নাম: _____ তারিখ: _____ নম্বর: _____

অ্যান্টিভাইরাস সফটওয়্যার ও এন্ডপয়েন্ট সুরক্ষা গাইড

সিগনেচর শনাক্তকরণ, হিউরিস্টিক্স, আচরণ পর্যবেক্ষণ, স্যান্ডবক্সিং, হালনাগাদ

অ্যান্টিভাইরাস সফটওয়্যার শিক্ষণ সংক্ষিপ্তসার

সুরক্ষিত
ডেটা এনক্রিপশন
256-বিট AES স্ট্যান্ডার্ড

সম্মতিপূর্ণ
বৈশ্বিক মান
GDPR ও CCPA কাঠামো

জিরো-ট্রাস্ট
অ্যাক্সেস নীতি
মাল্টি-ফ্যাক্টর অথেনটিকেশন

স্বাগতম! এই অ্যাক্টিভিটি প্যাকেট আপনাকে অ্যান্টিভাইরাস সফটওয়্যার ও এন্ডপয়েন্ট সুরক্ষা বিষয়ে গাইড করবে। আপনি সিগনেচার ডেটাবেস, হিউরিস্টিক স্ক্যানার, আচরণ পর্যবেক্ষণ, স্যান্ডবক্স ভার্চুয়াল ফাইল এবং ফলস পজিটিভ প্রশমন সম্পর্কে জানবেন।

ওয়ার্কশিট চেকপয়েন্ট

- [ ] অংশ 1-4: সাইবার নিরাপত্তা ও হুমকি প্রতিরোধে দক্ষতা অর্জন করুন।
- [ ] অংশ 5-7: ক্রসওয়ার্ড ও ওয়ার্ড সার্চ ধাঁধা সমাধান করুন।
- [ ] অংশ 8-9: কেস স্টাডি ও সংকেতবার্তা চ্যালেঞ্জ সমাধান করুন।
- [ ] অংশ 10: প্রাথমিক ও উন্নত স্তরের FAQ পেজ পর্যালোচনা করুন।
- [ ] অংশ 11: 10টি আকর্ষণীয় বাস্তব তথ্য অন্বেষণ করুন।
- [ ] অতিরিক্ত: দ্রুত ভাবুন চ্যালেঞ্জ।

VPN.com সাইবার নিরাপত্তা গাইড খুলুন

URL: https://www.vpn.com/bn/saibar-nirapotta/antivirus/

আপনার অ্যান্টিভাইরাস কৌশল শেখার রোডম্যাপ

- সিগনেচার-ভিত্তিক ও হিউরিস্টিক-ভিত্তিক ম্যালওয়্যার শনাক্তকরণের মধ্যে পার্থক্য করুন।
- আচরণ পর্যবেক্ষণ এবং স্যান্ডবক্স বিচ্ছিন্নকরণ প্রোটোকল বুঝুন।
- সিস্টেম পারফরম্যান্স ও এন্ডপয়েন্টে রিয়েল-টাইম স্ক্যানের প্রভাব মূল্যায়ন করুন।
- ডিজিটাল সার্টিফিকেট যাচাই ব্যবহার করে ভুল-পজিটিভ শ্রেণিবিন্যাস প্রশমিত করুন।
- কর্পোরেট এন্ডপয়েন্টজুড়ে দৈনিক ডেফিনিশন আপডেট বিতরণ পরিচালনা করুন।

অ্যান্টিভাইরাস নির্দেশিকা

বহুনির্বাচনী ও সত্য/মিথ্যা প্রশ্নের উত্তর দিন, শব্দভাণ্ডার ব্যবহার করে শূন্যস্থান পূরণ করুন, সংজ্ঞা মেলান এবং ক্রসওয়ার্ড ও শব্দ খোঁজার ধাঁধা সমাধান করুন। এন্ডপয়েন্ট অ্যান্টিভাইরাস নিরাপত্তা বিষয়ে আপনার জ্ঞান প্রয়োগ করুন। শেষে অতিরিক্ত কার্যক্রম দ্রুত ভাবুন সম্পন্ন করুন।

অ্যান্টিভাইরাস সুরক্ষা ও সিগনেচার স্ক্যানিং (ভূমিকা)

অ্যান্টিভাইরাস সফটওয়্যার ম্যালওয়্যার শনাক্ত, কোয়ারেন্টাইন ও অপসারণ করে এন্ডপয়েন্টকে সুরক্ষিত রাখে। আধুনিক সিস্টেম জিরো-ডে এক্সপ্লয়েট শনাক্ত করতে সিগনেচার ডেটাবেস (পরিচিত হুমকির হ্যাশ মেলানো), হিউরিস্টিক (ফাইলের কাঠামো বিশ্লেষণ) এবং আচরণ পর্যবেক্ষণ একসঙ্গে ব্যবহার করে।

প্রতিটি চেকপয়েন্ট মনোযোগ দিয়ে পড়ুন এবং বেছে নিন বা লিখুন সঠিক

চেকপয়েন্ট 1: বহুনির্বাচনী চ্যালেঞ্জ

1 1. সিগনেচার-ভিত্তিক শনাক্তকরণের একটি সীমাবদ্ধতা কী?

- A. এটি অজানা বা পরিবর্তিত ম্যালওয়্যার শনাক্ত করতে পারে না
- B. এটি উচ্চহারে ফলস পজিটিভ তৈরি করে
- C. এর জন্য উচ্চ CPU প্রসেসিং ক্ষমতা লাগে
- D. এটি শুধু ইন্টারনেটে সংযুক্ত থাকলেই কাজ করে

2 2. হিউরিস্টিক স্ক্যানার কীভাবে নতুন ম্যালওয়্যার ভ্যারিয়েন্ট শনাক্ত করে?

- A. সন্দেহজনক প্যাটার্ন ও কোড কাঠামো শনাক্ত করে
- B. ফাইল হ্যাশকে হুমকির ডেটাবেসের সঙ্গে মিলিয়ে
- C. সব স্বাক্ষরহীন এক্সিকিউটেবল স্বয়ংক্রিয়ভাবে মুছে ফেলে
- D. প্রতিটি ফাইল একটি পাবলিক ক্লাউড ফোল্ডারে আপলোড করে

3 3. অ্যান্টিভাইরাস স্যান্ডবক্স এক্সিকিউশনের উদ্দেশ্য কী?

- A. নিরাপদ ভার্চুয়াল ভল্টে ফাইল বিচ্ছিন্ন করে বিশ্লেষণ করা
- B. স্থানীয় ফাইল সিস্টেম ব্যাকআপ স্থানান্তরের গতি বাড়ানো
- C. স্থানীয় অপারেটিং সিস্টেমের নিরাপত্তা প্যাচ হালনাগাদ করা
- D. সংরক্ষণ স্থান বাঁচাতে বড় নথি ফাইল সংকুচিত করা

4 4. কোন শনাক্তকরণ পদ্ধতি রিয়েল টাইমে হুমকির আচরণ চিহ্নিত করে?

- A. সফটওয়্যারের কার্যকলাপ পর্যবেক্ষণ করা আচরণগত বিশ্লেষণ
- B. রাতারাতি সম্পন্ন ঐতিহাসিক লগ পরিদর্শন
- C. ধীর অ্যাপের কথা জানাতে ব্যবহারকারীর ম্যানুয়াল হস্তক্ষেপ
- D. ইনস্টল করা প্রোগ্রামের সাপ্তাহিক ম্যানুয়াল পর্যালোচনা

5 5. স্ক্যানারের জন্য নিয়মিত ডেফিনিশন আপডেট কেন গুরুত্বপূর্ণ?

- A. সিগনেচার ইঞ্জিনের ডেটাবেসে হুমকি শনাক্তকারী সরবরাহ করতে
- B. কার্যক্রমের সময় CPU ক্লক স্পিড বাড়াতে
- C. বৈশ্বিক DNS নেমসার্ভার ক্যাশিংয়ের সময় বদলাতে
- D. ওয়েব ব্রাউজারের কুকি সেটিংস অনুমোদন করতে

চেকপয়েন্ট 2: সত্য বা মিথ্যা চ্যালেঞ্জ

6 প্রশ্ন tf 6

6. সিগনেচর শনাক্তকরণ ক্রিপ্টোগ্রাফিক ফাইল হ্যাশকে ডেটাবেস তালিকার সঙ্গে মেলায়।

○ সত্য ○ মিথ্যা

7 প্রশ্ন tf 7

7. হিউরিস্টিক স্ক্যানার নিরাপদ ফাইলে ভুল পজিটিভ সতর্কতা দিতে পারে।

○ সত্য ○ মিথ্যা

8 প্রশ্ন tf 8

8. স্যান্ডবক্স ম্যালওয়্যারকে সীমাহীনভাবে নেটওয়ার্ক ফাইলে প্রবেশ করতে দেয়।

○ সত্য ○ মিথ্যা

9 প্রশ্ন tf 9

9. আচরণগত স্ক্যানিং ক্ষতিকর কাজ করলে ফাইল ব্লক করে।

○ সত্য ○ মিথ্যা

10 প্রশ্ন tf 10

10. স্ট্যান্ডার্ড অ্যান্টিভাইরাস সফটওয়্যার সব জিরো-ডে আক্রমণ সম্পূর্ণ ঠেকিয়ে দেয়।

○ সত্য ○ মিথ্যা

চেকপয়েন্ট 3: মূল পরিভাষা বসানো

নিচের প্রতিটি বাক্য পড়ুন এবং ওয়ার্ড ব্যাংক থেকে সঠিক শব্দ দিয়ে শূন্যস্থান পূরণ করুন।

1. একটি প্রচলিত স্ক্যানার পরিচিত ম্যালওয়্যার শনাক্ত করতে _____ মেলানোর ওপর নির্ভর করে।

2. ফাইলের কোডের ধরন বিশ্লেষণকে বলা হয় _____ স্ক্যানিং।

3. অ্যান্টিভাইরাস টুল সন্দেহজনক ফাইলকে একটি _____ পরিবেশে আলাদা করে রাখে।

4. রিয়েল-টাইম মনিটরিং সন্দেহজনক কার্যকলাপের জন্য প্রোগ্রামের _____ পর্যবেক্ষণ করে।

5. স্ক্যানার নতুন হুমকি চিনতে প্রতিদিন ডেটাবেসের _____ ডাউনলোড করে।

6. নিরাপদ প্রোগ্রামকে ম্যালওয়্যার হিসেবে চিহ্নিত করলে _____ তৈরি হয়।

পরিভাষা শব্দভাণ্ডার

আচরণ | আপডেট | ভাইরাস স্ক্যানার | ভুল সতর্কতা | সিগনেচার | স্যান্ডবক্স | হিউরিস্টিক | হুমকি বিচ্ছিন্নকরণ

এখানে আপনার উত্তর লিখুন:

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

চেকপয়েন্ট 4: নিরাপত্তা ধারণা মিলান

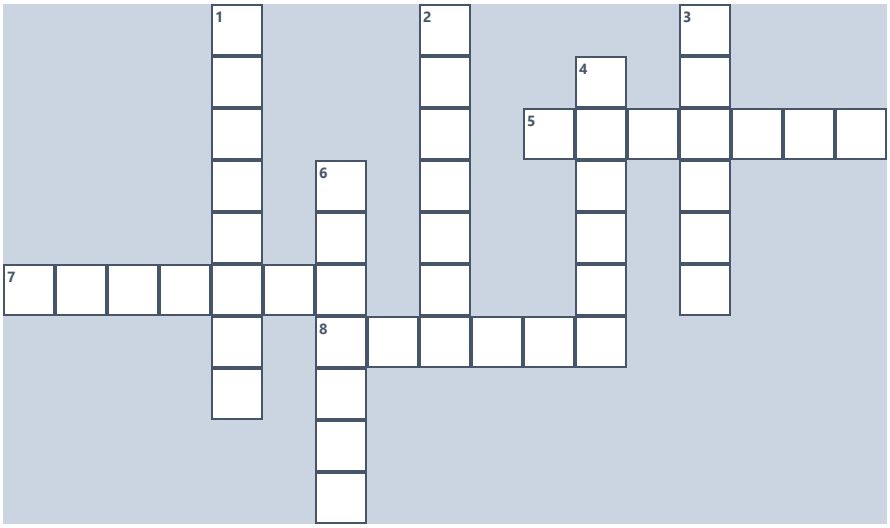
সংজ্ঞা মেলানো

পূরণযোগ্য ইনপুট বক্সে সংশ্লিষ্ট অক্ষর (A-H) লিখে বামদিকের প্রতিটি শব্দভাণ্ডার-পদকে ডানদিকের সঠিক সংজ্ঞার সঙ্গে মেলান।

☐	**1. হ্যাশ স্বাক্ষর**	**A**	স্থানীয় সিস্টেম ঝুঁকিতে পড়া ঠেকাতে সন্দেহজনক ফাইল আটকে রাখা।
☐	**2. কোড হিউরিস্টিক**	**B**	এক্সপ্লয়েট থেকে এন্ডপয়েন্ট স্ক্যান ও সুরক্ষা দেওয়া সফটওয়্যার স্যুট।
☐	**3. ফাইল স্যান্ডবক্স**	**C**	ক্ষতিকর কার্যপ্রণালীর ধরনের জন্য চলমান সফটওয়্যারের কার্যক্রম পর্যবেক্ষণ।
☐	**4. আচরণ স্ক্যান**	**D**	পরিচিত হুমকি শনাক্ত করতে ব্যবহৃত অনন্য ক্রিপ্টোগ্রাফিক ডেটাবেস ফুটপ্রিন্ট।
☐	**5. দৈনিক হালনাগাদ**	**E**	অবিশ্বস্ত কোড নিরাপদে চালানোর জন্য নিরাপদ ভার্চুয়াল পরীক্ষামূলক পরিবেশ।
☐	**6. ফলস পজিটিভ**	**F**	হুমকির ডেটাবেসকে তথ্য সরবরাহ করা নিয়মিত ডেফিনিশন ডাউনলোড।
☐	**7. হুমকি বিচ্ছিন্নকরণ**	**G**	সন্দেহজনক কোড বিন্যাসযুক্ত ফাইল চিহ্নিতকারী নিয়ম-ভিত্তিক বিশ্লেষণ।
☐	**8. অ্যান্টিভাইরাস টুল**	**H**	নিরাপদ সফটওয়্যারকে ভুলভাবে ম্যালওয়্যার হিসেবে শ্রেণিবদ্ধ করা নিরাপত্তা সতর্কতা।

চেকপয়েন্ট 5: ক্রসওয়ার্ড ধাঁধা

সক্রিয় সাদা ঘরে অক্ষর লিখে ক্রসওয়ার্ড পাজল সমাধান করুন। সংখ্যাগুলো নিচের সূত্রের সঙ্গে মেলে।



পাশাপাশি

5. এন্ডপয়েন্টকে এক্সপ্লয়েট থেকে স্ক্যান ও সুরক্ষা দেওয়া সফটওয়্যার স্যুট (7)

7. সন্দেহজনক কোড গঠনের ফাইল চিহ্নিতকারী নিয়মভিত্তিক বিশ্লেষণ (7)

8. ক্ষতিকর কার্যক্রমের ধরন খুঁজতে চলমান সফটওয়্যারের কাজ পর্যবেক্ষণ (6)

উপর-নিচ

1. অবিশ্বস্ত কোড নিরাপদে চালানোর সুরক্ষিত ভার্চুয়াল পরীক্ষার পরিবেশ (8)

2. পরিচিত হুমকি শনাক্তে ব্যবহৃত ডেটাবেসের অনন্য ক্রিপ্টোগ্রাফিক ছাপ (7)

3. নিরাপদ সফটওয়্যারকে ভুলভাবে ম্যালওয়্যার হিসেবে চিহ্নিত করা নিরাপত্তা সতর্কতা (6)

4. স্থানীয় সিস্টেমের ঝুঁকি এড়াতে সন্দেহজনক ফাইল আটকে রাখা (6)

6. হুমকির ডেটাবেসে তথ্য জোগানো নিয়মিত ডেফিনিশন ডাউনলোড (7)

চেকপয়েন্ট 5, বিকল্প: সহজবোধ্য ক্রসওয়ার্ড সূত্র

স্ক্রিন-রিডার ও কিবোর্ড ব্যবহারকারীরা নিচের টেক্সট ফিল্ডে সরাসরি ক্রসওয়ার্ডের উত্তর লিখতে পারেন। আড়াআড়ি সূত্র ওপর-নিচ সূত্র

পাশাপাশি

5 পাশাপাশি: এন্ডপয়েন্টকে এক্সপ্লয়েট থেকে স্ক্যান ও সুরক্ষা দেওয়া সফটওয়্যার স্যুট (7 অক্ষর):

7 পাশাপাশি: সন্দেহজনক কোড গঠনের ফাইল চিহ্নিতকারী নিয়মভিত্তিক বিশ্লেষণ (7 অক্ষর):

8 পাশাপাশি: ক্ষতিকর কার্যক্রমের ধরন খুঁজতে চলমান সফটওয়্যারের কাজ পর্যবেক্ষণ (6 অক্ষর):

উপর-নিচ

1 উপর-নিচ: অবিশ্বস্ত কোড নিরাপদে চালানোর সুরক্ষিত ভার্চুয়াল পরীক্ষার পরিবেশ (8 অক্ষর):

2 উপর-নিচ: পরিচিত হুমকি শনাক্তে ব্যবহৃত ডেটাবেসের অনন্য ক্রিপ্টোগ্রাফিক ছাপ (7 অক্ষর):

3 উপর-নিচ: নিরাপদ সফটওয়্যারকে ভুলভাবে ম্যালওয়্যার হিসেবে চিহ্নিত করা নিরাপত্তা সতর্কতা (6 অক্ষর):

4 উপর-নিচ: স্থানীয় সিস্টেমের ঝুঁকি এড়াতে সন্দেহজনক ফাইল আটকে রাখা (6 অক্ষর):

6 উপর-নিচ: হুমকির ডেটাবেসে তথ্য জোগানো নিয়মিত ডেফিনিশন ডাউনলোড (7 অক্ষর):

চেকপয়েন্ট 6: লুকানো শব্দ খোঁজা

নিচের গ্রিডে লুকানো ৪টি মূল শব্দভাণ্ডারের শব্দ খুঁজুন। শব্দগুলো অনুভূমিক, উল্লম্ব বা কোণাকুণি হতে পারে।

ক সি ন দ ঠ হ সা শ মে দে রা কি ঋ তে না
নে ছ স্ক্যা য প উ অ উ দৈ ঋ মা বা য ফ বা
ম দে ণ তি ভ ঘ রে ষ ফ নি ঘ দ হ স ভ
রি মি র না স্ক্যা স রা ই ভা ঢ ক ষ ষ রি সি
না তি চ তা ড স্যা ঊ নি তা রা কি আ থ সে ঊ
ক লি আ গ নি ন্ড জা হ্যা পি র্ক ঋ জি প লি ট
স্টি ভ ণ জে গ ব স ঘ শ রে ত দি মি ডে ঋ
রি পা উ অ জে ক্স কা গ ম সি আ স ঘ কি ট
উ ঘ ঝ ণ ধ প গ সি রি শ গ ছ ল দ সে
হি জি নি ঝ রে রি আ পে জ আ আ নে রে ভু মা
ড স মে তি দে বে ই রি ফ সি তি সে চা খ স
কো বে উ ট সে শ সো দি দা প আ সি জে র বি
বি য ড দ ষ সা লে ফ ল ল তা কে ণ রা রি
ণ জে ই কে পে ঠ শ পি ঊ বে সে বে উ ণ ল
জে ঢ ফ কি মে কা ন দা ঋ ল জে বে ঠ বি কে

পরিভাষা শব্দতালিকা

হ্যাশসিগনেচার কোডহিউরিস্টিক স্যান্ডবক্সপরিবেশ আচরণস্ক্যান দৈনিকআপডেট ভুলসতর্কতা আইসোলেশন ভাইরাসস্ক্যানার

চেকপয়েন্ট 6, বিকল্প: সহজবোধ্য শব্দভাণ্ডার মিলান

ফাঁকা জায়গায় অক্ষর (A-H) লিখে ওয়ার্ড সার্চের ৪টি শব্দভাণ্ডার-পদের প্রতিটিকে তার সঠিক সংজ্ঞার সঙ্গে মেলান।

পরিভাষা

A. হ্যাশসিগনেচার

B. কোডহিউরিস্টিক

C. স্যান্ডবক্সপরিবেশ

D. আচরণস্ক্যান

E. দৈনিকআপডেট

F. ভুলসতর্কতা

G. আইসোলেশন

H. ভাইরাসস্ক্যানার

সংজ্ঞা ও মিলের ঘর

1. ক্ষতিকর কার্যক্রমের ধরন খুঁজতে চলমান সফটওয়্যারের কাজ পর্যবেক্ষণ।

2. এন্ডপয়েন্টকে এক্সপ্লয়েট থেকে স্ক্যান ও সুরক্ষা দেওয়া সফটওয়্যার স্যুট।

3. হুমকির ডেটাবেসে তথ্য জোগানো নিয়মিত ডেফিনিশন ডাউনলোড।

4. সন্দেহজনক কোড গঠনের ফাইল চিহ্নিতকারী নিয়মভিত্তিক বিশ্লেষণ।

5. স্থানীয় সিস্টেমের ঝুঁকি এড়াতে সন্দেহজনক ফাইল আটকে রাখা।

6. পরিচিত হুমকি শনাক্তে ব্যবহৃত ডেটাবেসের অনন্য ক্রিপ্টোগ্রাফিক ছাপ।

7. অবিশ্বস্ত কোড নিরাপদে চালানোর সুরক্ষিত ভার্চুয়াল পরীক্ষার পরিবেশ।

8. নিরাপদ সফটওয়্যারকে ভুলভাবে ম্যালওয়্যার হিসেবে চিহ্নিত করা নিরাপত্তা সতর্কতা।

চেকপয়েন্ট 7: এলোমেলো শব্দ চ্যালেঞ্জ

সাইবার নিরাপত্তার মূল ধারণা ও পরিভাষা জানতে নিচের অক্ষরগুলো সাজান। উত্তর দেওয়া ইনপুট বাক্সে লিখুন।

1. গচাহ্যানেরসিশ
2. ক্সস্যাশন্ডবেরিপব
3. আদৈপটকডেনি
4. নলেসোশআই
5. রিকউহিকোস্টিড
6. স্ক্যাণআরনচ
7. র্কভুততাসল
8. ইসরভানাস্ক্যারা

অতিরিক্ত কার্যক্রম: দ্রুত ভাবুন

প্রতিটি বিভাগে ৩টি উত্তর। যে প্রথমে তালিকা পূরণ করবে, সে জিতবে।

1	সফটওয়্যার আপডেট করার কারণ			
2	IT সাহায্যের জন্য আপনি যাদের জিজ্ঞাসা করতে পারেন			
3	অ্যান্টিভাইরাস কিছু খুঁজে পেলে যা করবেন			
4	কম্পিউটার ভাইরাসের লক্ষণ			
5	যেসব জিনিস কোয়ারেন্টাইনে যায়			
6	যেসব জায়গায় ভাইরাস লুকিয়ে থাকে			
7	যে তথ্য আপনার কখনো শেয়ার করা উচিত নয়			
8	ক্ষতিকর সফটওয়্যারের ধরন			
9	আপনার জানা নিরাপত্তা টুল			
10	একটি অ্যান্টিভাইরাস যা যা স্ক্যান করে			
11	যা যা আপনি ব্যাকআপ করেন			
12	যেসব ডিভাইস হ্যাক হতে পারে			
13	আপনার জানা অ্যান্টিভাইরাস প্রোগ্রাম			
14	ভুল সতর্কতার কারণ			
15	যেসব নিরাপদ অভ্যাস আপনি আজই শুরু করতে পারেন			

চেকপয়েন্ট ৪: সাইবার নিরাপত্তা কেস স্টাডি

নিচের বাস্তব পরিস্থিতিগুলো সমাধান করতে শেখা ধারণাগুলো প্রয়োগ করুন।

কেস স্টাডি 1: সিগনেচার বনাম হিউরিস্টিক স্ক্যান

👷

পরিস্থিতি: একজন কর্মী অন্য একটি দলের অভ্যন্তরীণভাবে তৈরি একটি কাস্টম ইউটিলিটি ডাউনলোড করেন। সিগনেচার স্ক্যানার এটিকে পাস করিয়ে দেয়, কিন্তু হিউরিস্টিক স্ক্যানার এটিকে সন্দেহজনক হিসেবে চিহ্নিত করে।

আলোচনার প্রশ্ন: ব্যাখ্যা করুন কেন এমন হলো এবং ফাইলটি নিরাপদ কিনা তা কীভাবে যাচাই করবেন।

কেস স্টাডি 2: ভুল ইতিবাচক ফলাফল সামলানো

👷

পরিস্থিতি: একজন সফটওয়্যার ডেভেলপার তাঁর অ্যাপ্লিকেশন কম্পাইল করেন। সিস্টেমের অ্যান্টিভাইরাস নতুন এক্সিকিউটেবলটিকে ম্যালওয়্যার হিসেবে চিহ্নিত করে কোয়ারেন্টাইন করে দেয়।

আলোচনার প্রশ্ন: হোয়াইটলিস্ট করার ঝুঁকিগুলো সংক্ষেপে বর্ণনা করুন এবং সঠিক সমাধানের পথটি ব্যাখ্যা করুন।

চেকপয়েন্ট 9: সংকেতবার্তা ডিকোড করুন

একজন সাইবার নিরাপত্তা পেশাজীবী অনলাইন হুমকিদাতাদের হাত থেকে নেটওয়ার্ক সম্পদ রক্ষা করেন। নিচের অক্ষর-থেকে-সংখ্যা কী ব্যবহার করে ফাঁকা ঘরে মিলে যাওয়া অক্ষর লিখে বার্তাটি ডিক্রিপ্ট করুন।

অক্ষর-থেকে-সংখ্যা এনক্রিপশন কী

অ=1 আ=2 ই=3 ঈ=4 উ=5 ঊ=6 ঋ=7 এ=8 ঐ=9 ও=10 ঔ=11 ক=12

খ=13 গ=14 ঘ=15 ঙ=16 চ=17 ছ=18 জ=19 ঝ=20 ঞ=21 ট=22 ঠ=23 ড=24

ঢ=25 ণ=26 ত=27 থ=28 দ=29 ধ=30 ন=31 প=32 ফ=33 ব=34 ভ=35 ম=36

য=37 র=38 ল=39 শ=40 ষ=41 স=42 হ=43 ৎ=44 া=45 ি=46 ী=47 ু=48

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

12	53	24		34	46	40	58	39	51	41	26	51		31	27	48	31

36	58	37	45	39	10	37	59	58	37	45	38		40	31	45	12	58	27

ডিকোড করা বার্তা:

পরামর্শ: প্রতিটি সংখ্যা বর্ণমালায় সেই অক্ষরের অবস্থান বোঝায় (যেমন 1 = অ, 2 = আ, 63 = ়)।

চেকপয়েন্ট 10: মৌলিক সাইবার নিরাপত্তা FAQ (অংশ A)

অনলাইন হুমকি প্রশমন নিয়ে প্রচলিত প্রশ্ন ও উত্তরগুলো দেখে নিন।

Q1: অ্যান্টিভাইরাস সফটওয়্যার কীভাবে ম্যালওয়্যার শনাক্ত করে?

এটি ডেটাবেস সিগনেচার মিলানো, হিউরিস্টিক কোড বিন্যাস বিশ্লেষণ এবং রিয়েল-টাইম আচরণ মনিটরিংয়ের মাধ্যমে ম্যালওয়্যার শনাক্ত করে।

Q2: সিগনেচারভিত্তিক শনাক্তকরণ কী?

এটি একটি স্ক্যানিং পদ্ধতি, যা ক্রিপ্টোগ্রাফিক ফাইল হ্যাশকে পরিচিত ম্যালওয়্যার হুমকির ডেটাবেস তালিকার সঙ্গে মিলিয়ে দেখে।

Q3: হিউরিস্টিক স্ক্যানার কী?

হিউরিস্টিক একটি ফাইলের গঠন ও কোড নির্দেশনা বিশ্লেষণ করে ম্যালওয়্যার ভ্যারিয়েন্টে সাধারণ সন্দেহজনক ধরন চিহ্নিত করে।

Q4: কোনো ফাইল কোয়ারেন্টাইন করা হলে এর অর্থ কী?

অ্যান্টিভাইরাস ফাইলটিকে একটি সুরক্ষিত, বিচ্ছিন্ন ফোল্ডারে সরিয়ে নেয় এবং অপারেটিং সিস্টেম রক্ষায় তা চালানো ব্লক করে।

Q5: অ্যান্টিভাইরাস ফলস পজিটিভ কী?

এটি এমন একটি ত্রুটি, যেখানে বৈধ ও নিরাপদ সফটওয়্যারকে স্ক্যানিং অ্যালগরিদম ভুলভাবে ম্যালওয়্যার হিসেবে চিহ্নিত করে।

চেকপয়েন্ট 10: মৌলিক সাইবার নিরাপত্তা FAQ (অংশ B)

অনলাইন হুমকি প্রশমন নিয়ে প্রচলিত প্রশ্ন ও উত্তরগুলো দেখে নিন।

Q6: আচরণ পর্যবেক্ষণ কীভাবে সিস্টেম সুরক্ষিত রাখে?

এটি চলমান সফটওয়্যার রিয়েল টাইমে পর্যবেক্ষণ করে এবং কোড ইনজেক্ট করার মতো সন্দেহজনক পরিবর্তনের চেষ্টা করা প্রক্রিয়া ব্লক করে।

Q7: স্যান্ডবক্স টেস্টিং কেন গুরুত্বপূর্ণ?

স্যান্ডবক্সিং অবিশ্বস্ত ফাইল বিচ্ছিন্ন ভার্চুয়াল মেশিনে চালায় এবং সিস্টেমকে ঝুঁকিতে না ফেলে কার্যকলাপ নিরাপদে পর্যবেক্ষণ করে।

Q8: অ্যান্টিভাইরাসের ডেফিনিশন কত ঘন ঘন আপডেট হওয়া উচিত?

নতুন আবিষ্কৃত ম্যালওয়্যারের ধরন শনাক্ত করতে স্ক্যানারের ডেফিনিশন প্রতিদিন বা প্রতি ঘণ্টায় হালনাগাদ করা উচিত।

Q9: অ্যান্টিভাইরাস ও EDR-এর মধ্যে পার্থক্য কী?

অ্যান্টিভাইরাস ফাইল স্ক্যানিংয়ে মনোযোগ দেয়, আর Endpoint Detection and Response (EDR) নেটওয়ার্ক জুড়ে হুমকি ট্র্যাকিং ও নিয়ন্ত্রণ প্রদান করে।

Q10: আমি কি একসঙ্গে দুটি অ্যান্টিভাইরাস প্রোগ্রাম চালাতে পারি?

না। দুটি সক্রিয় স্ক্যানার চালালে সিস্টেম সংঘাত হয়, পারফরম্যান্স কমে এবং একে অপরের কার্যক্রম ব্লক করতে পারে।

চেকপয়েন্ট 10: উন্নত নিরাপত্তা FAQ (অংশ C)

নিরাপত্তা কাঠামো, ম্যালওয়্যার বিশ্লেষণ ও ডেটা সম্মতির উন্নত প্রযুক্তিগত দিক অন্বেষণ করুন।

Q1: হিউরিস্টিক নিয়ম কীভাবে হুমকি এড়িয়ে যাওয়া কমায়?

হিউরিস্টিক নির্দিষ্ট সিগনেচারের পরিবর্তে সাধারণ হুমকির ধরন বিশ্লেষণ করে, ফলে পরিচিত ম্যালওয়্যার পরিবারের পরিবর্তিত ভ্যারিয়েন্ট ধরা পড়ে।

Q2: পলিমরফিক ভাইরাস কী?

এটি এমন ম্যালওয়্যার, যা প্রতিবার চালু হওয়ার সময় ফাইলের বিন্যাস ও ডিক্রিপশন রুটিন বদলে ফেলে, ফলে সিগনেচার স্ক্যান অকার্যকর হয়।

Q3: স্যান্ডবক্স কীভাবে VM ইভেশন শনাক্ত করে?

আধুনিক স্যান্ডবক্স মাউস ক্লিক ও সিস্টেম আপটাইম নকল করে, ফলে ভার্চুয়াল মেশিনে চলার সময় লুকিয়ে থাকার জন্য ডিজাইন করা ম্যালওয়্যারকে ধোঁকা দেওয়া যায়।

Q4: সিগনেচার আপডেট ডাউনলোডের ফরম্যাটগুলো কী কী?

আপডেট সাধারণত হালকা ইনক্রিমেন্টাল বাইনারি ডিফ ফাইল, যা ক্লায়েন্টের নেটওয়ার্ক ব্যান্ডউইথ খরচ কমায়।

Q5: এন্ডপয়েন্ট এজেন্ট কীভাবে স্থানীয় স্ক্যান পরিচালনা করে?

এজেন্টরা হালকা ব্যাকগ্রাউন্ড পরীক্ষা চালায় এবং গভীর ক্রিপ্টোগ্রাফিক হ্যাশ লুকআপ ক্লাউড হুমকি ডেটাবেসে ছেড়ে দেয়।

চেকপয়েন্ট 10: উন্নত নিরাপত্তা FAQ (অংশ D)

নিরাপত্তা কাঠামো, ম্যালওয়্যার বিশ্লেষণ ও ডেটা সম্মতির উন্নত প্রযুক্তিগত দিক অন্বেষণ করুন।

Q6: রুটকিট শনাক্তকরণ স্ক্যানিং কী?

এটি কার্নেল-স্তরের মেমরি টেবিল স্ক্যান করে এবং রুটকিটগুলোর সক্রিয় থ্রেড লুকাতে হুক করা OS API এড়িয়ে যায়।

Q7: আচরণ স্ক্যানিং কীভাবে র‍্যানসমওয়্যার ব্লক করে?

এটি স্বয়ংক্রিয় গণ ফাইল এনক্রিপশন লুপ শনাক্ত করে এবং সিস্টেম ডেটাবেস লক হওয়ার আগেই হোস্ট প্রসেস বন্ধ করে দেয়।

Q8: কোড-সাইনিং সার্টিফিকেট যাচাই কী?

স্ক্যানার বিশ্বস্ত রুট সার্টিফিকেট অথরিটির সঙ্গে কোডের ডিজিটাল সিগনেচার মিলিয়ে দেখে সফটওয়্যার ডেভেলপারের পরিচয় যাচাই করে।

Q9: প্যাকার স্ক্যানিং ইঞ্জিনকে কীভাবে প্রভাবিত করে?

প্যাকার ম্যালওয়্যারের পেলোড কম্প্রেস বা এনক্রিপ্ট করে। সিগনেচার মেলানোর আগে স্ক্যানারকে ফাইলটি মেমরিতে আনপ্যাক করতে হয়।

Q10: EDR টুল কীভাবে আইসোলেশন স্বয়ংক্রিয় করে?

EDR এজেন্ট আপসকৃত এন্ডপয়েন্টকে নেটওয়ার্ক স্তরে কোয়ারেন্টাইন করে, পার্শ্বীয় চলাচল ব্লক করে এবং বিশ্লেষকের অ্যাকসেস বজায় রাখে।

অংশ 11: 10টি বাস্তব সাইবার নিরাপত্তা তথ্য ও অন্তর্দৃষ্টি

নিরাপত্তা লঙ্ঘন, প্রতিরক্ষা কৌশল ও সম্মতির মান সম্পর্কে বাস্তব তথ্য দেখে নিন।

1. নিরাপত্তা ইনসাইট

সিগনেচর ডেটাবেসে পরিচিত ম্যালওয়্যারের হ্যাশ সংরক্ষিত থাকে, তাই নতুন বা পরিবর্তিত ফাইল ডেফিনিশন হালনাগাদ না হওয়া পর্যন্ত শনাক্ত হয় না।

2. নিরাপত্তা ইনসাইট

হিউরিস্টিক ইঞ্জিন সিগনেচার তৈরির আগেই কিছু নতুন ম্যালওয়্যার ভ্যারিয়েন্ট শনাক্ত করতে পারে, তবে এতে ভুল সতর্কতা বেশি হয়।

3. নিরাপত্তা ইনসাইট

ফলস পজিটিভ সতর্কতা ভুলবশত কোয়ারেন্টাইন করা ফাইল যাচাই ও পুনরুদ্ধারে IT টিমের সময় নষ্ট করে।

4. নিরাপত্তা ইনসাইট

পলিমরফিক ম্যালওয়্যার প্রতিটি কপিতে নিজের কোড বদলে ফেলে, তাই ডিফেন্ডাররা সিগনেচারের সঙ্গে হিউরিস্টিক ও আচরণ পরীক্ষা মিলিয়ে ব্যবহার করে।

6. নিরাপত্তা ইনসাইট

ম্যালওয়্যার লেখকরা স্যান্ডবক্স পরিবেশ শনাক্ত করতে কাস্টম কোড লেখে, টাইমার এড়াতে কার্যকরণ বিলম্বিত করে।

5. নিরাপত্তা ইনসাইট

ক্লাউডভিত্তিক অ্যান্টিভাইরাস ইঞ্জিন প্রায় রিয়েল টাইমে সন্দেহজনক ফাইলের হ্যাশ বিশাল অনলাইন হুমকি ডাটাবেসের সঙ্গে মিলিয়ে দেখে।

7. সিকিউরিটি ইনসাইট

ভেন্ডররা নিয়মিত এন্ডপয়েন্টে ডেফিনিশন আপডেট পাঠায়, যাতে স্ক্যানার সদ্য নিশ্চিত হওয়া হুমকি চিনতে পারে।

8. সিকিউরিটি ইনসাইট

র‍্যানসমওয়্যার বিহেভিয়ারাল মনিটর ফাইল এনক্রিপশন ও শ্যাডো কপি মুছে ফেলার সঙ্গে সম্পর্কিত নির্দিষ্ট Win32 API কলকে লক্ষ্য করে।

9. সিকিউরিটি ইনসাইট

বৈধ কোড স্বাক্ষর মিথ্যা-পজিটিভের ঝুঁকি কমাতে পারে, তবে স্বাক্ষরিত ফাইলও স্ক্যান করা হয়, কারণ ম্যালওয়্যারও স্বাক্ষরিত হতে পারে।

10. নিরাপত্তা ইনসাইট

রুটকিট সিস্টেম কার্নেলের কাঠামো পরিবর্তন করে, তাই শনাক্ত ও পরিষ্কার করতে বিশেষায়িত বুট-টাইম স্ক্যানার প্রয়োজন।

প্রযুক্তিগত তথ্যসূত্র ও উৎস

স্টাডি গাইড ও ইন্টারঅ্যাক্টিভ ধাঁধাগুলো বৈশ্বিক NIST, OWASP এবং ডেটা গোপনীয়তা সম্মতির মানদণ্ড থেকে সংকলিত। একাডেমিক ও শিল্পক্ষেত্রের তথ্যসূত্র

গবেষণামূলক ও শিল্পক্ষেত্রের তথ্যসূত্র

[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

উত্তরমালা: চেকপয়েন্ট 1 – বহুনির্বাচনী

1 প্রশ্ন 1 সিগনেচারসমূহ **সঠিক উত্তর: A**

শিক্ষণ নোট

সিগনেচার স্ক্যানিং পরিচিত ডাটাবেস হ্যাশের ওপর নির্ভর করে, ফলে অজানা বা পরিবর্তিত ম্যালওয়্যার শনাক্ত করতে ব্যর্থ হয়। সূত্র: OWASP Secure Configuration।

2 প্রশ্ন 2 হিউরিস্টিক **সঠিক উত্তর: A**

শিক্ষণ নোট

হিউরিস্টিক কোডের বিন্যাস ও কমান্ড বিশ্লেষণ করে নতুন হুমকি প্রকরণের সন্দেহজনক বৈশিষ্ট্য শনাক্ত করে। সূত্র: Center for Internet Security (CIS)।

3 প্রশ্ন 3 স্যান্ডবক্সিং **সঠিক উত্তর: A**

শিক্ষণ নোট

স্যান্ডবক্স সন্দেহজনক ফাইল একটি বিচ্ছিন্ন ভার্চুয়াল মেশিনে চালিয়ে নিরাপদে কার্যকরের আচরণ পর্যবেক্ষণ করে। সূত্র: NIST Digital Identity।

4 প্রশ্ন 4 আচরণগত **সঠিক উত্তর: A**

শিক্ষণ নোট

আচরণ স্ক্যানিং চলমান প্রোগ্রামগুলোকে রিয়েল টাইমে পর্যবেক্ষণ করে অননুমোদিত সিস্টেম পরিবর্তন ব্লক করে। সূত্র: Center for Internet Security (CIS)।

5 প্রশ্ন 5 আপডেটসমূহ **সঠিক উত্তর: A**

শিক্ষণ নোট

স্ক্যানার হুমকির পরিস্থিতির সঙ্গে সমন্বিত থাকতে প্রতিদিন ক্রমবর্ধমান সংজ্ঞা হালনাগাদ ডাউনলোড করে। সূত্র: OWASP Secure Configuration।

উত্তরমালা: চেকপয়েন্ট 2 – সত্য বা মিথ্যা

6 **প্রশ্ন 6** সিগনেচারসমূহ **সঠিক উত্তর: সত্য**

শিক্ষণ নোট

সিগনেচার টুল ক্রিপ্টোগ্রাফিক হ্যাশ গণনা করে এবং পরিচিত হুমকির হ্যাশের ডাটাবেসের সঙ্গে মেলায়। সূত্র: OWASP Secure Configuration।

7 **প্রশ্ন 7** হিউরিস্টিক **সঠিক উত্তর: সত্য**

শিক্ষণ নোট

হিউরিস্টিক ইঞ্জিন নিয়মভিত্তিক বিন্যাস চালায়, যা বৈধ ও নিরাপদ ফাইলকেও সন্দেহজনক হিসেবে চিহ্নিত করতে পারে। সূত্র: Center for Internet Security (CIS)।

8 **প্রশ্ন 8** স্যান্ডবক্সিং **সঠিক উত্তর: মিথ্যা**

শিক্ষণ নোট

স্যান্ডবক্স কোড একটি ভার্চুয়াল কনটেইনারে চালায় এবং নেটওয়ার্ক শেয়ারে প্রবেশ কঠোরভাবে ব্লক করে। সূত্র: NIST Digital Identity।

9 **প্রশ্ন 9** আচরণগত **সঠিক উত্তর: সত্য**

শিক্ষণ নোট

রিয়েল-টাইম মনিটরিং সেইসব চলমান প্রসেসকে চিহ্নিত করে যা অবৈধ লেখা বা ফাইল লক করার চেষ্টা করে। সূত্র: Center for Internet Security (CIS)।

10 **প্রশ্ন 10** **সঠিক উত্তর: মিথ্যা**

শিক্ষণ নোট

। কোনো অ্যান্টিভাইরাসই প্রতিটি জিরো-ডে আক্রমণ ঠেকায় না; অজানা হুমকি সিগনেচার ও হিউরিস্টিককে ফাঁকি দিতে পারে।

শব্দভাণ্ডারের উত্তরমালা ও মূল্যায়ন রুব্রিক

শিক্ষকের মূল্যায়ন রুব্রিক: প্রতিটি সঠিক মিলের জন্য (মোট ৪ নম্বর) এবং প্রসঙ্গ পরিভাষার জন্য (মোট 6 নম্বর) 1 নম্বর দিন।

চেকপয়েন্ট 4: উত্তর – ধারণা মিলান

D 1. হ্যাশ স্বাক্ষর	G 2. কোড হিউরিস্টিক	E 3. ফাইল স্যান্ডবক্স	C 4. আচরণ স্ক্যান
F 5. দৈনিক হালনাগাদ	H 6. ফলস পজিটিভ	A 7. হুমকি বিচ্ছিন্নকরণ	B 8. অ্যান্টিভাইরাস টুল

চেকপয়েন্ট 3: উত্তর – মূল পরিভাষা

1 সিগনেচার	2 হিউরিস্টিক	3 স্যান্ডবক্স	4 আচরণ
5 আপডেট	6 ভুল সতর্কতা		

চেকপয়েন্ট 6, বিকল্প: উত্তর – শব্দ মিলান

1 D – আচরণস্ক্যান	2 H – ভাইরাসস্ক্যানার	3 E – দৈনিকআপডেট	4 B – কোডহিউরিস্টিক
5 G – আইসোলেশন	6 A – হ্যাশসিগনেচার	7 C – স্যান্ডবক্সপরিবেশ	8 F – ভুলসতর্কতা

শিক্ষকদের জন্য আলোচনা নোট

মূল পরিভাষা:
যাচাই করুন শিক্ষার্থীরা হ্যাশ স্বাক্ষর, কোড হিউরিস্টিক ও ফাইল স্যান্ডবক্স নিজের ভাষায় ব্যাখ্যা করতে এবং প্রতিটির একটি উদাহরণ দিতে পারে কি না।

কেস স্টাডি:
শিক্ষার্থীদের বলুন তারা যেন মতামতের বদলে ওয়ার্কশিটের তথ্যের ভিত্তিতে সুপারিশ করে।

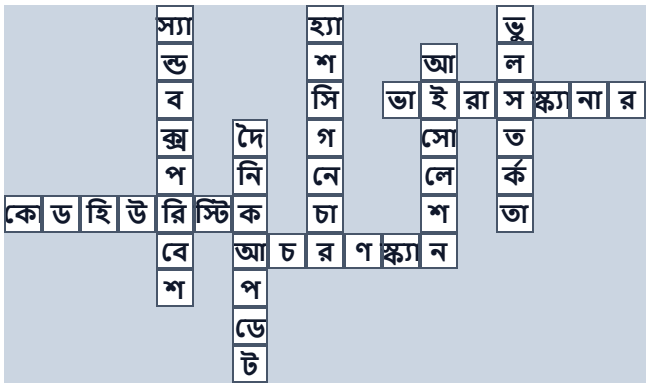
উৎস মূল্যায়ন:
শিক্ষার্থীদের ওয়ার্কশিটের উৎসে অন্তত একটি তথ্য যাচাই করতে বলুন এবং আলোচনা করুন কেন সংখ্যা, দাম ও নিয়ম সময়ের সঙ্গে বদলাতে পারে।

ধাঁধার উত্তরমালা ও শিক্ষকের নোট

শব্দ খোঁজার সমাধান

ক	সি	ন	দ	ঠ	হ	সা	শ	মে	দে	রা	কি	ঋ	তে	না
নে	ছ	স্ক্যা	য	প	উ	অ	উ	দৈ	ঋ	মা	বা	য	ফ	বা
ম	দে	ণ	তি	ভ	ঘ	রে	ষ	ফ	নি	ঘ	দ	হ	স	ভ
রি	মি	র	না	স্ক্যা	স	রা	ই	ভা	ঢ	ক	ষ	ষ	রি	সি
না	তি	চ	তা	ড	স্যা	ঊ	নি	তা	রা	কি	আ	থ	সে	ঊ
ক	লি	আ	গ	নি	ন্ড	জা	হ্যা	পি	র্ক	ঋ	জি	প	লি	ট
স্টি	ভ	ণ	জে	গ	ব	স	ঘ	শ	রে	ত	দি	মি	ডে	ঋ
রি	পা	উ	অ	জে	ক্স	কা	গ	ম	সি	আ	স	ঘ	কি	ট
উ	ঘ	ঝ	ণ	ধ	প	গ	সি	রি	শ	গ	ছ	ল	দ	সে
হি	জি	নি	ঝ	রে	রি	আ	পে	জ	আ	আ	নে	রে	ভু	মা
ড	স	মে	তি	দে	বে	ই	রি	ফ	সি	তি	সে	চা	খ	স
কো	বে	উ	ট	সে	শ	সো	দি	দা	প	আ	সি	জে	র	বি
বি	য	ড	দ	ষ	সা	লে	ফ	ল	ল	তা	কে	ণ	রা	রি
ণ	জে	ই	কে	পে	ঠ	শ	পি	ঊ	বে	সে	বে	উ	ণ	ল
জে	ঢ	ফ	কি	মে	কা	ন	দা	ঋ	ল	জে	বে	ঠ	বি	কে

ক্রসওয়ার্ডের সমাধান



পাশাপাশি

5 পাশাপাশি: ভাইরাসস্ক্যানার এন্ডপয়েন্টকে এক্সপ্লয়েট থেকে স্ক্যান ও সুরক্ষা দেওয়া সফটওয়্যার স্যুট (7 অক্ষর)

7 পাশাপাশি: কোডহিউরিস্টিক সন্দেহজনক কোড গঠনের ফাইল চিহ্নিতকারী নিয়মভিত্তিক বিশ্লেষণ (7 অক্ষর)

8 পাশাপাশি: আচরণস্ক্যান ক্ষতিকর কার্যক্রমের ধরন খুঁজতে চলমান সফটওয়্যারের কাজ পর্যবেক্ষণ (6 অক্ষর)

উপর-নিচ

1 উপর-নিচ: স্যান্ডবক্সপরিবেশ অবিশ্বস্ত কোড নিরাপদে চালানোর সুরক্ষিত ভার্চুয়াল পরীক্ষার পরিবেশ (8 অক্ষর)

2 উপর-নিচ: হ্যাশসিগনেচার পরিচিত হুমকি শনাক্তে ব্যবহৃত ডেটাবেসের অনন্য ক্রিপ্টোগ্রাফিক ছাপ (7 অক্ষর)

3 উপর-নিচ: ভুলসতর্কতা নিরাপদ সফটওয়্যারকে ভুলভাবে ম্যালওয়্যার হিসেবে চিহ্নিত করা নিরাপত্তা সতর্কতা (6 অক্ষর)

4 উপর-নিচ: আইসোলেশন স্থানীয় সিস্টেমের ঝুঁকি এড়াতে সন্দেহজনক ফাইল আটকে রাখা (6 অক্ষর)

6 উপর-নিচ: দৈনিকআপডেট হুমকির ডেটাবেসে তথ্য জোগানো নিয়মিত ডেফিনিশন ডাউনলোড (7 অক্ষর)

এলোমেলো শব্দ ও সংকেতবার্তা সমাধানের উত্তরমালা

শব্দভাণ্ডার অক্ষর-সাজানো কার্যক্রম ও Secret Cipher Challenge-এর মূল্যায়ন উত্তরমালা।

শব্দ সাজানোর উত্তরমালা

1. গচাহ্যানেরসিশ — **হ্যাশসিগনেচার**
2. ক্সস্যাশন্ডবেরিপব — **স্যান্ডবক্সপরিবেশ**
3. আদৈপটকডেনি — **দৈনিকআপডেট**
4. নলেসোশআই — **আইসোলেশন**
5. রিকউহিকোস্টিড — **কোডহিউরিস্টিক**
6. স্ক্যাণআরনচ — **আচরণস্ক্যান**
7. র্কভুততাসল — **ভুলসতর্কতা**
8. ইসরভানাস্ক্যারা — **ভাইরাসস্ক্যানার**

গোপন সংকেত চ্যালেঞ্জের উত্তরমালা

"কোড বিশ্লেষণে নতুন ম্যালওয়্যার শনাক্ত"

কেস স্টাডির উত্তর

A কেস স্টাডি 1: সিগনেচার বনাম হিউরিস্টিক স্ক্যান

শিক্ষকের সমাধান

মূল্যায়ন নির্দেশিকা

শিক্ষার্থীদের উত্তরে নিচের বিষয়গুলো থাকা উচিত:

- পরিস্থিতি বিশ্লেষণ: একজন কর্মী অন্য একটি দলের অভ্যন্তরীণভাবে তৈরি একটি কাস্টম ইউটিলিটি ডাউনলোড করেন। সিগনেচার স্ক্যানার এটি পাস করে, কিন্তু হিউরিস্টিক স্ক্যানার এটিকে সন্দেহজনক হিসেবে চিহ্নিত করে।
- প্রস্তাবিত কৌশল ও সমাধান: যা কেন ঘটল: সিগনেচার স্ক্যানিং ফাইলের হ্যাশ পরীক্ষা করে; ফাইলটি কাস্টম হওয়ায় এটি হুমকির ডেটাবেসে নেই। হিউরিস্টিক গঠন বিশ্লেষণ করে সন্দেহজনক কার্যকলাপ (যেমন রেজিস্ট্রিতে লেখা) চিহ্নিত করেছে। যাচাই: কার্যকলাপ পর্যবেক্ষণে ফাইলটি স্যান্ডবক্সে চালান, ডিজিটাল স্বাক্ষর পরীক্ষা করুন এবং হ্যাশ হুমকি-গোয়েন্দা পোর্টালে জমা দিন।

B কেস স্টাডি 2: ভুল ইতিবাচক ফলাফল সামলানো

শিক্ষকের সমাধান

মূল্যায়ন নির্দেশিকা

শিক্ষার্থীদের উত্তরে নিচের বিষয়গুলো থাকা উচিত:

- পরিস্থিতি বিশ্লেষণ: একজন সফটওয়্যার ডেভেলপার তার অ্যাপ্লিকেশন কম্পাইল করেন। সিস্টেমের অ্যান্টিভাইরাস নতুন এক্সিকিউটেবলকে ম্যালওয়্যার হিসেবে চিহ্নিত করে কোয়ারেন্টাইন করে।
- প্রস্তাবিত কৌশল ও সমাধান: হোয়াইটলিস্টিংয়ের ঝুঁকি: স্ক্যানার এড়ালে প্রকৃত সংক্রমিত কোড চলতে পারে। সমাধানের পথ: ফাইলটি বিশ্লেষণের জন্য অ্যান্টিভাইরাস বিক্রেতার কাছে জমা দিন, সার্টিফিকেট অথরিটির মাধ্যমে কোডে ডিজিটাল স্বাক্ষর করুন এবং অ্যান্টিভাইরাস বন্ধ করার বদলে সাময়িকভাবে নির্দিষ্ট ফোল্ডারের ব্যতিক্রম কনফিগার করুন।