DAWAN

Plan de la formation

www.dawan.fr

Formation Gestion d'incident / SOC / SIEM / traces / RETEX — 1 j

Durée :	1 jours (7 heures)
Tarif inter-entreprises :	1 175,00 € HT (Présentiel) 940,00 € HT (Distanciel)
Public :	RSSI / CISO - Responsables conformité - DSI et responsables sécurité des organismes concernés par NIS2
Pré-requis :	Administration Linux/Windows confirmée Notions de base en réseaux (TCP/IP, DNS, HTTP, pare-feu) Avoir suivi SEC-AIS-301 ou connaissances équivalentes en sécurité SI
Objectifs :	Comprendre l'organisation d'un SOC et le rôle de l'administrateur dans la chaîne de détection et de réponse Savoir qualifier un incident de sécurité et appliquer les étapes de réponse (PICERL) Exploiter un SIEM pour investiguer un incident — requêtes, corrélation, alertes Collecter et préserver les traces de manière forensiquement acceptable Conduire et rédiger un RETEX structuré et actionnable
Méthode pédagogique :	Fil rouge incident — un scénario d'attaque réaliste (compromission par phishing → mouvement latéral → exfiltration) traverse les 4 blocs ; chaque atelier exploite les livrables du précédent Hands-on SIEM — travaux pratiques sur stack Wazuh ou Elastic déployée en lab ; requêtes réelles sur des logs d'incidents synthétiques VM forensique — système Linux pré-compromis fourni ; collecte et analyse de traces en conditions réalistes Études de cas — incidents publics documentés (CERT-FR, ANSSI) utilisés pour illustrer les phases PICERL et les erreurs classiques de réponse Environnement : Linux natif recommandé — tous les outils sont open source (Wazuh, Elastic, Velociraptor, MISP, Wireshark, tcpdump)

Modalités pédagogiques, techniques et d’encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l’Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l’environnement adéquat. • Un formateur expert.
Modalité d'évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.
Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
Référence :	CYB102991-F
Note de satisfaction des participants :	Pas de données disponibles
Contacts :	commercial@dawan.fr - 09 72 37 73 73
Modalités d'accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
Délais d'accès :	Variable selon le type de financement.
Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

Bloc 1 — Organisation de la réponse à incident et rôle du SOC

- Cycle de vie d'un incident : détection → qualification → confinement → éradication → reprise → RETEX (modèle PICERL)
- Organisation d'un SOC : niveaux N1/N2/N3, rôles, outils, SLA de traitement
- Positionnement de l'administrateur infrastructure dans la chaîne de réponse — interface avec le RSSI, le SOC et les équipes métiers
- Qualification d'un incident : critères de sévérité, matrice d'escalade, notion de faux positif / vrai positif

- Procédures de gestion d'incident : déclenchement, communication de crise, traçabilité des actions

Atelier : À partir d'une alerte SIEM simulée, qualifier l'incident, remplir une fiche de qualification et déclencher la procédure d'escalade appropriée

Bloc 2 — SIEM et corrélation d'événements

- Architecture d'un SIEM : collecte, normalisation, corrélation, alerting, rétention
- Sources de logs essentielles : syslog Linux (/var/log/*, journald), Windows Event Log, logs réseau (pare-feu, proxy, DNS), logs applicatifs
- Normalisation et enrichissement des événements — CEF, ECS (Elastic Common Schema), LEEF
- Requêtes et investigation dans un SIEM (exemples sous **Elastic/Kibana** et **Wazuh**) : filtrage, agrégation, timeline d'événements
- Règles de corrélation : construction, test, gestion des faux positifs — exemples de règles SIGMA
- Tableaux de bord SOC : indicateurs temps réel, détection d'anomalies comportementales

Atelier : Investiguer un scénario d'incident complet dans un SIEM (Wazuh ou Elastic Stack) — reconstituer la timeline d'attaque à partir des logs, identifier le patient zéro et les systèmes compromis

Bloc 3 — Collecte et analyse de traces

- Principes de la forensique numérique : ordre de volatilité, intégrité des preuves, chaîne de custody
- Traces système Linux : auditd, journald, bash_history, /proc, last, wtmp, btmp, auth.log
- Traces système Windows : Event ID clés (4624, 4625, 4648, 4688, 4698, 7045...), prefetch, registre, LNK files
- Traces réseau : captures tcpdump/Wireshark, logs NetFlow, analyse DNS et proxy
- Collecte forensique live vs post-mortem — outils : dd, dc3dd, LiME (RAM), Velociraptor
- Détection d'indicateurs de compromission (IOC) : fichiers, hashes, IP, domaines — exploitation via MISP

Atelier : Sur un système Linux compromis (VM), collecter les traces volatiles et persistantes, calculer les hashes des artefacts, produire un rapport d'analyse synthétique

Bloc 4 — RETEX : méthode, rédaction et amélioration continue

- Objectifs et posture du RETEX : comprendre sans sanctionner, améliorer sans minimiser
- Structure d'un RETEX : chronologie des faits, analyse des causes racines (méthode des 5 pourquoi, arbre des causes), évaluation de la détection et de la réponse
- Identification des actions correctives : techniques, procédurales, organisationnelles — priorisation et responsables
- Rédaction du rapport de RETEX : à qui s'adresse-t-il, quel niveau de détail selon le destinataire (technique vs direction)
- Capitalisation : alimentation de la base de connaissance SOC, mise à jour des runbooks, révision des règles SIEM
- Boucle d'amélioration continue : lien entre RETEX, plan de traitement des risques et révision de la PSSI

Atelier fil rouge final : À partir du scénario d'incident investigué en Blocs 2 et 3, produire un RETEX complet — chronologie, analyse des causes, actions correctives priorisées, synthèse exécutive d'une page