이름: _____ 날짜: _____ 점수: _____

랜섬웨어 공격과 비즈니스 복구

페이로드 실행, 암호 기반 파일 암호화, 오프라인 백업, 격리 절차, 재해 복구.

랜섬웨어 공격 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 랜섬웨어 공격과 비즈니스 복구를 안내합니다. 페이로드 실행, 파일 암호화, 오프라인 백업, 위협 격리, 암호화폐 지불, 재해 복구 계획을 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/ransomware-attack/

나의 랜섬웨어 복구 학습 로드맵

- 트로이 목마, 랜섬웨어, 스파이웨어 페이로드를 구분하세요.
- 안전한 샌드박스 환경 안에서 악성 파일을 분석하세요.
- 신속한 네트워크 격리 및 차단 절차를 수립하세요.

랜섬웨어 공격 안내

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

랜섬웨어 공격 및 재해 복구 (소개)

랜섬웨어 페이로드는 시스템 저장소를 암호학적으로 잠그고 복호화 키의 대가로 암호화폐 지급을 요구합니다. 이 위협을 완화하려면 네트워크 격리 규칙, 샌드박스 악성코드 분석, 견고한 에어 갭 콜드 백업이 필요합니다.

각 체크포인트를 주의 깊게 읽고 올바른 답을 선택하거나 쓰세요.

체크포인트 1: 객관식 도전

1 1. 랜섬웨어 공격의 주된 작동 방식은 무엇입니까?

- A. 시스템 접근을 막기 위한 사용자 파일의 암호화
- B. 입력란에 악성 SQL 명령어 주입하기
- C. 공용 Wi-Fi 연결에서 네트워크 패킷 가로채기
- D. SPF 검증을 우회하려고 이메일 헤더 위조하기

2 2. 오프라인(콜드) 백업이란 무엇입니까?

- A. 악성코드 확산으로부터 보호하려고 네트워크에서 분리한 저장소 사본
- B. 기본 웹 서버 하드 드라이브에 저장된 백업
- C. 시스템 레지스트리 로그의 임시 캐시
- D. 사용자 비밀번호를 재설정하는 데 쓰는 관리 도구

3 3. 랜섬웨어 공격 중에 보안팀은 감염된 시스템을 어떻게 격리해야 하나요?

- A. 네트워크 케이블을 뽑고 무선 인터페이스를 즉시 비활성화함
- B. 백신 시그니처 데이터베이스 업그레이드하기
- C. 기본 DNS 서버 종료하기
- D. 손상된 파일 확장자 이름 바꾸기

4 4. 보안 기관이 랜섬웨어 요구에 응하지 말라고 권고하는 이유는 무엇입니까?

- A. 대금을 내면 공격자를 부추기고 복호화 키가 전달된다는 보장도 없음
- B. 모든 기업 보험 증권을 자동으로 무효화한다
- C. 모든 고객에게 이메일로 자동 알림을 보낸다
- D. 남은 시스템 백업 파일을 손상시킨다

5 5. 재해 복구 계획(DRP)이란 무엇입니까?

- A. 시스템이 침해된 뒤 운영과 데이터를 복구하는 체계적인 절차
- B. 들어오는 네트워크 포트를 매핑하는 방화벽 구성
- C. 사용자 관리 권한을 나열한 데이터베이스 스키마
- D. 위조된 도메인을 거부하는 이메일 인증 프로토콜

체크포인트 2: 참/거짓 도전

6 질문 6

6. 랜섬웨어 페이로드는 네트워크에 연결된 온라인 백업으로 쉽게 확산될 수 있습니다.

○ 참 ○ 거짓

7 질문 7

7. 암호화폐 몸값을 지불하면 파일이 성공적으로 복호화된다는 보장이 있습니다.

○ 참 ○ 거짓

8 질문 8

8. 감염된 시스템을 네트워크에서 분리하면 랜섬웨어가 인접 시스템으로 확산되는 것을 막는 데 도움이 됩니다.

○ 참 ○ 거짓

9 질문 9

9. 랜섬웨어는 시스템 저장소를 암호화하는 데 대칭 암호를 절대 사용하지 않습니다.

○ 참 ○ 거짓

10 질문 10

10. 데이터 복원 절차를 정기적으로 테스트하는 것은 재해 복구에서 매우 중요한 부분입니다.

○ 참 ○ 거짓

체크포인트 3: 핵심 용어 채우기

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

1. 암호 기술로 파일을 잠가 접근을 막는 것은 _____ 입니다.
2. 시스템에서 실행되는 활성 악성 코드를 _____ (이)라고 합니다.
3. 분리된 외부 저장소 복사본은 안전한 _____ 입니다.
4. 악성코드의 확산을 막으려면 엔드포인트 네트워크 _____ 이(가) 필요합니다.
5. 사이버 범죄자가 요구하는 암호화폐 지불금을 _____ (이)라고 합니다.
6. 운영 데이터 파일을 되살리는 일은 재해 _____ 에 해당합니다.

어휘 단어 목록

격리 몸값 백신 복구 암호화 첨부 파일 콜드 백업 페이로드

여기에 답을 쓰세요:

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

체크포인트 4: 보안 개념 연결

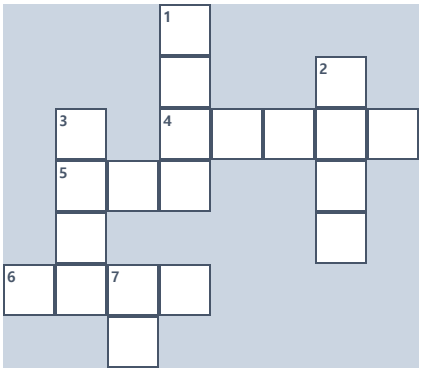
정의 연결하기

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

☐	**1. 암호화**	**A**	감염된 네트워크 시스템의 연결을 끊는 것.
☐	**2. 페이로드**	**B**	정상 파일로 위장한 악성 파일.
☐	**3. 콜드 백업**	**C**	파일을 암호학적으로 잠그기.
☐	**4. 격리**	**D**	주요 시스템 장애 사건.
☐	**5. 랜섬**	**E**	악성 소프트웨어 실행.
☐	**6. 복구**	**F**	연결이 끊긴 오프라인 사본.
☐	**7. 재해**	**G**	백업에서 데이터베이스 복원.
☐	**8. 트로이 목마**	**H**	암호화 키 지급 요청.

체크포인트 5: 십자말풀이

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



가로

4. 저장된 파일을 열 수 없게 암호로 잠그는 일 (5)

5. 인터넷으로 주고받는 전자 우편 (3)

6. 네트워크에서 분리해 오프라인으로 보관하는 백업본 (4)

세로

1. 이메일에 함께 붙여 보내는 파일 (4)

2. 잠긴 파일을 다시 열 수 있게 해 주는 열쇠 값 (4)

3. 악성코드가 실제로 피해를 입히는 실행 부분 (4)

7. 컴퓨터에서 악성코드를 찾아 없애 주는 프로그램 (2)

체크포인트 5 대체 활동: 접근성을 고려한 십자말풀이 단서

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

가로

4 가로: 저장된 파일을 열 수 없게 암호로 잠그는 일 (5 글자):

5 가로: 인터넷으로 주고받는 전자 우편 (3 글자):

6 가로: 네트워크에서 분리해 오프라인으로 보관하는 백업본 (4 글자):

세로

1 세로: 이메일에 함께 붙여 보내는 파일 (4 글자):

2 세로: 잠긴 파일을 다시 열 수 있게 해 주는 열쇠 값 (4 글자):

3 세로: 악성코드가 실제로 피해를 입히는 실행 부분 (4 글자):

7 세로: 컴퓨터에서 악성코드를 찾아 없애 주는 프로그램 (2 글자):

체크포인트 6: 숨은 단어 찾기

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

색	소	신	라	터	답	다	버	콜	보	정	백	청	값	소
파	번	격	개	암	워	험	번	이	라	청	카	다	도	벽
공	구	정	부	타	하	라	연	정	메	술	소	송	서	접
안	요	험	방	타	바	도	첨	다	워	일	넷	검	인	술
첨	값	속	메	드	파	다	리	방	하	방	복	이	구	험
키	몸	네	위	번	일	자	복	템	용	네	연	스	백	신
이	위	키	관	속	암	아	답	호	주	소	보	비	터	바
가	마	아	공	일	호	비	방	몸	화	암	키	청	벽	파
일	시	이	넷	타	화	용	연	송	벽	키	관	격	워	전
파	전	리	스	메	응	청	워	사	주	험	속	기	도	바
부	페	이	로	드	드	타	소	신	색	아	첨	드	네	벽
첨	정	부	카	콜	송	파	시	복	격	사	검	마	가	부
결	타	암	나	드	파	속	파	서	크	용	카	스	리	이
보	용	도	첨	백	주	서	시	로	안	나	다	시	공	연
위	응	키	관	업	방	템	응	도	차	송	값	바	네	도

어휘 단어 목록

페이로드 콜드백업 복호화키 파일암호화 몸값요구 백신 첨부파일 이메일

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. 페이로드
B. 콜드백업
C. 복호화키
D. 파일암호화
E. 몸값요구
F. 백신
G. 첨부파일
H. 이메일

정의 및 연결 항목
1. 잠긴 파일을 다시 열 수 있게 해 주는 열쇠 값.
2. 인터넷으로 주고받는 전자 우편.
3. 악성코드가 실제로 피해를 입히는 실행 부분.
4. 파일을 돌려주는 대가로 돈을 내라고 요구하는 일.
5. 저장된 파일을 열 수 없게 암호로 잠그는 일.
6. 이메일에 함께 붙여 보내는 파일.
7. 네트워크에서 분리해 오프라인으로 보관하는 백업본.
8. 컴퓨터에서 악성코드를 찾아 없애 주는 프로그램.

체크포인트 7: 뒤섞인 단어 도전

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

1. 로 페 드 이 _____

2. 복 화 키 호 _____

3. 구 몸 요 값 _____

4. 일 파 첨 부 _____

5. 업 콜 백 드 _____

6. 호 파 암 화 일 _____

7. 신 백 _____

8. 일 메 이 _____

보너스 활동: 빠르게 생각하기

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

1	절대 공유하면 안 되는 정보			
2	해킹당할 수 있는 기기			
3	몸값을 지불하지 말아야 하는 이유			
4	오늘부터 시작할 수 있는 안전 습관			
5	알고 있는 보안 도구			
6	계정을 보호하는 방법			
7	컴퓨터가 감염되었다는 신호			
8	백업을 보관할 장소			
9	절대 잃고 싶지 않은 파일			
10	랜섬웨어가 퍼지는 방법			
11	공격 후 첫 한 시간 동안 할 일			
12	공격 중에 연락할 사람			
13	랜섬웨어가 잠글 수 있는 것			
14	사이버 보안과 관련된 단어			
15	자주 표적이 되는 조직			

체크포인트 8: 사이버 보안 사례 연구

배운 개념을 적용하여 아래의 실제 시나리오를 해결하세요.

사례 연구 1: 기업 랜섬웨어 페이로드 차단

👷

상황: 한 기업의 근거리 통신망(LAN)이 활성 랜섬웨어에 침해되었습니다. 주요 파일 서버에서 파일 확장자가 .locked로 표시되기 시작했습니다.

토론 질문: 차단 단계를 자세히 설명하고, 데이터 복구 절차를 간략히 설명하세요.

사례 연구 2: 오프라인 백업 아키텍처 평가하기

👷

상황: 한 기업이 기본 로컬 네트워크가 랜섬웨어에 완전히 장악되더라도 백업이 침해될 위험을 줄이는 데이터 백업 전략을 설계하려고 합니다.

토론 질문: 안전한 오프라인 백업 저장 금고 시스템을 설계하세요.

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

12	28	18	38	6	20	12	40	3		8	21	1	12	24	8	12	38	6	28

10	40	10	38	17	25	7		8	28	1	12	34	3

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: 랜섬웨어란 무엇인가요?

랜섬웨어는 몸값이 지불될 때까지 컴퓨터 시스템이나 파일에 대한 접근을 차단하도록 설계된 악성 소프트웨어입니다.

Q2: 랜섬웨어는 어떻게 퍼지나요?

이메일 피싱 첨부 파일, 패치되지 않은 소프트웨어 취약점, 침해된 원격 접속 시스템을 통해서입니다. [1]

Q3: 암호화폐로 결제를 요구하는 이유는 무엇인가요?

비트코인 같은 암호화폐는 상대적인 익명성을 제공하여 수사 기관이 자금을 추적하기 어렵게 합니다.

Q4: 백신 프로그램이 랜섬웨어를 막아 주나요?

예, 하지만 시그니처 기반 백신은 새로 만들어진 제로데이 랜섬웨어 페이로드에는 실패할 수 있습니다.

Q5: 에어 갭 백업이란 무엇인가요?

기본 네트워크와 물리적·논리적 연결이 없어 확산으로부터 보호되는 백업 사본.

체크포인트 10: 기초 사이버 보안 FAQ (파트 B)

온라인 위협 대응에 관한 자주 묻는 질문과 답을 살펴보세요.

Q6: 이중 갈취란 무엇인가요?

공격자가 파일을 암호화할 뿐 아니라 민감한 데이터까지 훔쳐 대가를 내지 않으면 공개 유출하겠다고 협박하는 경우.

Q7: 복호화 도구(decryptor)란 무엇인가요?

잠긴 파일을 평문으로 복원하는 데 필요한 암호 키가 들어 있는 소프트웨어 유틸리티.

Q8: 랜섬웨어를 초기에 어떻게 탐지하나요?

갑작스러운 대량 파일 수정과 이름 변경 활동이 있는지 파일 시스템을 모니터링함으로써.

Q9: 보험의 역할은 무엇인가요?

사이버 보험은 복구 비용을 부담하는 데 도움이 될 수 있지만, 보장 조건과 랜섬 지불 규정은 보험 상품마다 다릅니다.

Q10: 감염된 시스템을 재부팅해야 하나요?

아니요, 재부팅하면 휘발성 메모리 증거가 사라질 수 있으므로 대신 네트워크에서 분리하세요. [1]

체크포인트 10: 심화 보안 FAQ (파트 C)

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

Q1: 랜섬웨어는 비대칭 암호화를 어떻게 사용하나요?

악성코드에 내장된 공개 키로 파일을 암호화하며, 복호화하려면 공격자의 개인 키가 필요합니다.

Q2: 대칭 암호화도 함께 사용하는 이유는 무엇인가요?

대칭 암호화(AES 등)는 빠르게 작동해 거대한 데이터베이스도 몇 분 안에 잠글 수 있으며, 비대칭 키는 AES 키를 보호합니다.

Q3: 논리적 분리란 무엇인가요?

네트워크를 격리된 영역으로 나누어 악성코드가 워크스테이션 노드에서 핵심 서버로 횡적으로 퍼지는 것을 막는 방식.

Q4: WORM 저장소란 무엇인가요?

한 번 쓰면 여러 번 읽을 수 있는(Write-Once, Read-Many) 매체로, 랜섬웨어 페이로드가 백업 데이터를 편집하거나 덮어쓰거나 삭제하지 못하게 합니다.

Q5: 섀도 복사본이란 무엇인가요?

Windows가 만드는 로컬 백업 스냅샷으로, 랜섬웨어는 보통 관리 도구를 사용해 이것을 가장 먼저 삭제합니다.

체크포인트 10: 심화 보안 FAQ (파트 D)

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

Q6: 자격 증명 탈취는 랜섬웨어를 어떻게 가능하게 하나요?

공격자는 유출된 관리자 로그인 정보를 구입해 원격 데스크톱으로 접속한 뒤 네트워크 전체에 랜섬웨어를 수동으로 실행합니다.

Q7: 모의 복원 테스트(dry-run)란 무엇인가요?

백업 데이터베이스를 격리된 테스트 환경에 정기적으로 복원해, 복원 속도와 데이터 무결성이 재해 복구 기준을 충족하는지 확인하는 것.

Q8: 엔드포인트 탐지(EDR)는 랜섬웨어를 어떻게 막나요?

프로세스 동작(예: 빠른 암호화)을 분석하고 이상 동작하는 애플리케이션을 신속히 중단시킴으로써.

Q9: 서비스형 랜섬웨어(RaaS) 모델이란 무엇인가요?

악성코드 개발자가 랜섬웨어 제작 도구를 제휴자에게 빌려주고 수익 일부를 받는 프랜차이즈 모델.

Q10: 패치되지 않은 RDP는 어떻게 랜섬웨어를 일으키나요?

노출되어 있고 패치되지 않은 원격 데스크톱 프로토콜 게이트웨이는 공격자가 로그인을 무차별 대입하고 악성코드를 직접 실행하게 만듭니다.

파트 11: 실제 사이버 보안 사실 10가지와 시사점

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

1. 보안 인사이트

랜섬웨어 공격자는 vssadmin.exe 같은 도구를 이용해 Windows 섀도 복사본을 삭제하고 로컬 복원을 막는 경우가 많습니다. [1]

2. 보안 인사이트

대칭 AES-256 키는 보통 파일 페이로드를 암호화하는 데 쓰이고, 그 키는 다시 공개 RSA 키로 잠깁니다.

3. 보안 인사이트

랜섬웨어 공격을 받은 뒤 복구하는 데는 몇 주가 걸릴 수 있으므로 테스트를 마친 오프라인 백업이 중요합니다.

4. 보안 인사이트

FBI는 몸값 지불을 지지하지 않으며, 지불해도 데이터를 되찾을 수 있다는 보장이 없다고 경고합니다. [2]

5. 보안 인사이트

재해 복구 계획(DRP)에는 복구 시간 목표(RTO)와 복구 시점 목표(RPO)를 정의해야 합니다.

6. 보안 인사이트

FBI는 암호화되고 변경 불가능한(바꾸거나 삭제할 수 없는) 백업을 권장합니다. [3]

7. 보안 인사이트

랜섬웨어 개발자는 고급 난독화 기법을 사용해 기존 시그니처 기반 백신 검사기를 우회합니다.

8. 보안 인사이트

네트워크 분리는 횡적 이동을 제한하여 랜섬웨어가 처음 감염된 호스트 밖으로 퍼지는 것을 막는 데 도움이 됩니다. [3]

9. 보안 인사이트

원격 데스크톱 프로토콜(RDP)처럼 노출되어 있고 보안이 허술한 원격 서비스는 흔한 랜섬웨어 침투 경로입니다. [1]

10. 보안 인사이트

CISA는 많은 랜섬웨어 변종이 접근 가능한 백업을 찾아 삭제하므로 암호화된 백업을 오프라인으로 보관하라고 권고합니다. [1]

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

[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

답안: 체크포인트 1 – 객관식

1 질문 1 정답: A

교사용 참고

랜섬웨어 공격의 주된 작동 방식은 무엇입니까? → 시스템 접근을 막기 위한 사용자 파일의 암호화

2 질문 2 정답: A

교사용 참고

오프라인(콜드) 백업이란 무엇입니까? → 악성코드 확산으로부터 보호하려고 네트워크에서 분리한 저장소 사본

3 질문 3 정답: A

교사용 참고

랜섬웨어 공격 중에 보안팀은 감염된 시스템을 어떻게 격리해야 하나요? → 네트워크 케이블을 뽑고 무선 인터페이스를 즉시 비활성화함

4 질문 4 정답: A

교사용 참고

보안 기관이 랜섬웨어 요구에 응하지 말라고 권고하는 이유는 무엇입니까? → 대금을 내면 공격자를 부추기고 복호화 키가 전달된다는 보장도 없음

5 질문 5 정답: A

교사용 참고

재해 복구 계획(DRP)이란 무엇입니까? → 시스템이 침해된 뒤 운영과 데이터를 복구하는 체계적인 절차

답안: 체크포인트 2 – 참 또는 거짓

6 질문 6 — 정답: 참

교사용 참고

랜섬웨어 페이로드는 네트워크에 연결된 온라인 백업으로 쉽게 확산될 수 있습니다.

7 질문 7 — 정답: 거짓

교사용 참고

거짓: FBI는 몸값을 지불해도 데이터를 되찾을 수 있다는 보장이 없다고 경고합니다.

8 질문 8 — 정답: 참

교사용 참고

참: CISA는 확산을 막기 위해 감염된 호스트의 연결을 끊거나 네트워크를 오프라인으로 전환하라고 권고합니다.

9 질문 9 — 정답: 거짓

교사용 참고

거짓: 랜섬웨어는 보통 AES 같은 빠른 대칭 암호로 파일을 암호화합니다.

10 질문 10 — 정답: 참

교사용 참고

데이터 복원 절차를 정기적으로 테스트하는 것은 재해 복구에서 매우 중요한 부분입니다.

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

C 1. 암호화	E 2. 페이로드	F 3. 콜드 백업	A 4. 격리
H 5. 랜섬	G 6. 복구	D 7. 재해	B 8. 트로이 목마

체크포인트 3: 답안 – 핵심 용어

1 암호화	2 페이로드	3 콜드 백업	4 격리
5 몸값	6 복구		

체크포인트 6 대체 활동: 답안 – 단어 연결

1 C – 복호화키	2 H – 이메일	3 A – 페이로드	4 E – 몸값요구
5 D – 파일암호화	6 G – 첨부파일	7 B – 콜드백업	8 F – 백신

교사를 위한 토론 참고

핵심 용어:
학생들이 암호화, 페이로드, 콜드 백업을 자신의 말로 설명하고 각각 예를 들 수 있는지 확인하세요.

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

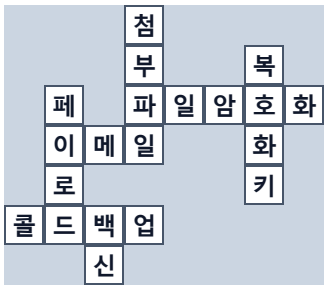
출처 평가:
학생들에게 워크시트의 참고 자료로 주장을 하나 이상 확인하게 하고, 수치·가격·규정이 시간이 지나면서 바뀔 수 있는 이유를 토론하게 하세요.

퍼즐 답안과 교사용 참고

단어 찾기 정답

색	소	신	라	터	답	다	버	콜	보	정	백	청	값	소
파	번	격	개	암	워	험	번	이	라	청	카	다	도	벽
공	구	정	부	타	하	라	연	정	메	술	소	송	서	접
안	요	험	방	타	바	도	첨	다	워	일	넷	검	인	술
첨	값	속	메	드	파	다	리	방	하	방	복	이	구	험
키	몸	네	위	번	일	자	복	템	용	네	연	스	백	신
이	위	키	관	속	암	아	답	호	주	소	보	비	터	바
가	마	아	공	일	호	비	방	몸	화	암	키	청	벽	파
일	시	이	넷	타	화	용	연	송	벽	키	관	격	워	전
파	전	리	스	메	응	청	워	사	주	험	속	기	도	바
부	페	이	로	드	드	타	소	신	색	아	첨	드	네	벽
첨	정	부	카	콜	송	파	시	복	격	사	검	마	가	부
결	타	암	나	드	파	속	파	서	크	용	카	스	리	이
보	용	도	첨	백	주	서	시	로	안	나	다	시	공	연
위	응	키	관	업	방	템	응	도	차	송	값	바	네	도

십자말풀이 정답



십자말풀이 정답 교사용 안내

가로

4 가로: 파일암호화 저장된 파일을 열 수 없게 암호로 잠그는 일 (5 글자)

5 가로: 이메일 인터넷으로 주고받는 전자 우편 (3 글자)

6 가로: 콜드백업 네트워크에서 분리해 오프라인으로 보관하는 백업본 (4 글자)

세로

1 세로: 첨부파일 이메일에 함께 붙여 보내는 파일 (4 글자)

2 세로: 복호화키 잠긴 파일을 다시 열 수 있게 해 주는 열쇠 값 (4 글자)

3 세로: 페이로드 악성코드가 실제로 피해를 입히는 실행 부분 (4 글자)

7 세로: 백신 컴퓨터에서 악성코드를 찾아 없애 주는 프로그램 (2 글자)

뒤섞인 단어 및 암호 해독 답안

어휘 단어 맞추기 활동과 비밀 암호 도전의 채점 기준.

단어 맞추기 정답

1. 로페드이 — **페이로드**
2. 복화키호 — **복호화키**
3. 구몸요값 — **몸값요구**
4. 일파첨부 — **첨부파일**
5. 업콜백드 — **콜드백업**
6. 호파암화일 — **파일암호화**
7. 신백 — **백신**
8. 일메이 — **이메일**

비밀 암호 도전 정답

"오프라인 백업으로 시스템 복원"

사례 연구 답안

A 사례 연구 1: 기업 랜섬웨어 페이로드 차단

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 상황 분석: 기업 로컬 영역 네트워크가 활성 랜섬웨어에 침해되었습니다. 주요 파일 서버에서 파일 확장자가 .locked로 표시되기 시작했습니다.
- 권장 전략 및 해결책: 영향을 받은 모든 서버를 로컬 영역 네트워크에서 분리합니다. 활성 관리자 세션을 종료합니다. 쓰기가 잠긴 안전한 오프라인 백업 시스템에서 손상되지 않은 파일을 복원합니다.

B 사례 연구 2: 오프라인 백업 아키텍처 평가하기

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 시나리오 분석: 한 기업이 기본 로컬 네트워크가 랜섬웨어에 완전히 장악되더라도 백업이 침해될 위험을 줄이는 데이터 백업 전략을 설계하려고 합니다.
- 권장 전략 및 해결책: 한 번 쓰고 여러 번 읽는(WORM) 저장소를 도입하세요. 백업 시스템을 모든 네트워크에서 분리해 논리적 에어갭을 구성하고, 매일 물리 매체를 교체하도록 하세요.