Emri: _____ Data: _____ Pikët: _____

Softueri antivirus dhe pikat fundore Udhëzues mbrojtjeje

Zbulimi me nënshkrime, heuristika, monitorimi i sjelljes, sandboxing, përditësimet

PËRMBLEDHJE MËSIMORE PËR SOFTUERIN ANTIVIRUS

I SIGURUAR

ENKRIPTIMI I TË DHËNAVE

Standardi AES 256-bit

I PËRPUTHSHËM

STANDARDET GLOBALE

Kornizat GDPR dhe CCPA

ZERO-TRUST

POLITIKA E QASJES

Autentikim me shumë faktorë

Mirë se vjen! Kjo paketë aktivitetesh të udhëheq përmes softuerit antivirus dhe mbrojtjes së pikave fundore. Do të eksplorosh bazat e të dhënave të firmave, skanerët heuristikë, monitorimin e sjelljes, skedarët virtualë në sandbox dhe zbutjen e pozitivëve të rremë.

PIKAT E KONTROLLIT TË FLETËS SË PUNËS

- [ ] **Pjesët 1-4: Zotëro sigurinë kibernetike dhe parandalimin e kërcënimeve.**
- [ ] **Pjesët 5-7: Zgjidh fjalëkryqe dhe enigma me kërkim fjalësh.**
- [ ] **Pjesët 8-9: Zgjidh studime rasti dhe sfidën e kodit.**
- [ ] **Pjesa 10: Shqyrto faqet e pyetjeve të shpeshta bazë dhe të avancuara.**
- [ ] **Pjesa 11: Eksploro 10 fakte interesante nga bota reale.**
- [ ] **Bonus: sfida Mendo shpejt.**

Hap Udhëzuesin VPN.com për sigurinë kibernetike

URL: https://www.vpn.com/sq/siguria-kibernetike/antivirus/

Udhërrëfyesi yt mësimor për strategjinë e antivirusit

- Dallo mes zbulimit të malware-it të bazuar në nënshkrime dhe atij të bazuar në heuristikë.
- Kupto protokollet e monitorimit të sjelljes dhe të izolimit në sandbox.
- Vlerëso ndikimet e skanimit në kohë reale në performancën e sistemit dhe të pikave fundore.
- Zbut klasifikimet false pozitive duke përdorur verifikimin e certifikatave dixhitale.
- Menaxho shpërndarjen ditore të përditësimeve të përkufizimeve nëpër pikat fundore korporative.

UDHËZIME PËR UDHËZUESIN E ANTIVIRUSIT

Përgjigju pyetjeve me zgjedhje të shumëfishtë dhe pyetjeve E vërtetë/E gabuar, plotëso fjalitë me vende bosh duke përdorur bankën e fjalëve, përputh përkufizimet dhe zgjidh fjalëkryqin dhe enigmën e kërkimit të fjalëve. Zbato njohuritë e tua për sigurinë antivirus të pikave fundore. Përfundo me aktivitetin bonus Mendo shpejt.

MBROJTJA ME ANTIVIRUS DHE SKANIMI I NËNSHKRIMEVE (HYRJE)

Softueri antivirus mbron pikat fundore duke identifikuar, karantinuar dhe hequr malware-in. Sistemet moderne kombinojnë bazat e të dhënave të nënshkrimeve (që përputhin hash-et e kërcënimeve të njohura) me heuristikat (që analizojnë strukturën e skedarit) dhe monitorimin e sjelljes për të zbuluar sulmet zero-day.

LEXO ÇDO PIKË KONTROLLI ME KUJDES DHE ZGJIDH OSE SHKRUAJ PËRGJIGJEN E

Pika e kontrollit 1: Sfida me zgjedhje të shumëfishtë

1. Cili është një kufizim i zbulimit të bazuar në nënshkrime?

- A. Nuk mund të identifikojë malware të panjohur ose të modifikuar
- B. Gjeneron shkallë të larta pozitivësh të rremë
- C. Kërkon fuqi të lartë përpunuese të CPU-së
- D. Funksionon vetëm kur është i lidhur me internetin

2. Si i zbulojnë skanerët heuristikë variantet e reja të malware-it?

- A. Duke identifikuar modele të dyshimta dhe struktura kodi
- B. Duke përputhur hash-et e skedarëve me një bazë të dhënash kërcënimesh
- C. Duke fshirë automatikisht të gjithë ekzekutuesit e pa nënshkruar
- D. Duke ngarkuar çdo skedar në një dosje publike cloud

3. Cili është qëllimi i ekzekutimit në sandbox të antivirusit?

- A. Izolimi dhe analizimi i skedarëve në një kasafortë të sigurt virtuale
- B. Përshpejtimi i transferimit të kopjes rezervë të sistemit lokal të skedarëve
- C. Përditësimi i arnimeve të sigurisë së sistemit operativ lokal
- D. Ngjeshja e skedarëve të mëdhenj të dokumenteve për të kursyer hapësirë

4. Cila metodë zbulimi shënon sjelljen e kërcënimeve në kohë reale?

- A. Analiza e sjelljes që monitoron veprimet e softuerit
- B. Inspektim historik i logjeve i kryer gjatë natës
- C. Ndërhyrje manuale e përdoruesit që raporton aplikacione të ngadalta
- D. Rishikime manuale javore të programeve të instaluara

5. Pse janë kritike përditësimet e rregullta të përkufizimeve për skanerët?

- A. Për të ushqyer motorët e nënshkrimeve me identifikues kërcënimesh nga baza e të dhënave
- B. Për të rritur frekuencat e orës së CPU-së gjatë operacioneve
- C. Për të ndryshuar kohët globale të ruajtjes në cache të serverëve të emrave DNS
- D. Për të autorizuar cilësimet e cookie-ve të shfletuesit

Pika e kontrollit 2: Sfida: E vërtetë ose e gabuar

6 Pyetje E/G 6

6. Zbulimi me nënshkrime përputh hash-et kriptografike të skedarëve me listat e bazave të të dhënave.

E vërtetë E gabuar

7 Pyetje E/G 7

7. Skanerët heuristikë mund të shkaktojnë alarme të rreme pozitive në skedarë të sigurt.

E vërtetë E gabuar

8 Pyetje E/G 8

8. Një sandbox i lejon malware-it të aksesojë skedarët e rrjetit pa kufizime.

E vërtetë E gabuar

9 Pyetje E/G 9

9. Skanimi sipas sjelljes bllokon skedarët kur shfaqin veprime keqdashëse.

E vërtetë E gabuar

10 Pyetje E/G 10

10. Softueri standard antivirus i ndalon plotësisht të gjitha sulmet zero-day.

E vërtetë E gabuar

Pika e kontrollit 3: Futja e termave kryesorë

Lexo secilën fjali më poshtë dhe plotëso vendin bosh me termin e saktë nga Banka e Fjalëve.

1. Skaneri tradicional identifikon malware-in e njohur duke përdorur përputhjen me një _____ unik.

2. Analizimi i modeleve të kodit të skedarëve quhet skanim me _____ .

3. Mjetet antivirus i izolojnë skedarët e dyshimtë në një mjedis _____ .

4. Skanimi në kohë reale i bazuar në _____ vëzhgon veprimet e programeve për aktivitete të dyshimta.

5. Skanerët shkarkojnë çdo ditë _____ të bazës së të dhënave për të njohur kërcënime të reja.

6. Programet e sigurta të shënuara si malware shkaktojnë një _____ .

BANKA E FJALËVE TË LEKSIKUT

ALARM I RREMË ANTIVIRUS FIREWALL HEURISTIKË KODI NËNSHKRIM HASH PËRDITËSIME SANDBOX SJELLJE

Shkruaj përgjigjet e tua këtu:

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

Pika e kontrollit 4: Përputhja e koncepteve të sigurisë

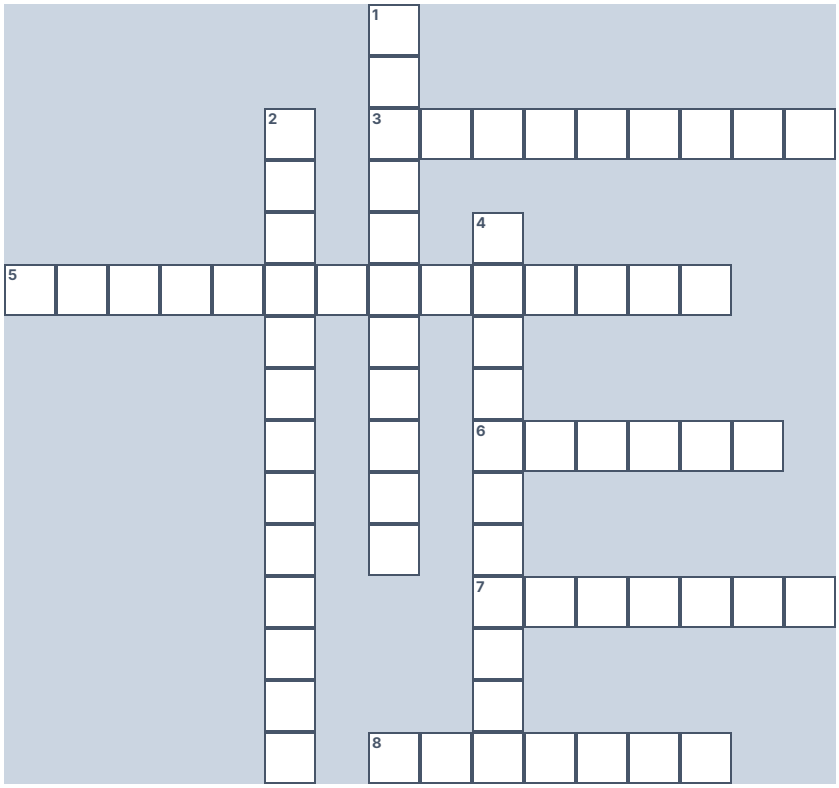
PËRPUTHJA E PËRKUFIZIMEVE

Përputh çdo term fjalori në të majtë me përkufizimin e tij të saktë në të djathtë, duke shkruar shkronjën përkatëse (A-H) në kutinë e plotësueshme.

☐	1. Nënshkrimi hash	A	Izolimi i skedarëve të dyshimtë për të parandaluar ekspozimin e sistemit lokal.
☐	2. Heuristika e kodit	B	Paketë softueri që skanon dhe mbron pikat fundore nga shfrytëzimet.
☐	3. Sandbox skedarësh	C	Monitorimi i veprimeve të softuerit në ekzekutim për modele operimi keqdashëse.
☐	4. Skanimi i sjelljes	D	Gjurmë unike kriptografike e bazës së të dhënave që përdoret për të identifikuar kërcënime të njohura.
☐	5. Përditësime ditore	E	Mjedis virtual i sigurt testimi që ekzekuton kod të pabesueshëm në mënyrë të sigurt.
☐	6. Pozitiv i rremë	F	Shkarkime të rregullta përkufizimesh që ushqejnë bazën e të dhënave të kërcënimeve.
☐	7. Izolimi i kërcënimeve	G	Analizë e bazuar në rregulla që shënon skedarët me struktura të dyshimta kodi.
☐	8. Mjet antivirus	H	Alarm sigurie që klasifikon gabimisht softuer të sigurt si malware.

Pika e kontrollit 5: Fjalëkryq

Zgjidhe fjalëkryqin duke shkruar shkronja në kutitë e bardha aktive. Numrat korrespondojnë me indiciet më poshtë.



HORIZONTALISHT

3. Paketë softuerike që skanon dhe mbron pajisjet fundore nga eksploitet (9)

5. Analizë e bazuar në rregulla që sinjalizon skedarët me struktura të dyshimta kodi (14)

6. Mbyllja e skedarëve të dyshimtë në një hapësirë të kufizuar për të parandaluar ekspozimin e sistemit lokal (6)

7. Mjedis i sigurt virtual testimi që ekzekuton kodin e pabesuar në mënyrë të sigurt (7)

8. Veprimet e softuerit që po ekzekutohet, të monitoruara për modele veprimi keqdashëse (7)

VERTIKALISHT

1. Sinjalizim sigurie që klasifikon gabimisht softuer të sigurt si malware (11)

2. Gjurmë kriptografike unike në bazën e të dhënave që përdoret për të identifikuar kërcënimet e njohura (13)

4. Shkarkime të rregullta të përkufizimeve që ushqejnë bazën e të dhënave të kërcënimeve (11)

Pika e kontrollit 5, alternativa: Çelësa të aksesueshëm të fjalëkryqit

Përdoruesit e lexuesve të ekranit dhe të tastierës mund t'i shkruajnë përgjigjet e fjalëkryqit drejtpërdrejt në fushat e tekstit më poshtë. INDICIET HORIZONTALE INDICIET VERTIKALE

HORIZONTALISHT

3 horizontalisht: Paketë softuerike që skanon dhe mbron pajisjet fundore nga eksploitet (9 shkronja):

5 horizontalisht: Analizë e bazuar në rregulla që sinjalizon skedarët me struktura të dyshimta kodi (14 shkronja):

6 horizontalisht: Mbyllja e skedarëve të dyshimtë në një hapësirë të kufizuar për të parandaluar ekspozimin e sistemit lokal (6 shkronja):

7 horizontalisht: Mjedis i sigurt virtual testimi që ekzekuton kodin e pabesuar në mënyrë të sigurt (7 shkronja):

8 horizontalisht: Veprimet e softuerit që po ekzekutohet, të monitoruara për modele veprimi keqdashëse (7 shkronja):

VERTIKALISHT

1 vertikalisht: Sinjalizim sigurie që klasifikon gabimisht softuer të sigurt si malware (11 shkronja):

2 vertikalisht: Gjurmë kriptografike unike në bazën e të dhënave që përdoret për të identifikuar kërcënimet e njohura (13 shkronja):

4 vertikalisht: Shkarkime të rregullta të përkufizimeve që ushqejnë bazën e të dhënave të kërcënimeve (11 shkronja):

Pika e kontrollit 6: Kërkimi i fjalës së fshehur

Gjej 8 termat kyç të fjalorit të fshehur në rrjetën më poshtë. Fjalët mund të jenë horizontale, vertikale ose diagonale.

H J S Q U P Z D G E Q C A J O

S Ë M E R R I M R A L A C S S

A Z K I I Z O L I M U Q J A T

H A R V I K K F F L G E N P Ë

M J S J Q V F B T E L D Y M Y

I V R F S X A O T L B M M Z N

R G O S G N T T J O N T S I A

K D N L J A M E X U Ë Ë O P X

H Y I I T I Y V X N I G Z H H

S L A S U R I V I T N A E G A

N H E U R I S T I K Ë K O D I

Ë R A I E V D I Z I D J P L I

N A P Ë R D I T Ë S I M E E N

I M Ç L C Ç F G B B N Q K O U

S G Y E Y Q F X V G E P S M T

LISTA E FJALËVE TË LEKSIKUT

NËNSHKRIMHASH HEURISTIKË KODI SANDBOX SJELLJE PËRDITËSIME ALARM IRREMË IZOLIM ANTIVIRUS

Pika e kontrollit 6, alternativa: Përputhja e aksesueshme e fjalorit

Përputh secilin nga 8 termat e fjalorit nga Kërkimi i fjalëve me përkufizimin e saktë të tij, duke shkruar shkronjën (A-H) në vendin bosh.

TERMA LEKSIKORË

- **A. NËNSHKRIMHASH**
- **B. HEURISTIKËKODI**
- **C. SANDBOX**
- **D. SJELLJE**
- **E. PËRDITËSIME**
- **F. ALARMIRREMË**
- **G. IZOLIM**
- **H. ANTIVIRUS**

PËRKUFIZIME DHE FUSHA PËRPUTHJEJE

1. Veprimet e softuerit që po ekzekutohet, të monitoruara për modele veprimi keqdashëse.
2. Paketë softuerike që skanon dhe mbron pajisjet fundore nga eksploitet.
3. Shkarkime të rregullta të përkufizimeve që ushqejnë bazën e të dhënave të kërcënimeve.
4. Analizë e bazuar në rregulla që sinjalizon skedarët me struktura të dyshimta kodi.
5. Mbyllja e skedarëve të dyshimtë në një hapësirë të kufizuar për të parandaluar ekspozimin e sistemit lokal.
6. Gjurmë kriptografike unike në bazën e të dhënave që përdoret për të identifikuar kërcënimet e njohura.
7. Mjedis i sigurt virtual testimi që ekzekuton kodin e pabesuar në mënyrë të sigurt.
8. Sinjalizim sigurie që klasifikon gabimisht softuer të sigurt si malware.

Pika e kontrollit 7: Sfida e fjalëve të përzier

Rirenditi shkronjat më poshtë për të zbuluar konceptet dhe termat kryesorë të sigurisë kibernetike. Shkruaji përgjigjet në kutitë e dhëna.

1. RNMSKËIHNA HHS

2. SNXOBDA

3. PËTSRËMEIID

4. MLOIIZ

5. ËUOEIKIISKT HDR

6. JELSLEJ

7. RMALRËEMAI R

8. SVUAINIRT

Aktivitet bonus: Mendo shpejt

3 PËRGJIGJE PËR ÇDO KATEGORI. FITON KUSH E PLOTËSON I PARI LISTËN.

1	Arsye për të përditësuar softuerin			
2	Njerëz që mund t'i pyesësh për ndihmë me IT-në			
3	Gjëra që bëhen kur antivirusi gjen diçka			
4	Shenja të një virusi kompjuterik			
5	Gjëra që vihen në karantinë			
6	Vende ku fshihen virusët			
7	Informacione që nuk duhet t'i ndash kurrë			
8	Lloje softueri keqdashës			
9	Mjete sigurie që njeh			
10	Gjëra që skanon një antivirus			
11	Gjëra që ruan si kopje rezervë			
12	Pajisje që mund të hakohen			
13	Programe antivirus që njeh			
14	Arsye për alarme të rreme			
15	Zakone të sigurta që mund t'i fillosh sot			

Pika e kontrollit 8: Studime rasti për sigurinë kibernetike

Zbato konceptet që ke mësuar për të zgjidhur skenarët reale më poshtë.

STUDIMI I RASTIT 1: SKANIMI ME NËNSHKRIME KUNDREJT ATIJ HEURISTIK



Skenari: Një punonjës shkarkon një mjet të përshtatur që e ka ndërtuar një ekip tjetër brenda kompanisë. Skaneri me nënshkrime e kalon, por skaneri heuristik e shënon si të dyshimtë.

Pyetje për diskutim: Shpjego pse ndodhi kjo dhe si mund të verifikohet nëse skedari është i sigurt.

STUDIMI I RASTIT 2: TRAJTIMI I POZITIVEVE TË RREME



Skenari: Një zhvillues softueri kompilon aplikacionin e tij. Antivirusi i sistemit e shënon skedarin e ri ekzekutues si malware dhe e vë në karantinë.

Pyetje për diskutim: Përshkruaj rreziqet e vendosjes në listën e bardhë dhe përshkruaj rrugën e saktë të zgjidhjes.

Pika e kontrollit 9: Deshifrimi i kodit

Një profesionist i sigurisë kibernetike mbron asetet e rrjetit nga aktorët e kërcënimeve online. Përdor çelësin shkronjë-numër më poshtë për të deshifruar mesazhin duke shkruar shkronjat përkatëse në hapësirat e zbrazëta.

ÇELËSI I ENKRIPTIMIT SHKRONJË-NË-NUMËR

A=1 B=2 C=3 Ç=4 D=5 E=6 Ë=7 F=8 G=9

H=10 I=11 J=12 K=13 L=14 M=15 N=16 O=17 P=18

Q=19 R=20 S=21 T=22 U=23 V=24 X=25 Y=26 Z=27

27	2	23	14	17		13	17	5		22	7		5	7	15	21	10	7	15

22	7		20	11		15	6		10	6	23	20	11	21	22	11	13	7

Mesazhi i deshifruar:

KËSHILLË: ÇDO NUMËR PËRFAQËSON POZICIONIN E ASAJ SHKRONJE NË ALFABET (P.SH. 1 = A, 2 = B, 27 = Z).

Pika e kontrollit 10: Pyetje të shpeshta bazë për sigurinë kibernetike (Pjesa A)

Rishiko pyetje dhe përgjigje të zakonshme për zbutjen e kërcënimeve në internet.

Q1: Si e identifikon softueri antivirus malware-in?

Identifikon malware-in duke përdorur përputhjen e nënshkrimeve nga bazat e të dhënave, analizën heuristike të strukturës së kodit dhe monitorimin e sjelljes në kohë reale.

Q2: Çfarë është zbulimi i bazuar në nënshkrime?

Është një metodë skanimi që përputh hash-et kriptografike të skedarëve me lista në baza të dhënash të kërcënimeve të njohura të malware-it.

Q3: Çfarë është një skaner heuristik?

Heuristika analizon strukturën e një skedari dhe udhëzimet e kodit, duke shënuar modele të dyshimta të zakonshme te variantet e malware-it.

Q4: Çfarë do të thotë kur një skedar vendoset në karantinë?

Antivirusi e zhvendos skedarin në një dosje të sigurt e të izoluar, duke bllokuar ekzekutimin për të mbrojtur sistemin operativ.

Q5: Çfarë është një e rreme pozitive e antivirusit?

Është një gabim ku softueri legjitim dhe i sigurt shënohet gabimisht si malware nga algoritmet e skanimit.

Pika e kontrollit 10: Pyetje të shpeshta bazë për sigurinë kibernetike (Pjesa B)

Rishiko pyetje dhe përgjigje të zakonshme për zbutjen e kërcënimeve në internet.

Q6: Si i mbron sistemet monitorimi i sjelljes?

Monitoron softuerin në ekzekutim në kohë reale, duke bllokuar proceset që përpiqen të bëjnë ndryshime të dyshimta si injektimi i kodit.

Q7: Pse është e rëndësishme testimi në sandbox?

Sandboxing i ekzekuton skedarët e pabesueshëm në një makinë virtuale të izoluar, duke vëzhguar veprimet në mënyrë të sigurt pa ekspozim të sistemit.

Q8: Sa shpesh duhet të përditësohen përkufizimet e antivirusit?

Skanerët duhet t'i përditësojnë përkufizimet çdo ditë ose çdo orë për të njohur variantet e malware-it të zbuluara rishtazi.

Q9: Cili është ndryshimi mes antivirusit dhe EDR?

Antivirusi përqendrohet te skanimi i skedarëve, ndërsa Endpoint Detection and Response (EDR) ofron gjurmim dhe izolim të kërcënimeve në të gjithë rrjetin.

Q10: A mund të ekzekutoj dy programe antivirus së bashku?

Jo. Ekzekutimi i dy skanerëve aktivë shkakton konflikte të sistemit, ngadalëson performancën dhe mund të bllokojë operacionet e njëri-tjetrit.

Pika e kontrollit 10: Pyetje të shpeshta të avancuara për sigurinë (Pjesa C)

Eksploro aspektet e avancuara teknike të kornizave të sigurisë, analizës së malware-it dhe pajtueshmërisë me të dhënat.

Q1: Si e minimizojnë kapërcimin e kërcënimeve rregullat heuristike?

Heuristika analizon modele të përgjithshme kërcënimesh në vend të nënshkrimeve specifike, duke kapur variante të modifikuara të familjeve të njohura të malware-it.

Q2: Çfarë është një virus polimorfik?

Është malware që ndryshon strukturën e skedarit dhe rutinën e dekriptimit me çdo ekzekutim, duke i bërë joefektive skanimet e nënshkrimeve.

Q3: Si e zbulojnë sandbox-et shmangien e VM-së?

Sandbox-et moderne simulojnë klikimet e mausit dhe kohën e funksionimit të sistemit, duke mashtruar malware-in e projektuar të fshihet kur ekzekutohet në makina virtuale.

Q4: Cilat janë formatet e shkarkimit të përditësimeve të nënshkrimeve?

Përditësimet janë zakonisht skedarë të lehtë diferencialë binarë shtesë, që minimizojnë konsumin e gjerësisë së brezit të rrjetit të klientit.

Q5: Si i menaxhojnë agjentët e pikës fundore skanimet lokale?

Agjentët kryejnë kontrolle të lehta në sfond, duke ia ngarkuar kërkimet e thella kriptografike të hash-eve bazave të të dhënave të kërcënimeve në cloud.

Pika e kontrollit 10: Pyetje të shpeshta të avancuara për sigurinë (Pjesa D)

Eksploro aspektet e avancuara teknike të kornizave të sigurisë, analizës së malware-it dhe pajtueshmërisë me të dhënat.

Q6: Çfarë është skanimi për zbulimin e rootkit-eve?

Skanon tabelat e memories në nivel kerneli, duke anashkaluar API-t e OS-it që rootkit-et i përgjojnë për të fshehur fijet e tyre aktive.

Q7: Si e bllokon skanimi i sjelljes ransomware-in?

Zbulon sythe të automatizuara të enkriptimit masiv të skedarëve, duke ndërprerë procesin pritës përpara se të bllokohen bazat e të dhënave të sistemit.

Q8: Çfarë është verifikimi i certifikatës së nënshkrimit të kodit?

Skanerët kontrollojnë nënshkrimet digjitale të kodit kundrejt autoriteteve të certifikatave rrënjë të besuara, duke validuar identitetin e zhvilluesit të softuerit.

Q9: Si ndikojnë packer-ët te motorët e skanimit?

Paketuesit (packers) i kompresojnë ose i enkriptojnë ngarkesat e malware-it. Skanerët duhet ta zhpaketojnë skedarin në memorie përpara se të ekzekutohen përputhjet e nënshkrimeve.

Q10: Si e automatizojnë izolimin mjetet EDR?

Agjentët EDR i vendosin në karantinë pikat fundore të kompromentuara në nivel rrjeti, duke bllokuar lëvizjen anësore ndërsa lejojnë qasjen e analistit.

Pjesa 11: 10 fakte dhe njohuri nga bota reale për sigurinë kibernetike

Rishiko fakte reale për shkeljet e sigurisë, mekanizmat e mbrojtjes dhe standardet e pajtueshmërisë.

1. PERSPEKTIVË PËR SIGURINË

Bazat e të dhënave të nënshkrimeve ruajnë hash-e të malware-ve të njohur, ndaj skedarët krejt të rinj ose të ndryshuar humbasin derisa të përditësohen përkufizimet.

2. PERSPEKTIVË PËR SIGURINË

Motorët heuristikë mund të shënojnë disa variante të reja të malware-it përpara se të ekzistojnë nënshkrimet, me koston e më shumë alarmeve të rreme.

3. PERSPEKTIVË PËR SIGURINË

Alarmet e rreme pozitive i kushtojnë ekipeve IT kohë për të verifikuar dhe rikthyer skedarët që u vendosën gabimisht në karantinë.

4. PERSPEKTIVË PËR SIGURINË

Malware-i polimorfik e ndryshon kodin e vet me çdo kopje, prandaj mbrojtësit i çiftojnë nënshkrimet me kontrolle heuristike dhe sjelljeje.

6. PERSPEKTIVË PËR SIGURINË

Autorët e malware-it shkruajnë kode të personalizuara për të kontrolluar mjediset sandbox, duke vonuar ekzekutimin për të anashkaluar kohëmatësit.

5. PERSPEKTIVË PËR SIGURINË

Motorët antivirus cloud i krahasojnë hash-et e skedarëve të dyshimtë me baza të mëdha online kërcënimesh pothuajse në kohë reale.

7. NJOHURI PËR SIGURINË

Shitësit i shtyjnë përditësimet e përkufizimeve te pikat fundore rregullisht, që skanuesit të njohin kërcënimet e sapo konfirmuara.

8. NJOHURI PËR SIGURINË

Monitorët e sjelljes së ransomware synojnë thirrje specifike të API-së Win32 që lidhen me enkriptimin e skedarëve dhe fshirjen e shadow copies.

9. NJOHURI PËR SIGURINË

Nënshkrimet e vlefshme të kodit mund të ulin rrezikun e rezultateve false pozitive, por skedarët e nënshkruar skanohen përsëri, pasi edhe malware mund të nënshkruhet.

10. PERSPEKTIVË PËR SIGURINË

Rootkit-et ndryshojnë strukturat e kernelit të sistemit, duke kërkuar skanerë të specializuar gjatë nisjes për t'i zbuluar dhe pastruar.

Referenca teknike dhe burime

Udhëzuesi i studimit dhe enigmat interaktive janë përpiluar nga standardet globale të NIST, OWASP dhe të pajtueshmërisë me privatësinë e të dhënave. REFERENCA AKADEMIKE DHE INDUSTRIALE

REFERENCA AKADEMIKE DHE TË INDUSTRISË

[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

Çelësi i përgjigjeve: Pika e kontrollit 1 - Zgjedhje e shumëfishtë

1 **Pyetja 1** NËNSHKRIME **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Skanimi me nënshkrime mbështetet te hash-et e njohura të bazës së të dhënave dhe nuk arrin të zbulojë malware të panjohur ose të modifikuar. Citim: OWASP Secure Configuration.

2 **Pyetja 2** HEURISTIKA **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Heuristikat analizojnë strukturën e kodit dhe komandat për të identifikuar veçoritë e dyshimta të varianteve të rinj të kërcënimeve. Citim: Center for Internet Security (CIS).

3 **Pyetja 3** SANDBOXING **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Një sandbox ekzekuton skedarët e dyshimtë në një makinë virtuale të izoluar për të vëzhguar me siguri sjelljen e ekzekutimit. Citim: NIST Digital Identity.

4 **Pyetja 4** SJELLJESOR **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Skanimi i sjelljes monitoron në kohë reale programet që ekzekutohen për të bllokuar ndryshimet e paautorizuara të sistemit. Citim: Center for Internet Security (CIS).

5 **Pyetja 5** PËRDITËSIME **Përgjigjja e saktë: A**

SHËNIM PËR MËSUESIN

Skanerët shkarkojnë përditësime ditore graduale të përkufizimeve për të qëndruar të sinkronizuar me peizazhin e kërcënimeve. Citim: OWASP Secure Configuration.

Çelësi i përgjigjeve: Pika e kontrollit 2 - E vërtetë ose e gabuar

6 **Pyetja 6** NËNSHKRIME **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Mjetet me nënshkrime llogaritin hash-e kriptografike dhe i përputhin me një bazë të dhënash hash-esh të njohura kërcënimesh. Citim: OWASP Secure Configuration.

7 **Pyetja 7** HEURISTIKA **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Motorët heuristikë ekzekutojnë struktura të bazuara në rregulla që mund t'i shënojnë si të dyshimta skedarë legjitimë dhe të sigurt. Citim: Center for Internet Security (CIS).

8 **Pyetja 8** SANDBOXING **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

Një sandbox ekzekuton kodin në një kontejner virtual, duke bllokuar rreptësisht qasjen në ndarjet e rrjetit. Citim: NIST Digital Identity.

9 **Pyetja 9** SJELLJESOR **Përgjigjja e saktë: E vërtetë**

SHËNIM PËR MËSUESIN

Monitorimi në kohë reale shënon proceset që ekzekutohen dhe përpiqen për shkrime të paligjshme ose bllokim skedarësh. Citim: Center for Internet Security (CIS).

10 **Pyetja 10** **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

Asnjë antivirus nuk e ndalon çdo sulm zero-day; kërcënimet e panjohura mund t'i shmangen nënshkrimeve dhe heuristikës.

Çelësat e fjalorit dhe rubrika e vlerësimit

Rubrika e vlerësimit për mësuesin: Jep 1 pikë për çdo përputhje të saktë (8 pikë gjithsej) dhe term konteksti (6 pikë gjithsej).

PIKA E KONTROLLIT 4: ÇELËSI – PËRPUTHJA E KONCEPTEVE

D 1. Nënshkrimi hash	G 2. Heuristika e kodit	E 3. Sandbox skedarësh	C 4. Skanimi i sjelljes
F 5. Përditësime ditore	H 6. Pozitiv i rremë	A 7. Izolimi i kërcënimeve	B 8. Mjet antivirus

PIKA E KONTROLLIT 3: ÇELËSI – TERMAT KRYESORË

1 NËNSHKRIM HASH	2 HEURISTIKË KODI	3 SANDBOX	4 SJELLJE
5 PËRDITËSIME	6 ALARM I RREMË		

PIKA E KONTROLLIT 6, ALTERNATIVA: ÇELËSI – PËRPUTHJA E FJALËVE

1 D – SJELLJE	2 H – ANTIVIRUS	3 E – PËRDITËSIME	4 B – HEURISTIKËKODI
5 G – IZOLIM	6 A – NËNSHKRIMHASH	7 C – SANDBOX	8 F – ALARMIRREMË

SHËNIME PËR DISKUTIM PËR MËSUESIT

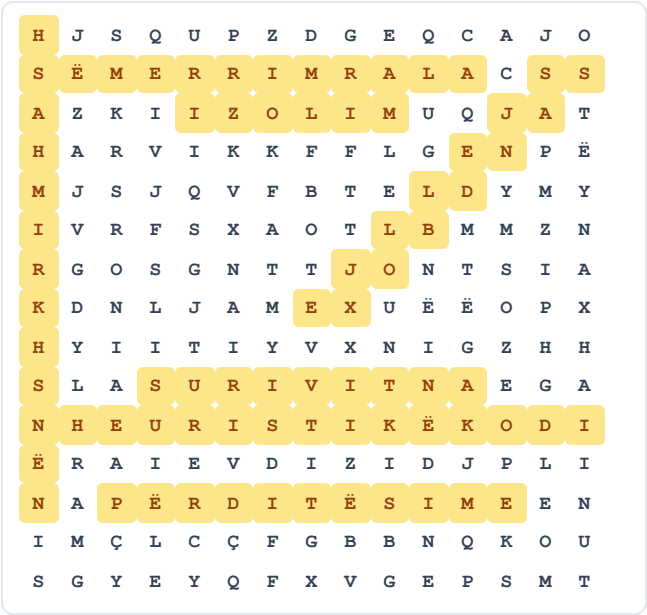
Termat kryesorë:
Kontrollo nëse nxënësit mund të shpjegojnë Nënshkrimi hash, Heuristika e kodit dhe Sandbox skedarësh me fjalët e tyre dhe të japin një shembull për secilin.

Studimet e rastit:
Kërkoju nxënësve t'i mbështesin rekomandimet me fakte nga fleta, jo me supozime.

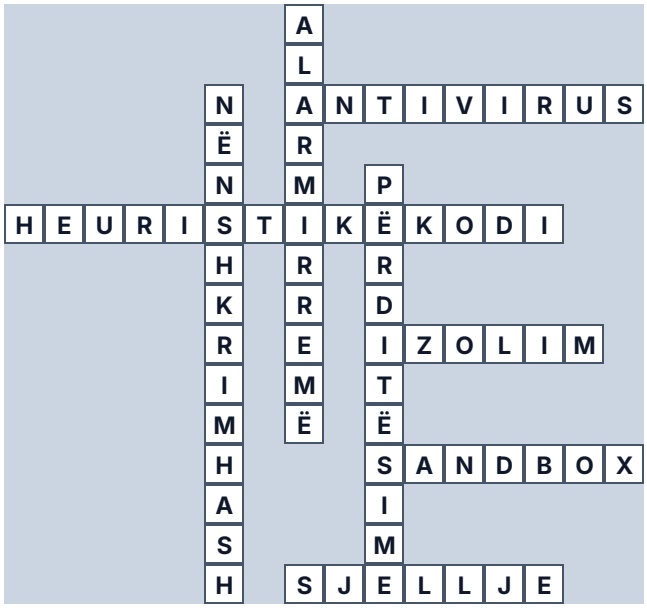
Vlerësimi i burimeve:
Kërkoju nxënësve të verifikojnë të paktën një pohim në burimet e fletës dhe diskutoni pse numrat, çmimet dhe rregullat mund të ndryshojnë me kalimin e kohës.

Çelësat e enigmave dhe shënimet për mësuesin

ZGJIDHJA E LOJËS ME FJALË



ZGJIDHJA E FJALËKRYQIT



HORIZONTALISHT

3 horizontalisht: ANTIVIRUS Paketë softuerike që skanon dhe mbron pajisjet fundore nga eksploitet (9 shkronja)

5 horizontalisht: HEURISTIKËKODI Analizë e bazuar në rregulla që sinjalizon skedarët me struktura të dyshimta kodi (14 shkronja)

6 horizontalisht: IZOLIM Mbyllja e skedarëve të dyshimtë në një hapësirë të kufizuar për të parandaluar ekspozimin e sistemit lokal (6 shkronja)

7 horizontalisht: SANDBOX Mjedis i sigurt virtual testimi që ekzekuton kodin e pabesuar në mënyrë të sigurt (7 shkronja)

8 horizontalisht: SJELLJE Veprimet e softuerit që po ekzekutohet, të monitoruara për modele veprimi keqdashëse (7 shkronja)

VERTIKALISHT

1 vertikalisht: ALARMIRREMË Sinjalizim sigurie që klasifikon gabimisht softuer të sigurt si malware (11 shkronja)

2 vertikalisht: NËNSHKRIMHASH Gjurmë kriptografike unike në bazën e të dhënave që përdoret për të identifikuar kërcënimet e njohura (13 shkronja)

4 vertikalisht: PËRDITËSIME Shkarkime të rregullta të përkufizimeve që ushqejnë bazën e të dhënave të kërcënimeve (11 shkronja)

Çelësi i fjalëve të përzierura dhe i zgjidhjes së kodit

Çelësi i vlerësimit për aktivitetin e rirenditjes së fjalorit dhe për Sfidën e Kodit të Fshehtë.

ÇELËSI I RIRENDITJES SË FJALËVE

1.	RNMSKËIHNAHHS	NËNSHKRIMHASH	5.	ËUOEIKIISKTHDR	HEURISTIKËKODI
2.	SNXOBDA	SANDBOX	6.	JELSLEJ	SJELLJE
3.	PËTSRËMEIID	PËRDITËSIME	7.	RMALRËEMAIR	ALARMIRREMË
4.	MLOIIZ	IZOLIM	8.	SVUAINIRT	ANTIVIRUS

ÇELËSI I SFIDËS SË KODIT TË FSHEHTË

"ZBULO KOD TË DËMSHËM TË RI ME HEURISTIKË"

Çelësi i studimeve të rastit

A Studimi i rastit 1: Skanimi me nënshkrime kundrejt atij heuristik

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një punonjës shkarkon një mjet të personalizuar të ndërtuar brenda kompanisë nga një ekip tjetër. Skaneri i nënshkrimeve e kalon, por skaneri heuristik e shënon si të dyshimtë.
- Strategjia dhe zgjidhja e rekomanduar: Pse ndodhi: Skanimi me nënshkrime kontrollon hash-et e skedarëve; meqenëse është i personalizuar, nuk është në bazën e të dhënave të kërcënimeve. Heuristika analizon strukturën dhe shënoi veprime të dyshimta (p.sh. shkrime në regjistër). Verifikimi: Ekzekuto skedarin në një sandbox për të vëzhguar veprimet, kontrollo nënshkrimet digjitale dhe dërgo hash-in te portalet e inteligjencës së kërcënimeve.

B Studimi i rastit 2: Trajtimi i pozitiveve të rreme

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një zhvillues softueri kompilon aplikacionin e tij. Antivirusi i sistemit e shënon ekzekutuesin e ri si malware dhe e vë në karantinë.
- Strategjia dhe zgjidhja e rekomanduar: Rreziqet e listës së bardhë: Anashkalimi i skanerëve mund të lejojë ekzekutimin e kodit të vërtetë të infektuar. Rruga e zgjidhjes: Dërgoje skedarin te shitësi i antivirusit për analizë, nënshkruaje kodin digjitalisht përmes autoriteteve të certifikatave dhe konfiguro përkohësisht përjashtime për dosje specifike në vend që ta fikësh antivirusin.