नाम: _____ दिनांक: _____ अंक: _____

एंटीवायरस सॉफ़्टवेयर और एंडपॉइंट सुरक्षा गाइड

सिग्नेचर डिटेक्शन, ह्यूरिस्टिक्स, व्यवहार निगरानी, सैंडबॉक्सिंग, अपडेट

एंटीवायरस सॉफ़्टवेयर सीखने का अवलोकन

सुरक्षित किया गया
डेटा एन्क्रिप्शन
256-बिट AES मानक

अनुपालक
वैश्विक मानक
GDPR और CCPA फ़्रेमवर्क

ज़ीरो-ट्रस्ट
एक्सेस नीति
मल्टी-फ़ैक्टर ऑथेंटिकेशन

स्वागत है! यह गतिविधि पैकेट आपको एंटीवायरस सॉफ़्टवेयर और एंडपॉइंट सुरक्षा से परिचित कराता है। आप सिग्नेचर डेटाबेस, ह्यूरिस्टिक स्कैनर, व्यवहार निगरानी, सैंडबॉक्स वर्चुअल फ़ाइलें और फ़ॉल्स पॉज़िटिव शमन का अध्ययन करेंगे।

वर्कशीट चेकपॉइंट

- [ ] **भाग 1-4: साइबर सुरक्षा और खतरों की रोकथाम में महारत हासिल करें।**
- [ ] **भाग 5-7: क्रॉसवर्ड और वर्ड सर्च पहेलियाँ हल करें।**
- [ ] **भाग 8-9: केस स्टडी और कूट संदेश की चुनौती हल करें।**
- [ ] **भाग 10: बुनियादी और उन्नत FAQ पेज देखें।**
- [ ] **भाग 11: 10 रोचक वास्तविक तथ्यों को जानें।**
- [ ] **अतिरिक्त: झटपट सोचें चुनौती।**

VPN.com साइबर सुरक्षा गाइड खोलें

URL: https://www.vpn.com/hi/saibhar-suraksha/antivirus/

आपका एंटीवायरस रणनीति लर्निंग रोडमैप

- सिग्नेचर-आधारित और ह्यूरिस्टिक-आधारित मैलवेयर पहचान में अंतर करें।
- व्यवहार निगरानी और सैंडबॉक्स आइसोलेशन प्रोटोकॉल को समझें।
- सिस्टम प्रदर्शन और एंडपॉइंट पर रियल-टाइम स्कैन के प्रभावों का मूल्यांकन करें।
- डिजिटल प्रमाणपत्र सत्यापन से गलत-पॉज़िटिव वर्गीकरण कम करें।
- कॉर्पोरेट एंडपॉइंट पर दैनिक डेफ़िनिशन अपडेट का वितरण प्रबंधित करें।

एंटीवायरस गाइड के निर्देश

बहुविकल्पीय और सही/गलत प्रश्नों के उत्तर दें, शब्द बैंक की मदद से रिक्त स्थान भरें, परिभाषाओं का मिलान करें, और क्रॉसवर्ड तथा वर्ड सर्च पहेलियाँ हल करें। अपने ज्ञान को एंडपॉइंट एंटीवायरस सुरक्षा पर लागू करें। अंत में अतिरिक्त गतिविधि झटपट सोचें पूरी करें।

एंटीवायरस सुरक्षा और सिग्नेचर स्कैनिंग (परिचय)

एंटीवायरस सॉफ़्टवेयर मैलवेयर की पहचान, क्वारंटीन और सफ़ाई करके एंडपॉइंट की रक्षा करता है। आधुनिक सिस्टम ज़ीरो-डे एक्सप्लॉइट पकड़ने के लिए सिग्नेचर डेटाबेस (ज्ञात खतरों के हैश का मिलान), ह्यूरिस्टिक्स (फ़ाइल संरचना का विश्लेषण) और व्यवहार निगरानी को मिलाते हैं।

प्रत्येक चेकपॉइंट को ध्यान से पढ़ें और सही

चेकपॉइंट 1: बहुविकल्पीय चुनौती

1 1. सिग्नेचर-आधारित पहचान की एक सीमा क्या है?

- A. यह अज्ञात या बदले हुए मैलवेयर की पहचान नहीं कर सकता
- B. यह बड़ी संख्या में फ़ॉल्स पॉज़िटिव पैदा करता है
- C. इसके लिए उच्च CPU प्रोसेसिंग क्षमता चाहिए
- D. यह केवल इंटरनेट से जुड़े होने पर ही काम करता है

2 2. ह्यूरिस्टिक स्कैनर नए मैलवेयर वेरिएंट का पता कैसे लगाते हैं?

- A. संदिग्ध पैटर्न और कोड संरचनाओं की पहचान करके
- B. फ़ाइल हैश को खतरों के डेटाबेस से मिलाकर
- C. सभी अहस्ताक्षरित एक्ज़ीक्यूटेबल अपने आप मिटाकर
- D. हर फ़ाइल को सार्वजनिक क्लाउड फ़ोल्डर में अपलोड करके

3 3. एंटीवायरस सैंडबॉक्स निष्पादन का उद्देश्य क्या है?

- A. फ़ाइलों को सुरक्षित वर्चुअल वॉल्ट में अलग करना और उनका विश्लेषण करना
- B. स्थानीय फ़ाइल सिस्टम बैकअप ट्रांसफ़र को तेज़ करना
- C. लोकल ऑपरेटिंग सिस्टम के सुरक्षा पैच अपडेट करना
- D. स्टोरेज बचाने के लिए बड़ी दस्तावेज़ फ़ाइलों को संपीड़ित करना

4 4. कौन-सी पहचान विधि खतरनाक व्यवहार को रियल टाइम में चिह्नित करती है?

- A. सॉफ़्टवेयर की क्रियाओं की निगरानी करने वाला व्यवहार विश्लेषण
- B. रात भर किया जाने वाला ऐतिहासिक लॉग निरीक्षण
- C. धीमे ऐप की रिपोर्ट करने वाला मैन्युअल उपयोगकर्ता हस्तक्षेप
- D. इंस्टॉल किए गए प्रोग्रामों की साप्ताहिक मैन्युअल समीक्षा

5 5. स्कैनर के लिए नियमित डेफ़िनिशन अपडेट क्यों महत्वपूर्ण हैं?

- A. सिग्नेचर इंजनों को डेटाबेस के ख़तरा पहचानकर्ता देना
- B. संचालन के दौरान CPU क्लॉक गति बढ़ाना
- C. वैश्विक DNS नेमसर्वर कैशिंग समय बदलने के लिए
- D. वेब ब्राउज़र की कुकी सेटिंग्स को अधिकृत करने के लिए

चेकपॉइंट 2: सही या गलत चुनौती

6 प्रश्न tf 6

6. सिग्नेचर डिटेक्शन क्रिप्टोग्राफ़िक फ़ाइल हैश को डेटाबेस सूचियों से मिलाता है।

सही गलत

7 प्रश्न tf 7

7. ह्यूरिस्टिक स्कैनर सुरक्षित फ़ाइलों पर फ़ॉल्स पॉज़िटिव अलर्ट दे सकते हैं।

सही गलत

8 प्रश्न tf 8

8. सैंडबॉक्स मैलवेयर को बिना सीमा के नेटवर्क फ़ाइलों तक पहुँचने देता है।

सही गलत

9 प्रश्न tf 9

9. व्यवहार स्कैनिंग उन फ़ाइलों को ब्लॉक करती है जो दुर्भावनापूर्ण क्रियाएँ दिखाती हैं।

सही गलत

10 प्रश्न tf 10

10. मानक एंटीवायरस सॉफ़्टवेयर सभी ज़ीरो-डे हमलों को पूरी तरह रोक देता है।

सही गलत

चेकपॉइंट 3: मुख्य शब्द भरें

नीचे दिए गए प्रत्येक वाक्य को पढ़ें और रिक्त स्थान को वर्ड बैंक के सही शब्द से भरें।

1. एक पारंपरिक स्कैनर ज्ञात मैलवेयर पहचानने के लिए _____ मिलान पर निर्भर करता है।
2. फ़ाइलों के कोड पैटर्न का विश्लेषण _____ स्कैनिंग कहलाता है।
3. एंटीवायरस टूल खतरे पहचानने के लिए संग्रहित _____ से फ़ाइलों का मिलान करते हैं।
4. रीयल-टाइम निगरानी संदिग्ध गतिविधियों के लिए प्रोग्राम के _____ पर नज़र रखती है।
5. स्कैनर नए खतरों को पहचानने के लिए हर दिन डेटाबेस _____ डाउनलोड करते हैं।
6. फ़ाइलें लॉक करके फिरौती मांगने वाला दुर्भावनापूर्ण प्रोग्राम _____ कहलाता है।

शब्दावली शब्द-बैंक

अपडेट | फ़ायरवॉल | फ़ॉल्स पॉज़िटिव | रैनसमवेयर | वायरस डेटाबेस | व्यवहार | सिग्नेचर | हयूरिस्टिक

अपने उत्तर यहाँ लिखें:

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

चेकपॉइंट 4: सुरक्षा अवधारणा मिलान

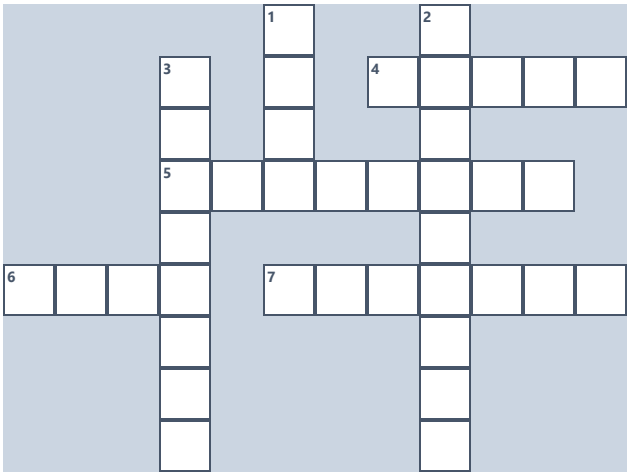
परिभाषा मिलान

बाईं ओर के प्रत्येक शब्दावली पद को दाईं ओर की सही परिभाषा से मिलाएँ; भरने योग्य इनपुट बॉक्स में संबंधित अक्षर (A-H) लिखें।

☐	**1. हैश हस्ताक्षर**	**A**	स्थानीय सिस्टम को खतरे से बचाने के लिए संदिग्ध फ़ाइलों को सीमित दायरे में रखना।
☐	**2. कोड ह्यूरिस्टिक्स**	**B**	सॉफ़्टवेयर सुइट, जो एंडपॉइंट को एक्सप्लॉइट से स्कैन और सुरक्षित करता है।
☐	**3. फ़ाइल सैंडबॉक्स**	**C**	चल रहे सॉफ़्टवेयर के कार्यों में दुर्भावनापूर्ण संचालन पैटर्न की निगरानी करना।
☐	**4. व्यवहार स्कैन**	**D**	ज्ञात खतरों की पहचान के लिए इस्तेमाल होने वाला अद्वितीय क्रिप्टोग्राफ़िक डेटाबेस फ़ुटप्रिंट।
☐	**5. दैनिक अपडेट**	**E**	सुरक्षित वर्चुअल टेस्ट वातावरण, जो अविश्वसनीय कोड को सुरक्षित ढंग से चलाता है।
☐	**6. फ़ॉल्स पॉज़िटिव**	**F**	थ्रेट डेटाबेस को अपडेट करने वाले नियमित डेफ़िनिशन डाउनलोड।
☐	**7. ख़तरा अलगाव**	**G**	संदिग्ध कोड संरचना वाली फ़ाइलों को फ़्लैग करने वाला नियम-आधारित विश्लेषण।
☐	**8. एंटीवायरस टूल**	**H**	सुरक्षा चेतावनी, जो सुरक्षित सॉफ़्टवेयर को गलती से मैलवेयर के रूप में वर्गीकृत कर देती है।

चेकपॉइंट 5: क्रॉसवर्ड पहेली

सक्रिय सफ़ेद खानों में अक्षर टाइप करके क्रॉसवर्ड पहेली हल करें। संख्याएँ नीचे दिए गए संकेतों से मेल खाती हैं।



बाएँ से दाएँ

4. नियमों के आधार पर नेटवर्क ट्रैफ़िक को रोकने या अनुमति देने वाली सुरक्षा दीवार (5)

5. ज्ञात खतरों की पहचान-सूचियों का संग्रह, जिससे फ़ाइलों का मिलान किया जाता है (8)

6. ज्ञात मैलवेयर की पहचान के लिए इस्तेमाल होने वाला अनोखा डिजिटल पैटर्न या फ़िंगरप्रिंट (4)

7. दुर्भावनापूर्ण प्रोग्राम, जो फ़ाइलें लॉक करके उन्हें खोलने के बदले फिरौती मांगता है (7)

ऊपर से नीचे

1. किसी प्रोग्राम की गतिविधियों का तरीका, जिसकी निगरानी से दुर्भावनापूर्ण संचालन पकड़ा जाता है (4)

2. सक्रिय निगरानी, जो फ़ाइल खुलते ही उसमें मौजूद खतरे को तुरंत पकड़ लेती है (9)

3. सॉफ़्टवेयर सूट, जो एंडपॉइंट को एक्सप्लॉइट से स्कैन और सुरक्षित करता है (8)

चेकपॉइंट 5, वैकल्पिक: सुलभ क्रॉसवर्ड संकेत

स्क्रीन-रीडर और कीबोर्ड उपयोगकर्ता क्रॉसवर्ड के उत्तर सीधे नीचे दिए गए टेक्स्ट फ़ील्ड में टाइप कर सकते हैं। आड़े संकेत खड़े संकेत

बाएँ से दाएँ

4 बाएँ से दाएँ: नियमों के आधार पर नेटवर्क ट्रैफ़िक को रोकने या अनुमति देने वाली सुरक्षा दीवार (5 अक्षर):

5 बाएँ से दाएँ: ज्ञात खतरों की पहचान-सूचियों का संग्रह, जिससे फ़ाइलों का मिलान किया जाता है (8 अक्षर):

6 बाएँ से दाएँ: ज्ञात मैलवेयर की पहचान के लिए इस्तेमाल होने वाला अनोखा डिजिटल पैटर्न या फ़िंगरप्रिंट (4 अक्षर):

7 बाएँ से दाएँ: दुर्भावनापूर्ण प्रोग्राम, जो फ़ाइलें लॉक करके उन्हें खोलने के बदले फिरौती मांगता है (7 अक्षर):

ऊपर से नीचे

1 ऊपर से नीचे: किसी प्रोग्राम की गतिविधियों का तरीका, जिसकी निगरानी से दुर्भावनापूर्ण संचालन पकड़ा जाता है (4 अक्षर):

2 ऊपर से नीचे: सक्रिय निगरानी, जो फ़ाइल खुलते ही उसमें मौजूद खतरे को तुरंत पकड़ लेती है (9 अक्षर):

3 ऊपर से नीचे: सॉफ़्टवेयर सूट, जो एंडपॉइंट को एक्सप्लॉइट से स्कैन और सुरक्षित करता है (8 अक्षर):

चेकपॉइंट 6: छिपे शब्द खोजें

नीचे दी गई ग्रिड में छिपे 8 प्रमुख शब्दावली शब्द खोजें। शब्द क्षैतिज, ऊर्ध्वाधर या तिरछे हो सकते हैं।

जा	सा	वा	ड	रे	स	ख	फ़ा	नि	फ	ढ	मा	ना	का	रे
दे	सि	मी	क	पि	ता	ति	य	रै	ज	श	भ	ऊ	अ	ऊ
ए	रि	र	वि	श	य	वि	र	व	न	वा	पा	ल	च	से
कि	य	हा	घ	प	के	की	वॉ	व	सि	स	री	त	की	कि
स	सि	व	ना	ने	रि	पा	ल	ते	ण	सि	म	ए	ता	सा
बे	मी	व्य	न	नी	य	ऋ	एं	ले	घ	ति	ग्रे	वे	जि	ला
टा	ए	जी	ले	ड	ल	ल	द	टी	जे	घ	के	च	य	च
डे	से	दे	री	ए	टा	पी	उ	अ	वा	जे	मि	घ	र	र
स	व	आ	च	मी	इ	च	ट	थ	फ	य	ग	ना	सी	का
र	ज	फ	नी	जी	म	ता	ठ	से	लि	ट	र	आ	इ	से
य	रा	के	री	पा	सु	वा	सि	य	नि	पि	ने	स	ख	के
वा	वे	ऊ	ड	नी	र	दे	दि	भ	र	आ	नि	जे	टू	वे
वे	ष	ण	प	कि	क्षा	से	य	न	ह	ह	ते	रा	द	ल
सा	सी	थ	जे	इ	मे	ला	स्कै	ढ	पे	ऋ	वे	नी	वे	उ
थ	ह	जे	त	य	मी	रे	मि	दि	ए	ह	जे	जा	ढ	वी

शब्दावली शब्द-सूची

एंटीवायरसटूल, सिग्नेचर, स्कैनर, रैनसमवेयर, फ़ायरवॉल, रियलटाइमसुरक्षा, वायरसडेटाबेस, व्यवहार

चेकपॉइंट 6, वैकल्पिक: सुलभ शब्दावली मिलान

वर्ड सर्च के 8 शब्दावली पदों में से प्रत्येक को उसकी सही परिभाषा से मिलाएँ; खाली स्थान में अक्षर (A-H) लिखें।

शब्दावली के शब्द

- **A. एंटीवायरसटूल**
- **B. सिग्नेचर**
- **C. स्कैनर**
- **D. रैनसमवेयर**
- **E. फ़ायरवॉल**
- **F. रियलटाइमसुरक्षा**
- **G. वायरसडेटाबेस**
- **H. व्यवहार**

परिभाषाएँ और मिलान फ़ील्ड

1. दुर्भावनापूर्ण प्रोग्राम, जो फ़ाइलें लॉक करके उन्हें खोलने के बदले फिरौती मांगता है। ____
2. किसी प्रोग्राम की गतिविधियों का तरीका, जिसकी निगरानी से दुर्भावनापूर्ण संचालन पकड़ा जाता है। ____
3. नियमों के आधार पर नेटवर्क ट्रैफ़िक को रोकने या अनुमति देने वाली सुरक्षा दीवार। ____
4. ज्ञात मैलवेयर की पहचान के लिए इस्तेमाल होने वाला अनोखा डिजिटल पैटर्न या फ़िंगरप्रिंट। ____
5. ज्ञात खतरों की पहचान-सूचियों का संग्रह, जिससे फ़ाइलों का मिलान किया जाता है। ____
6. सॉफ़्टवेयर सूट, जो एंडपॉइंट को एक्सप्लॉइट से स्कैन और सुरक्षित करता है। ____
7. प्रोग्राम, जो फ़ाइलों और मेमोरी की जांच करके खतरनाक कोड ढूंढता है। ____
8. सक्रिय निगरानी, जो फ़ाइल खुलते ही उसमें मौजूद खतरे को तुरंत पकड़ लेती है। ____

चेकपॉइंट 7: उलझे शब्दों की चुनौती

नीचे के अक्षरों को सुलझाकर साइबर सुरक्षा की प्रमुख अवधारणाएँ और शब्द पता करें। अपने उत्तर दिए गए इनपुट बॉक्स में लिखें।

1. ट्रूयरएंसटीलवा
2. रनस्कै
3. रफ़ालवॉय
4. सबेसटाडवायर
5. रसिचग्रे
6. यसवेरैमरन
7. मरिरक्षासुटायइल
8. व्यरहाव

अतिरिक्त गतिविधि: झटपट सोचें

हर श्रेणी में 3 उत्तर। जो सबसे पहले सूची भर दे, वह जीतता है।

1	सॉफ़्टवेयर अपडेट करने के कारण			
2	IT मदद के लिए आप जिनसे पूछ सकते हैं			
3	एंटीवायरस को कुछ मिलने पर आप जो करेंगे			
4	कंप्यूटर वायरस के संकेत			
5	ऐसी चीज़ें जिन्हें क्वारंटीन किया जाता है			
6	ऐसी जगहें जहाँ वायरस छिपते हैं			
7	ऐसी जानकारी जो आपको कभी साझा नहीं करनी चाहिए			
8	दुर्भावनापूर्ण सॉफ़्टवेयर के प्रकार			
9	आपके जाने-पहचाने सुरक्षा टूल			
10	ऐसी चीज़ें जिन्हें एंटीवायरस स्कैन करता है			
11	ऐसी चीज़ें जिनका आप बैकअप लेते हैं			
12	ऐसे डिवाइस जिन्हें हैक किया जा सकता है			
13	आपके जाने-पहचाने एंटीवायरस प्रोग्राम			
14	झूठे अलार्म के कारण			
15	सुरक्षित आदतें जो आप आज से शुरू कर सकते हैं			

चेकपॉइंट 8: साइबर सुरक्षा केस स्टडी

नीचे दिए गए वास्तविक परिदृश्यों को हल करने के लिए सीखी हुई अवधारणाओं का उपयोग करें।

केस स्टडी 1: सिग्नेचर बनाम ह्यूरिस्टिक स्कैन

👷

परिदृश्य: एक कर्मचारी किसी दूसरी टीम की आंतरिक रूप से बनाई गई कस्टम यूटिलिटी डाउनलोड करता है। सिग्नेचर स्कैनर उसे पास कर देता है, लेकिन ह्यूरिस्टिक स्कैनर उसे संदिग्ध बताता है।

चर्चा प्रश्न: समझाइए कि ऐसा क्यों हुआ और फ़ाइल सुरक्षित है या नहीं, यह कैसे जाँचा जाए।

केस स्टडी 2: फ़ॉल्स पॉज़िटिव को संभालना

👷

परिदृश्य: एक सॉफ़्टवेयर डेवलपर अपना ऐप्लिकेशन कंपाइल करता है। सिस्टम का एंटीवायरस नई एक्ज़ीक्यूटेबल फ़ाइल को मैलवेयर बताता है और उसे क्वारंटीन कर देता है।

चर्चा प्रश्न: व्हाइटलिस्टिंग के जोखिम बताइए और सही समाधान का रास्ता समझाइए।

चेकपॉइंट 9: कूट संदेश को डिकोड करें

साइबर सुरक्षा पेशेवर नेटवर्क संपत्तियों को ऑनलाइन ख़तरा पैदा करने वालों से बचाता है। नीचे दी गई अक्षर-से-संख्या कुंजी का उपयोग करके संदेश को डिक्रिप्ट करें और खाली स्थानों में मेल खाते अक्षर लिखें।

अक्षर-से-संख्या एन्क्रिप्शन कुंजी

अ=1 आ=2 इ=3 ई=4 उ=5 ऊ=6 ऋ=7 ए=8 ऐ=9 ओ=10 औ=11 ऑ=12

क=13 ख=14 ग=15 घ=16 ङ=17 च=18 छ=19 ज=20 झ=21 ञ=22 ट=23 ठ=24

ड=25 ढ=26 ण=27 त=28 थ=29 द=30 ध=31 न=32 प=33 फ=34 ब=35 भ=36

म=37 य=38 र=39 ल=40 व=41 श=42 ष=43 स=44 ह=45 ा=46 ि=47 ी=48

ु=49 ू=50 ृ=51 े=52 ै=53 ो=54 ौ=55 ॉ=56 ं=57 ँ=58 ः=59 ़=60

्=61

13	54	25		41	47	42	61	40	52	43	27		44	52		32	38	46

37	53	40	41	52	38	39		33	45	18	46	32	52	57

डिकोड किया गया संदेश:

सुझाव: हर संख्या वर्णमाला में उस अक्षर की स्थिति दर्शाती है (जैसे 1 = अ, 2 = आ, 61 = ्)।

चेकपॉइंट 10: बुनियादी साइबर सुरक्षा FAQ (भाग A)

ऑनलाइन खतरों को कम करने से जुड़े आम सवाल और जवाब देखें।

Q1: एंटीवायरस सॉफ़्टवेयर मैलवेयर की पहचान कैसे करता है?

यह डेटाबेस सिग्नेचर मिलान, ह्यूरिस्टिक कोड लेआउट विश्लेषण और रियल-टाइम व्यवहार निगरानी से मैलवेयर की पहचान करता है।

Q2: सिग्नेचर-आधारित पहचान क्या है?

यह स्कैनिंग विधि है जो क्रिप्टोग्राफ़िक फ़ाइल हैश को ज्ञात मैलवेयर ख़तरों की डेटाबेस सूचियों से मिलाती है।

Q3: हेयूरिस्टिक स्कैनर क्या है?

ह्यूरिस्टिक्स किसी फ़ाइल की संरचना और कोड निर्देशों का विश्लेषण करते हैं और मैलवेयर वेरिएंट में आम संदिग्ध पैटर्न को चिह्नित करते हैं।

Q4: किसी फ़ाइल के क्वारंटीन होने का क्या मतलब है?

एंटीवायरस फ़ाइल को सुरक्षित, अलग फ़ोल्डर में भेज देता है और ऑपरेटिंग सिस्टम की सुरक्षा के लिए उसका चलना रोक देता है।

Q5: एंटीवायरस फ़ॉल्स पॉज़िटिव क्या है?

यह ऐसी त्रुटि है जिसमें स्कैनिंग एल्गोरिदम वैध, सुरक्षित सॉफ़्टवेयर को गलती से मैलवेयर के रूप में चिह्नित कर देते हैं।

चेकपॉइंट 10: बुनियादी साइबर सुरक्षा FAQ (भाग B)

ऑनलाइन खतरों को कम करने से जुड़े आम सवाल और जवाब देखें।

Q6: व्यवहार निगरानी सिस्टम की सुरक्षा कैसे करती है?

यह चल रहे सॉफ़्टवेयर की रियल टाइम में निगरानी करता है और कोड इंजेक्ट करने जैसे संदिग्ध बदलाव का प्रयास करने वाली प्रक्रियाओं को ब्लॉक करता है।

Q7: सैंडबॉक्स टेस्टिंग महत्वपूर्ण क्यों है?

सैंडबॉक्सिंग अविश्वसनीय फ़ाइलों को अलग वर्चुअल मशीन में चलाती है और सिस्टम को जोखिम में डाले बिना उनकी क्रियाओं को सुरक्षित रूप से देखती है।

Q8: एंटीवायरस की डेफ़िनिशन कितनी बार अपडेट होनी चाहिए?

नए खोजे गए मैलवेयर प्रकारों को पहचानने के लिए स्कैनरों को डेफ़िनिशन रोज़ाना या हर घंटे अपडेट करनी चाहिए।

Q9: एंटीवायरस और EDR में क्या अंतर है?

एंटीवायरस फ़ाइल स्कैनिंग पर केंद्रित होता है, जबकि Endpoint Detection and Response (EDR) नेटवर्क-व्यापी खतरे की ट्रैकिंग और नियंत्रण प्रदान करता है।

Q10: क्या मैं दो एंटीवायरस प्रोग्राम एक साथ चला सकता हूँ?

नहीं। दो सक्रिय स्कैनर चलाने से सिस्टम में टकराव होता है, प्रदर्शन धीमा होता है और वे एक-दूसरे के कार्यों को ब्लॉक कर सकते हैं।

चेकपॉइंट 10: उन्नत सुरक्षा FAQ (भाग C)

सुरक्षा फ़्रेमवर्क, मैलवेयर विश्लेषण और डेटा अनुपालन के उन्नत तकनीकी पहलुओं को जानें।

Q1: ह्यूरिस्टिक नियम खतरे के बायपास को कैसे न्यूनतम करते हैं?

ह्यूरिस्टिक्स विशिष्ट सिग्नेचर के बजाय सामान्य ख़तरा पैटर्न का विश्लेषण करते हैं, जिससे ज्ञात मैलवेयर परिवारों के संशोधित वेरिएंट पकड़े जाते हैं।

Q2: पॉलिमॉर्फ़िक वायरस क्या है?

यह ऐसा मैलवेयर है जो हर निष्पादन के साथ अपना फ़ाइल लेआउट और डिक्रिप्शन रूटीन बदल लेता है, जिससे सिग्नेचर स्कैन बेअसर हो जाते हैं।

Q3: सैंडबॉक्स VM से बचने की कोशिश का पता कैसे लगाते हैं?

आधुनिक सैंडबॉक्स माउस क्लिक और सिस्टम अपटाइम की नकल करते हैं, जिससे वर्चुअल मशीन में चलने पर छिपने के लिए बने मैलवेयर को चकमा दिया जाता है।

Q4: सिग्नेचर अपडेट डाउनलोड के फ़ॉर्मेट क्या हैं?

अपडेट आमतौर पर हल्की इन्क्रीमेंटल बाइनरी डिफ़ फ़ाइलें होती हैं, जिससे क्लाइंट की नेटवर्क बैंडविड्थ कम खर्च होती है।

Q5: एंडपॉइंट एजेंट लोकल स्कैन कैसे प्रबंधित करते हैं?

एजेंट हल्की बैकग्राउंड जाँच करते हैं और गहरी क्रिप्टोग्राफ़िक हैश लुकअप को क्लाउड ख़तरा डेटाबेस पर भेज देते हैं।

चेकपॉइंट 10: उन्नत सुरक्षा FAQ (भाग D)

सुरक्षा फ़्रेमवर्क, मैलवेयर विश्लेषण और डेटा अनुपालन के उन्नत तकनीकी पहलुओं को जानें।

Q6: रूटकिट डिटेक्शन स्कैनिंग क्या है?

यह कर्नेल-स्तर की मेमोरी टेबल को स्कैन करता है और उन OS API को बायपास करता है जिन्हें रूटकिट अपने सक्रिय थ्रेड छिपाने के लिए हुक करते हैं।

Q7: बिहेवियर स्कैनिंग रैनसमवेयर को कैसे ब्लॉक करती है?

यह स्वचालित बड़े पैमाने की फ़ाइल एन्क्रिप्शन लूप का पता लगाता है और सिस्टम डेटाबेस लॉक होने से पहले होस्ट प्रोसेस को समाप्त कर देता है।

Q8: कोड-साइनिंग सर्टिफ़िकेट सत्यापन क्या है?

स्कैनर कोड के डिजिटल हस्ताक्षरों को विश्वसनीय रूट सर्टिफ़िकेट अथॉरिटी से मिलाकर जाँचते हैं और सॉफ़्टवेयर डेवलपर की पहचान सत्यापित करते हैं।

Q9: पैकर स्कैनिंग इंजन को कैसे प्रभावित करते हैं?

पैकर मैलवेयर पेलोड को कंप्रेस या एन्क्रिप्ट करते हैं। सिग्नेचर मिलान चलने से पहले स्कैनर को फ़ाइल को मेमोरी में अनपैक करना पड़ता है।

Q10: EDR टूल आइसोलेशन को स्वचालित कैसे करते हैं?

EDR एजेंट समझौता हो चुके एंडपॉइंट को नेटवर्क स्तर पर क्वारंटीन करते हैं, जिससे पार्श्व गति रुकती है जबकि विश्लेषक की पहुँच बनी रहती है।

भाग 11: 10 वास्तविक साइबर सुरक्षा तथ्य और अंतर्दृष्टियाँ

सुरक्षा उल्लंघनों, बचाव तंत्रों और अनुपालन मानकों से जुड़े वास्तविक तथ्य देखें।

1. सुरक्षा इनसाइट

सिग्नेचर डेटाबेस ज्ञात मैलवेयर के हैश संग्रहीत करते हैं, इसलिए डेफ़िनिशन अपडेट होने तक बिल्कुल नई या बदली हुई फ़ाइलें छूट जाती हैं।

2. सुरक्षा इनसाइट

ह्यूरिस्टिक इंजन सिग्नेचर बनने से पहले कुछ नए मैलवेयर वेरिएंट को चिह्नित कर सकते हैं, लेकिन इसकी कीमत अधिक फ़ॉल्स पॉज़िटिव है।

3. सुरक्षा इनसाइट

झूठे पॉज़िटिव अलर्ट से IT टीमों का वह समय लगता है जो गलती से क्वारंटीन की गई फ़ाइलों को जाँचने और बहाल करने में जाता है।

4. सुरक्षा इनसाइट

पॉलिमॉर्फ़िक मैलवेयर हर प्रति के साथ अपना कोड बदलता है, इसलिए रक्षक सिग्नेचर के साथ ह्यूरिस्टिक और व्यवहार जाँच भी जोड़ते हैं।

6. सुरक्षा इनसाइट

मैलवेयर लेखक ऐसे कस्टम कोड लिखते हैं जो सैंडबॉक्स माहौल की जाँच करते हैं और टाइमर से बचने के लिए निष्पादन में देरी करते हैं।

5. सुरक्षा इनसाइट

क्लाउड-आधारित एंटीवायरस इंजन संदिग्ध फ़ाइल हैश की जाँच लगभग रीयल-टाइम में बड़े ऑनलाइन खतरा डेटाबेस से करते हैं।

7. सिक्योरिटी इनसाइट

विक्रेता नियमित रूप से एंडपॉइंट पर डेफ़िनिशन अपडेट भेजते हैं, ताकि स्कैनर नए पुष्ट खतरों को पहचान सकें।

8. सिक्योरिटी इनसाइट

रैनसमवेयर बिहेवियरल मॉनिटर फ़ाइल एन्क्रिप्शन और शैडो कॉपी हटाने से जुड़ी विशिष्ट Win32 API कॉल को निशाना बनाते हैं।

9. सिक्योरिटी इनसाइट

वैध कोड हस्ताक्षर फ़ॉल्स-पॉज़िटिव का जोखिम घटा सकते हैं, लेकिन हस्ताक्षरित फ़ाइलें भी स्कैन की जाती हैं, क्योंकि मैलवेयर भी हस्ताक्षरित हो सकता है।

10. सुरक्षा इनसाइट

रूटकिट सिस्टम कर्नेल की संरचनाएँ बदल देते हैं, इसलिए उन्हें पहचानने और साफ़ करने के लिए विशेष बूट-टाइम स्कैनर चाहिए।

तकनीकी संदर्भ और स्रोत

यह अध्ययन गाइड और इंटरैक्टिव पहेलियाँ वैश्विक NIST, OWASP और डेटा गोपनीयता अनुपालन मानकों से तैयार की गई हैं। शैक्षणिक और उद्योग संदर्भ

शैक्षणिक और उद्योग संदर्भ

[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

उत्तर कुंजी: चेकपॉइंट 1 – बहुविकल्पीय

1 **प्रश्न 1** सिग्नेचर **सही उत्तर: A**

शिक्षण नोट

सिग्नेचर स्कैनिंग ज्ञात डेटाबेस हैश पर निर्भर करती है, इसलिए अज्ञात या संशोधित मैलवेयर को पहचानने में विफल रहती है। उद्धरण: OWASP Secure Configuration।

2 **प्रश्न 2** ह्यूरिस्टिक्स **सही उत्तर: A**

शिक्षण नोट

ह्यूरिस्टिक्स कोड की बनावट और कमांड का विश्लेषण करते हैं ताकि नए खतरों के वेरिएंट की संदिग्ध विशेषताएँ पहचानी जा सकें। उद्धरण: Center for Internet Security (CIS)।

3 **प्रश्न 3** सैंडबॉक्सिंग **सही उत्तर: A**

शिक्षण नोट

सैंडबॉक्स संदिग्ध फ़ाइलों को अलग वर्चुअल मशीन में चलाता है ताकि निष्पादन व्यवहार को सुरक्षित रूप से देखा जा सके। उद्धरण: NIST Digital Identity।

4 **प्रश्न 4** व्यवहारात्मक **सही उत्तर: A**

शिक्षण नोट

बिहेवियर स्कैनिंग चल रहे प्रोग्रामों की रीयल-टाइम निगरानी करती है ताकि अनधिकृत सिस्टम बदलावों को रोका जा सके। उद्धरण: Center for Internet Security (CIS)।

5 **प्रश्न 5** अपडेट **सही उत्तर: A**

शिक्षण नोट

स्कैनर खतरे के परिदृश्य से तालमेल बनाए रखने के लिए रोज़ाना क्रमिक डेफ़िनिशन अपडेट डाउनलोड करते हैं। उद्धरण: OWASP Secure Configuration।

उत्तर कुंजी: चेकपॉइंट 2 – सही या गलत

6 **प्रश्न 6** सिग्नेचर **सही उत्तर: सही**

शिक्षण नोट

सिग्नेचर टूल क्रिप्टोग्राफ़िक हैश की गणना करते हैं और उन्हें ज्ञात खतरों के हैश के डेटाबेस से मिलाते हैं। उद्धरण: OWASP Secure Configuration।

7 **प्रश्न 7** ह्यूरिस्टिक्स **सही उत्तर: सही**

शिक्षण नोट

ह्यूरिस्टिक इंजन नियम-आधारित लेआउट चलाते हैं, जो वैध और सुरक्षित फ़ाइलों को भी संदिग्ध के रूप में चिह्नित कर सकते हैं। उद्धरण: Center for Internet Security (CIS)।

8 **प्रश्न 8** सैंडबॉक्सिंग **सही उत्तर: गलत**

शिक्षण नोट

सैंडबॉक्स कोड को वर्चुअल कंटेनर में चलाता है और नेटवर्क शेयर तक पहुँच को पूरी तरह रोक देता है। उद्धरण: NIST Digital Identity।

9 **प्रश्न 9** व्यवहारात्मक **सही उत्तर: सही**

शिक्षण नोट

रीयल-टाइम मॉनिटरिंग उन चल रही प्रक्रियाओं को चिह्नित करती है जो अवैध राइट या फ़ाइल लॉकिंग का प्रयास करती हैं। उद्धरण: Center for Internet Security (CIS)।

10 **प्रश्न 10** **सही उत्तर: गलत**

शिक्षण नोट

कोई भी एंटीवायरस हर ज़ीरो-डे हमले को नहीं रोकता; अज्ञात खतरे सिग्नेचर और ह्यूरिस्टिक्स से बच सकते हैं।

शब्दावली कुंजियाँ और ग्रेडिंग रूब्रिक

शिक्षक के लिए ग्रेडिंग रूब्रिक: हर सही मिलान (कुल 8 अंक) और संदर्भ शब्द (कुल 6 अंक) के लिए 1 अंक दें।

चेकपॉइंट 4: उत्तर – अवधारणा मिलान

D 1. हैश हस्ताक्षर	G 2. कोड ह्यूरिस्टिक्स	E 3. फ़ाइल सैंडबॉक्स	C 4. व्यवहार स्कैन
F 5. दैनिक अपडेट	H 6. फ़ॉल्स पॉज़िटिव	A 7. ख़तरा अलगाव	B 8. एंटीवायरस टूल

चेकपॉइंट 3: उत्तर – प्रमुख शब्द

1 सिग्नेचर	2 ह्यूरिस्टिक	3 वायरस डेटाबेस	4 व्यवहार
5 अपडेट	6 रैनसमवेयर		

चेकपॉइंट 6, वैकल्पिक: उत्तर – शब्द मिलान

1 D – रैनसमवेयर	2 H – व्यवहार	3 E – फ़ायरवॉल	4 B – सिग्नेचर
5 G – वायरसडेटाबेस	6 A – एंटीवायरसटूल	7 C – स्कैनर	8 F – रियलटाइमसुरक्षा

शिक्षकों के लिए चर्चा नोट

प्रमुख शब्द:
जाँचें कि क्या विद्यार्थी हैश हस्ताक्षर, कोड ह्यूरिस्टिक्स और फ़ाइल सैंडबॉक्स को अपने शब्दों में समझा सकते हैं और हर एक का उदाहरण दे सकते हैं।

केस स्टडी:
विद्यार्थियों से कहें कि वे अपनी सिफ़ारिशें राय के बजाय वर्कशीट के तथ्यों पर आधारित करें।

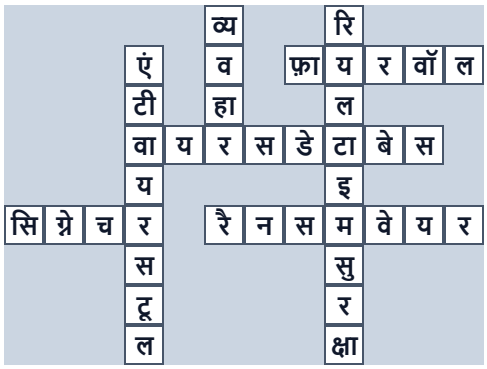
स्रोतों का मूल्यांकन:
विद्यार्थियों से वर्कशीट के स्रोतों में कम से कम एक कथन की पुष्टि करवाएँ और चर्चा करें कि आँकड़े, कीमतें और नियम समय के साथ क्यों बदल सकते हैं।

पहेलियों की कुंजियाँ और शिक्षक नोट

शब्द खोज समाधान

जा	सा	वा	ड	रे	स	ख	फ़ा	नि	फ	ढ	मा	ना	का	रे
दे	सि	मी	क	पि	ता	ति	य	रै	ज	श	भ	ऊ	अ	ऊ
ए	रि	र	वि	श	य	वि	र	व	न	वा	पा	ल	च	से
कि	य	हा	घ	प	के	की	वॉ	व	सि	स	री	त	की	कि
स	सि	व	ना	ने	रि	पा	ल	ते	ण	सि	म	ए	ता	सा
बे	मी	व्य	न	नी	य	ऋ	एं	ले	घ	ति	ग्रे	वे	जि	ला
टा	ए	जी	ले	ड	ल	ल	द	टी	जे	घ	के	च	य	च
डे	से	दे	री	ए	टा	पी	उ	अ	वा	जे	मि	घ	र	र
स	व	आ	च	मी	इ	च	ट	थ	फ	य	ग	ना	सी	का
र	ज	फ	नी	जी	म	ता	ठ	से	लि	ट	र	आ	इ	से
य	रा	के	री	पा	सु	वा	सि	य	नि	पि	ने	स	ख	के
वा	वे	ऊ	ड	नी	र	दे	दि	भ	र	आ	नि	जे	टू	वे
वे	ष	ण	प	कि	क्षा	से	य	न	ह	ह	ते	रा	द	ल
सा	सी	थ	जे	इ	मे	ला	स्कै	ढ	पे	ऋ	वे	नी	वे	उ
थ	ह	जे	त	य	मी	रे	मि	दि	ए	ह	जे	जा	ढ	वी

क्रॉसवर्ड समाधान



बाएँ से दाएँ

4 बाएँ से दाएँ: फ़ायरवॉल नियमों के आधार पर नेटवर्क ट्रैफ़िक को रोकने या अनुमति देने वाली सुरक्षा दीवार (5 अक्षर)

5 बाएँ से दाएँ: वायरसडेटाबेस ज्ञात खतरों की पहचान-सूचियों का संग्रह, जिससे फ़ाइलों का मिलान किया जाता है (8 अक्षर)

6 बाएँ से दाएँ: सिग्नेचर ज्ञात मैलवेयर की पहचान के लिए इस्तेमाल होने वाला अनोखा डिजिटल पैटर्न या फ़िंगरप्रिंट (4 अक्षर)

7 बाएँ से दाएँ: रैनसमवेयर दुर्भावनापूर्ण प्रोग्राम, जो फ़ाइलें लॉक करके उन्हें खोलने के बदले फिरौती मांगता है (7 अक्षर)

ऊपर से नीचे

1 ऊपर से नीचे: व्यवहार किसी प्रोग्राम की गतिविधियों का तरीका, जिसकी निगरानी से दुर्भावनापूर्ण संचालन पकड़ा जाता है (4 अक्षर)

2 ऊपर से नीचे: रियलटाइमसुरक्षा सक्रिय निगरानी, जो फ़ाइल खुलते ही उसमें मौजूद खतरे को तुरंत पकड़ लेती है (9 अक्षर)

3 ऊपर से नीचे: एंटीवायरसटूल सॉफ़्टवेयर सूट, जो एंडपॉइंट को एक्सप्लॉइट से स्कैन और सुरक्षित करता है (8 अक्षर)

अक्षर-फेर शब्द और कूट संदेश हल कुंजी

शब्द-अनस्क्रैम्बल गतिविधि और Secret Cipher Challenge की ग्रेडिंग कुंजी।

शब्द अनस्क्रैम्बल कुंजी

1. टूयरएंसटीलवा — **एंटीवायरसटूल**
2. रनस्कै — **स्कैनर**
3. रफ़ालवॉय — **फ़ायरवॉल**
4. सबेसटाडेवायर — **वायरसडेटाबेस**
5. रसिचग्रे — **सिग्नेचर**
6. यसवेरैमरन — **रैनसमवेयर**
7. मरिरक्षासुटायइल — **रियलटाइमसुरक्षा**
8. व्यरहाव — **व्यवहार**

गुप्त कूट चुनौती कुंजी

"कोड विश्लेषण से नया मैलवेयर पहचानें"

केस स्टडी के उत्तर

A केस स्टडी 1: सिग्नेचर बनाम ह्यूरिस्टिक स्कैन

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक कर्मचारी किसी दूसरी टीम द्वारा आंतरिक रूप से बनाई गई कस्टम यूटिलिटी डाउनलोड करता है। सिग्नेचर स्कैनर उसे पास कर देता है, लेकिन ह्यूरिस्टिक स्कैनर उसे संदिग्ध फ़्लैग करता है।
- अनुशंसित रणनीति और समाधान: ऐसा क्यों हुआ: सिग्नेचर स्कैनिंग फ़ाइल हैश जाँचती है; चूँकि फ़ाइल कस्टम है, वह थ्रेट डेटाबेस में नहीं है। ह्यूरिस्टिक संरचना का विश्लेषण करते हैं और संदिग्ध क्रियाओं (जैसे रजिस्ट्री राइट) को फ़्लैग करते हैं। सत्यापन: क्रियाओं को देखने के लिए फ़ाइल को सैंडबॉक्स में चलाएँ, डिजिटल हस्ताक्षर जाँचें, और हैश को थ्रेट इंटेलिजेंस पोर्टल पर सबमिट करें।

B केस स्टडी 2: फ़ॉल्स पॉज़िटिव को संभालना

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक सॉफ़्टवेयर डेवलपर अपना एप्लिकेशन कंपाइल करता है। सिस्टम एंटीवायरस नए एक्ज़ीक्यूटेबल को मैलवेयर बताकर क्वारंटीन कर देता है।
- अनुशंसित रणनीति और समाधान: व्हाइटलिस्टिंग के जोखिम: स्कैनर को बायपास करने से असली संक्रमित कोड चल सकता है। समाधान का रास्ता: फ़ाइल को विश्लेषण के लिए एंटीवायरस विक्रेता को भेजें, सर्टिफ़िकेट अथॉरिटी से कोड पर डिजिटल हस्ताक्षर करें, और एंटीवायरस बंद करने की बजाय अस्थायी रूप से विशिष्ट फ़ोल्डर अपवाद कॉन्फ़िगर करें।