이름: _____ 날짜: _____ 점수: _____

백신 소프트웨어와 엔드포인트 보호 가이드

시그니처 탐지, 휴리스틱, 행위 모니터링, 샌드박싱, 업데이트

백신 소프트웨어 학습 개요

보호됨
데이터 암호화
256비트 AES 표준

규정 준수
글로벌 표준
GDPR 및 CCPA 규정 체계

제로 트러스트
접근 정책
다중 요소 인증

환영합니다! 이 활동 자료집은 백신 소프트웨어와 엔드포인트 보호를 안내합니다. 시그니처 데이터베이스, 휴리스틱 검사기, 행위 모니터링, 샌드박스 가상 파일, 오탐 완화를 살펴봅니다.

워크시트 체크포인트

- [ ] 파트 1-4: 사이버 보안과 위협 예방을 익힙니다.
- [ ] 파트 5-7: 십자말풀이와 단어 찾기 퍼즐을 풉니다.
- [ ] 파트 8-9: 사례 연구와 암호 도전 과제를 풉니다.
- [ ] 파트 10: 기초 및 심화 FAQ 페이지를 살펴봅니다.
- [ ] 파트 11: 흥미로운 실제 사실 10가지를 살펴봅니다.
- [ ] 보너스: 빠르게 생각하기 도전

VPN.com 사이버 보안 가이드 열기

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

나의 백신 전략 학습 로드맵

- 시그니처 기반 악성코드 탐지와 휴리스틱 기반 악성코드 탐지를 구분하세요.
- 행동 모니터링과 샌드박스 격리 프로토콜을 이해합니다.
- 실시간 검사가 시스템 성능과 엔드포인트에 미치는 영향을 평가하세요.
- 디지털 인증서 검증을 사용해 오탐 분류를 줄입니다.
- 기업 엔드포인트 전반에 걸친 일일 정의 업데이트 배포를 관리합니다.

백신 가이드 안내

객관식과 참/거짓 문제에 답하고, 단어 은행을 사용해 빈칸을 채우고, 정의를 연결하고, 십자말풀이와 단어 찾기 퍼즐을 푸세요. 엔드포인트 백신 보안에 대한 지식을 적용해 보세요. 마지막으로 보너스 활동인 빠르게 생각하기를 해 보세요.

백신 보호 및 시그니처 검사(소개)

백신 소프트웨어는 악성코드를 식별, 격리, 제거하여 엔드포인트를 보호합니다. 최신 시스템은 시그니처 데이터베이스(알려진 위협의 해시와 대조), 휴리스틱(파일 구조 분석), 행위 모니터링을 결합하여 제로데이 공격을 탐지합니다.

각 체크포인트를 주의 깊게 읽고 올바른 답을 선택하거나 쓰세요

체크포인트 1: 객관식 도전

1. 1. 시그니처 기반 탐지의 한계는 무엇입니까?
   - A. 알려지지 않았거나 변형된 악성코드를 식별하지 못함
   - B. 오탐이 많이 발생한다
   - C. 높은 CPU 처리 능력이 필요하다
   - D. 인터넷에 연결되어 있을 때만 작동한다

2. 2. 휴리스틱 스캐너는 신종 악성코드 변종을 어떻게 탐지하나요?
   - A. 의심스러운 패턴과 코드 구조를 식별해서
   - B. 파일 해시를 위협 데이터베이스와 대조하여
   - C. 서명되지 않은 모든 실행 파일을 자동으로 삭제하여
   - D. 모든 파일을 공용 클라우드 폴더에 업로드해서

3. 3. 백신 샌드박스 실행의 목적은 무엇입니까?
   - A. 안전한 가상 보관소에서 파일을 격리하고 분석함
   - B. 로컬 파일 시스템 백업 전송 속도 높이기
   - C. 로컬 운영 체제 보안 패치 업데이트하기
   - D. 저장 공간을 아끼려고 대용량 문서 파일 압축하기

4. 4. 위협 행위를 실시간으로 포착하는 탐지 방식은 무엇입니까?
   - A. 소프트웨어 동작을 모니터링하는 행위 분석
   - B. 밤사이 수행하는 과거 로그 점검
   - C. 느린 앱을 신고하는 사용자의 수동 개입
   - D. 설치된 프로그램을 매주 수동으로 검토하기

5. 5. 스캐너에 정기적인 정의 파일 업데이트가 중요한 이유는 무엇입니까?
   - A. 시그니처 엔진 데이터베이스에 위협 식별자를 제공하기 위해
   - B. 작업 중 CPU 클럭 속도를 높이기 위해
   - C. 전역 DNS 네임서버 캐싱 시간을 수정하려고
   - D. 웹 브라우저 쿠키 설정을 승인하려고

체크포인트 2: 참/거짓 도전

6 **질문 tf 6**

6. 시그니처 탐지는 암호화 파일 해시를 데이터베이스 목록과 대조합니다.

○ 참 ○ 거짓

7 **질문 tf 7**

7. 휴리스틱 스캐너는 안전한 파일에 대해 오탐 경고를 일으킬 수 있습니다.

○ 참 ○ 거짓

8 **질문 tf 8**

8. 샌드박스는 악성코드가 네트워크 파일에 제한 없이 접근하도록 허용합니다.

○ 참 ○ 거짓

9 **질문 tf 9**

9. 행위 기반 검사는 파일이 악의적인 동작을 보이면 해당 파일을 차단합니다.

○ 참 ○ 거짓

10 **질문 tf 10**

10. 표준 백신 소프트웨어는 모든 제로데이 공격을 완벽하게 막습니다.

○ 참 ○ 거짓

체크포인트 3: 핵심 용어 채우기

아래 각 문장을 읽고 단어 목록에서 알맞은 용어를 골라 빈칸을 채우세요.

1. 전통적인 스캐너는 알려진 악성코드를 식별하기 위해 _____ 일치에 의존합니다.
2. 파일의 코드 패턴을 분석하는 것을 _____ 스캔이라고 합니다.
3. 백신 프로그램은 의심스러운 파일을 _____ 환경에 격리합니다.
4. 실시간 모니터링은 프로그램의 _____ 을(를) 감시해 의심스러운 활동을 찾습니다.
5. 스캐너는 새로운 위협을 인식하기 위해 매일 데이터베이스 _____ 을(를) 내려받습니다.
6. 안전한 프로그램이 악성코드로 표시되면 _____ 경보가 발생합니다.

어휘 단어 목록

샌드박스 | 시그니처 | 시스템 검사 | 업데이트 | 오탐 | 위협 격리 | 행동 | 휴리스틱

여기에 답을 쓰세요:

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

체크포인트 4: 보안 개념 연결

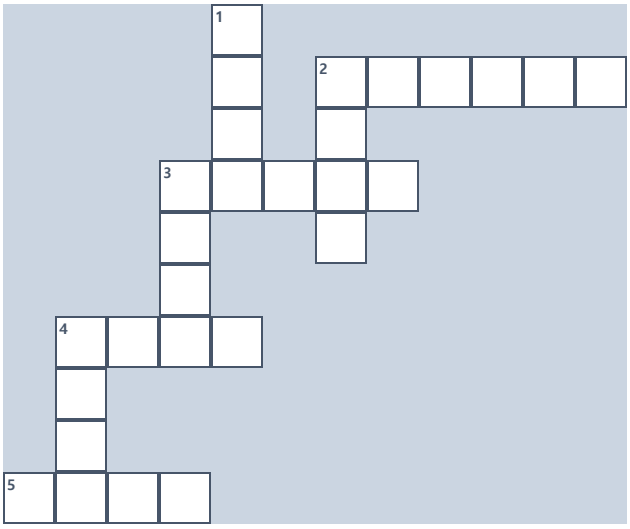
정의 연결하기

왼쪽의 각 어휘를 오른쪽의 알맞은 설명과 연결하고, 입력 칸에 해당하는 글자(A-H)를 쓰세요.

☐	**1. 해시 서명**	**A**	의심스러운 파일을 격리해 로컬 시스템 노출을 막기.
☐	**2. 코드 휴리스틱**	**B**	엔드포인트를 스캔하고 익스플로잇으로부터 보호하는 소프트웨어 모음.
☐	**3. 파일 샌드박스**	**C**	실행 중인 소프트웨어의 동작에서 악의적인 작동 패턴을 감시하기.
☐	**4. 행위 검사**	**D**	알려진 위협을 식별하는 데 사용되는 고유한 암호화 데이터베이스 지문입니다.
☐	**5. 일일 업데이트**	**E**	신뢰할 수 없는 코드를 안전하게 실행하는 보안 가상 테스트 환경.
☐	**6. 오탐**	**F**	위협 데이터베이스에 반영되는 정기적인 정의 파일 다운로드.
☐	**7. 위협 격리**	**G**	의심스러운 코드 구조를 가진 파일을 표시하는 규칙 기반 분석.
☐	**8. 백신 프로그램**	**H**	안전한 소프트웨어를 악성코드로 잘못 분류하는 보안 경고.

체크포인트 5: 십자말풀이

활성화된 흰색 칸에 글자를 입력해 십자말풀이를 푸세요. 숫자는 아래 열쇠에 해당합니다.



가로

2. 엔드포인트를 검사하고 익스플로잇으로부터 보호하는 소프트웨어 모음 (6)

3. 컴퓨터 전체를 훑어 위협을 찾는 작업 (5)

4. 발견한 위험 요소를 삭제하거나 치료하는 일 (4)

5. 알려지지 않은 위협을 의심스러운 특징으로 찾아내는 분석 방식 (4)

세로

1. 다른 파일에 붙어 스스로 퍼지는 악성 프로그램 (4)

2. 저장된 파일에 위협이 있는지 훑어보는 일 (4)

3. 알려진 위협을 식별하는 데 쓰는 고유한 암호화 데이터베이스 지문 (4)

4. 의심스러운 파일을 가둬 시스템이 노출되지 않도록 하는 일 (4)

체크포인트 5 대체 활동: 접근성을 고려한 십자말풀이 단서

화면 낭독기와 키보드 사용자는 아래 입력란에 십자말풀이 정답을 직접 입력할 수 있습니다. 가로 열쇠 세로 열쇠

가로

2 가로: 엔드포인트를 검사하고 익스플로잇으로부터 보호하는 소프트웨어 모음 (6 글자):

3 가로: 컴퓨터 전체를 훑어 위협을 찾는 작업 (5 글자):

4 가로: 발견한 위험 요소를 삭제하거나 치료하는 일 (4 글자):

5 가로: 알려지지 않은 위협을 의심스러운 특징으로 찾아내는 분석 방식 (4 글자):

세로

1 세로: 다른 파일에 붙어 스스로 퍼지는 악성 프로그램 (4 글자):

2 세로: 저장된 파일에 위협이 있는지 훑어보는 일 (4 글자):

3 세로: 알려진 위협을 식별하는 데 쓰는 고유한 암호화 데이터베이스 지문 (4 글자):

4 세로: 의심스러운 파일을 가둬 시스템이 노출되지 않도록 하는 일 (4 글자):

체크포인트 6: 숨은 단어 찾기

아래 격자에 숨어 있는 핵심 어휘 8개를 찾으세요. 단어는 가로, 세로, 대각선으로 배치될 수 있습니다.

라 인 요 다 서 니 하 크 처 주 백 도 타 밀 개
접 화 트 격 밀 라 소 카 백 다 스 방 속 크 램
타 리 파 라 전 크 기 메 전 신 안 연 안 격 넷
타 처 바 스 로 다 트 터 응 용 검 기 로 결 템
색 협 다 험 넷 백 파 넷 러 데 신 사 격 휴 버
공 위 밀 자 시 신 술 바 네 송 리 번 격 협 위
결 아 요 템 메 프 하 암 이 인 바 가 마 아 속
휴 암 넷 틱 벽 로 협 소 방 러 타 관 데 터 타
틱 술 전 이 화 그 위 공 워 이 스 이 험 리 템
스 요 주 트 사 램 도 위 결 호 스 바 그 카 도
리 시 스 템 검 사 프 답 아 로 그 버 화 크 위
휴 램 카 전 시 타 관 러 공 사 청 마 가 협 램
연 카 벽 나 그 타 결 타 안 크 술 카 격 리 험
데 하 술 스 니 로 도 안 관 검 보 리 나 다 관
속 전 공 소 처 휴 위 넷 시 요 스 차 전 백 마

어휘 단어 목록

시그니처 바이러스 위협처리 휴리스틱 백신검사 시스템검사 위협격리 백신프로그램

체크포인트 6 대체 활동: 접근성을 고려한 어휘 연결

단어 찾기의 8개 어휘를 각각 알맞은 설명과 연결하고, 빈칸에 글자(A-H)를 쓰세요.

어휘 용어
A. 시그니처
B. 바이러스
C. 위협처리
D. 휴리스틱
E. 백신검사
F. 시스템검사
G. 위협격리
H. 백신프로그램

정의 및 연결 항목
1. 알려지지 않은 위협을 의심스러운 특징으로 찾아내는 분석 방식.
2. 엔드포인트를 검사하고 익스플로잇으로부터 보호하는 소프트웨어 모음.
3. 저장된 파일에 위협이 있는지 훑어보는 일.
4. 다른 파일에 붙어 스스로 퍼지는 악성 프로그램.
5. 의심스러운 파일을 가둬 시스템이 노출되지 않도록 하는 일.
6. 알려진 위협을 식별하는 데 쓰는 고유한 암호화 데이터베이스 지문.
7. 발견한 위험 요소를 삭제하거나 치료하는 일.
8. 컴퓨터 전체를 훑어 위협을 찾는 작업.

체크포인트 7: 뒤섞인 단어 도전

아래 글자를 맞게 배열하여 핵심 사이버 보안 개념과 용어를 알아내세요. 정답을 제공된 입력란에 쓰세요.

1. 니 시 처 그 _____

2. 위 처 리 협 _____

3. 사 백 검 신 _____

4. 리 격 위 협 _____

5. 스 바 러 이 _____

6. 스 틱 휴 리 _____

7. 검 사 시 템 스 _____

8. 프 램 백 그 로 신 _____

보너스 활동: 빠르게 생각하기

각 범주마다 답을 3개씩 쓰세요. 목록을 가장 먼저 채운 사람이 이깁니다.

1	소프트웨어를 업데이트하는 이유			
2	IT 도움을 요청할 수 있는 사람			
3	백신이 무언가를 발견했을 때 할 일			
4	컴퓨터 바이러스의 징후			
5	격리되는 것			
6	바이러스가 숨어 있는 곳			
7	절대 공유하면 안 되는 정보			
8	악성 소프트웨어의 종류			
9	알고 있는 보안 도구			
10	백신이 검사하는 것			
11	백업하는 것			
12	해킹당할 수 있는 기기			
13	알고 있는 백신 프로그램			
14	오탐이 생기는 이유			
15	오늘부터 시작할 수 있는 안전 습관			

체크포인트 8: 사이버 보안 사례 연구

배운 개념을 적용하여 아래의 실제 시나리오를 해결하세요.

사례 연구 1: 시그니처 검사와 휴리스틱 검사 비교



상황: 한 직원이 다른 팀이 사내에서 만든 맞춤형 유틸리티를 다운로드합니다. 시그니처 검사기는 통과시키지만 휴리스틱 검사기는 의심스러운 파일로 표시합니다.

토론 질문: 이런 일이 생긴 이유와 파일이 안전한지 확인하는 방법을 설명하세요.

사례 연구 2: 오탐 처리하기



상황: 한 소프트웨어 개발자가 자신의 애플리케이션을 컴파일합니다. 시스템 백신이 새 실행 파일을 악성코드로 표시하고 격리합니다.

토론 질문: 화이트리스트 등록의 위험을 간략히 설명하고, 올바른 해결 절차를 설명하세요.

체크포인트 9: 암호 해독하기

사이버 보안 전문가는 온라인 위협 행위자로부터 네트워크 자산을 보호합니다. 아래의 자모-숫자 키를 사용해 해당하는 자모를 빈칸에 써서 메시지를 해독하세요.

자모-숫자 암호화 키

ㄱ=1 ㄲ=2 ㄴ=3 ㄷ=4 ㄸ=5 ㄹ=6 ㅁ=7 ㅂ=8 ㅃ=9 ㅅ=10
ㅆ=11 ㅇ=12 ㅈ=13 ㅉ=14 ㅊ=15 ㅋ=16 ㅌ=17 ㅍ=18 ㅎ=19 ㅏ=20
ㅐ=21 ㅑ=22 ㅒ=23 ㅓ=24 ㅔ=25 ㅕ=26 ㅖ=27 ㅗ=28 ㅘ=29 ㅙ=30
ㅚ=31 ㅛ=32 ㅜ=33 ㅝ=34 ㅞ=35 ㅟ=36 ㅠ=37 ㅡ=38 ㅢ=39 ㅣ=40

19	37	6	40	10	38	17	40	1		16	28	4	38	
8	**33**	**3**	**10**	**24**	**1**	**12**	**38**	**6**	**28**		**17**	**20**	**7**	**13**	**40**

해독된 메시지:

팁: 각 숫자는 아래 키의 한글 자모 하나를 나타냅니다. 자모를 차례로 모아 글자를 만드세요(예: ㅂ+ㅗ = 보).

체크포인트 10: 기초 사이버 보안 FAQ (파트 A)

온라인 위협 대응에 관한 자주 묻는 질문과 답을 살펴보세요.

Q1: 백신 소프트웨어는 악성코드를 어떻게 식별하나요?

데이터베이스 시그니처 대조, 휴리스틱 코드 구조 분석, 실시간 행위 모니터링으로 악성코드를 식별합니다.

Q2: 시그니처 기반 탐지란 무엇인가요?

파일의 암호화 해시를 알려진 악성코드 위협의 데이터베이스 목록과 대조하는 검사 방식입니다.

Q3: 휴리스틱 스캐너란 무엇인가요?

휴리스틱은 파일의 구조와 코드 명령을 분석하여 악성코드 변종에 흔한 의심스러운 패턴을 찾아냅니다.

Q4: 파일이 격리되었다는 것은 무슨 뜻인가요?

백신은 파일을 안전하게 격리된 폴더로 옮기고 실행을 차단하여 운영체제를 보호합니다.

Q5: 백신의 오탐(false positive)이란 무엇인가요?

정상적이고 안전한 소프트웨어가 검사 알고리즘에 의해 악성코드로 잘못 표시되는 오류입니다.

체크포인트 10: 기초 사이버 보안 FAQ (파트 B)

온라인 위협 대응에 관한 자주 묻는 질문과 답을 살펴보세요.

Q6: 동작 모니터링은 시스템을 어떻게 보호하나요?

실행 중인 소프트웨어를 실시간으로 모니터링하여 코드 삽입 같은 의심스러운 변경을 시도하는 프로세스를 차단합니다.

Q7: 샌드박스 테스트가 중요한 이유는 무엇인가요?

샌드박싱은 신뢰할 수 없는 파일을 격리된 가상 머신에서 실행하여, 시스템에 노출되지 않은 채 안전하게 동작을 관찰합니다.

Q8: 백신 정의 파일은 얼마나 자주 업데이트해야 하나요?

검사기는 새로 발견된 악성코드 계열을 인식하도록 정의 파일을 매일 또는 매시간 업데이트해야 합니다.

Q9: 백신과 EDR은 어떻게 다른가요?

백신은 파일 검사에 중점을 두는 반면, 엔드포인트 탐지 및 대응(EDR)은 네트워크 전체의 위협 추적과 차단을 제공합니다.

Q10: 백신 프로그램 두 개를 함께 실행해도 되나요?

아니요. 활성 검사기를 두 개 실행하면 시스템 충돌이 일어나고 성능이 느려지며 서로의 작동을 방해할 수 있습니다.

체크포인트 10: 심화 보안 FAQ (파트 C)

보안 프레임워크, 악성코드 분석, 데이터 규정 준수의 고급 기술적 측면을 탐구합니다.

Q1: 휴리스틱 규칙은 위협 우회를 어떻게 최소화하나요?

휴리스틱은 특정 시그니처가 아니라 일반적인 위협 패턴을 분석하므로, 알려진 악성코드 계열의 변형을 잡아낼 수 있습니다.

Q2: 다형성 바이러스란 무엇인가요?

실행할 때마다 파일 구조와 복호화 루틴을 바꾸어 시그니처 검사를 무력화하는 악성코드입니다.

Q3: 샌드박스는 VM 회피를 어떻게 탐지하나요?

최신 샌드박스는 마우스 클릭과 시스템 가동 시간을 흉내 내어, 가상 머신에서 실행될 때 숨도록 설계된 악성코드를 속입니다.

Q4: 시그니처 업데이트는 어떤 다운로드 형식으로 제공되나요?

업데이트는 대개 가벼운 증분 바이너리 차이 파일이어서 클라이언트의 네트워크 대역폭 사용을 최소화합니다.

Q5: 엔드포인트 에이전트는 로컬 검사를 어떻게 관리하나요?

에이전트는 가벼운 백그라운드 검사를 수행하고 심층 암호 해시 조회는 클라우드 위협 데이터베이스에 맡깁니다.

체크포인트 10: 심화 보안 FAQ (파트 D)

보안 프레임워크, 악성코드 분석, 데이터 규정 준수의 고급 기술적 측면을 탐구합니다.

Q6: 루트킷 탐지 검사란 무엇인가요?

루트킷이 활성 스레드를 숨기려고 후킹하는 OS API를 우회하여 커널 수준의 메모리 테이블을 검사합니다.

Q7: 동작 검사는 랜섬웨어를 어떻게 차단하나요?

자동화된 대량 파일 암호화 반복을 탐지하여 시스템 데이터베이스가 잠기기 전에 호스트 프로세스를 종료합니다.

Q8: 코드 서명 인증서 검증이란 무엇인가요?

검사기는 코드의 디지털 서명을 신뢰할 수 있는 루트 인증 기관과 대조해 소프트웨어 개발자의 신원을 확인합니다.

Q9: 패커는 검사 엔진에 어떤 영향을 주나요?

패커는 악성코드 페이로드를 압축하거나 암호화합니다. 시그니처 검사가 이루어지기 전에 스캐너가 메모리에서 파일의 압축을 풀어야 합니다.

Q10: EDR 도구는 격리를 어떻게 자동화하나요?

EDR 에이전트는 네트워크 수준에서 침해된 엔드포인트를 격리하여 횡적 이동을 막으면서 분석가의 접근은 허용합니다.

파트 11: 실제 사이버 보안 사실 10가지와 시사점

보안 침해, 방어 메커니즘, 규정 준수 표준에 관한 실제 사실을 살펴보세요.

1. 보안 인사이트

시그니처 데이터베이스에는 알려진 악성코드의 해시가 저장되므로, 완전히 새롭거나 변형된 파일은 정의가 업데이트될 때까지 탐지되지 않습니다.

2. 보안 인사이트

휴리스틱 엔진은 시그니처가 나오기 전에 일부 신종 악성코드 변종을 탐지할 수 있지만, 그 대가로 오탐이 늘어납니다.

3. 보안 인사이트

오탐 경보는 잘못 격리된 파일을 확인하고 복원하는 데 IT 팀의 시간을 소모하게 합니다.

4. 보안 인사이트

다형성 악성코드는 복사본마다 코드를 바꾸므로, 방어자는 시그니처 검사에 휴리스틱 및 행동 검사를 함께 사용합니다.

6. 보안 인사이트

악성코드 제작자는 샌드박스 환경을 확인하도록 설계된 맞춤형 코드를 작성하여, 실행을 지연시켜 타이머를 우회합니다.

5. 보안 인사이트

클라우드 기반 백신 엔진은 의심스러운 파일의 해시를 대규모 온라인 위협 데이터베이스와 거의 실시간으로 대조합니다.

7. 보안 인사이트

공급업체는 스캐너가 새로 확인된 위협을 인식할 수 있도록 엔드포인트에 정의 업데이트를 정기적으로 배포합니다.

8. 보안 인사이트

랜섬웨어 동작 모니터는 파일 암호화 및 섀도 복사본 삭제와 관련된 특정 Win32 API 호출을 대상으로 합니다.

9. 보안 인사이트

유효한 코드 서명은 오탐 위험을 낮출 수 있지만, 악성코드도 서명될 수 있으므로 서명된 파일도 검사합니다.

10. 보안 인사이트

루트킷은 시스템 커널 구조를 수정하므로 탐지하고 제거하려면 부팅 시 실행되는 전문 검사기가 필요합니다.

기술 참고 자료 및 출처

이 학습 가이드와 인터랙티브 퍼즐은 전 세계 NIST, OWASP, 개인정보 보호 규정 준수 표준을 바탕으로 만들었습니다. 학술 및 업계 참고 자료

학술 및 업계 참고 자료

[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

답안: 체크포인트 1 – 객관식

1 **질문 1** 시그니처 정답: A

교사용 참고

시그니처 검사는 알려진 데이터베이스 해시에 의존하므로 알려지지 않았거나 변형된 악성코드를 탐지하지 못합니다. 출처: OWASP 보안 구성.

2 **질문 2** 휴리스틱 정답: A

교사용 참고

휴리스틱은 코드 구조와 명령을 분석해 새로운 위협 변종의 의심스러운 특징을 식별합니다. 출처: Center for Internet Security(CIS).

3 **질문 3** 샌드박싱 정답: A

교사용 참고

샌드박스는 의심스러운 파일을 격리된 가상 머신에서 실행해 실행 동작을 안전하게 관찰합니다. 출처: NIST 디지털 신원.

4 **질문 4** 행위 기반 정답: A

교사용 참고

동작 검사는 실행 중인 프로그램을 실시간으로 감시해 무단 시스템 변경을 차단합니다. 출처: Center for Internet Security(CIS).

5 **질문 5** 업데이트 정답: A

교사용 참고

검사기는 위협 환경과 동기화를 유지하기 위해 매일 증분 정의 업데이트를 내려받습니다. 출처: OWASP 보안 구성.

답안: 체크포인트 2 – 참 또는 거짓

6 질문 6 시그니처 정답: 참

교사용 참고

시그니처 도구는 암호화 해시를 계산해 알려진 위협 해시 데이터베이스와 대조합니다. 출처: OWASP 보안 구성.

7 질문 7 휴리스틱 정답: 참

교사용 참고

휴리스틱 엔진은 규칙 기반 구조를 실행하므로 정상적이고 안전한 파일을 의심스럽다고 표시할 수 있습니다. 출처: Center for Internet Security(CIS).

8 질문 8 샌드박싱 정답: 거짓

교사용 참고

샌드박스는 가상 컨테이너에서 코드를 실행하며 네트워크 공유 접근을 엄격하게 차단합니다. 출처: NIST 디지털 신원.

9 질문 9 행위 기반 정답: 참

교사용 참고

실시간 모니터링은 불법적인 쓰기나 파일 잠금을 시도하는 실행 중 프로세스를 표시합니다. 출처: Center for Internet Security(CIS).

10 질문 10 정답: 거짓

교사용 참고

어떤 백신도 모든 제로데이 공격을 막지는 못합니다. 알려지지 않은 위협은 시그니처와 휴리스틱을 피할 수 있습니다.

어휘 정답 및 채점 기준표

교사용 채점 기준: 정확하게 연결한 항목마다 1점(총 8점), 문맥 용어마다 1점(총 6점)을 줍니다.

체크포인트 4: 답안 – 개념 연결

D 1. 해시 서명	G 2. 코드 휴리스틱	E 3. 파일 샌드박스	C 4. 행위 검사
F 5. 일일 업데이트	H 6. 오탐	A 7. 위협 격리	B 8. 백신 프로그램

체크포인트 3: 답안 – 핵심 용어

1 시그니처	2 휴리스틱	3 샌드박스	4 행동
5 업데이트	6 오탐		

체크포인트 6 대체 활동: 답안 – 단어 연결

1 D – 휴리스틱	2 H – 백신프로그램	3 E – 백신검사	4 B – 바이러스
5 G – 위협격리	6 A – 시그니처	7 C – 위협처리	8 F – 시스템검사

교사를 위한 토론 참고

핵심 용어:
학생들이 해시 서명, 코드 휴리스틱, 파일 샌드박스를 자신의 말로 설명하고 각각 예를 들 수 있는지 확인하세요.

사례 연구:
학생들이 의견이 아니라 워크시트의 사실을 근거로 권고안을 제시하게 하세요.

출처 평가:
학생들에게 워크시트의 참고 자료로 주장을 하나 이상 확인하게 하고, 수치·가격·규정이 시간이 지나면서 바뀔 수 있는 이유를 토론하게 하세요.

퍼즐 답안과 교사용 참고

단어 찾기 정답

라	인	요	다	서	니	하	크	처	주	백	도	타	밀	개
접	화	트	격	밀	라	소	카	백	다	스	방	속	크	램
타	리	파	라	전	크	기	메	전	신	안	연	안	격	넷
타	처	바	스	로	다	트	터	응	용	검	기	로	결	템
색	협	다	험	넷	백	파	넷	러	데	신	사	격	휴	버
공	위	밀	자	시	신	술	바	네	송	리	번	격	협	위
결	아	요	템	메	프	하	암	이	인	바	가	마	아	속
휴	암	넷	틱	벽	로	협	소	방	러	타	관	데	터	타
틱	술	전	이	화	그	위	공	워	이	스	이	험	리	템
스	요	주	트	사	램	도	위	결	호	스	바	그	카	도
리	시	스	템	검	사	프	답	아	로	그	버	화	크	위
휴	램	카	전	시	타	관	러	공	사	청	마	가	협	램
연	카	벽	나	그	타	결	타	안	크	술	카	격	리	험
데	하	술	스	니	로	도	안	관	검	보	리	나	다	관
속	전	공	소	처	휴	위	넷	시	요	스	차	전	백	마

십자말풀이 정답



가로

2 가로: 백신프로그램 엔드포인트를 검사하고 익스플로잇으로부터 보호하는 소프트웨어 모음 (6 글자)

3 가로: 시스템검사 컴퓨터 전체를 훑어 위협을 찾는 작업 (5 글자)

4 가로: 위협처리 발견한 위험 요소를 삭제하거나 치료하는 일 (4 글자)

5 가로: 휴리스틱 알려지지 않은 위협을 의심스러운 특징으로 찾아내는 분석 방식 (4 글자)

세로

1 세로: 바이러스 다른 파일에 붙어 스스로 퍼지는 악성 프로그램 (4 글자)

2 세로: 백신검사 저장된 파일에 위협이 있는지 훑어보는 일 (4 글자)

3 세로: 시그니처 알려진 위협을 식별하는 데 쓰는 고유한 암호화 데이터베이스 지문 (4 글자)

4 세로: 위협격리 의심스러운 파일을 가둬 시스템이 노출되지 않도록 하는 일 (4 글자)

뒤섞인 단어 및 암호 해독 답안

어휘 단어 맞추기 활동과 비밀 암호 도전의 채점 기준.

단어 맞추기 정답

1. 니시처그 — **시그니처**
2. 위처리협 — **위협처리**
3. 사백검신 — **백신검사**
4. 리격위협 — **위협격리**
5. 스바러이 — **바이러스**
6. 스틱휴리 — **휴리스틱**
7. 검사시템스 — **시스템검사**
8. 프램백그로신 — **백신프로그램**

비밀 암호 도전 정답

"휴리스틱 코드 분석으로 탐지"

사례 연구 답안

A 사례 연구 1: 시그니처 검사와 휴리스틱 검사 비교

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 상황 분석: 한 직원이 다른 팀이 내부에서 만든 맞춤 유틸리티를 내려받습니다. 시그니처 검사기는 통과시키지만 휴리스틱 검사기는 이를 의심스러운 파일로 표시합니다.
- 권장 전략 및 해결책: 발생한 이유: 시그니처 검사는 파일 해시를 확인하는데, 직접 만든 파일이라 위협 데이터베이스에 없습니다. 휴리스틱 분석은 구조를 살피고 의심스러운 동작(예: 레지스트리 쓰기)을 표시했습니다. 확인 방법: 파일을 샌드박스에서 실행해 동작을 관찰하고, 디지털 서명을 확인하며, 해시를 위협 인텔리전스 포털에 제출하세요.

B 사례 연구 2: 오탐 처리하기

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 상황 분석: 한 소프트웨어 개발자가 애플리케이션을 컴파일합니다. 시스템 백신이 새 실행 파일을 악성코드로 표시하고 격리합니다.
- 권장 전략 및 해결책: 예외 등록의 위험: 검사기를 우회하면 실제로 감염된 코드가 실행될 수 있습니다. 해결 방법: 파일을 백신 업체에 보내 분석을 요청하고, 인증 기관을 통해 코드에 디지털 서명을 하며, 백신을 끄는 대신 특정 폴더 예외만 일시적으로 설정하세요.