نام: _____ تاریخ: _____ نمبر: _____

اینٹی وائرس سافٹ ویئر اور اینڈ پوائنٹ تحفظ کی گائیڈ

سگنیچر ڈیٹیکشن، ہیورسٹکس، رویے کی نگرانی، سینڈ باکسنگ، اپ ڈیٹس

اینٹی وائرس سافٹ ویئر سیکھنے کا جائزہ

محفوظ شدہ
ڈیٹا کی خفیہ کاری
256 بٹ AES معیار

تعمیل شدہ
عالمی معیارات
GDPR اور CCPA فریم ورکس

زیرو ٹرسٹ
رسائی کی پالیسی
ملٹی فیکٹر تصدیق

خوش آمدید! یہ سرگرمی پیکٹ آپ کو اینٹی وائرس سافٹ ویئر اور اینڈ پوائنٹ پروٹیکشن سے متعارف کراتا ہے۔ آپ سگنیچر ڈیٹا بیسز، ہیورسٹک اسکینرز، رویے کی نگرانی، سینڈ باکس ورچوئل فائلوں، اور غلط مثبت نتائج میں کمی کا جائزہ لیں گے۔

ورک شیٹ کے چیک پوائنٹس

- ☐ **حصہ 1-4: سائبر سیکیورٹی اور خطرات سے بچاؤ میں مہارت حاصل کریں۔**
- ☐ **حصہ 5-7: کراس ورڈ اور ورڈ سرچ پہیلیاں حل کریں۔**
- ☐ **حصہ 8-9: کیس اسٹڈیز اور سائفر چیلنج حل کریں۔**
- ☐ **حصہ 10: بنیادی اور اعلیٰ FAQ صفحات کا جائزہ لیں۔**
- ☐ **حصہ 11: 10 دلچسپ حقیقی دنیا کے حقائق دریافت کریں۔**
- ☐ **اضافی: تیزی سے سوچیں چیلنج**

VPN.com سائبر سیکیورٹی گائیڈ کھولیں

URL: https://www.vpn.com/cybersecurity/antivirus/

آپ کی اینٹی وائرس حکمت عملی کا لرننگ روڈ میپ

- دستخط پر مبنی اور ہیورسٹک پر مبنی میل ویئر کی شناخت میں فرق واضح کریں۔
- رویے کی نگرانی اور سینڈ باکس آئسولیشن پروٹوکولز کو سمجھیں۔
- سسٹم کی کارکردگی اور اینڈ پوائنٹس پر ریئل ٹائم اسکین کے اثرات کا جائزہ لیں۔
- ڈیجیٹل سرٹیفکیٹ کی تصدیق کے ذریعے غلط مثبت درجہ بندیوں کو کم کریں۔
- کارپوریٹ اینڈ پوائنٹس میں روزانہ ڈیفینیشن اپڈیٹ کی تقسیم کا انتظام کریں۔

اینٹی وائرس گائیڈ کی ہدایات

کثیر انتخابی اور درست/غلط سوالات حل کریں، لفظوں کے ذخیرے کی مدد سے خالی جگہیں پُر کریں، تعریفوں کا ملان کریں، اور کراس ورڈ اور ورڈ سرچ پہیلیاں حل کریں۔ اپنے علم کو اینڈ پوائنٹ اینٹی وائرس سیکیورٹی پر لاگو کریں۔ اور آخر میں اضافی سرگرمی "تیزی سے سوچیں"۔

اینٹی وائرس تحفظ اور دستخطی اسکیننگ (تعارف)

اینٹی وائرس سافٹ ویئر میل ویئر کی نشاندہی، قرنطینہ اور خاتمے کے ذریعے اینڈ پوائنٹس کی حفاظت کرتا ہے۔ جدید سسٹمز زیرو ڈے حملوں کا پتہ لگانے کے لیے سگنیچر ڈیٹا بیس (معروف خطرات کے ہیشز سے ملان)، ہیورسٹکس (فائل کی ساخت کا تجزیہ) اور رویے کی نگرانی کو یکجا کرتے ہیں۔

ہر چیک پوائنٹ کو غور سے پڑھیں اور درست

چیک پوائنٹ 1: کثیر انتخابی چیلنج

1. دستخط پر مبنی شناخت کی ایک حد کیا ہے؟
   - A. یہ نامعلوم یا تبدیل شدہ میل ویئر کی شناخت نہیں کر سکتا
   - B. یہ غلط مثبت نتائج کی بلند شرح پیدا کرتا ہے
   - C. اس کے لیے زیادہ CPU پروسیسنگ طاقت درکار ہوتی ہے
   - D. یہ صرف انٹرنیٹ سے جڑے ہونے پر کام کرتا ہے

2. ہیورسٹک اسکینرز نئے میل ویئر ویریئنٹس کا پتا کیسے لگاتے ہیں؟
   - A. مشتبہ پیٹرن اور کوڈ ڈھانچوں کی نشاندہی کر کے
   - B. فائل ہیشز کو خطرات کے ڈیٹا بیس سے ملا کر
   - C. تمام غیر دستخط شدہ ایگزیکیوٹیبلز کو خودکار طور پر حذف کر کے
   - D. ہر فائل کو عوامی کلاؤڈ فولڈر میں اپ لوڈ کر کے

3. اینٹی وائرس سینڈ باکس ایگزیکیوشن کا مقصد کیا ہے؟
   - A. فائلوں کو محفوظ ورچوئل والٹ میں الگ کر کے ان کا تجزیہ کرنا
   - B. مقامی فائل سسٹم کی بیک اپ منتقلی کو تیز کرنا
   - C. مقامی آپریٹنگ سسٹم کے سیکیورٹی پیچز اپ ڈیٹ کرنا
   - D. اسٹوریج بچانے کے لیے بڑی دستاویزی فائلوں کو کمپریس کرنا

4. کون سا شناخت کا طریقہ خطرناک رویے کو حقیقی وقت میں نشان زد کرتا ہے؟
   - A. رویے کا تجزیہ جو سافٹ ویئر کی کارروائیوں کی نگرانی کرتا ہے
   - B. رات بھر کی جانے والی تاریخی لاگز کی جانچ
   - C. سست ایپس کی اطلاع دینے والے صارف کی دستی مداخلت
   - D. انسٹال شدہ پروگراموں کے ہفتہ وار دستی جائزے

5. اسکینرز کے لیے باقاعدہ تعریفی اپ ڈیٹس کیوں اہم ہیں؟
   - A. دستخط والے انجنوں کے ڈیٹا بیس کو خطرے کے شناخت کنندگان فراہم کرنا
   - B. آپریشنز کے دوران CPU کلاک اسپیڈ بڑھانے کے لیے
   - C. عالمی DNS نیم سرور کیشنگ کے اوقات تبدیل کرنے کے لیے
   - D. ویب براؤزر کی کوکی سیٹنگز کی اجازت دینے کے لیے

چیک پوائنٹ 2: درست یا غلط چیلنج

6 سوال (درست/غلط) 6

6. سگنیچر ڈیٹیکشن کرپٹوگرافک فائل ہیشز کا ڈیٹا بیس فہرستوں سے موازنہ کرتی ہے۔

درست غلط

7 سوال (درست/غلط) 7

7. ہیورسٹک اسکینرز محفوظ فائلوں پر غلط مثبت الرٹس دے سکتے ہیں۔

درست غلط

8 سوال (درست/غلط) 8

8. سینڈ باکس میل ویئر کو بغیر کسی حد کے نیٹ ورک فائلوں تک رسائی دیتا ہے۔

درست غلط

9 سوال (درست/غلط) 9

9. رویے کی اسکیننگ فائلوں کو اس وقت بلاک کرتی ہے جب وہ نقصان دہ کارروائیاں ظاہر کریں۔

درست غلط

10 سوال (درست/غلط) 10

10. معیاری اینٹی وائرس سافٹ ویئر تمام زیرو ڈے حملوں کو مکمل طور پر روک دیتا ہے۔

درست غلط

چیک پوائنٹ 3: کلیدی اصطلاح شامل کرنا

ذیل میں ہر جملہ پڑھیں اور خالی جگہ کو ورڈ بینک سے درست اصطلاح کے ساتھ پُر کریں۔

1. روایتی اسکینر معلوم میل ویئر کی شناخت کے لیے _____ کے ملان پر انحصار کرتا ہے۔
2. فائل کوڈ کے پیٹرن کا تجزیہ کرنا _____ اسکیننگ کہلاتا ہے۔
3. اینٹی وائرس ٹولز مشتبہ فائلوں کو ایک _____ ماحول میں الگ کر دیتے ہیں۔
4. ریئل ٹائم نگرانی مشتبہ سرگرمیوں کے لیے پروگراموں کے _____ پر نظر رکھتی ہے۔
5. اسکینرز نئے خطرات کو پہچاننے کے لیے ڈیٹا بیس کی _____ روزانہ ڈاؤن لوڈ کرتے ہیں۔
6. محفوظ پروگرام کو میل ویئر کے طور پر نشان زد کرنے سے _____ مثبت الرٹس جنم لیتے ہیں۔

الفاظ کا بینک

اپ ڈیٹس | رویے | سگنیچر | سینڈ باکس | علیحدگی | غلط | فائر وال | ہیورسٹکس

اپنے جوابات یہاں لکھیں:

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

چیک پوائنٹ 4: سیکیورٹی تصورات کا ملان

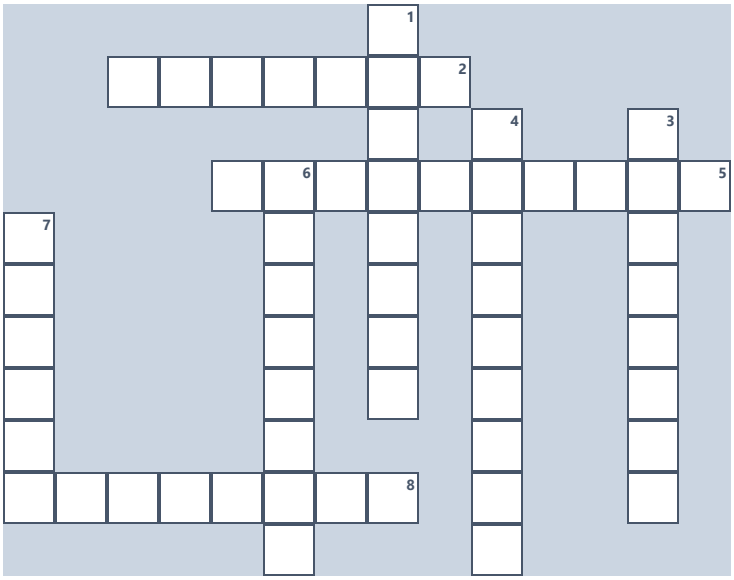
تعریفوں کا ملان

دائیں جانب کی ہر اصطلاح کو بائیں جانب کی درست تعریف سے ملائیں اور بھرے جانے والے ان پٹ باکس میں متعلقہ حرف (A-H) لکھیں۔

1. پیش دستخط	A	مشتبہ فائلوں کو محدود کرنا تاکہ مقامی سسٹم کے انکشاف سے بچا جا سکے۔
2. کوڈ ہیورسٹکس	B	سافٹ ویئر سوئٹ جو اینڈ پوائنٹس کو ایکسپلائٹس سے اسکین اور محفوظ کرتا ہے۔
3. فائل سینڈ باکس	C	چلتے ہوئے سافٹ ویئر کے اعمال میں نقصان دہ کارروائی کے پیٹرنز کی نگرانی۔
4. رویے کی اسکین	D	معلوم خطرات کی شناخت کے لیے استعمال ہونے والا منفرد کرپٹوگرافک ڈیٹا بیس نشان۔
5. روزانہ اپ ڈیٹس	E	محفوظ ورچوئل ٹیسٹ ماحول جو غیر معتبر کوڈ کو بحفاظت چلاتا ہے۔
6. غلط مثبت	F	باقاعدہ ڈیفینیشن ڈاؤن لوڈز جو تھریٹ ڈیٹا بیس کو مواد فراہم کرتے ہیں۔
7. خطرے کی علیحدگی	G	قواعد پر مبنی تجزیہ جو مشکوک کوڈ ساخت والی فائلوں کو نشان زد کرتا ہے۔
8. اینٹی وائرس ٹول	H	سیکیورٹی الرٹ جو محفوظ سافٹ ویئر کو غلطی سے میل ویئر قرار دے دیتا ہے۔

چیک پوائنٹ 5: کراس ورڈ پہیلی

فعال سفید خانوں میں حروف ٹائپ کر کے کراس ورڈ پہیلی حل کریں۔ نمبر نیچے دیے گئے سراغوں سے مطابقت رکھتے ہیں۔



افقی

2. مشتبہ فائلوں کو الگ تھلگ رکھنا تاکہ مقامی سسٹم خطرے سے دوچار نہ ہو (7)

5. سافٹ ویئر سوٹ جو اینڈ پوائنٹس کو حملوں سے اسکین کر کے محفوظ بناتا ہے (10)

8. محفوظ ورچوئل آزمائشی ماحول جس میں غیر معتبر کوڈ بحفاظت چلایا جاتا ہے (8)

عمودی

1. ایسا سیکیورٹی الرٹ جو محفوظ سافٹ ویئر کو غلطی سے میل ویئر قرار دے دے (8)

3. اصولوں پر مبنی تجزیہ جو مشتبہ کوڈ ساخت والی فائلوں کی نشاندہی کرتا ہے (8)

4. منفرد کرپٹوگرافک ڈیٹا بیس نشان جو معلوم خطرات کی شناخت کے لیے استعمال ہوتا ہے (9)

6. چلتے ہوئے سافٹ ویئر کی کارروائیوں پر نظر رکھنا تاکہ بدنیتی پر مبنی عمل کے نمونے ملیں (8)

7. باقاعدگی سے ڈاؤن لوڈ ہونے والی تعریفیں جو خطرات کے ڈیٹا بیس کو تازہ رکھتی ہیں (6)

چیک پوائنٹ 5 – متبادل سرگرمی: قابلِ رسائی کراس ورڈ سراغ

اسکرین ریڈر اور کی بورڈ استعمال کرنے والے صارفین نیچے دیے گئے ٹیکسٹ فیلڈز میں کراس ورڈ کے جوابات براہ راست ٹائپ کر سکتے ہیں۔ افقی سراغ عمودی سراغ

افقی

2 افقی: مشتبہ فائلوں کو الگ تھلگ رکھنا تاکہ مقامی سسٹم خطرے سے دوچار نہ ہو (7 حروف):

5 افقی: سافٹ ویئر سوٹ جو اینڈ پوائنٹس کو حملوں سے اسکین کر کے محفوظ بناتا ہے (10 حروف):

8 افقی: محفوظ ورچوئل آزمائشی ماحول جس میں غیر معتبر کوڈ بحفاظت چلایا جاتا ہے (8 حروف):

عمودی

1 عمودی: ایسا سیکیورٹی الرٹ جو محفوظ سافٹ ویئر کو غلطی سے میل ویئر قرار دے دے (8 حروف):

3 عمودی: اصولوں پر مبنی تجزیہ جو مشتبہ کوڈ ساخت والی فائلوں کی نشاندہی کرتا ہے (8 حروف):

4 عمودی: منفرد کرپٹوگرافک ڈیٹا بیس نشان جو معلوم خطرات کی شناخت کے لیے استعمال ہوتا ہے (9 حروف):

6 عمودی: چلتے ہوئے سافٹ ویئر کی کارروائیوں پر نظر رکھنا تاکہ بدنیتی پر مبنی عمل کے نمونے ملیں (8 حروف):

7 عمودی: باقاعدگی سے ڈاؤن لوڈ ہونے والی تعریفیں جو خطرات کے ڈیٹا بیس کو تازہ رکھتی ہیں (6 حروف):

چیک پوائنٹ 6: پوشیدہ الفاظ کی تلاش

نیچے گرڈ میں چھپی 8 اہم اصطلاحات تلاش کریں۔ الفاظ افقی، عمودی یا ترچھے ہو سکتے ہیں۔

ش	ک	ع	ن	پ	ب	ا	ر	ب	س	ک	ٹ	ے	ی	ڈ
ل	ل	ر	ت	غ	س	گ	و	و	ت	ش	ے	ع	ش	ح
پ	چ	ے	ے	ل	ی	ہ	ی	و	گ	گ	چ	ن	و	ش
غ	ئ	ی	ت	ط	ط	ب	ہ	ی	د	م	و	ی	س	ر
ل	ہ	ت	ئ	ا	د	ش	ج	ج	ا	ط	ئ	پ	ٹ	چ
ئ	ی	ا	ب	ل	ڈ	پ	ا	ن	ی	ع	و	ت	ی	ی
چ	و	ت	م	ا	ت	س	ن	ا	ن	ش	ت	ل	ڈ	ن
ٹ	ر	گ	و	ر	ع	ی	چ	ہ	ٹ	ت	ر	د	پ	گ
چ	س	غ	و	م	ل	ن	ج	ی	ی	ئ	ہ	ر	ا	س
ش	ٹ	و	ع	ے	ی	ڈ	ن	ل	و	م	و	ا	ا	ش
ع	ک	ی	چ	ب	ح	ب	ح	ل	ا	ت	ی	ڈ	ہ	ی
ر	س	چ	ک	ح	د	ا	ح	ئ	ئ	ہ	ا	س	ط	ہ
ئ	د	و	و	د	گ	ک	م	ے	ر	ک	گ	س	ہ	گ
ک	د	ب	ح	ہ	ی	س	ح	ب	س	ڈ	چ	غ	م	ا
ط	م	ح	چ	ح	ئ	گ	پ	ط	ل	ن	م	س	چ	ئ

الفاظ کی فہرست

ہیشسگنیچر
ہیورسٹکس
سینڈباکس
رویہجانچ
اینٹیوائرس
اپڈیٹس
غلطالارم
علیحدگی

چیک پوائنٹ 6 – متبادل سرگرمی: قابلِ رسائی الفاظ کا ملان

ورڈ سرچ کی 8 اصطلاحات میں سے ہر ایک کو اس کی درست تعریف سے ملائیں اور خالی جگہ میں حرف (A-H) لکھیں۔

اصطلاحات
A. ہیشسگنیچر
B. ہیورسٹکس
C. سینڈباکس
D. رویہجانچ
E. اپڈیٹس
F. غلطالارم
G. علیحدگی
H. اینٹیوائرس

تعریفیں اور ملان کے خانے	
1. چلتے ہوئے سافٹ ویئر کی کارروائیوں پر نظر رکھنا تاکہ بدنیتی پر مبنی عمل کے نمونے ملیں۔	
2. سافٹ ویئر سوٹ جو اینڈ پوائنٹس کو حملوں سے اسکین کر کے محفوظ بناتا ہے۔	
3. باقاعدگی سے ڈاؤن لوڈ ہونے والی تعریفیں جو خطرات کے ڈیٹا بیس کو تازہ رکھتی ہیں۔	
4. اصولوں پر مبنی تجزیہ جو مشتبہ کوڈ ساخت والی فائلوں کی نشاندہی کرتا ہے۔	
5. مشتبہ فائلوں کو الگ تھلگ رکھنا تاکہ مقامی سسٹم خطرے سے دوچار نہ ہو۔	
6. منفرد کرپٹوگرافک ڈیٹا بیس نشان جو معلوم خطرات کی شناخت کے لیے استعمال ہوتا ہے۔	
7. محفوظ ورچوئل آزمائشی ماحول جس میں غیر معتبر کوڈ بحفاظت چلایا جاتا ہے۔	
8. ایسا سیکیورٹی الرٹ جو محفوظ سافٹ ویئر کو غلطی سے میل ویئر قرار دے دے۔	

چیک پوائنٹ 7: الجھے الفاظ کا چیلنج

سائبر سیکیورٹی کے اہم تصورات اور اصطلاحات ظاہر کرنے کے لیے نیچے دیے گئے حروف کو درست ترتیب میں لائیں۔ اپنے جوابات دیے گئے ان پٹ باکسز میں لکھیں۔

1. ن گ س ی ہ ی چ ر ش
2. ڈ س س ی ک ا ب ن
3. ا ڈ ی س ٹ پ
4. ی ل د ح گ ع ی
5. س ٹ ی س ر ہ ک و
6. ن چ ہ ا ر چ و ی
7. غ م ل ا ر ل ا ط
8. ر ٹ و س ا ی ی ا ئ ن

اضافی سرگرمی: تیزی سے سوچیں

ہر زمرے کے لیے 3 جوابات لکھیں۔ جو سب سے پہلے فہرست مکمل کرے وہ جیتتا ہے۔

1	سافٹ ویئر اپ ڈیٹ کرنے کی وجوہات			
2	وہ لوگ جن سے آپ آئی ٹی مدد مانگ سکتے ہیں			
3	اینٹی وائرس کو کچھ ملنے پر کرنے کے کام			
4	کمپیوٹر وائرس کی علامات			
5	وہ چیزیں جو قرنطینہ میں چلی جاتی ہیں			
6	وہ مقامات جہاں وائرس چھپتے ہیں			
7	وہ معلومات جو آپ کو کبھی شیئر نہیں کرنی چاہئیں			
8	نقصان دہ سافٹ ویئر کی اقسام			
9	آپ کے جانے پہچانے سیکیورٹی ٹولز کے نام			
10	وہ چیزیں جنہیں اینٹی وائرس اسکین کرتا ہے			
11	وہ چیزیں جن کا آپ بیک اپ لیتے ہیں			
12	وہ ڈیوائسز جنہیں ہیک کیا جا سکتا ہے			
13	آپ کے جانے پہچانے اینٹی وائرس پروگرامز کے نام			
14	غلط الارم کی وجوہات			
15	محفوظ عادات جو آپ آج شروع کر سکتے ہیں			

چیک پوائنٹ 8: سائبر سیکیورٹی کیس اسٹڈیز

جو تصورات آپ نے سیکھے ہیں انہیں نیچے دیے گئے حقیقی منظرناموں کو حل کرنے میں استعمال کریں۔

کیس اسٹڈی 1: دستخط پر مبنی اور ہیورسٹک اسکین کا موازنہ



منظرنامہ: ایک ملازم ایسی کسٹم یوٹیلیٹی ڈاؤن لوڈ کرتا ہے جو کسی دوسری ٹیم نے اندرونی طور پر بنائی ہے۔ سگنیچر اسکینر اسے پاس کر دیتا ہے، لیکن ہیورسٹک اسکینر اسے مشکوک قرار دیتا ہے۔

بحث کا سوال: وضاحت کریں کہ ایسا کیوں ہوا، اور فائل کے محفوظ ہونے کی تصدیق کیسے کی جائے۔

کیس اسٹڈی 2: غلط مثبت نتائج سے نمٹنا



منظرنامہ: ایک سافٹ ویئر ڈویلپر اپنی ایپلیکیشن کمپائل کرتا ہے۔ سسٹم اینٹی وائرس نئی ایگزیکیوٹیبل کو میل ویئر قرار دے کر قرنطینہ میں ڈال دیتا ہے۔

بحث کا سوال: وائٹ لسٹ کرنے کے خطرات بیان کریں، اور درست حل کا طریقہ واضح کریں۔

چیک پوائنٹ 9: سائفر حل کریں

سائبر سیکیورٹی پیشہ ور نیٹ ورک اثاثوں کو آن لائن خطرات پیدا کرنے والوں سے بچاتا ہے۔ نیچے دی گئی حرف سے عدد کی کلید استعمال کر کے خالی جگہوں میں متعلقہ حروف لکھ کر پیغام ڈی کرپٹ کریں۔

حرف سے عدد خفیہ کاری کی کلید

ا=1 ب=2 پ=3 ت=4 ٹ=5 ث=6 ج=7 چ=8 ح=9 خ=10 د=11 ڈ=12 ذ=13

ر=14 ڑ=15 ز=16 ژ=17 س=18 ش=19 ص=20 ض=21 ط=22 ظ=23 ع=24 غ=25 ف=26

ق=27 ک=28 گ=29 ل=30 م=31 ن=32 ں=33 و=34 ہ=35 ھ=36 ی=37 ے=38 ئ=39

38	39	32		38	18		38	37	16	7	4		28	5	18	14	34	37	35

33	37	32	1	8	35	3		4	1	14	22	10

ڈی کوڈ شدہ پیغام:

ٹپ: ہر نمبر اوپر دی گئی کلید کے ایک اردو حرف کو ظاہر کرتا ہے۔

چیک پوائنٹ 10: سائبر سیکیورٹی عمومی سوالات – بنیادی (حصہ A)

آن لائن خطرات کی روک تھام کے بارے میں عام سوالات اور جوابات کا جائزہ لیں۔

Q1: اینٹی وائرس سافٹ ویئر میلویئر کی شناخت کیسے کرتا ہے؟

یہ ڈیٹا بیس دستخط کے ملان، ہیورسٹک کوڈ ساخت کے تجزیے اور حقیقی وقت کی رویے کی نگرانی کے ذریعے میل ویئر کی شناخت کرتا ہے۔

Q2: سگنیچر پر مبنی شناخت کیا ہے؟

یہ اسکیننگ کا طریقہ ہے جو کرپٹوگرافک فائل ہیشز کو معلوم میل ویئر خطرات کی ڈیٹا بیس فہرستوں سے ملاتا ہے۔

Q3: ہیورسٹک اسکینر کیا ہے؟

ہیورسٹکس فائل کی ساخت اور کوڈ ہدایات کا تجزیہ کرتی ہیں اور میل ویئر ویریئنٹس میں عام مشتبہ پیٹرنز کو نشان زد کرتی ہیں۔

Q4: جب کوئی فائل قرنطینہ میں چلی جائے تو اس کا کیا مطلب ہے؟

اینٹی وائرس فائل کو ایک محفوظ، الگ تھلگ فولڈر میں منتقل کر دیتا ہے اور آپریٹنگ سسٹم کے تحفظ کے لیے اس کا چلنا روک دیتا ہے۔

Q5: اینٹی وائرس فالس پازیٹیو کیا ہے؟

یہ ایک خرابی ہے جس میں جائز، محفوظ سافٹ ویئر کو اسکیننگ الگورتھمز غلطی سے میل ویئر کے طور پر نشان زد کر دیتے ہیں۔

چیک پوائنٹ 10: سائبر سیکیورٹی عمومی سوالات – بنیادی (حصہ B)

آن لائن خطرات کی روک تھام کے بارے میں عام سوالات اور جوابات کا جائزہ لیں۔

Q6: رویے کی نگرانی سسٹمز کا تحفظ کیسے کرتی ہے؟

یہ چلتے ہوئے سافٹ ویئر کی حقیقی وقت میں نگرانی کرتا ہے، اور کوڈ داخل کرنے جیسی مشتبہ تبدیلیوں کی کوشش کرنے والے پروسیسز کو بلاک کرتا ہے۔

Q7: سینڈ باکس ٹیسٹنگ اہم کیوں ہے؟

سینڈ باکسنگ غیر معتبر فائلوں کو الگ تھلگ ورچوئل مشین میں چلاتی ہے اور سسٹم کو خطرے میں ڈالے بغیر کارروائیوں کا محفوظ مشاہدہ کرتی ہے۔

Q8: اینٹی وائرس ڈیفی نیشنز کتنی بار اپ ڈیٹ ہونی چاہئیں؟

نئے دریافت شدہ میل ویئر اقسام کی شناخت کے لیے اسکینرز کو روزانہ یا ہر گھنٹے ڈیفینیشنز اپ ڈیٹ کرنی چاہئیں۔

Q9: اینٹی وائرس اور EDR میں کیا فرق ہے؟

اینٹی وائرس فائل اسکیننگ پر توجہ دیتا ہے، جبکہ اینڈ پوائنٹ ڈیٹیکشن اینڈ رسپانس (EDR) پورے نیٹ ورک میں خطرات کی نگرانی اور ان پر قابو فراہم کرتا ہے۔

Q10: کیا میں دو اینٹی وائرس پروگرام ایک ساتھ چلا سکتا ہوں؟

نہیں۔ دو فعال اسکینرز چلانے سے سسٹم میں تصادم ہوتا ہے، کارکردگی سست ہوتی ہے، اور وہ ایک دوسرے کے آپریشنز کو بلاک کر سکتے ہیں۔

چیک پوائنٹ 10: سیکیورٹی عمومی سوالات – اعلیٰ (حصہ C)

سیکیورٹی فریم ورکس، میل ویئر تجزیے اور ڈیٹا کمپلائنس کے جدید تکنیکی پہلوؤں کا جائزہ لیں۔

Q1: ہیورسٹک قواعد خطرے کے بائی پاس کو کیسے کم کرتے ہیں؟

ہیورسٹکس مخصوص دستخطوں کے بجائے عمومی خطرے کے پیٹرنز کا تجزیہ کرتی ہیں، اور معلوم میل ویئر خاندانوں کے تبدیل شدہ ویریئنٹس پکڑ لیتی ہیں۔

Q2: پولی مارفک وائرس کیا ہے؟

یہ میل ویئر ہے جو ہر بار چلنے پر اپنی فائل ساخت اور ڈی کرپشن روٹین تبدیل کر لیتا ہے، جس سے دستخطی اسکینز غیر مؤثر ہو جاتے ہیں۔

Q3: سینڈ باکسز VM سے بچنے کی کوششوں کا پتا کیسے لگاتے ہیں؟

جدید سینڈ باکسز ماؤس کلکس اور سسٹم اپ ٹائم کی نقل کرتے ہیں، جس سے وہ میل ویئر دھوکا کھاتا ہے جو ورچوئل مشینوں میں چلنے پر چھپنے کے لیے بنایا گیا ہو۔

Q4: سگنیچر اپ ڈیٹ ڈاؤن لوڈ کے فارمیٹس کیا ہیں؟

اپ ڈیٹس عموماً ہلکی انکریمنٹل بائنری ڈف فائلیں ہوتی ہیں، جو کلائنٹ کے نیٹ ورک بینڈوتھ کے استعمال کو کم کرتی ہیں۔

Q5: اینڈ پوائنٹ ایجنٹس مقامی اسکینز کو کیسے سنبھالتے ہیں؟

ایجنٹس ہلکے پھلکے پس منظر کی جانچیں کرتے ہیں اور گہری کرپٹوگرافک ہیش تلاش کو کلاؤڈ تھریٹ ڈیٹا بیسز کے حوالے کر دیتے ہیں۔

چیک پوائنٹ 10: سیکیورٹی عمومی سوالات – اعلیٰ (حصہ D)

سیکیورٹی فریم ورکس، میل ویئر تجزیے اور ڈیٹا کمپلائنس کے جدید تکنیکی پہلوؤں کا جائزہ لیں۔

Q6: روٹ کٹ کی شناخت کی اسکیننگ کیا ہے؟

یہ کرنل سطح کے میموری ٹیبلز کو اسکین کرتا ہے، اور ان OS APIs کو بائی پاس کرتا ہے جنہیں روٹ کٹس اپنے فعال تھریڈز چھپانے کے لیے ہُک کرتے ہیں۔

Q7: روبے کی اسکیننگ رینسم ویئر کو کیسے بلاک کرتی ہے؟

یہ خودکار بڑے پیمانے پر فائل خفیہ کاری کے لوپس کا پتا لگاتا ہے اور سسٹم ڈیٹا بیسز لاک ہونے سے پہلے ہوسٹ پروسیس ختم کر دیتا ہے۔

Q8: کوڈ سائننگ سرٹیفکیٹ کی تصدیق کیا ہے؟

اسکینرز کوڈ کے ڈیجیٹل دستخطوں کو قابلِ اعتماد روٹ سرٹیفکیٹ اتھارٹیز کے مقابل جانچتے ہیں اور سافٹ ویئر ڈیولپر کی شناخت کی توثیق کرتے ہیں۔

Q9: پیکرز اسکیننگ انجنوں پر کیسے اثر ڈالتے ہیں؟

پیکرز میلویئر پے لوڈز کو کمپریس یا انکرپٹ کرتے ہیں۔ سگنیچر میچ چلنے سے پہلے اسکینرز کو فائل کو میموری میں ان پیک کرنا پڑتا ہے۔

Q10: EDR ٹولز تنہائی کو خودکار کیسے بناتے ہیں؟

EDR ایجنٹس سمجھوتا شدہ اینڈ پوائنٹس کو نیٹ ورک سطح پر قرنطینہ کر دیتے ہیں، پہلو بہ پہلو نقل و حرکت کو روکتے ہیں اور تجزیہ کار کو رسائی دیتے ہیں۔

حصہ 11: 10 حقیقی دنیا کے سائبر سیکیورٹی حقائق اور بصیرتیں

سیکیورٹی خلاف ورزیوں، دفاعی نظاموں اور تعمیل کے معیارات کے بارے میں حقیقی دنیا کے حقائق کا جائزہ لیں۔

1. سیکیورٹی بصیرت

سگنیچر ڈیٹا بیسز معلوم میل ویئر کے ہیشز محفوظ کرتے ہیں، اس لیے بالکل نئی یا تبدیل شدہ فائلیں ڈیفنیشنز اپ ڈیٹ ہونے تک نظر سے رہ جاتی ہیں۔

2. سیکیورٹی بصیرت

ہیورسٹک انجن دستخط موجود ہونے سے پہلے بعض نئے میل ویئر ویریئنٹس کو نشان زد کر سکتے ہیں، البتہ اس کی قیمت زیادہ غلط الارمز ہے۔

3. سیکیورٹی بصیرت

غلط مثبت الرٹس IT ٹیموں کا وقت ضائع کرتے ہیں جو غلطی سے قرنطینہ کی گئی فائلوں کی تصدیق اور بحالی میں لگتا ہے۔

4. سیکیورٹی بصیرت

پولی مارفک میلویئر ہر کاپی کے ساتھ اپنا کوڈ بدل لیتا ہے، اس لیے دفاع کرنے والے سگنیچرز کے ساتھ ہیورسٹک اور رویے کی جانچ بھی استعمال کرتے ہیں۔

5. سیکیورٹی بصیرت

کلاؤڈ پر مبنی اینٹی وائرس انجن مشتبہ فائلوں کے ہیشز کو بڑے آن لائن خطرات کے ڈیٹا بیسز سے تقریباً ریئل ٹائم میں ملاتے ہیں۔

6. سیکیورٹی بصیرت

میل ویئر مصنفین حسبِ ضرورت کوڈ لکھتے ہیں جو سینڈ باکس ماحول کو جانچتے ہیں اور ٹائمرز سے بچنے کے لیے عمل درآمد میں تاخیر کرتے ہیں۔

7. سیکیورٹی کی بصیرت

ونڈرز اینڈ پوائنٹس کو باقاعدگی سے ڈیفینیشن اپ ڈیٹس بھیجتے ہیں تاکہ اسکینرز نئے تصدیق شدہ خطرات کو پہچان سکیں۔

8. سیکیورٹی کی بصیرت

رینسم ویئر کے رویے کے مانیٹرز فائل خفیہ کاری اور شیڈو کاپی مٹانے سے منسلک مخصوص Win32 API کالز کو ہدف بناتے ہیں۔

9. سیکیورٹی کی بصیرت

درست کوڈ دستخط غلط مثبت کا خطرہ کم کر سکتے ہیں، لیکن دستخط شدہ فائلیں پھر بھی اسکین کی جاتی ہیں، کیونکہ میل ویئر بھی دستخط شدہ ہو سکتا ہے۔

10. سیکیورٹی بصیرت

روٹ کٹس سسٹم کرنل کے ڈھانچوں میں ترمیم کرتے ہیں، جن کا پتا لگانے اور صفائی کے لیے بوٹ ٹائم کے مخصوص اسکینرز درکار ہوتے ہیں۔

تکنیکی حوالہ جات اور ماخذ

مطالعاتی گائیڈ اور انٹرایکٹو پہیلیاں عالمی NIST، OWASP اور ڈیٹا پرائیویسی کمپلائنس معیارات سے مرتب کی گئی ہیں۔ علمی اور صنعتی حوالہ جات

علمی اور صنعتی حوالہ جات

[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

جوابی کلید: چیک پوائنٹ 1 – کثیر انتخابی

1 سوال 1 — سگنیچرز — درست جواب: A

تدریسی نوٹ

دستخط پر مبنی اسکیننگ معلوم ڈیٹا بیس پیٹرن پر انحصار کرتی ہے، اس لیے نامعلوم یا تبدیل شدہ میل ویئر کی نشاندہی میں ناکام رہتی ہے۔ حوالہ: OWASP Secure Configuration۔

2 سوال 2 — ہیورسٹکس — درست جواب: A

تدریسی نوٹ

ہیورسٹکس کوڈ کی ساخت اور کمانڈز کا تجزیہ کرتی ہیں تاکہ نئے خطرے کی اقسام کی مشتبہ خصوصیات کی نشاندہی ہو سکے۔ حوالہ: Center for Internet Security (CIS)۔

3 سوال 3 — سینڈ باکسنگ — درست جواب: A

تدریسی نوٹ

سینڈ باکس مشتبہ فائلوں کو الگ تھلگ ورچوئل مشین میں چلاتا ہے تاکہ عمل درآمد کے رویے کو محفوظ طریقے سے دیکھا جا سکے۔ حوالہ: NIST Digital Identity۔

4 سوال 4 — رویے پر مبنی — درست جواب: A

تدریسی نوٹ

رویے کی اسکیننگ چلتے ہوئے پروگراموں کو ریئل ٹائم میں مانیٹر کرتی ہے تاکہ غیر مجاز سسٹم تبدیلیاں بلاک کی جا سکیں۔ حوالہ: Center for Internet Security (CIS)۔

5 سوال 5 — اپ ڈیٹس — درست جواب: A

تدریسی نوٹ

اسکینرز خطرات کے منظرنامے کے ساتھ ہم آہنگ رہنے کے لیے روزانہ بتدریج تعریفی اپ ڈیٹس ڈاؤن لوڈ کرتے ہیں۔ حوالہ: OWASP Secure Configuration۔

جوابی کلید: چیک پوائنٹ 2 – درست یا غلط

6 سوال 6 — سگنیچرز — درست جواب: درست

تدریسی نوٹ

درست جواب: درست دستخط پر مبنی ٹولز کرپٹوگرافک ہیشز کا حساب لگاتے ہیں اور انہیں معلوم خطرات کے ہیشز کے ڈیٹا بیس سے ملاتے ہیں۔ حوالہ: OWASP Secure Configuration۔

7 سوال 7 — ہیورسٹکس — درست جواب: درست

تدریسی نوٹ

درست جواب: درست ہیورسٹک انجن اصول پر مبنی ساخت چلاتے ہیں جو جائز، محفوظ فائلوں کو بھی مشتبہ قرار دے سکتی ہے۔ حوالہ: Center for Internet Security (CIS)۔

8 سوال 8 — سینڈ باکسنگ — درست جواب: غلط

تدریسی نوٹ

درست جواب: غلط سینڈ باکس کوڈ کو ورچوئل کنٹینر میں چلاتا ہے اور نیٹ ورک شیئرز تک رسائی کو سختی سے بلاک کرتا ہے۔ حوالہ: NIST Digital Identity۔

9 سوال 9 — رویے پر مبنی — درست جواب: درست

تدریسی نوٹ

درست جواب: درست ریئل ٹائم مانیٹرنگ ان چلتے ہوئے پروسیسز کی نشاندہی کرتی ہے جو غیر قانونی تحریر یا فائل لاکنگ کی کوشش کرتے ہیں۔ حوالہ: Center for Internet Security (CIS)۔

10 سوال 10 — درست جواب: غلط

تدریسی نوٹ

درست جواب: غلط۔ کوئی اینٹی وائرس ہر زیرو ڈے حملے کو نہیں روکتا؛ نامعلوم خطرات سگنیچرز اور ہیورسٹکس سے بچ سکتے ہیں۔

الفاظ کی کلید اور درجہ بندی کا معیار

استاد کی گریڈنگ روبرک: ہر درست ملان (کل 8 نمبر) اور سیاقی اصطلاح (کل 6 نمبر) کے لیے 1 نمبر دیں۔

چیک پوائنٹ 4: جوابی کلید – تصورات کا ملان

D 1. ہیش دستخط	G 2. کوڈ ہیورسٹکس	E 3. فائل سینڈ باکس	C 4. رویے کی اسکین
F 5. روزانہ اپ ڈیٹس	H 6. غلط مثبت	A 7. خطرے کی علیحدگی	B 8. اینٹی وائرس ٹول

چیک پوائنٹ 3: جوابی کلید – اہم اصطلاحات

1 سگنیچر	2 ہیورسٹکس	3 سینڈ باکس	4 رویے
5 اپ ڈیٹس	6 غلط		

چیک پوائنٹ 6 – متبادل سرگرمی: جوابی کلید – الفاظ کا ملان

1 D – رویہجانچ	2 H – اینٹیوائرس	3 E – اپڈیٹس	4 B – ہیورسٹکس
5 G – علیحدگی	6 A – ہیشسگنیچر	7 C – سینڈباکس	8 F – غلطالارم

اساتذہ کے لیے بحث کے نوٹس

اہم اصطلاحات:
یقینی بنائیں کہ طلبہ ہیش دستخط، کوڈ ہیورسٹکس اور فائل سینڈ باکس کو اپنے الفاظ میں سمجھا سکیں اور ہر ایک کی مثال دے سکیں۔

کیس اسٹڈیز:
طلبہ سے کہیں کہ اپنی سفارشات کو ورک شیٹ کے حقائق پر مبنی رکھیں، ذاتی رائے پر نہیں۔

ماخذ کی جانچ:
طلبہ سے کہیں کہ ورک شیٹ کے ماخذ میں کم از کم ایک دعوے کی تصدیق کریں، اور اس پر بات کریں کہ اعداد و شمار، قیمتیں اور قواعد وقت کے ساتھ کیوں بدل سکتے ہیں۔

پہیلیوں کی کلیدیں اور استاد کے نوٹس

الفاظ کی تلاش کا حل

ش	ک	ع	ن	پ	ب	ا	ر	ب	س	ک	ٹ	ے	ی	ڈ
ل	ل	ر	ت	غ	س	گ	و	و	ت	ش	ے	ع	ش	ح
پ	ج	ے	ے	ل	ی	ہ	ی	و	گ	گ	چ	ن	و	ش
غ	ئ	ی	ت	ط	ط	ب	ہ	ی	د	م	و	ی	س	ر
ل	ہ	ت	ئ	ا	د	ش	چ	چ	ا	ط	ئ	پ	ٹ	چ
ئ	ی	ا	ب	ل	ڈ	پ	ا	ن	ی	ع	و	ت	ی	ی
چ	و	ت	م	ا	ت	س	ن	ن	ن	ش	ت	ل	ڈ	ن
ٹ	ر	گ	و	ر	ع	ی	چ	ہ	ٹ	ت	ر	د	پ	گ
چ	س	غ	و	م	ل	ن	چ	ی	ی	ئ	ہ	ر	ا	س
ش	ٹ	ہ	ع	ے	ی	ڈ	ن	ل	و	م	و	ا	ا	ش
ع	ک	ی	چ	ب	ح	ب	ل	ح	ا	ت	ی	ڈ	ہ	ی
ر	س	چ	ک	ح	د	ا	ح	ئ	ئ	ہ	ا	س	ط	ہ
ئ	د	و	د	و	گ	ک	م	ے	ر	ک	گ	س	ہ	گ
ک	د	ب	ح	ہ	ی	س	ح	ب	س	ڈ	چ	غ	م	ا
ط	م	ح	چ	ح	ئ	گ	پ	ط	ل	ن	م	س	چ	ئ

کراس ورڈ کا حل

							غ							
			ی	گ	د	ح	ی	ل	ع					
								ط		ہ			ہ	
					س	ر	ئ	ا	و	ی	ٹ	ن	ی	ا
ا						و		ل		ش			و	
پ						ی		ا		س			ر	
ڈ						ہ		ر		گ			س	
ی						چ		م		ن			ٹ	
ٹ						ا				ی			ک	
س	ک	ا	ب	ڈ	ن	ی	س			چ			س	
					چ					ر				

افقی

2 افقی: علیحدگی مشتبہ فائلوں کو الگ تھلگ رکھنا تاکہ مقامی سسٹم خطرے سے دوچار نہ ہو (7 حروف)

5 افقی: اینٹیوائرس سافٹ ویئر سوٹ جو اینڈ پوائنٹس کو حملوں سے اسکین کر کے محفوظ بناتا ہے (10 حروف)

8 افقی: سینڈباکس محفوظ ورچوئل آزمائشی ماحول جس میں غیر معتبر کوڈ بحفاظت چلایا جاتا ہے (8 حروف)

عمودی

1 عمودی: غلطالارم ایسا سیکیورٹی الرٹ جو محفوظ سافٹ ویئر کو غلطی سے میل ویئر قرار دے دے (8 حروف)

3 عمودی: بیورسٹکس اصولوں پر مبنی تجزیہ جو مشتبہ کوڈ ساخت والی فائلوں کی نشاندہی کرتا ہے (8 حروف)

4 عمودی: بیشسگنیچر منفرد کرپٹوگرافک ڈیٹا بیس نشان جو معلوم خطرات کی شناخت کے لیے استعمال ہوتا ہے (9 حروف)

6 عمودی: رویہجانچ چلتے ہوئے سافٹ ویئر کی کارروائیوں پر نظر رکھنا تاکہ بدنیتی پر مبنی عمل کے نمونے ملیں (8 حروف)

7 عمودی: اپڈیٹس باقاعدگی سے ڈاؤن لوڈ ہونے والی تعریفیں جو خطرات کے ڈیٹا بیس کو تازہ رکھتی ہیں (6 حروف)

الفاظ کی ترتیب اور سائفر حل کی کلید

الفاظ کی ترتیب درست کرنے کی سرگرمی اور Secret Cipher Challenge کی گریڈنگ کلید۔

الفاظ کی ترتیب درست کرنے کی کلید

1. نگسیہیچرش — ہیشسگنیچر
2. ڈسسیکابن — سینڈباکس
3. اڈیسٹپ — اپڈیٹس
4. یلدحگعی — علیحدگی
5. سٹیسرہکو — ہیورسٹکس
6. نچہارجوی — رویہجانچ
7. غملارلاط — غلطالارم
8. رٹوساییائن — اینٹیوائرس

خفیہ سائفر چیلنج کی کلید

"ہیورسٹک تجزیے سے نئے خطرات پہچانیں"

کیس اسٹڈیز کی جوابی کلید

A کیس اسٹڈی 1: دستخط پر مبنی اور ہیورسٹک اسکین کا موازنہ

استاد کا حل

گریڈنگ کی ہدایت

طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:

- منظرنامے کا تجزیہ: ایک ملازم دوسری ٹیم کی اندرونی طور پر بنائی گئی حسبِ ضرورت یوٹیلیٹی ڈاؤن لوڈ کرتا ہے۔ سگنیچر اسکینر اسے پاس کر دیتا ہے، لیکن ہیورسٹک اسکینر اسے مشکوک نشان زد کرتا ہے۔
- تجویز کردہ حکمت عملی اور حل: ایسا کیوں ہوا: سگنیچر اسکیننگ فائل ہیشز کی جانچ کرتی ہے؛ چونکہ یہ حسبِ ضرورت بنی ہے، یہ تھریٹ ڈیٹا بیس میں موجود نہیں ہے۔ ہیورسٹکس ساخت کا تجزیہ کرتے ہیں اور مشکوک کارروائیوں (مثلاً رجسٹری میں تحریر) کو نشان زد کرتے ہیں۔ تصدیق: کارروائیاں دیکھنے کے لیے فائل کو سینڈ باکس میں چلائیں، ڈیجیٹل دستخط جانچیں، اور ہیش کو تھریٹ انٹیلی جنس پورٹلز پر جمع کرائیں۔

B کیس اسٹڈی 2: غلط مثبت نتائج سے نمٹنا

استاد کا حل

گریڈنگ کی ہدایت

طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:

- منظرنامے کا تجزیہ: ایک سافٹ ویئر ڈیولپر اپنی ایپلیکیشن کمپائل کرتا ہے۔ سسٹم اینٹی وائرس نئے ایگزیکیوٹیبل کو میل ویئر قرار دے کر قرنطینہ میں ڈال دیتا ہے۔
- تجویز کردہ حکمت عملی اور حل: وائٹ لسٹنگ کے خطرات: اسکینرز کو بائی پاس کرنے سے حقیقی، متاثرہ کوڈ چلنے کا امکان پیدا ہو سکتا ہے۔ حل کا راستہ: فائل تجزیے کے لیے اینٹی وائرس وینڈر کو جمع کرائیں، سرٹیفکیٹ اتھارٹیز کے ذریعے کوڈ پر ڈیجیٹل دستخط کریں، اور اینٹی وائرس بند کرنے کے بجائے عارضی طور پر مخصوص فولڈر استثنائیں ترتیب دیں۔