Cybersécurité et cyberdéfense

Non-certifiante | Formation continue

Réf. : 26205719F — Mise à jour : 17 avril 2026

Organisme responsable : **ECOLEFEST FORMATION EN SITUATION DE TRAVAIL**

Présentation de la formation

Objectifs

À l'issue de la formation, le participant sera capable de : Préparer les examens des épreuves en candidat libre - Comprendre les principaux types de menaces en cybersécurité - Connaitre les politiques de sécurité - Appliquer les évolutions du cybersécurité - Apprendre à se défendre contre les cyberattaques - Apprendre à utiliser d'outils de sécurité - Mettre en place des pratiques de navigation sécurisée - Pratiquer des méthodes de surveillance et des réponses aux incidents

Programme

Chapitre-I. Principaux Types de Menaces
Les meilleures pratiques de sécurité
Les dangers des cyber-menaces.
Les sauvegardes régulières et l'identification des priorités
Chapitre-II. Les politiques de sécurité
Stratégie pour établir et appliquer des politiques de sécurité claires et cohérentes au sein de l'organisation.
Normes et Régulations GDPR (Règlement Général sur la Protection des Données) : Régulation européenne sur la protection des données personnelles et la vie privée.
Chapitre-III. Les évolutions de la cybersécurité
Les modèles de conception relatifs aux accès aux données relationnelles ou non relationnelles (patrons de conception (Design Pattern), object-relational mapping (ORM), ...)
Comprendre le principe de connexion à une base de données à partir d'un logiciel d'interface (Middleware)
Apprendre à interpréter les formats de données (fichiers JSON, XML, ...)
Chapitre-IV Apprendre à se défendre contre les cyberattaques
Préparation à la certification pour comprendre les bases de la cybersécurité.
Les nouvelles menaces et techniques de cyberattaques
Mises à jour et Patch Management
Chapitre-V Application d'outils de sécurité
L'installation des logiciels antivirus et antimalware fiables et sa mise à jour.
Pare-feu, pour surveiller et contrôler le trafic réseau entrant et sortant.
Le MDM permet d'administrer et sécuriser les appareils mobiles, par exemple, celui-ci sera utilisé pour une application métier liée à une entreprise.
Chapitre-VI Sauvegardes régulières
Gérer les sauvegardes régulières de vos données importantes sur un support externe ou dans le cloud.
Plan de récupération, en cas de perte de données ou d'attaque par ransomware (logiciel malveillant qui prend en otage des données personnelles)
Identifier les ransomware (rançongiciel) et comment les éliminer
Comprendre l'algorithme DES (Data Encryption Standard)

La différence entre chiffrement (volonté d’empêcher l’accès au contenu) et codage
Chapitre-VII. Pratiques de navigation sécurisée
Identifier les liens suspects, dans des courriels ou des messages non sollicités.
Sites sécurisés en utilisant le protocole HTTPS.
Identifier les sources fiables pour réaliser les téléchargements
La sécurité du réseau domestique
La configuration du routeur, les identifiants par défaut et l’activation du cryptage WPA3.
Isolation du réseau par la création des réseaux séparés pour les appareils IoT (Internet of Things) et les ordinateurs principaux.
Chapitre -VIII. Surveillance et réponse aux incidents
Les outils pour surveiller les activités suspectes sur les systèmes.
Le développement d’un plan de réponse aux incidents pour savoir comment réagir en cas de cyberattaque.
Réalisation d’étude de cas par journée ou hebdomadaire si en distanciel.

Certifications préparées et métiers visés

Niveau d'entrée	Niveau de sortie
Niveau Préqualification / Collège	Sans niveau spécifique

Métiers associés

M1801 — Administration de systèmes d'information
M1802 — Expertise et support en systèmes d'information

Dates et lieux de formation

N° session	Modalité	Lieu	Du	Au
2270192S	Mixte	Betton	17/04/2026	17/04/2027

Source : GREF Bretagne #26205719F