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

Software antivirus e protezione degli endpoint
Guida alla protezione

Rilevamento basato su firme, euristica, monitoraggio del comportamento, sandboxing, aggiornamenti

PANORAMICA DI APPRENDIMENTO SUL SOFTWARE ANTIVIRUS

PROTETTO
CRITTOGRAFIA DEI DATI
Standard AES a 256 bit

CONFORME
STANDARD GLOBALI
Framework GDPR e CCPA

ZERO-TRUST
POLITICA DI ACCESSO
Autenticazione a più fattori

Benvenuto! Questo pacchetto di attività ti guida attraverso il software antivirus e la protezione degli endpoint. Esplorerai i database delle firme, gli scanner euristici, il monitoraggio comportamentale, i file virtuali in sandbox e la riduzione dei falsi positivi.

PUNTI DI CONTROLLO DELLA SCHEDA DI LAVORO

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

Apri la guida alla sicurezza informatica di VPN.com

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

Il tuo percorso di apprendimento sulla strategia antivirus

- Distingui tra rilevamento del malware basato su firme e basato su euristiche.
- Comprendi il monitoraggio del comportamento e i protocolli di isolamento in sandbox.
- Valuta l'impatto delle scansioni in tempo reale sulle prestazioni del sistema e degli endpoint.
- Mitigare le classificazioni di falsi positivi usando la verifica dei certificati digitali.
- Gestire la distribuzione quotidiana degli aggiornamenti delle definizioni sugli endpoint aziendali.

ISTRUZIONI DELLA GUIDA ANTIVIRUS

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

PROTEZIONE ANTIVIRUS E SCANSIONE BASATA SU FIRME (INTRODUZIONE)

Il software antivirus protegge gli endpoint identificando, mettendo in quarantena e rimuovendo il malware. I sistemi moderni combinano database di firme (che confrontano gli hash delle minacce note) con l'euristica (che analizza la struttura dei file) e il monitoraggio del comportamento per rilevare gli exploit zero-day.

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

Punto di controllo 1: Sfida a scelta multipla

1. Qual è un limite del rilevamento basato sulle firme?

- A. Non riesce a identificare malware sconosciuto o modificato
- B. Genera un alto tasso di falsi positivi
- C. Richiede un'elevata potenza di elaborazione della CPU
- D. Funziona solo quando è connesso a internet

2. Come rilevano gli scanner euristici le nuove varianti di malware?

- A. Individuando schemi sospetti e strutture di codice
- B. Confrontando gli hash dei file con un database di minacce
- C. Eliminando automaticamente tutti gli eseguibili non firmati
- D. Caricando ogni file in una cartella cloud pubblica

3. Qual è lo scopo dell'esecuzione in sandbox dell'antivirus?

- A. Isolare e analizzare i file in una cassaforte virtuale sicura
- B. Accelerare il trasferimento del backup del file system locale
- C. Aggiornare le patch di sicurezza del sistema operativo locale
- D. Comprimere file di documenti di grandi dimensioni per risparmiare spazio

4. Quale metodo di rilevamento segnala in tempo reale i comportamenti delle minacce?

- A. Analisi comportamentale che monitora le azioni del software
- B. Ispezione dei log storici eseguita durante la notte
- C. Intervento manuale dell'utente per segnalare le app lente
- D. Revisioni manuali settimanali dei programmi installati

5. Perché gli aggiornamenti regolari delle definizioni sono fondamentali per gli scanner?

- A. Alimentare i database degli identificatori di minacce dei motori basati su firme
- B. Aumentare le frequenze di clock della CPU durante le operazioni
- C. Per modificare i tempi di cache dei nameserver DNS globali
- D. Per autorizzare le impostazioni dei cookie del browser web

Punto di controllo 2: Sfida Vero o Falso

6 Domanda V/F 6

6. Il rilevamento basato su firme confronta gli hash crittografici dei file con elenchi presenti in un database.

- ◯ Vero
- ◯ Falso

7 Domanda V/F 7

7. Gli scanner euristici possono generare falsi positivi su file sicuri.

- ◯ Vero
- ◯ Falso

8 Domanda V/F 8

8. Una sandbox consente al malware di accedere ai file di rete senza limiti.

- ◯ Vero
- ◯ Falso

9 Domanda V/F 9

9. La scansione comportamentale blocca i file quando mostrano azioni dannose.

- ◯ Vero
- ◯ Falso

10 Domanda V/F 10

10. Il normale software antivirus blocca completamente tutti gli attacchi zero-day.

- ◯ Vero
- ◯ Falso

Punto di controllo 3: Inserimento dei termini chiave

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

1. Uno scanner tradizionale si basa sul confronto delle _____ per identificare il malware noto.

2. L'analisi dei modelli di codice dei file si chiama scansione _____ .

3. Gli antivirus isolano i file sospetti in un ambiente _____ .

4. Il monitoraggio in tempo reale controlla il _____ dei programmi per individuare attività sospette.

5. Ogni giorno gli scanner scaricano gli _____ del database per riconoscere le nuove minacce.

6. I programmi sicuri segnalati come malware generano avvisi di _____ positivo.

BANCA DELLE PAROLE DEL VOCABOLARIO

AGGIORNAMENTI COMPORTAMENTO EURISTICA FALSO FIREWALL FIRME RANSOMWARE SANDBOX

Scrivi qui le tue risposte:

1. **2.**

3. **4.**

5. **6.**

Punto di controllo 4: Abbinamento di concetti sulla sicurezza

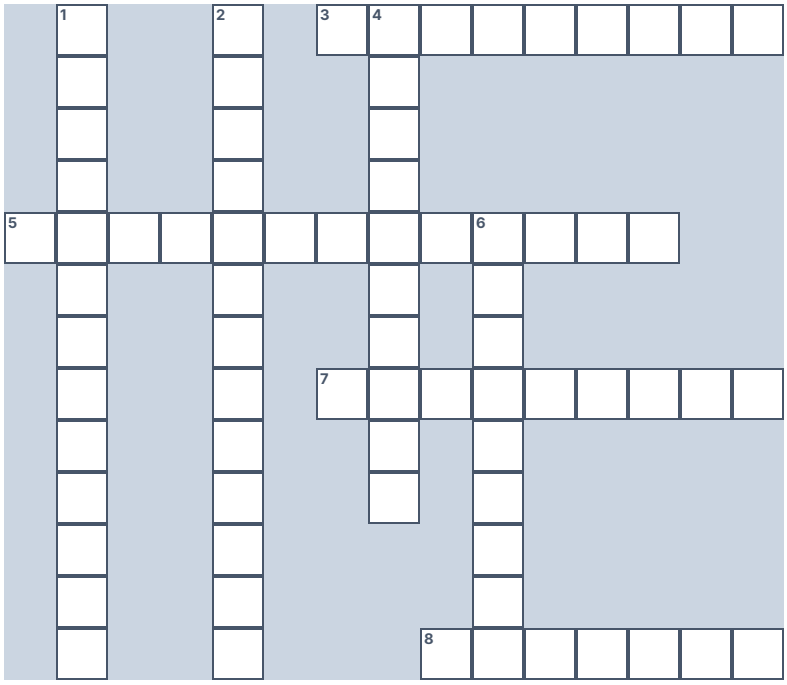
ABBINAMENTO DELLE DEFINIZIONI

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

☐	1. Firma hash	A	Isolare i file sospetti per evitare l'esposizione del sistema locale.
☐	2. Euristica del codice	B	Suite software che analizza e protegge gli endpoint dagli exploit.
☐	3. Sandbox dei file	C	Monitoraggio delle azioni del software in esecuzione per individuare schemi di comportamento dannosi.
☐	4. Scansione comportamentale	D	Impronta crittografica univoca del database usata per identificare le minacce note.
☐	5. Aggiornamenti giornalieri	E	Ambiente di test virtuale sicuro che esegue codice non attendibile in modo protetto.
☐	6. Falso positivo	F	Download regolari delle definizioni che alimentano il database delle minacce.
☐	7. Isolamento delle minacce	G	Analisi basata su regole che segnala i file con strutture di codice sospette.
☐	8. Strumento antivirus	H	Avviso di sicurezza che classifica erroneamente un software sicuro come malware.

Punto di controllo 5: Cruciverba

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



ORIZZONTALI

3. Impronta crittografica univoca nel database usata per identificare minacce note (9)

5. Monitoraggio delle azioni del software in esecuzione per individuare schemi di funzionamento dannosi (13)

7. Suite software che esegue la scansione e protegge i dispositivi dagli exploit (9)

8. Ambiente di prova virtuale sicuro in cui il codice non attendibile viene eseguito senza rischi (7)

VERTICALI

1. Avviso di sicurezza che classifica per errore un software sicuro come malware (13)

2. Download periodici delle definizioni che alimentano il database delle minacce (13)

4. Confinamento dei file sospetti per evitare l'esposizione del sistema locale (10)

6. Analisi basata su regole che segnala file con strutture di codice sospette (9)

Punto di controllo 5, alternativa: Indizi accessibili del cruciverba

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

ORIZZONTALI

3 orizzontale: Impronta crittografica univoca nel database usata per identificare minacce note (9 lettere):

5 orizzontale: Monitoraggio delle azioni del software in esecuzione per individuare schemi di funzionamento dannosi (13 lettere):

7 orizzontale: Suite software che esegue la scansione e protegge i dispositivi dagli exploit (9 lettere):

8 orizzontale: Ambiente di prova virtuale sicuro in cui il codice non attendibile viene eseguito senza rischi (7 lettere):

VERTICALI

1 verticale: Avviso di sicurezza che classifica per errore un software sicuro come malware (13 lettere):

2 verticale: Download periodici delle definizioni che alimentano il database delle minacce (13 lettere):

4 verticale: Confinamento dei file sospetti per evitare l'esposizione del sistema locale (10 lettere):

6 verticale: Analisi basata su regole che segnala file con strutture di codice sospette (9 lettere):

Punto di controllo 6: Cerca la parola nascosta

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

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

ELENCO DELLE PAROLE DEL VOCABOLARIO

FIRMAHASH EURISTICA SANDBOX COMPORTAMENTO AGGIORNAMENTI
FALSOPOSITIVO ISOLAMENTO ANTIVIRUS

Punto di controllo 6, alternativa: Abbinamento accessibile del vocabolario

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

TERMINI DEL VOCABOLARIO
A. FIRMAHASH
B. EURISTICA
C. SANDBOX
D. COMPORTAMENTO
E. AGGIORNAMENTI
F. FALSOPOSITIVO
G. ISOLAMENTO
H. ANTIVIRUS

DEFINIZIONI E CAMPI DI ABBINAMENTO
_____ 1. Monitoraggio delle azioni del software in esecuzione per individuare schemi di funzionamento dannosi.
_____ 2. Suite software che esegue la scansione e protegge i dispositivi dagli exploit.
_____ 3. Download periodici delle definizioni che alimentano il database delle minacce.
_____ 4. Analisi basata su regole che segnala file con strutture di codice sospette.
_____ 5. Confinamento dei file sospetti per evitare l'esposizione del sistema locale.
_____ 6. Impronta crittografica univoca nel database usata per identificare minacce note.
_____ 7. Ambiente di prova virtuale sicuro in cui il codice non attendibile viene eseguito senza rischi.
_____ 8. Avviso di sicurezza che classifica per errore un software sicuro come malware.

Punto di controllo 7: Sfida delle parole mescolate

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

1. HAMIFASHR
2. SNXOBDA
3. GAAEMTIGNORNI
4. MTAOLNEISO
5. ISUATIECR
6. OETRNMTMCOAOP
7. TISPFAIOOVLOS
8. SVUAINIRT

Attività bonus: Pensa veloce

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

1	Motivi per aggiornare il software			
2	Persone a cui puoi chiedere aiuto per l'IT			
3	Cose da fare quando l'antivirus trova qualcosa			
4	Segnali di un virus informatico			
5	Cose che vengono messe in quarantena			
6	Luoghi in cui si nascondono i virus			
7	Informazioni che non dovresti mai condividere			
8	Tipi di software dannoso			
9	Strumenti di sicurezza che conosci			
10	Cose che un antivirus analizza			
11	Cose di cui fai il backup			
12	Dispositivi che possono essere hackerati			
13	Programmi antivirus che conosci			
14	Motivi dei falsi allarmi			
15	Buone abitudini sicure che puoi iniziare oggi			

Punto di controllo 8: Casi di studio sulla sicurezza informatica

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

CASO DI STUDIO 1: SCANSIONE BASATA SU FIRME E SCANSIONE EURISTICA A CONFRONTO



Scenario: Un dipendente scarica un'utilità personalizzata creata internamente da un altro team. Lo scanner basato sulle firme la approva, ma lo scanner euristico la segnala come sospetta.

Domanda di discussione: Spiega perché è successo e come verificare se il file è sicuro.

CASO DI STUDIO 2: GESTIRE I FALSI POSITIVI



Scenario: Uno sviluppatore software compila la propria applicazione. L'antivirus del sistema segnala il nuovo eseguibile come malware e lo mette in quarantena.

Domanda di discussione: Descrivi i rischi della whitelist e illustra il corretto percorso di risoluzione.

Punto di controllo 9: Decifrare il codice

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

CHIAVE DI CIFRATURA LETTERA-NUMERO

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

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

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

18	9	12	5	22	1		13	1	12	23	1	18	5		14	21	15	22	9
3	15	14		5	21	18	9	19	20	9	3	1		4	5	12			
						3	15	4	9	3	5								

Messaggio decifrato:

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

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

Rivedi domande e risposte comuni sulla mitigazione delle minacce online.

Q1: Come identifica il malware un software antivirus?

Identifica il malware usando la corrispondenza delle firme in un database, l'analisi euristica della struttura del codice e il monitoraggio comportamentale in tempo reale.

Q2: Che cos'è il rilevamento basato su firme?

È un metodo di scansione che confronta gli hash crittografici dei file con gli elenchi di minacce malware note presenti in un database.

Q3: Cos'è uno scanner euristico?

L'analisi euristica esamina la struttura di un file e le sue istruzioni di codice, segnalando schemi sospetti comuni alle varianti di malware.

Q4: Cosa significa che un file è in quarantena?

L'antivirus sposta il file in una cartella sicura e isolata, bloccandone l'esecuzione per proteggere il sistema operativo.

Q5: Cos'è un falso positivo dell'antivirus?

È un errore in cui software legittimo e sicuro viene segnalato erroneamente come malware dagli algoritmi di scansione.

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

Rivedi domande e risposte comuni sulla mitigazione delle minacce online.

Q6: Come protegge i sistemi il monitoraggio del comportamento?

Monitora in tempo reale il software in esecuzione, bloccando i processi che tentano modifiche sospette come l'iniezione di codice.

Q7: Perché il test in sandbox è importante?

Il sandboxing esegue file non attendibili in una macchina virtuale isolata, osservandone le azioni in sicurezza senza esporre il sistema.

Q8: Ogni quanto devono aggiornarsi le definizioni dell'antivirus?

Gli scanner dovrebbero aggiornare le definizioni ogni giorno o ogni ora per riconoscere i ceppi di malware scoperti di recente.

Q9: Qual è la differenza tra antivirus ed EDR?

L'antivirus si concentra sulla scansione dei file, mentre l'Endpoint Detection and Response (EDR) offre il tracciamento e il contenimento delle minacce su tutta la rete.

Q10: Posso eseguire due programmi antivirus insieme?

No. Eseguire due scanner attivi causa conflitti di sistema, rallenta le prestazioni e può bloccare le operazioni dell'uno e dell'altro.

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

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

Q1: Come riducono le regole euristiche l'elusione delle minacce?

L'analisi euristica esamina schemi generali di minaccia anziché firme specifiche, individuando varianti modificate di famiglie di malware note.

Q2: Che cos'è un virus polimorfico?

È un malware che cambia la struttura del proprio file e la routine di decifratura a ogni esecuzione, rendendo inefficaci le scansioni basate sulle firme.

Q3: Come rilevano le sandbox l'elusione delle macchine virtuali?

Le sandbox moderne simulano i clic del mouse e il tempo di attività del sistema, ingannando i malware progettati per nascondersi quando vengono eseguiti nelle macchine virtuali.

Q4: Quali sono i formati di download degli aggiornamenti delle firme?

Gli aggiornamenti sono di solito file binari differenziali incrementali leggeri, che riducono al minimo il consumo di banda di rete del client.

Q5: Come gestiscono le scansioni locali gli agenti endpoint?

Gli agenti eseguono controlli leggeri in background, delegando le ricerche approfondite di hash crittografici ai database di minacce nel cloud.

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

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

Q6: Cos'è la scansione di rilevamento dei rootkit?

Analizza le tabelle di memoria a livello di kernel, aggirando le API del sistema operativo che i rootkit agganciano per nascondere i propri thread attivi.

Q7: Come blocca il ransomware la scansione del comportamento?

Rileva i cicli di cifratura di massa automatizzata dei file, terminando il processo dell'host prima che i database di sistema vengano bloccati.

Q8: Cos'è la verifica del certificato di firma del codice?

Gli scanner controllano le firme digitali del codice rispetto alle autorità di certificazione radice attendibili, convalidando l'identità dello sviluppatore del software.

Q9: Come influiscono i packer sui motori di scansione?

I packer comprimono o cifrano i payload dei malware. Gli scanner devono decomprimere il file in memoria prima che vengano eseguiti i confronti con le firme.

Q10: Come fanno gli strumenti EDR ad automatizzare l'isolamento?

Gli agent EDR mettono in quarantena gli endpoint compromessi a livello di rete, bloccando il movimento laterale e consentendo comunque l'accesso agli analisti.

Parte 11: 10 fatti e spunti reali sulla sicurezza informatica

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

1. APPROFONDIMENTO SULLA SICUREZZA

I database di firme archiviano gli hash del malware noto, quindi i file nuovi o alterati sfuggono finché le definizioni non vengono aggiornate.

2. APPROFONDIMENTO SULLA SICUREZZA

I motori euristici possono segnalare alcune nuove varianti di malware prima che esistano le firme, al prezzo di più falsi positivi.

3. APPROFONDIMENTO SULLA SICUREZZA

Gli avvisi di falsi positivi fanno perdere ai team IT tempo speso a verificare e ripristinare file messi in quarantena per errore.

4. APPROFONDIMENTO SULLA SICUREZZA

Il malware polimorfico cambia il proprio codice a ogni copia, quindi i difensori abbinano le firme a controlli euristici e comportamentali.

6. APPROFONDIMENTO SULLA SICUREZZA

Gli autori di malware scrivono codice personalizzato progettato per controllare gli ambienti sandbox, ritardando l'esecuzione per aggirare i timer.

5. APPROFONDIMENTO SULLA SICUREZZA

I motori antivirus basati su cloud confrontano in tempo quasi reale gli hash dei file sospetti con grandi database online di minacce.

7. APPROFONDIMENTO SULLA SICUREZZA

I fornitori inviano regolarmente agli endpoint aggiornamenti delle definizioni, così gli scanner possono riconoscere le minacce appena confermate.

8. APPROFONDIMENTO SULLA SICUREZZA

I monitor comportamentali per il ransomware prendono di mira specifiche chiamate API Win32 associate alla cifratura dei file e alla cancellazione delle copie shadow.

9. APPROFONDIMENTO SULLA SICUREZZA

Firme di codice valide possono ridurre il rischio di falsi positivi, ma i file firmati vengono comunque analizzati, perché anche il malware può essere firmato.

10. APPROFONDIMENTO SULLA SICUREZZA

I rootkit modificano le strutture del kernel di sistema, richiedendo scanner specializzati all'avvio per rilevarli e rimuoverli.

Riferimenti tecnici e fonti

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

RIFERIMENTI ACCADEMICI E DI SETTORE

[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

Soluzioni: Punto di controllo 1 – Scelta multipla

1 **Domanda 1** FIRME **Risposta corretta: A**

NOTA DIDATTICA

La scansione basata su firme si affida agli hash noti di un database, e non riesce a rilevare malware sconosciuto o modificato. Citazione: OWASP Secure Configuration.

2 **Domanda 2** EURISTICHE **Risposta corretta: A**

NOTA DIDATTICA

L'euristica analizza la struttura del codice e i comandi per individuare le caratteristiche sospette delle nuove varianti di minacce. Citazione: Center for Internet Security (CIS).

3 **Domanda 3** SANDBOXING **Risposta corretta: A**

NOTA DIDATTICA

Una sandbox esegue i file sospetti in una macchina virtuale isolata per osservare in sicurezza il comportamento di esecuzione. Citazione: NIST Digital Identity.

4 **Domanda 4** COMPORTAMENTALE **Risposta corretta: A**

NOTA DIDATTICA

L'analisi del comportamento monitora in tempo reale i programmi in esecuzione per bloccare le modifiche non autorizzate al sistema. Citazione: Center for Internet Security (CIS).

5 **Domanda 5** AGGIORNAMENTI **Risposta corretta: A**

NOTA DIDATTICA

Gli scanner scaricano aggiornamenti incrementali giornalieri delle definizioni per restare sincronizzati con il panorama delle minacce. Citazione: OWASP Secure Configuration.

Soluzioni: Punto di controllo 2 – Vero o falso

6 **Domanda 6** FIRME **Risposta corretta: Vero**

NOTA DIDATTICA

Gli strumenti basati su firme calcolano hash crittografici e li confrontano con un database di hash di minacce note. Citazione: OWASP Secure Configuration.

7 **Domanda 7** EURISTICHE **Risposta corretta: Vero**

NOTA DIDATTICA

I motori euristici eseguono schemi basati su regole che possono segnalare come sospetti file legittimi e sicuri. Citazione: Center for Internet Security (CIS).

8 **Domanda 8** SANDBOXING **Risposta corretta: Falso**

NOTA DIDATTICA

Una sandbox esegue il codice in un container virtuale, bloccando rigorosamente l'accesso alle condivisioni di rete. Citazione: NIST Digital Identity.

9 **Domanda 9** COMPORTAMENTALE **Risposta corretta: Vero**

NOTA DIDATTICA

Il monitoraggio in tempo reale segnala i processi in esecuzione che tentano scritture illecite o blocchi dei file. Citazione: Center for Internet Security (CIS).

10 **Domanda 10** **Risposta corretta: Falso**

NOTA DIDATTICA

Nessun antivirus ferma ogni attacco zero-day; le minacce sconosciute possono eludere le firme e le euristiche.

Chiavi del vocabolario e griglia di valutazione

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

PUNTO DI CONTROLLO 4: SOLUZIONI ABBINAMENTO DI CONCETTI

D 1. Firma hash	G 2. Euristica del codice	E 3. Sandbox dei file	C 4. Scansione comportamentale
F 5. Aggiornamenti giornalieri	H 6. Falso positivo	A 7. Isolamento delle minacce	B 8. Strumento antivirus

PUNTO DI CONTROLLO 3: SOLUZIONI TERMINI CHIAVE

1 FIRME	2 EURISTICA	3 SANDBOX	4 COMPORTAMENTO
5 AGGIORNAMENTI	6 FALSO		

PUNTO DI CONTROLLO 6, ALTERNATIVA: SOLUZIONI ABBINAMENTO DI PAROLE

1 D – COMPORTAMENTO	2 H – ANTIVIRUS	3 E – AGGIORNAMENTI	4 B – EURISTICA
5 G – ISOLAMENTO	6 A – FIRMAHASH	7 C – SANDBOX	8 F – FALSOPOSITIVO

NOTE DI DISCUSSIONE PER GLI INSEGNANTI

Termini chiave:
Verifica che gli studenti sappiano spiegare Firma hash, Euristica del codice e Sandbox dei file con parole proprie e fare un esempio per ciascuno.

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

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

Soluzioni dei rompicapi e note per l'insegnante

SOLUZIONE DELLA RICERCA DELLE PAROLE

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

SOLUZIONE DEL CRUCIVERBA

	F		A		F	I	R	M	A	H	A	S	H
	A		G			S							
	L		G			O							
	S		I			L							
C	O	M	P	O	R	T	A	M	E	N	T	O	
	P		R			M		U					
	O		N			E		R					
	S		A		A	N	T	I	V	I	R	U	S
	I		M			T		S					
	T		E			O		T					
	I		N					I					
	V		T					C					
	O		I				S	A	N	D	B	O	X

ORIZZONTALI

3 orizzontale: FIRMAHASH Impronta crittografica univoca nel database usata per identificare minacce note (9 lettere)

5 orizzontale: COMPORTAMENTO Monitoraggio delle azioni del software in esecuzione per individuare schemi di funzionamento dannosi (13 lettere)

7 orizzontale: ANTIVIRUS Suite software che esegue la scansione e protegge i dispositivi dagli exploit (9 lettere)

8 orizzontale: SANDBOX Ambiente di prova virtuale sicuro in cui il codice non attendibile viene eseguito senza rischi (7 lettere)

VERTICALI

1 verticale: FALSOPOSITIVO Avviso di sicurezza che classifica per errore un software sicuro come malware (13 lettere)

2 verticale: AGGIORNAMENTI Download periodici delle definizioni che alimentano il database delle minacce (13 lettere)

4 verticale: ISOLAMENTO Confinamento dei file sospetti per evitare l'esposizione del sistema locale (10 lettere)

6 verticale: EURISTICA Analisi basata su regole che segnala file con strutture di codice sospette (9 lettere)

Soluzioni delle parole mescolate e del codice cifrato

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

CHIAVE DELLE PAROLE DA RIORDINARE

1. HAMIFASHR — **FIRMAHASH**
2. SNXOBDA — **SANDBOX**
3. GAAEMTIGNORNI — **AGGIORNAMENTI**
4. MTAOLNEISO — **ISOLAMENTO**
5. ISUATIECR — **EURISTICA**
6. OETRNMTMCOAOP — **COMPORTAMENTO**
7. TISPFAIOOVLOS — **FALSOPOSITIVO**
8. SVUAINIRT — **ANTIVIRUS**

CHIAVE DELLA SFIDA DEL CODICE SEGRETO

"RILEVA MALWARE NUOVI CON EURISTICA DEL CODICE"

Soluzioni dei casi di studio

A Caso di studio 1: scansione basata su firme e scansione euristica a confronto

Soluzione per l'insegnante

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Analisi dello scenario: un dipendente scarica un'utilità personalizzata creata internamente da un altro team. Lo scanner delle firme la approva, ma lo scanner euristico la segnala come sospetta.
- Strategia e soluzione consigliate: Perché è successo: la scansione basata sulle firme controlla gli hash dei file; poiché è personalizzato, non è nel database delle minacce. L'euristica analizza la struttura e ha segnalato azioni sospette (ad es. scritture nel registro di sistema). Verifica: esegui il file in una sandbox per osservarne le azioni, controlla le firme digitali e invia l'hash ai portali di threat intelligence.

B Caso di studio 2: Gestire i falsi positivi

Soluzione per l'insegnante

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Analisi dello scenario: uno sviluppatore software compila la propria applicazione. L'antivirus di sistema segnala il nuovo eseguibile come malware e lo mette in quarantena.
- Strategia e soluzione consigliate: Rischi della whitelist: aggirare gli scanner può consentire l'esecuzione di codice realmente infetto. Percorso di risoluzione: invia il file al fornitore dell'antivirus per l'analisi, firma digitalmente il codice tramite le autorità di certificazione e configura temporaneamente eccezioni per cartelle specifiche anziché disattivare l'antivirus.