Nume: _____ **Data:** _____ **Punctaj:** _____

Software antivirus și protecția stațiilor terminale
Ghid de protecție

Detectarea pe bază de semnături, euristica, monitorizarea comportamentului, sandboxing-ul, actualizările

PREZENTARE GENERALĂ DE ÎNVĂȚARE: SOFTWARE ANTIVIRUS

SECURIZAT
CRIPTAREA DATELOR
Standardul AES pe 256 de biți

CONFORM
STANDARDE GLOBALE
Cadrele GDPR și CCPA

ZERO-TRUST
POLITICĂ DE ACCES
Autentificare multifactor

Bun venit! Acest pachet de activități te ghidează prin software antivirus și protecția punctelor terminale. Vei explora bazele de date de semnături, scanerele euristice, monitorizarea comportamentală, fișierele virtuale din sandbox și reducerea falsurilor pozitive.

PUNCTE DE CONTROL ALE FIȘEI DE LUCRU

- [ ] **Partea 1-4: Stăpânește securitatea cibernetică și prevenirea amenințărilor.**
- [ ] **Partea 5-7: Rezolvă puzzle-uri de tip cuvinte încrucișate și căutare de cuvinte.**
- [ ] **Partea 8-9: Rezolvă studii de caz și provocarea cu codul cifrat.**
- [ ] **Partea 10: Parcurge paginile de întrebări frecvente de bază și avansate.**
- [ ] **Partea 11: Explorează 10 fapte interesante din lumea reală.**
- [ ] **Bonus: provocarea Gândește repede.**

Deschide Ghidul VPN.com de securitate cibernetică

URL: https://www.vpn.com/ro/securitate-cibernetica/antivirus/

Harta ta de învățare despre strategia antivirus

- Diferențiază detectarea software-ului rău intenționat bazată pe semnături de cea bazată pe euristici.
- Înțelege monitorizarea comportamentului și protocoalele de izolare în sandbox.
- Evaluează impactul scanărilor în timp real asupra performanței sistemului și a punctelor finale.
- Reduce clasificările fals pozitive prin verificarea certificatelor digitale.
- Gestionează distribuirea zilnică a actualizărilor de definiții pe stațiile de lucru ale companiei.

INSTRUCȚIUNI DE GHID ANTIVIRUS

Răspunde la întrebările cu alegere multiplă și adevărat/fals, completează propozițiile cu spații libere folosind banca de cuvinte, asociază definițiile și rezolvă cuvintele încrucișate și puzzle-ul de căutare a cuvintelor. Aplică ce ai învățat despre securitatea antivirus pentru stațiile terminale. Încheie cu activitatea bonus Gândește repede.

PROTECȚIA ANTIVIRUS ȘI SCANAREA PE BAZĂ DE SEMNĂTURI (INTRODUCERE)

Software-ul antivirus protejează stațiile terminale prin identificarea, punerea în carantină și eliminarea software-ului rău intenționat. Sistemele moderne combină bazele de date de semnături (care potrivesc hash-urile amenințărilor cunoscute) cu euristica (care analizează structura fișierelor) și cu monitorizarea comportamentului pentru a detecta exploatările zero-day.

CITEȘTE ATENT FIECARE PUNCT DE CONTROL ȘI ALEGE SAU SCRIE RĂSPUNSUL CORECT

Punct de control 1: Provocare cu alegere multiplă

1. Care este o limitare a detectării bazate pe semnături?

- A. Nu poate identifica malware necunoscut sau modificat
- B. Generează rate mari de fals pozitive
- C. Necesită putere mare de procesare a procesorului
- D. Funcționează numai când este conectat la internet

2. Cum detectează scanerele euristice variantele noi de malware?

- A. Prin identificarea tiparelor și a structurilor de cod suspecte
- B. Prin potrivirea hash-urilor fișierelor cu o bază de date de amenințări
- C. Prin ștergerea automată a tuturor executabilelor nesemnate
- D. Încărcând fiecare fișier într-un dosar cloud public

3. Care este scopul execuției în sandbox a antivirusului?

- A. Izolarea și analizarea fișierelor într-un seif virtual securizat
- B. Accelerarea transferului copiei de rezervă a sistemului local de fișiere
- C. Actualizarea patch-urilor de securitate ale sistemului de operare local
- D. Comprimarea fișierelor mari de documente pentru a economisi spațiu de stocare

4. Ce metodă de detectare semnalează în timp real comportamentul amenințător?

- A. Analiză comportamentală care monitorizează acțiunile software-ului
- B. Inspectarea istoricului jurnalelor, efectuată peste noapte
- C. Intervenția manuală a utilizatorului care raportează aplicațiile lente
- D. Revizuiri manuale săptămânale ale programelor instalate

5. De ce sunt esențiale actualizările regulate ale definițiilor pentru scannere?

- A. Pentru a alimenta cu identificatori de amenințări baza de date a motoarelor bazate pe semnături
- B. Pentru a crește frecvența procesorului în timpul operațiunilor
- C. Pentru a modifica timpii de memorare în cache ai serverelor de nume DNS globale
- D. Pentru a autoriza setările cookie-urilor din browserul web

Punct de control 2: Provocare Adevărat sau Fals

6 Întrebare adevărat/fals 6

6. Detectarea pe bază de semnături compară hash-urile criptografice ale fișierelor cu liste din baze de date.

- ○ Adevărat
- ○ Fals

7 Întrebare adevărat/fals 7

7. Scanerele euristice pot declanșa alerte false pozitive pentru fișiere sigure.

- ○ Adevărat
- ○ Fals

8 Întrebare adevărat/fals 8

8. Un sandbox permite malware-ului să acceseze fișiere din rețea fără limite.

- ○ Adevărat
- ○ Fals

9 Întrebare adevărat/fals 9

9. Scanarea comportamentală blochează fișierele atunci când acestea manifestă acțiuni rău intenționate.

- ○ Adevărat
- ○ Fals

10 Întrebare adevărat/fals 10

10. Software-ul antivirus standard oprește complet toate atacurile zero-day.

- ○ Adevărat
- ○ Fals

Punct de control 3: Inserarea termenilor-cheie

Citește fiecare propoziție de mai jos și completează spațiul liber cu termenul corect din Banca de cuvinte.

1. Un scaner tradițional identifică malware-ul cunoscut prin potrivirea cu o _____ .

2. Analiza tiparelor de cod ale fișierelor se numește scanare _____ .

3. Instrumentele antivirus izolează fișierele suspecte într-un mediu de tip _____ .

4. Monitorizarea în timp real urmărește programele pentru a depista orice _____ suspect.

5. Scanerele descarcă zilnic _____ ale bazei de date pentru a recunoaște amenințările noi.

6. Programele sigure marcate drept malware declanșează o alertă de tip _____ .

BANCĂ DE CUVINTE DIN VOCABULAR

ACTUALIZĂRI ANTIVIRUS COMPORTAMENT FALS POZITIV FIREWALL HEURISTICĂ SANDBOX SEMNĂTURĂ

Scrie răspunsurile aici:

1.

2.

3.

4.

5.

6.

Punct de control 4: Asocierea conceptelor despre securitate

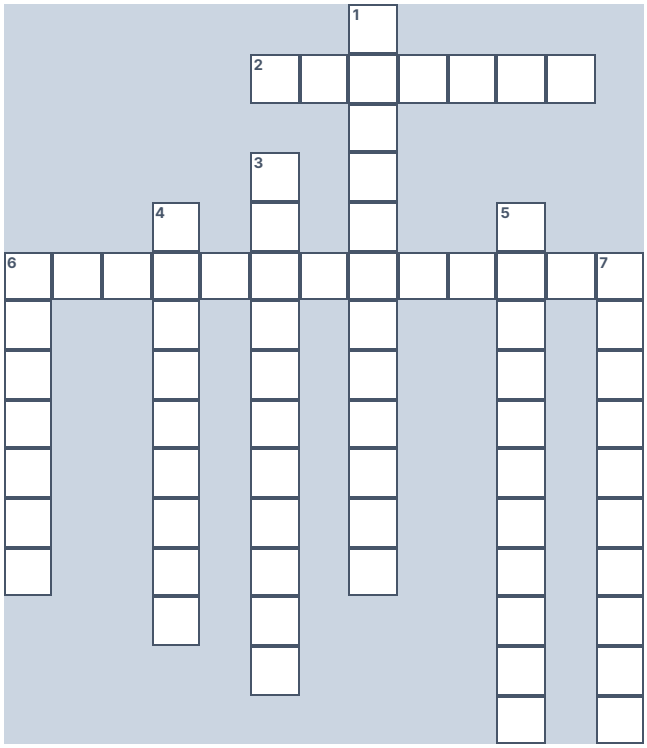
ASOCIEREA DEFINIȚIILOR

Asociază fiecare termen de vocabular din stânga cu definiția corectă din dreapta, scriind litera corespunzătoare (A-H) în câmpul de completare.

☐	1. Semnătură hash	A	Izolarea fișierelor suspecte pentru a preveni expunerea sistemului local.
☐	2. Euristica codului	B	Suită software care scanează și protejează punctele finale împotriva exploiturilor.
☐	3. Sandbox pentru fișiere	C	Monitorizarea acțiunilor software-ului în execuție pentru a identifica tipare de funcționare rău intenționate.
☐	4. Scanare comportamentală	D	Amprentă criptografică unică din baza de date, folosită pentru a identifica amenințările cunoscute.
☐	5. Actualizări zilnice	E	Mediu virtual de testare securizat care rulează cod nesigur în siguranță.
☐	6. Fals pozitiv	F	Descărcări regulate de definiții care alimentează baza de date de amenințări.
☐	7. Izolarea amenințărilor	G	Analiză bazată pe reguli care semnalează fișierele cu structuri de cod suspecte.
☐	8. Instrument antivirus	H	Alertă de securitate care clasifică greșit software sigur drept malware.

Punct de control 5: Careu de cuvinte încrucișate

Rezolvă careul de cuvinte încrucișate tastând litere în căsuțele albe active. Numerele corespund indiciilor de mai jos.



ORIZONTAL

2. Închiderea fișierelor suspecte într-un spațiu separat, pentru a evita expunerea sistemului local (7)

6. Amprentă criptografică unică din baza de date, folosită pentru a identifica amenințările cunoscute (13)

VERTICAL

1. Monitorizarea acțiunilor software-ului aflat în execuție, în căutarea tiparelor de funcționare rău intenționate (12)

3. Descărcări regulate de definiții care alimentează baza de date de amenințări (11)

4. Suită software care scanează și protejează dispozitivele finale împotriva exploatărilor (9)

5. Alertă de securitate care clasifică greșit un software sigur drept malware (11)

6. Mediu virtual de testare securizat, în care codul nesigur rulează în siguranță (7)

7. Analiză bazată pe reguli care marchează fișierele cu structuri de cod suspecte (10)

Punct de control 5, variantă alternativă: Indicii accesibile pentru cuvinte încrucișate

Utilizatorii de cititoare de ecran și de tastatură pot introduce răspunsurile la cuvintele încrucișate direct în câmpurile de text de mai jos. INDICII ORIZONTAL INDICII VERTICAL

ORIZONTAL

2 orizontal: Închiderea fișierelor suspecte într-un spațiu separat, pentru a evita expunerea sistemului local (7 litere):

6 orizontal: Amprentă criptografică unică din baza de date, folosită pentru a identifica amenințările cunoscute (13 litere):

VERTICAL

1 vertical: Monitorizarea acțiunilor software-ului aflat în execuție, în căutarea tiparelor de funcționare rău intenționate (12 litere):

3 vertical: Descărcări regulate de definiții care alimentează baza de date de amenințări (11 litere):

4 vertical: Suită software care scanează și protejează dispozitivele finale împotriva exploatărilor (9 litere):

5 vertical: Alertă de securitate care clasifică greșit un software sigur drept malware (11 litere):

6 vertical: Mediu virtual de testare securizat, în care codul nesigur rulează în siguranță (7 litere):

7 vertical: Analiză bazată pe reguli care marchează fișierele cu structuri de cod suspecte (10 litere):

Punct de control 6: Căutarea cuvintelor ascunse

Găsește în grila de mai jos cei 8 termeni cheie de vocabular ascunși. Cuvintele pot fi orizontale, verticale sau diagonale.

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

LISTĂ DE CUVINTE DIN VOCABULAR

SEMNĂTURĂHASH
HEURISTICĂ
SANDBOX
COMPORTAMENT
ACTUALIZĂRI
FALSPOZITIV
IZOLARE
ANTIVIRUS

Punct de control 6, variantă alternativă: Asocierea accesibilă a vocabularului

Asociază fiecare dintre cei 8 termeni de vocabular din Căutarea de cuvinte cu definiția corectă, scriind litera (A-H) în spațiul liber.

TERMENI DE VOCABULAR

- **A. SEMNĂTURĂHASH**
- **B. HEURISTICĂ**
- **C. SANDBOX**
- **D. COMPORTAMENT**
- **E. ACTUALIZĂRI**
- **F. FALSPOZITIV**
- **G. IZOLARE**
- **H. ANTIVIRUS**

DEFINIȚII ȘI CÂMPURI DE ASOCIERE

1. Monitorizarea acțiunilor software-ului aflat în execuție, în căutarea tiparelor de funcționare rău intenționate.
2. Suită software care scanează și protejează dispozitivele finale împotriva exploatărilor.
3. Descărcări regulate de definiții care alimentează baza de date de amenințări.
4. Analiză bazată pe reguli care marchează fișierele cu structuri de cod suspecte.
5. Închiderea fișierelor suspecte într-un spațiu separat, pentru a evita expunerea sistemului local.
6. Amprentă criptografică unică din baza de date, folosită pentru a identifica amenințările cunoscute.
7. Mediu virtual de testare securizat, în care codul nesigur rulează în siguranță.
8. Alertă de securitate care clasifică greșit un software sigur drept malware.

Punct de control 7: Provocare cu cuvinte amestecate

Descifrează literele de mai jos pentru a dezvălui conceptele și termenii-cheie de securitate cibernetică. Scrie răspunsurile în casetele de introducere furnizate.

1. UMĂSTERHSA HĂN
2. SNXOBDA
3. AILZTCRIAĂU
4. EZALRIO
5. ISĂERTIHCU
6. TOMERNACOT MP
7. IPFAZVTILOS
8. SVUAINIRT

Activitate bonus: Gândește repede

3 RĂSPUNSURI PE CATEGORIE. CÂȘTIGĂ CINE COMPLETEAZĂ PRIMUL LISTA.

1	Motive pentru care ar trebui să actualizezi software-ul			
2	Persoane pe care le poți întreba pentru ajutor IT			
3	Lucruri de făcut când antivirusul găsește ceva			
4	Semne ale unui virus de calculator			
5	Lucruri care ajung în carantină			
6	Locuri în care se ascund virușii			
7	Informații pe care nu ar trebui să le dai niciodată			
8	Tipuri de software rău intenționat			
9	Instrumente de securitate pe care le cunoști			
10	Lucruri pe care le scanează un antivirus			
11	Lucruri pe care le salvezi într-o copie de rezervă			
12	Dispozitive care pot fi sparte			
13	Programe antivirus pe care le cunoști			
14	Motive pentru alarme false			
15	Obiceiuri sigure pe care le poți începe de azi			

Punct de control 8: Studii de caz despre securitatea cibernetică

Aplică conceptele pe care le-ai învățat pentru a rezolva scenariile reale de mai jos.

STUDIU DE CAZ 1: SCANARE BAZATĂ PE SEMNĂTURI VS. SCANARE EURISTICĂ



Scenariu: Un angajat descarcă un utilitar personalizat, creat intern de o altă echipă. Scanerul bazat pe semnături îl lasă să treacă, dar scanerul euristic îl marchează ca suspect.

Întrebare de discuție: Explică de ce s-a întâmplat acest lucru și cum se poate verifica dacă fișierul este sigur.

STUDIU DE CAZ 2: GESTIONAREA FALSELOR POZITIVE



Scenariu: Un dezvoltator de software își compilează aplicația. Antivirusul sistemului marchează noul executabil drept malware și îl trimite în carantină.

Întrebare de discuție: Descrie pe scurt riscurile adăugării în lista de excepții și explică procedura corectă de rezolvare.

Punct de control 9: Descifrează codul

Un profesionist în securitate cibernetică protejează activele rețelei de actorii amenințărilor online. Folosește cheia literă–număr de mai jos pentru a descifra mesajul, scriind literele corespunzătoare în spațiile libere.

CHEIE DE CRIPTARE LITERĂ-NUMĂR

A=1 Ă=2 Â=3 B=4 C=5 D=6 E=7 F=8 G=9 H=10 I=11
Î=12 J=13 K=14 L=15 M=16 N=17 O=18 P=19 Q=20 R=21 S=22
Ș=23 T=24 Ț=25 U=26 V=27 W=28 X=29 Y=30 Z=31

6	7	19	11	22	24	7	1	31	2		16	1	15	28	1	21	7
17	18	26		19	21	11	17		1	17	1	15	11	31	2		
10	7	26	21	11	22	24	11	5	2								

Mesaj descifrat:

SFAT: FIECARE NUMĂR REPREZINTĂ POZIȚIA ACELEI LITERE ÎN ALFABET (DE EX. 1 = A, 2 = B, 31 = Z).

Punct de control 10: Întrebări frecvente de bază despre securitatea cibernetică (Partea A)

Parcurge întrebările și răspunsurile frecvente despre atenuarea amenințărilor online.

Q1: Cum identifică software-ul antivirus software-ul rău intenționat?

Identifică malware-ul prin potrivirea semnăturilor din baze de date, analiza euristică a structurii codului și monitorizarea comportamentală în timp real.

Q2: Ce este detecția bazată pe semnături?

Este o metodă de scanare care potrivește hash-urile criptografice ale fișierelor cu liste din baze de date de amenințări malware cunoscute.

Q3: Ce este un scaner euristic?

Analiza euristică examinează structura unui fișier și instrucțiunile din cod, semnalând tiparele suspecte comune variantelor de malware.

Q4: Ce înseamnă când un fișier este pus în carantină?

Antivirusul mută fișierul într-un folder securizat și izolat, blocându-i execuția pentru a proteja sistemul de operare.

Q5: Ce este un fals pozitiv al antivirusului?

Este o eroare în care software-ul legitim și sigur este semnalat incorect ca malware de algoritmii de scanare.

Punct de control 10: Întrebări frecvente de bază despre securitatea cibernetică (Partea B)

Parcurge întrebările și răspunsurile frecvente despre atenuarea amenințărilor online.

Q6: Cum protejează monitorizarea comportamentului sistemele?

Monitorizează în timp real software-ul care rulează, blocând procesele care încearcă modificări suspecte, precum injectarea de cod.

Q7: De ce este importantă testarea în sandbox?

Sandboxing-ul rulează fișiere nesigure într-o mașină virtuală izolată, observând acțiunile în siguranță, fără expunerea sistemului.

Q8: Cât de des ar trebui să se actualizeze definițiile antivirusului?

Scanerele ar trebui să-și actualizeze definițiile zilnic sau din oră în oră pentru a recunoaște tulpinile de malware nou descoperite.

Q9: Care este diferența dintre antivirus și EDR?

Antivirusul se concentrează pe scanarea fișierelor, în timp ce Endpoint Detection and Response (EDR) oferă urmărirea și izolarea amenințărilor la nivelul întregii rețele.

Q10: Pot rula două programe antivirus împreună?

Nu. Rularea a două scanere active provoacă conflicte de sistem, încetinește performanța și poate bloca operațiunile celuilalt.

Punct de control 10: Întrebări frecvente avansate despre securitate (Partea C)

Explorează aspecte tehnice avansate ale cadrelor de securitate, ale analizei software-ului rău intenționat și ale conformității datelor.

Q1: Cum reduc regulile euristice la minimum ocolirea amenințărilor?

Analiza euristică examinează tipare generale de amenințări, nu semnături specifice, depistând variantele modificate ale familiilor de malware cunoscute.

Q2: Ce este un virus polimorfic?

Este malware care își schimbă structura fișierului și rutina de decriptare la fiecare execuție, făcând scanările pe bază de semnături ineficiente.

Q3: Cum detectează sandbox-urile evitarea mașinilor virtuale?

Sandbox-urile moderne simulează clicurile de mouse și timpul de funcționare a sistemului, păcălind software-ul rău intenționat conceput să se ascundă când rulează în mașini virtuale.

Q4: Care sunt formatele de descărcare a actualizărilor de semnături?

Actualizările sunt de obicei fișiere diff binare incrementale ușoare, care reduc consumul de lățime de bandă a rețelei clientului.

Q5: Cum gestionează agenții endpoint scanările locale?

Agenții efectuează verificări ușoare în fundal, delegând căutările criptografice aprofundate de hash-uri către bazele de date cloud de amenințări.

Punct de control 10: Întrebări frecvente avansate despre securitate (Partea D)

Explorează aspecte tehnice avansate ale cadrelor de securitate, ale analizei software-ului rău intenționat și ale conformității datelor.

Q6: Ce este scanarea de detectare a rootkit-urilor?

Scanează tabelele de memorie de la nivelul nucleului, ocolind API-urile sistemului de operare pe care rootkit-urile le interceptează pentru a-și ascunde firele active.

Q7: Cum blochează scanarea comportamentală ransomware-ul?

Detectează buclele automate de criptare în masă a fișierelor, oprind procesul gazdă înainte ca bazele de date ale sistemului să fie blocate.

Q8: Ce este verificarea certificatului de semnare a codului?

Scanerele verifică semnăturile digitale ale codului față de autoritățile de certificare rădăcină de încredere, validând identitatea dezvoltatorului software.

Q9: Cum afectează packerele motoarele de scanare?

Packerele comprimă sau criptează sarcinile utile ale software-ului rău intenționat. Scanerele trebuie să despacheteze fișierul în memorie înainte de a rula potrivirile de semnături.

Q10: Cum automatizează instrumentele EDR izolarea?

Agenții EDR pun în carantină, la nivel de rețea, punctele finale compromise, blocând mișcarea laterală și permițând totodată accesul analiștilor.

Partea 11: 10 fapte și perspective din lumea reală despre securitatea cibernetică

Parcurge fapte din lumea reală despre breșele de securitate, mecanismele de apărare și standardele de conformitate.

1. INFORMAȚII DESPRE SECURITATE

Bazele de date de semnături stochează hash-urile malware-ului cunoscut, așa că fișierele noi sau modificate nu sunt detectate până la actualizarea definițiilor.

2. INFORMAȚII DESPRE SECURITATE

Motoarele euristice pot semnala unele variante noi de malware înainte să existe semnături, cu prețul unui număr mai mare de alarme false.

3. INFORMAȚII DESPRE SECURITATE

Alertele fals pozitive costă echipele IT timp petrecut verificând și restaurând fișiere puse în carantină din greșeală.

4. INFORMAȚII DESPRE SECURITATE

Software-ul rău intenționat polimorfic își schimbă codul la fiecare copie, așa că apărătorii îmbină semnăturile cu verificări euristice și comportamentale.

6. INFORMAȚII DESPRE SECURITATE

Autorii de software rău intenționat scriu coduri personalizate care verifică mediile sandbox și întârzie execuția pentru a ocoli temporizatoarele.

5. INFORMAȚII DESPRE SECURITATE

Motoarele antivirus din cloud compară hash-urile fișierelor suspecte cu baze mari de date online despre amenințări, aproape în timp real.

7. PERSPECTIVĂ ASUPRA SECURITĂȚII

Furnizorii transmit periodic actualizări de definiții către punctele terminale, astfel încât scanerele să poată recunoaște amenințările nou confirmate.

8. PERSPECTIVĂ ASUPRA SECURITĂȚII

Monitoarele comportamentale anti-ransomware vizează apeluri Win32 API specifice asociate cu criptarea fișierelor și ștergerea copiilor umbră.

9. PERSPECTIVĂ ASUPRA SECURITĂȚII

Semnăturile de cod valide pot reduce riscul fals-pozitivelor, dar fișierele semnate sunt scanate în continuare, deoarece și malware-ul poate fi semnat.

10. INFORMAȚII DESPRE SECURITATE

Rootkiturile modifică structurile kernelului sistemului, necesitând scanere specializate care rulează la pornire pentru detectare și curățare.

Referințe tehnice și surse

Ghidul de studiu și puzzle-urile interactive sunt alcătuite pe baza standardelor globale NIST, OWASP și de conformitate privind confidențialitatea datelor. REFERINȚE ACADEMICE ȘI DIN INDUSTRIE

REFERINȚE ACADEMICE ȘI DIN INDUSTRIE

[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

Barem: Punct de control 1 – Alegere multiplă

1 **Întrebarea 1** SEMNĂTURI **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Scanarea bazată pe semnături se bazează pe hash-uri cunoscute din baze de date și nu reușește să detecteze malware necunoscut sau modificat. Citare: OWASP Secure Configuration.

2 **Întrebarea 2** HEURISTICĂ **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Metodele euristice analizează structura codului și comenzile pentru a identifica trăsăturile suspecte ale variantelor noi de amenințări. Citare: Center for Internet Security (CIS).

3 **Întrebarea 3** SANDBOXING **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Un sandbox rulează fișierele suspecte într-o mașină virtuală izolată, pentru a observa în siguranță comportamentul la execuție. Citare: NIST Digital Identity.

4 **Întrebarea 4** COMPORTAMENTAL **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Scanarea comportamentală monitorizează în timp real programele care rulează pentru a bloca modificările neautorizate ale sistemului. Citare: Center for Internet Security (CIS).

5 **Întrebarea 5** ACTUALIZĂRI **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Scanerele descarcă zilnic actualizări incrementale ale definițiilor pentru a rămâne sincronizate cu peisajul amenințărilor. Citare: OWASP Secure Configuration.

Barem: Punct de control 2 – Adevărat sau fals

6 **Întrebarea 6** SEMNĂTURI — **Răspuns corect: Adevărat**

NOTĂ PENTRU PROFESOR

Instrumentele bazate pe semnături calculează hash-uri criptografice și le compară cu o bază de date de hash-uri de amenințări cunoscute. Citare: OWASP Secure Configuration.

7 **Întrebarea 7** HEURISTICĂ — **Răspuns corect: Adevărat**

NOTĂ PENTRU PROFESOR

Motoarele euristice rulează structuri bazate pe reguli care pot semnala drept suspecte fișiere legitime și sigure. Citare: Center for Internet Security (CIS).

8 **Întrebarea 8** SANDBOXING — **Răspuns corect: Fals**

NOTĂ PENTRU PROFESOR

Răspuns corect: Fals Un sandbox rulează codul într-un container virtual, blocând strict accesul la resursele partajate din rețea. Citare: NIST Digital Identity.

9 **Întrebarea 9** COMPORTAMENTAL — **Răspuns corect: Adevărat**

NOTĂ PENTRU PROFESOR

Monitorizarea în timp real semnalează procesele în execuție care încearcă scrieri ilegale sau blocarea fișierelor. Citare: Center for Internet Security (CIS).

10 **Întrebarea 10** — **Răspuns corect: Fals**

NOTĂ PENTRU PROFESOR

Răspuns corect: Fals Niciun antivirus nu oprește orice atac zero-day; amenințările necunoscute pot evita semnăturile și euristica.

Chei de vocabular și grilă de notare

Barem de notare pentru profesor: Acordă 1 punct pentru fiecare asociere corectă (8 puncte în total) și pentru fiecare termen din context (6 puncte în total).

PUNCT DE CONTROL 4: BAREM – ASOCIEREA CONCEPTELOR

D 1. Semnătură hash	G 2. Euristica codului	E 3. Sandbox pentru fișiere	C 4. Scanare comportamentală
F 5. Actualizări zilnice	H 6. Fals pozitiv	A 7. Izolarea amenințărilor	B 8. Instrument antivirus

PUNCT DE CONTROL 3: BAREM – TERMENI-CHEIE

1 SEMNĂTURĂ	2 HEURISTICĂ	3 SANDBOX	4 COMPORTAMENT
5 ACTUALIZĂRI	6 FALS POZITIV		

PUNCT DE CONTROL 6, VARIANTĂ ALTERNATIVĂ: BAREM – ASOCIEREA CUVINTELOR

1 D – COMPORTAMENT	2 H – ANTIVIRUS	3 E – ACTUALIZĂRI	4 B – HEURISTICĂ
5 G – IZOLARE	6 A – SEMNĂTURĂHASH	7 C – SANDBOX	8 F – FALSPOZITIV

NOTE DE DISCUȚIE PENTRU PROFESORI

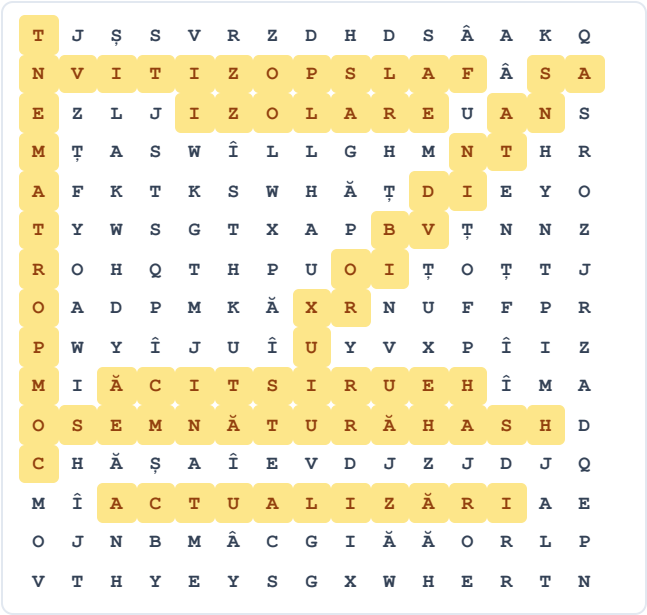
Termeni-cheie:
Verifică dacă elevii pot explica Semnătură hash, Euristica codului și Sandbox pentru fișiere cu propriile cuvinte și pot da câte un exemplu pentru fiecare.

Studii de caz:
Cere elevilor să își susțină recomandările cu fapte din fișă, nu cu presupuneri.

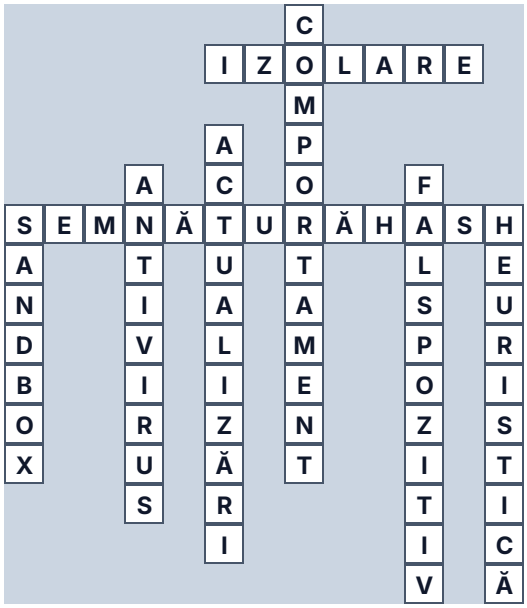
Evaluarea surselor:
Cere elevilor să verifice cel puțin o afirmație în sursele fișei și discutați de ce cifrele, prețurile și regulile se pot schimba în timp.

Chei de rezolvare ale puzzle-urilor și note pentru profesor

SOLUȚIA JOCULUI DE CĂUTARE DE CUVINTE



SOLUȚIA CUVINTELOR ÎNCRUCIȘATE



ORIZONTAL

2 orizontal: IZOLARE Închiderea fișierelor suspecte într-un spațiu separat, pentru a evita expunerea sistemului local (7 litere)

6 orizontal: SEMNĂTURĂHASH Amprentă criptografică unică din baza de date, folosită pentru a identifica amenințările cunoscute (13 litere)

VERTICAL

1 vertical: COMPORTAMENT Monitorizarea acțiunilor software-ului aflat în execuție, în căutarea tiparelor de funcționare rău intenționate (12 litere)

3 vertical: ACTUALIZĂRI Descărcări regulate de definiții care alimentează baza de date de amenințări (11 litere)

4 vertical: ANTIVIRUS Suită software care scanează și protejează dispozitivele finale împotriva exploatărilor (9 litere)

5 vertical: FALSPOZITIV Alertă de securitate care clasifică greșit un software sigur drept malware (11 litere)

6 vertical: SANDBOX Mediu virtual de testare securizat, în care codul nesigur rulează în siguranță (7 litere)

7 vertical: HEURISTICĂ Analiză bazată pe reguli care marchează fișierele cu structuri de cod suspecte (10 litere)

Cuvinte amestecate și barem pentru codul cifrat

Barem pentru activitatea de descifrare a cuvintelor de vocabular și pentru provocarea Codul secret.

BAREMUL PENTRU DESCIFRAREA CUVINTELOR

1. UMĂSTERHSAHĂN — SEMNĂTURĂHASH
2. SNXOBDA — SANDBOX
3. AILZTCRIAĂU — ACTUALIZĂRI
4. EZALRIO — IZOLARE
5. ISĂERTIHCU — HEURISTICĂ
6. TOMERNACOTMP — COMPORTAMENT
7. IPFAZVTILOS — FALSPOZITIV
8. SVUAINIRT — ANTIVIRUS

BAREMUL PROVOCĂRII CU CODUL SECRET

"DEPISTEAZĂ MALWARE NOU PRIN ANALIZĂ HEURISTICĂ"

Barem pentru studiile de caz

A Studiu de caz 1: Scanare bazată pe semnături vs. scanare euristică

Soluția profesorului

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: Un angajat descarcă un utilitar personalizat construit intern de o altă echipă. Scanerul bazat pe semnături îl acceptă, dar scanerul euristic îl marchează ca suspect.
- Strategie și soluție recomandată: De ce s-a întâmplat: Scanarea pe bază de semnături verifică hash-urile fișierelor; fiind personalizat, nu se află în baza de date de amenințări. Euristica analizează structura și a semnalat acțiuni suspecte (de ex. scrieri în registry). Verificare: Rulează fișierul într-un sandbox pentru a observa acțiunile, verifică semnăturile digitale și trimite hash-ul către portalurile de informații despre amenințări.

B Studiu de caz 2: Gestionarea falselor pozitive

Soluția profesorului

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: Un dezvoltator de software își compilează aplicația. Antivirusul sistemului marchează noul executabil ca malware și îl pune în carantină.
- Strategie și soluție recomandată: Riscurile listei albe: Ocolirea scanerelor poate permite rularea unui cod real, infectat. Calea de rezolvare: Trimite fișierul furnizorului de antivirus pentru analiză, semnează digital codul folosind autorități de certificare și configurează temporar excepții pentru anumite foldere, în loc să dezactivezi antivirusul.