Nom : _____ Date : _____ Note : _____

Logiciels antivirus et terminaux Guide de protection

Détection par signature, heuristique, surveillance du comportement, bac à sable (sandboxing), mises à jour

LOGICIELS ANTIVIRUS : 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 logiciels antivirus et la protection des terminaux. Vous étudierez les bases de signatures, les analyseurs heuristiques, la surveillance comportementale, les fichiers virtuels en bac à sable et l'atténuation des faux positifs.

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/antivirus/

Votre parcours d'apprentissage : stratégie antivirus

- Distinguer la détection des logiciels malveillants par signature de la détection heuristique.
- Comprendre la surveillance comportementale et les protocoles d'isolation en bac à sable.
- Évaluer l'impact de l'analyse en temps réel sur les performances du système et sur les terminaux.
- Atténuer les faux positifs grâce à la vérification des certificats numériques.
- Gérer la distribution quotidienne des mises à jour de définitions sur les terminaux de l'entreprise.

GUIDE ANTIVIRUS : 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 sécurité antivirus des terminaux. Terminez par l'activité bonus Réflexion rapide.

PROTECTION ANTIVIRUS ET ANALYSE PAR SIGNATURES (INTRODUCTION)

Les logiciels antivirus protègent les terminaux en identifiant, en mettant en quarantaine et en supprimant les logiciels malveillants. Les systèmes modernes combinent des bases de signatures (correspondance avec les empreintes de menaces connues), des méthodes heuristiques (analyse de la structure des fichiers) et la surveillance du comportement pour détecter les exploits zero-day.

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

Point de contrôle 1 : Défi QCM

1. Quelle est une limite de la détection par signatures ?

- A. Il ne peut pas identifier les logiciels malveillants inconnus ou modifiés
- B. Il génère un taux élevé de faux positifs
- C. Il nécessite une puissance de calcul processeur élevée
- D. Il ne fonctionne que lorsqu'on est connecté à Internet

2. Comment les analyseurs heuristiques détectent-ils les nouvelles variantes de logiciels malveillants ?

- A. En repérant des schémas et des structures de code suspects
- B. En comparant les empreintes des fichiers à une base de données de menaces
- C. En supprimant automatiquement tous les exécutables non signés
- D. En téléversant chaque fichier dans un dossier cloud public

3. À quoi sert l'exécution en sandbox d'un antivirus ?

- A. Isoler et analyser les fichiers dans un coffre virtuel sécurisé
- B. Accélérer le transfert de sauvegarde du système de fichiers local
- C. Installer les correctifs de sécurité du système d'exploitation local
- D. Compresser de gros fichiers de documents pour gagner de l'espace

4. Quelle méthode de détection signale les comportements malveillants en temps réel ?

- A. Analyse comportementale qui surveille les actions des logiciels
- B. Inspection des journaux historiques effectuée pendant la nuit
- C. Signalement manuel des applications lentes par l'utilisateur
- D. Vérifications manuelles hebdomadaires des programmes installés

5. Pourquoi les mises à jour régulières des définitions sont-elles essentielles pour les analyseurs ?

- A. Alimenter la base de données des moteurs de signatures en identifiants de menaces
- B. Augmenter la fréquence d'horloge du processeur pendant les opérations
- C. Pour modifier les durées de mise en cache des serveurs de noms DNS mondiaux
- D. Pour autoriser les paramètres de cookies du navigateur web

Point de contrôle 2 : Défi Vrai ou Faux

6 Question vrai/faux 6

6. La détection par signature compare les empreintes cryptographiques des fichiers aux listes d'une base de données.

- ◯ Vrai
- ◯ Faux

7 Question vrai/faux 7

7. Les analyseurs heuristiques peuvent déclencher de fausses alertes sur des fichiers sains.

- ◯ Vrai
- ◯ Faux

8 Question vrai/faux 8

8. Un bac à sable (sandbox) permet aux logiciels malveillants d'accéder sans limite aux fichiers du réseau.

- ◯ Vrai
- ◯ Faux

9 Question vrai/faux 9

9. L'analyse comportementale bloque les fichiers lorsqu'ils présentent des actions malveillantes.

- ◯ Vrai
- ◯ Faux

10 Question vrai/faux 10

10. Un antivirus standard bloque complètement toutes les attaques zero-day.

- ◯ 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. Un analyseur traditionnel s'appuie sur la détection par _____ pour identifier les logiciels malveillants connus.

2. L'examen des schémas de code des fichiers est appelé analyse _____ .

3. Les outils de protection isolent les fichiers suspects dans un environnement de type _____ .

4. La surveillance en temps réel observe le _____ des programmes pour repérer les activités suspectes.

5. Les analyseurs téléchargent chaque jour des _____ de leur base de données pour reconnaître les nouvelles menaces.

6. Des programmes sûrs signalés comme malveillants déclenchent des alertes de type _____ .

BANQUE DE MOTS DE VOCABULAIRE

ANTIVIRUS BAC À SABLE COMPORTEMENT FAUX POSITIF HEURISTIQUE MISES À JOUR QUARANTAINE SIGNATURE

Écrivez vos réponses ici :

1. **2.**

3. **4.**

5. **6.**

Point de contrôle 4 : Association de notions sur la sécurité

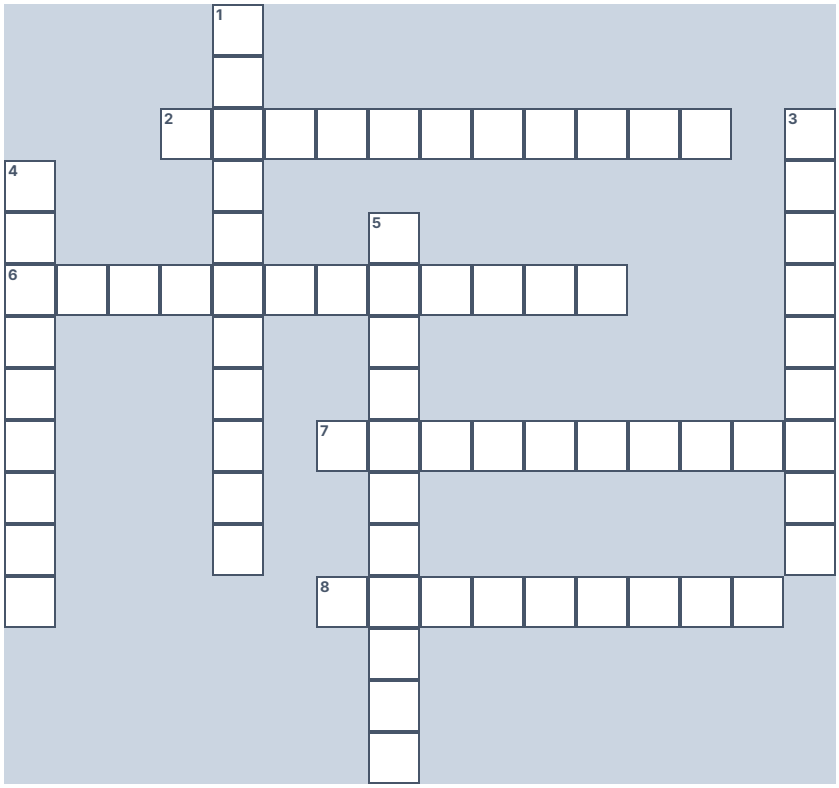
ASSOCIATION DE DÉFINITIONS

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. Signature de hachage	A	Isoler les fichiers suspects pour éviter d'exposer le système local.
☐	2. Heuristique du code	B	Suite logicielle qui analyse et protège les terminaux contre les exploits.
☐	3. Bac à sable de fichiers	C	Surveiller les actions des logiciels en cours d'exécution pour repérer des comportements malveillants.
☐	4. Analyse comportementale	D	Empreinte cryptographique unique, enregistrée dans une base de données, utilisée pour identifier des menaces connues.
☐	5. Mises à jour quotidiennes	E	Environnement de test virtuel sécurisé permettant d'exécuter du code non fiable en toute sécurité.
☐	6. Faux positif	F	Téléchargements réguliers de définitions alimentant la base de données des menaces.
☐	7. Isolation des menaces	G	Analyse à base de règles signalant les fichiers dont la structure de code est suspecte.
☐	8. Outil antivirus	H	Alerte de sécurité qui classe à tort un logiciel sûr comme malveillant.

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

2. Confinement des fichiers suspects pour éviter d'exposer le système local (11)

6. Ce que l'on surveille dans les actions des logiciels en cours d'exécution pour repérer des schémas d'opérations malveillantes (12)

7. Téléchargements réguliers de définitions qui alimentent la base de données des menaces (10)

8. Empreinte cryptographique unique, enregistrée dans une base de données, servant à identifier les menaces connues (9)

VERTICALEMENT

1. Alerte de sécurité qui classe à tort un logiciel sûr comme malveillant (11)

3. Suite logicielle qui analyse et protège les terminaux contre les exploits (9)

4. Environnement de test virtuel sécurisé qui exécute sans danger du code non fiable (9)

5. Analyse fondée sur des règles qui signale les fichiers dont la structure de code est suspecte (11)

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. DÉFINITIONS HORIZONTALES DÉFINITIONS VERTICALES

HORIZONTALEMENT

2 horizontal: Confinement des fichiers suspects pour éviter d'exposer le système local (11 lettres):

6 horizontal: Ce que l'on surveille dans les actions des logiciels en cours d'exécution pour repérer des schémas d'opérations malveillantes (12 lettres):

7 horizontal: Téléchargements réguliers de définitions qui alimentent la base de données des menaces (10 lettres):

8 horizontal: Empreinte cryptographique unique, enregistrée dans une base de données, servant à identifier les menaces connues (9 lettres):

VERTICALEMENT

1 vertical: Alerte de sécurité qui classe à tort un logiciel sûr comme malveillant (11 lettres):

3 vertical: Suite logicielle qui analyse et protège les terminaux contre les exploits (9 lettres):

4 vertical: Environnement de test virtuel sécurisé qui exécute sans danger du code non fiable (9 lettres):

5 vertical: Analyse fondée sur des règles qui signale les fichiers dont la structure de code est suspecte (11 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.

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

LISTE DE MOTS DE VOCABULAIRE

SIGNATURE HEURISTIQUE BACASABLE COMPORTEMENT MISESAJOUR
FAUXPOSITIF QUARANTAINE ANTIVIRUS

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. SIGNATURE
B. HEURISTIQUE
C. BACASABLE
D. COMPORTEMENT
E. MISESAJOUR
F. FAUXPOSITIF
G. QUARANTAINE
H. ANTIVIRUS

	DÉFINITIONS ET CHAMPS D'ASSOCIATION
	1. Ce que l'on surveille dans les actions des logiciels en cours d'exécution pour repérer des schémas d'opérations malveillantes.
	2. Suite logicielle qui analyse et protège les terminaux contre les exploits.
	3. Téléchargements réguliers de définitions qui alimentent la base de données des menaces.
	4. Analyse fondée sur des règles qui signale les fichiers dont la structure de code est suspecte.
	5. Confinement des fichiers suspects pour éviter d'exposer le système local.
	6. Empreinte cryptographique unique, enregistrée dans une base de données, servant à identifier les menaces connues.
	7. Environnement de test virtuel sécurisé qui exécute sans danger du code non fiable.
	8. Alerte de sécurité qui classe à tort un logiciel sûr comme malveillant.

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. TANISUREG
2. EBLAAABSC
3. MAUJISREOS
4. TNENAAIAQUR
5. QEITUEISHUR
6. TOMERNECOTMP
7. IPFASFTIUOX
8. SVUAINIRT

Activité bonus : Réflexion rapide

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

1	Raisons de mettre à jour les logiciels			
2	Personnes à qui demander de l'aide informatique			
3	Choses à faire quand l'antivirus détecte quelque chose			
4	Signes d'un virus informatique			
5	Choses mises en quarantaine			
6	Endroits où se cachent les virus			
7	Informations que vous ne devriez jamais partager			
8	Types de logiciels malveillants			
9	Outils de sécurité que vous connaissez			
10	Choses qu'un antivirus analyse			
11	Choses que vous sauvegardez			
12	Appareils qui peuvent être piratés			
13	Logiciels antivirus que vous connaissez			
14	Raisons des fausses alertes			
15	Bonnes habitudes de sécurité à adopter dès aujourd'hui			

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 : ANALYSE PAR SIGNATURE OU HEURISTIQUE



Scénario : Un employé télécharge un utilitaire personnalisé développé en interne par une autre équipe. Le scanner à signatures le laisse passer, mais le scanner heuristique le signale comme suspect.

Question de discussion : Expliquez pourquoi cela s'est produit et comment vérifier si le fichier est sûr.

ÉTUDE DE CAS 2 : GÉRER LES FAUX POSITIFS



Scénario : Un développeur compile son application. L'antivirus du système signale le nouvel exécutable comme un logiciel malveillant et le met en quarantaine.

Question de discussion : Exposez les risques de la mise en liste blanche et décrivez la bonne façon de résoudre le problème.

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

4	5	20	5	3	20	5	26		12	5	19		14	15	21	22	5	1	21	24

13	1	12	23	1	18	5	19		16	1	18

8	5	21	18	9	19	20	9	17	21	5

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: Comment un antivirus identifie-t-il les logiciels malveillants ?

Il identifie les logiciels malveillants par comparaison avec une base de signatures, par analyse heuristique de la structure du code et par surveillance comportementale en temps réel.

Q2: Qu'est-ce que la détection par signatures ?

Il s'agit d'une méthode d'analyse qui compare les empreintes cryptographiques (hachages) des fichiers à des listes de menaces connues.

Q3: Qu'est-ce qu'un analyseur heuristique ?

L'heuristique analyse la structure et les instructions du code d'un fichier, en signalant les schémas suspects courants dans les variantes de logiciels malveillants.

Q4: Que signifie la mise en quarantaine d'un fichier ?

L'antivirus déplace le fichier dans un dossier sécurisé et isolé, empêchant son exécution pour protéger le système d'exploitation.

Q5: Qu'est-ce qu'un faux positif d'antivirus ?

Il s'agit d'une erreur par laquelle un logiciel légitime et sûr est signalé à tort comme malveillant par les algorithmes d'analyse.

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: Comment la surveillance comportementale protège-t-elle les systèmes ?

Il surveille les logiciels en cours d'exécution en temps réel et bloque les processus qui tentent des modifications suspectes, comme l'injection de code.

Q7: Pourquoi les tests en sandbox sont-ils importants ?

Le sandboxing exécute les fichiers non fiables dans une machine virtuelle isolée, ce qui permet d'observer leurs actions en toute sécurité sans exposer le système.

Q8: À quelle fréquence les définitions antivirus doivent-elles être mises à jour ?

Les analyseurs doivent mettre à jour leurs définitions chaque jour ou chaque heure pour reconnaître les nouvelles souches de logiciels malveillants.

Q9: Quelle est la différence entre un antivirus et un EDR ?

L'antivirus se concentre sur l'analyse des fichiers, tandis que l'EDR (Endpoint Detection and Response) assure le suivi et le confinement des menaces à l'échelle du réseau.

Q10: Puis-je faire tourner deux antivirus en même temps ?

Non. Faire tourner deux analyseurs actifs provoque des conflits système, ralentit les performances et peut bloquer leurs opérations mutuelles.

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 les règles heuristiques réduisent-elles le contournement des menaces ?

L'heuristique analyse des schémas de menace généraux plutôt que des signatures précises, ce qui permet de détecter des variantes modifiées de familles de logiciels malveillants connues.

Q2: Qu'est-ce qu'un virus polymorphe ?

Il s'agit d'un logiciel malveillant qui modifie la structure de son fichier et sa routine de déchiffrement à chaque exécution, ce qui rend inefficaces les analyses par signature.

Q3: Comment les sandbox détectent-elles l'évasion de machine virtuelle ?

Les bacs à sable modernes simulent des clics de souris et la durée de fonctionnement du système, ce qui trompe les logiciels malveillants conçus pour se cacher dans les machines virtuelles.

Q4: Quels sont les formats de téléchargement des mises à jour de signatures ?

Les mises à jour sont généralement de légers fichiers de différences binaires incrémentielles, ce qui réduit la consommation de bande passante du client.

Q5: Comment les agents de terminal gèrent-ils les analyses locales ?

Les agents effectuent des vérifications légères en arrière-plan et confient les recherches approfondies d'empreintes cryptographiques à des bases de données de menaces dans le cloud.

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: Qu'est-ce que l'analyse de détection des rootkits ?

Il analyse les tables mémoire du noyau, en contournant les API de l'OS que les rootkits détournent pour cacher leurs threads actifs.

Q7: Comment l'analyse comportementale bloque-t-elle les rançongiciels ?

Il détecte les boucles automatisées de chiffrement massif de fichiers et met fin au processus hôte avant que les bases de données du système ne soient verrouillées.

Q8: Qu'est-ce que la vérification des certificats de signature de code ?

Les analyseurs vérifient les signatures numériques du code auprès d'autorités de certification racines de confiance, ce qui valide l'identité du développeur du logiciel.

Q9: Quel est l'impact des packers sur les moteurs d'analyse ?

Les packers compressent ou chiffrent les charges utiles des logiciels malveillants. Les analyseurs doivent décompresser le fichier en mémoire avant de comparer les signatures.

Q10: Comment les outils EDR automatisent-ils l'isolement ?

Les agents EDR mettent en quarantaine les terminaux compromis au niveau du réseau, ce qui bloque les déplacements latéraux tout en laissant l'accès aux analystes.

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 bases de signatures stockent les empreintes (hachages) de logiciels malveillants connus, de sorte que les fichiers tout nouveaux ou modifiés passent inaperçus jusqu'à la mise à jour des définitions.

2. APERÇU SÉCURITÉ

Les moteurs heuristiques peuvent signaler certaines nouvelles variantes de logiciels malveillants avant l'existence de signatures, au prix de davantage de faux positifs.

3. APERÇU SÉCURITÉ

Les fausses alertes coûtent du temps aux équipes informatiques, qui doivent vérifier et restaurer les fichiers mis en quarantaine à tort.

4. APERÇU SÉCURITÉ

Un logiciel malveillant polymorphe modifie son code à chaque copie ; les défenseurs associent donc les signatures à des contrôles heuristiques et comportementaux.

6. APERÇU SÉCURITÉ

Les auteurs de logiciels malveillants écrivent du code sur mesure qui vérifie la présence d'un bac à sable et retarde l'exécution pour déjouer les minuteries.

5. APERÇU SÉCURITÉ

Les moteurs antivirus dans le cloud comparent quasiment en temps réel les empreintes des fichiers suspects à de vastes bases de données de menaces en ligne.

7. ZOOM SUR LA SÉCURITÉ

Les éditeurs envoient régulièrement des mises à jour des définitions aux terminaux pour que les analyseurs reconnaissent les menaces nouvellement confirmées.

8. ZOOM SUR LA SÉCURITÉ

Les moniteurs comportementaux anti-rançongiciel ciblent des appels d'API Win32 précis associés au chiffrement de fichiers et à la suppression des clichés instantanés.

9. ZOOM SUR LA SÉCURITÉ

Des signatures de code valides peuvent réduire le risque de faux positifs, mais les fichiers signés sont tout de même analysés, car un logiciel malveillant peut lui aussi être signé.

10. APERÇU SÉCURITÉ

Les rootkits modifient les structures du noyau du système, ce qui exige des analyseurs spécialisés au démarrage pour les détecter et les supprimer.

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 UNIVERSITAIRES ET PROFESSIONNELLES

RÉFÉRENCES ACADÉMIQUES ET PROFESSIONNELLES

[1] NIST. (2013). SP 800-83 Rev. 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops.

https://csrc.nist.gov/pubs/sp/800/83/r1/final

[2] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[3] CISA. (2023). #StopRansomware Guide.

https://www.cisa.gov/stopransomware/ransomware-guide

[4] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[5] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.

https://csrc.nist.gov/pubs/sp/800/61/r3/final

Corrigé : Point de contrôle 1 – Choix multiple

1 Question 1 — SIGNATURES — Bonne réponse : A

NOTE PÉDAGOGIQUE

L'analyse par signature s'appuie sur des empreintes connues dans une base de données et ne détecte pas les logiciels malveillants inconnus ou modifiés. Source : OWASP Secure Configuration.

2 Question 2 — HEURISTIQUE — Bonne réponse : A

NOTE PÉDAGOGIQUE

L'analyse heuristique examine la structure et les commandes du code pour repérer les caractéristiques suspectes de nouvelles variantes de menaces. Source : Center for Internet Security (CIS).

3 Question 3 — SANDBOXING (MISE EN BAC À SABLE) — Bonne réponse : A

NOTE PÉDAGOGIQUE

Un bac à sable exécute les fichiers suspects dans une machine virtuelle isolée pour observer leur comportement en toute sécurité. Source : NIST Digital Identity.

4 Question 4 — COMPORTEMENTAL — Bonne réponse : A

NOTE PÉDAGOGIQUE

L'analyse comportementale surveille en temps réel les programmes en cours d'exécution pour bloquer les modifications non autorisées du système. Source : Center for Internet Security (CIS).

5 Question 5 — MISES À JOUR — Bonne réponse : A

NOTE PÉDAGOGIQUE

Les analyseurs téléchargent chaque jour des mises à jour incrémentielles de définitions pour rester à jour face à l'évolution des menaces. Source : OWASP Secure Configuration.

Corrigé : Point de contrôle 2 – Vrai ou faux

6 Question 6

SIGNATURES

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Les outils par signature calculent des empreintes cryptographiques et les comparent à une base de données d'empreintes de menaces connues. Source : OWASP Secure Configuration.

7 Question 7

HEURISTIQUE

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

Les moteurs heuristiques appliquent des règles qui peuvent signaler comme suspects des fichiers légitimes et sûrs. Source : Center for Internet Security (CIS).

8 Question 8

SANDBOXING (MISE EN BAC À SABLE)

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

Un bac à sable exécute le code dans un conteneur virtuel et bloque strictement l'accès aux partages réseau. Source : NIST Digital Identity.

9 Question 9

COMPORTEMENTAL

Bonne réponse : Vrai

NOTE PÉDAGOGIQUE

La surveillance en temps réel signale les processus en cours qui tentent des écritures illicites ou le verrouillage de fichiers. Source : Center for Internet Security (CIS).

10 Question 10

Bonne réponse : Faux

NOTE PÉDAGOGIQUE

Aucun antivirus n'arrête toutes les attaques zero-day ; des menaces inconnues peuvent échapper aux signatures et aux heuristiques.

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

D 1. Signature de hachage	G 2. Heuristique du code	E 3. Bac à sable de fichiers	C 4. Analyse comportementale
F 5. Mises à jour quotidiennes	H 6. Faux positif	A 7. Isolation des menaces	B 8. Outil antivirus

POINT DE CONTRÔLE 3 : CORRIGÉ DES TERMES CLÉS

1 SIGNATURE	2 HEURISTIQUE	3 BAC À SABLE	4 COMPORTEMENT
5 MISES À JOUR	6 FAUX POSITIF		

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

1 D – COMPORTEMENT	2 H – ANTIVIRUS	3 E – MISESAJOUR	4 B – HEURISTIQUE
5 G – QUARANTAINE	6 A – SIGNATURE	7 C – BACASABLE	8 F – FAUXPOSITIF

NOTES DE DISCUSSION POUR LES ENSEIGNANTS

Termes clés :
Vérifiez que les élèves savent expliquer Signature de hachage, Heuristique du code et Bac à sable de fichiers 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.

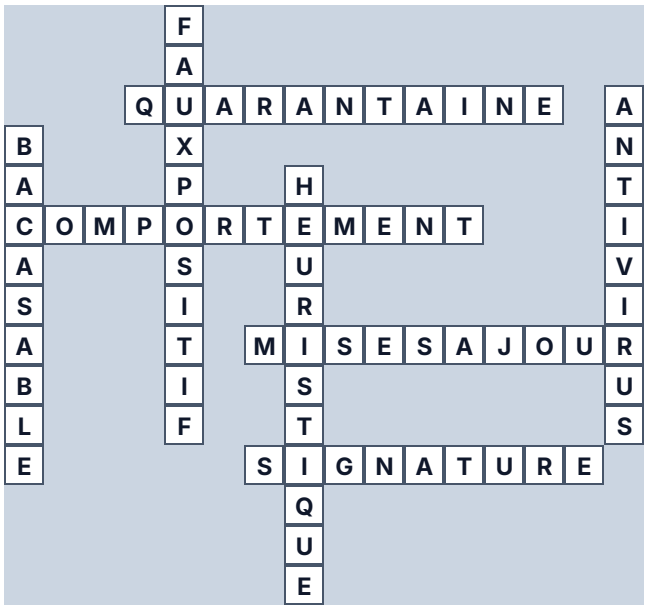
Évaluation des sources :
Faites vérifier au moins une affirmation à l'aide des sources de la fiche et discutez des raisons pour lesquelles les chiffres, les prix et les règles peuvent évoluer avec le temps.

Corrigés des jeux et notes pour l'enseignant

SOLUTION DES MOTS CACHÉS

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

SOLUTION DES MOTS CROISÉS



HORIZONTALEMENT

2 horizontal: QUARANTAINE Confinement des fichiers suspects pour éviter d'exposer le système local (11 lettres)

6 horizontal: COMPORTEMENT Ce que l'on surveille dans les actions des logiciels en cours d'exécution pour repérer des schémas d'opérations malveillantes (12 lettres)

7 horizontal: MISESAJOUR Téléchargements réguliers de définitions qui alimentent la base de données des menaces (10 lettres)

8 horizontal: SIGNATURE Empreinte cryptographique unique, enregistrée dans une base de données, servant à identifier les menaces connues (9 lettres)

VERTICALEMENT

1 vertical: FAUXPOSITIF Alerte de sécurité qui classe à tort un logiciel sûr comme malveillant (11 lettres)

3 vertical: ANTIVIRUS Suite logicielle qui analyse et protège les terminaux contre les exploits (9 lettres)

4 vertical: BACASABLE Environnement de test virtuel sécurisé qui exécute sans danger du code non fiable (9 lettres)

5 vertical: HEURISTIQUE Analyse fondée sur des règles qui signale les fichiers dont la structure de code est suspecte (11 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. TANISUREG — **SIGNATURE**
2. EBLAAABSC — **BACASABLE**
3. MAUJISREOS — **MISESAJOUR**
4. TNENAAIAQUR — **QUARANTAINE**
5. QEITUEISHUR — **HEURISTIQUE**
6. TOMERNECOTMP — **COMPORTEMENT**
7. IPFASFTIUOX — **FAUXPOSITIF**
8. SVUAINIRT — **ANTIVIRUS**

CORRIGÉ DU DÉFI DU CODE SECRET

"DETECTEZ LES NOUVEAUX MALWARES PAR HEURISTIQUE"

Corrigé des études de cas

A Étude de cas 1 : Analyse par signature ou heuristique

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : un employé télécharge un utilitaire personnalisé développé en interne par une autre équipe. L'analyseur par signatures le laisse passer, mais l'analyseur heuristique le signale comme suspect.
- Stratégie et solution recommandées : Pourquoi c'est arrivé : l'analyse par signatures vérifie les empreintes (hash) des fichiers ; comme le logiciel est personnalisé, il ne figure pas dans la base de données des menaces. L'heuristique analyse la structure et a signalé des actions suspectes (par ex. des écritures dans le registre). Vérification : exécutez le fichier dans un bac à sable (sandbox) pour observer ses actions, vérifiez les signatures numériques et soumettez l'empreinte à des portails de renseignement sur les menaces.

B Étude de cas 2 : Gérer les faux positifs

Corrigé de l'enseignant

CONSIGNE DE NOTATION

Les réponses des élèves doivent couvrir les points suivants :

- Analyse de scénario : un développeur compile son application. L'antivirus du système signale le nouvel exécutable comme logiciel malveillant et le met en quarantaine.
- Stratégie et solution recommandées : Risques de la liste blanche : contourner les analyseurs peut permettre l'exécution de code réellement infecté. Démarche de résolution : soumettez le fichier à l'éditeur de l'antivirus pour analyse, signez numériquement le code à l'aide d'autorités de certification et configurez temporairement des exceptions pour des dossiers précis plutôt que de désactiver l'antivirus.