Jméno: _____ Datum: _____ Body: _____

Antivirový software a koncové body Průvodce ochranou

Detekce podle signatur, heuristika, sledování chování, sandboxing, aktualizace

PŘEHLED UČIVA: ANTIVIROVÝ SOFTWARE

ZABEZPEČENO
ŠIFROVÁNÍ DAT
Standard 256bitového AES

VYHOVUJÍCÍ
GLOBÁLNÍ STANDARDY
Rámce GDPR a CCPA

ZERO-TRUST
ZÁSADY PŘÍSTUPU
Vícefaktorové ověřování

Vítejte! Tento balíček aktivit vás provede antivirovým softwarem a ochranou koncových bodů. Prozkoumáte databáze signatur, heuristické skenery, sledování chování, virtuální soubory sandboxu a omezování falešných poplachů.

KONTROLNÍ BODY PRACOVNÍHO LISTU

- [ ] **Část 1-4: Zvládněte kyberbezpečnost a prevenci hrozeb.**
- [ ] **Část 5-7: Vyřešte křížovku a osmisměrku.**
- [ ] **Část 8-9: Vyřešte případové studie a šifrovací výzvu.**
- [ ] **Část 10: Projděte si stránky se základními i pokročilými FAQ.**
- [ ] **Část 11: Prozkoumejte 10 zajímavých faktů z praxe.**
- [ ] **Bonus: výzva Mysli rychle.**

Otevřete průvodce kyberbezpečností od VPN.com

URL: https://www.vpn.com/cs/kyberneticka-bezpecnost/antivirus/

Váš studijní plán: antivirová strategie

- Rozlište detekci malwaru na základě signatur a heuristiky.
- Pochopte monitorování chování a protokoly izolace v sandboxu.
- Vyhodnoťte dopady skenování v reálném čase na výkon systému a koncové body.
- Omezte falešně pozitivní klasifikace pomocí ověřování digitálních certifikátů.
- Spravujte denní distribuci aktualizací definic na firemní koncová zařízení.

POKYNY K PRŮVODCI ANTIVIREM

Odpovězte na otázky s výběrem odpovědí a otázky pravda/nepravda, doplňte věty s vynechanými slovy pomocí banky slov, přiřaďte definice a vyřešte křížovku a osmisměrku. Uplatněte své znalosti na antivirovou ochranu koncových bodů. Zakončete bonusovou aktivitou Mysli rychle.

ANTIVIROVÁ OCHRANA A SIGNATUROVÉ SKENOVÁNÍ (ÚVOD)

Antivirový software chrání koncové body identifikací, karanténou a odstraňováním malwaru. Moderní systémy kombinují databáze signatur (porovnávání hashů známých hrozeb) s heuristikou (analýzou struktury souborů) a sledováním chování k detekci zero-day exploitů.

PŘEČTĚTE SI POZORNĚ KAŽDÝ KONTROLNÍ BOD A VYBERTE NEBO NAPIŠTE SPRÁVNOU

Kontrolní bod 1: Výzva s výběrem odpovědí

1. Jaké je omezení detekce založené na signaturách?

- A. Nedokáže rozpoznat neznámý nebo upravený malware
- B. Generuje vysokou míru falešných poplachů
- C. Vyžaduje vysoký výpočetní výkon CPU
- D. Funguje jen při připojení k internetu

2. Jak heuristické skenery detekují nové varianty malwaru?

- A. Rozpoznáváním podezřelých vzorců a struktur kódu
- B. Porovnáváním hashů souborů s databází hrozeb
- C. Automatickým mazáním všech nepodepsaných spustitelných souborů
- D. Nahráním každého souboru do veřejné cloudové složky

3. Jaký je účel spouštění v sandboxu u antiviru?

- A. Izolace a analýza souborů v zabezpečeném virtuálním trezoru
- B. Zrychlení přenosu zálohy místního souborového systému
- C. Aktualizace bezpečnostních záplat místního operačního systému
- D. Komprese velkých dokumentů kvůli úspoře místa

4. Jaká detekční metoda označuje hrozby podle chování v reálném čase?

- A. Behaviorální analýza sledující akce softwaru
- B. Kontrola historických logů prováděná přes noc
- C. Ruční zásah uživatelů hlásících pomalé aplikace
- D. Týdenní ruční kontroly nainstalovaných programů

5. Proč jsou pravidelné aktualizace definic pro skenery kritické?

- A. Dodávat signaturovým enginům databázové identifikátory hrozeb
- B. Zvýšit taktovací frekvence CPU během operací
- C. Změnit globální doby kešování DNS jmenných serverů
- D. Autorizovat nastavení cookies ve webovém prohlížeči

Kontrolní bod 2: Výzva Pravda/Nepravda

6 Otázka tf 6

6. Detekce podle signatur porovnává kryptografické hashe souborů se seznamy v databázi.

- ○ Pravda
- ○ Nepravda

7 Otázka tf 7

7. Heuristické skenery mohou spouštět falešné poplachy u bezpečných souborů.

- ○ Pravda
- ○ Nepravda

8 Otázka tf 8

8. Sandbox umožňuje malwaru neomezený přístup k síťovým souborům.

- ○ Pravda
- ○ Nepravda

9 Otázka tf 9

9. Behaviorální skenování blokuje soubory, když vykazují škodlivé chování.

- ○ Pravda
- ○ Nepravda

10 Otázka tf 10

10. Standardní antivirový software zcela zastaví všechny zero-day útoky.

- ○ Pravda
- ○ Nepravda

Kontrolní bod 3: Doplňování klíčových pojmů

Přečtěte si každou větu níže a doplňte do vynechaného místa správný termín ze slovní banky.

1. Otisk, podle kterého tradiční skener rozpoznává známý malware, se nazývá _____ .

2. Zkoumání vzorců v kódu souborů, které odhaluje neznámé hrozby, se označuje jako _____ .

3. Antivirové nástroje spouštějí podezřelé soubory v izolovaném prostředí zvaném _____ .

4. Sledování v reálném čase pozoruje _____ programů a hledá podezřelé aktivity.

5. Aby skener rozpoznal nové hrozby, stahuje každý den _____ své databáze.

6. Hlášení, které mylně označí bezpečný program za malware, se nazývá _____ , hovorově falešný poplach.

ZÁSOBNÍK SLOV

AKTUALIZACE ANTIVIROVÝ NÁSTROJ FALEŠNĚ POZITIVNÍ NÁLEZ HEURISTICKÁ ANALÝZA CHOVÁNÍ IZOLACE SANDBOX SIGNATURA

Sem napište své odpovědi:

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

Kontrolní bod 4: Přiřazování bezpečnostních pojmů

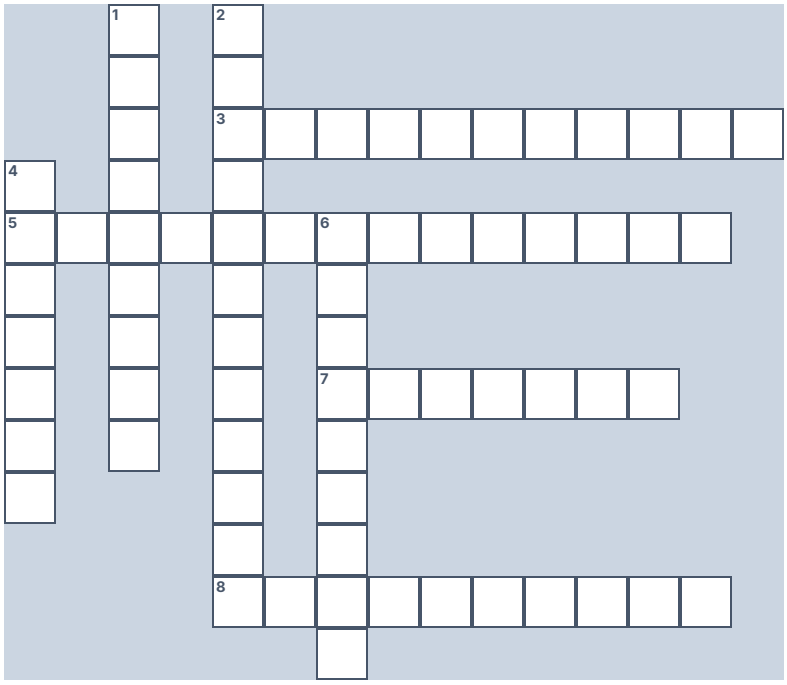
PŘIŘAZOVÁNÍ DEFINIC

Přiřaďte každý slovníčkový pojem vlevo k jeho správné definici vpravo zapsáním odpovídajícího písmene (A–H) do vyplnitelného pole.

☐	1. Hash podpis	A	Uzavření podezřelých souborů, aby nedošlo k ohrožení místního systému.
☐	2. Heuristika kódu	B	Softwarová sada skenující a chránící koncové body před exploity.
☐	3. Souborový sandbox	C	Monitorování činnosti běžícího softwaru kvůli vzorcům škodlivých operací.
☐	4. Sken chování	D	Jedinečný kryptografický databázový otisk používaný k identifikaci známých hrozeb.
☐	5. Denní aktualizace	E	Zabezpečené virtuální testovací prostředí bezpečně spouštějící nedůvěryhodný kód.
☐	6. Falešně pozitivní nález	F	Pravidelné stahování definic plnící databázi hrozeb.
☐	7. Izolace hrozeb	G	Analýza založená na pravidlech označující soubory s podezřelou strukturou kódu.
☐	8. Antivirový nástroj	H	Bezpečnostní výstraha nesprávně klasifikující bezpečný software jako malware.

Kontrolní bod 5: Křížovka

Vyřešte křížovku zapisováním písmen do aktivních bílých políček. Čísla odpovídají nápovědám níže.



VODOROVNÉ NÁPOVĚDY

3. Pravidelné stahování definic doplňující databázi hrozeb (11)

5. Sledování akcí běžícího softwaru kvůli vzorcům škodlivých operací (14)

7. Uzavření podezřelých souborů, aby se zabránilo ohrožení místního systému (7)

8. Analýza založená na pravidlech označující soubory s podezřelou strukturou kódu (10)

SVISLÉ NÁPOVĚDY

1. Jedinečný kryptografický otisk v databázi používaný k identifikaci známých hrozeb (9)

2. Bezpečnostní upozornění, které mylně označí bezpečný software za malware (12)

4. Zabezpečené virtuální testovací prostředí bezpečně spouštějící nedůvěryhodný kód (7)

6. Softwarová sada skenující koncová zařízení a chránící je před exploity (9)

Kontrolní bod 5, alternativa: Přístupná zadání křížovky

Uživatelé čteček obrazovky a klávesnice mohou odpovědi křížovky zapisovat přímo do textových polí níže. NÁPOVĚDY VODOROVNĚ NÁPOVĚDY SVISLE

VODOROVNÉ NÁPOVĚDY

3 vodorovně: Pravidelné stahování definic doplňující databázi hrozeb (11 písmen):

5 vodorovně: Sledování akcí běžícího softwaru kvůli vzorcům škodlivých operací (14 písmen):

7 vodorovně: Uzavření podezřelých souborů, aby se zabránilo ohrožení místního systému (7 písmen):

8 vodorovně: Analýza založená na pravidlech označující soubory s podezřelou strukturou kódu (10 písmen):

SVISLÉ NÁPOVĚDY

1 svisle: Jedinečný kryptografický otisk v databázi používaný k identifikaci známých hrozeb (9 písmen):

2 svisle: Bezpečnostní upozornění, které mylně označí bezpečný software za malware (12 písmen):

4 svisle: Zabezpečené virtuální testovací prostředí bezpečně spouštějící nedůvěryhodný kód (7 písmen):

6 svisle: Softwarová sada skenující koncová zařízení a chránící je před exploity (9 písmen):

Kontrolní bod 6: Hledání skrytých slov

Najděte 8 klíčových pojmů skrytých v mřížce níže. Slova mohou být vodorovně, svisle nebo úhlopříčně.

H Ž N K V Š Ú Á Š X J N N G H

C Ň A K I T S I R U E H H S Ě

A L Ť M S A N D B O X S X H B

L Ú É Ý Ó Z X E T G Ť Y A Q Ú

P O O Z P H C R Ť H Q Ů U P Ú

O U K A E A P Ň L Á O Ů Ě F R

P Ř X Ý L J J Ů J Z W Y Q J I

Ý Ž I O Í S U R I V I T N A Ň

N A Z E H Á T A J É W E K Ž K

A I Ď A R U T A N G I S L Ř Ň

L A N A L Ý Z A C H O V Á N Í

P J A Ě P K O Č Ň C D G I B Á

P S A K T U A L I Z A C E M Q

V U I Ý Ě Z Š F Y W H É S U Ó

Ú K S D Ť T M Q L Ň T H K Q H

SEZNAM SLOV

SIGNATURA HEURISTIKA SANDBOX ANALÝZACHOVÁNÍ AKTUALIZACE PLANÝPOPLACH IZOLACE ANTIVIRUS

Kontrolní bod 6, alternativa: Přístupné přiřazování slovíček

Přiřaďte každý z 8 slovníčkových pojmů z osmisměrky k jeho správné definici zapsáním písmene (A–H) do prázdného pole.

POJMY SLOVNÍ ZÁSOBY

- **A. SIGNATURA**
- **B. HEURISTIKA**
- **C. SANDBOX**
- **D. ANALÝZACHOVÁNÍ**
- **E. AKTUALIZACE**
- **F. PLANÝPOPLACH**
- **G. IZOLACE**
- **H. ANTIVIRUS**

DEFINICE A POLE K PŘIŘAZENÍ

1. Sledování akcí běžícího softwaru kvůli vzorcům škodlivých operací.
2. Softwarová sada skenující koncová zařízení a chránící je před exploity.
3. Pravidelné stahování definic doplňující databázi hrozeb.
4. Analýza založená na pravidlech označující soubory s podezřelou strukturou kódu.
5. Uzavření podezřelých souborů, aby se zabránilo ohrožení místního systému.
6. Jedinečný kryptografický otisk v databázi používaný k identifikaci známých hrozeb.
7. Zabezpečené virtuální testovací prostředí bezpečně spouštějící nedůvěryhodný kód.
8. Bezpečnostní upozornění, které mylně označí bezpečný software za malware.

Kontrolní bod 7: Výzva s přeházenými slovy

Přeuspořádejte písmena níže a odhalte klíčové pojmy a termíny kybernetické bezpečnosti. Odpovědi pište do připravených polí.

1. **TANISURAG**
2. **SNXOBDA**
3. **AILZTKCEAAU**
4. **EZALCIO**
5. **ISAERTIHKU**
6. **ZAVÝAÁCNOANHÍL**
7. **PLÝPLOHACAPN**
8. **SVUAINIRT**

Bonusová aktivita: Mysli rychle

3 ODPOVĚDI V KAŽDÉ KATEGORII. VYHRÁVÁ, KDO PRVNÍ VYPLNÍ CELÝ SEZNAM.

1	Důvody, proč aktualizovat software			
2	Lidé, které můžete požádat o pomoc s IT			
3	Věci, které je třeba udělat, když antivirus něco najde			
4	Známky počítačového viru			
5	Věci, které se dostanou do karantény			
6	Místa, kde se skrývají viry			
7	Informace, které byste nikdy neměli sdílet			
8	Typy škodlivého softwaru			
9	Bezpečnostní nástroje, které znáte			
10	Věci, které antivirus kontroluje			
11	Věci, které si zálohujete			
12	Zařízení, která lze hacknout			
13	Antivirové programy, které znáte			
14	Důvody planých poplachů			
15	Bezpečné návyky, se kterými můžete začít už dnes			

Kontrolní bod 8: Případové studie kyberbezpečnosti

Použijte naučené koncepty k vyřešení níže uvedených reálných scénářů.

PŘÍPADOVÁ STUDIE 1: SKEN PODLE SIGNATUR VS. HEURISTICKÝ SKEN



Scénář: Zaměstnanec si stáhne vlastní utilitu, kterou interně vytvořil jiný tým. Signaturový skener ji propustí, ale heuristický skener ji označí jako podezřelou.

Otázka k diskusi: Vysvětlete, proč k tomu došlo a jak ověřit, zda je soubor bezpečný.

PŘÍPADOVÁ STUDIE 2: ŘEŠENÍ FALEŠNÝCH POPLACHŮ



Scénář: Softwarový vývojář zkompiluje svou aplikaci. Systémový antivirus označí nový spustitelný soubor jako malware a umístí jej do karantény.

Otázka k diskusi: Popište rizika whitelistování a správný postup řešení.

Kontrolní bod 9: Dešifrování šifry

Profesionál v kyberbezpečnosti chrání síťová aktiva před online útočníky. Pomocí níže uvedeného klíče písmeno–číslo dešifrujte zprávu zapsáním odpovídajících písmen do prázdných polí.

ŠIFROVACÍ KLÍČ PÍSMENO–ČÍSLO

A=1 Á=2 B=3 C=4 Č=5 D=6 Ď=7 E=8 É=9 Ě=10 F=11 G=12 H=13 I=14
Í=15 J=16 K=17 L=18 M=19 N=20 Ň=21 O=22 Ó=23 P=24 Q=25 R=26 Ř=27 S=28
Š=29 T=30 Ť=31 U=32 Ú=33 Ů=34 V=35 W=36 X=37 Y=38 Ý=39 Z=40 Ž=41

22 6 13 1 18 30 8 20 22 35 39 19 1 18 36 1 26 8

13 8 32 26 14 28 30 14 4 17 22 32

1 20 1 18 39 40 22 32 17 23 6 32

Dešifrovaná zpráva:

TIP: KAŽDÉ ČÍSLO PŘEDSTAVUJE POZICI DANÉHO PÍSMENE V ABECEDĚ (NAPŘ. 1 = A, 2 = B, 41 = Ž).

Kontrolní bod 10: Základní časté otázky ke kyberbezpečnosti (část A)

Projděte si časté otázky a odpovědi ohledně zmírňování online hrozeb.

Q1: Jak antivirový software rozpoznává malware?

Identifikuje malware pomocí porovnávání signatur v databázi, heuristické analýzy struktury kódu a behaviorálního monitorování v reálném čase.

Q2: Co je detekce založená na signaturách?

Je to metoda skenování, která porovnává kryptografické haše souborů s databázovými seznamy známých malwarových hrozeb.

Q3: Co je heuristický skener?

Heuristika analyzuje strukturu souboru a instrukce kódu a označuje podezřelé vzory běžné u variant malwaru.

Q4: Co znamená, že je soubor v karanténě?

Antivirus přesune soubor do zabezpečené izolované složky a zablokuje jeho spuštění, aby ochránil operační systém.

Q5: Co je falešný poplach antiviru?

Je to chyba, kdy je legitimní, bezpečný software nesprávně označen skenovacími algoritmy za malware.

Kontrolní bod 10: Základní časté otázky ke kyberbezpečnosti (část B)

Projděte si časté otázky a odpovědi ohledně zmírňování online hrozeb.

Q6: Jak monitorování chování chrání systémy?

Monitoruje běžící software v reálném čase a blokuje procesy, které se pokoušejí o podezřelé změny, jako je injektáž kódu.

Q7: Proč je testování v sandboxu důležité?

Sandboxing spouští nedůvěryhodné soubory v izolovaném virtuálním stroji a bezpečně sleduje jejich akce bez vystavení systému.

Q8: Jak často se mají aktualizovat antivirové definice?

Skenery by měly aktualizovat definice denně nebo každou hodinu, aby rozpoznaly nově objevené kmeny malwaru.

Q9: Jaký je rozdíl mezi antivirem a EDR?

Antivirus se zaměřuje na skenování souborů, zatímco Endpoint Detection and Response (EDR) poskytuje sledování a izolaci hrozeb v celé síti.

Q10: Mohu spustit dva antivirové programy zároveň?

Ne. Provoz dvou aktivních skenerů způsobuje systémové konflikty, zpomaluje výkon a mohou si navzájem blokovat operace.

Kontrolní bod 10: Pokročilé časté otázky k bezpečnosti (část C)

Prozkoumejte pokročilé technické aspekty bezpečnostních rámců, analýzy malwaru a datové compliance.

Q1: Jak heuristická pravidla minimalizují obcházení hrozeb?

Heuristika analyzuje obecné vzory hrozeb místo konkrétních signatur a zachycuje upravené varianty známých rodin malwaru.

Q2: Co je polymorfní virus?

Je to malware, který mění strukturu souboru a dešifrovací rutinu při každém spuštění, čímž činí skenování signatur neúčinným.

Q3: Jak sandboxy odhalují únikové techniky proti VM?

Moderní sandboxy simulují kliknutí myší a dobu běhu systému, čímž klamou malware navržený tak, aby se ve virtuálních strojích skrýval.

Q4: V jakých formátech se stahují aktualizace signatur?

Aktualizace jsou obvykle lehké přírůstkové binární diffy, které minimalizují spotřebu šířky pásma klienta.

Q5: Jak agenti na koncových bodech spravují lokální skeny?

Agenti provádějí odlehčené kontroly na pozadí a hluboké kryptografické vyhledávání hašů přenechávají cloudovým databázím hrozeb.

Kontrolní bod 10: Pokročilé časté otázky k bezpečnosti (část D)

Prozkoumejte pokročilé technické aspekty bezpečnostních rámců, analýzy malwaru a datové compliance.

Q6: Co je skenování k detekci rootkitů?

Skenuje paměťové tabulky na úrovni jádra a obchází API operačního systému, která rootkity háčkují ke skrytí svých aktivních vláken.

Q7: Jak skenování chování blokuje ransomware?

Detekuje automatizované smyčky hromadného šifrování souborů a ukončí hostitelský proces dříve, než jsou systémové databáze uzamčeny.

Q8: Co je ověřování podpisových certifikátů kódu?

Skenery porovnávají digitální podpisy kódu s důvěryhodnými kořenovými certifikačními autoritami a ověřují identitu vývojáře softwaru.

Q9: Jak packery ovlivňují skenovací enginy?

Packery komprimují nebo šifrují payloady malwaru. Skenery musí soubor před porovnáváním signatur rozbalit v paměti.

Q10: Jak nástroje EDR automatizují izolaci?

Agenti EDR umísťují kompromitované koncové body do karantény na úrovni sítě, blokují laterální pohyb a přitom umožňují přístup analytikům.

Část 11: 10 faktů a poznatků o kyberbezpečnosti z praxe

Projděte si fakta z praxe o bezpečnostních incidentech, obranných mechanismech a standardech souladu.

1. BEZPEČNOSTNÍ POSTŘEH

Databáze signatur ukládají hashe známého malwaru, takže zcela nové nebo upravené soubory unikají detekci, dokud se definice neaktualizují.

2. BEZPEČNOSTNÍ POSTŘEH

Heuristické motory dokážou označit některé nové varianty malwaru dříve, než existují signatury, za cenu více falešných poplachů.

3. BEZPEČNOSTNÍ POSTŘEH

Falešně pozitivní upozornění stojí IT týmy čas strávený ověřováním a obnovou souborů, které byly chybně umístěny do karantény.

4. BEZPEČNOSTNÍ POSTŘEH

Polymorfní malware mění s každou kopií svůj kód, takže obránci kombinují signatury s heuristickými a behaviorálními kontrolami.

6. BEZPEČNOSTNÍ POSTŘEH

Autoři malwaru píší vlastní kód, který kontroluje sandboxová prostředí a odkládá spuštění, aby obešel časovače.

5. BEZPEČNOSTNÍ POSTŘEH

Cloudové antivirové enginy porovnávají hashe podezřelých souborů s rozsáhlými online databázemi hrozeb téměř v reálném čase.

7. POSTŘEH K BEZPEČNOSTI

Dodavatelé pravidelně posílají na koncové body aktualizace definic, aby skenery rozpoznaly nově potvrzené hrozby.

8. POSTŘEH K BEZPEČNOSTI

Behaviorální monitory ransomwaru se zaměřují na konkrétní volání Win32 API spojená se šifrováním souborů a mazáním stínových kopií.

9. POSTŘEH K BEZPEČNOSTI

Platné podpisy kódu mohou snížit riziko falešných poplachů, ale podepsané soubory se přesto skenují, protože podepsaný může být i malware.

10. BEZPEČNOSTNÍ POSTŘEH

Rootkity upravují struktury jádra systému a k jejich detekci a odstranění jsou potřeba specializované skenery spouštěné při startu.

Technické reference a zdroje

Studijní příručka a interaktivní hádanky jsou sestaveny z globálních standardů NIST, OWASP a předpisů o ochraně osobních údajů. AKADEMICKÉ A OBOROVÉ REFERENCE

AKADEMICKÉ A OBOROVÉ REFERENCE

[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

Klíč odpovědí: Kontrolní bod 1 - Výběr z možností

1 **Otázka 1** SIGNATURY **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Skenování podle signatur spoléhá na známé hashe v databázi a nedokáže odhalit neznámý nebo upravený malware.

2 **Otázka 2** HEURISTICS **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Heuristika analyzuje strukturu kódu a příkazy, aby identifikovala podezřelé rysy nových variant hrozeb.

3 **Otázka 3** SANDBOXING **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Sandbox spouští podezřelé soubory v izolovaném virtuálním stroji, aby bylo možné bezpečně sledovat jejich chování.

4 **Otázka 4** BEHAVIORÁLNÍ **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Behaviorální skenování sleduje běžící programy v reálném čase a blokuje neoprávněné změny systému.

5 **Otázka 5** AKTUALIZACE **Správná odpověď: A**

POZNÁMKA PRO VYUČUJÍCÍ

Skenery denně stahují přírůstkové aktualizace definic, aby držely krok s vývojem hrozeb.

Klíč odpovědí: Kontrolní bod 2 - Pravda, nebo nepravda

6 **Otázka 6** SIGNATURY **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Nástroje založené na signaturách počítají kryptografické hashe a porovnávají je s databází známých hrozeb.

7 **Otázka 7** HEURISTICS **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Heuristické enginy používají pravidlové vzory, které mohou označit legitimní, bezpečné soubory za podezřelé.

8 **Otázka 8** SANDBOXING **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Sandbox spouští kód ve virtuálním kontejneru a striktně blokuje přístup k síťovým sdílením.

9 **Otázka 9** BEHAVIORÁLNÍ **Správná odpověď: Pravda**

POZNÁMKA PRO VYUČUJÍCÍ

Monitorování v reálném čase označuje běžící procesy, které se pokoušejí o nepovolené zápisy nebo zamykání souborů.

10 **Otázka 10** **Správná odpověď: Nepravda**

POZNÁMKA PRO VYUČUJÍCÍ

Žádný antivirus nezastaví každý útok zero-day; neznámé hrozby mohou obejít signatury i heuristiku.

Klíče slovní zásoby a hodnoticí rubrika

Hodnoticí rubrika pro vyučující: Udělte 1 bod za každé správné přiřazení (celkem 8 bodů) a kontextový termín (celkem 6 bodů).

KONTROLNÍ BOD 4: KLÍČ K PŘIŘAZOVÁNÍ POJMŮ

D 1. Hash podpis	G 2. Heuristika kódu	E 3. Souborový sandbox	C 4. Sken chování
F 5. Denní aktualizace	H 6. Falešně pozitivní nález	A 7. Izolace hrozeb	B 8. Antivirový nástroj

KONTROLNÍ BOD 3: KLÍČ KE KLÍČOVÝM POJMŮM

1 SIGNATURA	2 HEURISTICKÁ ANALÝZA	3 SANDBOX	4 CHOVÁNÍ
5 AKTUALIZACE	6 FALEŠNĚ POZITIVNÍ NÁLEZ		

KONTROLNÍ BOD 6, ALTERNATIVA: KLÍČ K PŘIŘAZOVÁNÍ SLOV

1 D – ANALÝZACHOVÁNÍ	2 H – ANTIVIRUS	3 E – AKTUALIZACE	4 B – HEURISTIKA
5 G – IZOLACE	6 A – SIGNATURA	7 C – SANDBOX	8 F – PLANÝPOPLACH

POZNÁMKY K DISKUSI PRO VYUČUJÍCÍ

Klíčové pojmy:
Ověřte, že studenti umí vlastními slovy vysvětlit pojmy Hash podpis, Heuristika kódu a Souborový sandbox a ke každému uvést příklad.

Případové studie:
Požádejte studenty, aby svá doporučení zdůvodnili fakty z pracovního listu, nikoli domněnkami.

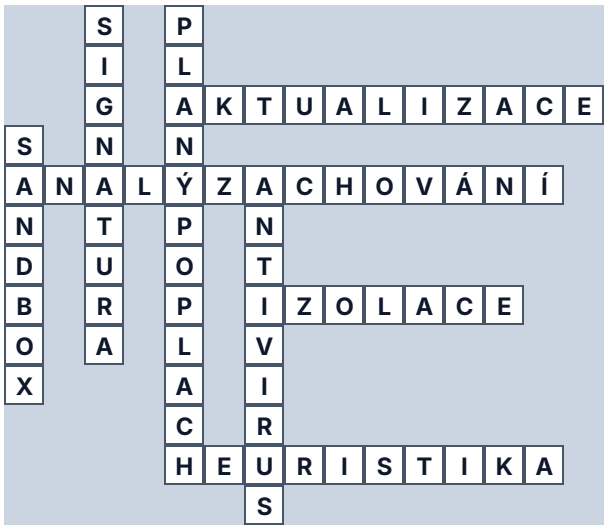
Práce se zdroji:
Nechte studenty ověřit alespoň jedno tvrzení proti referencím v pracovním listu a proberte, proč se čísla, ceny a pravidla mohou v čase měnit.

Klíče k úlohám a poznámky pro vyučující

ŘEŠENÍ OSMISMĚRKY

H	Ž	N	K	V	Š	Ú	Á	Š	X	J	N	N	G	H
C	Ň	A	K	I	T	S	I	R	U	E	H	H	S	Ě
A	L	Ť	M	S	A	N	D	B	O	X	S	X	H	B
L	Ú	É	Ý	Ó	Z	X	E	T	G	Ť	Y	A	Q	Ú
P	O	O	Z	P	H	C	R	Ť	H	Q	Ů	U	P	Ú
O	U	K	A	E	A	P	Ň	L	Á	O	Ů	Ě	F	R
P	Ř	X	Ý	L	J	J	Ů	J	Z	W	Y	Q	J	I
Ý	Ž	I	O	Í	S	U	R	I	V	I	T	N	A	Ň
N	A	Z	E	H	Á	T	A	J	É	W	E	K	Ž	K
A	I	Ď	A	R	U	T	A	N	G	I	S	L	Ř	Ň
L	A	N	A	L	Ý	Z	A	C	H	O	V	Á	N	Í
P	J	A	Ě	P	K	O	Č	Ň	C	D	G	I	B	Á
P	S	A	K	T	U	A	L	I	Z	A	C	E	M	Q
V	U	I	Ý	Ě	Z	Š	F	Y	W	H	É	S	U	Ó
Ú	K	S	D	Ť	T	M	Q	L	Ň	T	H	K	Q	H

ŘEŠENÍ KŘÍŽOVKY



VODOROVNÉ NÁPOVĚDY

3 vodorovně: AKTUALIZACE Pravidelné stahování definic doplňující databázi hrozeb (11 písmen)

5 vodorovně: ANALÝZACHOVÁNÍ Sledování akcí běžícího softwaru kvůli vzorcům škodlivých operací (14 písmen)

7 vodorovně: IZOLACE Uzavření podezřelých souborů, aby se zabránilo ohrožení místního systému (7 písmen)

8 vodorovně: HEURISTIKA Analýza založená na pravidlech označující soubory s podezřelou strukturou kódu (10 písmen)

SVISLÉ NÁPOVĚDY

1 svisle: SIGNATURA Jedinečný kryptografický otisk v databázi používaný k identifikaci známých hrozeb (9 písmen)

2 svisle: PLANÝPOPLACH Bezpečnostní upozornění, které mylně označí bezpečný software za malware (12 písmen)

4 svisle: SANDBOX Zabezpečené virtuální testovací prostředí bezpečně spouštějící nedůvěryhodný kód (7 písmen)

6 svisle: ANTIVIRUS Softwarová sada skenující koncová zařízení a chránící je před exploity (9 písmen)

Klíč řešení přesmyček a šifry

Klíč k hodnocení aktivity s přesmyčkami slovní zásoby a výzvy Tajná šifra.

KLÍČ K PŘESMYČKÁM

1. TANISURAG — **SIGNATURA**
2. SNXOBDA — **SANDBOX**
3. AILZTKCEAAU — **AKTUALIZACE**
4. EZALCIO — **IZOLACE**
5. ISAERTIHKU — **HEURISTIKA**
6. ZAVÝAÁCNOANHÍL — **ANALÝZACHOVÁNÍ**
7. PLÝPLOHACAPN — **PLANÝPOPLACH**
8. SVUAINIRT — **ANTIVIRUS**

KLÍČ TAJNÉ ŠIFROVACÍ VÝZVY

"ODHALTE NOVÝ MALWARE HEURISTICKOU ANALÝZOU KÓDU"

Klíč k případovým studiím

A Případová studie 1: Sken podle signatur vs. heuristický sken

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Zaměstnanec si stáhne interní utilitu vytvořenou jiným týmem. Signaturový skener ji propustí, ale heuristický skener ji označí jako podezřelou.
- Doporučená strategie a řešení: Proč k tomu došlo: Signaturové skenování kontroluje hashe souborů; jelikož jde o vlastní software, v databázi hrozeb není. Heuristika analyzuje strukturu a označila podezřelé akce (např. zápisy do registru). Ověření: Spusťte soubor v sandboxu a sledujte jeho chování, zkontrolujte digitální podpisy a odešlete hash na portály threat intelligence.

B Případová studie 2: Řešení falešných poplachů

Řešení pro vyučující

POKYNY K HODNOCENÍ

Odpovědi studentů by měly pokrýt následující body:

- Analýza scénáře: Softwarový vývojář zkompiluje svou aplikaci. Systémový antivirus nový spustitelný soubor označí jako malware a umístí do karantény.
- Doporučená strategie a řešení: Rizika whitelistingu: Obcházení skenerů může pustit ke spuštění skutečně infikovaný kód. Postup řešení: Odešlete soubor výrobci antiviru k analýze, digitálně podepište kód pomocí certifikačních autorit a dočasně nastavte výjimky pro konkrétní složky místo vypínání antiviru.