

|                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| — <b>Public</b>                           | Utilisateur ou technicien IT                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| — <b>Durée</b>                            | ½ journée - 4 heures                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| — <b>Pré-requis</b>                       | Aucun                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| — <b>Objectifs</b>                        | <p>Identifier les principales menaces cyber et comprendre leurs mécanismes.</p> <p>Appliquer les bonnes pratiques de cybersécurité au quotidien, tant en usage personnel que professionnel.</p> <p>Reconnaître et réagir face à une tentative de phishing, ransomware ou compromission de compte.</p> <p>Comprendre les enjeux de sécurité liés à l'administration des systèmes d'information.</p>                                                                                                                                                                                                                                                                                                                                                            |
| — <b>Méthodes pédagogiques</b>            | <p>Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire.</p> <p>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.</p> <p>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.</p> |
| — <b>Moyens techniques</b>                | <p>1 poste de travail complet par personne</p> <p>De nombreux exercices d'application</p> <p>Mise en place d'ateliers pratiques</p> <p>Remise d'un support de cours</p> <p>Passage de certification(s) dans le cadre du CPF</p> <p>Remise d'une attestation de stage</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| — <b>Modalité d'évaluation des acquis</b> | <p>Evaluation des besoins et objectifs en pré et post formation</p> <p>Evaluation technique des connaissances en pré et post formation</p> <p>Evaluation générale du stage</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| — <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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

## INTRODUCTION : LES CYBERATTAQUES, UN SUJET D'ACTUALITÉ (30 MIN)

### 1. CONTENU

- Quelques faits marquants récents (attaques de collectivités, hôpitaux, entreprises).
- Typologie des cyberattaques : ransomware, phishing / Spear-phishing, compromission de compte, fraude au président
- Motivations des attaquants (cybercriminalité, espionnage, activisme, etc.)
- Pourquoi les équipes IT sont critiques en cybersécurité

### 2. MÉTHODE

- Présentation avec schémas et chiffres clés (ANSSI, ENISA, rapports du Clusif).
- Échange participatif : avez-vous été témoin ou victime d'une attaque ?

## ANALYSE D'UNE MENACE EN FORTE CROISSANCE (30 MIN)

### 1. CONTENU

- Focus sur le ransomware (ex. : Lockbit, Hive, Ryuk) : chaîne d'attaque typique, moyens d'intrusion, propagation et chiffrement
- Étude d'un cas réel (ou mise en situation simplifiée)
- Impacts : opérationnels, financiers, réputationnels, juridiques

## 2. MÉTHODE

- Mini scénario à décrypter collectivement
- Discussion sur les points d'entrée techniques et humains

## RAPPEL DES BONNES PRATIQUES AU QUOTIDIEN (30 MIN)

### 1. CONTENU

- Sécurité des mots de passe (et MFA)
- Reconnaître un email suspect
- Sécurité mobile et télétravail
- Sauvegarde, mises à jour, vigilance
- Réflexes à adopter en cas d'incident

### 2. MÉTHODE

- Quiz interactif ou cas pratiques (identification d'un phishing)
- Infographies pédagogiques

## PARTIE 1 BONNES PRATIQUES POUR L'ADMINISTRATION DES SI (30 MIN)

### 1. SÉCURITÉ DÈS LA CONCEPTION

- Notions de Security by Design et Secure by Default

### 2. VULNÉRABILITÉS APPLICATIVES FRÉQUENTES

- Injection SQL / XSS / CSRF / Insecure Deserialization
- Gestion des erreurs et fuites d'information
- Exposition des API sans authentification

### 3. GESTION DES SECRETS ET CONFIGURATIONS

- Ne jamais versionner des mots de passe / clés d'API
- Utilisation de vaults ou variables d'environnement

### 4. BONNES PRATIQUES DANS LE CYCLE DEVOPS

- Intégration de scans de sécurité dans les pipelines CI/CD
- Revues de code et linting de sécurité
- Validation des dépendances (SCA, SBOM)

### 5. SUIVI DE LA SÉCURITÉ EN PRODUCTION

- Logging, alerting, détection d'anomalies
- Retours d'expérience sur incidents applicatifs

### 6. MÉTHODE

- Présentation illustrée avec extraits de code/commentaires typiques
- Mini cas pratique : analyse d'un morceau de code vulnérable

## PARTIE 2 BONNES PRATIQUES POUR L'ADMINISTRATION DES SI (30 MIN)

## 1. CONTENU

- Principes du "moindre privilège"
- Gestion des comptes et droits
- Journalisation, supervision, alertes
- Gestion des vulnérabilités (scanners, CVE, patching priorisé)
- Durcissement SSH / services exposés
- Segmentation réseau, durcissement des postes et serveurs
- Plan de sauvegarde et PRA/PCA

## 2. MÉTHODE

- Liste de contrôle / check-list
- Discussion sur les écarts fréquents

## ACTIVITÉS ET PILOTAGE DE LA SSI (30 MIN)

### 1. CONTENU

- Organisation de la SSI dans une entreprise : RSSI, DPO, DSI, prestataires
- Politique de sécurité
- Cartographie des risques
- Tableaux de bord et indicateurs
- Gestion des incidents

### 2. MÉTHODE

- Présentation synthétique + matrice de responsabilités (RACI)
- Exemples de tableaux de bord (KPI SSI)

## RÉGLEMENTATION ET CORPUS DOCUMENTAIRE (20 MIN)

### 1. CONTENU

- Obligations légales : RGPD, LPM, NIS2, RGS
- Normes et référentiels : ISO 27001 / 27005, guide d'hygiène informatique ANSSI, politique de sécurité / PSSI / charte utilisateur
- Rôle de la documentation et de la sensibilisation

### 2. MÉTHODE

- Synthèse comparative (ex : RGPD vs ISO 27001)
- Extraits concrets de documents internes

## CONCLUSION ET ÉCHANGES (15 MIN)

### 1. CONTENU

- Synthèse des points clés
- Questions / réponses
- Ressources complémentaires (liens ANSSI, Clusif, CNIL, etc.)

---

## NOUS CONTACTER

### Siège social

16, ALLÉE FRANÇOIS VILLON  
38130 ÉCHIROLLES

### Téléphone

04 76 23 20 50 - 06 81 73 19 35

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



ACF Audit Conseil Formation



@ACF\_Formation

Dernière mise à jour : 05/03/2026

PROFIL Formateur : Les formateurs sont recrutés selon plusieurs critères :  
Expérience, pédagogie, dynamisme et prévoyance.