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

Arhitectură și securitate Zero Trust

Verificare continuă, microsegmentarea rețelei, Identity and Access Management, privilegii minime și verificări ale posturii.

PREZENTARE GENERALĂ A ÎNVĂȚĂRII DESPRE SECURITATEA ZERO TRUST

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 arhitectura și securitatea Zero Trust. Vei explora verificarea continuă, micro-segmentarea rețelei, gestionarea identității și a accesului (IAM), privilegiul minim și auditarea sesiunilor.

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/securitate-cibernetica-zero-trust/

Harta ta de învățare despre strategia Zero Trust

- Înțelege principiul de bază al verificării continue.
- Implementează micro-segmentarea rețelei și accesul cu privilegii minime.
- Configurează verificările posturii dispozitivului și auditarea sesiunilor active.

INSTRUCȚIUNI PENTRU GHIDUL DE SECURITATE ZERO TRUST

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 arhitectura Zero Trust. Încheie cu activitatea bonus Gândește repede.

ARHITECTURĂ ȘI SECURITATE ZERO TRUST (INTRODUCERE)

Securitatea Zero Trust înlocuiește vechile modele cu perimetru de rețea cu o politică strictă „nu avea niciodată încredere, verifică întotdeauna”. Implementarea microsegmentării, a gestionării identității și accesului (IAM), a drepturilor de privilegiu minim și a verificărilor de postură blochează mișcarea laterală a amenințărilor.

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

Punct de control 1: Provocare cu alegere multiplă

1. Care este principiul de bază al securității Zero Trust?

- A. Nu avea niciodată încredere, verifică întotdeauna fiecare cerere de acces, indiferent de sursă
- B. Presupunerea că tot traficul din interiorul firewall-ului corporativ este sigur
- C. Stocarea fișierelor bazei de date fără criptare pentru a crește viteza
- D. Impunerea autentificării e-mailului folosind doar înregistrări SPF

2. Ce este microsegmentarea rețelei?

- A. Împărțirea rețelelor în zone mici, izolate, pentru a limita mișcarea laterală
- B. Criptarea plăcilor de rețea în timpul transferului de date
- C. Conectarea tuturor serverelor locale la o singură adresă IP publică
- D. Monitorizarea apăsărilor de taste ale utilizatorilor în sesiunile de browser

3. Ce este principiul privilegiului minim?

- A. Restricționarea permisiunilor de acces ale utilizatorilor doar la ce este necesar pentru activitatea lor
- B. Acordarea tuturor privilegiilor de sistem fiecărui utilizator în mod implicit
- C. Permiterea autentificărilor anonime pe serverele de baze de date corporative
- D. Configurarea routerelor Wi-Fi publice fără parole

4. Ce este gestionarea identității și a accesului (IAM)?

- A. Cadre care gestionează identitățile digitale și controlează privilegiile din sistem
- B. Utilitare antivirus care scanează directoarele locale de fișiere
- C. Un sistem de stocare a copiilor de rezervă care folosește medii izolate fizic (air-gapped)
- D. Un protocol de gateway de e-mail care respinge domeniile falsificate

5. Ce înseamnă autentificare continuă?

- A. Verificarea repetată a identității utilizatorului și a posturii dispozitivului în timpul unei sesiuni active
- B. Schimbarea parolei principale la fiecare 10 minute
- C. Calcularea valorilor hash pentru înregistrările din baza de date cu mai mulți algoritmi
- D. Criptarea pachetelor de rețea aflate în tranzit cu chei TLS

Punct de control 2: Provocare Adevărat sau Fals

6 Întrebare 6

6. Zero Trust presupune că tot traficul din interiorul firewall-ului corporativ este sigur.

○ Adevărat ○ Fals

7 Întrebare 7

7. Micro-segmentarea limitează capacitatea atacatorilor de a se deplasa lateral între serverele interne.

○ Adevărat ○ Fals

8 Întrebare 8

8. Privilegiile minime acordă implicit acces la toate fișierele bazei de date.

○ Adevărat ○ Fals

9 Întrebare 9

9. Verificarea continuă validează starea dispozitivului și credențialele pe parcursul unei sesiuni de autentificare.

○ Adevărat ○ Fals

10 Întrebare 10

10. Implementarea Zero Trust reduce impactul datelor de autentificare corporative compromise.

○ 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. Solicitarea credențialelor la fiecare punct de acces este o _____ continuă.

2. Împărțirea rețelei corporative în zone foarte mici se numește micro- _____ .

3. Configurarea identităților digitale și a controlului accesului folosește un sistem _____ .

4. Restricționarea permisiunilor utilizatorilor folosește principiul celor mai puține _____ .

5. Evaluarea stării dispozitivelor conectate verifică așa-numita _____ a dispozitivului.

6. Înregistrarea și analiza sesiunilor active reprezintă _____ de securitate.

BANCĂ DE CUVINTE DIN VOCABULAR

AUDITARE FIREWALL IAM POSTURĂ PRIVILEGII ROUTER SEGMENTARE VERIFICARE

Scrie răspunsurile aici:

1. **2.**

3. **4.**

5. **6.**

Punct de control 4: Asocierea conceptelor despre securitate

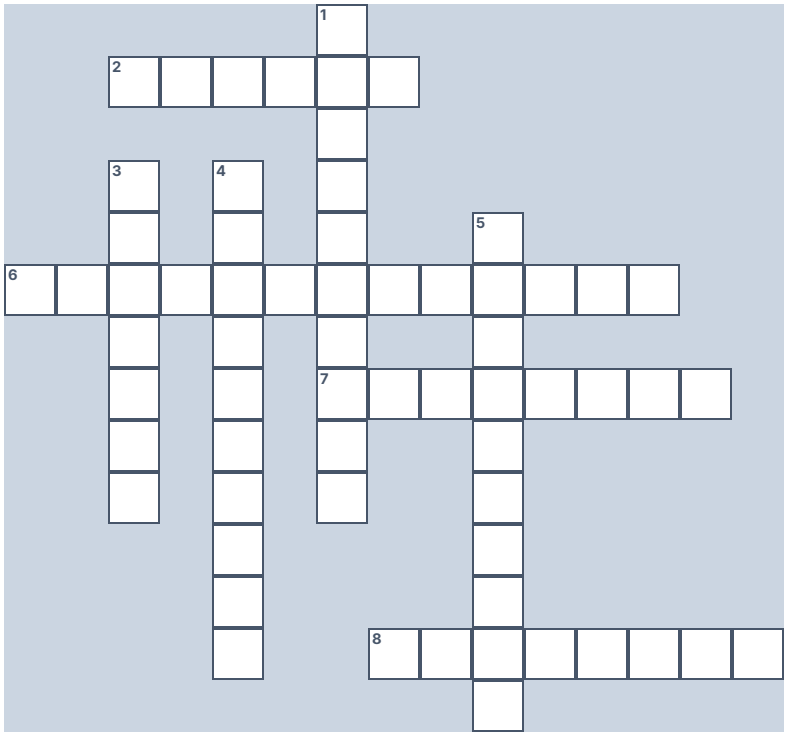
ASOCIEREA DEFINIȚIILOR

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

☐	1. VERIFICARE	A	Gestionarea accesului la credențialele utilizatorilor.
☐	2. SEGMENTARE	B	Principiul drepturilor minime de acces.
☐	3. IAM	C	Direcționarea traficului de pachete de rețea.
☐	4. PRIVILEGIU	D	Protecție de barieră externă a rețelei.
☐	5. POSTURĂ	E	Examinarea sesiunilor de acces înregistrate.
☐	6. AUDITARE	F	Împărțirea zonelor interne de rețea.
☐	7. FIREWALL	G	Verifică întotdeauna datele de autentificare ale utilizatorului.
☐	8. ROUTER	H	Evaluarea stării de sănătate a dispozitivului.

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. Rutarea traficului de pachete din rețea. (6)

6. Gestionarea accesului la credențialele utilizatorilor. (13)

7. Examinarea sesiunilor de acces înregistrate. (8)

8. Protecție de barieră a rețelei externe. (8)

VERTICAL

1. Împărțirea zonelor rețelei interne. (10)

3. Evaluarea stării de sănătate a dispozitivului. (7)

4. Principiul drepturilor minime de acces. (10)

5. Verificarea permanentă a credențialelor utilizatorilor. (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.

ORIZONTAL

2 orizontal: Rutarea traficului de pachete din rețea. (6 litere):

6 orizontal: Gestionarea accesului la credențialele utilizatorilor. (13 litere):

7 orizontal: Examinarea sesiunilor de acces înregistrate. (8 litere):

8 orizontal: Protecție de barieră a rețelei externe. (8 litere):

VERTICAL

1 vertical: Împărțirea zonelor rețelei interne. (10 litere):

3 vertical: Evaluarea stării de sănătate a dispozitivului. (7 litere):

4 vertical: Principiul drepturilor minime de acces. (10 litere):

5 vertical: Verificarea permanentă a credențialelor utilizatorilor. (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.

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

LISTĂ DE CUVINTE DIN VOCABULAR

VERIFICARE SEGMENTARE GESTIONAREIAM PRIVILEGII POSTURĂ AUDITARE FIREWALL ROUTER

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. VERIFICARE
B. SEGMENTARE
C. GESTIONAREIAM
D. PRIVILEGII
E. POSTURĂ
F. AUDITARE
G. FIREWALL
H. ROUTER

DEFINIȚII ȘI CÂMPURI DE ASOCIERE

1. Protecție de barieră a rețelei externe. ____
2. Examinarea sesiunilor de acces înregistrate. ____
3. Principiul drepturilor minime de acces. ____
4. Împărțirea zonelor rețelei interne. ____
5. Rutarea traficului de pachete din rețea. ____
6. Evaluarea stării de sănătate a dispozitivului. ____
7. Gestionarea accesului la credențialele utilizatorilor. ____
8. Verificarea permanentă a credențialelor utilizatorilor. ____

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. RCIFEVAEIR
2. AIEOSGINMRE AT
3. TPUĂSRO
4. ELLAWFIR
5. ANEEMTESRG
6. IIVEGPRLII
7. AETARUID
8. URRETO

Activitate bonus: Gândește repede

3 RĂSPUNSURI PE CATEGORIE. CÂȘTIGĂ CINE COMPLETEAZĂ PRIMUL LISTA.

1	Informații pe care nu ar trebui să le dai niciodată			
2	Obiceiuri sigure pe care le poți începe de azi			
3	Lucruri verificate pe un dispozitiv			
4	Lucruri care sunt înregistrate în jurnale			
5	Cuvinte legate de securitatea cibernetică			
6	Lucruri pe care le verifică Zero Trust			
7	Locuri în care îți arăți actul de identitate în viața de zi cu zi			
8	Moduri de a dovedi că ești chiar tu			
9	Lucruri de făcut după o scurgere de date			
10	Semne că un calculator este infectat			
11	Motive pentru care ar trebui să actualizezi software-ul			
12	Niveluri de acces într-o companie			
13	Instrumente de securitate pe care le cunoști			
14	Zone în care poate fi împărțită o rețea			
15	Proverbe despre încredere			

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: TRECEREA LA O ARHITECTURĂ DE REȚEA ZERO TRUST

👷

Scenariu: O companie mare folosește în prezent o rețea internă plată, în care orice dispozitiv din rețeaua locală poate accesa toate serverele și bazele de date corporative.

Întrebare de discuție: Proiectează o strategie de micro-segmentare a rețelei pentru a limita mișcarea laterală.

STUDIU DE CAZ 2: IMPLEMENTAREA CONTROALELOR DE ACCES CU PRIVILEGII MINIME

👷

Scenariu: Jurnalele de audit arată că utilizatorii temporari ai bazelor de date și angajații de nivel inferior dețin permisiuni globale de citire și scriere asupra bazelor de date contabile critice.

Întrebare de discuție: Auditează și restricționează privilegiile IAM ale bazelor de date pentru a impune principiul privilegiului minim.

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

27	7	21	11	8	11	5	2		16	7	21	7	26		5	26
1	21	10	11	24	7	5	24	26	21	1		31	7	21	18	
						24	21	26	22	24						

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: Ce este Zero Trust?

Zero Trust este un cadru de securitate care presupune că amenințările există atât în afara, cât și în interiorul perimetrului rețelei, necesitând verificarea fiecărei cereri. [1]

Q2: Care este regula de bază a Zero Trust?

Nu avea încredere niciodată, verifică întotdeauna.

Q3: Ce este microsegmentarea?

Împărțirea unei rețele în segmente logice mici și sigure pentru a controla traficul și a limita încălcările de securitate.

Q4: Ce este privilegiul minim?

Acordarea utilizatorilor doar a drepturilor minime de acces necesare pentru a-și îndeplini sarcinile specifice de lucru. [2]

Q5: Ce înseamnă IAM?

Managementul identității și al accesului.

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

Parcurge întrebările și răspunsurile frecvente despre atenuarea amenințărilor online.

Q6: Cum ajută verificarea posturii dispozitivului?

Verifică dacă un dispozitiv are actualizările instalate, rulează un antivirus activ și este sigur înainte de a permite accesul.

Q7: Ce este mișcarea laterală?

Procesul prin care atacatorii se deplasează printr-o rețea, de la un nod compromis inițial către sisteme cu valoare mai mare.

Q8: Înlocuiește Zero Trust firewall-urile?

Nu, le îmbunătățește adăugând verificări centrate pe identitate și firewall-uri interne de segmentare.

Q9: Ce este autentificarea continuă?

Verificare continuă a identității utilizatorului pe parcursul unei sesiuni de autentificare active, nu doar la prima conectare.

Q10: De ce este periculoasă o rețea plată?

În rețelele plate, un singur nod compromis le permite atacatorilor să acceseze cu ușurință orice bază de date din rețea.

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 abordează Zero Trust modelul perimetrului?

Înlocuiește modelul depășit „castel și șanț”, mutând apărarea de la rețelele de perimetru la identități și resurse specifice ale utilizatorilor.

Q2: Ce este un punct de decizie a politicii (PDP)?

Componenta de sistem care evaluează cererile de autorizare în raport cu regulile de securitate pentru a decide dacă accesul trebuie acordat.

Q3: Ce este un punct de aplicare a politicilor (PEP)?

Nodul de sistem (precum un gateway sau un proxy) care permite sau blochează fizic cererile de conectare pe baza deciziei PDP.

Q4: Cum susține controlul accesului bazat pe roluri (RBAC) modelul Zero Trust?

RBAC grupează permisiunile în roluri specifice, ceea ce ajută la prevenirea moștenirii de către utilizatori a unor privilegii administrative excesive.

Q5: Ce este controlul contextual al accesului?

Evaluarea cererilor de autentificare folosind indicii secundare precum locația geografică, postura dispozitivului și ora autentificării, pentru a estima riscul.

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: Prin ce diferă microsegmentarea de VLAN-urile standard?

VLAN-urile împart rețelele în segmente logice largi la nivelul 2, în timp ce micro-segmentarea folosește politici software pentru a izola sarcinile individuale.

Q7: Ce este accesul just-in-time (JIT)?

Acordarea temporară și automată a permisiunilor administrative extinse și revocarea lor imediat ce sarcina este finalizată.

Q8: Cum securizezi API-urile într-un cadru Zero Trust?

Prin solicitarea unor token-uri OAuth semnate criptografic și auditarea semnăturilor cererilor la fiecare gateway API.

Q9: Ce este un client zero-trust network access (ZTNA)?

Un agent software care stabilește conexiuni de ieșire securizate și criptate către aplicații specifice, nu către subrețele brute.

Q10: Cum ajută auditarea jurnalelor la Zero Trust?

Jurnalizarea continuă permite instrumentelor automate de analiză a securității să detecteze anomalii și să suspende imediat autentificările suspecte.

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

Arhitecturile Zero Trust înlocuiesc vechiul model „castel și șanț” cu reguli de verificare centrate pe identitate.

2. INFORMAȚII DESPRE SECURITATE

Micro-segmentarea rețelei reduce zona pe care o poate atinge software-ul rău intenționat, izolând sarcinile de lucru în zone mici protejate.

3. INFORMAȚII DESPRE SECURITATE

Zero Trust se concentrează pe protejarea resurselor, precum active, servicii și conturi, nu a segmentelor de rețea. [1]

4. INFORMAȚII DESPRE SECURITATE

Politicile de acces cu privilegii minime reduc riscul exfiltrării de date de către persoane din interior din bazele de date centrale.

5. INFORMAȚII DESPRE SECURITATE

Validarea posturii dispozitivului verifică în timp real nivelul de actualizare al sistemului de operare și starea antivirusului activ.

6. INFORMAȚII DESPRE SECURITATE

Brokerii Zero Trust Network Access (ZTNA) pot înlocui sau completa VPN-urile corporative pentru a restrânge sfera accesului utilizatorilor.

7. PERSPECTIVĂ ASUPRA SECURITĂȚII

Delegarea privilegiilor administrative Just-in-Time (JIT) reduce riscul furtului de date de autentificare pe controlerele de domeniu.

8. PERSPECTIVĂ ASUPRA SECURITĂȚII

Jurnalele de validare continuă și auditările comportamentului sesiunii suspendă utilizatorii care prezintă tipare anormale de execuție a scripturilor.

9. PERSPECTIVĂ ASUPRA SECURITĂȚII

Apărările tradiționale de perimetru nu reușesc să blocheze atacurile laterale după ce o credențială administrativă a fost divulgată.

10. INFORMAȚII DESPRE SECURITATE

Publicația specială NIST 800-207 (2020) oferă o definiție abstractă a arhitecturii Zero Trust, cu modele de implementare. [1]

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

[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

Barem: Punct de control 1 – Alegere multiplă

1 Întrebarea 1 — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Care este principiul de bază al securității Zero Trust? → Nu avea niciodată încredere, verifică întotdeauna fiecare cerere de acces, indiferent de sursă

2 Întrebarea 2 — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Ce este microsegmentarea rețelei? → Împărțirea rețelelor în zone mici, izolate, pentru a limita mișcarea laterală

3 Întrebarea 3 — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Ce este principiul privilegiului minim? → Restricționarea permisiunilor de acces ale utilizatorilor doar la ce este necesar pentru activitatea lor

4 Întrebarea 4 — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Ce este gestionarea identității și a accesului (IAM)? → Cadre care gestionează identitățile digitale și controlează privilegiile din sistem

5 Întrebarea 5 — **Răspuns corect: A**

NOTĂ PENTRU PROFESOR

Ce înseamnă autentificare continuă? → Verificarea repetată a identității utilizatorului și a posturii dispozitivului în timpul unei sesiuni active

Barem: Punct de control 2 – Adevărat sau fals

6 Întrebarea 6

Răspuns corect: Fals

NOTĂ PENTRU PROFESOR

Fals: Zero Trust nu acordă nicio încredere implicită pe baza locației din rețea, nici în interior, nici în exterior.

7 Întrebarea 7

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Adevărat: zonele mici izolate limitează cât de departe se poate deplasa un intrus între servere.

8 Întrebarea 8

Răspuns corect: Fals

NOTĂ PENTRU PROFESOR

Fals: privilegiul minim acordă doar accesul minim de care are nevoie fiecare rol.

9 Întrebarea 9

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Verificarea continuă validează starea dispozitivului și credențialele pe parcursul unei sesiuni de autentificare.

10 Întrebarea 10

Răspuns corect: Adevărat

NOTĂ PENTRU PROFESOR

Implementarea Zero Trust reduce impactul datelor de autentificare corporative compromise.

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

G 1. VERIFICARE	F 2. SEGMENTARE	A 3. IAM	B 4. PRIVILEGIU
H 5. POSTURĂ	E 6. AUDITARE	D 7. FIREWALL	C 8. ROUTER

PUNCT DE CONTROL 3: BAREM – TERMENI-CHEIE

1 VERIFICARE	2 SEGMENTARE	3 IAM	4 PRIVILEGII
5 POSTURĂ	6 AUDITARE		

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

1 G – FIREWALL	2 F – AUDITARE	3 D – PRIVILEGII	4 B – SEGMENTARE
5 H – ROUTER	6 E – POSTURĂ	7 C – GESTIONAREIAM	8 A – VERIFICARE

NOTE DE DISCUȚIE PENTRU PROFESORI

Termeni-cheie:
Verifică dacă elevii pot explica VERIFICARE, SEGMENTARE și IAM 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.

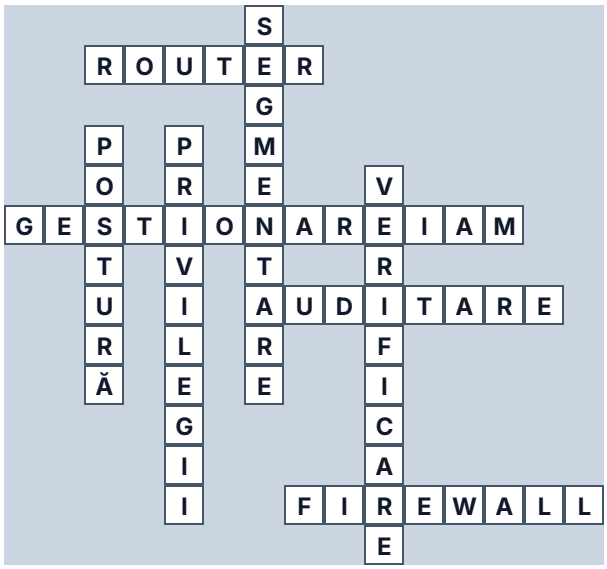
Evaluarea surselor:
Cere elevilor să verifice cel puțin o afirmație în sursele fișei și discutați de ce cifrele, prețurile și regulile se pot schimba în timp.

Chei de rezolvare ale puzzle-urilor și note pentru profesor

SOLUȚIA JOCULUI DE CĂUTARE DE CUVINTE

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

SOLUȚIA CUVINTELOR ÎNCRUCIȘATE



GHID PENTRU PROFESOR: SOLUȚIILE LA CUVINTELE ÎNCRUCIȘATE

ORIZONTAL

2 orizontal: ROUTER Rutarea traficului de pachete din rețea. (6 litere)

6 orizontal: GESTIONAREIAM Gestionarea accesului la credențialele utilizatorilor. (13 litere)

7 orizontal: AUDITARE Examinarea sesiunilor de acces înregistrate. (8 litere)

8 orizontal: FIREWALL Protecție de barieră a rețelei externe. (8 litere)

VERTICAL

1 vertical: SEGMENTARE Împărțirea zonelor rețelei interne. (10 litere)

3 vertical: POSTURĂ Evaluarea stării de sănătate a dispozitivului. (7 litere)

4 vertical: PRIVILEGII Principiul drepturilor minime de acces. (10 litere)

5 vertical: VERIFICARE Verificarea permanentă a credențialelor utilizatorilor. (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. R C I F E V A E I R — **VERIFICARE**
2. A I E O S G I N M R E A T — **GESTIONAREIAM**
3. T P U Ă S R O — **POSTURĂ**
4. E L L A W F I R — **FIREWALL**
5. A N E E M T E S R G — **SEGMENTARE**
6. I I V E G P R L I I — **PRIVILEGII**
7. A E T A R U I D — **AUDITARE**
8. U R R E T O — **ROUTER**

BAREMUL PROVOCĂRII CU CODUL SECRET

"VERIFICĂ MEREU CU ARHITECTURA ZERO TRUST"

Barem pentru studiile de caz

A Studiu de caz 1: Trecerea la o arhitectură de rețea Zero Trust

Soluția profesorului

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: O întreprindere mare folosește în prezent o rețea internă plată, în care orice dispozitiv din rețeaua locală poate accesa toate serverele și bazele de date corporative.
- Strategie și soluție recomandată: Segmentează rețeaua plată în zone departamentale izolate. Instalează firewall-uri interne pentru a controla traficul dintre zone și impune validarea token-urilor de conexiune pentru tot accesul.

B Studiu de caz 2: Implementarea controalelor de acces cu privilegii minime

Soluția profesorului

GHID DE NOTARE

Răspunsurile elevilor ar trebui să acopere următoarele puncte:

- Analiza scenariului: Jurnalele de audit arată că utilizatorii temporari ai bazei de date și angajații de nivel inferior dețin permisiuni globale de citire și scriere asupra unor baze de date contabile critice.
- Strategie și soluție recomandată: Revocă toate privilegiile administrative globale. Implementează controlul accesului bazat pe roluri (RBAC) care să corespundă exact rolurilor din posturi și stabilește revizuiri automate săptămânale ale permisiunilor.