



## IEEPI - Fiche formation

### Cybersécurité et Propriété Intellectuelle : Diagnostiquer, comprendre, agir

#### Objectifs :

- Analyser les risques spécifiques liés à la détention et à la circulation d'informations sensibles (brevets, savoir-faire, données techniques) dans un environnement numérique
- Appliquer les bonnes pratiques de protection des données et de sécurisation des communications dans le cadre d'activités de propriété intellectuelle
- Évaluer le niveau de maturité cybersécurité dans une organisation au regard des menaces ciblant les actifs immatériels
- Mettre en œuvre des réflexes structurés de prévention et de réaction face aux incidents cyber ciblant les actifs de propriété intellectuelle

#### Public :

- Responsables PI
- Juristes PI
- Conseils en propriété industrielle
- Ingénieurs brevets
- Mandataires européens
- Responsables innovation
- DPO / RSSI / DSI

#### Caractéristiques :

**Durée :** 7h

**Horaires :** Jour 1: 14h00-17h30 Jour 2: 09h00 à 12h30

**Niveau :** Perfectionnement

**Référence :** S01P103

#### Programme :

#### Introduction : PI & cybersécurité, un duo stratégique

- Définition des enjeux croisés : cybersécurité, innovation, propriété intellectuelle
- Typologie des actifs sensibles : brevets, secrets industriels, bases de données techniques
- Auto-diagnostic : évaluation du niveau de maturité cybersécurité
- *Exercice : Auto-diagnostic individuel en 10 critères de maturité cybersécurité*

#### La PI, cible privilégiée des cyberattaques

- Panorama des menaces : espionnage industriel, ransomware, fuites internes
- Les 4 profils d'attaquants ciblant la PI
- L'effet « coffre-fort » : pourquoi les cabinets et services PI sont des cibles à haute valeur
- *Quiz interactif sur les idées reçues*

#### Anatomie des attaques ciblant les brevets et le savoir-faire

- Points de vulnérabilité dans le cycle de vie d'un brevet
- Risques liés aux partenariats, aux dépôts, aux publications et à la sous-traitance
- Cas concrets d'attaques ciblées sur des portefeuilles de brevets
- *Étude de cas – Analyse d'incidents de fuite d'information brevetable et de fraude aux renouvellements de marques*

#### Bonnes pratiques de protection au quotidien

- Mots de passe, authentification multifacteur, chiffrement
- Classification de l'information et hygiène numérique





- Sécurisation du poste de travail et sensibilisation des équipes
- *Quiz interactif sur les bonnes pratiques*

## Sécuriser les communications et les documents sensibles

- Sécurisation des échanges : chiffrement, plateformes sécurisées
- Les métadonnées : un risque méconnu pour la confidentialité
- Démonstration : inspection et nettoyage d'un document
- *Exercice : Inspection et nettoyage des métadonnées d'un document Word réel*

## Cadre réglementaire et obligations

- RGPD, Cybersecurity Act, NIS2, DORA : panorama et évolution
- Obligations de notification et sanctions
- Impacts concrets pour les professionnels de la PI
- *Quiz interactif sur le cadre réglementaire*

## Réagir en cas d'incident : simulation de crise

- Les 5 réflexes d'urgence face à un incident cyber
- Simulation complète : scénario de compromission de messagerie dans un cabinet de CPI
- Communication de crise : informer et rassurer les clients
- *Simulation de crise (exercice individuel) et jeu de rôle*

## Plan d'action personnalisé, synthèse et clôture

- Les 5 actions prioritaires pour les 30 prochains jours
- Construction du plan d'action individuel
- Récapitulatif de la formation et ressources complémentaires
- *Exercice : Élaboration du plan d'action personnalisé et restitution collective*

### Détails:

## Prérequis

Aucun pré-requis technique en cybersécurité n'est exigé. Les participants doivent exercer ou avoir exercé une activité professionnelle en lien avec la propriété intellectuelle

## Méthodes

- Cours magistral
- Étude de cas ou cas pratique
- Partage d'expérience ou échanges entre pairs
- Simulation ou jeu de rôle

## Évaluation

- Exercices
- Quiz

## Intervenants

Conseil en propriété industrielle

