Nama: _____ Tanggal: _____ Nilai: _____

Arsitektur & Keamanan Zero Trust

Verifikasi berkelanjutan, mikrosegmentasi jaringan, Manajemen Identitas dan Akses, hak akses minimum, dan pemeriksaan postur.

GAMBARAN PEMBELAJARAN KEAMANAN ZERO TRUST

TERAMANKAN
ENKRIPSI DATA
Standar AES 256-bit

PATUH
STANDAR GLOBAL
Kerangka GDPR & CCPA

ZERO TRUST
KEBIJAKAN AKSES
Autentikasi Multifaktor

Selamat datang! Paket aktivitas ini memandu Anda mempelajari arsitektur dan keamanan Zero Trust. Anda akan mempelajari verifikasi berkelanjutan, mikrosegmentasi jaringan, pengelolaan identitas dan akses (IAM), hak akses minimal, serta audit sesi.

POS-POS LEMBAR KERJA

- [ ] **Bagian 1-4: Kuasai keamanan siber dan pencegahan ancaman.**
- [ ] **Bagian 5-7: Selesaikan teka-teki silang & pencarian kata.**
- [ ] **Bagian 8-9: Selesaikan studi kasus & tantangan sandi.**
- [ ] **Bagian 10: Pelajari halaman FAQ dasar & lanjutan.**
- [ ] **Bagian 11: Jelajahi 10 fakta menarik dari dunia nyata.**
- [ ] **Bonus: Tantangan Berpikir Cepat.**

Buka Panduan Keamanan Siber VPN.com

URL: https://www.vpn.com/cybersecurity/zero-trust-cyber-security/

Peta Belajar Strategi Zero Trust Anda

- Pahami prinsip inti verifikasi berkelanjutan.
- Terapkan mikrosegmentasi jaringan dan akses dengan hak minimal.
- Atur pemeriksaan postur perangkat dan audit sesi yang aktif.

PETUNJUK PANDUAN KEAMANAN ZERO TRUST

Jawab soal pilihan ganda dan benar/salah, lengkapi kalimat rumpang dengan kata dari bank kata, cocokkan definisi, lalu selesaikan teka-teki silang dan pencarian kata. Terapkan pengetahuan Anda pada arsitektur Zero Trust. Akhiri dengan aktivitas bonus Berpikir Cepat.

ARSITEKTUR & KEAMANAN ZERO TRUST (PENGANTAR)

Keamanan Zero Trust menggantikan model perimeter jaringan lama dengan kebijakan ketat 'jangan pernah percaya, selalu verifikasi'. Penerapan mikrosegmentasi, pengelolaan identitas dan akses (IAM), hak akses minimal, dan pemeriksaan postur perangkat menghambat pergerakan lateral ancaman.

BACA SETIAP POS DENGAN SAKSAMA DAN PILIH ATAU TULIS JAWABAN YANG BENAR.

Pos 1: Tantangan Pilihan Ganda

1. **1. Apa prinsip inti keamanan Zero Trust?**
   - A. Jangan pernah percaya; selalu verifikasi setiap permintaan akses apa pun sumbernya
   - B. Menganggap semua lalu lintas di dalam firewall perusahaan aman
   - C. Menyimpan file basis data tanpa enkripsi agar lebih cepat
   - D. Menerapkan autentikasi email hanya dengan catatan SPF

2. **2. Apa itu mikrosegmentasi jaringan?**
   - A. Membagi jaringan menjadi zona kecil yang terisolasi untuk membendung pergerakan lateral
   - B. Mengenkripsi kartu jaringan selama data dikirim
   - C. Menghubungkan semua server lokal ke satu alamat IP publik
   - D. Memantau ketikan pengguna di sesi browser

3. **3. Apa prinsip hak akses minimal?**
   - A. Membatasi izin akses pengguna hanya pada yang diperlukan untuk pekerjaannya
   - B. Memberikan semua hak sistem kepada setiap pengguna secara bawaan
   - C. Mengizinkan login anonim ke server basis data perusahaan
   - D. Mengatur router Wi-Fi publik tanpa kata sandi

4. **4. Apa itu pengelolaan identitas dan akses (IAM)?**
   - A. Kerangka kerja untuk mengelola identitas digital dan mengendalikan hak sistem
   - B. Utilitas antivirus yang memindai direktori file lokal
   - C. Sistem penyimpanan cadangan dengan media yang terputus dari jaringan
   - D. Protokol gateway email yang menolak domain tiruan

5. **5. Apa arti autentikasi berkelanjutan?**
   - A. Memverifikasi identitas pengguna dan postur perangkat berulang kali selama sesi aktif
   - B. Mengganti kata sandi utama setiap 10 menit
   - C. Melakukan hashing catatan basis data dengan beberapa algoritme
   - D. Mengenkripsi paket jaringan yang sedang dikirim dengan kunci TLS

Pos 2: Tantangan Benar atau Salah

6 Pertanyaan 6

6. Zero Trust menganggap semua lalu lintas di dalam firewall perusahaan aman.

Benar Salah

7 Pertanyaan 7

7. Mikrosegmentasi membatasi kemampuan penyerang untuk bergerak lateral di antara server internal.

Benar Salah

8 Pertanyaan 8

8. Hak akses minimal memberi akses ke semua file basis data secara bawaan.

Benar Salah

9 Pertanyaan 9

9. Verifikasi berkelanjutan memeriksa kesehatan perangkat dan kredensial selama sesi login berlangsung.

Benar Salah

10 Pertanyaan 10

10. Penerapan Zero Trust mengurangi dampak login perusahaan yang dibobol.

Benar Salah

Pos 3: Mengisi Istilah Kunci

Baca setiap kalimat di bawah ini dan isi bagian yang kosong dengan istilah yang tepat dari Bank Kata.

1. Pemeriksaan kredensial di setiap titik akses disebut _____ .
2. Membagi jaringan perusahaan menjadi zona-zona kecil disebut _____ .
3. Pengaturan identitas digital dan kontrol akses memakai _____ sebagai sistemnya.
4. Pembatasan izin pengguna memakai prinsip _____ .
5. Menilai kesehatan perangkat yang terhubung berarti memeriksa _____ .
6. Mencatat dan meninjau sesi yang aktif disebut _____ .

BANK KATA KOSAKATA

AUDIT KEAMANAN FIREWALL HAK AKSES MINIMAL IAM MIKROSEGMENTASI POSTUR PERANGKAT ROUTER VERIFIKASI BERKELANJUTAN

Tulis jawaban Anda di sini:

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

Pos 4: Pencocokan Konsep Keamanan

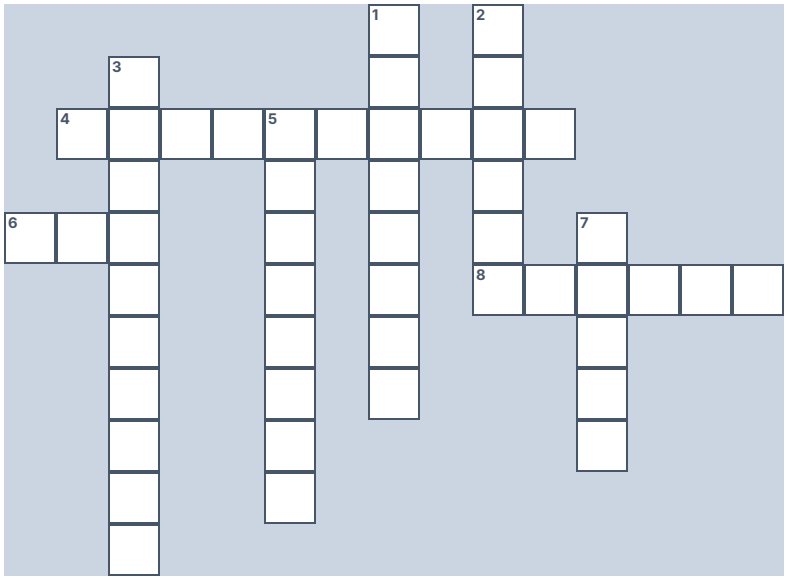
MENCOCOKKAN DEFINISI

Cocokkan setiap istilah di sebelah kiri dengan definisi yang benar di sebelah kanan dengan menulis huruf yang sesuai (A-H) di kotak isian.

☐	1. VERIFIKASI BERKELANJUTAN	A	Mengelola akses kredensial pengguna.
☐	2. MIKROSEGMENTASI	B	Prinsip hak akses paling sedikit.
☐	3. IAM	C	Merutekan lalu lintas paket jaringan.
☐	4. HAK AKSES MINIMAL	D	Penghalang pelindung dari jaringan luar.
☐	5. POSTUR PERANGKAT	E	Meninjau sesi akses yang tercatat.
☐	6. AUDIT KEAMANAN	F	Membagi zona jaringan internal.
☐	7. FIREWALL	G	Selalu memeriksa kredensial pengguna.
☐	8. ROUTER	H	Menilai status kesehatan perangkat.

Pos 5: Teka-Teki Silang

Selesaikan teka-teki silang dengan mengetik huruf di kotak putih yang aktif. Nomor-nomornya sesuai dengan petunjuk di bawah.



PETUNJUK MENDATAR

4. Pemeriksaan kredensial terus-menerus di setiap titik akses (10)

6. Singkatan untuk pengelolaan identitas digital dan akses (3)

8. Perangkat yang meneruskan paket data antarjaringan (6)

PETUNJUK MENURUN

1. Prinsip ... minimum membatasi apa yang boleh dilakukan pengguna (8)

2. Kondisi keamanan yang dinilai saat perangkat terhubung (6)

3. Pembagian jaringan menjadi zona kecil yang terisolasi (10)

5. Penghalang yang melindungi dari jaringan luar (8)

7. Pencatatan dan pemeriksaan sesi yang aktif (5)

Alternatif Pos 5: Petunjuk Teka-Teki Silang yang Aksesibel

Pengguna pembaca layar dan keyboard dapat mengetik jawaban teka-teki silang langsung di kolom teks di bawah ini.

PETUNJUK MENDATAR

4 mendatar: Pemeriksaan kredensial terus-menerus di setiap titik akses (10 huruf):

6 mendatar: Singkatan untuk pengelolaan identitas digital dan akses (3 huruf):

8 mendatar: Perangkat yang meneruskan paket data antarjaringan (6 huruf):

PETUNJUK MENURUN

1 menurun: Prinsip ... minimum membatasi apa yang boleh dilakukan pengguna (8 huruf):

2 menurun: Kondisi keamanan yang dinilai saat perangkat terhubung (6 huruf):

3 menurun: Pembagian jaringan menjadi zona kecil yang terisolasi (10 huruf):

5 menurun: Penghalang yang melindungi dari jaringan luar (8 huruf):

7 menurun: Pencatatan dan pemeriksaan sesi yang aktif (5 huruf):

Pos 6: Mencari Kata Tersembunyi

Temukan 8 istilah kunci yang tersembunyi dalam kisi di bawah ini. Kata dapat tersusun mendatar, menurun, atau diagonal.

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

DAFTAR KOSAKATA

VERIFIKASI SEGMENTASI IAM HAKAKSES ROUTER POSTUR AUDIT FIREWALL

Alternatif Pos 6: Pencocokan Kosakata yang Aksesibel

Cocokkan kedelapan istilah dari Pencarian Kata dengan definisi yang benar dengan menulis hurufnya (A-H) di tempat kosong.

ISTILAH KOSAKATA
A. VERIFIKASI
B. SEGMENTASI
C. IAM
D. HAKAKSES
E. POSTUR
F. AUDIT
G. FIREWALL
H. ROUTER

DEFINISI & KOLOM PENCOCOKAN

1. Penghalang yang melindungi dari jaringan luar.
2. Pencatatan dan pemeriksaan sesi yang aktif.
3. Prinsip ... minimum membatasi apa yang boleh dilakukan pengguna.
4. Pembagian jaringan menjadi zona kecil yang terisolasi.
5. Perangkat yang meneruskan paket data antarjaringan.
6. Kondisi keamanan yang dinilai saat perangkat terhubung.
7. Singkatan untuk pengelolaan identitas digital dan akses.
8. Pemeriksaan kredensial terus-menerus di setiap titik akses.

Pos 7: Tantangan Kata Acak

Susun ulang huruf di bawah ini untuk menemukan konsep dan istilah kunci keamanan siber. Tulis jawaban Anda di kotak isian yang tersedia.

1. **SKIFEVAIIR** _____
2. **MAI** _____
3. **PSTRUO** _____
4. **ELLAWFIR** _____
5. **ANIEMTESSG** _____
6. **ESASHKAK** _____
7. **ITADU** _____
8. **URRETO** _____

Aktivitas Bonus: Berpikir Cepat

3 JAWABAN UNTUK SETIAP KATEGORI. ORANG PERTAMA YANG MELENGKAPI DAFTAR MENANG.

1	Informasi yang tidak boleh dibagikan			
2	Kebiasaan aman yang bisa dimulai hari ini			
3	Hal yang diperiksa pada perangkat			
4	Hal yang dicatat dalam log			
5	Kata yang berkaitan dengan keamanan siber			
6	Hal yang diperiksa Zero Trust			
7	Tempat Anda menunjukkan identitas sehari-hari			
8	Cara membuktikan bahwa itu Anda			
9	Hal yang dilakukan setelah kebocoran data			
10	Tanda komputer terinfeksi			
11	Alasan memperbarui perangkat lunak			
12	Tingkat akses di perusahaan			
13	Alat keamanan yang Anda ketahui			
14	Zona yang bisa dibagi dalam jaringan			
15	Peribahasa tentang kepercayaan			

Pos 8: Studi Kasus Keamanan Siber

Terapkan konsep yang telah Anda pelajari untuk menyelesaikan skenario nyata di bawah ini.

STUDI KASUS 1: BERALIH KE ARSITEKTUR JARINGAN ZERO TRUST

👷

Skenario: Sebuah perusahaan besar memakai jaringan internal datar, sehingga perangkat mana pun di jaringan lokal dapat mengakses semua server dan basis data perusahaan.

Pertanyaan Diskusi: Rancang strategi mikrosegmentasi jaringan untuk membatasi pergerakan lateral.

STUDI KASUS 2: MENERAPKAN KONTROL AKSES DENGAN HAK MINIMAL

👷

Skenario: Log audit menunjukkan bahwa pengguna basis data sementara dan karyawan tingkat bawah memiliki izin baca dan tulis penuh ke basis data akuntansi yang penting.

Pertanyaan Diskusi: Audit dan batasi hak IAM basis data untuk menerapkan prinsip hak akses minimal.

Pos 9: Memecahkan Sandi

Seorang profesional keamanan siber melindungi aset jaringan dari pelaku ancaman online. Gunakan kunci Huruf-ke-Angka di bawah untuk memecahkan pesan dengan menulis huruf yang sesuai di tempat kosong.

KUNCI ENKRIPSI HURUF-KE-ANGKA

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

10	1	14	7	1	14		16	5	18	14	1	8		16	5	18	3	1	25	1

19	5	12	1	12	21		22	5	18	9	6	9	11	1	19	9

Pesan yang dipecahkan:

TIPS: SETIAP ANGKA MEWAKILI POSISI HURUF TERSEBUT DALAM ALFABET (MISALNYA 1 = A, 2 = B, 26 = Z).

Pos 10: FAQ Dasar Keamanan Siber (Bagian A)

Pelajari pertanyaan dan jawaban umum tentang cara mengurangi ancaman online.

Q1: Apa itu Zero Trust?

Zero Trust adalah kerangka keamanan yang menganggap ancaman ada di luar maupun di dalam batas jaringan, sehingga setiap permintaan harus diverifikasi. [1]

Q2: Apa aturan inti Zero Trust?

Jangan pernah percaya, selalu verifikasi.

Q3: Apa itu mikrosegmentasi?

Membagi jaringan menjadi segmen logis kecil yang aman untuk mengendalikan lalu lintas dan membendung pembobolan.

Q4: Apa itu hak akses minimal?

Memberi pengguna hanya hak akses minimum yang diperlukan untuk tugas pekerjaannya. [2]

Q5: Apa kepanjangan IAM?

Identity and Access Management (pengelolaan identitas dan akses).

Pos 10: FAQ Dasar Keamanan Siber (Bagian B)

Pelajari pertanyaan dan jawaban umum tentang cara mengurangi ancaman online.

Q6: Bagaimana pemeriksaan postur perangkat membantu?

Pemeriksaan ini memastikan perangkat sudah diperbarui, menjalankan antivirus aktif, dan aman sebelum diberi akses.

Q7: Apa itu pergerakan lateral?

Cara penyerang bergerak di dalam jaringan dari node pertama yang dibobol menuju sistem yang lebih berharga.

Q8: Apakah Zero Trust menggantikan firewall?

Tidak, Zero Trust memperkuat firewall dengan menambahkan pemeriksaan berbasis identitas dan firewall segmentasi internal.

Q9: Apa itu autentikasi berkelanjutan?

Verifikasi identitas pengguna secara terus-menerus selama sesi login aktif, bukan hanya saat pertama masuk.

Q10: Mengapa jaringan datar berbahaya?

Di jaringan datar, satu node yang dibobol memungkinkan penyerang dengan mudah mengakses basis data mana pun di jaringan itu.

Pos 10: FAQ Lanjutan Keamanan (Bagian C)

Jelajahi aspek teknis lanjutan dari kerangka keamanan, analisis malware, dan kepatuhan data.

Q1: Bagaimana Zero Trust menangani model perimeter?

Zero Trust menggantikan model usang 'benteng dan parit' dan memindahkan pertahanan dari batas jaringan ke identitas pengguna dan sumber daya tertentu.

Q2: Apa itu policy decision point (PDP)?

Komponen sistem yang menilai permintaan otorisasi berdasarkan aturan keamanan untuk memutuskan apakah akses diberikan.

Q3: Apa itu policy enforcement point (PEP)?

Node sistem (misalnya gateway atau proxy) yang benar-benar mengizinkan atau memblokir permintaan koneksi berdasarkan keputusan PDP.

Q4: Bagaimana Role-Based Access Control (RBAC) mendukung Zero Trust?

RBAC mengelompokkan izin ke dalam peran tertentu, membantu mencegah pengguna mewarisi hak administratif yang berlebihan.

Q5: Apa itu kontrol akses kontekstual?

Menilai permintaan login dengan petunjuk tambahan seperti lokasi geografis, postur perangkat, dan waktu login untuk memperkirakan risiko.

Pos 10: FAQ Lanjutan Keamanan (Bagian D)

Jelajahi aspek teknis lanjutan dari kerangka keamanan, analisis malware, dan kepatuhan data.

Q6: Apa bedanya mikrosegmentasi dengan VLAN standar?

VLAN membagi jaringan menjadi segmen logis yang luas di lapisan 2, sedangkan mikro-segmentasi menggunakan kebijakan perangkat lunak untuk mengisolasi beban kerja individual.

Q7: Apa itu akses just-in-time (JIT)?

Memberi izin administratif tambahan untuk sementara dan otomatis mencabutnya setelah tugas selesai.

Q8: Bagaimana mengamankan API dalam kerangka Zero Trust?

Dengan mewajibkan token OAuth yang ditandatangani secara kriptografis dan mengaudit tanda tangan permintaan di setiap gateway API.

Q9: Apa itu klien zero-trust network access (ZTNA)?

Agen perangkat lunak yang membangun koneksi keluar terenkripsi yang aman ke aplikasi tertentu, bukan ke seluruh subnet jaringan.

Q10: Bagaimana audit log membantu Zero Trust?

Pencatatan log terus-menerus memungkinkan alat analitik keamanan otomatis mendeteksi anomali dan segera menangguhkan login yang mencurigakan.

Bagian 11: 10 Fakta & Wawasan Keamanan Siber di Dunia Nyata

Pelajari fakta nyata tentang pelanggaran keamanan, mekanisme pertahanan, dan standar kepatuhan.

1. WAWASAN KEAMANAN

Arsitektur Zero Trust menggantikan model lama 'benteng dan parit' dengan aturan verifikasi berbasis identitas.

2. WAWASAN KEAMANAN

Mikro-segmentasi jaringan memperkecil area yang dapat dijangkau malware dengan mengisolasi beban kerja ke dalam zona-zona kecil yang terlindungi.

3. WAWASAN KEAMANAN

Zero Trust berfokus pada perlindungan sumber daya seperti aset, layanan, dan akun, alih-alih segmen jaringan. [1]

4. WAWASAN KEAMANAN

Kebijakan hak akses minimal mengurangi risiko data keluar dari basis data inti akibat ancaman orang dalam.

5. WAWASAN KEAMANAN

Validasi postur perangkat memeriksa tingkat pembaruan sistem operasi dan status antivirus aktif secara real time.

6. WAWASAN KEAMANAN

Broker Zero Trust Network Access (ZTNA) dapat menggantikan atau melengkapi VPN perusahaan untuk membatasi cakupan akses pengguna.

7. WAWASAN KEAMANAN

Pemberian hak administratif Just-in-Time (JIT) mengurangi risiko pencurian kredensial di domain controller.

8. WAWASAN KEAMANAN

Validasi berkelanjutan mencatat dan mengaudit perilaku sesi, lalu menangguhkan pengguna yang menunjukkan pola eksekusi skrip yang janggal.

9. WAWASAN KEAMANAN

Pertahanan perimeter tradisional gagal memblokir serangan lateral begitu kredensial administratif bocor.

10. WAWASAN KEAMANAN

NIST Special Publication 800-207 (2020) memberikan definisi abstrak arsitektur Zero Trust, beserta model penerapannya. [1]

Referensi & Sumber Teknis

Panduan belajar dan teka-teki interaktif ini disusun berdasarkan standar global NIST, OWASP, dan kepatuhan privasi data.

REFERENSI AKADEMIK & INDUSTRI

[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

Kunci Jawaban: Pos 1 - Pilihan Ganda

1 Soal 1

Jawaban Benar: A

CATATAN PENGAJAR

Apa prinsip inti keamanan Zero Trust? → Jangan pernah percaya; selalu verifikasi setiap permintaan akses apa pun sumbernya

2 Soal 2

Jawaban Benar: A

CATATAN PENGAJAR

Apa itu mikrosegmentasi jaringan? → Membagi jaringan menjadi zona kecil yang terisolasi untuk membendung pergerakan lateral

3 Soal 3

Jawaban Benar: A

CATATAN PENGAJAR

Apa prinsip hak akses minimal? → Membatasi izin akses pengguna hanya pada yang diperlukan untuk pekerjaannya [2]

4 Soal 4

Jawaban Benar: A

CATATAN PENGAJAR

Apa itu pengelolaan identitas dan akses (IAM)? → Kerangka kerja untuk mengelola identitas digital dan mengendalikan hak sistem

5 Soal 5

Jawaban Benar: A

CATATAN PENGAJAR

Apa arti autentikasi berkelanjutan? → Memverifikasi identitas pengguna dan postur perangkat berulang kali selama sesi aktif

Kunci Jawaban: Pos 2 - Benar atau Salah

6 **Soal 6** — **Jawaban Benar: Salah**

CATATAN PENGAJAR

Salah: Zero Trust tidak memberikan kepercayaan implisit berdasarkan lokasi jaringan, baik di dalam maupun di luar.

7 **Soal 7** — **Jawaban Benar: Benar**

CATATAN PENGAJAR

Benar: zona kecil yang terisolasi membatasi seberapa jauh penyusup dapat berpindah antar-server.

8 **Soal 8** — **Jawaban Benar: Salah**

CATATAN PENGAJAR

Salah: prinsip hak akses minimum hanya memberikan akses paling sedikit yang dibutuhkan setiap peran.

9 **Soal 9** — **Jawaban Benar: Benar**

CATATAN PENGAJAR

Verifikasi berkelanjutan memeriksa kesehatan perangkat dan kredensial selama sesi login berlangsung.

10 **Soal 10** — **Jawaban Benar: Benar**

CATATAN PENGAJAR

Penerapan Zero Trust mengurangi dampak login perusahaan yang dibobol.

Kunci Kosakata & Rubrik Penilaian

Rubrik Penilaian Pengajar: Berikan 1 poin untuk setiap pencocokan yang benar (total 8 poin) dan setiap istilah konteks yang benar (total 6 poin).

POS 4: KUNCI PENCOCOKAN KONSEP

G 1. VERIFIKASI BERKELANJUTAN	F 2. MIKROSEGMENTASI	A 3. IAM	B 4. HAK AKSES MINIMAL
H 5. POSTUR PERANGKAT	E 6. AUDIT KEAMANAN	D 7. FIREWALL	C 8. ROUTER

POS 3: KUNCI ISTILAH KUNCI

1 VERIFIKASI BERKELANJUTAN	2 MIKROSEGMENTASI	3 IAM	4 HAK AKSES MINIMAL
5 POSTUR PERANGKAT	6 AUDIT KEAMANAN		

ALTERNATIF POS 6: KUNCI PENCOCOKAN KOSAKATA

1 G – FIREWALL	2 F – AUDIT	3 D – HAKAKSES	4 B – SEGMENTASI
5 H – ROUTER	6 E – POSTUR	7 C – IAM	8 A – VERIFIKASI

CATATAN DISKUSI UNTUK PENGAJAR

Istilah Kunci:
Pastikan siswa dapat menjelaskan VERIFIKASI BERKELANJUTAN, MIKROSEGMENTASI, dan IAM dengan kata-kata sendiri serta memberi contoh untuk setiap istilah.

Studi Kasus:
Minta siswa mendukung rekomendasi mereka dengan fakta dari lembar kerja, bukan asumsi.

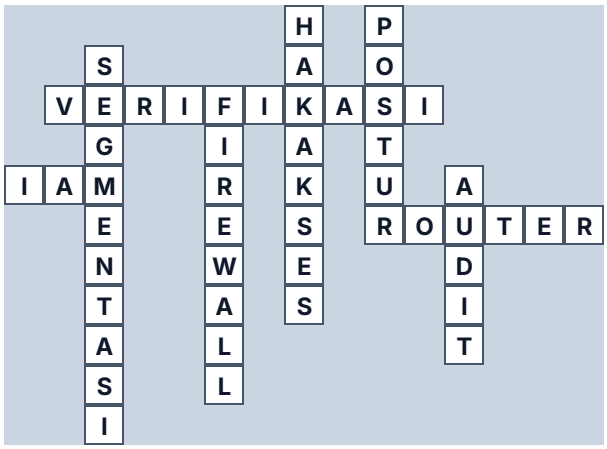
Evaluasi Sumber:
Minta siswa memeriksa setidaknya satu klaim terhadap referensi di lembar kerja, lalu diskusikan mengapa angka, harga, dan aturan dapat berubah seiring waktu.

Kunci Teka-Teki & Catatan Pengajar

JAWABAN PENCARIAN KATA

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

JAWABAN TEKA-TEKI SILANG



PANDUAN PENGAJAR UNTUK JAWABAN TEKA-TEKI SILANG

PETUNJUK MENDATAR

4 mendatar: VERIFIKASI Pemeriksaan kredensial terus-menerus di setiap titik akses (10 huruf)

6 mendatar: IAM Singkatan untuk pengelolaan identitas digital dan akses (3 huruf)

8 mendatar: ROUTER Perangkat yang meneruskan paket data antarjaringan (6 huruf)

PETUNJUK MENURUN

1 menurun: HAKAKSES Prinsip ... minimum membatasi apa yang boleh dilakukan pengguna (8 huruf)

2 menurun: POSTUR Kondisi keamanan yang dinilai saat perangkat terhubung (6 huruf)

3 menurun: SEGMENTASI Pembagian jaringan menjadi zona kecil yang terisolasi (10 huruf)

5 menurun: FIREWALL Penghalang yang melindungi dari jaringan luar (8 huruf)

7 menurun: AUDIT Pencatatan dan pemeriksaan sesi yang aktif (5 huruf)

Kunci Jawaban Kata Acak & Sandi

Kunci penilaian untuk aktivitas menyusun kata acak dan Tantangan Sandi Rahasia.

KUNCI KATA ACAK

1.	SKIFEVAIIR	VERIFIKASI	5.	ANIEMTESSG	SEGMENTASI
2.	MAI	IAM	6.	ESASHKAK	HAKAKSES
3.	PSTRUO	POSTUR	7.	ITADU	AUDIT
4.	ELLAWFIR	FIREWALL	8.	URRETO	ROUTER

KUNCI TANTANGAN SANDI RAHASIA

"JANGAN PERNAH PERCAYA SELALU VERIFIKASI"

Kunci Jawaban Studi Kasus

A Studi Kasus 1: Beralih ke Arsitektur Jaringan Zero Trust

Jawaban Pengajar

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Analisis Skenario: Sebuah perusahaan besar memakai jaringan internal datar sehingga perangkat mana pun di jaringan lokal dapat mengakses semua server dan basis data perusahaan.
- Strategi & Solusi yang Disarankan: Bagi jaringan datar menjadi zona per departemen yang terisolasi. Pasang firewall internal untuk mengendalikan lalu lintas antarzona, dan wajibkan validasi token koneksi untuk setiap akses.

B Studi Kasus 2: Menerapkan Kontrol Akses dengan Hak Minimal

Jawaban Pengajar

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Analisis Skenario: Log audit menunjukkan bahwa pengguna basis data sementara dan karyawan tingkat bawah memiliki izin baca dan tulis penuh ke basis data akuntansi yang penting.
- Strategi & Solusi yang Disarankan: Cabut semua hak administratif global. Terapkan Role-Based Access Control (RBAC) sesuai peran pekerjaan, dan jadwalkan peninjauan izin otomatis setiap minggu.