PROGRAMME DE FORMATION

Détection et réponse aux incidents : SOC, SIEM et analyse de journaux

Cybersécurité & Protection des données

RÉFÉRENCE	VERSION	ÉDITION	DOMAINE
WF-0461	V2026-010	3 novembre 2026	Cybersécurité & Protection des données

DURÉE	MODALITÉ	PROGRAMME	SANCTION
155 h	Distanciel asynchrone (e-learning)	11 modules 122 leçons	Attestation et certificat de réalisation

Objectifs pédagogiques

Situer l'organisation d'un SOC (niveaux, procédures, escalade) et suivre une alerte de sa création à sa clôture motivée.

Collecter, normaliser et horodater des journaux de sources multiples, puis les interroger et les corréler dans un SIEM.

Analyser les journaux Windows, Linux, réseau, messagerie et cloud et qualifier une activité suspecte avec MITRE ATT&CK.

Écrire, tester et régler une règle de détection au format Sigma, et trier des alertes en limitant les faux positifs.

Conduire la réponse à un incident (identification, confinement, éradication, reprise, retour d'expérience) en préservant les preuves et rédiger le rapport d'incident.

L'essentiel de la formation

Public visé

Techniciens et administrateurs systèmes et réseaux qui veulent évoluer vers la cybersécurité opérationnelle : analyste de SOC de niveau 1 ou 2, référent détection, membre d'une cellule de réponse à incident.

Prérequis

Utiliser la ligne de commande Linux (fichiers, filtres, services, SSH) ; à défaut, les leçons de GNU / Linux (WF-0259) sont réemployées en rappel.

Connaître les bases des réseaux (adresses IP, ports, DNS, HTTP) et de l'administration d'un poste ou d'un domaine Windows.

Disposer d'un ordinateur avec une connexion internet et un navigateur récent ; un second écran est conseillé pour les investigations.

Modalités et déroulement

Formation à distance, en ligne, à rythme libre, sur la plateforme de l'organisme : dix modules de cours, puis un module d'évaluation finale. Les cas pratiques s'appuient sur des organisations fictives (Kestrel Mobilité, vélos électriques en libre-service avec application et API ; Imprimerie Brasselin, PME de 45 salariés sur deux sites ; Collectif Ombelle, studio de design et de vidéo ; Médiathèques de Valtorne, réseau intercommunal avec portail en ligne ; Les Vergers de Lirac, coopérative fruitière) et sur des journaux, alertes et extraits de requêtes fictifs reproduits dans les leçons. La première leçon comprend un positionnement, non éliminatoire, qui aide à repérer les notions à rafraîchir. Chaque leçon associe une vidéo animée de démonstration, des notions illustrées d'exemples (lignes de journaux Linux, Windows, pare-feu, proxy, DNS, messagerie, requêtes de SIEM, règles Sigma), un scénario à embranchements, des cartes de révision, une mise en pratique écrite (analyse de journaux, requête ou règle de détection à écrire, décision de triage, chronologie, note ou rapport à rédiger) corrigée par l'IA de la plateforme sur une grille de critères avec un corrigé modèle, et un quiz. Chaque module comprend un atelier de synthèse et se clôt par un QCM de fin de module. Aucune installation, aucune licence ni aucun compte payant n'est nécessaire ; les requêtes et règles étudiées peuvent être reprises sur son propre poste ou dans l'outil de son employeur. Accompagnement par un formateur par messagerie (réponse sous 48 h ouvrées), correction individuelle des livrables sur demande.

Méthodes pédagogiques

- Positionnement en début de parcours
- Apports en vidéo : explications et démonstrations
- Mises en situation et scénarios à décisions
- Études de cas
- Exercices d'application et mises en pratique corrigées
- Production de livrables professionnels
- Atelier de synthèse en fin de module
- Cartes de révision
- Quiz et QCM d'auto-évaluation
- Accompagnement et retours du formateur

Répartition du temps de formation : **22 %** théorique · **61 %** pratique · **17 %** évaluation

Moyens pédagogiques et techniques

- Plateforme de formation en ligne, accès individuel à distance
- Vidéos pédagogiques
- Modèles et supports téléchargeables
- Quiz et exercices interactifs en ligne
- Correction des productions sur grille de critères
- Messagerie avec le formateur (réponse sous 48 h ouvrées)

Modalités d'évaluation

Positionnement initial (non éliminatoire) ; dans chaque leçon, mise en pratique écrite corrigée sur une grille de critères et quiz de 6 à 8 questions ; atelier de synthèse et QCM de fin de module (14 ou 15 questions, seuil de réussite : 70 %, trois tentatives) à la fin de chacun des dix modules ; évaluation finale interne : étude de cas (intrusion sur l'extranet d'une PME fictive : qualification, chronologie en UTC, confinement, éradication et reprise, preuves, communication, rédigées en note de réponse à incident) corrigée sur grille, puis examen final de 30 questions en 60 minutes, deux tentatives au plus. Seuil de réussite de l'examen final : 70 % des points. Une attestation de fin de formation précise les compétences évaluées ; aucune certification, ni d'éditeur ni d'État, n'est délivrée ni préparée.

Sanction

Une attestation de fin de formation et un certificat de réalisation sont remis au participant sous réserve de la réalisation du parcours.

Cette formation n'est pas présentée comme préparant à une certification enregistrée : elle ne comprend ni inscription ni présentation à des épreuves de certification, et n'ouvre droit à aucune délivrance de certification ni au financement par le CPF.

Modalités et délais d'accès

La demande d'inscription peut être effectuée par téléphone, par courrier électronique ou au moyen du formulaire en ligne.

Un entretien ou un questionnaire de positionnement permet de vérifier l'adéquation de la formation avec les besoins, le niveau initial et les prérequis du candidat.

L'inscription devient définitive après validation du dossier administratif, acceptation des documents contractuels et, le cas échéant, confirmation du financement.

Les accès à la plateforme sont généralement activés sous 48 à 72 heures ouvrées après validation complète du dossier.

Les formations à distance sont proposées en entrées et sorties permanentes, sous réserve des délais ou dates imposés par le financeur ou le certificateur.

Accessibilité aux personnes en situation de handicap

Vidéos sous-titrées et transcrites, fiches pratiques, énoncés et corrigés en version texte lisible par les lecteurs d'écran, code et commandes fournis en texte copiable (jamais en image), contrastes et tailles de police réglables dans l'environnement d'exercice, navigation au clavier, rythme libre et durée allongeable pour les exercices chronométrés. Référent handicap joignable à handicap@will-formation.com pour étudier toute adaptation (durée, supports, outils, modalités d'évaluation).

Tarif de la formation

Prix : **3 875 €**

Financement : prise en charge possible par les organismes financeurs, selon les critères d'éligibilité applicables.

Qualiopi processus certifié

La certification qualité a été délivrée au titre de la catégorie d'action suivante : ACTIONS DE FORMATION. Certificat QUA25070009. WILL FORMATION — Société par actions simplifiée à associé unique au capital de 30 000 € — NDA 11757059675 (cet enregistrement ne vaut pas agrément de l'État) — SIRET 893 713 180 00014 — 01 85 09 25 99 — info@will-formation.com — www.will-formation.com

Programme détaillé

11 modules, 122 leçons — durée totale 155 h.

01 Le SOC et le cycle de vie des alertes

1. Positionnement — journaux, réseau et sécurité
2. Rappels Linux pour lire des journaux
3. Organisation d'un SOC : niveaux, rôles et procédures
4. Du signal à l'incident : cycle de vie d'une alerte
5. Les métiers du SOC : analystes N1, N2, N3, chasseurs et ingénieurs détection
6. Piloter un SOC : indicateurs de délai, de volume et de qualité des alertes
7. SOC interne, externalisé ou hybride : contrat, niveaux de service et responsabilités
8. Cadre réglementaire de la détection : NIS 2, RGPD et notification des incidents
9. Les outils du SOC : SIEM, EDR, SOAR, gestion des tickets et plateforme de renseignement
10. Main courante, passation entre équipes et documentation des alertes
11. Étude de cas : une semaine dans le SOC de Kestrel Mobilité
12. Atelier de synthèse — Le SOC et le cycle de vie des alertes
13. QCM de fin de module — Le SOC et le cycle de vie des alertes

02 Sources de journaux, collecte et horodatage

1. Cartographier les sources de journaux
2. Collecter et normaliser les journaux
3. Horodatage : aligner les événements dans le temps
4. Journaux système Linux : syslog, journald et auditd
5. Journalisation Windows : stratégies d'audit, Sysmon et transfert d'événements
6. Journaux applicatifs et web : serveurs HTTP, API et bases de données
7. Formats et schémas : JSON, CEF, LEEF et modèle commun de données
8. Fiabilité de la collecte : pertes, files d'attente, volumétrie et surveillance des sources
9. Conservation, intégrité et protection des journaux
10. Étude de cas : bâtir le plan de journalisation de l'Imprimerie Brasselin
11. Atelier de synthèse — Sources de journaux, collecte et horodatage
12. QCM de fin de module — Sources de journaux, collecte et horodatage

03 Chercher et corréler dans un SIEM

1. Premières requêtes : filtrer, compter, trier
2. Statistiques dans le temps et seuils
3. Corréler plusieurs sources
4. Expressions régulières et extraction de champs
5. Jointures, sous-requêtes et listes de référence
6. Détecter les anomalies : moyennes, écarts, percentiles et rareté
7. Tableaux de bord et visualisations pour le SOC
8. Chasser la menace : requêtes guidées par des hypothèses
9. Performances des requêtes et maîtrise des coûts d'un SIEM
10. Étude de cas : enquête complète dans le SIEM des Médiathèques de Valtorne
11. Atelier de synthèse — Chercher et corréler dans un SIEM
12. QCM de fin de module — Chercher et corréler dans un SIEM

04 Journaux Windows et Linux : authentification et privilèges

1. Les événements Windows qui comptent
2. Ouvertures de session : types, échecs et anomalies
3. Comptes, groupes et persistance : repérer les changements sensibles
4. Kerberos et NTLM : lire les événements d'authentification du domaine
5. Attaques sur l'Active Directory : force brute, pulvérisation de mots de passe, Kerberoasting, DCSync
6. Élévation de privilèges sous Windows : services, tâches planifiées et contrôle de compte
7. Authentification sous Linux : sudo, SSH, PAM et journaux d'authentification
8. Persistance sous Linux : cron, systemd, clés SSH et comptes cachés
9. PowerShell et lignes de commande : journaliser et détecter les abus
10. Étude de cas : compromission d'un compte administrateur
11. Atelier de synthèse — Journaux Windows et Linux : authentification et privilèges
12. QCM de fin de module — Journaux Windows et Linux : authentification et privilèges

05 Réseau, messagerie et cloud

1. Journaux de pare-feu et de proxy
2. DNS : repérer les requêtes anormales
3. Messagerie et Microsoft 365 : hameçonnage et compte compromis
4. Flux réseau et détection des communications de commande et de contrôle
5. Journaux des VPN et des accès à distance
6. Exfiltration de données : volumes, protocoles et canaux détournés
7. Authentification de la messagerie : SPF, DKIM, DMARC et lecture des en-têtes
8. Journaux d'audit Microsoft Entra ID et Microsoft 365
9. Journaux des fournisseurs de cloud : activité, identités et accès
10. Étude de cas : boîte de messagerie compromise et fraude au virement au Collectif Ombelle
11. Atelier de synthèse — Réseau, messagerie et cloud
12. QCM de fin de module — Réseau, messagerie et cloud

06 Postes, EDR et chronologie d'attaque

1. Ce que voit un EDR : processus, arborescence, télémétrie
2. Qualifier avec MITRE ATT&CK
3. Reconstituer une chronologie d'attaque
4. Télémétrie Sysmon : processus, connexions réseau et chargements de modules
5. Exécution et contournement des défenses : les binaires légitimes détournés
6. Mouvements latéraux : RDP, SMB, PsExec et WMI
7. Rançongiciels : signes précurseurs et chronologie type
8. Premier examen d'un fichier suspect sans l'exécuter : empreintes, chaînes et réputation
9. Super-chronologie : fusionner les sources et outiller la frise
10. Étude de cas : chronologie complète d'une intrusion aux Vergers de Lirac
11. Atelier de synthèse — Postes, EDR et chronologie d'attaque
12. QCM de fin de module — Postes, EDR et chronologie d'attaque

07 Écrire des règles de détection

1. Du scénario d'attaque à la règle de détection
2. Écrire une règle au format Sigma
3. Tester, régler et maintenir ses règles
4. Sigma avancé : modificateurs, conditions et agrégations
5. Convertir et déployer une règle Sigma dans son SIEM
6. Couverture de détection : cartographie MITRE ATT&CK et priorités
7. Détecter des comportements plutôt que des indicateurs : la pyramide de la douleur
8. Règles YARA : principes, lecture et usages
9. La détection comme du code : versions, revue et tests
10. Étude de cas : programme de détection pour Kestrel Mobilité
11. Atelier de synthèse — Écrire des règles de détection
12. QCM de fin de module — Écrire des règles de détection

08 Triage et renseignement sur la menace

1. Trier une alerte : méthode et priorisation
2. Faux positifs et vrais positifs : documenter sa décision
3. Exploiter des indicateurs de compromission
4. Enrichir une alerte : réputation, géolocalisation et contexte interne
5. Sources de renseignement : flux ouverts, CERT-FR et partage (MISP, STIX, TAXII)
6. Niveaux de renseignement : stratégique, opérationnel, tactique et technique
7. Analyser un adversaire : modèle du losange et chaîne d'attaque
8. Lutter contre la fatigue d'alertes : regroupement, suppression et priorisation par le risque
9. Escalade et communication : du N1 au N2, au client et à la direction
10. Étude de cas : une journée de triage, vingt alertes à traiter
11. Atelier de synthèse — Triage et renseignement sur la menace
12. QCM de fin de module — Triage et renseignement sur la menace

09 Réponse à incident

1. Préparer la réponse : rôles, contacts et procédures
2. Identifier l'étendue et confiner
3. Éradiquer, reprendre l'activité et tirer les leçons
4. Plan de réponse et cadres de référence : NIST et ANSSI
5. Gestion de crise cyber : cellule de crise, décisions et communication
6. Répondre à un rançongiciel : confinement, sauvegardes et restauration
7. Répondre à la compromission d'un compte dans le cloud
8. Obligations de notification : CNIL, NIS 2 et dépôt de plainte
9. Exercice sur table : préparer et animer une simulation d'incident
10. Étude de cas : gestion complète d'un incident à l'Imprimerie Brasselin
11. Atelier de synthèse — Réponse à incident
12. QCM de fin de module — Réponse à incident

10 Preuves, rapport et automatisation

1. Préserver les preuves : horodatage, intégrité, traçabilité
2. Rédiger le rapport d'incident
3. Playbooks et automatisation légère
4. Acquérir des preuves : mémoire, disque, journaux et ordre de volatilité
5. Chaîne de traçabilité et valeur probante des preuves
6. Rapport technique et note de synthèse pour la direction
7. SOAR : concevoir un playbook d'enrichissement et de confinement
8. Automatisation légère : analyser des journaux avec Python
9. Retour d'expérience et amélioration continue du SOC
10. Étude de cas intégrée : de l'alerte au rapport final
11. Atelier de synthèse — Preuves, rapport et automatisation
12. QCM de fin de module — Preuves, rapport et automatisation

11 Évaluation finale

1. Évaluation finale : questionnaire et étude de cas (de l'alerte au rapport d'incident)