Họ tên: _____ Ngày: _____ Điểm: _____

Phần mềm diệt virus và thiết bị đầu cuối Hướng dẫn bảo vệ

Phát hiện theo chữ ký, heuristic, giám sát hành vi, sandbox, cập nhật

TỔNG QUAN HỌC TẬP VỀ PHẦN MỀM DIỆT VIRUS

ĐÃ BẢO MẬT
MÃ HÓA DỮ LIỆU
Chuẩn AES 256 bit

TUÂN THỦ
TIÊU CHUẨN TOÀN CẦU
Khung GDPR và CCPA

ZERO TRUST
CHÍNH SÁCH TRUY CẬP
Xác thực đa yếu tố

Chào mừng bạn! Bộ hoạt động này hướng dẫn bạn về phần mềm diệt virus và bảo vệ điểm cuối. Bạn sẽ khám phá cơ sở dữ liệu chữ ký, trình quét heuristic, giám sát hành vi, tệp ảo trong sandbox và cách giảm thiểu cảnh báo sai.

CÁC ĐIỂM KIỂM TRA CỦA PHIẾU HỌC TẬP

- ☐ **Phần 1-4: Nắm vững an ninh mạng và phòng chống mối đe dọa.**
- ☐ **Phần 5-7: Giải các câu đố ô chữ và tìm từ.**
- ☐ **Phần 8-9: Giải các nghiên cứu tình huống và thử thách mật thư.**
- ☐ **Phần 10: Xem lại các trang câu hỏi thường gặp cơ bản và nâng cao.**
- ☐ **Phần 11: Khám phá 10 sự thật thú vị trong thực tế.**
- ☐ **Thưởng: thử thách Nghĩ nhanh.**

Mở Hướng dẫn an ninh mạng của VPN.com

URL: https://www.vpn.com/vi/an-ninh-mang/phan-mem-diet-virus/

Lộ trình học về chiến lược diệt virus của bạn

- Phân biệt phát hiện phần mềm độc hại dựa trên chữ ký và dựa trên heuristic.
- Hiểu về giám sát hành vi và các giao thức cô lập sandbox.
- Đánh giá tác động của quét theo thời gian thực đến hiệu suất hệ thống và các điểm cuối.
- Giảm thiểu việc phân loại nhầm (dương tính giả) bằng cách xác minh chứng chỉ số.
- Quản lý việc phân phối bản cập nhật định nghĩa hằng ngày trên các thiết bị đầu cuối của doanh nghiệp.

HƯỚNG DẪN PHẦN MỀM DIỆT VIRUS

Trả lời các câu hỏi trắc nghiệm và đúng/sai, hoàn thành các câu điền vào chỗ trống bằng ngân hàng từ, ghép các định nghĩa, rồi giải ô chữ và tìm từ. Hãy vận dụng kiến thức của bạn về bảo mật diệt virus cho thiết bị đầu cuối. Kết thúc với hoạt động thưởng Nghĩ nhanh.

BẢO VỆ CHỐNG VIRUS VÀ QUÉT CHỮ KÝ (GIỚI THIỆU)

Phần mềm diệt virus bảo vệ thiết bị đầu cuối bằng cách phát hiện, cách ly và loại bỏ phần mềm độc hại. Các hệ thống hiện đại kết hợp cơ sở dữ liệu chữ ký (đối chiếu mã băm của mối đe dọa đã biết) với phương pháp heuristic (phân tích cấu trúc tệp) và giám sát hành vi để phát hiện khai thác zero-day.

ĐỌC KỸ TỪNG ĐIỂM KIỂM TRA VÀ CHỌN HOẶC VIẾT CÂU TRẢ LỜI ĐÚNG

Điểm kiểm tra 1: Thử thách trắc nghiệm

1. **1. Hạn chế của phương pháp phát hiện dựa trên chữ ký là gì?**
   - A. Không thể nhận diện phần mềm độc hại chưa biết hoặc đã bị sửa đổi
   - B. Tạo ra tỷ lệ dương tính giả cao
   - C. Nó đòi hỏi sức mạnh xử lý CPU cao
   - D. Nó chỉ hoạt động khi được kết nối internet

2. **2. Trình quét heuristic phát hiện các biến thể phần mềm độc hại mới bằng cách nào?**
   - A. Bằng cách nhận diện các mẫu và cấu trúc mã đáng ngờ
   - B. Bằng cách đối chiếu mã băm tệp với cơ sở dữ liệu mối đe dọa
   - C. Bằng cách tự động xóa mọi tệp thực thi không có chữ ký
   - D. Bằng cách tải mọi tệp lên thư mục đám mây công cộng

3. **3. Mục đích của việc thực thi trong sandbox của phần mềm diệt virus là gì?**
   - A. Cô lập và phân tích tệp trong một hầm ảo an toàn
   - B. Tăng tốc việc truyền sao lưu hệ thống tệp cục bộ
   - C. Cập nhật các bản vá bảo mật của hệ điều hành cục bộ
   - D. Nén các tệp tài liệu lớn để tiết kiệm dung lượng lưu trữ

4. **4. Phương pháp phát hiện nào gắn cờ hành vi đe dọa theo thời gian thực?**
   - A. Phân tích hành vi giám sát các hành động của phần mềm
   - B. Kiểm tra nhật ký lịch sử được thực hiện qua đêm
   - C. Người dùng tự báo cáo các ứng dụng chậm
   - D. Xem xét thủ công hằng tuần các chương trình đã cài đặt

5. **5. Vì sao việc cập nhật định nghĩa thường xuyên lại quan trọng đối với các trình quét?**
   - A. Để cung cấp các định danh mối đe dọa cho cơ sở dữ liệu của công cụ nhận diện chữ ký
   - B. Tăng xung nhịp CPU trong khi hoạt động
   - C. Để thay đổi thời gian lưu đệm máy chủ tên DNS toàn cầu
   - D. Để cho phép các cài đặt cookie của trình duyệt web

Điểm kiểm tra 2: Thử thách Đúng hoặc Sai

6 Câu hỏi đúng/sai 6

6. Phát hiện theo chữ ký đối chiếu mã băm mật mã của tệp với danh sách trong cơ sở dữ liệu.

○ Đúng ○ Sai

7 Câu hỏi đúng/sai 7

7. Trình quét heuristic có thể kích hoạt cảnh báo dương tính giả trên các tệp an toàn.

○ Đúng ○ Sai

8 Câu hỏi đúng/sai 8

8. Sandbox cho phép phần mềm độc hại truy cập tệp mạng mà không giới hạn.

○ Đúng ○ Sai

9 Câu hỏi đúng/sai 9

9. Quét theo hành vi chặn tệp khi chúng có hành động độc hại.

○ Đúng ○ Sai

10 Câu hỏi đúng/sai 10

10. Phần mềm diệt virus tiêu chuẩn ngăn chặn hoàn toàn mọi cuộc tấn công zero-day.

○ Đúng ○ Sai

Điểm kiểm tra 3: Điền thuật ngữ chính

Đọc từng câu dưới đây và điền vào chỗ trống thuật ngữ đúng từ Ngân hàng từ.

1. Trình quét truyền thống dựa vào việc đối sánh _____ để nhận diện phần mềm độc hại đã biết.

2. Việc phân tích các mẫu mã của tệp được gọi là quét _____ .

3. Phần mềm diệt virus cách ly các tệp đáng ngờ trong một môi trường _____ .

4. Cách theo dõi hành động của chương trình trong thời gian thực để phát hiện hoạt động đáng ngờ gọi là _____ .

5. Trình quét tải về _____ cơ sở dữ liệu hằng ngày để nhận diện các mối đe dọa mới.

6. Chương trình an toàn bị đánh dấu là phần mềm độc hại sẽ gây ra cảnh báo dương tính giả, hay còn gọi là _____ .

NGÂN HÀNG TỪ VỰNG

BẢN CẬP NHẬT | BÁO ĐỘNG GIẢ | CÁCH LY | CHỮ KÝ BĂM | DIỆT VIRUS | HEURISTIC | QUÉT HÀNH VI | SANDBOX

Viết câu trả lời của bạn tại đây:

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

Điểm kiểm tra 4: Ghép nối khái niệm bảo mật

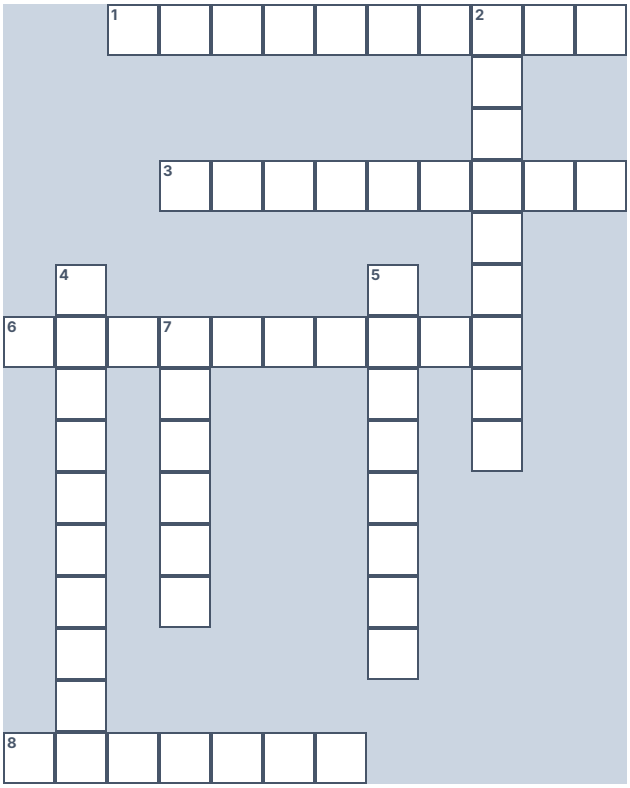
GHÉP ĐỊNH NGHĨA

Ghép mỗi thuật ngữ từ vựng ở bên trái với định nghĩa đúng ở bên phải bằng cách nhập chữ cái tương ứng (A-H) vào ô nhập liệu.

☐	1. Chữ ký băm	A	Cô lập các tệp đáng ngờ để ngăn hệ thống cục bộ bị phơi nhiễm.
☐	2. Phương pháp heuristic mã	B	Bộ phần mềm quét và bảo vệ các điểm cuối khỏi các lỗ hổng bị khai thác.
☐	3. Hộp cát tệp	C	Giám sát các hành động của phần mềm đang chạy để phát hiện mẫu hoạt động độc hại.
☐	4. Quét hành vi	D	Dấu vân tay cơ sở dữ liệu mật mã duy nhất dùng để nhận dạng các mối đe dọa đã biết.
☐	5. Cập nhật hằng ngày	E	Môi trường kiểm thử ảo an toàn chạy mã không đáng tin cậy một cách an toàn.
☐	6. Dương tính giả	F	Tải xuống định nghĩa thường xuyên để cung cấp cho cơ sở dữ liệu mối đe dọa.
☐	7. Cô lập mối đe dọa	G	Phân tích dựa trên quy tắc, đánh dấu các tệp có bố cục mã đáng ngờ.
☐	8. Công cụ diệt virus	H	Cảnh báo bảo mật phân loại nhầm phần mềm an toàn là phần mềm độc hại.

Điểm kiểm tra 5: Trò chơi ô chữ

Giải ô chữ bằng cách nhập chữ cái vào các ô trắng đang hoạt động. Các số tương ứng với các gợi ý bên dưới.



HÀNG NGANG

1. Giám sát hành động của phần mềm đang chạy để tìm các mẫu hoạt động độc hại (10)

3. Bộ phần mềm quét và bảo vệ các thiết bị đầu cuối khỏi các mã khai thác (9)

6. Các bản định nghĩa được tải về đều đặn để bổ sung cho cơ sở dữ liệu mối đe dọa (10)

8. Môi trường kiểm thử ảo an toàn để chạy mã không đáng tin cậy một cách an toàn (7)

HÀNG DỌC

2. Phân tích dựa trên quy tắc, đánh dấu các tệp có cấu trúc mã đáng ngờ (9)

4. Cảnh báo bảo mật phân loại nhầm phần mềm an toàn thành phần mềm độc hại (10)

5. Dấu vân tay mật mã duy nhất trong cơ sở dữ liệu, dùng để nhận diện các mối đe dọa đã biết (8)

7. Giam các tệp đáng ngờ lại để tránh gây nguy cơ cho hệ thống cục bộ (6)

Điểm kiểm tra 5, phương án khác: Gợi ý ô chữ dễ tiếp cận

Người dùng trình đọc màn hình và bàn phím có thể nhập trực tiếp đáp án ô chữ vào các trường văn bản bên dưới. GỢI Ý HÀNG NGANG GỢI Ý HÀNG DỌC

HÀNG NGANG

1 hàng ngang: Giám sát hành động của phần mềm đang chạy để tìm các mẫu hoạt động độc hại (10 chữ cái):

3 hàng ngang: Bộ phần mềm quét và bảo vệ các thiết bị đầu cuối khỏi các mã khai thác (9 chữ cái):

6 hàng ngang: Các bản định nghĩa được tải về đều đặn để bổ sung cho cơ sở dữ liệu mối đe dọa (10 chữ cái):

8 hàng ngang: Môi trường kiểm thử ảo an toàn để chạy mã không đáng tin cậy một cách an toàn (7 chữ cái):

HÀNG DỌC

2 hàng dọc: Phân tích dựa trên quy tắc, đánh dấu các tệp có cấu trúc mã đáng ngờ (9 chữ cái):

4 hàng dọc: Cảnh báo bảo mật phân loại nhầm phần mềm an toàn thành phần mềm độc hại (10 chữ cái):

5 hàng dọc: Dấu vân tay mật mã duy nhất trong cơ sở dữ liệu, dùng để nhận diện các mối đe dọa đã biết (8 chữ cái):

7 hàng dọc: Giam các tệp đáng ngờ lại để tránh gây nguy cơ cho hệ thống cục bộ (6 chữ cái):

Điểm kiểm tra 6: Tìm từ ẩn

Tìm 8 thuật ngữ từ vựng chính ẩn trong lưới bên dưới. Các từ có thể nằm ngang, dọc hoặc chéo.

S Q R D K H Ă D A Ă Â O V K I
V K V S I C Ơ I M H C C G M M
T I Ơ Ô E M M Ê Ơ P H Q S R E
Â Y Â Q Ơ O Ê T Q Â Ư U C R X
H L T Â Y Q U V Đ I K Ê Y B B
N H M C Ơ U Ư I Ô Â Y S Ă A A
P C Y N C E K R H A B C O O C
Â A D E G T B U E S Ă P Ơ Đ L
C C D G Q H Y S U A M Q Đ Ô Ơ
N U D A A A Ơ O R N M Ô S N V
A Ơ I P S N Q B I D M X Ă G Đ
B Q Ư Ư H H A P S B Y X X G K
E G M P I V L L T O R O Ê I Ơ
Ơ E Y A O I T Đ I X T Â X A P
X Ă Ê L Y E H N C Ô N Ư Â L Y

DANH SÁCH TỪ VỰNG

CHƯKYBĂM HEURISTIC SANDBOX QUETHANHVI BANCÂPNHÂT BAOĐÔNGGIA CACHLY DIÊTVIRUS

Điểm kiểm tra 6, phương án khác: Ghép từ vựng dễ tiếp cận

Ghép từng thuật ngữ trong số 8 thuật ngữ từ vựng ở phần Tìm từ với định nghĩa đúng bằng cách viết chữ cái (A-H) vào chỗ trống.

THUẬT NGỮ TỪ VỰNG
A. CHƯKYBĂM
B. HEURISTIC
C. SANDBOX
D. QUETHANHVI
E. BANCẬPNHẬT
F. BAOĐÔNGGIA
G. CACHLY
H. DIÊTVIRUS

ĐỊNH NGHĨA VÀ CÁC TRƯỜNG GHÉP
☐ 1. Giám sát hành động của phần mềm đang chạy để tìm các mẫu hoạt động độc hại.
☐ 2. Bộ phần mềm quét và bảo vệ các thiết bị đầu cuối khỏi các mã khai thác.
☐ 3. Các bản định nghĩa được tải về đều đặn để bổ sung cho cơ sở dữ liệu mối đe dọa.
☐ 4. Phân tích dựa trên quy tắc, đánh dấu các tệp có cấu trúc mã đáng ngờ.
☐ 5. Giam các tệp đáng ngờ lại để tránh gây nguy cơ cho hệ thống cục bộ.
☐ 6. Dấu vân tay mật mã duy nhất trong cơ sở dữ liệu, dùng để nhận diện các mối đe dọa đã biết.
☐ 7. Môi trường kiểm thử ảo an toàn để chạy mã không đáng tin cậy một cách an toàn.
☐ 8. Cảnh báo bảo mật phân loại nhầm phần mềm an toàn thành phần mềm độc hại.

Điểm kiểm tra 7: Thử thách từ bị xáo trộn

Sắp xếp lại các chữ cái bên dưới để tìm ra các khái niệm và thuật ngữ chính về an ninh mạng. Viết đáp án của bạn vào các ô nhập đã cung cấp.

1. **ĂKYCBHMƯ** _____

2. **SNXOBDA** _____

3. **BPÂNAÂTCHN** _____

4. **YHCLCA** _____

5. **TIECSRHIU** _____

6. **VHTNHQUAIE** _____

7. **AĐBGNGIAÔO** _____

8. **SVUDTIIRÊ** _____

Hoạt động thưởng: Nghĩ nhanh

3 CÂU TRẢ LỜI CHO MỖI CHỦ ĐỀ. AI HOÀN THÀNH DANH SÁCH TRƯỚC SẼ THẮNG.

1	Lý do cập nhật phần mềm			
2	Những người bạn có thể nhờ giúp về CNTT			
3	Những việc cần làm khi phần mềm diệt virus phát hiện điều gì đó			
4	Những dấu hiệu của virus máy tính			
5	Những thứ bị cách ly			
6	Những nơi virus ẩn náu			
7	Những thông tin bạn không bao giờ nên chia sẻ			
8	Những loại phần mềm độc hại			
9	Những công cụ bảo mật bạn biết			
10	Những thứ mà phần mềm diệt virus quét			
11	Những thứ bạn sao lưu			
12	Những thiết bị có thể bị tấn công			
13	Những chương trình diệt virus bạn biết			
14	Lý do báo động giả			
15	Những thói quen an toàn bạn có thể bắt đầu ngay hôm nay			

Điểm kiểm tra 8: Nghiên cứu tình huống về an ninh mạng

Hãy vận dụng các khái niệm bạn đã học để giải các tình huống thực tế dưới đây.

NGHIÊN CỨU TÌNH HUỐNG 1: QUÉT THEO CHỮ KÝ VÀ QUÉT HEURISTIC

👷

Tình huống: Một nhân viên tải xuống một tiện ích tùy chỉnh do một nhóm khác xây dựng nội bộ. Trình quét theo chữ ký cho qua, nhưng trình quét heuristic gắn cờ nó là đáng ngờ.

Câu hỏi thảo luận: Hãy giải thích vì sao điều này xảy ra, và cách xác minh tệp có an toàn hay không.

NGHIÊN CỨU TÌNH HUỐNG 2: XỬ LÝ CẢNH BÁO SAI

👷

Tình huống: Một nhà phát triển phần mềm biên dịch ứng dụng của mình. Phần mềm diệt virus của hệ thống gắn cờ tệp thực thi mới là phần mềm độc hại và cách ly nó.

Câu hỏi thảo luận: Hãy nêu các rủi ro của việc đưa vào danh sách cho phép (whitelist), và mô tả cách xử lý đúng đắn.

Điểm kiểm tra 9: Giải mã mật thư

Chuyên gia an ninh mạng bảo vệ tài sản mạng khỏi các tác nhân đe dọa trực tuyến. Hãy dùng bảng khóa Chữ-Số bên dưới để giải mã thông điệp bằng cách viết các chữ cái tương ứng vào chỗ trống.

KHÓA MÃ HÓA CHỮ SANG SỐ

A=1 Ă=2 Â=3 B=4 C=5 D=6 Đ=7 E=8 Ê=9 G=10

H=11 I=12 K=13 L=14 M=15 N=16 O=17 Ô=18 Ơ=19 P=20

Q=21 R=22 S=23 T=24 U=25 Ư=26 V=27 X=28 Y=29

20	11	1	24		11	12	9	16		15	1		7	18	5		15	19	12
				4	2	16	10		20	11	3	16		24	12	5	11		
						11	8	25	22	12	23	24	12	5					

Thông điệp đã giải mã:

MẸO: MỖI SỐ ĐẠI DIỆN CHO VỊ TRÍ CỦA CHỮ CÁI ĐÓ TRONG BẢNG CHỮ CÁI (VÍ DỤ 1 = A, 2 = B, 29 = Y).

Điểm kiểm tra 10: Câu hỏi thường gặp cơ bản về an ninh mạng (Phần A)

Xem lại các câu hỏi và câu trả lời thường gặp về cách giảm thiểu các mối đe dọa trực tuyến.

Q1: Phần mềm diệt virus nhận diện phần mềm độc hại như thế nào?

Nó nhận diện phần mềm độc hại bằng đối sánh chữ ký trong cơ sở dữ liệu, phân tích cấu trúc mã heuristic và giám sát hành vi theo thời gian thực.

Q2: Phát hiện dựa trên chữ ký là gì?

Đây là phương pháp quét đối sánh các giá trị băm mật mã của tệp với danh sách trong cơ sở dữ liệu về các mối đe dọa phần mềm độc hại đã biết.

Q3: Trình quét heuristic là gì?

Heuristic phân tích cấu trúc và các lệnh mã của một tệp, gắn cờ các mẫu đáng ngờ thường gặp ở các biến thể phần mềm độc hại.

Q4: Tệp bị cách ly nghĩa là gì?

Phần mềm diệt virus chuyển tệp vào một thư mục an toàn, cô lập, chặn việc thực thi để bảo vệ hệ điều hành.

Q5: Dương tính giả của phần mềm diệt virus là gì?

Đây là lỗi khi phần mềm hợp pháp, an toàn bị các thuật toán quét gắn cờ nhầm là phần mềm độc hại.

Điểm kiểm tra 10: Câu hỏi thường gặp cơ bản về an ninh mạng (Phần B)

Xem lại các câu hỏi và câu trả lời thường gặp về cách giảm thiểu các mối đe dọa trực tuyến.

Q6: Giám sát hành vi bảo vệ hệ thống như thế nào?

Nó giám sát phần mềm đang chạy theo thời gian thực, chặn các tiến trình cố thực hiện thay đổi đáng ngờ như chèn mã.

Q7: Vì sao kiểm thử sandbox quan trọng?

Sandbox chạy các tệp không đáng tin cậy trong một máy ảo cô lập, quan sát hành vi một cách an toàn mà không để lộ hệ thống.

Q8: Định nghĩa virus của phần mềm diệt virus nên được cập nhật bao lâu một lần?

Trình quét nên cập nhật định nghĩa hằng ngày hoặc hằng giờ để nhận diện các chủng phần mềm độc hại mới phát hiện.

Q9: Phần mềm diệt virus và EDR khác nhau như thế nào?

Phần mềm diệt virus tập trung vào quét tệp, còn Endpoint Detection and Response (EDR) theo dõi và ngăn chặn mối đe dọa trên toàn mạng.

Q10: Tôi có thể chạy hai chương trình diệt virus cùng lúc không?

Không. Chạy hai trình quét hoạt động cùng lúc gây xung đột hệ thống, làm chậm hiệu năng và có thể chặn hoạt động của nhau.

Điểm kiểm tra 10: Câu hỏi thường gặp nâng cao về bảo mật (Phần C)

Khám phá các khía cạnh kỹ thuật nâng cao của khung bảo mật, phân tích phần mềm độc hại và tuân thủ dữ liệu.

Q1: Các quy tắc heuristic giảm thiểu việc né mối đe dọa như thế nào?

Heuristic phân tích các mẫu đe dọa chung thay vì chữ ký cụ thể, nhờ đó phát hiện các biến thể đã sửa đổi của các họ phần mềm độc hại đã biết.

Q2: Virus đa hình là gì?

Đây là phần mềm độc hại thay đổi bố cục tệp và quy trình giải mã sau mỗi lần thực thi, khiến việc quét chữ ký không hiệu quả.

Q3: Sandbox phát hiện hành vi né tránh máy ảo như thế nào?

Các hộp cát (sandbox) hiện đại mô phỏng thao tác nhấp chuột và thời gian hoạt động của hệ thống, đánh lừa phần mềm độc hại được thiết kế để ẩn mình khi chạy trong máy ảo.

Q4: Các định dạng tải xuống bản cập nhật chữ ký là gì?

Các bản cập nhật thường là các tệp chênh lệch nhị phân tăng dần nhẹ, giảm thiểu mức tiêu thụ băng thông mạng của máy khách.

Q5: Tác nhân điểm cuối quản lý các lần quét cục bộ như thế nào?

Các tác nhân thực hiện kiểm tra nền nhẹ, chuyển việc tra cứu băm mật mã sâu sang các cơ sở dữ liệu mối đe dọa trên đám mây.

Điểm kiểm tra 10: Câu hỏi thường gặp nâng cao về bảo mật (Phần D)

Khám phá các khía cạnh kỹ thuật nâng cao của khung bảo mật, phân tích phần mềm độc hại và tuân thủ dữ liệu.

Q6: Quét phát hiện rootkit là gì?

Nó quét các bảng bộ nhớ cấp nhân, vượt qua các API hệ điều hành mà rootkit móc vào để ẩn các luồng đang hoạt động của chúng.

Q7: Quét hành vi chặn ransomware như thế nào?

Nó phát hiện các vòng lặp mã hóa tệp hàng loạt tự động, chấm dứt tiến trình máy chủ trước khi cơ sở dữ liệu hệ thống bị khóa.

Q8: Xác minh chứng chỉ ký mã là gì?

Trình quét kiểm tra chữ ký số của mã so với các tổ chức cấp chứng chỉ gốc đáng tin cậy, xác thực danh tính nhà phát triển phần mềm.

Q9: Packer ảnh hưởng thế nào đến các công cụ quét?

Trình đóng gói (packer) nén hoặc mã hóa dữ liệu của phần mềm độc hại. Trình quét phải giải nén tệp trong bộ nhớ trước khi so khớp chữ ký.

Q10: Các công cụ EDR tự động hóa việc cô lập như thế nào?

Các tác nhân EDR cách ly các điểm cuối bị xâm nhập ở cấp mạng, chặn di chuyển ngang đồng thời vẫn cho phép nhà phân tích truy cập.

Phần 11: 10 sự thật và hiểu biết thực tế về an ninh mạng

Xem lại các sự thật thực tế về vi phạm bảo mật, cơ chế phòng thủ và tiêu chuẩn tuân thủ.

1. THÔNG TIN VỀ AN NINH

Cơ sở dữ liệu chữ ký lưu mã băm của phần mềm độc hại đã biết, nên các tệp hoàn toàn mới hoặc bị thay đổi sẽ bị bỏ sót cho đến khi định nghĩa được cập nhật.

2. THÔNG TIN VỀ AN NINH

Công cụ heuristic có thể gắn cờ một số biến thể phần mềm độc hại mới trước khi có chữ ký, đổi lại là nhiều kết quả dương tính giả hơn.

3. THÔNG TIN VỀ AN NINH

Cảnh báo dương tính giả khiến các nhóm CNTT mất thời gian xác minh và khôi phục các tệp bị cách ly nhầm.

4. THÔNG TIN VỀ AN NINH

Phần mềm độc hại đa hình thay đổi mã của nó ở mỗi bản sao, nên bên phòng thủ kết hợp chữ ký với các kiểm tra heuristic và hành vi.

6. THÔNG TIN VỀ AN NINH

Tác giả phần mềm độc hại viết mã tùy chỉnh để kiểm tra môi trường hộp cát, trì hoãn việc thực thi nhằm vượt qua bộ hẹn giờ.

5. THÔNG TIN VỀ AN NINH

Các công cụ diệt virus trên đám mây đối chiếu hàm băm của tệp đáng ngờ với các cơ sở dữ liệu mối đe dọa trực tuyến lớn gần như theo thời gian thực.

7. THÔNG TIN VỀ BẢO MẬT

Các nhà cung cấp thường xuyên đẩy cập nhật định nghĩa tới các điểm cuối để trình quét nhận diện được các mối đe dọa mới được xác nhận.

8. THÔNG TIN VỀ BẢO MẬT

Trình giám sát hành vi ransomware nhắm vào các lệnh gọi API Win32 cụ thể liên quan đến mã hóa tệp và xóa bản sao bóng.

9. THÔNG TIN VỀ BẢO MẬT

Chữ ký mã hợp lệ có thể giảm rủi ro báo động giả, nhưng các tệp đã ký vẫn được quét, vì phần mềm độc hại cũng có thể được ký.

10. THÔNG TIN VỀ AN NINH

Rootkit sửa đổi cấu trúc nhân hệ thống, đòi hỏi các trình quét chuyên dụng lúc khởi động để phát hiện và dọn dẹp.

Tài liệu tham khảo kỹ thuật và nguồn

Tài liệu học tập và các câu đố tương tác được biên soạn từ các tiêu chuẩn toàn cầu của NIST, OWASP và tuân thủ quyền riêng tư dữ liệu. TÀI LIỆU HỌC THUẬT VÀ NGÀNH

TÀI LIỆU THAM KHẢO HỌC THUẬT VÀ NGÀNH

[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

Đáp án: Điểm kiểm tra 1 – Trắc nghiệm

1 Câu hỏi 1 CHỮ KÝ **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Quét theo chữ ký dựa vào hàm băm đã biết trong cơ sở dữ liệu, nên không phát hiện được phần mềm độc hại chưa biết hoặc đã bị sửa đổi. Trích dẫn: OWASP Secure Configuration.

2 Câu hỏi 2 HEURISTIC **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Heuristic phân tích bố cục mã và các lệnh để xác định các đặc điểm đáng ngờ của biến thể mối đe dọa mới. Trích dẫn: Center for Internet Security (CIS).

3 Câu hỏi 3 CÁCH LY SANDBOX **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Sandbox chạy các tệp đáng ngờ trong máy ảo cô lập để quan sát hành vi thực thi một cách an toàn. Trích dẫn: NIST Digital Identity.

4 Câu hỏi 4 THEO HÀNH VI **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Quét hành vi giám sát các chương trình đang chạy theo thời gian thực để chặn các thay đổi hệ thống trái phép. Trích dẫn: Center for Internet Security (CIS).

5 Câu hỏi 5 CÁC BẢN CẬP NHẬT **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Trình quét tải xuống các bản cập nhật định nghĩa tăng dần hằng ngày để luôn đồng bộ với bối cảnh mối đe dọa. Trích dẫn: OWASP Secure Configuration.

Đáp án: Điểm kiểm tra 2 – Đúng hay Sai

6 **Câu hỏi 6** CHỮ KÝ **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Công cụ theo chữ ký tính hàm băm mật mã và đối chiếu với cơ sở dữ liệu các hàm băm mối đe dọa đã biết. Trích dẫn: OWASP Secure Configuration.

7 **Câu hỏi 7** HEURISTIC **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Công cụ heuristic chạy các bố cục dựa trên quy tắc có thể gắn cờ nhầm các tệp hợp pháp, an toàn là đáng ngờ. Trích dẫn: Center for Internet Security (CIS).

8 **Câu hỏi 8** CÁCH LY SANDBOX **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

Sandbox chạy mã trong container ảo, chặn nghiêm ngặt quyền truy cập vào các thư mục chia sẻ mạng. Trích dẫn: NIST Digital Identity.

9 **Câu hỏi 9** THEO HÀNH VI **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Giám sát theo thời gian thực gắn cờ các tiến trình đang chạy cố gắng ghi trái phép hoặc khóa tệp. Trích dẫn: Center for Internet Security (CIS).

10 **Câu hỏi 10** **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

Không có phần mềm diệt virus nào ngăn chặn được mọi cuộc tấn công zero-day; các mối đe dọa chưa biết có thể né được chữ ký và phương pháp heuristic.

Đáp án từ vựng và thang chấm điểm

Thang chấm điểm cho giáo viên: Cho 1 điểm với mỗi cặp ghép đúng (tổng cộng 8 điểm) và mỗi thuật ngữ ngữ cảnh (tổng cộng 6 điểm).

ĐIỂM KIỂM TRA 4: ĐÁP ÁN – GHÉP NỐI KHÁI NIỆM

D 1. Chữ ký băm	G 2. Phương pháp heuristic mã	E 3. Hộp cát tệp	C 4. Quét hành vi
F 5. Cập nhật hằng ngày	H 6. Dương tính giả	A 7. Cô lập mối đe dọa	B 8. Công cụ diệt virus

ĐIỂM KIỂM TRA 3: ĐÁP ÁN – THUẬT NGỮ CHÍNH

1 CHỮ KÝ BĂM	2 HEURISTIC	3 SANDBOX	4 QUÉT HÀNH VI
5 BẢN CẬP NHẬT	6 BÁO ĐỘNG GIẢ		

ĐIỂM KIỂM TRA 6, PHƯƠNG ÁN KHÁC: ĐÁP ÁN – GHÉP TỪ

1 D – QUETHANHVI	2 H – DIÊTVIRUS	3 E – BANCÂPNHÂT	4 B – HEURISTIC
5 G – CACHLY	6 A – CHƯKYBĂM	7 C – SANDBOX	8 F – BAOĐÔNGGIA

GHI CHÚ THẢO LUẬN CHO GIÁO VIÊN

Thuật ngữ chính:
Kiểm tra xem học sinh có giải thích được Chữ ký băm, Phương pháp heuristic mã và Hộp cát tệp bằng lời của mình và nêu một ví dụ cho mỗi thuật ngữ hay không.

Nghiên cứu tình huống:
Yêu cầu học sinh dùng dữ kiện trong phiếu, không dùng phỏng đoán, để chứng minh khuyến nghị của mình.

Đánh giá nguồn:
Yêu cầu học sinh kiểm chứng ít nhất một nhận định trong các nguồn của phiếu và thảo luận vì sao số liệu, giá cả và quy định có thể thay đổi theo thời gian.

Đáp án câu đố và ghi chú cho giáo viên

ĐÁP ÁN TÌM TỪ

S	Q	R	D	K	H	Ă	D	A	Ă	Â	O	V	K	I
V	K	V	S	I	C	Ơ	I	M	H	C	C	G	M	M
T	I	Ơ	Ô	E	M	M	Ê	Ơ	P	H	Q	S	R	E
Â	Y	Â	Q	Ơ	O	Ê	T	Q	Â	Ư	U	C	R	X
H	L	T	Â	Y	Q	U	V	Đ	I	K	Ê	Y	B	B
N	H	M	C	Ơ	U	Ư	I	Ô	Â	Y	S	Ă	A	A
P	C	Y	N	C	E	K	R	H	A	B	C	O	O	C
Â	A	D	E	G	T	B	U	E	S	Ă	P	Ơ	Đ	L
C	C	D	G	Q	H	Y	S	U	A	M	Q	Đ	Ô	Ơ
N	U	D	A	A	A	Ơ	O	R	N	M	Ô	S	N	V
A	Ơ	I	P	S	N	Q	B	I	D	M	X	Ă	G	Đ
B	Q	Ư	Ư	H	H	A	P	S	B	Y	X	X	G	K
E	G	M	P	I	V	L	L	T	O	R	O	Ê	I	Ơ
Ơ	E	Y	A	O	I	T	Đ	I	X	T	Â	X	A	P
X	Ă	Ê	L	Y	E	H	N	C	Ô	N	Ư	Â	L	Y

ĐÁP ÁN Ô CHỮ

		Q	U	E	T	H	A	N	H	V	I
									E		
									U		
			D	I	Ê	T	V	I	R	U	S
									I		
	B						C		S		
B	A	N	C	Â	P	N	H	Â	T		
	O		A				Ư		I		
	Đ		C				K		C		
	Ô		H				Y				
	N		L				B				
	G		Y				Ă				
	G						M				
	I										
S	A	N	D	B	O	X					

HÀNG NGANG

1 hàng ngang: QUETHANHVI Giám sát hành động của phần mềm đang chạy để tìm các mẫu hoạt động độc hại (10 chữ cái)

3 hàng ngang: DIÊTVIRUS Bộ phần mềm quét và bảo vệ các thiết bị đầu cuối khỏi các mã khai thác (9 chữ cái)

6 hàng ngang: BANCÂPNHÂT Các bản định nghĩa được tải về đều đặn để bổ sung cho cơ sở dữ liệu mối đe dọa (10 chữ cái)

8 hàng ngang: SANDBOX Môi trường kiểm thử ảo an toàn để chạy mã không đáng tin cậy một cách an toàn (7 chữ cái)

HÀNG DỌC

2 hàng dọc: HEURISTIC Phân tích dựa trên quy tắc, đánh dấu các tệp có cấu trúc mã đáng ngờ (9 chữ cái)

4 hàng dọc: BAOĐÔNGGIA Cảnh báo bảo mật phân loại nhầm phần mềm an toàn thành phần mềm độc hại (10 chữ cái)

5 hàng dọc: CHƯKYBĂM Dấu vân tay mật mã duy nhất trong cơ sở dữ liệu, dùng để nhận diện các mối đe dọa đã biết (8 chữ cái)

7 hàng dọc: CACHLY Giam các tệp đáng ngờ lại để tránh gây nguy cơ cho hệ thống cục bộ (6 chữ cái)

Đáp án: Từ bị xáo trộn và mật thư

Đáp án cho hoạt động sắp xếp lại chữ cái từ vựng và Thử thách mật mã bí mật.

ĐÁP ÁN SẮP XẾP LẠI CHỮ CÁI

1.	Ă K Y C B H M Ư	CHƯKYBĂM	5.	T I E C S R H I U	HEURISTIC
2.	S N X O B D A	SANDBOX	6.	V H T N H Q U A I E	QUETHANHVI
3.	B P Â N A Â T C H N	BANCÂPNHÂT	7.	A Đ B G N G I A Ô O	BAOĐÔNGGIA
4.	Y H C L C A	CACHLY	8.	S V U D T I I R Ê	DIÊTVIRUS

KHÓA THỬ THÁCH MẬT THƯ BÍ MẬT

"PHAT HIÊN MA ĐÔC MƠI BĂNG PHÂN TICH HEURISTIC"

Đáp án nghiên cứu tình huống

A Nghiên cứu tình huống 1: Quét theo chữ ký và quét heuristic

Lời giải dành cho giáo viên

HƯỚNG DẪN CHẤM ĐIỂM

Câu trả lời của học sinh cần đề cập các điểm sau:

- Phân tích tình huống: Một nhân viên tải xuống một tiện ích tùy chỉnh do một nhóm khác xây dựng nội bộ. Trình quét chữ ký cho qua, nhưng trình quét heuristic đánh dấu là đáng ngờ.
- Chiến lược và giải pháp đề xuất: Vì sao xảy ra: Quét chữ ký kiểm tra mã băm tệp; vì là tệp tùy chỉnh nên không có trong cơ sở dữ liệu mối đe dọa. Phương pháp heuristic phân tích cấu trúc và đánh dấu các hành vi đáng ngờ (ví dụ ghi registry). Xác minh: Chạy tệp trong sandbox để quan sát hành vi, kiểm tra chữ ký số và gửi mã băm lên các cổng thông tin tình báo mối đe dọa.

B Nghiên cứu tình huống 2: Xử lý cảnh báo sai

Lời giải dành cho giáo viên

HƯỚNG DẪN CHẤM ĐIỂM

Câu trả lời của học sinh cần đề cập các điểm sau:

- Phân tích tình huống: Một nhà phát triển phần mềm biên dịch ứng dụng của mình. Phần mềm diệt virus của hệ thống đánh dấu tệp thực thi mới là phần mềm độc hại và cách ly nó.
- Chiến lược và giải pháp đề xuất: Rủi ro khi đưa vào danh sách cho phép: Bỏ qua các trình quét có thể cho phép mã bị nhiễm thật chạy. Hướng giải quyết: Gửi tệp cho nhà cung cấp phần mềm diệt virus để phân tích, ký số mã bằng các tổ chức cấp chứng chỉ, và tạm thời cấu hình ngoại lệ cho thư mục cụ thể thay vì tắt phần mềm diệt virus.