Durée :
1 jour
(9h - 15h30)

RENFORCER LA CYBERSÉCURITÉ EN ENTREPRISE : VIGILANCE ET RÉFLEXES AVANCÉS

(Perfectionnement 2)

Aspects pédagogiques

- Questionnaire numérique de prise en compte des attentes spécifiques envoyé dès la validation de l'inscription ;
- Quizz/Cas pratiques envoyés quelques jours avant la formation pour permettre aux participants de s'entrainer ;
- Evaluation (numérique) par chaque participant, dès la fin de la session, de la qualité de la formation (formateur, écoute, réponses aux questions, conditions matérielles, etc.) ;
- Attestation de formation ;
- Evaluation « à froid » 1 à 2 mois après la formation ;
- Formation animée par des professionnels expérimentés du réseau Bakertilly.

PLAN DÉTAILLÉ

1.Introduction & attentes

- Présentation des objectifs et du déroulé ;
- Recueil des attentes et expériences depuis Initiation 1 ;
- Discussion interactive sur les situations rencontrées et le niveau de vigilance.

2.Cybermenaces avancées

- Spear-phishing, whaling, ransomware, supply chain, menaces internes ;
- Scénario pratique : email ciblé à un manager ;
- Analyse de l'impact et des signaux d'alerte ;
- QCM / Quiz.

3.Communication professionnelle avancée

- Techniques de manipulation sophistiquées ;
- Exercice : détecter un changement de politique RH frauduleux ;
- Twist rôle : Finance, RH, Opérations ;
- QCM / Quiz.

4.Gestion avancée des informations sensibles

- Classification, confidentialité et conformité ;
- Scénario pratique : partage cloud avec partenaire externe ;
- Exercice décisionnel : que faire, comment protéger les données ;
- QCM / Quiz.

5.Utilisation sécurisée des outils collaboratifs

- Cloud, fichiers macros, liens cachés ;
- Exercice pratique : détecter et gérer un lien malveillant ;
- QCM / Quiz.

6.Risques liés aux équipements et mobilité

- Ordinateurs, smartphones, BYOD, Wi-Fi public ;
- Scénario : pop-up suspect sur laptop public ;
- Exercice décisionnel : verrouiller, signaler, sécuriser ;
- QCM / Quiz.

7.Simulation d'incident avancée

- Ransomware téléchargé accidentellement ;
- Exercices pas-à-pas : isolation, signalement, communication interne ;
- Débrief organisationnel : impact, responsabilité, prévention ;
- QCM / Quiz.

8.Évaluation finale et synthèse

- Quiz pratique basé sur des scénarios réels ;
- Discussion sur décisions, meilleures pratiques ;
- Synthèse des bonnes pratiques et règles essentielles à retenir ;
- Questions / réponses et conclusion.

9.LIVRABLES

- Support de formation complet et avancé ;
- Fiche synthèse « Bonnes pratiques cybersécurité – Perfectionnement 2 » ;
- Attestation de formation ;
- Suivi recommandé : évaluation à froid 1–2 mois après formation.

POINTS CLÉS

- Formation pour non-IT uniquement, consolidation et progression des connaissances ;
- Scénarios plus complexes et ciblés : menace interne, fraude ciblée, décisions sous pression ;
- 70 % pratique / 30 % théorie, exercices role-based ;
- Évaluation continue et à froid pour assurer adoption durable.