Nama: _____ Tanggal: _____ Nilai: _____

Serangan Ransomware & Pemulihan Bisnis

Eksekusi muatan, enkripsi berkas kriptografis, cadangan offline, prosedur penahanan, dan pemulihan bencana.

GAMBARAN PEMBELAJARAN SERANGAN RANSOMWARE

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 serangan ransomware dan pemulihan bisnis. Anda akan mempelajari eksekusi muatan, enkripsi berkas, cadangan offline, penahanan ancaman, pembayaran kripto, dan rencana pemulihan bencana.

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/ransomware-attack/

Peta Belajar Pemulihan Ransomware Anda

- Bedakan muatan trojan, ransomware, dan spyware.
- Analisis berkas jahat di dalam sandbox yang aman.
- Susun prosedur isolasi dan penahanan jaringan yang cepat.

PETUNJUK PANDUAN SERANGAN RANSOMWARE

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 pemulihan dari ransomware. Akhiri dengan aktivitas bonus Berpikir Cepat.

SERANGAN RANSOMWARE & PEMULIHAN BENCANA (PENGANTAR)

Muatan ransomware mengunci penyimpanan sistem secara kriptografis dan meminta tebusan kripto untuk kunci dekripsi. Mitigasinya meliputi aturan isolasi jaringan, analisis malware di sandbox, dan cadangan offline terpisah yang kuat.

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

Pos 1: Tantangan Pilihan Ganda

1. **1. Apa mekanisme utama serangan ransomware?**
   - A. Enkripsi kriptografis berkas pengguna untuk menolak akses sistem
   - B. Menyisipkan perintah SQL jahat ke kolom formulir
   - C. Menyadap paket jaringan di Wi-Fi publik
   - D. Memalsukan header email untuk melewati SPF

2. **2. Apa itu cadangan offline (dingin)?**
   - A. Salinan penyimpanan yang terputus dari jaringan agar terlindung dari penyebaran malware
   - B. Cadangan di hard drive server web utama
   - C. Cache sementara log registri sistem
   - D. Alat admin untuk mengatur ulang kata sandi

3. **3. Bagaimana tim keamanan mengisolasi sistem terinfeksi saat serangan ransomware?**
   - A. Segera cabut kabel jaringan dan matikan antarmuka nirkabel
   - B. Memperbarui basis data tanda tangan antivirus
   - C. Mematikan server DNS utama
   - D. Mengganti ekstensi berkas yang terdampak

4. **4. Mengapa lembaga keamanan menyarankan tidak membayar tebusan?**
   - A. Membayar mendorong penyerang dan tidak menjamin kunci dekripsi diberikan
   - B. Otomatis membatalkan semua polis asuransi perusahaan
   - C. Hal itu otomatis memberi tahu setiap pelanggan lewat email
   - D. Merusak berkas cadangan yang tersisa

5. **5. Apa itu rencana pemulihan bencana (DRP)?**
   - A. Proses terstruktur untuk memulihkan operasional dan data setelah sistem dibobol
   - B. Konfigurasi firewall untuk port masuk
   - C. Skema basis data hak admin pengguna
   - D. Protokol autentikasi email yang menolak domain tiruan

Pos 2: Tantangan Benar atau Salah

6 Pertanyaan 6

6. Muatan ransomware mudah menyebar ke cadangan online yang terhubung ke jaringan.

- ◯ Benar
- ◯ Salah

7 Pertanyaan 7

7. Membayar tebusan kripto menjamin berkas berhasil didekripsi.

- ◯ Benar
- ◯ Salah

8 Pertanyaan 8

8. Memutus sistem yang terinfeksi dari jaringan membantu menghentikan penyebaran ransomware ke sistem di sekitarnya.

- ◯ Benar
- ◯ Salah

9 Pertanyaan 9

9. Kriptografi simetris tidak pernah dipakai ransomware untuk mengenkripsi penyimpanan.

- ◯ Benar
- ◯ Salah

10 Pertanyaan 10

10. Menguji prosedur pemulihan data secara rutin adalah bagian penting pemulihan bencana.

- ◯ 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. Menolak akses ke berkas lokal memakai _____ .
2. Kode jahat aktif yang dijalankan di sistem disebut _____ .
3. Salinan penyimpanan luar lokasi yang terputus adalah _____ .
4. Menghentikan penyebaran malware memerlukan tindakan jaringan endpoint berupa _____ .
5. Pembayaran kripto yang diminta penjahat siber disebut _____ .
6. Mengembalikan berkas data operasional setelah bencana disebut _____ .

BANK KATA KOSAKATA

BENCANA CADANGAN LURING ENKRIPSI ISOLASI KUDA TROJAN MUATAN PEMULIHAN TEBUSAN

Tulis jawaban Anda di sini:

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

Pos 4: Pencocokan Konsep Keamanan

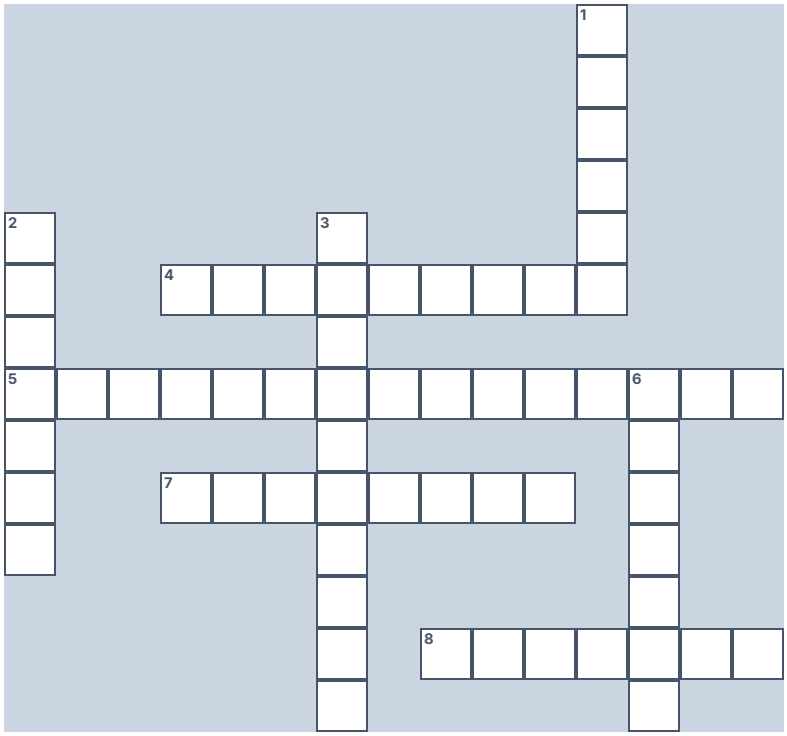
MENCOCOKKAN DEFINISI

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	Memutus sistem jaringan yang terinfeksi.
☐	2. MUATAN	B	Berkas jahat yang menyamar sebagai berkas bersih.
☐	3. CADANGAN LURING	C	Mengunci berkas secara kriptografis.
☐	4. ISOLASI	D	Peristiwa gangguan sistem yang besar.
☐	5. TEBUSAN	E	Menjalankan perangkat lunak jahat.
☐	6. PEMULIHAN	F	Salinan offline yang terputus.
☐	7. BENCANA	G	Memulihkan basis data dari cadangan.
☐	8. KUDA TROJAN	H	Permintaan bayaran untuk kunci kriptografis.

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. Mengembalikan data operasional setelah bencana (9)

5. Salinan terputus di luar lokasi yang tak terjangkau malware (15)

7. Yang dipakai ransomware untuk mengunci akses ke berkas lokal (8)

8. Pembayaran kripto yang diminta penjahat (7)

PETUNJUK MENURUN

1. Kode jahat aktif yang dijalankan di sistem (6)

2. Gangguan serius yang harus ditangani rencana DRP (7)

3. Berkas jahat yang menyamar sebagai program bersih (10)

6. Memutus perangkat terinfeksi agar malware tidak menyebar (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

4 mendatar: Mengembalikan data operasional setelah bencana (9 huruf):

5 mendatar: Salinan terputus di luar lokasi yang tak terjangkau malware (15 huruf):

7 mendatar: Yang dipakai ransomware untuk mengunci akses ke berkas lokal (8 huruf):

8 mendatar: Pembayaran kripto yang diminta penjahat (7 huruf):

PETUNJUK MENURUN

1 menurun: Kode jahat aktif yang dijalankan di sistem (6 huruf):

2 menurun: Gangguan serius yang harus ditangani rencana DRP (7 huruf):

3 menurun: Berkas jahat yang menyamar sebagai program bersih (10 huruf):

6 menurun: Memutus perangkat terinfeksi agar malware tidak menyebar (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.

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

DAFTAR KOSAKATA

ENKRIPSI MUATAN CADANGANOFFLINE ISOLASI TEBUSAN PEMULIHAN BENCANA KUDATROJAN

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. ENKRIPSI
B. MUATAN
C. CADANGANOFFLINE
D. ISOLASI
E. TEBUSAN
F. PEMULIHAN
G. BENCANA
H. KUDATROJAN

DEFINISI & KOLOM PENCOCOKAN

_____ 1. Salinan terputus di luar lokasi yang tak terjangkau malware.

_____ 2. Berkas jahat yang menyamar sebagai program bersih.

_____ 3. Yang dipakai ransomware untuk mengunci akses ke berkas lokal.

_____ 4. Pembayaran kripto yang diminta penjahat.

_____ 5. Memutus perangkat terinfeksi agar malware tidak menyebar.

_____ 6. Gangguan serius yang harus ditangani rencana DRP.

_____ 7. Kode jahat aktif yang dijalankan di sistem.

_____ 8. Mengembalikan data operasional setelah bencana.

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. **SRIEPNIK** _____
2. **AGFADNICEN AFLON** _____
3. **UTSNBAE** _____
4. **AEACNBN** _____
5. **TANMAU** _____
6. **SOAILIS** _____
7. **IPANHUELM** _____
8. **AARNKTUOJD** _____

Aktivitas Bonus: Berpikir Cepat

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

1	Informasi yang tidak boleh dibagikan			
2	Perangkat yang bisa diretas			
3	Alasan tidak membayar tebusan			
4	Kebiasaan aman yang bisa dimulai hari ini			
5	Alat keamanan yang Anda ketahui			
6	Cara melindungi akun Anda			
7	Tanda komputer terinfeksi			
8	Tempat menyimpan cadangan			
9	File yang tidak ingin Anda kehilangan			
10	Cara ransomware menyebar			
11	Hal yang dilakukan di jam pertama serangan			
12	Orang yang dihubungi saat terjadi serangan			
13	Hal yang bisa dikunci ransomware			
14	Kata yang berkaitan dengan keamanan siber			
15	Organisasi yang sering diserang			

Pos 8: Studi Kasus Keamanan Siber

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

STUDI KASUS 1: PENAHANAN MUATAN RANSOMWARE PERUSAHAAN



Skenario: Jaringan lokal sebuah perusahaan dibobol ransomware yang aktif. Server berkas utama mulai menampilkan ekstensi .locked.

Pertanyaan Diskusi: Uraikan langkah penahanan, dan susun rencana pemulihan protokol.

STUDI KASUS 2: MENILAI ARSITEKTUR CADANGAN OFFLINE



Skenario: Sebuah perusahaan ingin merancang strategi pencadangan data yang mengurangi risiko cadangan ikut dibobol, meskipun jaringan lokal utama sepenuhnya dikuasai ransomware.

Pertanyaan Diskusi: Rancang sistem penyimpanan cadangan offline 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		1	14	4	1

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 ransomware?

Ransomware adalah perangkat lunak jahat yang memblokir akses ke sistem atau berkas sampai tebusan dibayar.

Q2: Bagaimana ransomware menyebar?

Lewat lampiran email phishing, celah perangkat lunak yang belum ditambal, dan sistem akses jarak jauh yang dibobol. [1]

Q3: Mengapa tebusan diminta dalam mata uang kripto?

Mata uang kripto seperti Bitcoin relatif anonim, sehingga aparat sulit melacak dananya.

Q4: Apakah antivirus memblokir ransomware?

Ya, tetapi antivirus berbasis tanda tangan bisa gagal melawan ransomware zero-day yang baru dibuat.

Q5: Apa itu cadangan air-gapped?

Salinan cadangan tanpa hubungan fisik maupun logis ke jaringan utama, sehingga terlindung dari penyebaran.

Pos 10: FAQ Dasar Keamanan Siber (Bagian B)

Pelajari pertanyaan dan jawaban umum tentang cara mengurangi ancaman online.

Q6: Apa itu pemerasan ganda?

Saat penyerang tidak hanya mengenkripsi berkas tetapi juga mencuri data sensitif dan mengancam membocorkannya jika tidak dibayar.

Q7: Apa itu dekriptor?

Utilitas berisi kunci kriptografis untuk mengembalikan berkas yang terkunci.

Q8: Bagaimana mendeteksi ransomware sejak dini?

Dengan memantau sistem berkas untuk perubahan dan penggantian nama berkas massal yang tiba-tiba.

Q9: Apa peran asuransi?

Asuransi siber dapat membantu menanggung biaya pemulihan, tetapi ketentuan pertanggungan dan aturan pembayaran tebusan berbeda-beda menurut polis.

Q10: Perlukah sistem terinfeksi dinyalakan ulang?

Tidak, menyalakan ulang dapat menghapus bukti di memori; isolasi dari jaringan saja. [1]

Pos 10: FAQ Lanjutan Keamanan (Bagian C)

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

Q1: Bagaimana ransomware memakai enkripsi asimetris?

Kunci publik di dalam malware dipakai untuk mengenkripsi berkas, dan dekripsinya butuh kunci privat penyerang.

Q2: Mengapa enkripsi simetris juga dipakai?

Enkripsi simetris (seperti AES) cepat dan bisa mengunci basis data besar dalam hitungan menit, sementara kunci asimetris mengamankan kunci AES.

Q3: Apa itu segmentasi logis?

Membagi jaringan menjadi zona terisolasi agar malware tidak menyebar dari komputer kerja ke server inti.

Q4: Apa itu penyimpanan WORM?

Media Write-Once, Read-Many yang mencegah data cadangan diubah, ditimpa, atau dihapus ransomware.

Q5: Apa itu shadow copy?

Snapshot cadangan lokal buatan Windows; ransomware biasanya menghapusnya lebih dulu dengan alat admin.

Pos 10: FAQ Lanjutan Keamanan (Bagian D)

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

Q6: Bagaimana pencurian kredensial memungkinkan ransomware?

Penyerang membeli login admin yang bocor untuk masuk lewat remote desktop, lalu menjalankan ransomware secara manual di jaringan.

Q7: Apa itu uji coba pemulihan?

Rutin memulihkan cadangan ke lingkungan uji terisolasi untuk memastikan kecepatan pemulihan dan keutuhan data memenuhi target.

Q8: Bagaimana EDR menghentikan ransomware?

Dengan menganalisis perilaku proses (misalnya enkripsi yang cepat) dan segera menangguhkan aplikasi jahat tersebut.

Q9: Apa itu model ransomware-as-a-service (RaaS)?

Model waralaba saat pembuat malware menyewakan alat ransomware ke afiliasi dengan imbalan persentase tebusan.

Q10: Bagaimana RDP yang belum ditambal memicu ransomware?

Gateway Remote Desktop Protocol yang terbuka dan belum ditambal memungkinkan penyerang membobol login dan menjalankan malware secara manual.

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

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

1. WAWASAN KEAMANAN

Pelaku ransomware sering menggunakan alat seperti vssadmin.exe untuk menghapus shadow copy Windows dan memblokir pemulihan lokal. [1]

2. WAWASAN KEAMANAN

Kunci simetris AES-256 biasanya dipakai mengenkripsi berkas, lalu dikunci dengan kunci publik RSA.

3. WAWASAN KEAMANAN

Pemulihan dari serangan ransomware yang berhasil dapat memakan waktu berminggu-minggu, itulah sebabnya cadangan offline yang telah diuji itu penting.

4. WAWASAN KEAMANAN

FBI tidak mendukung pembayaran tebusan dan memperingatkan bahwa membayar tidak menjamin Anda akan mendapatkan data kembali. [2]

5. WAWASAN KEAMANAN

Rencana pemulihan bencana (DRP) harus menetapkan Recovery Time Objective (RTO) dan Recovery Point Objective (RPO).

6. WAWASAN KEAMANAN

FBI merekomendasikan cadangan yang terenkripsi dan immutable, artinya tidak dapat diubah atau dihapus. [3]

7. WAWASAN KEAMANAN

Pembuat ransomware memakai obfuskasi canggih untuk lolos dari antivirus berbasis tanda tangan.

8. WAWASAN KEAMANAN

Segmentasi jaringan membatasi pergerakan lateral, sehingga membantu mencegah ransomware menyebar melampaui host pertama yang terinfeksi. [3]

9. WAWASAN KEAMANAN

Layanan jarak jauh yang terekspos dan kurang aman seperti Remote Desktop Protocol (RDP) adalah titik masuk ransomware yang umum. [1]

10. WAWASAN KEAMANAN

CISA menyarankan agar cadangan terenkripsi disimpan secara offline, karena banyak varian ransomware mencari dan menghapus cadangan yang dapat dijangkau. [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] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[2] FBI Internet Crime Complaint Center. (n.d.). Ransomware.
https://www.ic3.gov/CrimeInfo/Ransomware

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

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

Kunci Jawaban: Pos 1 - Pilihan Ganda

1 Soal 1

Jawaban Benar: A

CATATAN PENGAJAR

Apa mekanisme utama serangan ransomware? → Enkripsi kriptografis berkas pengguna untuk menolak akses sistem

2 Soal 2

Jawaban Benar: A

CATATAN PENGAJAR

Apa itu cadangan offline (dingin)? → Salinan penyimpanan yang terputus dari jaringan agar terlindung dari penyebaran malware

3 Soal 3

Jawaban Benar: A

CATATAN PENGAJAR

Bagaimana tim keamanan mengisolasi sistem terinfeksi saat serangan ransomware? → Segera cabut kabel jaringan dan matikan antarmuka nirkabel

4 Soal 4

Jawaban Benar: A

CATATAN PENGAJAR

Mengapa lembaga keamanan menyarankan tidak membayar tebusan? → Membayar mendorong penyerang dan tidak menjamin kunci dekripsi diberikan

5 Soal 5

Jawaban Benar: A

CATATAN PENGAJAR

Apa itu rencana pemulihan bencana (DRP)? → Proses terstruktur untuk memulihkan operasional dan data setelah sistem dibobol

Kunci Jawaban: Pos 2 - Benar atau Salah

6 Soal 6

Jawaban Benar: Benar

CATATAN PENGAJAR

Muatan ransomware mudah menyebar ke cadangan online yang terhubung ke jaringan.

7 Soal 7

Jawaban Benar: Salah

CATATAN PENGAJAR

Salah: FBI memperingatkan bahwa membayar tidak menjamin Anda akan mendapatkan data kembali. [2]

8 Soal 8

Jawaban Benar: Benar

CATATAN PENGAJAR

Benar: CISA menyarankan mencabut host yang terinfeksi atau memutus jaringan untuk menahan penyebaran.

9 Soal 9

Jawaban Benar: Salah

CATATAN PENGAJAR

Salah: ransomware biasanya mengenkripsi berkas dengan cipher simetris yang cepat seperti AES.

10 Soal 10

Jawaban Benar: Benar

CATATAN PENGAJAR

Menguji prosedur pemulihan data secara rutin adalah bagian penting pemulihan bencana.

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

C 1. ENKRIPSI	E 2. MUATAN	F 3. CADANGAN LURING	A 4. ISOLASI
H 5. TEBUSAN	G 6. PEMULIHAN	D 7. BENCANA	B 8. KUDA TROJAN

POS 3: KUNCI ISTILAH KUNCI

1 ENKRIPSI	2 MUATAN	3 CADANGAN LURING	4 ISOLASI
5 TEBUSAN	6 PEMULIHAN		

ALTERNATIF POS 6: KUNCI PENCOCOKAN KOSAKATA

1 C – CADANGANOFFLINE	2 H – KUDATROJAN	3 A – ENKRIPSI	4 E – TEBUSAN
5 D – ISOLASI	6 G – BENCANA	7 B – MUATAN	8 F – PEMULIHAN

CATATAN DISKUSI UNTUK PENGAJAR

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

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

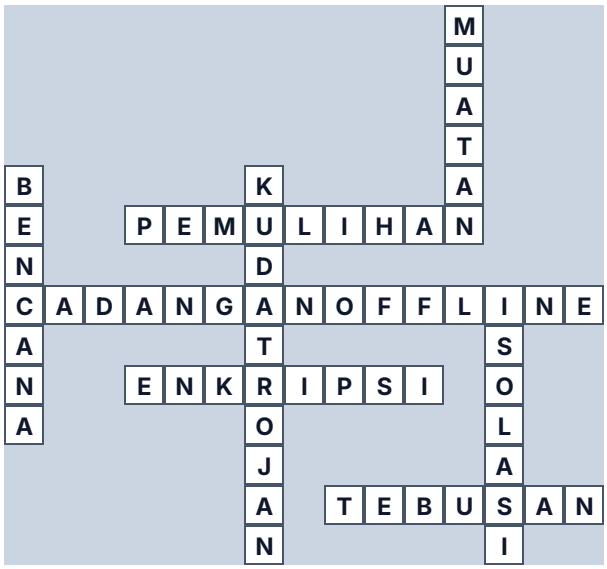
Evaluasi Sumber:
Minta siswa memeriksa setidaknya satu klaim terhadap referensi di lembar kerja, lalu diskusikan mengapa angka, harga, dan aturan dapat berubah seiring waktu.

Kunci Teka-Teki & Catatan Pengajar

JAWABAN PENCARIAN KATA

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

JAWABAN TEKA-TEKI SILANG



PANDUAN PENGAJAR UNTUK JAWABAN TEKA-TEKI SILANG

PETUNJUK MENDATAR

4 mendatar: PEMULIHAN Mengembalikan data operasional setelah bencana (9 huruf)

5 mendatar: CADANGANOFFLINE Salinan terputus di luar lokasi yang tak terjangkau malware (15 huruf)

7 mendatar: ENKRIPSI Yang dipakai ransomware untuk mengunci akses ke berkas lokal (8 huruf)

8 mendatar: TEBUSAN Pembayaran kripto yang diminta penjahat (7 huruf)

PETUNJUK MENURUN

1 menurun: MUATAN Kode jahat aktif yang dijalankan di sistem (6 huruf)

2 menurun: BENCANA Gangguan serius yang harus ditangani rencana DRP (7 huruf)

3 menurun: KUDATROJAN Berkas jahat yang menyamar sebagai program bersih (10 huruf)

6 menurun: ISOLASI Memutus perangkat terinfeksi agar malware tidak menyebar (7 huruf)

Kunci Jawaban Kata Acak & Sandi

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

KUNCI KATA ACAK

1. SRIEPNIK — **ENKRIPSI**
2. AGFADNICENAFLON — **CADANGANOFFLINE**
3. UTSNBAE — **TEBUSAN**
4. AEACNBN — **BENCANA**
5. TANMAU — **MUATAN**
6. SOAILIS — **ISOLASI**
7. IPANHUELM — **PEMULIHAN**
8. AARNKTUOJD — **KUDATROJAN**

KUNCI TANTANGAN SANDI RAHASIA

"SIMPAN CADANGAN ANDA SECARA OFFLINE"

Kunci Jawaban Studi Kasus

A Studi Kasus 1: Penahanan Muatan Ransomware Perusahaan

Jawaban Pengajar

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Analisis Skenario: Jaringan lokal sebuah perusahaan dibobol ransomware yang aktif. Server berkas utama mulai menampilkan ekstensi .locked.
- Strategi & Solusi yang Disarankan: Putuskan semua server terdampak dari jaringan lokal. Hentikan sesi administratif yang aktif. Pulihkan berkas yang tidak terdampak dari sistem cadangan offline yang aman dan terkunci dari penulisan.

B Studi Kasus 2: Menilai Arsitektur Cadangan Offline

Jawaban Pengajar

PEDOMAN PENILAIAN

Jawaban siswa harus mencakup poin-poin berikut:

- Analisis Skenario: Sebuah perusahaan ingin merancang strategi pencadangan data yang mengurangi risiko cadangan ikut dibobol, meskipun jaringan lokal utama sepenuhnya dikuasai ransomware.
- Strategi & Solusi yang Disarankan: Terapkan penyimpanan write-once-read-many (WORM). Buat pemisahan logis dengan memutus sistem cadangan dari semua jaringan, dan wajibkan rotasi media fisik setiap hari.