Nama: _____ Tanggal: _____ Nilai: _____

Perlindungan Data & Keamanan Penyimpanan Perusahaan

Penyamaran data, tokenisasi, enkripsi saat disimpan vs saat transit, cadangan offline

GAMBARAN PEMBELAJARAN PERLINDUNGAN DATA

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 standar dan kontrol perlindungan data. Anda akan mempelajari enkripsi disk penuh, kontrol akses yang aman, cadangan perangkat keras, postur keamanan cloud, dan teknik penyamaran data.

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/data-protection/

Peta Belajar Strategi Perlindungan Data Anda

- Bedakan teknik penyamaran data dan tokenisasi.
- Terapkan enkripsi saat disimpan untuk drive dan enkripsi saat transit dengan TLS.
- Rancang sistem cadangan offline yang terpisah dari jaringan untuk melindungi dari ransomware.

PETUNJUK PANDUAN PERLINDUNGAN DATA

Jawab soal pilihan ganda dan benar/salah, lengkapi kalimat rumpang dengan bank kata, cocokkan definisi, serta selesaikan teka-teki silang dan pencarian kata. Terapkan pengetahuan Anda tentang perlindungan data. Akhiri dengan aktivitas bonus Berpikir Cepat.

PERLINDUNGAN DATA & KEAMANAN PENYIMPANAN PERUSAHAAN (PENGANTAR)

Perlindungan data menjaga aset data perusahaan melalui masking, tokenisasi, enkripsi basis data saat tersimpan, dan protokol transmisi yang aman. Merancang cadangan yang terisolasi dari jaringan membantu memastikan basis data penting dapat dipulihkan saat terjadi intrusi aktif.

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

Pos 1: Tantangan Pilihan Ganda

1. Apa tujuan utama penyamaran data?

- A. Mengganti pengenal sensitif dengan karakter fiktif yang realistis untuk melindungi privasi
- B. Memadatkan berkas basis data besar untuk menghemat ruang server
- C. Menghapus email kontak pelanggan lama dari sistem arsip cadangan
- D. Menyembunyikan IP publik server basis data dari pemindaian internet

2. Mekanisme mana yang mengenkripsi berkas di hard drive server basis data?

- A. Enkripsi disk penuh saat disimpan
- B. Protokol handshake sesi TLS saat transit
- C. Aturan penerusan nameserver DNS dinamis
- D. Autentikasi multifaktor dengan kunci perangkat keras

3. Apa yang termasuk data saat transit?

- A. Paket data yang bergerak melewati router dan switch jaringan
- B. Log transaksi basis data di drive cadangan dingin
- C. Berkas pengguna yang diarsipkan di brankas cloud terisolasi
- D. Berkas konfigurasi statis di penyimpanan desktop lokal

4. Mengapa cadangan offline rutin penting untuk melindungi dari ransomware?

- A. Menyediakan salinan offline yang bersih untuk memulihkan berkas tanpa membayar tebusan
- B. Mencegah peretas memindai konfigurasi port terbuka
- C. Menaikkan kecepatan bandwidth jaringan lokal
- D. Mengotomatiskan log persetujuan cookie di browser

5. Apa fungsi tokenisasi data?

- A. Mengganti nomor kartu sensitif dengan token acak yang tidak sensitif
- B. Merutekan lalu lintas web lewat beberapa node onion
- C. Memindai direktori sistem dari malware berbasis signature
- D. Mengaudit waktu login administrator basis data

Pos 2: Tantangan Benar atau Salah

6 Pertanyaan 6

6. Penyamaran data mengubah catatan basis data produksi secara permanen.

Benar Salah

7 Pertanyaan 7

7. Cadangan di luar lokasi harus dipisahkan dari jaringan utama perusahaan agar ransomware tidak menyebar.

Benar Salah

8 Pertanyaan 8

8. Sertifikat SSL/TLS mengamankan basis data dengan mengenkripsi data yang tersimpan di media fisik.

Benar Salah

9 Pertanyaan 9

9. Zero-trust network access (ZTNA) memverifikasi identitas setiap pengguna sebelum memberi akses basis data.

Benar Salah

10 Pertanyaan 10

10. Tokenisasi berbasis vault menyimpan nilai kartu asli di token vault terpusat yang aman.

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. Mengganti nama pribadi dengan data pengganti yang realistis disebut _____ data.

2. Mengenkripsi blok penyimpanan fisik melindungi aset basis data _____ .

3. Protokol TLS mengenkripsi paket data aktif yang sedang dalam _____ .

4. Izin berbasis peran membatasi pengguna mana yang bisa mendapatkan _____ basis data.

5. Memulihkan file perusahaan yang bersih setelah kebocoran memerlukan _____ offline yang aman.

6. Mengaudit konfigurasi cloud menilai _____ keamanan sebuah organisasi.

BANK KATA KOSAKATA

CADANGAN ENKRIPSI HAKAKSES MINIMISASI PENYAMARAN POSTUR SAAT DISIMPAN TRANSIT

Tulis jawaban Anda di sini:

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

Pos 4: Pencocokan Konsep Keamanan

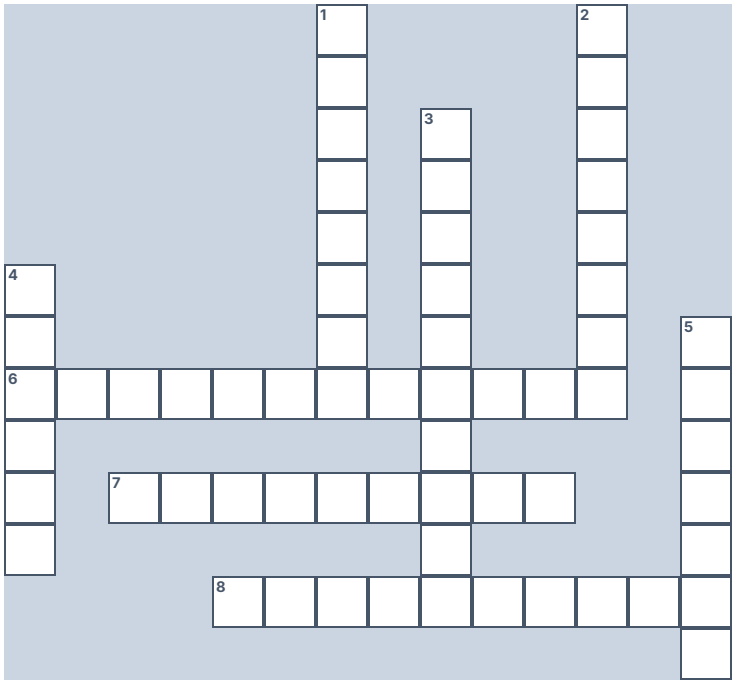
MENCOCOKKAN DEFINISI

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

☐	1. ENKRIPSI	A	Membuat salinan data yang aman di luar lokasi untuk pemulihan saat sistem gagal.
☐	2. CADANGAN	B	Mengubah teks biasa menjadi ciphertext yang tidak terbaca agar data yang disadap tetap privat.
☐	3. MINIMISASI	C	Status keamanan dan kesiapan pertahanan cloud organisasi secara keseluruhan.
☐	4. HAKAKSES	D	Memenuhi standar regulasi seperti GDPR atau CCPA dalam mengelola data pribadi pengguna.
☐	5. POSTUR PERANGKAT	E	Insiden keamanan ketika data yang dilindungi diakses atau diungkapkan tanpa izin.
☐	6. KEBOCORAN	F	Membatasi izin baca dan tulis basis data hanya untuk peran pengguna terautentikasi.
☐	7. KEPATUHAN	G	Mengganti karakter sensitif di kolom basis data untuk melindungi identitas pribadi.
☐	8. PENYAMARAN	H	Membatasi pengumpulan data pribadi seminimal yang diperlukan untuk operasional.

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

6. Kondisi data tersimpan yang dilindungi dengan mengenkripsi blok penyimpanan fisik (12)

7. Insiden keamanan saat data terlindungi diakses atau diungkap tanpa izin (9)

8. Penggantian data sensitif dengan token acak yang tidak bermakna (10)

PETUNJUK MENURUN

1. Izin baca dan tulis basis data yang dibatasi pada peran pengguna terautentikasi (8)

2. Salinan data aman di luar lokasi untuk pemulihan saat sistem gagal (8)

3. Penggantian karakter sensitif di kolom basis data untuk melindungi identitas pribadi (10)

4. Status keamanan dan kesiapan pertahanan cloud sebuah organisasi secara keseluruhan (6)

5. Kondisi paket data aktif yang sedang bergerak dan dienkripsi dengan protokol TLS (7)

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

6 mendatar: Kondisi data tersimpan yang dilindungi dengan mengenkripsi blok penyimpanan fisik (12 huruf):

7 mendatar: Insiden keamanan saat data terlindungi diakses atau diungkap tanpa izin (9 huruf):

8 mendatar: Penggantian data sensitif dengan token acak yang tidak bermakna (10 huruf):

PETUNJUK MENURUN

1 menurun: Izin baca dan tulis basis data yang dibatasi pada peran pengguna terautentikasi (8 huruf):

2 menurun: Salinan data aman di luar lokasi untuk pemulihan saat sistem gagal (8 huruf):

3 menurun: Penggantian karakter sensitif di kolom basis data untuk melindungi identitas pribadi (10 huruf):

4 menurun: Status keamanan dan kesiapan pertahanan cloud sebuah organisasi secara keseluruhan (6 huruf):

5 menurun: Kondisi paket data aktif yang sedang bergerak dan dienkripsi dengan protokol TLS (7 huruf):

Pos 6: Mencari Kata Tersembunyi

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

T R A N S I T K S Z V C Z W F

K N H Z D N D E Q X H P C U B

N A A Z N D K B A D A O D F H

A G I D R Q M O E I K R Z S F

R N Q V F A A C Q O A N P T T

A A X Q K R U O S D K N Y O B

M D F S X W J R A R S Z Y K Y

A A L G I M R A J M E L T E O

Y C H Q Q H Z N A O S V G N U

N B Y R Y B H L Z G J O P I N

E S A A T D I S I M P A N S W

P C M Z Y G Y O W U K V P A B

N V P O S T U R T M G V D S Y

U K R B X Z Y M R Q X I P I D

A D J Q V W W L J H T H G B E

DAFTAR KOSAKATA

PENYAMARAN SAATDISIMPAN TRANSIT HAKAKSES CADANGAN POSTUR KEBOCORAN TOKENISASI

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. PENYAMARAN**
- **B. SAATDISIMPAN**
- **C. TRANSIT**
- **D. HAKAKSES**
- **E. CADANGAN**
- **F. POSTUR**
- **G. KEBOCORAN**
- **H. TOKENISASI**

DEFINISI & KOLOM PENCOCOKAN

_____ 1. Status keamanan dan kesiapan pertahanan cloud sebuah organisasi secara keseluruhan.

_____ 2. Penggantian data sensitif dengan token acak yang tidak bermakna.

_____ 3. Izin baca dan tulis basis data yang dibatasi pada peran pengguna terautentikasi.

_____ 4. Salinan data aman di luar lokasi untuk pemulihan saat sistem gagal.

_____ 5. Insiden keamanan saat data terlindungi diakses atau diungkap tanpa izin.

_____ 6. Kondisi paket data aktif yang sedang bergerak dan dienkripsi dengan protokol TLS.

_____ 7. Penggantian karakter sensitif di kolom basis data untuk melindungi identitas pribadi.

_____ 8. Kondisi data tersimpan yang dilindungi dengan mengenkripsi blok penyimpanan fisik.

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. **AAMAEPRNYN** _____

2. **TATISNR** _____

3. **AACNGNAD** _____

4. **CNAOROKEB** _____

5. **APISNADMISAT** _____

6. **ESASHKAK** _____

7. **UPTRSO** _____

8. **SEIITNOSAK** _____

Aktivitas Bonus: Berpikir Cepat

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

1	Hal yang Anda cadangkan			
2	Kata yang berkaitan dengan keamanan siber			
3	Orang yang boleh melihat data sensitif			
4	Cara menghapus data dengan aman			
5	Tempat data disimpan			
6	Hal yang sebaiknya dienkripsi			
7	Data yang harus dilindungi rumah sakit			
8	Jenis cadangan data			
9	Informasi yang tidak boleh dibagikan			
10	Tanda bahaya dalam email			
11	Kebiasaan aman yang bisa dimulai hari ini			
12	Orang yang bisa dimintai bantuan TI			
13	Perangkat yang bisa diretas			
14	Cara melindungi data			
15	Hal yang bisa merusak data			

Pos 8: Studi Kasus Keamanan Siber

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

STUDI KASUS 1: PENINGKATAN ENKRIPSI BASIS DATA SAAT DISIMPAN



Skenario: Sebuah peritel daring menyimpan database transaksi di penyimpanan cloud tanpa enkripsi seluruh disk. Audit kepatuhan terbaru menandai hal ini sebagai risiko keamanan data CCPA yang serius. Rancang arsitektur pemulihan.

Pertanyaan Diskusi: Analisis risiko kepatuhan CCPA dan usulkan strategi enkripsi saat disimpan.

STUDI KASUS 2: PEMBENDUNGAN RANSOMWARE DAN PEMULIHAN DATA



Skenario: Serangan ransomware aktif sedang mengenkripsi drive jaringan di jaringan lokal perusahaan. Administrator mendeteksi infeksi sejak dini. Rencanakan langkah pembendungan dan pemulihan.

Pertanyaan Diskusi: Uraikan tindakan pembendungan segera dan rencanakan proses pemulihan yang aman.

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

19	9	13	16	1	14		3	1	4	1	14	7	1	14

19	5	3	1	18	1		15	6	6	12	9	14	5

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 perlindungan data?

Proses mengamankan data pribadi dan bisnis dari akses tanpa izin, kehilangan, atau kerusakan melalui kontrol teknis.

Q2: Mengapa enkripsi disk penuh penting?

Enkripsi ini mengamankan blok data di drive fisik sehingga tak seorang pun bisa membacanya jika hard drive dicuri.

Q3: Apa beda enkripsi saat disimpan dan saat transit?

Enkripsi saat disimpan mengamankan berkas di drive, sedangkan enkripsi saat transit mengamankan paket jaringan yang bergerak melewati router.

Q4: Apa itu penyamaran data?

Penyamaran mengganti detail sensitif (seperti nomor kartu kredit) dengan data fiktif yang realistis untuk pengujian tanpa membuka data asli.

Q5: Mengapa cadangan offline penting?

Metode ini menyimpan salinan bersih file Anda yang terisolasi dari jaringan, sehingga membantu melindungi cadangan Anda agar tidak dienkripsi oleh ransomware.

Pos 10: FAQ Dasar Keamanan Siber (Bagian B)

Pelajari pertanyaan dan jawaban umum tentang cara mengurangi ancaman online.

Q6: Apa itu brankas tokenisasi data?

Basis data aman dan terisolasi yang memetakan token acak ke nilai sensitif aslinya (seperti nomor kartu kredit).

Q7: Apa arti akses basis data zero-trust?

Artinya identitas dan kondisi perangkat setiap pengguna diverifikasi di setiap login, bukan langsung memercayai siapa pun di dalam jaringan.

Q8: Bagaimana TLS melindungi data saat transit?

TLS mengenkripsi muatan sesi TCP sehingga pelaku jahat di jaringan publik tidak bisa menyadap atau mengubah paket.

Q9: Apa itu audit akses basis data?

Pencatatan kueri dan login basis data secara terus-menerus untuk mendeteksi pola akses tanpa izin atau anomali keamanan.

Q10: Apa itu audit postur keamanan cloud?

Proses menganalisis konfigurasi cloud untuk menemukan port terbuka, aturan akses yang salah, dan celah kepatuhan keamanan.

Pos 10: FAQ Lanjutan Keamanan (Bagian C)

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

Q1: Bagaimana envelope encryption bekerja?

Data dienkripsi dengan kunci data, lalu kunci data itu dienkripsi dengan kunci induk, sehingga penyimpanan dan rotasi kunci lebih mudah.

Q2: Apa itu enkripsi homomorfik?

Metode enkripsi lanjutan yang memungkinkan operasi dilakukan langsung pada data terenkripsi tanpa mendekripsinya dulu.

Q3: Mengapa enkripsi tingkat kolom dipakai?

Enkripsi ini mengenkripsi kolom sensitif tertentu (seperti nomor jaminan sosial) satu per satu, sehingga tetap terlindungi meski admin bisa membaca tabel.

Q4: Apa itu data loss prevention (DLP)?

Perangkat lunak yang memantau titik keluar jaringan untuk mendeteksi dan memblokir pengiriman berkas sensitif tanpa izin.

Q5: Bagaimana cadangan write-once-read-many (WORM) melindungi dari ransomware?

Cadangan WORM mencegah berkas dihapus atau diubah selama jangka waktu tertentu, sehingga ransomware tidak bisa mengenkripsi cadangan yang ada.

Pos 10: FAQ Lanjutan Keamanan (Bagian D)

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

Q6: Apa risiko memakai ulang kunci?

Memakai kunci kriptografis yang sama di banyak basis data berarti satu kunci bocor membuka semua basis data.

Q7: Bagaimana tokenisasi basis data meningkatkan kepatuhan CCPA?

Token menyamarkan catatan (pseudonimisasi) di sistem non-produksi dan membatasi paparan saat terjadi kebocoran, tetapi data yang ditokenisasi tetap bisa tergolong informasi pribadi.

Q8: Mengapa klasifikasi data sangat penting?

Metode ini mengelompokkan file berdasarkan tingkat sensitivitas, membantu organisasi menerapkan enkripsi dan kontrol akses terkuat pada data berisiko tinggi.

Q9: Apa peran rotasi kunci?

Memperbarui kunci enkripsi secara rutin membatasi jumlah data lama yang terbuka jika satu kunci akhirnya dibobol.

Q10: Bagaimana secure enclave melindungi kueri basis data di memori?

Secure enclave mengisolasi operasi kueri di blok memori yang dilindungi CPU, sehingga administrator host tidak bisa melihat teks biasa di RAM.

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

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

1. WAWASAN KEAMANAN

Regulasi GDPR berlaku sejak Mei 2018 dan mengubah cara situs global mengelola persetujuan cookie dan data pribadi.

2. WAWASAN KEAMANAN

Denda pelanggaran GDPR bisa mencapai 20 juta Euro atau 4% omzet global, risiko hukum yang sangat besar. [4]

3. WAWASAN KEAMANAN

CCPA berlaku sejak Januari 2020 dan menjadi pelopor hak privasi digital konsumen di Amerika Serikat.

4. WAWASAN KEAMANAN

Minimisasi data memperkecil jejak penyimpanan, memangkas biaya operasional server sekaligus mengurangi skala dampak kebocoran.

5. WAWASAN KEAMANAN

Penghancuran kriptografis mengatasi sulitnya menghapus cadangan dengan menghapus kunci, bukan mengubah berkas pita cadangan lama.

6. WAWASAN KEAMANAN

Sebagian besar negara di dunia kini telah memberlakukan undang-undang pelindungan data pribadi untuk melindungi hak privasi konsumen.

7. WAWASAN KEAMANAN

Formulir persetujuan dengan kotak yang sudah dicentang secara tegas dilarang menurut definisi regulasi privasi data Eropa.

8. WAWASAN KEAMANAN

GDPR mewajibkan pelaporan pelanggaran data pribadi kepada otoritas pengawas dalam 72 jam sejak diketahui, jika memungkinkan. [3]

9. WAWASAN KEAMANAN

Melakukan hashing kata sandi dengan algoritma lambat seperti bcrypt atau Argon2 membuat pembobolan offline terhadap hash curian jauh lebih sulit. [6]

10. WAWASAN KEAMANAN

Data saat disimpan adalah berkas basis data tersimpan, sedangkan data saat transit adalah paket yang sedang bergerak melewati router jaringan.

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. (2025). SP 800-88 Rev. 2, Guidelines for Media Sanitization.
https://csrc.nist.gov/pubs/sp/800/88/r2/final

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

[3] Intersoft Consulting. (n.d.). Art. 33 GDPR – Notification of a personal data breach to the supervisory authority.
https://gdpr-info.eu/art-33-gdpr/

[4] Intersoft Consulting. (n.d.). Art. 83 GDPR – General conditions for imposing administrative fines.
https://gdpr-info.eu/art-83-gdpr/

[5] California Privacy Protection Agency. (n.d.). Frequently Asked Questions (FAQs).
https://cppa.ca.gov/faq.html

[6] OWASP. (n.d.). Password Storage Cheat Sheet.
https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

Kunci Jawaban: Pos 1 - Pilihan Ganda

1 Soal 1

Jawaban Benar: A

CATATAN PENGAJAR

Apa tujuan utama penyamaran data? → Mengganti pengenal sensitif dengan karakter fiktif yang realistis untuk melindungi privasi

2 Soal 2

Jawaban Benar: A

CATATAN PENGAJAR

Mekanisme mana yang mengenkripsi berkas di hard drive server basis data? → Enkripsi disk penuh saat disimpan

3 Soal 3

Jawaban Benar: A

CATATAN PENGAJAR

Apa yang termasuk data saat transit? → Paket data yang bergerak melewati router dan switch jaringan

4 Soal 4

Jawaban Benar: A

CATATAN PENGAJAR

Mengapa cadangan offline rutin penting untuk melindungi dari ransomware? → Menyediakan salinan offline yang bersih untuk memulihkan berkas tanpa membayar tebusan

5 Soal 5

Jawaban Benar: A

CATATAN PENGAJAR

Apa fungsi tokenisasi data? → Mengganti nomor kartu sensitif dengan token acak yang tidak sensitif

Kunci Jawaban: Pos 2 - Benar atau Salah

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

CATATAN PENGAJAR

Masking mengubah salinan uji atau menyembunyikan nilai saat kueri dijalankan; catatan produksi tetap tidak berubah.

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

CATATAN PENGAJAR

Cadangan di luar lokasi harus dipisahkan dari jaringan utama perusahaan agar ransomware tidak menyebar.

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

CATATAN PENGAJAR

Sertifikat TLS melindungi data saat transit; data saat disimpan memerlukan enkripsi disk, file, atau basis data.

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

CATATAN PENGAJAR

Zero-trust network access (ZTNA) memverifikasi identitas setiap pengguna sebelum memberi akses basis data.

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

CATATAN PENGAJAR

Tokenisasi berbasis vault menyimpan nilai asli di token vault aman yang memetakan setiap token kembali ke datanya.

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

B 1. ENKRIPSI	A 2. CADANGAN	H 3. MINIMISASI	F 4. HAKAKSES
C 5. POSTUR PERANGKAT	E 6. KEBOCORAN	D 7. KEPATUHAN	G 8. PENYAMARAN

POS 3: KUNCI ISTILAH KUNCI

1 PENYAMARAN	2 SAAT DISIMPAN	3 TRANSIT	4 HAKAKSES
5 CADANGAN	6 POSTUR		

ALTERNATIF POS 6: KUNCI PENCOCOKAN KOSAKATA

1 F – POSTUR	2 H – TOKENISASI	3 D – HAKAKSES	4 E – CADANGAN
5 G – KEBOCORAN	6 C – TRANSIT	7 A – PENYAMARAN	8 B – SAATDISIMPAN

CATATAN DISKUSI UNTUK PENGAJAR

Istilah Kunci:
Pastikan siswa dapat menjelaskan ENKRIPSI, CADANGAN, dan MINIMISASI dengan kata-kata sendiri serta memberi contoh untuk setiap istilah.

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

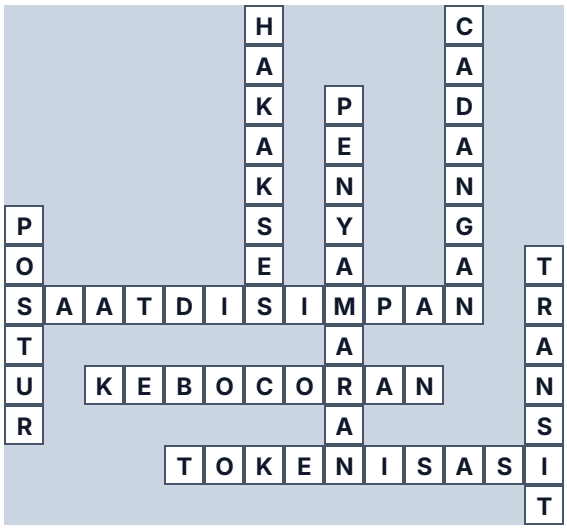
Evaluasi Sumber:
Minta siswa memeriksa setidaknya satu klaim terhadap referensi di lembar kerja, lalu diskusikan mengapa angka, harga, dan aturan dapat berubah seiring waktu.

Kunci Teka-Teki & Catatan Pengajar

JAWABAN PENCARIAN KATA

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

JAWABAN TEKA-TEKI SILANG



PANDUAN PENGAJAR UNTUK JAWABAN TEKA-TEKI SILANG

PETUNJUK MENDATAR

6 mendatar: SAATDISIMPAN Kondisi data tersimpan yang dilindungi dengan mengenkripsi blok penyimpanan fisik (12 huruf)

7 mendatar: KEBOCORAN Insiden keamanan saat data terlindungi diakses atau diungkap tanpa izin (9 huruf)

8 mendatar: TOKENISASI Penggantian data sensitif dengan token acak yang tidak bermakna (10 huruf)

PETUNJUK MENURUN

1 menurun: HAKAKSES Izin baca dan tulis basis data yang dibatasi pada peran pengguna terautentikasi (8 huruf)

2 menurun: CADANGAN Salinan data aman di luar lokasi untuk pemulihan saat sistem gagal (8 huruf)

3 menurun: PENYAMARAN Penggantian karakter sensitif di kolom basis data untuk melindungi identitas pribadi (10 huruf)

4 menurun: POSTUR Status keamanan dan kesiapan pertahanan cloud sebuah organisasi secara keseluruhan (6 huruf)

5 menurun: TRANSIT Kondisi paket data aktif yang sedang bergerak dan dienkripsi dengan protokol TLS (7 huruf)

Kunci Jawaban Kata Acak & Sandi

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

KUNCI KATA ACAK

1.	AAMAEPRNYN	PENYAMARAN	5.	APISNADMISAT	SAATDISIMPAN
2.	TATISNR	TRANSIT	6.	ESASHKAK	HAKAKSES
3.	AACNGNAD	CADANGAN	7.	UPTRSO	POSTUR
4.	CNAOROKEB	KEBOCORAN	8.	SEIITNOSAK	TOKENISASI

KUNCI TANTANGAN SANDI RAHASIA

"SIMPAN CADANGAN SECARA OFFLINE"

Kunci Jawaban Studi Kasus

A Studi Kasus 1: Peningkatan Enkripsi Basis Data Saat Disimpan

Jawaban Pengajar

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Analisis Skenario: Sebuah peritel daring menyimpan database transaksi di penyimpanan cloud tanpa enkripsi seluruh disk. Audit kepatuhan terbaru menandai hal ini sebagai risiko keamanan data CCPA yang serius. Rancang arsitektur pemulihan.
- Strategi & Solusi yang Disarankan: Terapkan enkripsi disk penuh AES-256 saat disimpan di semua sistem berkas. Gunakan Key Management Service (KMS) terpusat dengan rotasi otomatis dan terapkan kebijakan IAM yang ketat untuk mengendalikan akses dekripsi.

B Studi Kasus 2: Pembendungan Ransomware dan Pemulihan Data

Jawaban Pengajar

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Analisis Skenario: Serangan ransomware aktif sedang mengenkripsi drive jaringan di jaringan lokal perusahaan. Administrator mendeteksi infeksi sejak dini. Rencanakan langkah pembendungan dan pemulihan.
- Strategi & Solusi yang Disarankan: Segera isolasi segmen yang dibobol. Format endpoint yang terdampak dan pulihkan dari cadangan offline write-once-read-many (WORM) terbaru. Periksa keutuhan cadangan sebelum menyambungkan kembali sistem.