নাম: _____ তারিখ: _____ নম্বর: _____

র‍্যানসমওয়্যার আক্রমণ ও ব্যবসা পুনরুদ্ধার

পেলোড কার্যকর হওয়া, ক্রিপ্টোগ্রাফিক ফাইল এনক্রিপশন, অফলাইন ব্যাকআপ, নিয়ন্ত্রণ ব্যবস্থা এবং দুর্যোগ পুনরুদ্ধার।

র‍্যানসমওয়্যার আক্রমণ শেখার সংক্ষিপ্ত বিবরণ

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 র‍্যানসমওয়্যার আক্রমণ ও ব্যবসা পুনরুদ্ধার বিষয়ে গাইড করবে। আপনি পেলোড এক্সিকিউশন, ফাইল এনক্রিপশন, অফলাইন ব্যাকআপ, হুমকি নিয়ন্ত্রণ, ক্রিপ্টোকারেন্সি পেমেন্ট এবং দুর্যোগ পুনরুদ্ধার পরিকল্পনা 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/ransomware-akromon/

আপনার র‍্যানসমওয়্যার পুনরুদ্ধার শেখার রোডম্যাপ

- ট্রোজান, র‍্যানসমওয়্যার ও স্পাইওয়্যার পেলোডের মধ্যে পার্থক্য করুন।
- নিরাপদ স্যান্ডবক্স পরিবেশের ভেতরে ক্ষতিকর ফাইল বিশ্লেষণ করুন।
- দ্রুত নেটওয়ার্ক বিচ্ছিন্নকরণ ও নিয়ন্ত্রণ পদ্ধতি তৈরি করুন।

র‍্যানসমওয়্যার আক্রমণ গাইড নির্দেশনা

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

র‍্যানসমওয়্যার আক্রমণ ও দুর্যোগ পুনরুদ্ধার (ভূমিকা)

র‍্যানসমওয়্যার পেলোড ক্রিপ্টোগ্রাফিকভাবে সিস্টেমের স্টোরেজ লক করে এবং ডিক্রিপশন কী-র জন্য ক্রিপ্টোকারেন্সিতে অর্থ দাবি করে। এই হুমকি প্রশমনে নেটওয়ার্ক আইসোলেশন রুল, স্যান্ডবক্সে ম্যালওয়্যার বিশ্লেষণ এবং শক্তিশালী এয়ার-গ্যাপড কোল্ড ব্যাকআপ সহায়ক।

প্রতিটি চেকপয়েন্ট মনোযোগ দিয়ে পড়ুন এবং সঠিক উত্তরটি বেছে নিন বা লিখুন।

চেকপয়েন্ট 1: বহুনির্বাচনী চ্যালেঞ্জ

1 **1. র‍্যানসমওয়্যার আক্রমণের প্রধান কার্যপদ্ধতি কী?**

- A. সিস্টেম অ্যাক্সেস অস্বীকার করতে ব্যবহারকারীর ফাইলের ক্রিপ্টোগ্রাফিক এনক্রিপশন
- B. ফর্ম ফিল্ডে ক্ষতিকর SQL কমান্ড ঢোকানো
- C. পাবলিক Wi-Fi সংযোগে নেটওয়ার্ক প্যাকেট স্নিফ করা
- D. SPF যাচাই এড়াতে ইমেইল হেডার জাল করা

2 **2. অফলাইন (কোল্ড) ব্যাকআপ কী?**

- A. ম্যালওয়্যার ছড়ানো ঠেকাতে নেটওয়ার্ক থেকে বিচ্ছিন্ন রাখা একটি স্টোরেজ কপি
- B. প্রাথমিক ওয়েব সার্ভারের হার্ড ড্রাইভে রাখা ব্যাকআপ
- C. সিস্টেম রেজিস্ট্রি লগের একটি অস্থায়ী ক্যাশ
- D. ব্যবহারকারীর পাসওয়ার্ড রিসেট করতে ব্যবহৃত একটি প্রশাসনিক টুল

3 **3. র‍্যানসমওয়্যার আক্রমণের সময় নিরাপত্তা দলগুলোর সংক্রমিত সিস্টেম কীভাবে বিচ্ছিন্ন করা উচিত?**

- A. নেটওয়ার্ক তার খুলে ফেলা এবং ওয়্যারলেস ইন্টারফেস অবিলম্বে নিষ্ক্রিয় করা
- B. অ্যান্টিভাইরাস সিগনেচার ডেটাবেস হালনাগাদ করুন
- C. প্রাইমারি DNS সার্ভার বন্ধ করে দিন
- D. আক্রান্ত ফাইলের এক্সটেনশন বদলে ফেলুন

4 **4. নিরাপত্তা সংস্থাগুলো কেন র‍্যানসমওয়্যারের দাবি মেটাতে নিষেধ করে?**

- A. অর্থ দিলে আক্রমণকারীরা উৎসাহিত হয় এবং ডিক্রিপশন কী পাওয়ার নিশ্চয়তা থাকে না
- B. এটি স্বয়ংক্রিয়ভাবে সব কর্পোরেট বিমা পলিসি বাতিল করে দেয়
- C. এটি স্বয়ংক্রিয়ভাবে প্রতিটি গ্রাহককে ইমেইলে জানায়
- D. এটি অবশিষ্ট সিস্টেম ব্যাকআপ ফাইল নষ্ট করে

5 **5. দুর্যোগ পুনরুদ্ধার পরিকল্পনা (DRP) কী?**

- A. সিস্টেম আপসের পর কার্যক্রম ও ডেটা পুনরুদ্ধারের একটি কাঠামোবদ্ধ প্রক্রিয়া
- B. ইনবাউন্ড নেটওয়ার্ক পোর্ট ম্যাপ করা ফায়ারওয়াল কনফিগারেশন
- C. ব্যবহারকারীর প্রশাসনিক সুবিধার তালিকা সংবলিত একটি ডেটাবেস স্কিমা
- D. স্পুফ করা ডোমেইন প্রত্যাখ্যানকারী একটি ইমেইল প্রমাণীকরণ প্রোটোকল

চেকপয়েন্ট 2: সত্য বা মিথ্যা চ্যালেঞ্জ

6 প্রশ্ন 6

6. র‍্যানসমওয়্যার পেলোড নেটওয়ার্কে সংযুক্ত অনলাইন ব্যাকআপে সহজেই ছড়িয়ে পড়তে পারে।

○ সত্য ○ মিথ্যা

7 প্রশ্ন 7

7. ক্রিপ্টোকারেন্সিতে মুক্তিপণ দিলে ফাইল সফলভাবে ডিক্রিপ্ট হওয়ার নিশ্চয়তা মেলে।

○ সত্য ○ মিথ্যা

8 প্রশ্ন 8

8. সংক্রমিত সিস্টেম নেটওয়ার্ক থেকে বিচ্ছিন্ন করলে র‍্যানসমওয়্যার পার্শ্ববর্তী সিস্টেমে ছড়ানো ঠেকাতে সহায়তা করে।

○ সত্য ○ মিথ্যা

9 প্রশ্ন 9

9. র‍্যানসমওয়্যার সিস্টেম স্টোরেজ এনক্রিপ্ট করতে কখনোই সিমেট্রিক ক্রিপ্টোগ্রাফি ব্যবহার করে না।

○ সত্য ○ মিথ্যা

10 প্রশ্ন 10

10. ডেটা পুনরুদ্ধার পদ্ধতি নিয়মিত পরীক্ষা করা দুর্যোগ পুনরুদ্ধারের একটি গুরুত্বপূর্ণ অংশ।

○ সত্য ○ মিথ্যা

চেকপয়েন্ট 3: মূল পরিভাষা বসানো

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

1. স্থানীয় ফাইলে প্রবেশ আটকাতে ব্যবহৃত হয় ক্রিপ্টোগ্রাফিক _____ ।
2. সিস্টেমে চালানো সক্রিয় ক্ষতিকর কোডটি হলো _____ ।
3. বিচ্ছিন্ন অফসাইট স্টোরেজ কপি একটি নিরাপদ _____ -এর উদাহরণ।
4. ম্যালওয়্যার ছড়ানো থামাতে এন্ডপয়েন্ট নেটওয়ার্ক _____ দরকার।
5. সাইবার অপরাধীদের দাবি করা ক্রিপ্টোকারেন্সি পেমেন্টটি হলো _____ ।
6. চালু ডেটা ফাইল ফিরিয়ে আনা হলো বিপর্যয় _____ ।

পরিভাষা শব্দভাণ্ডার

আইসোলেশন এনক্রিপশন কোল্ড ব্যাকআপ ট্রোজান পুনরুদ্ধার পেলোড মুক্তিপণ ম্যালওয়্যার

এখানে আপনার উত্তর লিখুন:

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

চেকপয়েন্ট 4: নিরাপত্তা ধারণা মিলান

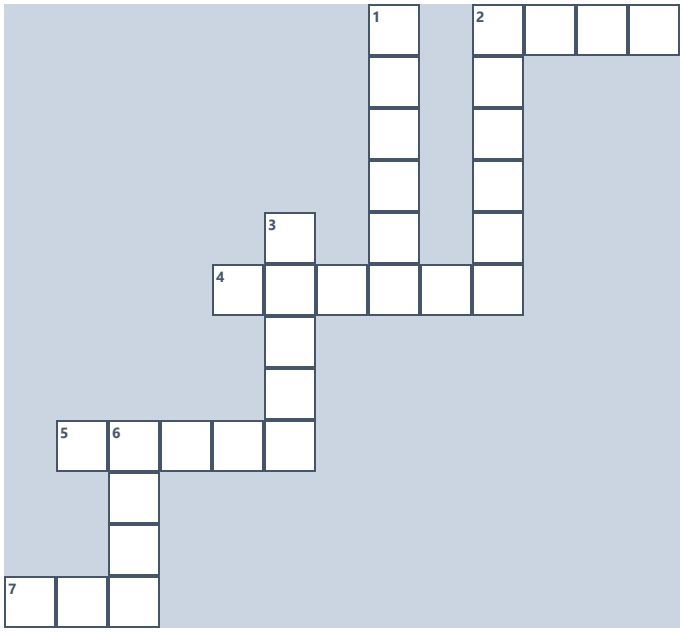
সংজ্ঞা মেলানো

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

☐	1. এনক্রিপশন	A	সংক্রমিত নেটওয়ার্ক সিস্টেমের সংযোগ বিচ্ছিন্ন করা।
☐	2. পেলোড	B	পরিষ্কার ফাইলের ছদ্মবেশে ক্ষতিকর ফাইল।
☐	3. কোল্ড ব্যাকআপ	C	ফাইল ক্রিপ্টোগ্রাফিকভাবে লক করা।
☐	4. বিচ্ছিন্নকরণ	D	বড় ধরনের সিস্টেম বিপর্যয়ের ঘটনা।
☐	5. মুক্তিপণ	E	ক্ষতিকর সফটওয়্যার চালানো।
☐	6. পুনরুদ্ধার	F	বিচ্ছিন্ন অফলাইন কপি।
☐	7. দুর্যোগ	G	ব্যাকআপ থেকে ডেটাবেস পুনরুদ্ধার।
☐	8. ট্রোজান	H	ক্রিপ্টোগ্রাফিক কী পেআউটের অনুরোধ।

চেকপয়েন্ট 5: ক্রসওয়ার্ড ধাঁধা

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



পাশাপাশি

2. সিস্টেম বা ব্যবহারকারীর ওপর চালানো ক্ষতিকর প্রচেষ্টা (4)

4. ফাইলকে ক্রিপ্টোগ্রাফিক উপায়ে তালাবদ্ধ করা (6)

5. ক্ষতি করার উদ্দেশ্যে তৈরি যেকোনো ক্ষতিকর সফটওয়্যার (5)

7. নিরীহ ফাইলের ছদ্মবেশে ক্ষতিকর ফাইল (3)

উপর-নিচ

1. বিচ্ছিন্ন অফলাইন কপি (6)

2. সংক্রমিত নেটওয়ার্ক সিস্টেম বিচ্ছিন্ন করা (6)

3. ব্যাকআপ থেকে ডেটাবেস ফিরিয়ে আনা (5)

6. নাম ও পাসওয়ার্ড দিয়ে অ্যাকাউন্টে প্রবেশের প্রক্রিয়া (4)

চেকপয়েন্ট 5, বিকল্প: সহজবোধ্য ক্রসওয়ার্ড সূত্র

স্ক্রিন-রিডার ও কিবোর্ড ব্যবহারকারীরা নিচের টেক্সট ফিল্ডে সরাসরি ক্রসওয়ার্ডের উত্তর লিখতে পারেন।

পাশাপাশি

2 পাশাপাশি: সিস্টেম বা ব্যবহারকারীর ওপর চালানো ক্ষতিকর প্রচেষ্টা (4 অক্ষর):

4 পাশাপাশি: ফাইলকে ক্রিপ্টোগ্রাফিক উপায়ে তালাবদ্ধ করা (6 অক্ষর):

5 পাশাপাশি: ক্ষতি করার উদ্দেশ্যে তৈরি যেকোনো ক্ষতিকর সফটওয়্যার (5 অক্ষর):

7 পাশাপাশি: নিরীহ ফাইলের ছদ্মবেশে ক্ষতিকর ফাইল (3 অক্ষর):

উপর-নিচ

1 উপর-নিচ: বিচ্ছিন্ন অফলাইন কপি (6 অক্ষর):

2 উপর-নিচ: সংক্রমিত নেটওয়ার্ক সিস্টেম বিচ্ছিন্ন করা (6 অক্ষর):

3 উপর-নিচ: ব্যাকআপ থেকে ডেটাবেস ফিরিয়ে আনা (5 অক্ষর):

6 উপর-নিচ: নাম ও পাসওয়ার্ড দিয়ে অ্যাকাউন্টে প্রবেশের প্রক্রিয়া (4 অক্ষর):

চেকপয়েন্ট 6: লুকানো শব্দ খোঁজা

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

ই ট লে ছ ণ লে তা বি নি ঘ ল মি কে ভ ড
রা র র ঈ তি গ ই সে ল ভ মা ণ জে ঘ চ
ই দ্ধা হ ণ দ নে স ঝ কা গ জ রা ফ ঘ উ
সে রু জি আ ড প পা ধ দ জি ই কি না লি ই
রে ন ফ চ ব এ দি শ জা রা দে ন ট মে র
ক পু সি দ ঠ ন হ আ সা শ মে ট্রো জা ন দে
রা কি ঋ তে না ক্রি নে ছ ই য প উ অ উ ঋ
র মা বা য ফ প বা ম দে সো তি ভ ঘ রে ষ
য়্যা ফ ঘ দ হ শ স ভ রি মি লে ঢ ষ ষ রি
ও সি না তি তা ন ড ঊ নি রা কি শ থ সে ঊ
ল কো ল্ড ব্যা ক আ প লি গ নি জা পি ন ঋ আ
ম্যা জি লি ট ভ ণ জে গ স ঘ রে দি মি ক্র ঋ
পা উ অ জে কা গ ম আ ঘ কি ঘ ঝ ম ণ ধ
গ সি রি শ ছ দ সে জি নি ঝ রে ণ পে জ আ
আ রে মা স মে তি দে রি ফ সি তি সে খ স বে

পরিভাষা শব্দতালিকা

এনক্রিপশন, কোল্ডব্যাকআপ, আইসোলেশন, পুনরুদ্ধার, ট্রোজান, ম্যালওয়্যার, লগইন, আক্রমণ

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. এনক্রিপশন

B. কোল্ডব্যাকআপ

C. আইসোলেশন

D. পুনরুদ্ধার

E. ট্রোজান

F. ম্যালওয়্যার

G. লগইন

H. আক্রমণ

সংজ্ঞা ও মিলের ঘর

1. সংক্রমিত নেটওয়ার্ক সিস্টেম বিচ্ছিন্ন করা।
2. সিস্টেম বা ব্যবহারকারীর ওপর চালানো ক্ষতিকর প্রচেষ্টা।
3. ফাইলকে ক্রিপ্টোগ্রাফিক উপায়ে তালাবদ্ধ করা।
4. নিরীহ ফাইলের ছদ্মবেশে ক্ষতিকর ফাইল।
5. ব্যাকআপ থেকে ডেটাবেস ফিরিয়ে আনা।
6. নাম ও পাসওয়ার্ড দিয়ে অ্যাকাউন্টে প্রবেশের প্রক্রিয়া।
7. বিচ্ছিন্ন অফলাইন কপি।
8. ক্ষতি করার উদ্দেশ্যে তৈরি যেকোনো ক্ষতিকর সফটওয়্যার।

চেকপয়েন্ট 7: এলোমেলো শব্দ চ্যালেঞ্জ

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

1. ক্রি এ প শ ন ন
2. ন আ সো শ লে ই
3. ন জা ট্রো
4. ন ই ল গ
5. ক ব্যা প কো আ ল্ড
6. দ্ধা পু রু র ন
7. য়্যা র ম্যা ও ল
8. আ ণ ম ক্র

অতিরিক্ত কার্যক্রম: দ্রুত ভাবুন

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

1	যে তথ্য আপনার কখনো শেয়ার করা উচিত নয়			
2	যেসব ডিভাইস হ্যাক হতে পারে			
3	মুক্তিপণ না দেওয়ার কারণ			
4	যেসব নিরাপদ অভ্যাস আপনি আজই শুরু করতে পারেন			
5	আপনার জানা নিরাপত্তা টুল			
6	আপনার অ্যাকাউন্ট সুরক্ষিত রাখার উপায়			
7	কম্পিউটার সংক্রমিত হওয়ার লক্ষণ			
8	ব্যাকআপ রাখার জায়গা			
9	যেসব ফাইল আপনি কখনো হারাতে চান না			
10	র‍্যানসমওয়্যার ছড়ানোর উপায়			
11	আক্রমণের প্রথম ঘণ্টায় যা করবেন			
12	আক্রমণের সময় যাদের সঙ্গে যোগাযোগ করবেন			
13	র‍্যানসমওয়্যার যা যা লক করে দিতে পারে			
14	সাইবার নিরাপত্তার সঙ্গে সম্পর্কিত শব্দ			
15	যেসব প্রতিষ্ঠান প্রায়ই লক্ষ্যবস্তু হয়			

চেকপয়েন্ট ৪: সাইবার নিরাপত্তা কেস স্টাডি

নিচের বাস্তব পরিস্থিতিগুলো সমাধান করতে শেখা ধারণাগুলো প্রয়োগ করুন।

কেস স্টাডি 1: এন্টারপ্রাইজ র‍্যানসমওয়্যার পেলোড নিয়ন্ত্রণ



পরিস্থিতি: একটি কর্পোরেট লোকাল এরিয়া নেটওয়ার্ক সক্রিয় র‍্যানসমওয়্যারে আক্রান্ত হয়েছে। মূল ফাইল সার্ভারগুলোতে .locked এক্সটেনশন দেখা যেতে শুরু করেছে।

আলোচনার প্রশ্ন: নিয়ন্ত্রণমূলক ধাপগুলো বিস্তারিত বর্ণনা করুন এবং ডেটা পুনরুদ্ধার প্রোটোকলের রূপরেখা দিন।

কেস স্টাডি 2: অফলাইন ব্যাকআপ আর্কিটেকচার মূল্যায়ন



পরিস্থিতি: একটি এন্টারপ্রাইজ এমন একটি ডেটা ব্যাকআপ কৌশল ডিজাইন করতে চায় যা প্রাথমিক লোকাল নেটওয়ার্ক র‍্যানসমওয়্যারে সম্পূর্ণ হাইজ্যাক হয়ে গেলেও ব্যাকআপ আপস হওয়ার ঝুঁকি কমায়।

আলোচনার প্রশ্ন: একটি নিরাপদ অফলাইন ব্যাকআপ স্টোরেজ ভল্ট সিস্টেম নকশা 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	39	58	24		34	58	37	45	12	2	32	51		24	51	22	45

33	46	38	46	37	59	51		2	31	48	31

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: র‍্যানসমওয়্যার কী?

র‍্যানসমওয়্যার হলো ক্ষতিকর সফটওয়্যার, যা মুক্তিপণ পরিশোধ না হওয়া পর্যন্ত কম্পিউটার সিস্টেম বা ফাইলে প্রবেশাধিকার আটকে রাখার জন্য তৈরি।

Q2: র‍্যানসমওয়্যার কীভাবে ছড়ায়?

ইমেইল ফিশিং সংযুক্তি, প্যাচ-না-করা সফটওয়্যারের দুর্বলতা এবং আপসকৃত দূরবর্তী অ্যাক্সেস সিস্টেমের মাধ্যমে। [1]

Q3: ক্রিপ্টোকারেন্সিতে পেমেন্ট কেন চাওয়া হয়?

Bitcoin-এর মতো ক্রিপ্টোকারেন্সি আপেক্ষিক পরিচয়গোপনতা দেয়, ফলে আইন প্রয়োগকারী সংস্থার জন্য অর্থের গতিপথ অনুসরণ করা কঠিন হয়।

Q4: অ্যান্টিভাইরাস কি র‍্যানসমওয়্যার ঠেকায়?

হ্যাঁ, তবে সিগনেচার-ভিত্তিক অ্যান্টিভাইরাস নতুন তৈরি জিরো-ডে র‍্যানসমওয়্যার পেলোডের বিরুদ্ধে ব্যর্থ হতে পারে।

Q5: এয়ার-গ্যাপড ব্যাকআপ কী?

প্রধান নেটওয়ার্কের সঙ্গে ভৌত বা যৌক্তিক কোনো সংযোগ নেই এমন একটি ব্যাকআপ কপি, যা একে সংক্রমণ ছড়ানো থেকে রক্ষা করে।

চেকপয়েন্ট 10: মৌলিক সাইবার নিরাপত্তা FAQ (অংশ B)

অনলাইন হুমকি প্রশমন নিয়ে প্রচলিত প্রশ্ন ও উত্তরগুলো দেখে নিন।

Q6: ডাবল এক্সটর্শন কী?

যখন আক্রমণকারীরা শুধু ফাইল এনক্রিপ্টই করে না, সংবেদনশীল ডেটাও চুরি করে এবং অর্থ না দিলে প্রকাশ্যে ফাঁসের হুমকি দেয়।

Q7: ডিক্রিপ্টর কী?

লক হওয়া ফাইল প্লেইনটেক্সটে ফিরিয়ে আনতে প্রয়োজনীয় ক্রিপ্টোগ্রাফিক কী ধারণকারী একটি সফটওয়্যার ইউটিলিটি।

Q8: আপনি কীভাবে র‍্যানসমওয়্যার আগেভাগে শনাক্ত করবেন?

হঠাৎ বিপুল সংখ্যক ফাইল পরিবর্তন ও নাম বদলের কার্যকলাপের জন্য ফাইল সিস্টেম পর্যবেক্ষণ করে।

Q9: বিমার ভূমিকা কী?

সাইবার বিমা পুনরুদ্ধারের খরচ মেটাতে সাহায্য করতে পারে, তবে কভারেজের শর্ত ও মুক্তিপণ প্রদানের নিয়ম পলিসিভেদে ভিন্ন।

Q10: সংক্রমিত সিস্টেম কি রিবুট করা উচিত?

না, রিবুট করলে উবে যাওয়া মেমোরির প্রমাণ নষ্ট হতে পারে; এর বদলে এটিকে নেটওয়ার্ক থেকে আলাদা করুন। [1]

চেকপয়েন্ট 10: উন্নত নিরাপত্তা FAQ (অংশ C)

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

Q1: র‍্যানসমওয়্যার কীভাবে অ্যাসিমেট্রিক এনক্রিপশন ব্যবহার করে?

এটি ফাইল এনক্রিপ্ট করতে ম্যালওয়্যারে এমবেড করা একটি পাবলিক কী ব্যবহার করে, এবং ডিক্রিপ্ট করতে আক্রমণকারীর প্রাইভেট কী প্রয়োজন হয়।

Q2: সিমেট্রিক এনক্রিপশনও কেন ব্যবহার করা হয়?

সিমেট্রিক এনক্রিপশন (যেমন AES) দ্রুত এবং কয়েক মিনিটেই বিশাল ডেটাবেস লক করতে পারে, আর অ্যাসিমেট্রিক কী AES কী-কে সুরক্ষিত করে।

Q3: লজিক্যাল সেগমেন্টেশন কী?

নেটওয়ার্ককে বিচ্ছিন্ন জোনে ভাগ করা, যাতে ম্যালওয়্যার ওয়ার্কস্টেশন নোড থেকে কোর সার্ভারে পার্শ্বীয়ভাবে ছড়াতে না পারে।

Q4: WORM স্টোরেজ কী?

রাইট-ওয়ান্স, রিড-মেনি মিডিয়া, যা র‍্যানসমওয়্যার পেলোডকে ব্যাকআপ ডেটা সম্পাদনা, ওভাররাইট বা মুছে ফেলা থেকে বিরত রাখে।

Q5: শ্যাডো কপি কী?

Windows-এর তৈরি স্থানীয় ব্যাকআপ স্ন্যাপশট; র‍্যানসমওয়্যার সাধারণত প্রশাসনিক টুল ব্যবহার করে সবার আগে এগুলো মুছে ফেলে।

চেকপয়েন্ট 10: উন্নত নিরাপত্তা FAQ (অংশ D)

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

Q6: ক্রেডেনশিয়াল চুরি কীভাবে র‍্যানসমওয়্যারের পথ খুলে দেয়?

আক্রমণকারীরা ফাঁস হওয়া অ্যাডমিন লগইন কিনে রিমোট ডেস্কটপের মাধ্যমে সাইন ইন করে এবং নেটওয়ার্ক জুড়ে হাতে-কলমে র‍্যানসমওয়্যার চালায়।

Q7: ড্রাই-রান রিস্টোরেশন টেস্টিং কী?

পুনরুদ্ধারের গতি ও ডেটার অখণ্ডতা দুর্যোগ-মানদণ্ড পূরণ করে কি না যাচাই করতে নিয়মিত ব্যাকআপ ডেটাবেস আলাদা টেস্ট পরিবেশে পুনরুদ্ধার করা।

Q8: এন্ডপয়েন্ট ডিটেকশন (EDR) কীভাবে র‍্যানসমওয়্যার ঠেকায়?

প্রসেসের আচরণ বিশ্লেষণ (যেমন দ্রুত এনক্রিপশন) করে এবং বেপরোয়া অ্যাপ্লিকেশনকে দ্রুত স্থগিত করে।

Q9: র‍্যানসমওয়্যার-অ্যাজ-আ-সার্ভিস (RaaS) মডেল কী?

একটি ফ্র্যাঞ্চাইজ মডেল, যেখানে ম্যালওয়্যার ডেভেলপাররা আয়ের একটি শতাংশের বিনিময়ে অ্যাফিলিয়েটদের কাছে র‍্যানসমওয়্যার বিল্ডার ভাড়া দেয়।

Q10: প্যাচ না করা RDP কীভাবে র‍্যানসমওয়্যার ঘটায়?

উন্মুক্ত, প্যাচ না করা Remote Desktop Protocol গেটওয়ে আক্রমণকারীদের লগইন ব্রুট-ফোর্স করতে ও হাতে-কলমে ম্যালওয়্যার চালাতে দেয়।

অংশ 11: 10টি বাস্তব সাইবার নিরাপত্তা তথ্য ও অন্তর্দৃষ্টি

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

1. নিরাপত্তা ইনসাইট

র‍্যানসমওয়্যার আক্রমণকারীরা প্রায়ই vssadmin.exe-এর মতো টুল ব্যবহার করে Windows শ্যাডো কপি মুছে দেয় এবং স্থানীয় রিস্টোর ব্লক করে। [1]

2. নিরাপত্তা ইনসাইট

সিমেট্রিক AES-256 কী সাধারণত ফাইল পেলোড এনক্রিপ্ট করতে ব্যবহৃত হয়, যা পরে পাবলিক RSA কী দিয়ে লক করা হয়।

3. নিরাপত্তা ইনসাইট

সফল র‍্যান্সমওয়্যার আক্রমণ থেকে পুনরুদ্ধারে কয়েক সপ্তাহ লাগতে পারে, তাই পরীক্ষিত অফলাইন ব্যাকআপ গুরুত্বপূর্ণ।

4. নিরাপত্তা ইনসাইট

FBI মুক্তিপণ দেওয়া সমর্থন করে না এবং সতর্ক করে যে মুক্তিপণ দিলেও কোনো ডেটা ফেরত পাওয়ার নিশ্চয়তা নেই। [2]

5. নিরাপত্তা ইনসাইট

ডিজাস্টার রিকভারি পরিকল্পনায় (DRP) একটি Recovery Time Objective (RTO) ও একটি Recovery Point Objective (RPO) নির্ধারণ করা উচিত।

6. নিরাপত্তা ইনসাইট

FBI এনক্রিপ্টেড ও অপরিবর্তনীয় ব্যাকআপের সুপারিশ করে, অর্থাৎ যা পরিবর্তন বা মুছে ফেলা যায় না। [3]

7. সিকিউরিটি ইনসাইট

র‍্যানসমওয়্যার ডেভেলপাররা প্রচলিত সিগনেচার-ভিত্তিক অ্যান্টিভাইরাস স্ক্যানার এড়াতে উন্নত অবফাসকেশন কৌশল ব্যবহার করে।

8. সিকিউরিটি ইনসাইট

নেটওয়ার্ক সেগমেন্টেশন পার্শ্বিক চলাচল সীমিত করে, ফলে র‍্যানসমওয়্যার প্রথম আক্রান্ত হোস্টের বাইরে ছড়ানো ঠেকাতে সাহায্য করে। [3]

9. সিকিউরিটি ইনসাইট

Remote Desktop Protocol (RDP)-এর মতো উন্মুক্ত, দুর্বলভাবে সুরক্ষিত রিমোট সার্ভিস র‍্যানসমওয়্যারের একটি সাধারণ প্রবেশপথ। [1]

10. নিরাপত্তা ইনসাইট

CISA পরামর্শ দেয় এনক্রিপ্ট করা ব্যাকআপ অফলাইনে রাখতে, কারণ অনেক র‍্যানসমওয়্যার প্রকরণ নাগালের মধ্যে থাকা ব্যাকআপ খুঁজে মুছে ফেলে। [1]

প্রযুক্তিগত তথ্যসূত্র ও উৎস

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

গবেষণামূলক ও শিল্পক্ষেত্রের তথ্যসূত্র

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

[2] FBI Internet Crime Complaint Center. (n.d.). Ransomware.
https://www.ic3.gov/CrimeInfo/Ransomware

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

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

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

উত্তরমালা: চেকপয়েন্ট 1 – বহুনির্বাচনী

1 প্রশ্ন 1

সঠিক উত্তর: A

শিক্ষণ নোট

র‍্যানসমওয়্যার আক্রমণের প্রধান কার্যপদ্ধতি কী? → সিস্টেম অ্যাক্সেস অস্বীকার করতে ব্যবহারকারীর ফাইলের ক্রিপ্টোগ্রাফিক এনক্রিপশন

2 প্রশ্ন 2

সঠিক উত্তর: A

শিক্ষণ নোট

অফলাইন (কোল্ড) ব্যাকআপ কী? → ম্যালওয়্যার ছড়ানো ঠেকাতে নেটওয়ার্ক থেকে বিচ্ছিন্ন রাখা একটি স্টোরেজ কপি

3 প্রশ্ন 3

সঠিক উত্তর: A

শিক্ষণ নোট

র‍্যানসমওয়্যার আক্রমণের সময় নিরাপত্তা দলগুলোর সংক্রমিত সিস্টেম কীভাবে বিচ্ছিন্ন করা উচিত? → নেটওয়ার্ক তার খুলে ফেলা এবং ওয়্যারলেস ইন্টারফেস অবিলম্বে নিষ্ক্রিয় করা

4 প্রশ্ন 4

সঠিক উত্তর: A

শিক্ষণ নোট

নিরাপত্তা সংস্থাগুলো কেন র‍্যানসমওয়্যারের দাবি মেটাতে নিষেধ করে? → অর্থ দিলে আক্রমণকারীরা উৎসাহিত হয় এবং ডিক্রিপশন কী পাওয়ার নিশ্চয়তা থাকে না

5 প্রশ্ন 5

সঠিক উত্তর: A

শিক্ষণ নোট

দুর্যোগ পুনরুদ্ধার পরিকল্পনা (DRP) কী? → সিস্টেম আপসের পর কার্যক্রম ও ডেটা পুনরুদ্ধারের একটি কাঠামোবদ্ধ প্রক্রিয়া

উত্তরমালা: চেকপয়েন্ট 2 – সত্য বা মিথ্যা

6 প্রশ্ন 6 — সঠিক উত্তর: সত্য

শিক্ষণ নোট

র‍্যানসমওয়্যার পেলোড নেটওয়ার্কে সংযুক্ত অনলাইন ব্যাকআপে সহজেই ছড়িয়ে পড়তে পারে।

7 প্রশ্ন 7 — সঠিক উত্তর: মিথ্যা

শিক্ষণ নোট

মিথ্যা: FBI সতর্ক করে যে মুক্তিপণ দিলে কোনো ডেটা ফেরত পাওয়ার নিশ্চয়তা নেই।

8 প্রশ্ন 8 — সঠিক উত্তর: সত্য

শিক্ষণ নোট

সত্য: CISA সংক্রমিত হোস্ট আনপ্লাগ করার বা নেটওয়ার্ক অফলাইনে নেওয়ার পরামর্শ দেয়, যাতে ছড়ানো সীমিত থাকে।

9 প্রশ্ন 9 — সঠিক উত্তর: মিথ্যা

শিক্ষণ নোট

মিথ্যা: র‍্যানসমওয়্যার সাধারণত AES-এর মতো দ্রুত সিমেট্রিক সাইফার দিয়ে ফাইল এনক্রিপ্ট করে।

10 প্রশ্ন 10 — সঠিক উত্তর: সত্য

শিক্ষণ নোট

ডেটা পুনরুদ্ধার পদ্ধতি নিয়মিত পরীক্ষা করা দুর্যোগ পুনরুদ্ধারের একটি গুরুত্বপূর্ণ অংশ।

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

C 1. এনক্রিপশন	E 2. পেলোড	F 3. কোল্ড ব্যাকআপ	A 4. বিচ্ছিন্নকরণ
H 5. মুক্তিপণ	G 6. পুনরুদ্ধার	D 7. দুর্যোগ	B 8. ট্রোজান

চেকপয়েন্ট 3: উত্তর – মূল পরিভাষা

1 এনক্রিপশন	2 পেলোড	3 কোল্ড ব্যাকআপ	4 আইসোলেশন
5 মুক্তিপণ	6 পুনরুদ্ধার		

চেকপয়েন্ট 6, বিকল্প: উত্তর – শব্দ মিলান

1 C – আইসোলেশন	2 H – আক্রমণ	3 A – এনক্রিপশন	4 E – ট্রোজান
5 D – পুনরুদ্ধার	6 G – লগইন	7 B – কোল্ডব্যাকআপ	8 F – ম্যালওয়্যার

শিক্ষকদের জন্য আলোচনা নোট

মূল পরিভাষা:
যাচাই করুন শিক্ষার্থীরা এনক্রিপশন, পেলোড ও কোল্ড ব্যাকআপ 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।

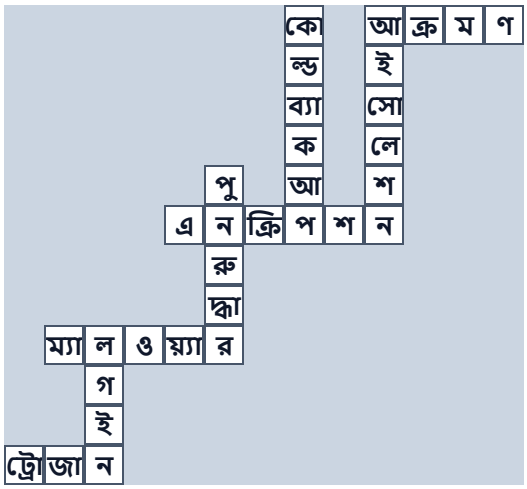
উৎস মূল্যায়ন:
শিক্ষার্থীদের ওয়ার্কশিটের উৎসে অন্তত একটি তথ্য যাচাই করতে বলুন এবং আলোচনা করুন কেন সংখ্যা, দাম ও নিয়ম সময়ের সঙ্গে বদলাতে পারে।

ধাঁধার উত্তরমালা ও শিক্ষকের নোট

শব্দ খোঁজার সমাধান

ই	ট	লে	ছ	ণ	লে	তা	বি	নি	ঘ	ল	মি	কে	ভ	ড
রা	র	র	ঈ	তি	গ	ই	সে	ল	ভ	মা	ণ	জে	ঘ	চ
ই	দ্ধা	হ	ণ	দ	নে	স	ঝ	কা	গ	জ	রা	ফ	ঘ	উ
সে	রু	জি	আ	ড	প	পা	ধ	দ	জি	ই	কি	না	লি	ই
রে	ন	ফ	চ	ব	এ	দি	শ	জা	রা	দে	ন	ট	মে	র
ক	পু	সি	দ	ঠ	ন	হ	আ	সা	শ	মে	ট্রো	জা	ন	দে
রা	কি	ঋ	তে	না	ক্রি	নে	ছ	ই	য	প	উ	অ	উ	ঋ
র	মা	বা	য	ফ	প	বা	ম	দে	সো	তি	ভ	ঘ	রে	ষ
য়্যা	ফ	ঘ	দ	হ	শ	স	ভ	রি	মি	লে	ঢ	ষ	ষ	রি
ও	সি	না	তি	তা	ন	ড	ঊ	নি	রা	কি	শ	থ	সে	ঊ
ল	কো	ল্ড	ব্যা	ক	আ	প	লি	গ	নি	জা	পি	ন	ঋ	আ
ম্যা	জি	লি	ট	ভ	ণ	জে	গ	স	ঘ	রে	দি	মি	ক্র	ঋ
পা	উ	অ	জে	কা	গ	ম	আ	ঘ	কি	ঘ	ঝ	ম	ণ	ধ
গ	সি	রি	শ	ছ	দ	সে	জি	নি	ঝ	রে	ণ	পে	জ	আ
আ	রে	মা	স	মে	তি	দে	রি	ফ	সি	তি	সে	খ	স	বে

ক্রসওয়ার্ডের সমাধান



ক্রসওয়ার্ড সমাধানের জন্য শিক্ষকের নির্দেশিকা

পাশাপাশি

2 পাশাপাশি: আক্রমণ সিস্টেম বা ব্যবহারকারীর ওপর চালানো ক্ষতিকর প্রচেষ্টা (4 অক্ষর)

4 পাশাপাশি: এনক্রিপশন ফাইলকে ক্রিপ্টোগ্রাফিক উপায়ে তালাবদ্ধ করা (6 অক্ষর)

5 পাশাপাশি: ম্যালওয়্যার ক্ষতি করার উদ্দেশ্যে তৈরি যেকোনো ক্ষতিকর সফটওয়্যার (5 অক্ষর)

7 পাশাপাশি: ট্রোজান নিরীহ ফাইলের ছদ্মবেশে ক্ষতিকর ফাইল (3 অক্ষর)

উপর-নিচ

1 উপর-নিচ: কোল্ডব্যাকআপ বিচ্ছিন্ন অফলাইন কপি (6 অক্ষর)

2 উপর-নিচ: আইসোলেশন সংক্রমিত নেটওয়ার্ক সিস্টেম বিচ্ছিন্ন করা (6 অক্ষর)

3 উপর-নিচ: পুনরুদ্ধার ব্যাকআপ থেকে ডেটাবেস ফিরিয়ে আনা (5 অক্ষর)

6 উপর-নিচ: লগইন নাম ও পাসওয়ার্ড দিয়ে অ্যাকাউন্টে প্রবেশের প্রক্রিয়া (4 অক্ষর)

এলোমেলো শব্দ ও সংকেতবার্তা সমাধানের উত্তরমালা

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

শব্দ সাজানোর উত্তরমালা

1. ক্রিএপশনন	এনক্রিপশন	5. কব্যাপকোআল্ড	কোল্ডব্যাকআপ
2. নআসোশলেই	আইসোলেশন	6. দ্ধাপুরুরন	পুনরুদ্ধার
3. নজাট্রো	ট্রোজান	7. য়্যারম্যাওল	ম্যালওয়্যার
4. নইলগ	লগইন	8. আণমক্র	আক্রমণ

গোপন সংকেত চ্যালেঞ্জের উত্তরমালা

"কোল্ড ব্যাকআপে ডেটা ফিরিয়ে আনুন"

কেস স্টাডির উত্তর

A কেস স্টাডি 1: এন্টারপ্রাইজ র‍্যানসমওয়্যার পেলোড নিয়ন্ত্রণ

শিক্ষকের সমাধান

মূল্যায়ন নির্দেশিকা

শিক্ষার্থীদের উত্তরে নিচের বিষয়গুলো থাকা উচিত:

- পরিস্থিতি বিশ্লেষণ: একটি কর্পোরেট লোকাল এরিয়া নেটওয়ার্ক সক্রিয় র‍্যান্সমওয়্যারে আক্রান্ত হয়েছে। মূল ফাইল সার্ভারগুলোর ফাইল এক্সটেনশন .locked দেখাতে শুরু করেছে।
- প্রস্তাবিত কৌশল ও সমাধান: প্রভাবিত সব সার্ভার লোকাল এরিয়া নেটওয়ার্ক থেকে বিচ্ছিন্ন করুন। সক্রিয় প্রশাসনিক সেশন বন্ধ করুন। নিরাপদ, রাইট-লকড অফলাইন ব্যাকআপ সিস্টেম থেকে অক্ষত ফাইল পুনরুদ্ধার করুন।

B কেস স্টাডি 2: অফলাইন ব্যাকআপ আর্কিটেকচার মূল্যায়ন

শিক্ষকের সমাধান

মূল্যায়ন নির্দেশিকা

শিক্ষার্থীদের উত্তরে নিচের বিষয়গুলো থাকা উচিত:

- পরিস্থিতি বিশ্লেষণ: একটি এন্টারপ্রাইজ এমন একটি ডেটা ব্যাকআপ কৌশল তৈরি করতে চায়, যা প্রাথমিক লোকাল নেটওয়ার্ক র‍্যানসমওয়্যারে সম্পূর্ণ দখল হয়ে গেলেও ব্যাকআপ আপস হওয়ার ঝুঁকি কমায়।
- প্রস্তাবিত কৌশল ও সমাধান: write-once-read-many (WORM) স্টোরেজ চালু করুন। ব্যাকআপ সিস্টেমকে সব নেটওয়ার্ক থেকে বিচ্ছিন্ন করে একটি লজিক্যাল এয়ার-গ্যাপ তৈরি করুন এবং প্রতিদিন ফিজিক্যাল মিডিয়া ঘোরানো বাধ্যতামূলক করুন।