Formation Cybersécurité opérationnelle – Sécuriser les systèmes et réseaux

Jour 1 – Sécurisation des systèmes

- Panorama des principales menaces.
- Notion de surface d'attaque.
- Durcissement de Windows.
- Durcissement de Linux.
- Désactivation des services inutiles.
- Gestion des mises à jour.
- Sécurité des comptes utilisateurs.
- Comptes administrateurs et comptes privilégiés.
- Principe du moindre privilège.
- Authentification multifacteur.
- Bonnes pratiques de gestion des mots de passe.

Jour 2 – Sécurisation des réseaux

- Segmentation réseau.
- VLAN de sécurité.
- Principes des pare-feu.
- Règles entrantes et sortantes.
- ACL.
- Accès distant et VPN.
- Sécurisation des services réseau.
- Ports et services exposés.
- Introduction aux vulnérabilités.
- Découverte et analyse réseau avec Nmap.
- Interprétation des résultats.

Jour 3 – Surveillance, sauvegarde et réponse à incident

- Journaux Windows et Linux.
- Introduction à la centralisation des logs.
- Identification d'activités suspectes.
- Principes de sauvegarde.
- Règle de sauvegarde 3-2-1.
- Tests de restauration.
- Notions de PRA et PCA.
- Phishing et ingénierie sociale.
- Premières étapes de gestion d'un incident.
- Isolation d'un poste compromis.

- Préservation des traces.
- Bonnes pratiques de documentation et d’escalade.

Travaux pratiques

Analyse d’un environnement présentant plusieurs mauvaises configurations : identification des risques, correction des paramètres, analyse réseau et préparation d’une procédure simple de réponse à incident.