Nama: _____ Tanggal: _____ Nilai: _____

# Perangkat Lunak Antivirus & Perlindungan Endpoint

Deteksi signature, heuristik, pemantauan perilaku, sandbox, pembaruan

## GAMBARAN PEMBELAJARAN PERANGKAT LUNAK ANTIVIRUS

**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** perangkat lunak antivirus dan perlindungan endpoint. Anda akan mempelajari basis data signature, pemindai heuristik, pemantauan perilaku, file virtual di sandbox, dan cara mengurangi positif palsu.

**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/antivirus/

# Peta Belajar Strategi Antivirus Anda

- Bedakan deteksi malware berbasis signature dan berbasis heuristik.
- Pahami pemantauan perilaku dan protokol isolasi sandbox.
- Evaluasi dampak pemindaian waktu nyata terhadap kinerja sistem dan endpoint.
- Kurangi positif palsu dengan verifikasi sertifikat digital.
- Kelola distribusi pembaruan definisi harian ke seluruh endpoint perusahaan.

## PETUNJUK PANDUAN ANTIVIRUS

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 keamanan antivirus di endpoint. Akhiri dengan aktivitas bonus Berpikir Cepat.

## PERLINDUNGAN ANTIVIRUS & PEMINDAIAN SIGNATURE (PENGANTAR)

Perangkat lunak antivirus melindungi endpoint dengan mengenali, mengarantina, dan menghapus malware. Sistem modern menggabungkan basis data signature (mencocokkan hash ancaman yang dikenal) dengan heuristik (menganalisis struktur file) dan pemantauan perilaku untuk mendeteksi eksploit zero-day.

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

## Pos 1: Tantangan Pilihan Ganda

**1. Apa kelemahan deteksi berbasis signature?**

- A. Tidak dapat mengenali malware yang tidak dikenal atau sudah dimodifikasi
- B. Menghasilkan banyak positif palsu
- C. Membutuhkan daya prosesor yang besar
- D. Hanya bekerja saat terhubung ke internet

**2. Bagaimana pemindai heuristik mendeteksi varian malware baru?**

- A. Dengan mengenali pola dan struktur kode yang mencurigakan
- B. Dengan mencocokkan hash file dengan basis data ancaman
- C. Dengan otomatis menghapus semua program tanpa tanda tangan digital
- D. Dengan mengunggah setiap file ke folder cloud publik

**3. Apa tujuan menjalankan file di sandbox antivirus?**

- A. Mengisolasi dan menganalisis file di ruang virtual yang aman
- B. Mempercepat pencadangan sistem file lokal
- C. Memperbarui patch keamanan sistem operasi
- D. Mengompres dokumen besar untuk menghemat ruang

**4. Metode deteksi apa yang menandai perilaku ancaman secara waktu nyata?**

- A. Analisis perilaku yang memantau tindakan perangkat lunak
- B. Pemeriksaan log lama pada malam hari
- C. Laporan manual pengguna tentang aplikasi yang lambat
- D. Peninjauan manual mingguan atas program yang terpasang

**5. Mengapa pembaruan definisi rutin penting bagi pemindai?**

- A. Untuk memasok mesin signature dengan penanda ancaman terbaru
- B. Untuk meningkatkan kecepatan prosesor
- C. Untuk mengubah waktu cache nameserver DNS
- D. Untuk mengizinkan pengaturan cookie browser

## Pos 2: Tantangan Benar atau Salah

### 6 Pertanyaan 6

6. Deteksi signature mencocokkan hash kriptografis file dengan daftar di basis data.

Benar Salah

### 7 Pertanyaan 7

7. Pemindai heuristik dapat memicu peringatan positif palsu pada file yang aman.

Benar Salah

### 8 Pertanyaan 8

8. Sandbox mengizinkan malware mengakses file jaringan tanpa batas.

Benar Salah

### 9 Pertanyaan 9

9. Pemindaian perilaku memblokir file saat file itu menunjukkan tindakan berbahaya.

Benar Salah

### 10 Pertanyaan 10

10. Antivirus standar sepenuhnya menghentikan semua serangan zero-day.

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. Pemindai tradisional mengandalkan pencocokan _____ untuk mengenali malware yang sudah dikenal.**

**2. Menganalisis pola kode file disebut pemindaian _____ .**

**3. Antivirus mengisolasi file mencurigakan di dalam _____ (lingkungan terisolasi).**

**4. Pemantauan waktu nyata mengawasi _____ program untuk mendeteksi aktivitas mencurigakan.**

**5. Pemindai mengunduh _____ basis data setiap hari untuk mengenali ancaman baru.**

**6. Program aman yang ditandai sebagai malware memicu peringatan _____ .**

**BANK KATA KOSAKATA**

ALAT ANTIVIRUS HEURISTIK ISOLASI ANCAMAN PALSU PEMBARUAN PERILAKU SANDBOX SIGNATURE

**Tulis jawaban Anda di sini:**

**1.** **2.**

**3.** **4.**

**5.** **6.**

# Pos 4: Pencocokan Konsep Keamanan

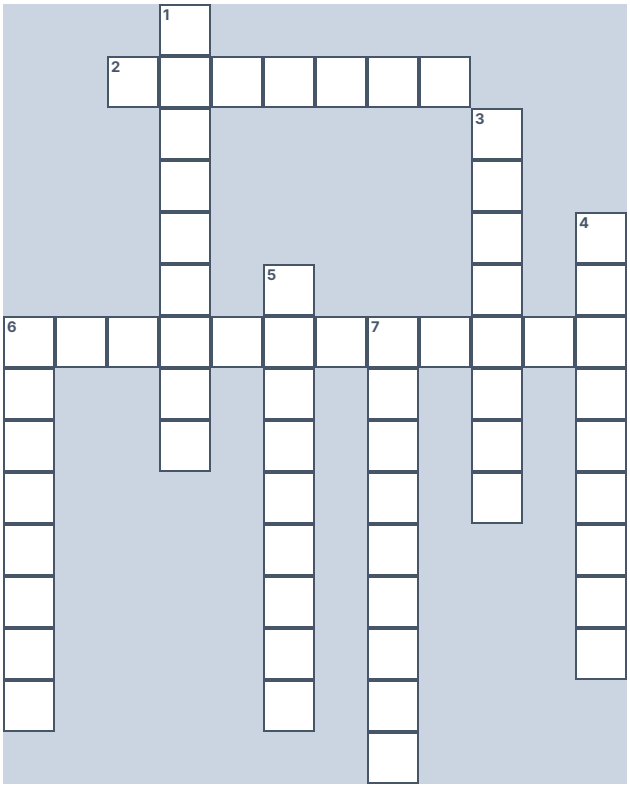
**MENCOCOKKAN DEFINISI**

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

| | | | |
|---|---|---|---|
| ☐ | 1. Signature Hash | A | Mengurung file mencurigakan agar tidak membahayakan sistem lokal. |
| ☐ | 2. Heuristik Kode | B | Paket perangkat lunak yang memindai dan melindungi endpoint dari eksploit. |
| ☐ | 3. Sandbox File | C | Memantau tindakan perangkat lunak yang berjalan untuk mencari pola berbahaya. |
| ☐ | 4. Pemindaian Perilaku | D | Jejak kriptografis unik dalam basis data untuk mengenali ancaman yang sudah dikenal. |
| ☐ | 5. Pembaruan Harian | E | Lingkungan uji virtual yang aman untuk menjalankan kode tak tepercaya. |
| ☐ | 6. Positif Palsu | F | Unduhan definisi rutin untuk memperbarui basis data ancaman. |
| ☐ | 7. Isolasi Ancaman | G | Analisis berbasis aturan yang menandai file dengan susunan kode mencurigakan. |
| ☐ | 8. Alat Antivirus | H | Peringatan keamanan yang keliru menganggap perangkat lunak aman sebagai malware. |

## 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

**2. Lingkungan uji virtual yang aman untuk menjalankan kode tak dikenal (7)**

**6. Peringatan yang keliru menganggap perangkat lunak aman sebagai malware (12)**

### PETUNJUK MENURUN

**1. Folder terisolasi tempat file mencurigakan dikurung (9)**

**3. Hal yang diawasi pemantauan saat program sedang berjalan (8)**

**4. Analisis berbasis aturan yang menandai file dengan kode mencurigakan (9)**

**5. Jejak kriptografis unik untuk mengenali ancaman yang sudah dikenal (9)**

**6. Bagian program yang menelusuri file dan endpoint untuk mencari ancaman (8)**

**7. Unduhan definisi baru secara rutin untuk basis data ancaman (9)**

# 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 PETUNJUK MENURUN

## PETUNJUK MENDATAR

**2 mendatar: Lingkungan uji virtual yang aman untuk menjalankan kode tak dikenal (7 huruf):**

**6 mendatar: Peringatan yang keliru menganggap perangkat lunak aman sebagai malware (12 huruf):**

## PETUNJUK MENURUN

**1 menurun: Folder terisolasi tempat file mencurigakan dikurung (9 huruf):**

**3 menurun: Hal yang diawasi pemantauan saat program sedang berjalan (8 huruf):**

**4 menurun: Analisis berbasis aturan yang menandai file dengan kode mencurigakan (9 huruf):**

**5 menurun: Jejak kriptografis unik untuk mengenali ancaman yang sudah dikenal (9 huruf):**

**6 menurun: Bagian program yang menelusuri file dan endpoint untuk mencari ancaman (8 huruf):**

**7 menurun: Unduhan definisi baru secara rutin untuk basis data ancaman (9 huruf):**

## Pos 6: Mencari Kata Tersembunyi

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

I D R Q M E I P R Z S F Q V F

A U A Q O N P E T X K Q K R U

S K D N Y B F M S X A W J A R

E A Z Y S Y L B G I R M R J M

R L L T A O H A Q Q A H Z H A

U I O V N G U R B Y N R Y E B

T R H L D Z G U J O T P N U W

A E C M B Z Y A G Y I O W R U

N P K V O P B N N V N T M I G

G V D Y X U K R B X A Z Y S M

I P O S I T I F P A L S U T R

S Q X I P D A D J Q V W W I L

J H P E M I N D A I T H G K B

E I K T S V R Z E H E S C A L

Q C Z M K V R U A S W J M M H

**DAFTAR KOSAKATA**

SIGNATURE HEURISTIK SANDBOX PERILAKU PEMBARUAN KARANTINA POSITIFPALSU PEMINDAI

# 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. SIGNATURE |
| B. HEURISTIK |
| C. SANDBOX |
| D. PERILAKU |
| E. PEMBARUAN |
| F. KARANTINA |
| G. POSITIFPALSU |
| H. PEMINDAI |

**DEFINISI & KOLOM PENCOCOKAN**

1. Hal yang diawasi pemantauan saat program sedang berjalan.
2. Bagian program yang menelusuri file dan endpoint untuk mencari ancaman.
3. Unduhan definisi baru secara rutin untuk basis data ancaman.
4. Analisis berbasis aturan yang menandai file dengan kode mencurigakan.
5. Peringatan yang keliru menganggap perangkat lunak aman sebagai malware.
6. Jejak kriptografis unik untuk mengenali ancaman yang sudah dikenal.
7. Lingkungan uji virtual yang aman untuk menjalankan kode tak dikenal.
8. Folder terisolasi tempat file mencurigakan dikurung.

## 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. **TANISUREG** _____

2. **SNXOBDA** _____

3. **PRAEUNBAM** _____

4. **SPTSFUILAPOI** _____

5. **TIEKSRHIU** _____

6. **KUIAPLER** _____

7. **TKNAIAANR** _____

8. **IENIPADM** _____

# Aktivitas Bonus: Berpikir Cepat

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

| | | | | |
|---|---|---|---|---|
| 1 | Alasan memperbarui perangkat lunak | | | |
| 2 | Orang yang bisa dimintai bantuan TI | | | |
| 3 | Hal yang dilakukan saat antivirus menemukan ancaman | | | |
| 4 | Tanda virus komputer | | | |
| 5 | Hal yang dikarantina | | | |
| 6 | Tempat virus bersembunyi | | | |
| 7 | Informasi yang tidak boleh dibagikan | | | |
| 8 | Jenis perangkat lunak berbahaya | | | |
| 9 | Alat keamanan yang Anda ketahui | | | |
| 10 | Hal yang dipindai antivirus | | | |
| 11 | Hal yang Anda cadangkan | | | |
| 12 | Perangkat yang bisa diretas | | | |
| 13 | Program antivirus yang Anda ketahui | | | |
| 14 | Alasan alarm palsu | | | |
| 15 | Kebiasaan aman yang bisa dimulai hari ini | | | |

# Pos 8: Studi Kasus Keamanan Siber

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

## STUDI KASUS 1: SIGNATURE VS. HEURISTIK



**Skenario: Seorang karyawan mengunduh alat buatan internal dari tim lain.** Pemindai signature meloloskannya, tetapi pemindai heuristik menandainya sebagai mencurigakan.

**Pertanyaan Diskusi: Jelaskan mengapa hal ini terjadi dan bagaimana memastikan file** tersebut aman.

## STUDI KASUS 2: MENANGANI POSITIF PALSU



**Skenario: Seorang pengembang mengompilasi aplikasinya. Antivirus sistem** menandai file program baru itu sebagai malware dan mengarantinanya.

**Pertanyaan Diskusi: Uraikan risiko whitelisting dan jelaskan cara** penyelesaian yang benar.

## 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**

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 20 | 5 | 13 | 21 | 11 | 1 | 14 | | 13 | 1 | 12 | 23 | 1 | 18 | 5 | | 2 | 1 | 18 | 21 |
| | | | | | | | | | | | | | | | | | | | |
| 4 | 5 | 14 | 7 | 1 | 14 | | 8 | 5 | 21 | 18 | 9 | 19 | 20 | 9 | 11 | | | | |
| | | | | | | | | | | | | | | | | | | | |

**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: Bagaimana antivirus mengenali malware?

Dengan mencocokkan signature di basis data, menganalisis susunan kode secara heuristik, dan memantau perilaku secara waktu nyata.

### Q2: Apa itu deteksi berbasis signature?

Metode pemindaian yang mencocokkan hash kriptografis file dengan daftar malware yang sudah dikenal.

### Q3: Apa itu pemindai heuristik?

Heuristik menganalisis struktur dan instruksi kode file, lalu menandai pola mencurigakan yang umum pada varian malware.

### Q4: Apa artinya jika file dikarantina?

Antivirus memindahkan file ke folder terisolasi yang aman dan mencegahnya dijalankan untuk melindungi sistem operasi.

### Q5: Apa itu positif palsu pada antivirus?

Kesalahan saat perangkat lunak yang sah dan aman keliru ditandai sebagai malware oleh algoritme pemindai.

# Pos 10: FAQ Dasar Keamanan Siber (Bagian B)

Pelajari pertanyaan dan jawaban umum tentang cara mengurangi ancaman online.

### Q6: Bagaimana pemantauan perilaku melindungi sistem?

Pemantauan ini mengawasi perangkat lunak secara waktu nyata dan memblokir proses yang mencoba perubahan mencurigakan seperti menyisipkan kode.

### Q7: Mengapa pengujian di sandbox penting?

Sandbox menjalankan file tak tepercaya di mesin virtual terisolasi sehingga tindakannya dapat diamati tanpa membahayakan sistem.

### Q8: Seberapa sering definisi antivirus harus diperbarui?

Pemindai sebaiknya memperbarui definisi setiap hari atau setiap jam agar mengenali jenis malware baru.

### Q9: Apa perbedaan antivirus dan EDR?

Antivirus berfokus pada pemindaian file, sedangkan Endpoint Detection and Response (EDR) melacak dan membendung ancaman di seluruh jaringan.

### Q10: Bolehkah menjalankan dua antivirus sekaligus?

Tidak. Dua pemindai aktif menimbulkan konflik sistem, memperlambat kinerja, dan dapat saling memblokir.

# Pos 10: FAQ Lanjutan Keamanan (Bagian C)

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

### Q1: Bagaimana aturan heuristik mengurangi ancaman yang lolos?

Heuristik menganalisis pola ancaman secara umum, bukan signature tertentu, sehingga dapat menangkap varian modifikasi dari keluarga malware yang dikenal.

### Q2: Apa itu virus polimorfik?

Malware yang mengubah susunan file dan rutinitas dekripsinya setiap kali dijalankan sehingga pemindaian signature tidak efektif.

### Q3: Bagaimana sandbox mendeteksi upaya menghindari mesin virtual?

Sandbox modern meniru klik mouse dan waktu aktif sistem untuk mengelabui malware yang dirancang bersembunyi saat berjalan di mesin virtual.

### Q4: Dalam format apa pembaruan signature diunduh?

Biasanya berupa file selisih biner bertahap yang ringan sehingga hemat bandwidth.

### Q5: Bagaimana agen endpoint mengelola pemindaian lokal?

Agen melakukan pemeriksaan ringan di latar belakang dan menyerahkan pencarian hash yang berat ke basis data ancaman di cloud.

# Pos 10: FAQ Lanjutan Keamanan (Bagian D)

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

### Q6: Apa itu pemindaian deteksi rootkit?

Pemindaian tabel memori di tingkat kernel yang melewati API sistem operasi yang dibajak rootkit untuk menyembunyikan dirinya.

### Q7: Bagaimana pemindaian perilaku memblokir ransomware?

Pemindaian ini mendeteksi enkripsi file massal otomatis dan menghentikan prosesnya sebelum basis data terkunci.

### Q8: Apa itu verifikasi sertifikat penandatanganan kode?

Pemindai memeriksa tanda tangan digital kode terhadap otoritas sertifikat tepercaya untuk memastikan identitas pengembang.

### Q9: Bagaimana packer memengaruhi mesin pemindai?

Packer mengompres atau mengenkripsi muatan malware, sehingga pemindai harus membongkar file di memori sebelum pencocokan signature dilakukan.

### Q10: Bagaimana EDR mengisolasi secara otomatis?

Agen EDR mengarantina endpoint yang terinfeksi di tingkat jaringan untuk mencegah pergerakan lateral, sambil tetap memberi akses kepada analis.

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

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

**1. WAWASAN KEAMANAN**

Basis data signature menyimpan hash malware yang sudah dikenal, sehingga file yang benar-benar baru atau diubah akan lolos sampai definisi diperbarui.

**2. WAWASAN KEAMANAN**

Mesin heuristik dapat menandai sebagian varian malware baru sebelum signature-nya tersedia, dengan konsekuensi lebih banyak positif palsu.

**3. WAWASAN KEAMANAN**

Peringatan positif palsu menyita waktu tim TI untuk memverifikasi dan memulihkan file yang keliru dikarantina.

**4. WAWASAN KEAMANAN**

Malware polimorfik mengubah kodenya di setiap salinan, sehingga pihak bertahan memadukan signature dengan pemeriksaan heuristik dan perilaku.

**6. WAWASAN KEAMANAN**

Pembuat malware menulis kode khusus untuk memeriksa lingkungan sandbox dan menunda eksekusi agar lolos dari batas waktu.

**5. WAWASAN KEAMANAN**

Mesin antivirus berbasis cloud mencocokkan hash file mencurigakan dengan basis data ancaman daring berskala besar secara hampir real-time.

**7. WAWASAN KEAMANAN**

Vendor mengirim pembaruan definisi ke endpoint secara berkala agar pemindai dapat mengenali ancaman yang baru dikonfirmasi.

**8. WAWASAN KEAMANAN**

Pemantau perilaku ransomware mengawasi panggilan API Win32 tertentu yang terkait enkripsi file dan penghapusan shadow copy.

**9. WAWASAN KEAMANAN**

Signature kode yang valid dapat menurunkan risiko positif palsu, tetapi file bertanda tangan tetap dipindai, karena malware pun bisa ditandatangani.

**10. WAWASAN KEAMANAN**

Rootkit mengubah struktur kernel sistem sehingga dibutuhkan pemindai khusus saat boot untuk mendeteksi dan membersihkannya.

# Referensi & Sumber Teknis

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

## REFERENSI AKADEMIK & INDUSTRI

[1] NIST. (2013). SP 800-83 Rev. 1, Guide to Malware Incident Prevention and Handling for Desktops and Laptops.
https://csrc.nist.gov/pubs/sp/800/83/r1/final

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

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

[4] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[5] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.
https://csrc.nist.gov/pubs/sp/800/61/r3/final

## Kunci Jawaban: Pos 1 - Pilihan Ganda

**1 Soal 1** SIGNATURE — **Jawaban Benar: A**

### CATATAN PENGAJAR

Pemindaian signature mengandalkan hash yang sudah dikenal sehingga gagal mendeteksi malware yang tidak dikenal atau dimodifikasi.

**2 Soal 2** HEURISTIK — **Jawaban Benar: A**

### CATATAN PENGAJAR

Heuristik menganalisis susunan kode dan perintah untuk mengenali ciri mencurigakan dari varian ancaman baru.

**3 Soal 3** SANDBOX — **Jawaban Benar: A**

### CATATAN PENGAJAR

Sandbox menjalankan file mencurigakan di mesin virtual terisolasi untuk mengamati perilakunya dengan aman.

**4 Soal 4** PERILAKU — **Jawaban Benar: A**

### CATATAN PENGAJAR

Pemindaian perilaku memantau program yang berjalan secara waktu nyata untuk memblokir perubahan sistem tanpa izin.

**5 Soal 5** PEMBARUAN — **Jawaban Benar: A**

### CATATAN PENGAJAR

Pemindai mengunduh pembaruan definisi bertahap setiap hari agar selalu mengikuti perkembangan ancaman.

## Kunci Jawaban: Pos 2 - Benar atau Salah

**6** **Soal 6** SIGNATURE — **Jawaban Benar: Benar**

### CATATAN PENGAJAR

Alat signature menghitung hash kriptografis lalu mencocokkannya dengan basis data hash ancaman yang dikenal.

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

### CATATAN PENGAJAR

Mesin heuristik memakai aturan yang dapat menandai file sah dan aman sebagai mencurigakan.

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

### CATATAN PENGAJAR

Sandbox menjalankan kode di wadah virtual dan memblokir akses ke folder bersama di jaringan.

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

### CATATAN PENGAJAR

Pemantauan waktu nyata menandai proses yang mencoba menulis atau mengunci file secara tidak sah.

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

### CATATAN PENGAJAR

Tidak ada antivirus yang menghentikan setiap serangan zero-day; ancaman yang belum dikenal dapat lolos dari signature dan heuristik.

# Kunci Kosakata & Rubrik Penilaian

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

## POS 4: KUNCI PENCOCOKAN KONSEP

| | | | |
|---|---|---|---|
| D 1. Signature Hash | G 2. Heuristik Kode | E 3. Sandbox File | C 4. Pemindaian Perilaku |
| F 5. Pembaruan Harian | H 6. Positif Palsu | A 7. Isolasi Ancaman | B 8. Alat Antivirus |

## POS 3: KUNCI ISTILAH KUNCI

| | | | |
|---|---|---|---|
| 1 SIGNATURE | 2 HEURISTIK | 3 SANDBOX | 4 PERILAKU |
| 5 PEMBARUAN | 6 PALSU | | |

## ALTERNATIF POS 6: KUNCI PENCOCOKAN KOSAKATA

| | | | |
|---|---|---|---|
| 1 D – PERILAKU | 2 H – PEMINDAI | 3 E – PEMBARUAN | 4 B – HEURISTIK |
| 5 G – POSITIFPALSU | 6 A – SIGNATURE | 7 C – SANDBOX | 8 F – KARANTINA |

### CATATAN DISKUSI UNTUK PENGAJAR

**Istilah Kunci:**
Pastikan siswa dapat menjelaskan Signature Hash, Heuristik Kode, dan Sandbox File dengan kata-kata sendiri serta memberi contoh untuk setiap istilah.

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

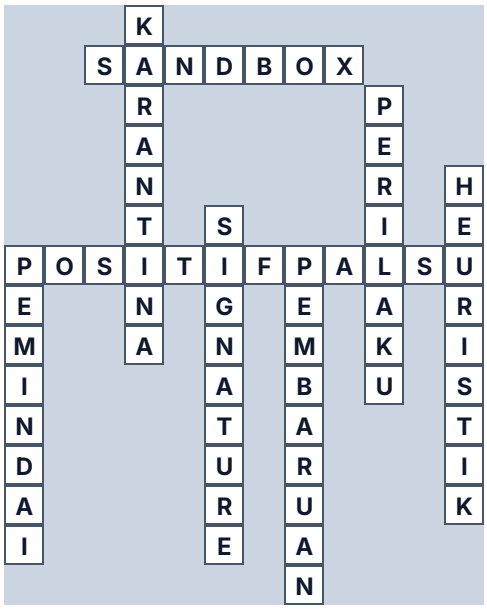
**Evaluasi Sumber:**
Minta siswa memeriksa setidaknya satu klaim terhadap referensi di lembar kerja, lalu diskusikan mengapa angka, harga, dan aturan dapat berubah seiring waktu.

# Kunci Teka-Teki & Catatan Pengajar

## JAWABAN PENCARIAN KATA

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

## JAWABAN TEKA-TEKI SILANG




### PETUNJUK MENDATAR

**2 mendatar: SANDBOX** Lingkungan uji virtual yang aman untuk menjalankan kode tak dikenal (7 huruf)

**6 mendatar: POSITIFPALSU** Peringatan yang keliru menganggap perangkat lunak aman sebagai malware (12 huruf)

### PETUNJUK MENURUN

**1 menurun: KARANTINA** Folder terisolasi tempat file mencurigakan dikurung (9 huruf)

**3 menurun: PERILAKU** Hal yang diawasi pemantauan saat program sedang berjalan (8 huruf)

**4 menurun: HEURISTIK** Analisis berbasis aturan yang menandai file dengan kode mencurigakan (9 huruf)

**5 menurun: SIGNATURE** Jejak kriptografis unik untuk mengenali ancaman yang sudah dikenal (9 huruf)

**6 menurun: PEMINDAI** Bagian program yang menelusuri file dan endpoint untuk mencari ancaman (8 huruf)

**7 menurun: PEMBARUAN** Unduhan definisi baru secara rutin untuk basis data ancaman (9 huruf)

# Kunci Jawaban Kata Acak & Sandi

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

### KUNCI KATA ACAK

| | | | | | |
|---|---|---|---|---|---|
| 1. | T A N I S U R E G | SIGNATURE | 5. | T I E K S R H I U | HEURISTIK |
| 2. | S N X O B D A | SANDBOX | 6. | K U I A P L E R | PERILAKU |
| 3. | P R A E U N B A M | PEMBARUAN | 7. | T K N A I A A N R | KARANTINA |
| 4. | S P T S F U I L A P O I | POSITIFPALSU | 8. | I E N I P A D M | PEMINDAI |

### KUNCI TANTANGAN SANDI RAHASIA

**"TEMUKAN MALWARE BARU DENGAN HEURISTIK"**

# Kunci Jawaban Studi Kasus

## A Studi Kasus 1: Signature vs. Heuristik

Jawaban Pengajar

### PEDOMAN PENILAIAN

**Jawaban siswa harus mencakup poin-poin berikut:**

- Analisis Skenario: Karyawan mengunduh alat buatan internal dari tim lain. Pemindai signature meloloskannya, tetapi pemindai heuristik menandainya mencurigakan.
- Strategi & Solusi yang Disarankan: Penyebab: Pemindaian signature memeriksa hash file, dan alat buatan sendiri tidak ada di basis data ancaman. Heuristik menganalisis struktur dan menandai tindakan mencurigakan (misalnya menulis ke registry). Verifikasi: Jalankan file di sandbox, periksa tanda tangan digital, dan kirim hash-nya ke portal intelijen ancaman.

## B Studi Kasus 2: Menangani Positif Palsu

Jawaban Pengajar

### PEDOMAN PENILAIAN

**Jawaban siswa harus mencakup poin-poin berikut:**

- Analisis Skenario: Pengembang mengompilasi aplikasinya, lalu antivirus menandai file baru itu sebagai malware dan mengarantinanya.
- Strategi & Solusi yang Disarankan: Risiko whitelisting: Melewati pemindai dapat membuat kode yang benar-benar terinfeksi berjalan. Penyelesaian: Kirim file ke vendor antivirus untuk dianalisis, tandatangani kode secara digital melalui otoritas sertifikat, dan buat pengecualian sementara untuk folder tertentu alih-alih mematikan antivirus.