



# ANALYSTE SOC (SECURITY OPERATIONS CENTER) ET DURCISSEMENT WINDOWS



— <b>Public</b>	Techniciens et administrateurs Systèmes et Réseaux, responsables informatiques, consultants en sécurité, ingénieurs, responsables techniques, architectes réseaux, chefs de projets...
— <b>Durée</b>	3 jours - 21 heures
— <b>Pré-requis</b>	Avoir des connaissances en réseau Avoir suivi le parcours introductif à la cybersécurité ou posséder des connaissances équivalentes
— <b>Objectifs</b>	Connaître l'organisation d'un SOC Appréhender les outils utilisés par les analystes SOC Identifier les principales problématiques à travers des cas d'usage Apprendre à détecter des intrusions Optimiser la sécurité d'un système d'information Comprendre l'intérêt des techniques de durcissement systèmes et réseau
— <b>Méthodes pédagogiques</b>	Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire. La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification. Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par Audit Conseil Formation.
— <b>Moyens techniques</b>	1 poste de travail complet par personne De nombreux exercices d'application Mise en place d'ateliers pratiques Remise d'un support de cours Passage de certification(s) dans le cadre du CPF Remise d'une attestation de stage
— <b>Modalité d'évaluation des acquis</b>	Evaluation des besoins et objectifs en pré et post formation Evaluation technique des connaissances en pré et post formation Evaluation générale du stage
— <b>Planning</b>	Du 03/09/2024 au 05/09/2024 Du 10/12/2024 au 12/12/2024
— <b>Délai d'accès</b>	L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session
— <b>Accessibilité handicapés</b>	Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil.

## 1. PRINCIPES ET RÉFÉRENTIELS DE GESTION DES INCIDENTS CYBERSÉCURITÉ

- Introduction à la gestion des incidents cybersécurité
- NIST SP 800-61 Vs ISO / CEI 27035
- Les phases de gestion d'incident de cybersécurité
- Partage d'informations

## 2. ORGANISATION ET OUTILS DU SOC : CYBERSECURITY MONITORING ET SOC FOUNDATION

- Les enjeux de la surveillance du SI et SOC
- Introduction à « Security Monitoring »
- Security Operational Center – SOC
- Les modèles de SOC
- Les bases du SIEM
- Comment Fonctionne SIEM ?
- Évolution du SIEM
- Réponse aux incidents et automatisation avec SIEM
- Cas d'utilisation d'un NG-SIEM

## 3. VULNERABILITY MANAGEMENT

- Introduction à la gestion des vulnérabilités
- Processus de gestion des vulnérabilités
- L'évolution du cycle de gestion des vulnérabilités
- Les nouveaux systèmes de gestion des vulnérabilités – VMS

## 4. IMPLÉMENTATION DU SIEM : CENTRALISATION DES ALERTES AVEC LA STACK ELK

- La stack ELK
- Allez plus loin avec ELK

## 5. LES SCÉNARIOS D'ATTAQUE AVEC LA MATRICE ATTETCK ET ANALYSES TACTIQUES

- Utilisation de la matrice ATTetCK
- Identification des scénarios d'attaque
- Réflexions et analyses tactiques (SIEM)

## 6. DURCISSEMENT DES DOMAINES WINDOWS

- Utilisation d'une infrastructure de clés publiques (PKI) pour la création de stratégies de sécurité réseau (NPS, Radius)
- Sécurité des réseaux Wi-Fi
- Sécurisation de l'administration du domaine (WinRM, RPC, WMI, RDP)
- Sécurité des services et comptes de services managés (MSA)
- Classification et marquage de l'information pour les systèmes de prévention de pertes de données (DLP)

## NOUS CONTACTER

### Siège social

16, ALLÉE FRANÇOIS VILLON  
38130 ÉCHIROLLES

### Téléphone

04 76 23 20 50 - 06 81 73 19 35

### Centre de formation

87, RUE GÉNÉRAL MANGIN  
38000 GRENOBLE

### E-mail

contact@audit-conseil-formation.com

Suivez-nous sur les réseaux sociaux, rejoignez la communauté !



ACF Audit Conseil Formation



@ACF\_Formation



ACFauditconseilformation