

## ASSURANCE ET RANSOMWARE : QUELLE COUVERTURE ?

Référence : DL367	Durée :	Niveau : Bases	Modalités : E-Learning	Tarifs : Nous consulter
----------------------	---------	-------------------	---------------------------	----------------------------

### LIEUX ET DATES :

### A distance

Nous consulter

### OBJECTIFS

- Comprendre la notion de couverture du risque cyber
- Déconstruire le mythe du paiement de la rançon

### Information complémentaire :

Module disponible dans l'**Université Digitale Ifpass** accessible par abonnement.

Pour plus de renseignements [cliquez ici](#) ou [contactez-nous](#)

[\*\*Consultez le taux de satisfaction de nos formations\*\*](#)  
[e-learning ici >>](#)

### POINTS FORTS

#### **Modalités pédagogiques :**

**Une pédagogie pensée pour articuler efficacité et autonomie. Une vidéo donnant de nombreux conseils concrets et opérationnels pour une mise en pratique immédiate. Un quiz final permettant de valider la bonne acquisition des connaissances. Une fiche pratique pour avoir les points clés de la formation toujours sous la main. De nombreux exemples illustrant les connaissances transmises.**

#### **Formateur(s) :**

**Alexia Morot, experte de la quantification du risque et de la réponse à incident, est responsable de l'offre cyber chez DATTAK.**

**Elle est diplômée de Neoma Business School et CentraleSupélec. Elle débute sa carrière chez Wavestone en 2016 en tant que consultante Cybersecurity & Digital Trust où elle accompagne des grands groupes (Engie, Saint-Gobain et Crédit agricole...) dans leur prise en compte du risque cyber, et leurs stratégies de réponse à incident.**

**Quatre ans plus tard, elle intègre Scor, premier réassureur français, et devient Cyber Underwriting Analyst. Elle participe notamment au lancement de l'offre cyber et à la stratégie de souscription. Experte reconnue de l'offre cyber, elle crée la Cyber Academy pour former l'ensemble des collaborateurs de Scor à l'offre cyber.**

#### **Les plus de la formation :**

Parmi la variété de cyberattaques qui ciblent les entreprises, le ransomware fait figure d'ennemi numéro un : il s'agit de l'attaque la plus signalée par les entreprises, toutes tailles confondues. La majorité des réclamations d'assurance cyber sont liées à des attaques par ransomware (ANSSI), principalement des attaques par rançon bloquant l'accès à des systèmes informatiques. Les petites et moyennes entreprises sont particulièrement vulnérables, représentant 40% des victimes (ANSSI).

En termes simples, un ransomware est un type de logiciel malveillant qui crypte les fichiers d'un utilisateur ou d'une organisation, rendant ces fichiers inaccessibles. Les attaquants exigent ensuite une rançon, généralement en Bitcoins ou autre cryptomonnaie, pour fournir la clé de déchiffrement.

Pour les personnes en situation de handicap souhaitant suivre une formation en e-learning, nous vous invitons à contacter notre référente handicap, Nadia Benakli, par e-mail à [nbenakli@ifpass.fr](mailto:nbenakli@ifpass.fr) ou par téléphone au 01 47 76 58 35, afin de déterminer les formations accessibles.

#### **Consultez le taux de satisfaction de nos formations**

**PLANETE CSCA RH ici >>**

#### **PROGRAMME**

- A. Types de ransomware
- B. Méthodes d'infiltration
- C. Assurance et cyber
- D. Paiement de la rançon

#### **Modalités pédagogiques :**

Une pédagogie pensée pour articuler efficacité et autonomie. Des podcasts donnant de nombreux conseils concrets et opérationnels pour une mise en pratique immédiate. Un quiz final permettant de valider la bonne acquisition des

connaissances. Des fiches pratiques pour avoir les points clés de la formation toujours sous la main. De nombreux exemples illustrant les connaissances transmises.

**Validation des acquis :**

**Comment est-elle évaluée ?**

Une évaluation vous attend, mais rassurez-vous, il n'y a pas de pièges, ni même de mauvaises surprises... dès lors que vous suivez normalement votre formation ! Obtenez un score minimum de 80% de bonnes réponses et inscrivez cette formation à votre tableau des réussites ! Vous pouvez refaire le questionnaire autant de fois que vous le souhaitez !

**Comment cette formation est-elle validée ?**

Pour valider cette formation, vous devez avoir :

Lu l'ensemble des ressources écrites mises à disposition : objectifs, parcours, présentation du formateur, déroulé pédagogique, ... ;

Visionné d'un bout à l'autre les vidéos ;

Téléchargé et consulté le support de conférence ;

Téléchargé et consulté la fiche pratique ou infographique ;

Réussi l'évaluation dans les conditions mentionnées ci-dessus.

## **Validation DDA**

Pour répondre à l'obligation de formation continue des distributeurs d'assurance d'au moins 15 heures annuelles, cette formation doit être impérativement réalisée dans le cadre d'un plan de développement des compétences personnalisé du participant (article A512-8 2° du Code des assurances).

### **Personnalisation parcours :**

**Une question technique ? Pédagogique ? Notre équipe pédagogique, community managers et webcocooners, est là pour y répondre ! Nous nous engageons à vous apporter une réponse dans un délai de 48 heures ouvrées après le dépôt de la question sur le forum dans l'onglet "Communauté".**

**Vous avez dit webcocooner ? Tout à fait ! Le webcocooner est notre couteau suisse, professionnel de l'assurance formé à l'accompagnement des participants en ligne. Son rôle ? Répondre aux questions pédagogiques, techniques et administratives que vous pouvez vous poser !!**

### **PUBLIC**

Agents, courtiers, intermédiaires ou tout professionnel exerçant une activité dans le domaine de l'assurance, de la banque ou de la finance et intéressé par la cybersécurité.

### **Pour les personnes en situation de handicap** souhaitant réaliser une formation e-learning :

Nous vous invitons à prendre contact avec notre référent handicap (Nadia Benakli - [nbenakli@ifpass.fr](mailto:nbenakli@ifpass.fr)) afin de déterminer les formations accessibles.

### **PRÉ-REQUIS**

#### **Prérequis pédagogiques :**

Cette formation ne nécessite pas de prérequis spécifiques.

#### **Prérequis techniques :**

- Navigateurs internet
- Chrome (2 dernières versions majeures)
- Firefox (2 dernières versions majeures)
- Edge (2 dernières versions majeures)
- Safari sur OSX (2 dernières versions majeures)

Les vidéos de cette formation sont hébergées sur le site vimeo.com. Elles sont sous-titrées.

#### **Logiciels :**

- Lecteur PDF (pour les documents associés)
  - Lecteur audio/vidéo
  - Suite Microsoft Office (pour la restitution des missions)
- Un casque audio peut être nécessaire si les formations sont suivies dans un espace partagé.

#### **Modalité d'accès :**

- Les demandes d'inscription se font par mail à [mo-inscriptions@ifpass.fr](mailto:mo-inscriptions@ifpass.fr)
- Toutes les démarches administratives et financières doivent être réglées avant le début de la formation. Veuillez noter qu'en cas de demande de financement à un organisme financeur, la démarche de prise en charge est à réaliser par le candidat ou l'entreprise et doivent être réalisées à l'avance

#### **TARIFS ET FINANCEMENTS**

Exonérés de TVA

Module disponible dans l'Université Digitale Ifpass accessible par abonnement.  
Pour plus de renseignement contactez-nous !

#### **CONTACT**

[mo-inscriptions@ifpass.fr](mailto:mo-inscriptions@ifpass.fr) / 01 47 76 58 70

Généré le 28/01/2026 à 01:10