Nome: _____ **Data:** _____ **Punteggio:** _____

Architettura e sicurezza Zero Trust

Verifica continua, micro-segmentazione della rete, Identity and Access Management, privilegi minimi e controlli di postura.

PANORAMICA DI APPRENDIMENTO SULLA SICUREZZA ZERO TRUST

PROTETTO
CRITTOGRAFIA DEI DATI
Standard AES a 256 bit

CONFORME
STANDARD GLOBALI
Framework GDPR e CCPA

ZERO-TRUST
POLITICA DI ACCESSO
Autenticazione a più fattori

Benvenuto! Questo pacchetto di attività ti guida attraverso l'architettura Zero Trust e la sicurezza. Esplorerai la verifica continua, la microsegmentazione della rete, la gestione di identità e accessi (IAM), il privilegio minimo e l'auditing delle sessioni.

PUNTI DI CONTROLLO DELLA SCHEDA DI LAVORO

- [ ] **Parti 1-4: Padroneggia la sicurezza informatica e la prevenzione delle minacce.**
- [ ] **Parti 5-7: Risolvi cruciverba e parole nascoste.**
- [ ] **Parti 8-9: Risolvi casi di studio e la sfida del codice.**
- [ ] **Parte 10: Consulta le pagine delle domande frequenti di base e avanzate.**
- [ ] **Parte 11: Esplora 10 fatti interessanti dal mondo reale.**
- [ ] **Bonus: sfida Pensa veloce.**

Apri la guida alla sicurezza informatica di VPN.com

URL: https://www.vpn.com/it/sicurezza-informatica/sicurezza-zero-trust/

Il tuo percorso di apprendimento sulla strategia Zero Trust

- Comprendi il principio fondamentale della verifica continua.
- Implementa la microsegmentazione della rete e l'accesso con il minimo privilegio.
- Configura i controlli di postura dei dispositivi e l'auditing delle sessioni attive.

ISTRUZIONI DELLA GUIDA ALLA SICUREZZA ZERO TRUST

Rispondi alle domande a scelta multipla e vero/falso, completa le frasi con gli spazi vuoti usando l'elenco di parole, abbina le definizioni e risolvi il cruciverba e la ricerca di parole. Applica le tue conoscenze all'architettura Zero Trust. Concludi con l'attività bonus Pensa veloce.

ARCHITETTURA E SICUREZZA ZERO TRUST (INTRODUZIONE)

La sicurezza Zero Trust sostituisce i vecchi modelli di perimetro di rete con una rigorosa politica «non fidarti mai, verifica sempre». L'implementazione di microsegmentazione, Identity and Access Management (IAM), diritti di privilegio minimo e controlli della postura blocca il movimento laterale delle minacce.

LEGGI CON ATTENZIONE OGNI PUNTO DI CONTROLLO E SELEZIONA O SCRIVI LA RISPOSTA CORRETTA.

Punto di controllo 1: Sfida a scelta multipla

1. Qual è il principio fondamentale della sicurezza Zero Trust?

- A. Non fidarsi mai, verificare sempre ogni richiesta di accesso indipendentemente dalla fonte
- B. Presumere che tutto il traffico all'interno del firewall aziendale sia sicuro
- C. Archiviare i file del database senza crittografia per migliorare la velocità
- D. Applicare l'autenticazione delle email usando solo record SPF

2. Che cos'è la microsegmentazione della rete?

- A. Suddividere le reti in zone piccole e isolate per contenere il movimento laterale
- B. Crittografare le schede di rete durante il transito dei dati
- C. Collegare tutti i server locali a un unico indirizzo IP pubblico
- D. Monitorare i tasti premuti dall'utente nelle sessioni del browser

3. Che cos'è il principio del privilegio minimo?

- A. Limitare i permessi di accesso degli utenti a ciò che è strettamente necessario per il loro lavoro
- B. Concedere per impostazione predefinita tutti i privilegi di sistema a ogni utente
- C. Consentire accessi anonimi ai server di database aziendali
- D. Configurare router Wi-Fi pubblici senza password

4. Che cos'è la gestione delle identità e degli accessi (IAM)?

- A. Framework che gestiscono le identità digitali e controllano i privilegi di sistema
- B. Utility antivirus che scansionano le directory dei file locali
- C. Un sistema di archiviazione di backup che usa supporti air-gapped
- D. Un protocollo di gateway email che rifiuta i domini contraffatti

5. Che cosa significa autenticazione continua?

- A. Verificare ripetutamente l'identità dell'utente e la postura del dispositivo durante una sessione attiva
- B. Cambiare la password principale ogni 10 minuti
- C. Calcolare l'hash dei record di un database usando più algoritmi
- D. Cifrare i pacchetti di rete in transito usando chiavi TLS

Punto di controllo 2: Sfida Vero o Falso

6 Domanda 6

6. Lo Zero Trust presuppone che tutto il traffico all'interno del firewall aziendale sia sicuro.

- ◯ Vero
- ◯ Falso

7 Domanda 7

7. La micro-segmentazione limita la capacità degli aggressori di muoversi lateralmente tra i server interni.

- ◯ Vero
- ◯ Falso

8 Domanda 8

8. Il privilegio minimo concede per impostazione predefinita l'accesso a tutti i file del database.

- ◯ Vero
- ◯ Falso

9 Domanda 9

9. La verifica continua convalida lo stato di salute del dispositivo e le credenziali durante tutta la sessione di accesso.

- ◯ Vero
- ◯ Falso

10 Domanda 10

10. L'adozione di Zero Trust riduce l'impatto di credenziali aziendali compromesse.

- ◯ Vero
- ◯ Falso

Punto di controllo 3: Inserimento dei termini chiave

Leggi ogni frase qui sotto e completa lo spazio vuoto con il termine corretto dell'elenco di parole.

1. Richiedere le credenziali a ogni punto di accesso è la _____ continua.
2. Dividere la rete aziendale in piccole zone è la micro- _____ .
3. Configurare le identità digitali e il controllo degli accessi richiede un sistema di _____ .
4. Limitare i permessi degli utenti applica il principio del minimo _____ .
5. Valutare lo stato di salute dei dispositivi connessi analizza la _____ dei dispositivi.
6. Registrare e rivedere le sessioni attive è l' _____ di sicurezza.

BANCA DELLE PAROLE DEL VOCABOLARIO

AUDITING FIREWALL GESTIONE IAM POSTURA PRIVILEGIO ROUTER SEGMENTAZIONE VERIFICA

Scrivi qui le tue risposte:

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

Punto di controllo 4: Abbinamento di concetti sulla sicurezza

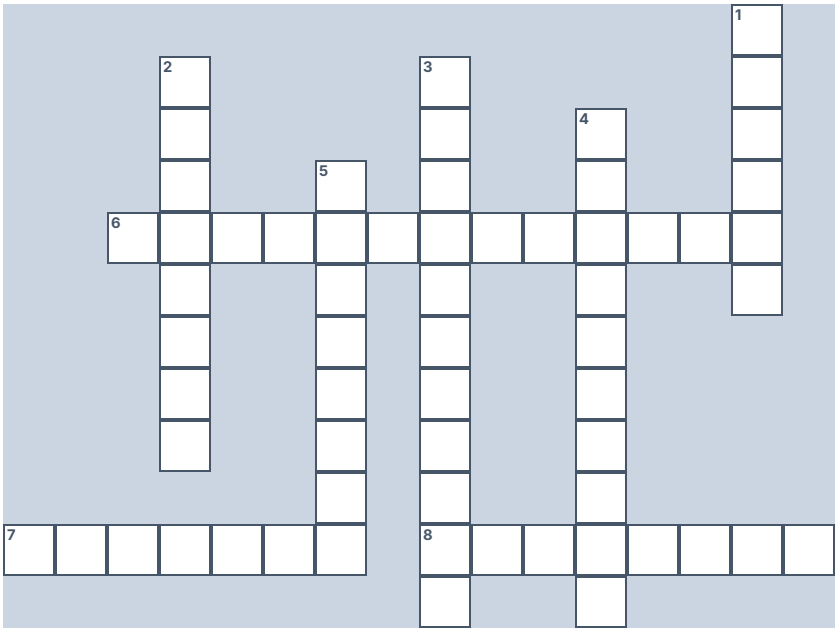
ABBINAMENTO DELLE DEFINIZIONI

Abbina ogni termine del vocabolario a sinistra alla sua definizione corretta a destra scrivendo la lettera corrispondente (A-H) nella casella compilabile.

☐	1. VERIFICA	A	Gestione dell'accesso alle credenziali degli utenti.
☐	2. SEGMENTAZIONE	B	Principio dei minimi diritti di accesso.
☐	3. IAM	C	Instradamento del traffico dei pacchetti di rete.
☐	4. PRIVILEGIO	D	Protezione della barriera di rete esterna.
☐	5. POSTURA DI SICUREZZA	E	Revisione delle sessioni di accesso registrate.
☐	6. AUDITING	F	Dividere le zone di rete interne.
☐	7. FIREWALL	G	Controllare sempre le credenziali dell'utente.
☐	8. ROUTER	H	Valutazione dello stato di salute del dispositivo.

Punto di controllo 5: Cruciverba

Risolvi il cruciverba digitando le lettere nelle caselle bianche attive. I numeri corrispondono alle definizioni qui sotto.



ORIZZONTALI

6. Suddivisione delle zone interne della rete. (13)

7. Valutazione dello stato di salute dei dispositivi. (7)

8. Revisione delle sessioni di accesso registrate. (8)

VERTICALI

1. Instradamento del traffico di pacchetti di rete. (6)

2. Protezione di barriera della rete esterna. (8)

3. Gestione dell'accesso alle credenziali degli utenti. (11)

4. Principio dei diritti di accesso minimi. (10)

5. Controllo costante delle credenziali degli utenti. (8)

Punto di controllo 5, alternativa: Indizi accessibili del cruciverba

Gli utenti di screen reader e di tastiera possono digitare le risposte del cruciverba direttamente nei campi di testo qui sotto.

ORIZZONTALI

6 orizzontale: Suddivisione delle zone interne della rete. (13 lettere):

7 orizzontale: Valutazione dello stato di salute dei dispositivi. (7 lettere):

8 orizzontale: Revisione delle sessioni di accesso registrate. (8 lettere):

VERTICALI

1 verticale: Instradamento del traffico di pacchetti di rete. (6 lettere):

2 verticale: Protezione di barriera della rete esterna. (8 lettere):

3 verticale: Gestione dell'accesso alle credenziali degli utenti. (11 lettere):

4 verticale: Principio dei diritti di accesso minimi. (10 lettere):

5 verticale: Controllo costante delle credenziali degli utenti. (8 lettere):

Punto di controllo 6: Cerca la parola nascosta

Trova gli 8 termini chiave del vocabolario nascosti nella griglia qui sotto. Le parole possono essere orizzontali, verticali o diagonali.

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

ELENCO DELLE PAROLE DEL VOCABOLARIO

VERIFICA SEGMENTAZIONE GESTIONEIAM PRIVILEGIO POSTURA AUDITING FIREWALL ROUTER

Punto di controllo 6, alternativa: Abbinamento accessibile del vocabolario

Abbina ciascuno degli 8 termini del vocabolario della Ricerca di parole alla sua definizione corretta scrivendo la lettera (A-H) nello spazio vuoto.

TERMINI DEL VOCABOLARIO	DEFINIZIONI E CAMPI DI ABBINAMENTO
A. VERIFICA	1. Protezione di barriera della rete esterna.
B. SEGMENTAZIONE	2. Revisione delle sessioni di accesso registrate.
C. GESTIONEIAM	3. Principio dei diritti di accesso minimi.
D. PRIVILEGIO	4. Suddivisione delle zone interne della rete.
E. POSTURA	5. Instradamento del traffico di pacchetti di rete.
F. AUDITING	6. Valutazione dello stato di salute dei dispositivi.
G. FIREWALL	7. Gestione dell'accesso alle credenziali degli utenti.
H. ROUTER	8. Controllo costante delle credenziali degli utenti.

Punto di controllo 7: Sfida delle parole mescolate

Riordina le lettere qui sotto per scoprire concetti e termini chiave della sicurezza informatica. Scrivi le tue risposte nelle caselle fornite.

1. CIFVIEAR
2. IMEGAOSIENT
3. TPUASRO
4. ELLAWFIR
5. ZOEGAEENITS NM
6. IIVEGPRLOI
7. AGTINUID
8. URRETO

Attività bonus: Pensa veloce

3 RISPOSTE PER CATEGORIA. VINCE CHI COMPLETA PER PRIMO LA LISTA.

1	Informazioni che non dovresti mai condividere			
2	Buone abitudini sicure che puoi iniziare oggi			
3	Cose controllate su un dispositivo			
4	Cose che vengono registrate nei log			
5	Parole legate alla sicurezza informatica			
6	Cose che lo Zero Trust verifica			
7	Luoghi in cui mostri un documento nella vita quotidiana			
8	Modi per dimostrare che sei davvero tu			
9	Cose da fare dopo una fuga di dati			
10	Segnali che indicano che un computer è infetto			
11	Motivi per aggiornare il software			
12	Livelli di accesso in un'azienda			
13	Strumenti di sicurezza che conosci			
14	Zone in cui si può dividere una rete			
15	Proverbi sulla fiducia			

Punto di controllo 8: Casi di studio sulla sicurezza informatica

Applica i concetti che hai imparato per risolvere gli scenari reali qui sotto.

CASO DI STUDIO 1: PASSAGGIO A UN'ARCHITETTURA DI RETE ZERO TRUST

👷

Scenario: Una grande azienda usa attualmente una rete interna piatta in cui qualsiasi dispositivo della rete locale può accedere a tutti i server e i database aziendali.

Domanda di discussione: Progetta una strategia di micro-segmentazione della rete per limitare il movimento laterale.

CASO DI STUDIO 2: IMPLEMENTARE CONTROLLI DI ACCESSO A PRIVILEGI MINIMI

👷

Scenario: I log di audit rivelano che utenti temporanei del database e dipendenti di basso livello hanno autorizzazioni globali di lettura e scrittura sui database contabili critici.

Domanda di discussione: Verifica e limita i privilegi IAM del database per applicare il principio del privilegio minimo.

Punto di controllo 9: Decifrare il codice

Un professionista della sicurezza informatica protegge le risorse di rete dagli attori delle minacce online. Usa la chiave lettera-numero qui sotto per decifrare il messaggio scrivendo le lettere corrispondenti negli spazi vuoti.

CHIAVE DI CIFRATURA LETTERA-NUMERO

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26

22	5	18	9	6	9	3	1		19	5	13	16	18	5		3	15	14
1	18	3	8	9	20	5	20	20	21	18	1		26	5	18	15		
20	18	21	19	20														

Messaggio decifrato:

SUGGERIMENTO: OGNI NUMERO RAPPRESENTA LA POSIZIONE DI QUELLA LETTERA NELL'ALFABETO (AD ES. 1 = A, 2 = B, 26 = Z).

Punto di controllo 10: Domande frequenti di base sulla sicurezza informatica (Parte A)

Rivedi domande e risposte comuni sulla mitigazione delle minacce online.

Q1: Che cos'è lo Zero Trust?

Lo Zero Trust è un framework di sicurezza che presuppone che le minacce esistano sia all'esterno sia all'interno del perimetro di rete e richiede la verifica di ogni richiesta. [1]

Q2: Qual è la regola fondamentale dello Zero Trust?

Non fidarti mai, verifica sempre.

Q3: Cos'è la microsegmentazione?

Dividere una rete in piccoli segmenti logici e sicuri per controllare il traffico e contenere le violazioni.

Q4: Cos'è il privilegio minimo?

Concedere agli utenti solo i diritti di accesso minimi necessari per svolgere i loro compiti specifici. [2]

Q5: Cosa significa IAM?

Gestione delle identità e degli accessi.

Punto di controllo 10: Domande frequenti di base sulla sicurezza informatica (Parte B)

Rivedi domande e risposte comuni sulla mitigazione delle minacce online.

Q6: Come aiuta il controllo di postura del dispositivo?

Verifica che un dispositivo sia aggiornato, abbia un antivirus attivo e sia sicuro prima di consentire l'accesso.

Q7: Cos'è il movimento laterale?

Il processo con cui gli aggressori si spostano in una rete da un nodo iniziale compromesso verso sistemi di maggior valore.

Q8: Lo Zero Trust sostituisce i firewall?

No, li rafforza aggiungendo controlli incentrati sull'identità e firewall di segmentazione interna.

Q9: Cos'è l'autenticazione continua?

Verifica continua dell'identità dell'utente durante tutta la sessione di accesso attiva, non solo al primo accesso.

Q10: Perché una rete piatta è pericolosa?

Nelle reti piatte, un singolo nodo compromesso consente agli aggressori di accedere facilmente a qualsiasi database della rete.

Punto di controllo 10: Domande frequenti avanzate sulla sicurezza (Parte C)

Esplora gli aspetti tecnici avanzati dei framework di sicurezza, dell'analisi del malware e della conformità dei dati.

Q1: Come affronta lo Zero Trust il modello perimetrale?

Sostituisce il vecchio modello "castello e fossato", spostando la difesa dalle reti perimetrali a specifiche identità e risorse degli utenti.

Q2: Che cos'è un policy decision point (PDP)?

Il componente di sistema che valuta le richieste di autorizzazione in base alle regole di sicurezza per decidere se concedere l'accesso.

Q3: Cos'è un punto di applicazione delle policy (PEP)?

Il nodo di sistema (come un gateway o un proxy) che consente o blocca fisicamente le richieste di connessione in base alla decisione del PDP.

Q4: Come supporta il Zero Trust il controllo degli accessi basato sui ruoli (RBAC)?

L'RBAC raggruppa i permessi in ruoli specifici, aiutando a evitare che gli utenti ereditino privilegi amministrativi eccessivi.

Q5: Cos'è il controllo degli accessi contestuale?

Valutare le richieste di accesso usando indizi secondari come posizione geografica, postura del dispositivo e orario di accesso per stimare il rischio.

Punto di controllo 10: Domande frequenti avanzate sulla sicurezza (Parte D)

Esplora gli aspetti tecnici avanzati dei framework di sicurezza, dell'analisi del malware e della conformità dei dati.

Q6: In cosa la microsegmentazione si differenzia dalle VLAN standard?

Le VLAN dividono le reti in ampi segmenti logici a livello 2, mentre la microsegmentazione usa policy software per isolare i singoli carichi di lavoro.

Q7: Cos'è l'accesso just-in-time (JIT)?

Concedere temporaneamente permessi amministrativi elevati e revocarli automaticamente al termine dell'attività.

Q8: Come si proteggono le API in un framework Zero Trust?

Richiedendo token OAuth firmati crittograficamente e verificando le firme delle richieste a ogni gateway API.

Q9: Cos'è un client per l'accesso alla rete Zero Trust (ZTNA)?

Un agente software che stabilisce connessioni in uscita sicure e cifrate verso applicazioni specifiche anziché verso sottoreti di rete grezze.

Q10: Come aiuta l'audit dei log lo Zero Trust?

Il logging continuo consente agli strumenti di analisi della sicurezza automatizzati di rilevare anomalie e sospendere immediatamente gli accessi non autorizzati.

Parte 11: 10 fatti e spunti reali sulla sicurezza informatica

Rivedi fatti reali su violazioni della sicurezza, meccanismi di difesa e standard di conformità.

1. APPROFONDIMENTO SULLA SICUREZZA

Le architetture Zero Trust sostituiscono il vecchio modello castello e fossato con regole di verifica incentrate sull'identità.

2. APPROFONDIMENTO SULLA SICUREZZA

La microsegmentazione della rete riduce l'area raggiungibile dal malware isolando i carichi di lavoro in piccole zone protette.

3. APPROFONDIMENTO SULLA SICUREZZA

Lo Zero Trust si concentra sulla protezione di risorse come asset, servizi e account, anziché dei segmenti di rete. [1]

4. APPROFONDIMENTO SULLA SICUREZZA

Le politiche di accesso con privilegio minimo riducono il rischio di esfiltrazione di dati dai database principali da parte di insider.

5. APPROFONDIMENTO SULLA SICUREZZA

La convalida della postura del dispositivo controlla in tempo reale i livelli di patch del sistema operativo e lo stato dell'antivirus attivo.

6. APPROFONDIMENTO SULLA SICUREZZA

I broker di Zero Trust Network Access (ZTNA) possono sostituire o integrare le VPN aziendali per limitare l'ambito di accesso degli utenti.

7. APPROFONDIMENTO SULLA SICUREZZA

La delega just-in-time (JIT) dei privilegi amministrativi riduce il rischio di furto di credenziali sui domain controller.

8. APPROFONDIMENTO SULLA SICUREZZA

La convalida continua registra e controlla il comportamento della sessione, sospendendo gli utenti che mostrano schemi anomali di esecuzione di script.

9. APPROFONDIMENTO SULLA SICUREZZA

Le difese perimetrali tradizionali non riescono a bloccare gli attacchi laterali una volta che una credenziale amministrativa è stata divulgata.

10. APPROFONDIMENTO SULLA SICUREZZA

La NIST Special Publication 800-207 (2020) fornisce una definizione astratta dell'architettura Zero Trust, con modelli di distribuzione. [1]

Riferimenti tecnici e fonti

La guida di studio e i puzzle interattivi sono compilati a partire dagli standard globali NIST, OWASP e di conformità alla privacy dei dati.

RIFERIMENTI ACCADEMICI E DI SETTORE

[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

Soluzioni: Punto di controllo 1 – Scelta multipla

1 Domanda 1

Risposta corretta: A

NOTA DIDATTICA

Qual è il principio fondamentale della sicurezza Zero Trust? → Non fidarsi mai, verificare sempre ogni richiesta di accesso indipendentemente dalla fonte

2 Domanda 2

Risposta corretta: A

NOTA DIDATTICA

Che cos'è la microsegmentazione della rete? → Suddividere le reti in zone piccole e isolate per contenere il movimento laterale

3 Domanda 3

Risposta corretta: A

NOTA DIDATTICA

Che cos'è il principio del privilegio minimo? → Limitare i permessi di accesso degli utenti a ciò che è strettamente necessario per il loro lavoro

4 Domanda 4

Risposta corretta: A

NOTA DIDATTICA

Che cos'è la gestione delle identità e degli accessi (IAM)? → Framework che gestiscono le identità digitali e controllano i privilegi di sistema

5 Domanda 5

Risposta corretta: A

NOTA DIDATTICA

Che cosa significa autenticazione continua? → Verificare ripetutamente l'identità dell'utente e la postura del dispositivo durante una sessione attiva

Soluzioni: Punto di controllo 2 – Vero o falso

6 **Domanda 6** — **Risposta corretta: Falso**

NOTA DIDATTICA

Falso: lo Zero Trust non concede alcuna fiducia implicita in base alla posizione nella rete, né all'interno né all'esterno.

7 **Domanda 7** — **Risposta corretta: Vero**

NOTA DIDATTICA

Vero: piccole zone isolate limitano fino a dove un intruso può spostarsi tra i server.

8 **Domanda 8** — **Risposta corretta: Falso**

NOTA DIDATTICA

Falso: il privilegio minimo concede solo l'accesso minimo necessario a ciascun ruolo.

9 **Domanda 9** — **Risposta corretta: Vero**

NOTA DIDATTICA

La verifica continua convalida lo stato di salute del dispositivo e le credenziali durante tutta la sessione di accesso.

10 **Domanda 10** — **Risposta corretta: Vero**

NOTA DIDATTICA

L'adozione di Zero Trust riduce l'impatto di credenziali aziendali compromesse.

Chiavi del vocabolario e griglia di valutazione

Griglia di valutazione per l'insegnante: assegna 1 punto per ogni abbinamento corretto (8 punti in totale) e per ogni termine di contesto (6 punti in totale).

PUNTO DI CONTROLLO 4: SOLUZIONI ABBINAMENTO DI CONCETTI

G 1. VERIFICA	F 2. SEGMENTAZIONE	A 3. IAM	B 4. PRIVILEGIO
H 5. POSTURA DI SICUREZZA	E 6. AUDITING	D 7. FIREWALL	C 8. ROUTER

PUNTO DI CONTROLLO 3: SOLUZIONI TERMINI CHIAVE

1 VERIFICA	2 SEGMENTAZIONE	3 GESTIONE IAM	4 PRIVILEGIO
5 POSTURA	6 AUDITING		

PUNTO DI CONTROLLO 6, ALTERNATIVA: SOLUZIONI ABBINAMENTO DI PAROLE

1 G – FIREWALL	2 F – AUDITING	3 D – PRIVILEGIO	4 B – SEGMENTAZIONE
5 H – ROUTER	6 E – POSTURA	7 C – GESTIONEIAM	8 A – VERIFICA

NOTE DI DISCUSSIONE PER GLI INSEGNANTI

Termini chiave:
Verifica che gli studenti sappiano spiegare VERIFICA, SEGMENTAZIONE e IAM con parole proprie e fare un esempio per ciascuno.

Casi di studio:
Chiedi agli studenti di motivare le loro raccomandazioni con fatti tratti dalla scheda anziché con supposizioni.

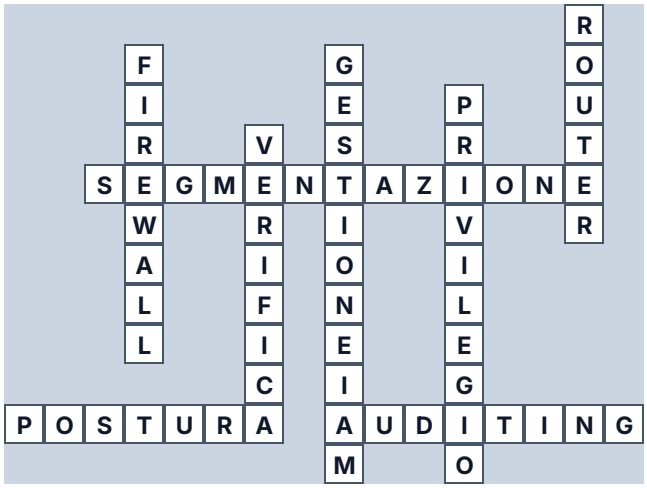
Valutazione delle fonti:
Fai verificare almeno un'affermazione con le fonti della scheda e discuti perché cifre, prezzi e regole possono cambiare nel tempo.

Soluzioni dei rompicapi e note per l'insegnante

SOLUZIONE DELLA RICERCA DELLE PAROLE

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

SOLUZIONE DEL CRUCIVERBA



GUIDA PER L'INSEGNANTE: SOLUZIONI DEL CRUCIVERBA

ORIZZONTALI

6 orizzontale: SEGMENTAZIONE Suddivisione delle zone interne della rete. (13 lettere)

7 orizzontale: POSTURA Valutazione dello stato di salute dei dispositivi. (7 lettere)

8 orizzontale: AUDITING Revisione delle sessioni di accesso registrate. (8 lettere)

VERTICALI

1 verticale: ROUTER Instradamento del traffico di pacchetti di rete. (6 lettere)

2 verticale: FIREWALL Protezione di barriera della rete esterna. (8 lettere)

3 verticale: GESTIONEIAM Gestione dell'accesso alle credenziali degli utenti. (11 lettere)

4 verticale: PRIVILEGIO Principio dei diritti di accesso minimi. (10 lettere)

5 verticale: VERIFICA Controllo costante delle credenziali degli utenti. (8 lettere)

Soluzioni delle parole mescolate e del codice cifrato

Chiave di valutazione per l'attività di riordino delle parole del vocabolario e per la sfida del codice segreto.

CHIAVE DELLE PAROLE DA RIORDINARE

1. CIFVIEAR — VERIFICA
2. IMEGAOSIENT — GESTIONEIAM
3. TPUASRO — POSTURA
4. ELLAWFIR — FIREWALL
5. ZOEGAEENITSNM — SEGMENTAZIONE
6. IIVEGPRLOI — PRIVILEGIO
7. AGTINUID — AUDITING
8. URRETO — ROUTER

CHIAVE DELLA SFIDA DEL CODICE SEGRETO

"VERIFICA SEMPRE CON ARCHITETTURA ZERO TRUST"

Soluzioni dei casi di studio

A Caso di studio 1: Passaggio a un'architettura di rete zero trust

Soluzione per l'insegnante

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Analisi dello scenario: una grande azienda usa attualmente una rete interna piatta in cui qualsiasi dispositivo della rete locale può accedere a tutti i server e i database aziendali.
- Strategia e soluzione consigliate: Segmenta la rete piatta in zone dipartimentali isolate. Installa firewall interni per controllare il traffico tra le zone e rendi obbligatoria la convalida dei token di connessione per tutti gli accessi.

B Caso di studio 2: Implementare controlli di accesso a privilegi minimi

Soluzione per l'insegnante

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Analisi dello scenario: I log di audit rivelano che utenti temporanei del database e dipendenti di basso livello hanno permessi globali di lettura e scrittura sui database contabili critici.
- Strategia e soluzione consigliate: Revoca tutti i privilegi amministrativi globali. Implementa il controllo degli accessi basato sui ruoli (RBAC) per corrispondere esattamente ai ruoli lavorativi e stabilisci revisioni settimanali automatiche dei permessi.