# SENSIBILISATION À LA CYBERSÉCURITÉ IT

| | |
|---|---|
| **Public** | Utilisateur ou technicien IT |
| **Durée** | ½ journée - 4 heures |
| **Pré-requis** | Aucun |
| **Objectifs** | Identifier les principales menaces cyber et comprendre leurs mécanismes.<br>Appliquer les bonnes pratiques de cybersécurité au quotidien, tant en usage personnel que professionnel.<br>Reconnaître et réagir face à une tentative de phishing, ransomware ou compromission de compte.<br>Comprendre les enjeux de sécurité liés à l'administration des systèmes d'information. |
| **Méthodes pédagogiques** | Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire.<br>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.<br>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. |
| **Moyens techniques** | 1 poste de travail complet par personne<br>De nombreux exercices d'application<br>Mise en place d'ateliers pratiques<br>Remise d'un support de cours<br>Passage de certification(s) dans le cadre du CPF<br>Remise d'une attestation de stage |
| **Modalité d'évaluation des acquis** | Evaluation des besoins et objectifs en pré et post formation<br>Evaluation technique des connaissances en pré et post formation<br>Evaluation générale du stage |
| **Délai d'accès** | L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session |
| **Accessibilité handicapés** | Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil. |

## 1. INTRODUCTION : LES CYBERATTAQUES, UN SUJET D'ACTUALITÉ (25 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 ?

## 2. ANALYSE D'UNE MENACE EN FORTE CROISSANCE (25 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

## 3. RAPPEL DES BONNES PRATIQUES AU QUOTIDIEN (20 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

## 4.A BONNES PRATIQUES POUR LES DÉVELOPPEURS ET ÉQUIPES APPLICATIVES (30 MIN)

### 1. CONTENU

- Sécurité dès la conception : notions de Security by Design et Secure by Default
- Vulnérabilités applicatives fréquentes : Injection SQL / XSS / CSRF / Insecure Deserialization; Gestion des erreurs et fuites d'information; Exposition des API sans authentification
- Gestion des secrets et configurations : Ne jamais versionner des mots de passe / clés d'API; Utilisation de vaults ou variables d'environnement
- 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)
- Suivi de la sécurité en production : Logging, alerting, détection d'anomalies; Retours d'expérience sur incidents applicatifs

### 2. MÉTHODE

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

## 4-B. BONNES PRATIQUES POUR L'ADMINISTRATION DES SI (25 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

## 5. PRINCIPAUX RISQUES LIÉS À L'IA (30 MN)

### 1. CONTENU

- Fuite de données sensibles
- Hallucinations et désinformation
- Plagiat et propriété intellectuelle
- Ingénierie sociale assistée par IA
- Biais et discrimination
- Dépendance et perte d'esprit critique
- Les bonnes pratiques de l'utilisation de l'IA.

### 2. MÉTHODE

- Présentation synthétique.
- Etudes de cas réels.

## 6. ACTIVITÉS ET PILOTAGE DE LA SSI (25 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)

## 7. RÉGLEMENTATION ET CORPUS DOCUMENTAIRE (15 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

## 8. 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 : 09/09/2025