DAWAN

Plan de la formation

www.dawan.fr

Formation Analyste SOC (Security Operations Center)

Durée :	8 jours (56 heures)
Tarifs inter-entreprise :	5 775,00 CHF HT (standard) 4 620,00 CHF HT (remisé)
Public :	Techniciens et administrateurs systèmes et réseaux, responsables informatiques, consultants en sécurité, ingénieurs, architectes réseaux, chefs de projets techniques
Pré-requis :	Bonnes connaissances des réseaux et des systèmes d'information
Objectifs :	Comprendre le rôle, les missions et l'environnement d'un analyste SOC - Maîtriser les fondamentaux de la cybersécurité défensive (logs, vulnérabilités, détection, corrélation) - Utiliser les principaux outils du SOC (SIEM, EDR, sondes, outils de ticketing et de CTI)- Analyser et corréler les événements de sécurité, qualifier et traiter les incidents- Collaborer avec les autres équipes de cybersécurité et réaliser une veille active
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.
Modalités 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 :	CYB102772-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

Définir le rôle de l'analyste SOC et les fondamentaux SOC & Threat Intelligence

Comprendre l'organisation et les missions d'un SOC (Niveaux 1, 2, 3, management)
Identifier les rôles et responsabilités d'un analyste SOC dans la chaîne de défense
Découvrir les principaux types de menaces et les concepts de base de la CTI (Cyber Threat Intelligence)
Relier SOC, CTI, gestion des vulnérabilités et gestion des incidents
Atelier fil rouge : cartographier les flux d'informations entre SOC, CTI, équipes réseau/systèmes et RSSI

Maîtriser la collecte de logs, la détection et la gestion des vulnérabilités

Comprendre les sources de logs : systèmes, applications, réseaux, sécurité, cloud
Configurer et interpréter les logs les plus importants pour la détection d'incidents
Découvrir les outils de gestion des vulnérabilités et leur intégration dans le SOC
Prioriser les vulnérabilités en tenant compte du contexte et des menaces actives
Atelier fil rouge : analyser un jeu de logs et de vulnérabilités et en extraire les événements les plus critiques

Utiliser un SIEM et automatiser les tâches récurrentes

Comprendre l'architecture et les fonctionnalités d'un SIEM
Créer et affiner des règles de corrélation et des alertes pertinentes
Mettre en place des tableaux de bord et des rapports pour le suivi des événements
Découvrir les principes d'automatisation via SOAR et scripts (playbooks, réponses automatiques)
Atelier fil rouge : construire une règle de corrélation simple dans un SIEM de

labo et analyser les alertes générées

Investiguer des scénarios d’attaques et gérer les incidents

Suivre une chaîne d’attaque typique (kill chain) à partir d’alertes SIEM et d’indices techniques
Recouper différentes sources (logs, CTI, vulnérabilités) pour qualifier un incident
Appliquer les procédures de réponse : containment, éradication, remédiation, restauration
Documenter l’incident et assurer le transfert vers les équipes concernées (forensic, réseau, systèmes, gouvernance)
Atelier fil rouge : conduire une investigation complète sur un scénario d’attaque simulée et rédiger une fiche d’incident

Travailler en coordination et assurer la veille cyber

Collaborer avec les équipes réseau, systèmes, développement, DPO, RSSI
Communiquer efficacement les risques et incidents aux différents interlocuteurs
Mettre en place une veille structurée sur les menaces, vulnérabilités et techniques d’attaque
Construire un plan de montée en compétences et de spécialisation pour un analyste SOC
Atelier fil rouge final : élaborer un mini-plan d’amélioration pour un SOC (processus, outils, CTI, compétences)