

Formation SSI : Comment se protéger de la Cybercriminalité

PLUS D'INFOS

- Contactez-nous

CONTACT REFERENT

- Commercial@ageris-group.com
- +33 3 87 62 06 00

MODALITES D'ACCES

- Accessible à distance
- Accessible en présentiel

DELAI D'ACCES

- La durée estimée entre la demande du stagiaire et le début de la formation est de 7 jours (peut être raccourci pour le mode distanciel)

ACCESSIBILITE AUX PERSONNES EN SITUATION D'HANDICAP

- Accessible à distance pour les personnes à mobilité réduite
- Pour connaître l'accessibilité aux salles de formation, vous pouvez nous joindre au +33 3 87 62 06 00

REFERENCE

- SSICYBERCRIM

TARIF

- 1490€ HT

DUREE DE LA FORMATION

- 2 jours – 14 heures

DATES DES SESSIONS

- Voir site internet

FORMULE INTRA-ENTREPRISE

Formulaire : [soumettez votre projet](#)

RESSOURCES PEDAGOGIQUES

- Cours théorique
- Exemples de faits et incidents de sécurité réels et récents et jurisprudence en France et en Europe
- Evaluation des compétences par un quizz en cours et en fin de formation
- Support de cours remis au stagiaire en fin de formation
- Outil distanciel : Teams

PRESENTATION DE LA FORMATION

La cybercriminalité est une menace qui touche toutes les organisations, sociétés, administrations. Elle a explosé de 60% entre 2019 et 2020. La question qui importe est de savoir si votre organisation sera prête lorsqu'elle se fera attaquer.

OBJECTIFS DE CETTE FORMATION

A l'issue de cette formation, le stagiaire aura les compétences pour :

- Comprendre les enjeux de la cybercriminalité
- Identifier les biens essentiels à protéger
- Identifier les sources de risques dans son organisation
- Détecter des actes de malveillance
- Réagir face à un acte de malveillance.

PUBLIC

RSSI, Fonction SSI, direction générale, DSI, juristes

PREREQUIS

Aucun prérequis n'est nécessaire

PROGRAMME DETAILLE

En présentiel/à distance

1. L'évolution de la cybercriminalité

- Internet aujourd'hui, données et chiffres
- Les nouveaux marchés de la cybercriminalité
- Approche économique de la cybercriminalité
- Comprendre le darknet
- Les outils des cybercriminels (botnets, attaques etc...)
- Quelques typologies d'attaque.

2. Droit des TIC et organisation de la cybersécurité en France

- Organisation de la cybersécurité en France
- Contexte juridique
- Droit des TIC
- La lutte contre la cybercriminalité, ANSSI et cybermalveillance.
- Le rôle de la CNIL et la protection des données personnelles.

3. Protéger son organisation

- Lexique et définitions (vulnérabilités, menaces, risques...)
- Les enjeux des Systèmes d'Information
- Identifier les biens essentiels et les biens supports
- Intégrer la sécurité au sein de son organisation
- Intégrer la sécurité au sein d'un projet
- Identification des difficultés liées à la prise en compte de la sécurité

4. Identifier et prévenir les sources de risques

- Gouvernance et cybersécurité, définition des rôles et responsabilités
- Définir une stratégie de sécurité des systèmes d'information
- La Charte Informatique

Formation SSI : Comment se protéger de la Cybercriminalité

POUR ALLER PLUS LOIN

- RGPD – Exercer le métier de DPO
- RGPD – Auditer sa conformité et se préparer à un contrôle de la CNIL

- La gestion des contrats
- Mettre en place un système de gestion des risques.
- Aperçu des ISO 27001 et 27005

5. Prévenir les risques : Les bonnes pratiques

- Les contrôles d'accès (physiques, logiques...)
- La gestion des comptes administrateurs
- La gestion des mots de passe
- Gérer les développements, les mises à jours et les déploiements
- Mettre en place une procédure d'escalade d'incidents
- Procédures ANSSI et CNIL de déclaration d'actes de malveillance.

MODALITES D'EVALUATION

Validation des connaissances et compétences par un quizz à la fin de chaque chapitre.