midi

Supervision, mesure et amélioration continue

- Indicateurs de performance et de maturité
 - MTTD, MTTR, taux d'automatisation et taux de succès des playbooks
 - Couverture par tactique / technique MITRE ATT&CK
- Gestion du changement et revue des playbooks
 - Processus de revue régulière et validation et mise en production
 - Documentation, knowledge base et retour d'expérience
- Sécurité, conformité et risques liés à l'automatisation
 - Garde-fous, approbations manuelles et séparation des environnements
 - Considérations réglementaires et preuves d'audit

Exemples de travaux pratiques (à titre indicatif)

- *Définir un ensemble d'indicateurs et d'alertes sur les playbooks*
- *Proposer un plan d'amélioration continue pour 6-12 mois*

Roadmap SOAR et clôture

- Tendances
 - Intégration accrue d'IA/ML pour la priorisation, la corrélation et la réduction de bruit
 - Evolutions des frameworks (MITRE ATT&CK et nouvelles techniques)
- Stratégie de déploiement et d'adoption
 - Approche pilote, itération par cas d'usage et scaling progressif
 - Implication des parties prenantes SOC, IT, métier et gouvernance

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](#)

Sessions

À distance

Du 12 octobre 2026 au 14 octobre 2026

Du 5 janvier 2027 au 7 janvier 2027

Paris La Défense

Du 12 janvier 2027 au 14 janvier 2027