이름: _____ 날짜: _____ 점수: _____

사이버 보안 기초와 온라인 위협 예방

사이버 보안 위협, 네트워크 방화벽, 다단계 인증, 보안 프레임워크

사이버 보안 기초 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 사이버 보안 기초 및 온라인 위협 예방의 기본 원리를 안내합니다. 악성코드 위협, 다중 인증, 네트워크 방화벽, 사고 대응 프레임워크를 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/

나의 사이버 보안 기초 학습 로드맵

- 악성코드, 피싱, 기업 네트워크 침입의 흔한 경로를 파악하세요.
- MFA, 방화벽, 엔드포인트 방어를 포함한 표준 사이버 보안 통제를 도입하세요.
- 데이터 유출의 영향을 줄이기 위한 사고 대응 절차를 평가하세요.
- NIST 지침에 따른 조직의 위험 요인과 보안 정합성을 분석하세요.
- 자동화된 자격 증명 스터핑을 완화하기 위한 보안 위생 수칙을 구성하세요.

사이버 보안 가이드 안내

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

사이버 보안 기초와 위협 예방(소개)

사이버 보안은 네트워크, 시스템, 데이터를 무단 디지털 공격으로부터 보호합니다. 탄탄한 보안 습관을 기르고, 방화벽을 구성하고, 다단계 인증을 요구하고, 직원에게 위협 인식 교육을 하는 것은 기업 네트워크 방어의 필수 요소입니다.

각 체크포인트를 주의 깊게 읽고 올바른 답을 선택하거나 쓰세요.

체크포인트 1: 객관식 도전

1 1. 피싱 공격의 주된 목적은 무엇입니까?

- A. 자격 증명과 민감한 사용자 데이터를 훔침
- B. 웹사이트의 검색 엔진 노출도 높이기
- C. 네트워크 대역폭 용량 늘리기
- D. 백업 데이터 센터 복제 관리하기

2 2. 가장 강력한 계정 보호를 제공하는 메커니즘은 무엇입니까?

- A. 하드웨어 키를 사용하는 다중 인증
- B. 30일마다 갱신하는 복잡한 비밀번호
- C. 계정 로그인을 업무 시간으로 제한하기
- D. 공개 디렉터리에서 계정 사용자 이름 숨기기

3 3. 랜섬웨어 감염 페이로드는 무엇으로 정의됩니까?

- A. 시스템 파일을 암호화하고 대금을 요구함
- B. 키 입력을 원격 서버로 몰래 기록하기
- C. 브라우저에 무단으로 광고 삽입하기
- D. 로컬 CPU 자원으로 암호화폐 채굴하기

4 4. 제로데이 취약점 공격은 보안 방어에 어떤 영향을 미치나요?

- A. 패치되지 않은 미확인 취약점을 노림
- B. 기업 방화벽을 자동으로 비활성화한다
- C. 시스템이 강제로 완전히 재부팅된다
- D. 복구하는 데 예산이 전혀 들지 않는다

5 5. 기업의 보안 통제를 규율하는 프레임워크는 무엇입니까?

- A. NIST 사이버 보안 프레임워크 지침
- B. W3C HTML5 문서 스키마 사양
- C. 프린터 드라이버 설치 설명서
- D. IETF 라우팅 프로토콜 정의

체크포인트 2: 참/거짓 도전

6 **질문 tf 6**

6. 피싱 공격은 개인 이메일 계정만 노립니다.

○ 참 ○ 거짓

7 **질문 tf 7**

7. 다중 인증(MFA)은 크리덴셜 스터핑 공격을 막는 데 도움이 됩니다.

○ 참 ○ 거짓

8 **질문 tf 8**

8. 방화벽은 네트워크 트래픽을 검사하여 허가되지 않은 포트 접근을 차단합니다.

○ 참 ○ 거짓

9 **질문 tf 9**

9. 제로데이 익스플로잇 해결에는 표준 백신 정의 파일 업데이트가 필요합니다.

○ 참 ○ 거짓

10 **질문 tf 10**

10. 허니팟은 사이버 범죄자를 유인하는 데 쓰는 미끼 서버입니다.

○ 참 ○ 거짓

체크포인트 3: 핵심 용어 채우기

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

1. 네트워크 관리자는 들어오는 트래픽을 걸러 내려고 _____ 을(를) 설치합니다.
2. 공격자는 제로데이 _____ 을(를) 이용해 시스템 패치를 우회합니다.
3. 공격자는 직원을 노리는 _____ 캠페인을 벌이려고 위조 이메일을 보냅니다.
4. 랜섬웨어는 사용자 데이터를 잠그는 파괴적인 형태의 _____ 입니다.
5. 강력한 비밀번호 _____ 을(를) 지키면 자격 증명 탈취 위험을 줄일 수 있습니다.
6. 민감한 통신을 보호하려고 사용자는 _____ 프로토콜을 적용합니다.

어휘 단어 목록

방화벽 보안 프레임워크 악성코드 암호화 위생 이중 인증 익스플로잇 피싱

여기에 답을 쓰세요:

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

체크포인트 4: 보안 개념 연결

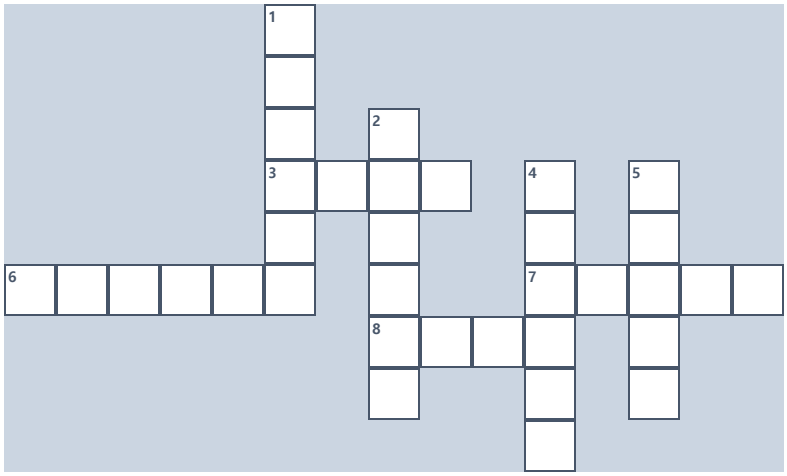
정의 연결하기

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

☐	**1. 랜섬웨어 위협**	**A**	사이버 위험을 관리하는 데 쓰이는 NIST 같은 체계적 지침.
☐	**2. 다중 요소 인증**	**B**	보안 침해를 처리하고 완화하기 위한 체계적인 계획.
☐	**3. 제로데이 공격**	**C**	보안 규칙에 따라 트래픽을 필터링하는 네트워크 장벽.
☐	**4. 미끼 허니팟**	**D**	데이터를 암호화하고 복호화를 대가로 금전을 요구하는 악성코드.
☐	**5. 침입 방화벽**	**E**	공급업체의 패치가 나오기 전에 노리는 취약점 공격.
☐	**6. 사고 대응**	**F**	자격 증명과 인증 키를 관리하는 모범 사례입니다.
☐	**7. 비밀번호 위생**	**G**	둘 이상의 인증 요소를 요구하는 보안 검증.
☐	**8. 보안 프레임워크**	**H**	악의적인 공격자를 유인하고 분석하기 위해 설치한 미끼 시스템.

체크포인트 5: 십자말풀이

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



가로

3. 비밀번호 외에 한 가지를 더 확인하는 방식 (4)

6. 데이터를 암호화한 뒤 복호화 대가로 금전을 요구하는 악성코드 (6)

7. 비밀번호와 업데이트를 꾸준히 챙기는 기본 습관 (5)

8. 정보가 새거나 시스템이 뚫린 사건 (4)

세로

1. 공급업체가 패치를 내놓기 전에 노리는 취약점 공격 (6)

2. 개인정보를 안전하게 지키는 일 (6)

4. 보안 침해를 처리하고 피해를 줄이기 위한 체계적인 계획 (6)

5. 컴퓨터 네트워크를 노린 공격 (5)

체크포인트 5 대체 활동: 접근성을 고려한 십자말풀이 단서

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

가로

3 가로: 비밀번호 외에 한 가지를 더 확인하는 방식 (4 글자):

6 가로: 데이터를 암호화한 뒤 복호화 대가로 금전을 요구하는 악성코드 (6 글자):

7 가로: 비밀번호와 업데이트를 꾸준히 챙기는 기본 습관 (5 글자):

8 가로: 정보가 새거나 시스템이 뚫린 사건 (4 글자):

세로

1 세로: 공급업체가 패치를 내놓기 전에 노리는 취약점 공격 (6 글자):

2 세로: 개인정보를 안전하게 지키는 일 (6 글자):

4 세로: 보안 침해를 처리하고 피해를 줄이기 위한 체계적인 계획 (6 글자):

5 세로: 컴퓨터 네트워크를 노린 공격 (5 글자):

체크포인트 6: 숨은 단어 찾기

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

소	응	침	메	파	번	공	속	벽	트	위	밀	라	요	카
다	대	스	화	개	크	증	타	사	파	라	송	크	술	주
전	고	안	결	안	위	방	타	바	이	템	증	다	워	터
답	사	용	기	중	결	템	악	다	관	버	넷	파	방	제
데	해	해	격	고	악	버	격	밀	자	스	공	술	이	네
송	침	리	데	격	성	로	제	위	접	아	청	격	중	도
주	하	암	터	바	코	가	마	로	아	개	고	암	인	방
생	생	벽	로	요	드	화	타	관	데	데	넷	타	증	술
위	송	전	벽	험	공	공	워	이	이	이	험	시	도	요
버	소	트	사	도	격	위	접	호	템	바	공	성	카	메
이	개	인	정	보	보	호	대	검	아	중	성	격	버	보
사	화	크	증	카	전	타	관	제	공	사	응	마	안	가
증	연	카	벽	나	타	접	타	안	크	술	카	사	시	험
데	하	술	스	중	메	서	관	색	안	나	고	다	관	속
송	공	요	고	험	방	스	청	템	차	전	침	마	버	템

어휘 단어 목록

악성코드공격 개인정보보호 제로데이공격 보안사고 사이버위생 침해사고대응 사이버공격 이중인증

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. 악성코드공격
B. 개인정보보호
C. 제로데이공격
D. 보안사고
E. 사이버위생
F. 침해사고대응
G. 사이버공격
H. 이중인증

정의 및 연결 항목
1. 비밀번호와 업데이트를 꾸준히 챙기는 기본 습관.
2. 보안 침해를 처리하고 피해를 줄이기 위한 체계적인 계획.
3. 데이터를 암호화한 뒤 복호화 대가로 금전을 요구하는 악성코드.
4. 개인정보를 안전하게 지키는 일.
5. 컴퓨터 네트워크를 노린 공격.
6. 비밀번호 외에 한 가지를 더 확인하는 방식.
7. 공급업체가 패치를 내놓기 전에 노리는 취약점 공격.
8. 정보가 새거나 시스템이 뚫린 사건.

체크포인트 7: 뒤섞인 단어 도전

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

1. 코 악 드 공 격 성 _____

2. 격 제 데 공 이 로 _____

3. 버 사 생 위 이 _____

4. 버 격 공 사 이 _____

5. 보 정 호 개 보 인 _____

6. 사 고 보 안 _____

7. 대 침 고 응 사 해 _____

8. 이 증 인 중 _____

보너스 활동: 빠르게 생각하기

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

1	사이버 보안 분야의 직업			
2	소프트웨어를 업데이트하는 이유			
3	방화벽이 차단할 수 있는 것			
4	이메일의 경고 신호			
5	백업하는 것			
6	잘 알려진 사이버 공격의 종류			
7	허니팟이 유인할 수 있는 것			
8	절대 공유하면 안 되는 정보			
9	컴퓨터가 감염되었다는 신호			
10	해커가 나오는 영화나 드라마			
11	구축할 수 있는 보안 계층			
12	보안 훈련에서 연습할 것			
13	알고 있는 보안 도구			
14	IT 도움을 요청할 수 있는 사람			
15	'사이버'로 시작하는 단어			

체크포인트 8: 사이버 보안 사례 연구

배운 개념을 적용하여 아래의 실제 시나리오를 해결하세요.

사례 연구 1: 랜섬웨어 복구 전략



상황: 한 기업 네트워크가 랜섬웨어에 감염되어 핵심 데이터베이스가 잠겼습니다. 공격자들은 100,000달러 상당의 암호화폐를 요구합니다. 이 회사에는 24시간 전의 오프라인 백업이 있습니다.

토론 질문: 비용을 지불할 때의 위험을 분석하고, 복구 전략을 평가하세요.

사례 연구 2: 자격 증명 스터핑 방어



상황: 한 온라인 서비스가 해커들이 다른 사이트에서 훔친 수백만 개의 사용자 이름과 비밀번호 쌍을 시험해 보는 크리덴셜 스터핑 공격을 받습니다.

토론 질문: 이 공격의 작동 방식을 자세히 설명하고, 두 가지 방어 체계를 간략히 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

4	20	13	33	12		12	40	3	13	38	12	12	38	6	28

10	40	10	38	17	25	7		8	28	19	28

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: 사이버 보안의 주요 목적은 무엇인가요?

주된 목표는 네트워크, 기기, 데이터를 무단 접근, 공격, 우발적 손상으로부터 보호하는 것입니다.

Q2: 피싱은 스피어 피싱과 어떻게 다른가요?

피싱은 무작위 사용자를 노리는 대규모 이메일 캠페인이고, 스피어 피싱은 개인화된 데이터를 이용해 특정 개인을 노립니다.

Q3: 네트워크 방화벽이란 무엇인가요?

방화벽은 미리 정해진 보안 규칙에 따라 들어오고 나가는 트래픽을 감시하고 필터링하는 네트워크 보안 시스템입니다.

Q4: 다중 인증(MFA)이 필요한 이유는 무엇인가요?

MFA는 공격자가 기본 비밀번호 인증 정보를 훔치거나 풀어내더라도 접근을 막아 주는 중요한 방어 계층을 더해 줍니다.

Q5: 컴퓨터 바이러스는 무엇으로 정의되나요?

바이러스는 정상 파일에 달라붙어 스스로 복제하다가 실행되면 시스템 전체로 퍼지는 악성코드입니다.

체크포인트 10: 기초 사이버 보안 FAQ (파트 B)

온라인 위협 대응에 관한 자주 묻는 질문과 답을 살펴보세요.

Q6: 랜섬웨어는 로컬 데이터를 어떻게 잠그나요?

랜섬웨어는 암호화 알고리즘으로 사용자 파일을 암호화하여 복호화 키를 적용하기 전까지 읽을 수 없게 만듭니다.

Q7: 제로데이 취약점이란 무엇인가요?

제로데이는 공급업체가 모르는 소프트웨어 보안 결함으로, 악용되기 전에 패치를 개발할 시간이 없습니다.

Q8: NIST 프레임워크의 역할은 무엇인가요?

NIST 프레임워크는 조직이 사이버 보안 위험을 관리하고 줄이는 데 도움이 되는 자율적 지침과 표준을 제공합니다.

Q9: 보안 사고 대응 계획이란 무엇인가요?

보안 침해와 네트워크 침해를 탐지, 차단, 복구하기 위한 문서화된 절차 모음입니다.

Q10: 사회공학은 사용자를 어떻게 악용하나요?

사회공학은 심리적 조작으로 직원을 속여 비밀번호를 알려 주거나 악성 파일을 내려받게 합니다.

체크포인트 10: 심화 보안 FAQ (파트 C)

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

Q1: DDoS 공격은 웹 서버를 어떻게 마비시키나요?

DDoS 공격은 감염된 수백만 대의 봇넷 기기를 조율해 서버에 트래픽을 쏟아부어 대역폭과 CPU 한도를 소진시킵니다.

Q2: 대칭 암호화와 비대칭 암호화의 차이는 무엇인가요?

대칭 암호화는 암호화와 복호화에 하나의 키를 사용하고, 비대칭 암호화는 공개 키와 개인 키 쌍을 사용합니다.

Q3: 해커는 SQL 인젝션 공격을 어떻게 실행하나요?

공격자는 입력란에 악성 SQL 명령어를 입력해 백엔드 데이터베이스가 무단으로 사용자 기록을 내놓도록 속입니다.

Q4: 네트워크 침입에서 측면 이동이란 무엇인가요?

공격자가 처음 얻은 서버 접근 권한을 이용하여 내부 네트워크에 연결된 다른 시스템까지 장악하는 기법입니다.

Q5: DNS 스푸핑은 웹 트래픽을 어떻게 다른 곳으로 보내나요?

DNS 스푸핑은 네임서버 캐시 레코드를 변경하여, 정상 사용자를 목표 도메인 대신 악성 유사 웹사이트로 보냅니다.

체크포인트 10: 심화 보안 FAQ (파트 D)

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

Q6: 하드웨어 보안 토큰이란 무엇인가요?

암호화 인증 증명을 생성하는 물리적 장치(YubiKey 등)로, 원격 피싱에 대한 최고 수준의 방어를 제공합니다.

Q7: 보안 팀은 미끼 허니팟을 어떻게 활용하나요?

팀은 비운영 미끼 서버를 배치해 침입을 조기에 탐지하고 무단 행위자의 공격 패턴을 분석합니다.

Q8: 최소 권한 원칙이란 무엇인가요?

사용자의 접근 권한을 업무 역할 수행에 꼭 필요한 최소한으로 제한하는 보안 표준입니다.

Q9: 중간자 공격은 연결을 어떻게 악용하나요?

공격자가 암호화되지 않은 네트워크에서 두 기기 사이의 통신을 가로채 변조하고 세션 토큰과 자격 증명을 훔칩니다.

Q10: 침해 지표(IOC)란 무엇인가요?

IOC는 비정상적인 레지스트리 변경이나 불법 IP 트래픽 같은 포렌식 단서로, 시스템이 침해되었음을 보여 줍니다.

파트 11: 실제 사이버 보안 사실 10가지와 시사점

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

1. 보안 인사이트

공격자는 취약한 서버를 찾기 위해 인터넷을 끊임없이 스캔하고 직원 받은편지함에 피싱 이메일을 보냅니다.

2. 보안 인사이트

피싱 링크 클릭 같은 사람의 실수는 데이터 침해의 흔한 요인이며, 그래서 교육이 중요합니다.

3. 보안 인사이트

데이터 유출 비용에는 법적 벌금, 고객 이탈, 조사 및 복구 비용이 포함되며 수백만 달러에 이를 수 있습니다.

4. 보안 인사이트

하드웨어 보안 키 같은 피싱 방지 MFA가 가장 강력한 유형의 MFA이며 CISA가 권고하는 표준입니다. [2]

5. 보안 인사이트

랜섬웨어는 여전히 기업 네트워크에 대한 주요 위협이며, CISA는 핵심 방어책으로 오프라인 암호화 백업을 권고합니다. [4]

6. 보안 인사이트

NIST 사이버 보안 프레임워크 2.0(2024)에는 거버넌스, 식별, 보호, 탐지, 대응, 복구의 여섯 가지 핵심 기능이 있습니다. [1]

7. 보안 인사이트

자격 증명 스터핑 봇은 유출된 사용자 이름과 비밀번호 쌍을 은행과 전자상거래 로그인 포털에 대규모로 대입해 봅니다.

8. 보안 인사이트

전 세계에 제로데이 익스플로잇 시장이 존재하며, 심각도가 높은 취약점은 패치되기 전에 큰 금액에 팔릴 수 있습니다.

9. 보안 인사이트

허니팟 미끼 시스템은 정상 사용자가 접근할 이유가 없으므로 침입 경고를 즉시 알려 줍니다.

10. 보안 인사이트

전송 계층 보안(TLS)은 브라우저 세션을 암호화하여 공용 Wi-Fi 네트워크에서의 패킷 스니핑을 막습니다.

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] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[2] CISA. (n.d.). More than a Password.
https://www.cisa.gov/MFA

[3] 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

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

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

[6] 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

[7] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[8] OWASP. (n.d.). SQL Injection.
https://owasp.org/www-community/attacks/SQL_Injection

답안: 체크포인트 1 – 객관식

1 **피싱 공격** 피싱 정답: A

교사용 참고

피싱 캠페인은 위조된 이메일을 이용해 자격 증명과 민감한 사용자 데이터를 훔치려 합니다. 인용: OWASP Secure Configuration.

2 **계정 보호** MFA 키 정답: A

교사용 참고

하드웨어 토큰을 사용하는 다중 요소 인증(MFA)은 가장 강력한 계정 접근 방어를 제공합니다. 출처: NIST Digital Identity.

3 **랜섬웨어 위협** 랜섬웨어 정답: A

교사용 참고

랜섬웨어는 핵심 시스템과 데이터를 암호화한 뒤 복호화 키의 대가로 암호화폐 지불을 요구합니다. 출처: Center for Internet Security (CIS).

4 **제로데이 취약점** 제로데이 정답: A

교사용 참고

제로데이 위협은 공급업체의 패치가 나오기 전에 패치되지 않은 알려지지 않은 보안 결함을 악용합니다. 출처: OWASP Secure Configuration.

5 **보안 프레임워크** 프레임워크 정답: A

교사용 참고

NIST 같은 프레임워크는 조직이 사이버 위험을 관리하고 줄이는 데 도움이 되는 체계적인 지침을 제공합니다. 출처: NIST Digital Identity.

답안: 체크포인트 2 – 참 또는 거짓

6 **표적 피싱** 피싱 정답: 거짓

교사용 참고

피싱 공격은 공격 경로를 넓히기 위해 기업 네트워크와 개인 계정을 모두 노립니다. 인용: OWASP Secure Configuration.

7 **질문 7** 정답: 참

교사용 참고

MFA는 두 번째 인증 요소를 요구하므로, 도난당한 비밀번호만으로는 보통 로그인할 수 없습니다.

8 **트래픽 방화벽** 방화벽 정답: 참

교사용 참고

방화벽은 특정 네트워크 포트의 트래픽을 검사하고 차단하여 허가되지 않은 연결을 걸러냅니다. 출처: Center for Internet Security (CIS).

9 **제로데이 대응** 제로데이 정답: 거짓

교사용 참고

제로데이 취약점을 해결하려면 아직 시그니처가 없으므로 코드 패치와 WAF 필터링이 필요합니다. 출처: OWASP Secure Configuration.

10 **유인용 허니팟** 허니팟 정답: 참

교사용 참고

허니팟은 보안팀이 악의적인 행위자를 유인하고, 경고를 받고, 연구하기 위해 사용하는 위장 서버입니다. 출처: Center for Internet Security (CIS).

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. 랜섬웨어 위협	G 2. 다중 요소 인증	E 3. 제로데이 공격	H 4. 미끼 허니팟
C 5. 침입 방화벽	B 6. 사고 대응	F 7. 비밀번호 위생	A 8. 보안 프레임워크

체크포인트 3: 답안 – 핵심 용어

1 방화벽	2 익스플로잇	3 피싱	4 악성코드
5 위생	6 암호화		

체크포인트 6 대체 활동: 답안 – 단어 연결

1 E – 사이버위생	2 F – 침해사고대응	3 A – 악성코드공격	4 B – 개인정보보호
5 G – 사이버공격	6 H – 이중인증	7 C – 제로데이공격	8 D – 보안사고

교사를 위한 토론 참고

핵심 용어:
학생들이 랜섬웨어 위협, 다중 요소 인증, 제로데이 공격을 자신의 말로 설명하고 각각 예를 들 수 있는지 확인하세요.

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

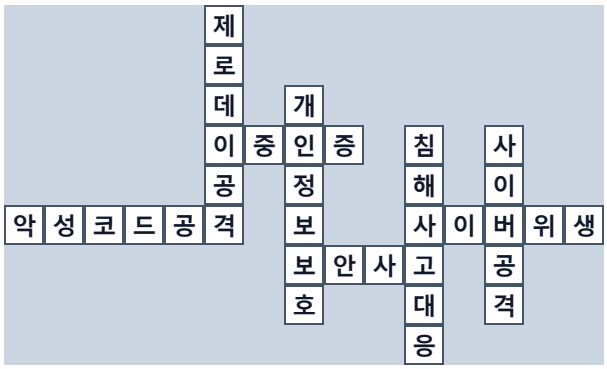
출처 평가:
학생들에게 워크시트의 참고 자료로 주장을 하나 이상 확인하게 하고, 수치·가격·규정이 시간이 지나면서 바뀔 수 있는 이유를 토론하게 하세요.

퍼즐 답안과 교사용 참고

단어 찾기 정답

소	응	침	메	파	번	공	속	벽	트	위	밀	라	요	카
다	대	스	화	개	크	증	타	사	파	라	송	크	술	주
전	고	안	결	안	위	방	타	바	이	템	중	다	워	터
답	사	용	기	중	결	템	악	다	관	버	넷	파	방	제
데	해	해	격	고	악	버	격	밀	자	스	공	술	이	네
송	침	리	데	격	성	로	제	위	접	아	청	격	증	도
주	하	암	터	바	코	가	마	로	아	개	고	암	인	방
생	생	벽	로	요	드	화	타	관	데	데	넷	타	증	술
위	송	전	벽	험	공	공	워	이	이	이	험	시	도	요
버	소	트	사	도	격	위	접	호	템	바	공	성	카	메
이	개	인	정	보	보	호	대	검	아	중	성	격	버	보
사	화	크	증	카	전	타	관	제	공	사	응	마	안	가
증	연	카	벽	나	타	접	타	안	크	술	카	사	시	험
데	하	술	스	중	메	서	관	색	안	나	고	다	관	속
송	공	요	고	험	방	스	청	템	차	전	침	마	버	템

십자말풀이 정답



십자말풀이 정답 교사용 안내

가로

3 가로: 이중인증 비밀번호 외에 한 가지를 더 확인하는 방식 (4 글자)

6 가로: 악성코드공격 데이터를 암호화한 뒤 복호화 대가로 금전을 요구하는 악성코드 (6 글자)

7 가로: 사이버위생 비밀번호와 업데이트를 꾸준히 챙기는 기본 습관 (5 글자)

8 가로: 보안사고 정보가 새거나 시스템이 뚫린 사건 (4 글자)

세로

1 세로: 제로데이공격 공급업체가 패치를 내놓기 전에 노리는 취약점 공격 (6 글자)

2 세로: 개인정보보호 개인정보를 안전하게 지키는 일 (6 글자)

4 세로: 침해사고대응 보안 침해를 처리하고 피해를 줄이기 위한 체계적인 계획 (6 글자)

5 세로: 사이버공격 컴퓨터 네트워크를 노린 공격 (5 글자)

뒤섞인 단어 및 암호 해독 답안

어휘 단어 맞추기 활동과 비밀 암호 도전의 채점 기준.

단어 맞추기 정답

1. 코악드공격성 — **악성코드공격**
2. 격제데공이로 — **제로데이공격**
3. 버사생위이 — **사이버위생**
4. 버격공사이 — **사이버공격**
5. 보정호개보인 — **개인정보보호**
6. 사고보안 — **보안사고**
7. 대침고응사해 — **침해사고대응**
8. 이증인중 — **이중인증**

비밀 암호 도전 정답

"다중 인증으로 시스템 보호"

사례 연구 답안

A 사례 연구 1: 랜섬웨어 복구 전략

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 상황 분석: 기업 네트워크가 랜섬웨어에 감염되어 핵심 데이터베이스가 잠겼습니다. 공격자는 100,000달러의 암호화폐 지급을 요구합니다. 회사에는 24시간 전의 오프라인 백업이 있습니다.
- 권장 전략 및 해결책: 지불의 위험: 돈을 내도 파일이 복호화된다는 보장이 없고, 회사가 돈을 내는 표적이라는 낙인이 찍히며, 범죄 활동에 자금을 대게 됩니다. 복구 전략: 팀은 감염된 호스트를 격리하고, 침해된 서버를 초기화하며, 오프라인 백업에서 데이터를 복원해야 합니다. 즉각적인 재감염을 막으려면 최초 침투 경로(피싱 또는 취약점 악용)를 패치해야 합니다.

B 사례 연구 2: 자격 증명 스터핑 방어

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 시나리오 분석: 한 온라인 서비스가 해커들이 다른 사이트에서 훔친 수백만 개의 사용자 이름/비밀번호 쌍을 대입하는 크리덴셜 스터핑 공격을 받습니다.
- 권장 전략 및 해결책: 원리: 공격자는 자동화된 봇으로 여러 사이트에서 재사용된 비밀번호를 이용해 사용자 계정에 로그인합니다. 방어: 1. 다중 인증(MFA)은 비밀번호가 맞아도 로그인 시도를 차단합니다. 2. 속도 제한과 CAPTCHA를 적용하면 로그인 엔드포인트로 몰리는 자동화 봇 트래픽을 막을 수 있습니다.