

Your Cyber INSURANCE



Plan de formation : Endpoint Security (SEP)

Jours	thème de formation	Contenu
2 jours	Gestion des vulnérabilités Responsable de la gestion des vulnérabilités	1. Introduction à la gestion des vulnérabilités. 2. Mise en œuvre d'un processus de gestion des vulnérabilités. 3. Application pratique de la gestion des vulnérabilités. 4. Évolution du cycle de gestion des vulnérabilités. 5. Présentation des solutions de gestion des vulnérabilités (VMS – Vulnerability Management Systems).
1 jour	Sécurité des plateformes mobiles	1. Vecteurs d'attaque sur les plateformes mobiles. 2. Piratage d'Android et d'iOS. 3. Gestion des appareils mobiles (MDM – Mobile Device Management) et BYOD (Bring Your Own Device). 4. Bonnes pratiques de protection.
1 jour	Sécurité des objets connectés (IoT)	1. Concepts de l'Internet des Objets (IoT). 2. Attaques ciblant les objets connectés. 3. Méthodologies d'attaque sur les environnements IoT. 4. Contre-mesures et mécanismes de protection.
2 jours	Fondamentaux de la sécurité Windows	1. Sécurité de Windows 10 Desktop. 2. Sécurité de Windows Server 2016.
2 jours	Sécurisation d'un domaine avec Active Directory	1. Active Directory : concepts et mise en œuvre. 2. Contrôle de l'application des stratégies de groupe (GPO – Group Policy Objects). 3. Recommandations pour la sécurisation des ressources du domaine.
3 jours	Maîtrise de la sécurité Linux et durcissement (Hardening)	1. Sécurisation des comptes utilisateurs. 2. Protection des serveurs par un pare-feu. 3. Configuration et gestion du service SSH. 4. Contrôle d'accès discrétionnaire (DAC – Discretionary Access Control). 5. Listes de contrôle d'accès (ACL) et gestion des répertoires partagés. 6. Contrôle d'accès obligatoire (MAC – Mandatory Access Control). 7. Audit et durcissement (Hardening) des systèmes Linux.