COMMENT LUTTER CONTRE LA CYBERCRIMINALITÉ

Menaces, risques et solutions pratiques pour les combattre

,

CYBER SÉCURITÉ

Objectifs de la formation

Comprendre les types de cyber risques auxquels votre organisation est ou sera confrontée

Savoir comment réagir face à ces multiples menaces

Identifier les ressorts du management de la sécurité des systèmes d'information

Avancer dans votre transformation digitale en anticipant les risques de malveillance

Parmi nos formateurs

- Professionnel(s) du secteur

Public concernés

- PDG, Directeur général
- Directeur de la stratégie
- Directeur innovation, R&D
- Directeur Marketing/Digital
- DSI
- Directeur Financier
- Tout cadre dirigeant qui a besoin d'y voir clair sur les niveaux de cyber risques pesant sur son organisation et comment y faire face : cette formation est accessible à tous les non spécialistes.

Prérequis

- Aucun prérequis n'est nécessaire

Accueil des participants

Répertorier les différents Cyber risques et mesurer leurs impacts

- Quelles sont les typologies d'attaque auxquelles vous pouvez faire face
- Quels sont les moyens utilisés
- Qui sont les attaquants
- Identifier les types de dommages possibles et évaluer leurs conséquences en termes financier, juridique et d'image de marque
- Estimer le coût des cyber-attaques

CAS PRATIQUE **Exemples de cyber attaques médiatisées illustreront cette première partie**

Comprendre les acteurs et l'écosystème du cyber risque en France

- Suivre l'évolution du système de défense nationale et ses conséquences pour votre organisation : loi de programmation militaire et loi renseignement, rôle de l'ANSSI et des CERT dans le système de défense français
- Maîtriser les points clés du cadre juridique lié à la protection des données : rôle de la CNIL et projet de réglementation européenne
- Identifier les prestataires et prestations possibles en matière de cyber défense : Qui fait quoi ? A qui s'adresser en fonction de vos difficultés ?

Déterminer les risques spécifiques associés aux outils digitaux

- Réseaux sociaux
- Messagerie
- Smartphones / tablettes
- Cloud
- Objets connectés

Adapter vos systèmes de défense en fonction des attaques

- Au quotidien, définir les bonnes pratiques de sécurité
- Connaître les antivirus, leurs capacités et leurs limites
- Rôle et impact des Firewall
- Pourquoi intégrer des outils de DLP (lutte contre la fuite des données)
- Utiliser les outils de SIEM (gestion des traces informatiques)
- Pratiquer des audits de sécurité (pentest)

Mettre en place et faire vivre les outils de management des risques au sein de votre organisation

- Définir le rôle du RSSI et de la DSI
- Top management : quel rôle à jouer
- Bien délimiter le rôle des prestataires
- Quels sont les systèmes de gestion et les normes de sécurité informatique gouvernant les bonnes pratiques (la famille des normes ISO 2700x)
- Qu'attendre en matière de tableaux de bord et de systèmes d'alertes pour piloter les niveaux de risques
- Quelles démarches de prévention mettre en place auprès des salariés : les principaux leviers pour protéger votre capital numérique et garantir la continuité de votre activité
- Construire votre système de prévention juridique
- Comment vous équiper en cyber assurance

Fin de journée

Dates

Modalités pédagogiques, d'évaluation et techniques

- **Modalités pédagogiques:**

Pour les formations synchrones-présentiel ou classes virtuelles (formations à distance, en direct), les stages sont limités, dans la mesure du possible, à une douzaine de participants, et cherchent à respecter un équilibre entre théorie et pratique. Chaque fois que cela est possible et pertinent, des études de cas, des mises en pratique ou en situation, des exercices sont proposées aux stagiaires, permettant ainsi de valider les acquis au cours de la formation. Les stagiaires peuvent interagir avec le formateur ou les autres participants tout au long de la formation, y compris sur les classes virtuelles durant lesquelles le formateur, comme en présentiel peut distribuer des documents tout au long de la formation via la plateforme. Un questionnaire

préalable dit 'questionnaire pédagogique' est envoyé aux participants pour recueillir leurs besoins et attentes spécifiques. Il est transmis aux intervenant(e)s avant la formation, leur permettant de s'adapter aux publics. Pour les formations en E-learning (formations à distance, asynchrones), le stagiaire peut suivre la formation à son rythme, quand il le souhaite. L'expérience alterne des vidéos de contenu et des activités pédagogiques de type quizz permettant de tester et de valider ses acquis tout au long du parcours. Des fiches mémos reprenant l'essentiel de la formation sont téléchargeables. La présence d'un forum de discussion permet un accompagnement pédagogique personnalisé. Un quizz de validation des acquis clôture chaque parcours. Enfin, le blended-learning est un parcours alternant présentiel, classes virtuelles et/ou e-learning.

- **Modalités d'évaluation:**

Toute formation se clôture par une évaluation à chaud de la satisfaction du stagiaire sur le déroulement, l'organisation et les activités pédagogiques de la formation. Les intervenant(e)s évaluent également la session. La validation des acquis se fait en contrôle continu tout au long des parcours, via les exercices proposés. Sur certaines formations, une validation formelle des acquis peut se faire via un examen ou un QCM en fin de parcours. Une auto-évaluation des acquis pré et post formation est effectuée en ligne afin de permettre à chaque participant de mesurer sa progression à l'issue de la formation. Une évaluation à froid systématique sera effectuée à 6 mois et 12 mois pour s'assurer de l'ancrage des acquis et du transfert de compétences en situation professionnelle, soit par téléphone soit par questionnaire en ligne.

- **Modalités techniques FOAD:**

Les parcours sont accessibles depuis un simple lien web, envoyé par Email aux stagiaires. L'accès au module de E-learning se fait via la plateforme 360Learning. La durée d'accès au module se déclenche à partir de la réception de l'invitation de connexion. L'accès aux classes virtuelles se fait via la plateforme Teams. Le(a) stagiaire reçoit une invitation en amont de la session lui permettant de se connecter via un lien. Pour une bonne utilisation des fonctionnalités multimédia, vous devez disposer d'un poste informatique équipé d'une carte son et d'un dispositif vous permettant d'écouter du son (enceintes ou casque). En ce qui concerne la classe virtuelle, d'un microphone (éventuellement intégré au casque audio ou à la webcam), et éventuellement d'une webcam qui permettra aux autres participants et au formateur de vous voir. En cas de difficulté technique, le(a) stagiaire pourra contacter la hotline au 01 70 72 25 81, entre 9h et 17h ou par mail au logistiqueformations@infopro-digital.com et la prise en compte de la demande se fera dans les 48h.