

MAÎTRISER LA SÉCURITÉ NUMÉRIQUE AU QUOTIDIEN

Analyse des menaces et bonnes pratiques pour sécuriser son activité professionnelle

1 JOUR, 7 HEURES

CONFORMITÉ / RISK
MANAGEMENT

CODE :
ARM41

Objectifs de la formation

Cartographier le cyberspace pour en comprendre les enjeux

Décoder les modes opératoires des pirates

Détecter les vulnérabilités du quotidien

Devenir acteur de la cyber-résilience

Parmi nos formateurs

- LE GUENNEC Régis
CEO,
IPCYB

Public concernés

- Toutes fonctions confondues

Prérequis

- Aucun prérequis

Tarifs

- Tarif Session en classe virtuelle : 995,00 €HT

Dans le secteur de l'assurance, la protection des données clients constitue le socle de la relation de confiance. La cybersécurité ne relève désormais plus seulement de l'informatique : c'est un impératif métier lié au devoir de conseil, à la conformité réglementaire et à la continuité de l'activité.

Un incident de sécurité peut paralyser le fonctionnement d'un organisme d'assurance, compromettre l'intégrité des dossiers et nuire à la réputation professionnelle. La vigilance représente la première ligne de défense.

Durant cette journée, la théorie laisse place à l'action. Au travers d'un scénario de gestion de crise au sein d'un cabinet fictif, les pratiques sont confrontées aux menaces réelles. À l'issue de ce parcours, les compétences opérationnelles sont acquises pour transformer la sécurité numérique en un levier de professionnalisme et garantir la résilience des outils de travail au quotidien.

Identifier les fondamentaux de la sécurité informatique

- Définitions clés : cyberspace, cybersécurité et cybercriminalité
- Les fonctions de sécurité : protéger, détecter, défendre et repartir
- Le triangle CID : Garantir la Confidentialité, l'Intégrité et la Disponibilité des données
- Analyser la valeur des données
- Panorama des profils d'attaquants

EXERCICE Identifier la sensibilité des données métiers selon le triangle CID (Confidentialité, Intégrité, Disponibilité)

Analyser les vecteurs d'attaque et les menaces

- Les vecteurs d'attaques : techniques (logiciels) vs humains (ingénierie sociale)
- Expliquer le cheminement d'une intrusion
- Focus sur les menaces : Vol (phishing), Extorsion (rançongiciel), Sabotage et Espionnage.
- Étude des impacts : préjudices financiers, juridiques (ACPR) et réputationnels

CAS PRATIQUE Reconstituer les étapes d'une attaque pour comprendre comment un simple vecteur humain devient une brèche technique

Diagnostiquer les failles techniques et comportementales

- Panorama des logiciels malveillants : vers, virus, ransomware, spyware.
- Identifier les failles techniques (systèmes non à jour, Wi-Fi public).
- Les failles humaines : ressorts psychologiques (urgence, peur, autorité)
- La vulnérabilité spécifique du smartphone professionnel
- Analyser les points de rupture dans le parcours de vente à distance

ILLUSTRATION Identifier les vulnérabilités (techniques/humaines) dans un environnement de travail afin de détecter les points de rupture

Adopter les bonnes pratiques et postures de sécurité

- Définition d'un modèle de menaces personnel
- Mesures de sécurité : comportementales, organisationnelles et techniques.
- Protéger ses données clients et son matériel en mobilité
- Utiliser la cybersécurité comme argument de vente
- Ressources à consulter pour rester alerte: MOOC ANSSI, podcasts et veille juridique

CAS PRATIQUE Quiz: Appliquer les mesures correctives et les réflexes conformes au cadre réglementaire (NIS2/ACPR) pour sécuriser l'activité

Dates

Classe virtuelle

24/09/2026

15/12/2026

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.