Nom : _____ Date : _____ Note : _____

Rançongiciels et entreprises Récupération

Exécution de la charge utile, chiffrement cryptographique des fichiers, sauvegardes hors ligne, procédures de confinement et reprise après sinistre.

ATTAQUES PAR RANÇONGICIEL : PRÉSENTATION

SÉCURISÉ
CHIFFREMENT DES DONNÉES
Norme AES 256 bits

CONFORME
NORMES MONDIALES
Cadres RGPD (GDPR) et CCPA

ZERO TRUST
POLITIQUE D'ACCÈS
Authentification multifacteur

Bienvenue ! Ce dossier d'activités vous guide à travers les attaques par rançongiciel et la reprise d'activité. Vous étudierez l'exécution de la charge utile, le chiffrement des fichiers, les sauvegardes hors ligne, le confinement des menaces, les paiements en cryptomonnaie et les plans de reprise après sinistre.

POINTS DE CONTRÔLE DE LA FICHE

- [ ] **Parties 1-4 : maîtrisez la cybersécurité et la prévention des menaces.**
- [ ] **Parties 5-7 : résolvez les mots croisés et les mots mêlés.**
- [ ] **Parties 8-9 : résolvez les études de cas et le défi de déchiffrement.**
- [ ] **Partie 10 : consultez les FAQ de base et avancées.**
- [ ] **Partie 11 : découvrez 10 faits concrets intéressants.**
- [ ] **Bonus : défi Réflexion rapide.**

Ouvrir le guide VPN.com de la cybersécurité

URL: https://www.vpn.com/fr/cybersecurite/attaque-ransomware/

Votre parcours d'apprentissage : reprise après un rançongiciel

- Distinguer les charges de type cheval de Troie, rançongiciel et logiciel espion.
- Analysez des fichiers malveillants dans des environnements de bac à sable sécurisés.
- Élaborer des procédures rapides d'isolement et de confinement du réseau.

GUIDE DES ATTAQUES PAR RANÇONGICIEL : CONSIGNES

Répondez aux questions à choix multiple et vrai/faux, complétez les phrases à trous à l'aide de la banque de mots, associez les définitions et résolvez les mots croisés et les mots mêlés. Appliquez vos connaissances à la récupération après une attaque par rançongiciel. Terminez par l'activité bonus Réflexion rapide.

ATTAQUES PAR RANÇONGICIEL ET REPRISE APRÈS SINISTRE (INTRODUCTION)

Les charges de rançongiciel verrouillent le stockage du système par chiffrement et exigent des paiements en cryptomonnaie en échange des clés de déchiffrement. Pour atténuer cette menace, on s'appuie sur des règles d'isolement du réseau, l'analyse des logiciels malveillants en sandbox et des sauvegardes à froid isolées (air-gapped) robustes.

LISEZ ATTENTIVEMENT CHAQUE POINT DE CONTRÔLE ET CHOISISSEZ OU ÉCRIVEZ LA BONNE RÉPONSE.

Point de contrôle 1 : Défi QCM

1. Quel est le mécanisme principal d'une attaque par rançongiciel ?

- A. Chiffrement cryptographique des fichiers de l'utilisateur pour bloquer l'accès au système
- B. Injecter des commandes SQL malveillantes dans des champs de formulaire
- C. Intercepter les paquets réseau sur une connexion Wi-Fi publique
- D. Falsifier les en-têtes d'e-mail pour contourner la validation SPF

2. Qu'est-ce qu'une sauvegarde hors ligne (à froid) ?

- A. Une copie de stockage déconnectée du réseau pour la protéger de la propagation des logiciels malveillants
- B. Une sauvegarde stockée sur le disque dur du serveur web principal
- C. Un cache temporaire des journaux du registre système
- D. Un outil d'administration servant à réinitialiser les mots de passe des utilisateurs

3. Comment les équipes de sécurité doivent-elles isoler les systèmes infectés lors d'une attaque par rançongiciel ?

- A. Débrancher immédiatement les câbles réseau et désactiver les interfaces sans fil
- B. Mettre à jour la base de signatures de l'antivirus
- C. Arrêter le serveur DNS principal
- D. Renommer les extensions des fichiers compromis

4. Pourquoi les agences de sécurité déconseillent-elles de payer les rançons exigées par les rançongiciels ?

- A. Payer encourage les attaquants et ne garantit pas la remise de la clé de déchiffrement
- B. Il annule automatiquement toutes les polices d'assurance de l'entreprise
- C. Il prévient automatiquement chaque client par e-mail
- D. Il corrompt les fichiers de sauvegarde restants du système

5. Qu'est-ce qu'un plan de reprise après sinistre (DRP) ?

- A. Un processus structuré pour rétablir les opérations et les données après la compromission d'un système
- B. Une configuration de pare-feu qui répertorie les ports réseau entrants
- C. Un schéma de base de données qui répertorie les privilèges d'administration des utilisateurs
- D. Un protocole d'authentification des e-mails qui rejette les domaines usurpés

Point de contrôle 2 : Défi Vrai ou Faux

6 Question 6

6. Les charges de rançongiciel peuvent facilement se propager aux sauvegardes en ligne connectées au réseau.

- ○ Vrai
- ○ Faux

7 Question 7

7. Payer la rançon en cryptomonnaie garantit que les fichiers seront bien déchiffrés.

- ○ Vrai
- ○ Faux

8 Question 8

8. Déconnecter du réseau les systèmes infectés aide à empêcher le rançongiciel de se propager aux systèmes voisins.

- ○ Vrai
- ○ Faux

9 Question 9

9. Les rançongiciels n'utilisent jamais la cryptographie symétrique pour chiffrer le stockage du système.

- ○ Vrai
- ○ Faux

10 Question 10

10. Tester régulièrement les procédures de restauration des données est un élément essentiel de la reprise après sinistre.

- ○ Vrai
- ○ Faux

Point de contrôle 3 : Insertion des termes clés

Lisez chaque phrase ci-dessous et complétez le blanc avec le terme correct de la banque de mots.

1. Bloquer l'accès aux fichiers locaux fait appel au _____ cryptographique.
2. Le code malveillant actif exécuté sur un système est la _____ .
3. Les copies de stockage déconnectées et hors site constituent une _____ sûre.
4. Empêcher la propagation d'un malware exige l' _____ réseau des terminaux.
5. Le paiement en cryptomonnaie exigé par les cybercriminels est la _____ .
6. La restauration des fichiers de données opérationnels relève de la _____ après sinistre.

BANQUE DE MOTS DE VOCABULAIRE

CHARGE UTILE CHEVAL DE TROIE CHIFFREMENT COPIE HORS LIGNE ISOLEMENT
RANÇON REPRISE SINISTRE

Écrivez vos réponses ici :

1.
2.
3.
4.
5.
6.

Point de contrôle 4 : Association de notions sur la sécurité

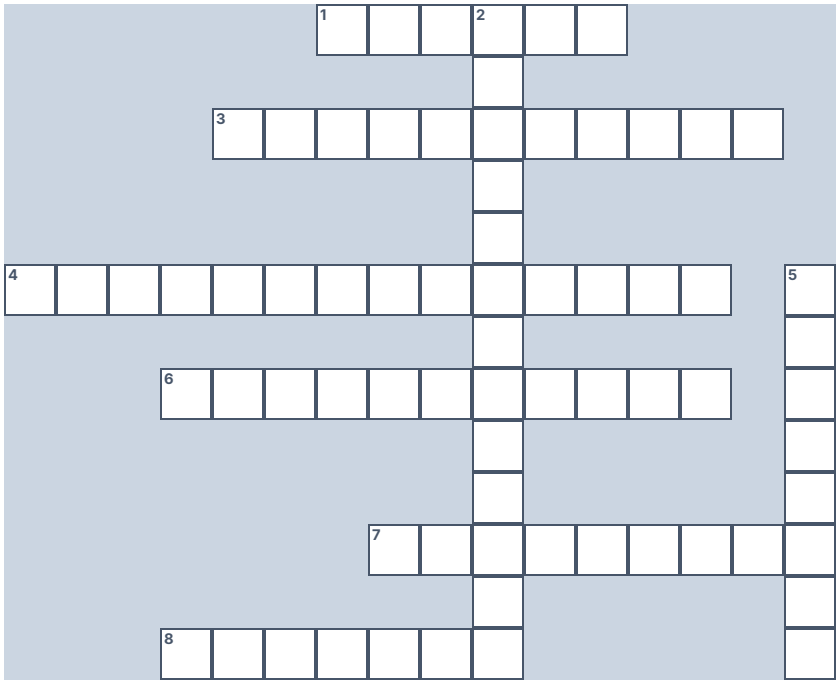
ASSOCIATION DE DÉFINITIONS

Associez chaque terme de vocabulaire à gauche à sa définition à droite en écrivant la lettre correspondante (A-H) dans la case à remplir.

☐	1. CHIFFREMENT	A	Déconnexion des systèmes réseau infectés.
☐	2. CHARGE UTILE	B	Fichier malveillant déguisé en fichier sain.
☐	3. SAUVEGARDE À FROID	C	Verrouiller des fichiers par la cryptographie.
☐	4. ISOLEMENT	D	Incident perturbant gravement le système.
☐	5. RANÇON	E	Exécution d'un logiciel malveillant.
☐	6. RÉCUPÉRATION	F	Copie hors ligne déconnectée.
☐	7. CATASTROPHE	G	Restauration d'une base de données à partir d'une sauvegarde.
☐	8. CHEVAL DE TROIE	H	Demande de paiement d'une clé cryptographique.

Point de contrôle 5 : Mots croisés

Résolvez la grille de mots croisés en tapant des lettres dans les cases blanches actives. Les numéros correspondent aux définitions ci-dessous.



HORIZONTALEMENT

1. Demande de paiement en échange de la clé cryptographique. (6)

3. Exécution d'un logiciel malveillant. (11)

4. Copie déconnectée, conservée hors réseau (sauvegarde à froid). (14)

6. Verrouillage cryptographique des fichiers. (11)

7. Déconnexion des systèmes infectés du réseau. (9)

8. Rétablissement de la base de données à partir d'une sauvegarde. (7)

VERTICALEMENT

2. Fichier malveillant déguisé en fichier sain. (13)

5. Événement de perturbation majeure du système. (8)

Point de contrôle 5, variante : Définitions de mots croisés accessibles

Les utilisateurs de lecteurs d'écran et de clavier peuvent saisir les réponses des mots croisés directement dans les champs de texte ci-dessous.

HORIZONTALEMENT

1 horizontal: Demande de paiement en échange de la clé cryptographique. (6 lettres):

3 horizontal: Exécution d'un logiciel malveillant. (11 lettres):

4 horizontal: Copie déconnectée, conservée hors réseau (sauvegarde à froid). (14 lettres):

6 horizontal: Verrouillage cryptographique des fichiers. (11 lettres):

7 horizontal: Déconnexion des systèmes infectés du réseau. (9 lettres):

8 horizontal: Rétablissement de la base de données à partir d'une sauvegarde. (7 lettres):

VERTICALEMENT

2 vertical: Fichier malveillant déguisé en fichier sain. (13 lettres):

5 vertical: Événement de perturbation majeure du système. (8 lettres):

Point de contrôle 6 : Mots cachés

Trouvez les 8 termes de vocabulaire clés cachés dans la grille ci-dessous. Les mots peuvent être horizontaux, verticaux ou en diagonale.

N C D H I B A C P R L P W T I

Y F Y S G X W H H F R T N U K

T R D T S L N E P L M S H K P

N H Y P L O W V R E P R I S E

E U N Y C Q Q A B A L P M B L

M I F N I N Y L B Z Z Y B N V

E X A M C F P D W Q Q X H E Y

R R C W L T N E M E L O S I F

F G H Z W C O T R J X X R K Z

F A N R Z R M R G S W G L W J

I C O P I E H O R S L I G N E

H B Y C C Y O I U Z O Z U T B

C H C H A R G E U T I L E V P

X C N M H P X Y Z X H O I O S

W E R T S I N I S G U V F W H

LISTE DE MOTS DE VOCABULAIRE

CHIFFREMENT CHARGEUTILE COPIEHORSLIGNE ISOLEMENT RANCON REPRISE SINISTRE CHEVALDETROIE

Point de contrôle 6, variante : Association de vocabulaire accessible

Associez chacun des 8 termes de vocabulaire de la grille de mots cachés à sa définition en écrivant la lettre (A-H) dans l'espace prévu.

TERMES DE VOCABULAIRE
A. CHIFFREMENT
B. CHARGEUTILE
C. COPIEHORSLIGNE
D. ISOLEMENT
E. RANCON
F. REPRISE
G. SINISTRE
H. CHEVALDETROIE

DÉFINITIONS ET CHAMPS D'ASSOCIATION
1. Copie déconnectée, conservée hors réseau (sauvegarde à froid).
2. Fichier malveillant déguisé en fichier sain.
3. Verrouillage cryptographique des fichiers.
4. Demande de paiement en échange de la clé cryptographique.
5. Déconnexion des systèmes infectés du réseau.
6. Événement de perturbation majeure du système.
7. Exécution d'un logiciel malveillant.
8. Rétablissement de la base de données à partir d'une sauvegarde.

Point de contrôle 7 : Défi des mots mélangés

Remettez les lettres ci-dessous dans l'ordre pour découvrir des notions et termes clés de la cybersécurité. Écrivez vos réponses dans les champs prévus.

1. FENHRMCEITF
2. EOHPONCGRE LISI
3. RNCNOA
4. IRETSSIN
5. IHTUAEGECLR
6. NLSEMIETO
7. RSIEERP
8. TEALOEECDHI RV

Activité bonus : Réflexion rapide

3 RÉPONSES PAR CATÉGORIE. LE PREMIER À REMPLIR SA LISTE GAGNE.

1	Informations que vous ne devriez jamais partager			
2	Appareils qui peuvent être piratés			
3	Raisons de ne pas payer de rançon			
4	Bonnes habitudes de sécurité à adopter dès aujourd'hui			
5	Outils de sécurité que vous connaissez			
6	Façons de protéger vos comptes			
7	Signes qu'un ordinateur est infecté			
8	Endroits où conserver une sauvegarde			
9	Fichiers que vous ne voulez jamais perdre			
10	Façons dont un rançongiciel se propage			
11	Choses à faire dans la première heure d'une attaque			
12	Personnes à contacter pendant une attaque			
13	Choses qu'un rançongiciel peut verrouiller			
14	Mots liés à la cybersécurité			
15	Organisations souvent ciblées			

Point de contrôle 8 : Études de cas sur la cybersécurité

Appliquez les notions apprises pour résoudre les scénarios réels ci-dessous.

ÉTUDE DE CAS 1 : CONFINEMENT D'UNE CHARGE DE RANÇONGICIEL EN ENTREPRISE



Scénario : le réseau local d'une entreprise a été compromis par un rançongiciel actif. Sur des serveurs de fichiers clés, des fichiers commencent à apparaître avec l'extension .locked.

Question de discussion : Détaillez les étapes de confinement et décrivez le protocole de récupération des données.

ÉTUDE DE CAS 2 : ÉVALUER DES ARCHITECTURES DE SAUVEGARDE HORS LIGNE



Scénario : Une entreprise veut concevoir une stratégie de sauvegarde des données qui réduise le risque de compromission des sauvegardes, même si le réseau local principal est entièrement pris en otage par un rançongiciel.

Question de discussion : concevez un système de coffre de stockage de sauvegardes hors ligne sécurisé.

Point de contrôle 9 : Déchiffrer le code

Un professionnel de la cybersécurité protège les ressources réseau contre les acteurs malveillants en ligne. Utilisez la clé de correspondance lettres-chiffres ci-dessous pour déchiffrer le message en écrivant les lettres correspondantes dans les cases vides.

CLÉ DE CHIFFREMENT LETTRE-CHIFFRE

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

18	5	19	20	1	21	18	5	26		22	15	19		4	15	14	14	5	5	19

4	5	16	21	9	19		21	14	5		3	15	16	9	5		1	

6	18	15	9	4

Message déchiffré :

ASTUCE : CHAQUE NOMBRE REPRÉSENTE LA POSITION DE LA LETTRE DANS L'ALPHABET (P. EX. 1 = A, 2 = B, 26 = Z).

Point de contrôle 10 : Questions fréquentes de base sur la cybersécurité (Partie A)

Passez en revue les questions et réponses courantes sur la réduction des menaces en ligne.

Q1: Qu'est-ce qu'un rançongiciel ?

Un rançongiciel est un logiciel malveillant conçu pour bloquer l'accès à des systèmes informatiques ou à des fichiers jusqu'au paiement d'une rançon.

Q2: Comment un rançongiciel se propage-t-il ?

Par des pièces jointes d'e-mails d'hameçonnage, des vulnérabilités logicielles non corrigées et des systèmes d'accès à distance compromis. [1]

Q3: Pourquoi le paiement est-il demandé en cryptomonnaie ?

Les cryptomonnaies comme le Bitcoin offrent un anonymat relatif, ce qui rend difficile le suivi des fonds par les forces de l'ordre.

Q4: L'antivirus bloque-t-il les rançongiciels ?

Oui, mais un antivirus fondé sur les signatures peut échouer face à des charges utiles de rançongiciels zero-day nouvellement créées.

Q5: Qu'est-ce qu'une sauvegarde isolée (air-gapped) ?

Une copie de sauvegarde sans aucune connexion physique ou logique avec le réseau principal, ce qui la protège contre la propagation.

Point de contrôle 10 : Questions fréquentes de base sur la cybersécurité (Partie B)

Passez en revue les questions et réponses courantes sur la réduction des menaces en ligne.

Q6: Qu'est-ce que la double extorsion ?

Lorsque les attaquants ne se contentent pas de chiffrer les fichiers, mais volent aussi des données sensibles et menacent de les divulguer publiquement en cas de non-paiement.

Q7: Qu'est-ce qu'un outil de déchiffrement (decryptor) ?

Un utilitaire logiciel contenant la clé cryptographique nécessaire pour remettre les fichiers verrouillés en clair.

Q8: Comment détecter tôt un rançongiciel ?

En surveillant les systèmes de fichiers pour détecter une activité soudaine et massive de modification et de renommage de fichiers.

Q9: Quel est le rôle de l'assurance ?

Une cyberassurance peut aider à couvrir les frais de rétablissement, mais les conditions de couverture et les règles sur le paiement des rançons varient selon les contrats.

Q10: Faut-il redémarrer un système infecté ?

Non, un redémarrage peut détruire les preuves en mémoire volatile ; isolez plutôt la machine du réseau. [1]

Point de contrôle 10 : Questions fréquentes avancées sur la sécurité (Partie C)

Découvrez les aspects techniques avancés des cadres de sécurité, de l'analyse des logiciels malveillants et de la conformité des données.

Q1: Comment un rançongiciel utilise-t-il le chiffrement asymétrique ?

Il utilise une clé publique intégrée au logiciel malveillant pour chiffrer les fichiers, la clé privée de l'attaquant étant nécessaire pour les déchiffrer.

Q2: Pourquoi le chiffrement symétrique est-il aussi utilisé ?

Le chiffrement symétrique (comme AES) est rapide et peut verrouiller d'immenses bases de données en quelques minutes, tandis que les clés asymétriques sécurisent la clé AES.

Q3: Qu'est-ce que la segmentation logique ?

Diviser les réseaux en zones isolées, ce qui empêche les logiciels malveillants de se propager latéralement des postes de travail vers les serveurs centraux.

Q4: Qu'est-ce que le stockage WORM ?

Support WORM (Write-Once, Read-Many, écriture unique et lectures multiples), qui empêche les données de sauvegarde d'être modifiées, écrasées ou supprimées par des charges utiles de rançongiciels.

Q5: Que sont les clichés instantanés (shadow copies) ?

Instantanés de sauvegarde locaux créés par Windows ; les rançongiciels les suppriment généralement en premier à l'aide d'outils d'administration.

Point de contrôle 10 : Questions fréquentes avancées sur la sécurité (Partie D)

Découvrez les aspects techniques avancés des cadres de sécurité, de l'analyse des logiciels malveillants et de la conformité des données.

Q6: Comment le vol d'identifiants permet-il les attaques par rançongiciel ?

Des attaquants achètent des identifiants d'administrateur ayant fuité pour se connecter via le bureau à distance, puis exécutent manuellement un rançongiciel sur tout le réseau.

Q7: Qu'est-ce qu'un test de restauration à blanc ?

Restauration régulière des bases de données de sauvegarde dans des environnements de test isolés pour vérifier que la vitesse de restauration et l'intégrité des données respectent les indicateurs de reprise après sinistre.

Q8: Comment la détection sur les terminaux (EDR) bloque-t-elle les rançongiciels ?

En analysant le comportement des processus (par exemple un chiffrement rapide) et en suspendant rapidement l'application malveillante.

Q9: Qu'est-ce que le modèle du rançongiciel en tant que service (RaaS) ?

Un modèle de franchise dans lequel les développeurs de logiciels malveillants louent des générateurs de rançongiciels à des affiliés en échange d'un pourcentage des rançons.

Q10: Comment un RDP non corrigé déclenche-t-il un rançongiciel ?

Les passerelles Remote Desktop Protocol exposées et non corrigées permettent aux attaquants de forcer les identifiants par force brute et de lancer manuellement des logiciels malveillants.

Partie 11 : 10 faits et enseignements concrets sur la cybersécurité

Découvrez des faits concrets sur les failles de sécurité, les mécanismes de défense et les normes de conformité.

1. APERÇU SÉCURITÉ

Les auteurs de rançongiciels utilisent souvent des outils comme vssadmin.exe pour supprimer les clichés instantanés de Windows et empêcher les restaurations locales. [1]

2. APERÇU SÉCURITÉ

Les clés symétriques AES-256 servent généralement à chiffrer le contenu des fichiers, qui est ensuite verrouillé à l'aide de clés publiques RSA.

3. APERÇU SÉCURITÉ

Se remettre d'une attaque par rançongiciel réussie peut prendre des semaines, d'où l'importance de sauvegardes hors ligne testées.

4. APERÇU SÉCURITÉ

Le FBI ne soutient pas le paiement d'une rançon et avertit que payer ne garantit pas que vous récupérerez vos données. [2]

5. APERÇU SÉCURITÉ

Les plans de reprise après sinistre (DRP) doivent définir un objectif de délai de reprise (RTO) et un objectif de point de reprise (RPO).

6. APERÇU SÉCURITÉ

Le FBI recommande des sauvegardes chiffrées et immuables, c'est-à-dire qu'elles ne peuvent être ni modifiées ni supprimées. [3]

7. ZOOM SUR LA SÉCURITÉ

Les développeurs de rançongiciels utilisent des techniques d'obfuscation avancées pour contourner les antivirus traditionnels fondés sur les signatures.

8. ZOOM SUR LA SÉCURITÉ

La segmentation du réseau limite les déplacements latéraux, ce qui aide à empêcher un rançongiciel de se propager au-delà du premier hôte infecté. [3]

9. ZOOM SUR LA SÉCURITÉ

Les services d'accès à distance exposés et mal sécurisés, comme le protocole Remote Desktop (RDP), sont un point d'entrée courant des rançongiciels. [1]

10. APERÇU SÉCURITÉ

La CISA conseille de conserver des sauvegardes chiffrées hors ligne, car de nombreuses variantes de rançongiciels recherchent et suppriment les sauvegardes accessibles. [1]

Références techniques et sources

Le guide d'étude et les énigmes interactives sont tirés des normes internationales du NIST, de l'OWASP et de conformité en matière de protection des données.

RÉFÉRENCES ACADÉMIQUES ET PROFESSIONNELLES

[1] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[2] FBI Internet Crime Complaint Center. (n.d.). Ransomware.
https://www.ic3.gov/CrimeInfo/Ransomware

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

Corrigé : Point de contrôle 1 – Choix multiple

1 Question 1

Bonne réponse : A

NOTE PÉDAGOGIQUE

Quel est le mécanisme principal d'une attaque par rançongiciel ? → Chiffrement cryptographique des fichiers de l'utilisateur pour bloquer l'accès au système

2 Question 2

Bonne réponse : A

NOTE PÉDAGOGIQUE

Qu'est-ce qu'une sauvegarde hors ligne (à froid) ? → Une copie de stockage déconnectée du réseau pour la protéger de la propagation des logiciels malveillants

3 Question 3

Bonne réponse : A

NOTE PÉDAGOGIQUE

Comment les équipes de sécurité doivent-elles isoler les systèmes infectés lors d'une attaque par rançongiciel ? → Débrancher immédiatement les câbles réseau et désactiver les interfaces sans fil

4 Question 4

Bonne réponse : A

NOTE PÉDAGOGIQUE

Pourquoi les agences de sécurité déconseillent-elles de payer les rançons exigées par les rançongiciels ? → Payer encourage les attaquants et ne garantit pas la remise de la clé de déchiffrement

5 Question 5

Bonne réponse : A

NOTE PÉDAGOGIQUE

Qu'est-ce qu'un plan de reprise après sinistre (DRP) ? → Un processus structuré pour rétablir les opérations et les données après la compromission d'un système

Corrigé : Point de contrôle 2 – Vrai ou faux

6 Question 6

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Les charges de rançongiciel peuvent facilement se propager aux sauvegardes en ligne connectées au réseau.

7 Question 7

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

Faux : le FBI avertit que payer ne garantit pas que vous récupériez vos données. [2]

8 Question 8

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Vrai : la CISA conseille de débrancher les hôtes infectés ou de mettre le réseau hors ligne pour contenir la propagation.

9 Question 9

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

Faux : les rançongiciels chiffrent généralement les fichiers avec des algorithmes symétriques rapides comme AES.

10 Question 10

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Tester régulièrement les procédures de restauration des données est un élément essentiel de la reprise après sinistre.

Corrigés du vocabulaire et grille d'évaluation

Grille de notation de l'enseignant : attribuez 1 point par association correcte (8 points au total) et par terme en contexte (6 points au total).

POINT DE CONTRÔLE 4 : CORRIGÉ DE L'ASSOCIATION DE NOTIONS

C 1. CHIFFREMENT	E 2. CHARGE UTILE	F 3. SAUVEGARDE À FROID	A 4. ISOLEMENT
H 5. RANÇON	G 6. RÉCUPÉRATION	D 7. CATASTROPHE	B 8. CHEVAL DE TROIE

POINT DE CONTRÔLE 3 : CORRIGÉ DES TERMES CLÉS

1 CHIFFREMENT	2 CHARGE UTILE	3 COPIE HORS LIGNE	4 ISOLEMENT
5 RANÇON	6 REPRISE		

POINT DE CONTRÔLE 6, VARIANTE : CORRIGÉ DE L'ASSOCIATION DE MOTS

1 C – COPIEHORSLIGNE	2 H – CHEVALDETROIE	3 A – CHIFFREMENT	4 E – RANCON
5 D – ISOLEMENT	6 G – SINISTRE	7 B – CHARGEUTILE	8 F – REPRISE

NOTES DE DISCUSSION POUR LES ENSEIGNANTS

Termes clés :
Vérifiez que les élèves savent expliquer CHIFFREMENT, CHARGE UTILE et SAUVEGARDE À FROID avec leurs propres mots et donner un exemple pour chacun.

Études de cas :
Demandez aux élèves de justifier leurs recommandations par des faits tirés de la fiche plutôt que par des suppositions.

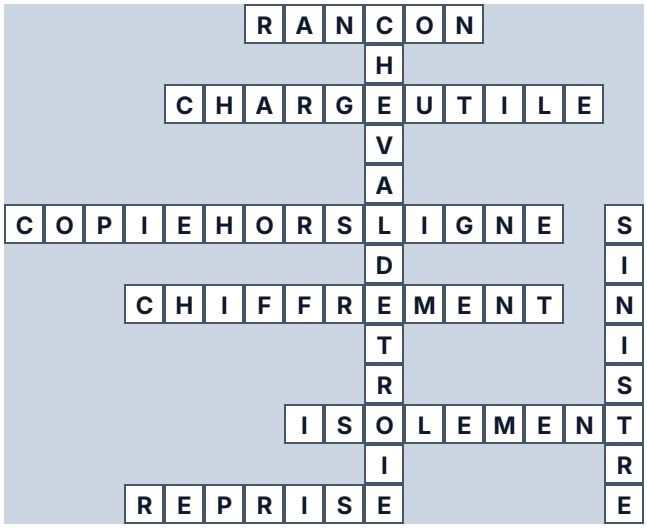
Évaluation des sources :
Faites vérifier au moins une affirmation à l'aide des sources de la fiche et discutez des raisons pour lesquelles les chiffres, les prix et les règles peuvent évoluer avec le temps.

Corrigés des jeux et notes pour l'enseignant

SOLUTION DES MOTS CACHÉS

N	C	D	H	I	B	A	C	P	R	L	P	W	T	I
Y	F	Y	S	G	X	W	H	H	F	R	T	N	U	K
T	R	D	T	S	L	N	E	P	L	M	S	H	K	P
N	H	Y	P	L	O	W	V	R	E	P	R	I	S	E
E	U	N	Y	C	Q	Q	A	B	A	L	P	M	B	L
M	I	F	N	I	N	Y	L	B	Z	Z	Y	B	N	V
E	X	A	M	C	F	P	D	W	Q	Q	X	H	E	Y
R	R	C	W	L	T	N	E	M	E	L	O	S	I	F
F	G	H	Z	W	C	O	T	R	J	X	X	R	K	Z
F	A	N	R	Z	R	M	R	G	S	W	G	L	W	J
I	C	O	P	I	E	H	O	R	S	L	I	G	N	E
H	B	Y	C	C	Y	O	I	U	Z	O	Z	U	T	B
C	H	C	H	A	R	G	E	U	T	I	L	E	V	P
X	C	N	M	H	P	X	Y	Z	X	H	O	I	O	S
W	E	R	T	S	I	N	I	S	G	U	V	F	W	H

SOLUTION DES MOTS CROISÉS



GUIDE DE L'ENSEIGNANT : SOLUTIONS DES MOTS CROISÉS

HORIZONTALEMENT

1 horizontal: RANCON Demande de paiement en échange de la clé cryptographique. (6 lettres)

3 horizontal: CHARGEUTILE Exécution d'un logiciel malveillant. (11 lettres)

4 horizontal: COPIEHORSLIGNE Copie déconnectée, conservée hors réseau (sauvegarde à froid). (14 lettres)

6 horizontal: CHIFFREMENT Verrouillage cryptographique des fichiers. (11 lettres)

7 horizontal: ISOLEMENT Déconnexion des systèmes infectés du réseau. (9 lettres)

8 horizontal: REPRISE Rétablissement de la base de données à partir d'une sauvegarde. (7 lettres)

VERTICALEMENT

2 vertical: CHEVALDETROIE Fichier malveillant déguisé en fichier sain. (13 lettres)

5 vertical: SINISTRE Événement de perturbation majeure du système. (8 lettres)

Corrigé des mots mélangés et du code

Corrigé de l'activité de remise en ordre des lettres du vocabulaire et du défi du code secret.

CORRIGÉ DES MOTS MÉLANGÉS

1. FENHRMCEITF — **CHIFFREMENT**
2. EOHPONCGRELISI — **COPIEHORSLIGNE**
3. RNCNOA — **RANCON**
4. IRETSSIN — **SINISTRE**
5. IHTUAEGECLR — **CHARGEUTILE**
6. NLSEMIETO — **ISOLEMENT**
7. RSIEERP — **REPRISE**
8. TEALOEECDHIRV — **CHEVALDETROIE**

CORRIGÉ DU DÉFI DU CODE SECRET

"RESTAUREZ VOS DONNEES DEPUIS UNE COPIE A FROID"

Corrigé des études de cas

A Étude de cas 1 : Confinement d'une charge de rançongiciel en entreprise

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : le réseau local d'une entreprise a été compromis par un rançongiciel actif. Des serveurs de fichiers essentiels commencent à afficher des fichiers avec l'extension .locked.
- Stratégie et solution recommandées : déconnecter tous les serveurs touchés du réseau local. Mettre fin aux sessions d'administration actives. Restaurer les fichiers non compromis à partir d'un système de sauvegarde hors ligne sécurisé et verrouillé en écriture.

B Étude de cas 2 : Évaluer des architectures de sauvegarde hors ligne

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : une entreprise veut concevoir une stratégie de sauvegarde des données qui réduit le risque de compromission des sauvegardes, même si le réseau local principal est entièrement pris en otage par un rançongiciel.
- Stratégie et solution recommandées : mettez en place un stockage WORM (write-once-read-many, écriture unique et lectures multiples). Créez une isolation logique (air gap) en déconnectant le système de sauvegarde de tous les réseaux, et imposez une rotation quotidienne des supports physiques.