Emri: _____ Data: _____ Pikët: _____

Arkitektura dhe siguria Zero Trust

Verifikimi i vazhdueshëm, mikro-segmentimi i rrjetit, Identity and Access Management, privilegji më i vogël dhe kontrollet e gjendjes së pajisjes.

PËRMBLEDHJE MËSIMORE E SIGURISË ZERO TRUST

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 arkitekturës dhe sigurisë Zero Trust. Do të eksplorosh verifikimin e vazhdueshëm, mikro-segmentimin e rrjetit, menaxhimin e identitetit dhe qasjes (IAM), privilegjin më të vogël dhe auditimin e seancave.

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/siguria-kibernetike-zero-trust/

Udhërrëfyesi yt mësimor për strategjinë Zero Trust

- Kupto parimin kryesor të verifikimit të vazhdueshëm.
- Zbato mikrosegmentimin e rrjetit dhe qasjen me privilegjet më të pakta.
- Konfiguro kontrollet e gjendjes së pajisjes dhe auditimin e sesioneve aktive.

UDHËZIME PËR UDHËZUESIN E SIGURISË ZERO TRUST

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 arkitekturën Zero Trust. Përfundo me aktivitetin bonus Mendo shpejt.

ARKITEKTURA DHE SIGURIA ZERO TRUST (HYRJE)

Siguria Zero Trust i zëvendëson modelet e vjetra të perimetrit të rrjetit me një politikë të rreptë 'mos i beso kurrë, verifiko gjithmonë'. Zbatimi i mikrosegmentimit, menaxhimit të identitetit dhe qasjes (IAM), të drejtave të privilegjit më të vogël dhe kontrolleve të qëndrimit bllokon lëvizjen anësore të kërcënimeve.

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

Pika e kontrollit 1: Sfida me zgjedhje të shumëfishtë

1. Cili është parimi thelbësor i sigurisë Zero Trust?

- A. Mos i beso kurrë, verifiko gjithmonë çdo kërkesë qasjeje pavarësisht nga burimi
- B. Supozimi se i gjithë trafiku brenda firewall-it të korporatës është i sigurt
- C. Ruajtja e skedarëve të bazës së të dhënave pa enkriptim për të përmirësuar shpejtësinë
- D. Zbatimi i autentikimit të email-it duke përdorur vetëm regjistrime SPF

2. Çfarë është mikrosegmentimi i rrjetit?

- A. Ndarja e rrjeteve në zona të vogla të izoluara për të përmbajtur lëvizjen anësore
- B. Enkriptimi i kartave të rrjetit gjatë transitit të të dhënave
- C. Lidhja e të gjithë serverëve lokalë me një adresë të vetme IP publike
- D. Monitorimi i shtypjeve të tastave të përdoruesit në sesionet e shfletuesit

3. Çfarë është parimi i privilegjit më të vogël?

- A. Kufizimi i lejeve të qasjes së përdoruesit vetëm në atë që është e nevojshme për punën e tij
- B. Dhënia e të gjitha privilegjeve të sistemit çdo përdoruesi si parazgjedhje
- C. Lejimi i hyrjeve anonime në serverët e bazave të të dhënave korporative
- D. Konfigurimi i router-ave publikë Wi-Fi pa fjalëkalime

4. Çfarë është Identity and Access Management (IAM)?

- A. Kornizat që menaxhojnë identitetet dixhitale dhe kontrollojnë privilegjet e sistemit
- B. Mjete antivirus që skanojnë direktoritë lokale të skedarëve
- C. Një sistem ruajtjeje rezervë që përdor media të izoluara nga rrjeti (air-gapped)
- D. Një protokoll gateway-i i email-it që refuzon domenet e falsifikuara

5. Çfarë do të thotë autentikim i vazhdueshëm?

- A. Verifikimi i përsëritur i identitetit të përdoruesit dhe i gjendjes së pajisjes gjatë një sesioni aktiv
- B. Ndryshimi i fjalëkalimit kryesor çdo 10 minuta
- C. Hashimi i regjistrimeve të bazës së të dhënave me disa algoritme
- D. Enkriptimi i paketave të transitit të rrjetit duke përdorur çelësa TLS

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

6 Pyetja 6

6. Zero Trust supozon se i gjithë trafiku brenda firewall-it të korporatës është i sigurt.

E vërtetë E gabuar

7 Pyetja 7

7. Mikrosegmentimi kufizon aftësinë e sulmuesve për të lëvizur anash nëpër serverët e brendshëm.

E vërtetë E gabuar

8 Pyetja 8

8. Privilegji minimal u jep akses të gjitha skedarëve të bazës së të dhënave si parazgjedhje.

E vërtetë E gabuar

9 Pyetja 9

9. Verifikimi i vazhdueshëm validon shëndetin e pajisjes dhe kredencialet gjatë gjithë sesionit të hyrjes.

E vërtetë E gabuar

10 Pyetja 10

10. Zbatimi i Zero Trust zvogëlon ndikimin e hyrjeve të kompromentuara në korporatë.

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. Kërkimi i kredencialeve në çdo pikë qasjeje është _____ i vazhdueshëm.

2. Ndarja e rrjetit korporativ në zona shumë të vogla është mikro- _____ .

3. Konfigurimi i identiteteve dixhitale dhe kontrolli i qasjes përdor sistemin: _____ .

4. Kufizimi i lejeve të përdoruesit në minimumin e nevojshëm quhet parimi i _____ më të vogël.

5. Vlerësimi i shëndetit të pajisjeve të lidhura skanon pajisjen për: _____ .

6. Regjistrimi dhe rishikimi i seancave aktive është _____ sigurie.

BANKA E FJALËVE TË LEKSIKUT

AUDITIM FIREWALL MENAXHIM IAM POSTURË PRIVILEGJ RUTER SEGMENTIM VERIFIKIM

Shkruaj përgjigjet e tua këtu:

1.

2.

3.

4.

5.

6.

Pika e kontrollit 4: Përputhja e koncepteve të sigurisë

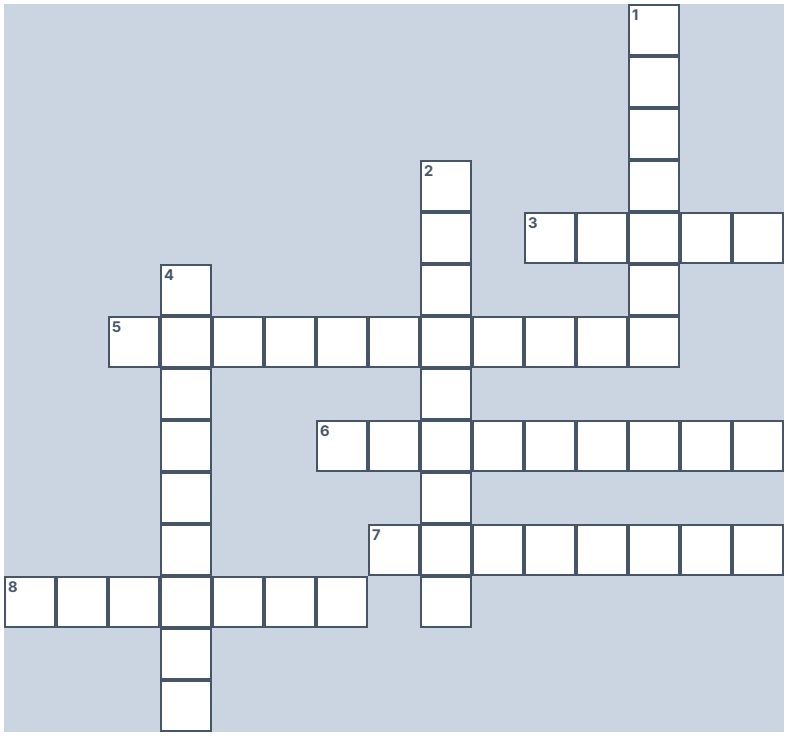
PËRPUTHJA E PËRKUFIZIMEVE

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. VERIFIKIM	**A**	Menaxhimi i aksesit në kredencialet e përdoruesve.
☐	2. SEGMENTIMI	**B**	Parimi i të drejtave minimale të aksesit.
☐	3. IAM	**C**	Rrugëzimi i trafikut të paketave të rrjetit.
☐	4. PRIVILEG	**D**	Mbrojtje e barrierës së jashtme të rrjetit.
☐	5. QËNDRIM	**E**	Rishikimi i seancave të qasjes së regjistruara.
☐	6. AUDITIM	**F**	Ndarja e zonave të brendshme të rrjetit.
☐	7. FIREWALL	**G**	Kontrollimi gjithmonë i kredencialeve të përdoruesit.
☐	8. RUTER	**H**	Vlerësimi i gjendjes së shëndetit të pajisjes.

Pika e kontrollit 5: Fjalëkryq

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



HORIZONTALISHT

3. Rrugëzimi i trafikut të paketave të rrjetit. (5)

5. Menaxhimi i qasjes në kredencialet e përdoruesve. (11)

6. Parimi i të drejtave minimale të qasjes. (9)

7. Mbrojtje e kufirit të jashtëm të rrjetit. (8)

8. Vlerësimi i gjendjes së shëndetit të pajisjes. (7)

VERTIKALISHT

1. Rishikimi i seancave të regjistruara të qasjes. (7)

2. Kontrollimi i vazhdueshëm i kredencialeve të përdoruesit. (9)

4. Ndarja e zonave të brendshme të rrjetit. (9)

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.

HORIZONTALISHT

3 horizontalisht: Rrugëzimi i trafikut të paketave të rrjetit. (5 shkronja):

5 horizontalisht: Menaxhimi i qasjes në kredencialet e përdoruesve. (11 shkronja):

6 horizontalisht: Parimi i të drejtave minimale të qasjes. (9 shkronja):

7 horizontalisht: Mbrojtje e kufirit të jashtëm të rrjetit. (8 shkronja):

8 horizontalisht: Vlerësimi i gjendjes së shëndetit të pajisjes. (7 shkronja):

VERTIKALISHT

1 vertikalisht: Rishikimi i seancave të regjistruara të qasjes. (7 shkronja):

2 vertikalisht: Kontrollimi i vazhdueshëm i kredencialeve të përdoruesit. (9 shkronja):

4 vertikalisht: Ndarja e zonave të brendshme të rrjetit. (9 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.

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

LISTA E FJALËVE TË LEKSIKUT

VERIFIKIM SEGMENTIM MENAXHIMIAM PRIVILEGJ POSTURË AUDITIM FIREWALL RUTER

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. VERIFIKIM
B. SEGMENTIM
C. MENAXHIMIAM
D. PRIVILEGJ
E. POSTURË
F. AUDITIM
G. FIREWALL
H. RUTER

PËRKUFIZIME DHE FUSHA PËRPUTHJEJE
1. Mbrojtje e kufirit të jashtëm të rrjetit.
2. Rishikimi i seancave të regjistruara të qasjes.
3. Parimi i të drejtave minimale të qasjes.
4. Ndarja e zonave të brendshme të rrjetit.
5. Rrugëzimi i trafikut të paketave të rrjetit.
6. Vlerësimi i gjendjes së shëndetit të pajisjes.
7. Menaxhimi i qasjes në kredencialet e përdoruesve.
8. Kontrollimi i vazhdueshëm i kredencialeve të përdoruesit.

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. **IFIEVKIMR** _____
2. **XMEMAHNIMIA** _____
3. **TPUËSRO** _____
4. **ELLAWFIR** _____
5. **TEEMNMSIG** _____
6. **GVRELPIJI** _____
7. **AITMUID** _____
8. **RRTEU** _____

Aktivitet bonus: Mendo shpejt

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

1	Informacione që nuk duhet t'i ndash kurrë			
2	Zakone të sigurta që mund t'i fillosh sot			
3	Gjëra që kontrollohen në një pajisje			
4	Gjëra që regjistrohen në log			
5	Fjalë që lidhen me sigurinë kibernetike			
6	Gjëra që kontrollon Zero Trust			
7	Vende ku tregon identitetin në jetën e përditshme			
8	Mënyra për të provuar se je vërtet ti			
9	Gjëra që bëhen pas një rrjedhjeje të dhënash			
10	Shenja që një kompjuter është i infektuar			
11	Arsye për të përditësuar softuerin			
12	Nivele qasjeje në një kompani			
13	Mjete sigurie që njeh			
14	Zona në të cilat mund të ndahet një rrjet			
15	Thënie për besimin			

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: KALIMI TE ARKITEKTURA E RRJETIT ZERO TRUST



Skenari: Një ndërmarrje e madhe aktualisht përdor një rrjet të brendshëm të sheshtë ku çdo pajisje në rrjetin lokal mund të hyjë në të gjithë serverët dhe bazat e të dhënave të kompanisë.

Pyetje për diskutim: Harto një strategji mikrosegmentimi të rrjetit për të kufizuar lëvizjen anësore.

STUDIMI I RASTIT 2: VENDOSJA E KONTROLLEVE TË QASJES ME PRIVILEGJIN MË TË VOGËL



Skenari: Regjistrat e auditimit zbulojnë se përdoruesit e përkohshëm të bazës së të dhënave dhe punonjësit e nivelit të ulët kanë leje globale leximi dhe shkrimi mbi bazat e të dhënave kritike të kontabilitetit.

Pyetje për diskutim: Audito dhe kufizo privilegjet IAM të bazës së të dhënave për të zbatuar privilegjin më të vogël.

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

24	6	20	11	8	11	13	17		9	12	11	22	10	15	17	16	7	15	6
1	20	13	11	22	6	13	22	23	20	7		27	6	20	17				
						22	20	23	21	22									

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: Çfarë është Zero Trust?

Zero Trust është një kuadër sigurie që supozon se kërcënimet ekzistojnë si jashtë ashtu edhe brenda kufirit të rrjetit, duke kërkuar verifikim për çdo kërkesë. [1]

Q2: Cili është rregulli thelbësor i Zero Trust?

Mos i beso kurrë, verifiko gjithmonë.

Q3: Çfarë është mikrosegmentimi?

Ndarja e një rrjeti në segmente të vogla logjike të sigurta për të kontrolluar trafikun dhe për të përmbajtur shkeljet.

Q4: Çfarë është privilegji më i vogël (least privilege)?

Dhënia e përdoruesve vetëm të të drejtave minimale të qasjes që nevojiten për të kryer detyrat e tyre specifike. [2]

Q5: Çfarë do të thotë IAM?

Menaxhimi i identitetit dhe i qasjes.

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 ndihmon kontrolli i qëndrimit të pajisjes?

Verifikon që një pajisje është e përditësuar, ka antivirus aktiv dhe është e sigurt përpara se të lejojë qasjen.

Q7: Çfarë është lëvizja anësore (lateral movement)?

Procesi që përdorin sulmuesit për t'u lëvizur nëpër një rrjet nga një nyje fillestare e kompromentuar drejt sistemeve me vlerë më të lartë.

Q8: A i zëvendëson Zero Trust firewall-et?

Jo, i përmirëson ato duke shtuar kontrolle të përqendruara te identiteti dhe firewall-e të brendshëm segmentimi.

Q9: Çfarë është vërtetimi i vazhdueshëm?

Verifikim i vazhdueshëm i identitetit të përdoruesit gjatë gjithë seancës aktive të hyrjes, jo vetëm në hyrjen fillestare.

Q10: Pse është i rrezikshëm një rrjet i sheshtë?

Në rrjetet e sheshta, një nyje e vetme e kompromentuar u lejon sulmuesve të hyjnë lehtë në çdo bazë të dhënash në rrjet.

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 trajton Zero Trust modelin e perimetrit?

Zëvendëson modelin e vjetruar 'kështjellë-dhe-hendek', duke e zhvendosur mbrojtjen nga rrjetet e perimetrit te identitetet dhe burimet specifike të përdoruesve.

Q2: Çfarë është një pikë vendimmarrjeje e politikave (PDP)?

Komponenti i sistemit që vlerëson kërkesat e autorizimit ndaj rregullave të sigurisë për të vendosur nëse duhet dhënë qasja.

Q3: Çfarë është një pikë zbatimi e politikave (PEP)?

Nyja e sistemit (si një portë ose proxy) që fizikisht lejon ose bllokon kërkesat e lidhjes sipas vendimit të PDP-së.

Q4: Si e mbështet Kontrolli i Aksesit i Bazuar në Role (RBAC) modelin Zero Trust?

RBAC i grupon lejet në role specifike, duke ndihmuar në parandalimin e trashëgimisë së privilegjeve të tepruara administrative nga përdoruesit.

Q5: Çfarë është kontrolli i aksesit kontekstual?

Vlerësimi i kërkesave të hyrjes duke përdorur sinjale dytësore si vendndodhja gjeografike, gjendja e pajisjes dhe ora e hyrjes për të vlerësuar rrezikun.

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: Si ndryshon mikrosegmentimi nga VLAN-et standarde?

VLAN-et i ndajnë rrjetet në segmente të gjera logjike në shtresën 2, ndërsa mikro-segmentimi përdor politika softuerike për të izoluar ngarkesa individuale.

Q7: Çfarë është aksesi just-in-time (JIT)?

Dhënia e përkohshme e lejeve administrative të ngritura dhe revokimi automatik i tyre pasi të përfundojë detyra.

Q8: Si t'i sigurosh API-të në një kuadër Zero Trust?

Duke kërkuar token OAuth të nënshkruar kriptografikisht dhe duke audituar nënshkrimet e kërkesave në çdo portë API.

Q9: Çfarë është një klient zero-trust network access (ZTNA)?

Një agjent softuerik që krijon lidhje të sigurta dhe të enkriptuara dalëse me aplikacione të caktuara në vend të nënrrjeteve të papërpunuara të rrjetit.

Q10: Si e ndihmon auditimi i regjistrave Zero Trust?

Regjistrimi i vazhdueshëm u lejon mjeteve të automatizuara të analizave të sigurisë të zbulojnë anomali dhe të pezullojnë menjëherë hyrjet e dyshimta.

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

Arkitekturat Zero Trust e zëvendësojnë modelin e vjetër kështjellë-dhe-hendek me rregulla verifikimi të përqendruara te identiteti.

2. PERSPEKTIVË PËR SIGURINË

Mikro-segmentimi i rrjetit e zvogëlon zonën që mund të arrijë malware-i duke i izoluar ngarkesat e punës në zona të vogla të mbrojtura.

3. PERSPEKTIVË PËR SIGURINË

Zero Trust përqendrohet te mbrojtja e burimeve si aktivet, shërbimet dhe llogaritë dhe jo e segmenteve të rrjetit. [1]

4. PERSPEKTIVË PËR SIGURINË

Politikat e aksesit me privilegje minimale zvogëlojnë rrezikun e nxjerrjes së të dhënave nga bazat kryesore nga kërcënimet e brendshme.

5. PERSPEKTIVË PËR SIGURINË

Validimi i gjendjes së pajisjes kontrollon në kohë reale nivelet e përditësimeve të sistemit operativ dhe gjendjen aktive të antivirusit.

6. PERSPEKTIVË PËR SIGURINË

Ndërmjetësit e Zero Trust Network Access (ZTNA) mund t'i zëvendësojnë ose plotësojnë VPN-të e korporatës për të kufizuar fushëveprimin e qasjes së përdoruesve.

7. NJOHURI PËR SIGURINË

Delegimi Just-in-Time (JIT) i privilegjeve administrative zvogëlon rrezikun e vjedhjes së kredencialeve në kontrollorët e domenit.

8. NJOHURI PËR SIGURINË

Regjistrat dhe auditimet e vazhdueshme të validimit vëzhgojnë sjelljen e sesionit, duke pezulluar përdoruesit që tregojnë modele anomale të ekzekutimit të skripteve.

9. NJOHURI PËR SIGURINË

Mbrojtjet tradicionale të perimetrit dështojnë të bllokojnë sulmet anësore pasi të rrjedhë një kredencial administrativ.

10. PERSPEKTIVË PËR SIGURINË

Botimi Special i NIST 800-207 (2020) jep një përkufizim abstrakt të arkitekturës Zero Trust, me modele vendosjeje. [1]

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 TË INDUSTRISË

[1] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[2] CISA. (2023). Zero Trust Maturity Model.
https://www.cisa.gov/zero-trust-maturity-model

[3] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

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

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

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

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

SHËNIM PËR MËSUESIN

Cili është parimi thelbësor i sigurisë Zero Trust? → Mos i beso kurrë, verifiko gjithmonë çdo kërkesë qasjeje pavarësisht nga burimi

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

SHËNIM PËR MËSUESIN

Çfarë është mikrosegmentimi i rrjetit? → Ndarja e rrjeteve në zona të vogla të izoluara për të përmbajtur lëvizjen anësore

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

SHËNIM PËR MËSUESIN

Çfarë është parimi i privilegjit më të vogël? → Kufizimi i lejeve të qasjes së përdoruesit vetëm në atë që është e nevojshme për punën e tij

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

SHËNIM PËR MËSUESIN

Çfarë është Identity and Access Management (IAM)? → Kornizat që menaxhojnë identitetet dixhitale dhe kontrollojnë privilegjet e sistemit

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

SHËNIM PËR MËSUESIN

Çfarë do të thotë autentikim i vazhdueshëm? → Verifikimi i përsëritur i identitetit të përdoruesit dhe i gjendjes së pajisjes gjatë një sesioni aktiv

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

6 **Pyetja 6** **Përgjigjja e saktë: E gabuar**

SHËNIM PËR MËSUESIN

E gabuar: Zero Trust nuk jep asnjë besim të nënkuptuar bazuar në vendndodhjen e rrjetit, brenda ose jashtë.

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

SHËNIM PËR MËSUESIN

E vërtetë: zonat e vogla të izoluara kufizojnë sa larg mund të lëvizë një ndërhyrës mes serverëve.

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

SHËNIM PËR MËSUESIN

E gabuar: privilegji më i vogël jep vetëm qasjen minimale që i duhet çdo roli.

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

SHËNIM PËR MËSUESIN

Verifikimi i vazhdueshëm validon shëndetin e pajisjes dhe kredencialet gjatë gjithë sesionit të hyrjes.

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

SHËNIM PËR MËSUESIN

Zbatimi i Zero Trust zvogëlon ndikimin e hyrjeve të kompromentuara në korporatë.

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

G 1. VERIFIKIM	F 2. SEGMENTIMI	A 3. IAM	B 4. PRIVILEG
H 5. QËNDRIM	E 6. AUDITIM	D 7. FIREWALL	C 8. RUTER

PIKA E KONTROLLIT 3: ÇELËSI – TERMAT KRYESORË

1 VERIFIKIM	2 SEGMENTIM	3 MENAXHIM IAM	4 PRIVILEGJ
5 POSTURË	6 AUDITIM		

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

1 G – FIREWALL	2 F – AUDITIM	3 D – PRIVILEGJ	4 B – SEGMENTIM
5 H – RUTER	6 E – POSTURË	7 C – MENAXHIMIAM	8 A – VERIFIKIM

SHËNIME PËR DISKUTIM PËR MËSUESIT

Termat kryesorë:
Kontrollo nëse nxënësit mund të shpjegojnë VERIFIKIM, SEGMENTIMI dhe IAM 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.

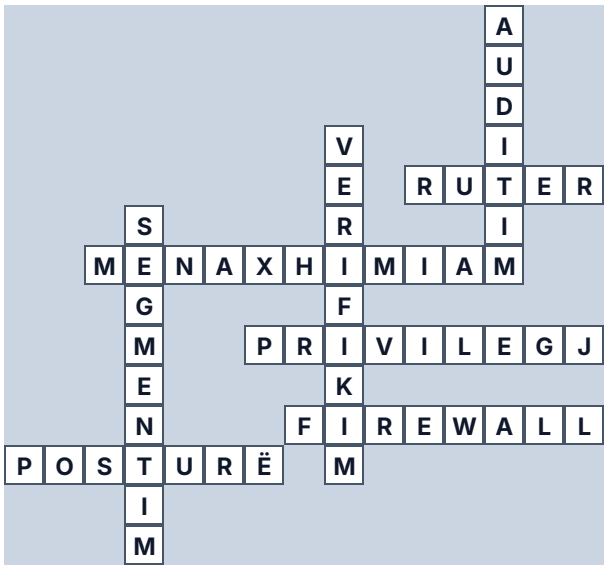
Vlerësimi i burimeve:
Kërkoju nxënësve të verifikojnë të paktën një pohim në burimet e fletës dhe diskutoni pse numrat, çmimet dhe rregullat mund të ndryshojnë me kalimin e kohës.

Çelësat e enigmave dhe shënimet për mësuesin

ZGJIDHJA E LOJËS ME FJALË

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

ZGJIDHJA E FJALËKRYQIT



UDHËZUES PËR MËSUESIN PËR ZGJIDHJET E KRYQËZËS

HORIZONTALISHT

3 horizontalisht: RUTER Rrugëzimi i trafikut të paketave të rrjetit. (5 shkronja)

5 horizontalisht: MENAXHIMIAM Menaxhimi i qasjes në kredencialet e përdoruesve. (11 shkronja)

6 horizontalisht: PRIVILEGJ Parimi i të drejtave minimale të qasjes. (9 shkronja)

7 horizontalisht: FIREWALL Mbrojtje e kufirit të jashtëm të rrjetit. (8 shkronja)

8 horizontalisht: POSTURË Vlerësimi i gjendjes së shëndetit të pajisjes. (7 shkronja)

VERTIKALISHT

1 vertikalisht: AUDITIM Rishikimi i seancave të regjistruara të qasjes. (7 shkronja)

2 vertikalisht: VERIFIKIM Kontrollimi i vazhdueshëm i kredencialeve të përdoruesit. (9 shkronja)

4 vertikalisht: SEGMENTIM Ndarja e zonave të brendshme të rrjetit. (9 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. IFIEVKIMR	VERIFIKIM	5. TEEMNMSIG	SEGMENTIM
2. XMEMAHNIMIA	MENAXHIMIAM	6. GVRELPIJI	PRIVILEGJ
3. TPUËSRO	POSTURË	7. AITMUID	AUDITIM
4. ELLAWFIR	FIREWALL	8. RRTEU	RUTER

ÇELËSI I SFIDËS SË KODIT TË FSHEHTË

"VERIFIKO GJITHMONË ME ARKITEKTURË ZERO TRUST"

Çelësi i studimeve të rastit

A Studimi i rastit 1: Kalimi te arkitektura e rrjetit Zero Trust

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Një ndërmarrje e madhe përdor aktualisht një rrjet të brendshëm të sheshtë ku çdo pajisje në rrjetin lokal mund të hyjë në të gjithë serverët dhe bazat e të dhënave të korporatës.
- Strategjia dhe zgjidhja e rekomanduar: Segmento rrjetin e sheshtë në zona departamentale të izoluara. Instalo firewall-e të brendshëm për të kontrolluar trafikun mes zonave dhe bëj të detyrueshme vlefshmërinë e tokenit të lidhjes për çdo qasje.

B Studimi i rastit 2: Vendosja e kontrolleve të qasjes me privilegjin më të vogël

Zgjidhja për mësuesin

UDHËZUES VLERËSIMI

Përgjigjet e studentëve duhet të mbulojnë pikat e mëposhtme:

- Analiza e skenarit: Regjistrat e auditimit tregojnë se përdoruesit e përkohshëm të bazës së të dhënave dhe punonjësit e nivelit të ulët kanë leje globale leximi dhe shkrimi në bazat e të dhënave kritike të kontabilitetit.
- Strategjia dhe zgjidhja e rekomanduar: Shfuqizo të gjitha privilegjet globale administrative. Zbato Kontrollin e Qasjes Sipas Roleve (RBAC) që t'u përshtatet saktësisht roleve të punës dhe krijo rishikime javore të automatizuara të lejeve.