이름: _____ 날짜: _____ 점수: _____

제로 트러스트 아키텍처 및 보안

지속적 검증, 네트워크 마이크로 세그멘테이션, ID 및 접근 관리, 최소 권한, 보안 상태 점검.

제로 트러스트 보안 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 제로 트러스트 아키텍처와 보안을 안내합니다. 지속적인 검증, 네트워크 마이크로 세분화, 신원 및 접근 관리(IAM), 최소 권한, 세션 감사를 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/zero-trust-cyber-security/

나의 제로 트러스트 전략 학습 로드맵

- 지속적인 검증의 핵심 원칙을 이해합니다.
- 네트워크 마이크로 세그먼테이션과 최소 권한 접근을 도입하세요.
- 기기 보안 상태 점검과 활성 세션 감사를 구성하세요.

제로 트러스트 보안 가이드 안내

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

제로 트러스트 아키텍처 및 보안(입문)

제로 트러스트 보안은 기존의 네트워크 경계 모델을 '절대 신뢰하지 말고 항상 검증하라'는 엄격한 정책으로 대체합니다. 마이크로 세분화, ID 및 접근 관리(IAM), 최소 권한, 상태 점검을 적용하면 위협의 횡적 이동을 막을 수 있습니다.

각 체크포인트를 주의 깊게 읽고 올바른 답을 선택하거나 쓰세요.

체크포인트 1: 객관식 도전

1. 1. 제로 트러스트 보안의 핵심 원칙은 무엇입니까?
   - A. 출처와 관계없이 모든 접근 요청을 절대 신뢰하지 않고 항상 검증함
   - B. 기업 방화벽 안쪽의 모든 트래픽이 안전하다고 가정하기
   - C. 속도를 높이려고 데이터베이스 파일을 암호화하지 않고 저장하기
   - D. SPF 레코드만으로 이메일 인증 적용하기

2. 2. 네트워크 마이크로 세그멘테이션이란 무엇입니까?
   - A. 네트워크를 작고 격리된 구역으로 나눠 수평 이동을 차단함
   - B. 데이터 전송 중 네트워크 카드 암호화하기
   - C. 모든 로컬 서버를 하나의 공인 IP 주소에 연결하기
   - D. 브라우저 세션에서 사용자 키 입력 감시하기

3. 3. 최소 권한 원칙이란 무엇입니까?
   - A. 사용자 접근 권한을 업무에 꼭 필요한 것으로만 제한함
   - B. 기본적으로 모든 사용자에게 모든 시스템 권한 주기
   - C. 기업 데이터베이스 서버에 익명 로그인 허용하기
   - D. 비밀번호 없이 공용 Wi-Fi 라우터 구성하기

4. 4. ID 및 접근 관리(IAM)란 무엇입니까?
   - A. 디지털 신원을 관리하고 시스템 권한을 제어하는 프레임워크
   - B. 로컬 파일 디렉터리를 검사하는 백신 유틸리티
   - C. 에어갭 매체를 사용하는 백업 저장 시스템
   - D. 위조된 도메인을 거부하는 이메일 게이트웨이 프로토콜

5. 5. 지속적 인증이란 무엇을 의미합니까?
   - A. 활성 세션 중에 사용자 신원과 기기 상태를 반복해서 검증함
   - B. 마스터 비밀번호를 10분마다 바꾸기
   - C. 여러 알고리즘으로 데이터베이스 레코드 해시하기
   - D. TLS 키로 네트워크 전송 패킷 암호화하기

체크포인트 2: 참/거짓 도전

6 질문 6

6. 제로 트러스트는 기업 방화벽 안의 모든 트래픽이 안전하다고 가정합니다.

○ 참 ○ 거짓

7 질문 7

7. 마이크로 세분화는 공격자가 내부 서버 사이를 옆으로 이동하는 능력을 제한합니다.

○ 참 ○ 거짓

8 질문 8

8. 최소 권한은 기본적으로 모든 데이터베이스 파일에 대한 접근 권한을 부여합니다.

○ 참 ○ 거짓

9 질문 9

9. 지속적 검증은 로그인 세션 내내 기기 상태와 자격 증명을 확인합니다.

○ 참 ○ 거짓

10 질문 10

10. 제로 트러스트를 도입하면 탈취된 기업 로그인으로 인한 영향이 줄어듭니다.

○ 참 ○ 거짓

체크포인트 3: 핵심 용어 채우기

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

1. 모든 접근 지점에서 자격 증명을 요구하는 것은 지속적인 _____ 입니다.
2. 기업 네트워크를 아주 작은 구역으로 나누는 것은 마이크로 _____ 입니다.
3. 디지털 신원과 접근 제어를 구성할 때는 _____ 시스템을 사용합니다.
4. 사용자가 가질 수 있는 접근 범위를 제한하는 것은 최소 _____ 원칙에 따른 것입니다.
5. 연결된 기기의 건강 상태를 평가하려면 기기 _____ 을(를) 점검합니다.
6. 세션을 기록하고 검토하는 것은 보안 _____ 입니다.

어휘 단어 목록

감사 검증 권한 라우터 방화벽 보안 상태 세분화 IAM

여기에 답을 쓰세요:

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

체크포인트 4: 보안 개념 연결

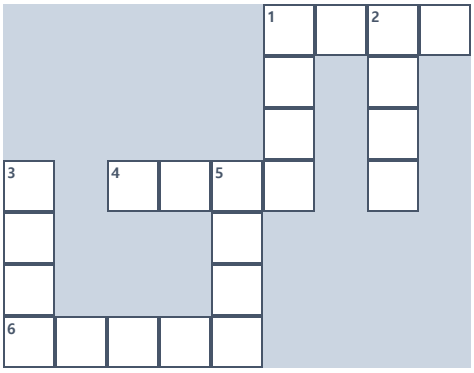
정의 연결하기

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

☐	**1. 검증**	**A**	사용자 인증 정보 접근 관리하기.
☐	**2. 세분화**	**B**	최소 접근 권한 원칙.
☐	**3. IAM**	**C**	네트워크 패킷 트래픽 라우팅.
☐	**4. 권한**	**D**	외부 네트워크 장벽 보호.
☐	**5. 보안 상태**	**E**	기록된 접근 세션 검토.
☐	**6. 감사**	**F**	내부 네트워크 영역 분리.
☐	**7. 방화벽**	**G**	항상 사용자 자격 증명을 확인함.
☐	**8. 라우터**	**H**	기기 상태 평가.

체크포인트 5: 십자말풀이

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



가로

1. 조직이 정보를 지키기 위해 정해 둔 규칙 (4)

4. 접속하는 기기가 보안 기준에 맞는지를 나타내는 상태 (4)

6. 접속하는 사람이 본인이 맞는지 확인하는 일 (5)

세로

1. 기기와 시스템이 얼마나 안전한 상태인지를 나타내는 정도 (4)

2. 접근을 허용할지 판단하는 규칙을 적용하는 시스템 (4)

3. 접근 기록을 살펴 보안 규칙이 지켜지는지 점검하는 일 (4)

5. 사용자와 기기를 접속하는 동안 계속 확인하는 일 (4)

체크포인트 5 대체 활동: 접근성을 고려한 십자말풀이 단서

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

가로

1 가로: 조직이 정보를 지키기 위해 정해 둔 규칙 (4 글자):

4 가로: 접속하는 기기가 보안 기준에 맞는지를 나타내는 상태 (4 글자):

6 가로: 접속하는 사람이 본인이 맞는지 확인하는 일 (5 글자):

세로

1 세로: 기기와 시스템이 얼마나 안전한 상태인지를 나타내는 정도 (4 글자):

2 세로: 접근을 허용할지 판단하는 규칙을 적용하는 시스템 (4 글자):

3 세로: 접근 기록을 살펴 보안 규칙이 지켜지는지 점검하는 일 (4 글자):

5 세로: 사용자와 기기를 접속하는 동안 계속 확인하는 일 (4 글자):

체크포인트 6: 숨은 단어 찾기

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

라 용 주 다 안 검 하 워 색 도 진 스 타 비 접
결 방 네 개 암 라 메 카 기 다 리 넷 접 워 감
카 안 파 다 이 워 호 템 데 기 보 송 보 개 터
타 보 바 리 태 나 트 인 소 술 상 호 태 송 시
답 계 다 격 터 사 파 터 증 밀 경 태 개 책 서
속 경 암 자 관 용 기 정 버 이 험 밀 개 증 공
송 아 주 시 템 자 하 벽 책 용 바 가 마 사 결
엔 화 터 엔 방 인 증 메 넷 엔 타 위 밀 인 카
태 기 이 데 방 증 공 속 트 번 진 번 격 험 시
상 메 도 네 사 스 공 송 정 리 바 답 카 스 계
안 상 시 검 증 요 아 태 답 서 넷 워 감 차 보
보 데 타 위 보 상 속 사 소 마 가 감 전 안 카
방 나 타 송 안 타 안 워 기 차 험 격 감 밀 하
기 리 태 스 정 안 위 응 보 나 다 사 위 결 이
속 메 책 공 책 터 관 주 리 자 데 경 마 서 리

어휘 단어 목록

상시검증 보안정책 정책엔진 사용자인증 경계보안 보안상태 기기상태 보안감사

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. 상시검증
B. 보안정책
C. 정책엔진
D. 사용자인증
E. 경계보안
F. 보안상태
G. 기기상태
H. 보안감사

정의 및 연결 항목
1. 접속하는 기기가 보안 기준에 맞는지를 나타내는 상태.
2. 기기와 시스템이 얼마나 안전한 상태인지를 나타내는 정도.
3. 접속하는 사람이 본인이 맞는지 확인하는 일.
4. 조직이 정보를 지키기 위해 정해 둔 규칙.
5. 접근 기록을 살펴 보안 규칙이 지켜지는지 점검하는 일.
6. 내부와 외부 사이에 벽을 세워 지키는 전통적인 보안 방식.
7. 접근을 허용할지 판단하는 규칙을 적용하는 시스템.
8. 사용자와 기기를 접속하는 동안 계속 확인하는 일.

체크포인트 7: 뒤섞인 단어 도전

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

1. **검 상 증 시** _____

2. **정 엔 진 책** _____

3. **안 경 보 계** _____

4. **태 상 기 기** _____

5. **책 보 정 안** _____

6. **인 사 자 증 용** _____

7. **상 보 태 안** _____

8. **보 사 감 안** _____

보너스 활동: 빠르게 생각하기

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

1	절대 공유하면 안 되는 정보			
2	오늘부터 시작할 수 있는 안전 습관			
3	기기에서 확인하는 것			
4	기록되는 것			
5	사이버 보안과 관련된 단어			
6	제로 트러스트가 확인하는 것			
7	일상에서 신분증을 보여 주는 곳			
8	진짜 본인임을 증명하는 방법			
9	데이터가 유출된 후에 할 일			
10	컴퓨터가 감염되었다는 신호			
11	소프트웨어를 업데이트하는 이유			
12	회사의 접근 수준			
13	알고 있는 보안 도구			
14	네트워크를 나눌 수 있는 구역			
15	신뢰에 관한 속담			

체크포인트 8: 사이버 보안 사례 연구

배운 개념을 적용하여 아래의 실제 시나리오를 해결하세요.

사례 연구 1: 제로 트러스트 네트워크 아키텍처로 전환하기



상황: 한 대기업이 현재 로컬 네트워크에 있는 어떤 기기든 모든 회사 서버와 데이터베이스에 접근할 수 있는 평면적인 내부 네트워크를 사용하고 있습니다.

토론 질문: 횡적 이동을 제한하는 네트워크 마이크로 세분화 전략을 설계하세요.

사례 연구 2: 최소 권한 접근 제어 적용하기



상황: 감사 로그를 보니 임시 데이터베이스 사용자와 하급 직원이 중요한 회계 데이터베이스에 대한 전역 읽기 및 쓰기 권한을 가지고 있습니다.

토론 질문: 최소 권한을 시행하도록 데이터베이스 IAM 권한을 감사하고 제한하세요.

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

13	25	6	28		17	38	6	24	10	38	17	38	6	28

19	20	12	10	20	12		19	29	1	12	40	3	19	20	10	25	12	32

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: 제로 트러스트란 무엇인가요?

제로 트러스트는 위협이 네트워크 경계 바깥과 안쪽 모두에 존재한다고 가정하고 모든 요청에 대한 검증을 요구하는 보안 프레임워크입니다. [1]

Q2: 제로 트러스트의 핵심 원칙은 무엇인가요?

절대 신뢰하지 말고 항상 검증하라.

Q3: 마이크로 세그멘테이션이란 무엇인가요?

네트워크를 작고 안전한 논리적 구역으로 나누어 트래픽을 통제하고 침해를 가두는 방식.

Q4: 최소 권한이란 무엇인가요?

사용자에게 특정 업무를 수행하는 데 필요한 최소한의 접근 권한만 부여하는 것. [2]

Q5: IAM은 무엇의 약자인가요?

신원 및 접근 관리.

체크포인트 10: 기초 사이버 보안 FAQ (파트 B)

온라인 위협 대응에 관한 자주 묻는 질문과 답을 살펴보세요.

Q6: 기기 상태 점검은 어떤 도움이 되나요?

접근을 허용하기 전에 기기에 패치가 적용되었는지, 활성 바이러스 백신이 실행 중인지, 안전한지 확인합니다.

Q7: 측면 이동이란 무엇인가요?

공격자가 처음 침해한 노드에서 더 가치 있는 시스템으로 네트워크 안을 이동하는 과정입니다.

Q8: 제로 트러스트가 방화벽을 대체하나요?

아니요, 신원 중심 확인과 내부 분리 방화벽을 추가하여 이를 강화합니다.

Q9: 지속적 인증이란 무엇인가요?

처음 로그인할 때뿐 아니라 로그인 세션이 유지되는 동안 계속 사용자 신원을 확인하는 것.

Q10: 플랫 네트워크는 왜 위험한가요?

플랫 네트워크에서는 노드 하나만 탈취되어도 공격자가 네트워크의 모든 데이터베이스에 쉽게 접근할 수 있습니다.

체크포인트 10: 심화 보안 FAQ (파트 C)

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

Q1: 제로 트러스트는 경계 모델 문제를 어떻게 해결하나요?

구식 '성과 해자' 모델을 대체하여 방어의 중심을 경계 네트워크에서 특정 사용자 신원과 리소스로 옮깁니다.

Q2: 정책 결정 지점(PDP)이란 무엇인가요?

접근을 허용할지 결정하기 위해 보안 규칙에 따라 권한 요청을 평가하는 시스템 구성 요소입니다.

Q3: 정책 시행 지점(PEP)이란 무엇인가요?

PDP의 결정에 따라 연결 요청을 실제로 허용하거나 차단하는 시스템 노드(게이트웨이나 프록시 등)입니다.

Q4: 역할 기반 접근 제어(RBAC)는 제로 트러스트를 어떻게 뒷받침하나요?

RBAC는 권한을 특정 역할로 묶어 사용자가 과도한 관리자 권한을 물려받는 것을 막는 데 도움이 됩니다.

Q5: 상황 인식 접근 제어란 무엇인가요?

위치, 기기 상태, 로그인 시간 같은 보조 단서를 사용해 로그인 요청을 평가하여 위험을 판단하는 것.

체크포인트 10: 심화 보안 FAQ (파트 D)

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

Q6: 마이크로 세그멘테이션은 일반 VLAN과 어떻게 다른가요?

VLAN은 2계층에서 네트워크를 넓은 논리 구획으로 나누는 반면, 마이크로 세분화는 소프트웨어 정책으로 개별 워크로드를 격리합니다.

Q7: 적시(JIT) 접근이란 무엇인가요?

상승된 관리자 권한을 일시적으로 부여하고 작업이 끝나면 자동으로 회수하는 것.

Q8: 제로 트러스트 프레임워크에서 API를 어떻게 보호하나요?

암호화 서명된 OAuth 토큰을 요구하고 모든 API 게이트웨이에서 요청 서명을 감사함으로써.

Q9: 제로 트러스트 네트워크 접근(ZTNA) 클라이언트란 무엇인가요?

원시 네트워크 서브넷이 아니라 특정 애플리케이션으로 안전한 암호화 송신 연결을 만드는 소프트웨어 에이전트.

Q10: 로그 감사는 제로 트러스트에 어떻게 도움이 되나요?

지속적인 로그 기록 덕분에 자동화된 보안 분석 도구가 이상 징후를 감지하고 비정상 로그인을 즉시 중지할 수 있습니다.

파트 11: 실제 사이버 보안 사실 10가지와 시사점

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

1. 보안 인사이트

제로 트러스트 아키텍처는 기존의 성과 해자 모델을 신원 중심의 검증 규칙으로 대체합니다.

2. 보안 인사이트

네트워크 마이크로 세분화는 워크로드를 작고 보호된 영역으로 격리하여 악성코드가 도달할 수 있는 범위를 줄입니다.

3. 보안 인사이트

제로 트러스트는 네트워크 구간이 아니라 자산, 서비스, 계정 같은 리소스를 보호하는 데 중점을 둡니다. [1]

4. 보안 인사이트

최소 권한 접근 정책은 핵심 데이터베이스에서 내부자가 데이터를 유출할 위험을 줄입니다.

5. 보안 인사이트

기기 상태 검증은 운영체제 패치 수준과 활성 백신 상태를 실시간으로 확인합니다.

6. 보안 인사이트

제로 트러스트 네트워크 접근(ZTNA) 브로커는 기업 VPN을 대체하거나 보완하여 사용자 접근 범위를 제한할 수 있습니다.

7. 보안 인사이트

Just-in-Time(JIT) 관리자 권한 위임은 도메인 컨트롤러에서 인증 정보 탈취 위험을 줄입니다.

8. 보안 인사이트

지속적인 검증은 세션 동작을 기록하고 감사하며, 비정상적인 스크립트 실행 패턴을 보이는 사용자를 중지시킵니다.

9. 보안 인사이트

관리자 자격 증명이 유출되면 기존의 경계 방어로는 횡적 공격을 막지 못합니다.

10. 보안 인사이트

NIST 특별 간행물 800-207(2020)은 배포 모델과 함께 제로 트러스트 아키텍처의 추상적인 정의를 제시합니다. [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] NIST. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[2] CISA. (2023). Zero Trust Maturity Model.
https://www.cisa.gov/zero-trust-maturity-model

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

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

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

답안: 체크포인트 1 – 객관식

1 질문 1 정답: A

교사용 참고

제로 트러스트 보안의 핵심 원칙은 무엇입니까? → 출처와 관계없이 모든 접근 요청을 절대 신뢰하지 않고 항상 검증함

2 질문 2 정답: A

교사용 참고

네트워크 마이크로 세그멘테이션이란 무엇입니까? → 네트워크를 작고 격리된 구역으로 나눠 수평 이동을 차단함

3 질문 3 정답: A

교사용 참고

최소 권한 원칙이란 무엇입니까? → 사용자 접근 권한을 업무에 꼭 필요한 것으로만 제한함

4 질문 4 정답: A

교사용 참고

ID 및 접근 관리(IAM)란 무엇입니까? → 디지털 신원을 관리하고 시스템 권한을 제어하는 프레임워크

5 질문 5 정답: A

교사용 참고

지속적 인증이란 무엇을 의미합니까? → 활성 세션 중에 사용자 신원과 기기 상태를 반복해서 검증함

답안: 체크포인트 2 – 참 또는 거짓

6 질문 6 정답: 거짓

교사용 참고

거짓: 제로 트러스트는 내부든 외부든 네트워크 위치를 근거로 한 암묵적 신뢰를 부여하지 않습니다.

7 질문 7 정답: 참

교사용 참고

참: 작고 격리된 구역은 침입자가 서버 사이를 이동할 수 있는 범위를 제한합니다.

8 질문 8 정답: 거짓

교사용 참고

거짓: 최소 권한은 각 역할에 필요한 최소한의 접근만 부여합니다.

9 질문 9 정답: 참

교사용 참고

지속적 검증은 로그인 세션 내내 기기 상태와 자격 증명을 확인합니다.

10 질문 10 정답: 참

교사용 참고

제로 트러스트를 도입하면 탈취된 기업 로그인으로 인한 영향이 줄어듭니다.

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

G 1. 검증	F 2. 세분화	A 3. IAM	B 4. 권한
H 5. 보안 상태	E 6. 감사	D 7. 방화벽	C 8. 라우터

체크포인트 3: 답안 – 핵심 용어

1 검증	2 세분화	3 IAM	4 권한
5 보안 상태	6 감사		

체크포인트 6 대체 활동: 답안 – 단어 연결

1 G – 기기상태	2 F – 보안상태	3 D – 사용자인증	4 B – 보안정책
5 H – 보안감사	6 E – 경계보안	7 C – 정책엔진	8 A – 상시검증

교사를 위한 토론 참고

핵심 용어:
학생들이 검증, 세분화, IAM을(를) 자신의 말로 설명하고 각각 예를 들 수 있는지 확인하세요.

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

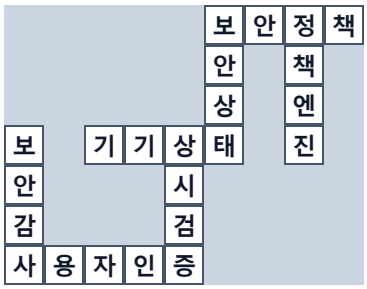
출처 평가:
학생들에게 워크시트의 참고 자료로 주장을 하나 이상 확인하게 하고, 수치·가격·규정이 시간이 지나면서 바뀔 수 있는 이유를 토론하게 하세요.

퍼즐 답안과 교사용 참고

단어 찾기 정답

라	용	주	다	안	검	하	워	색	도	진	스	타	비	접
결	방	네	개	암	라	메	카	기	다	리	넷	접	워	감
카	안	파	다	이	워	호	템	데	기	보	송	보	개	터
타	보	바	리	태	나	트	인	소	술	상	호	태	송	시
답	계	다	격	터	사	파	터	증	밀	경	태	개	책	서
속	경	암	자	관	용	기	정	버	이	험	밀	개	증	공
송	아	주	시	템	자	하	벽	책	용	바	가	마	사	결
엔	화	터	엔	방	인	증	메	넷	엔	타	위	밀	인	카
태	기	이	데	방	증	공	속	트	번	진	번	격	험	시
상	메	도	네	사	스	공	송	정	리	바	답	카	스	계
안	상	시	검	증	요	아	태	답	서	넷	워	감	차	보
보	데	타	위	보	상	속	사	소	마	가	감	전	안	카
방	나	타	송	안	타	안	워	기	차	험	격	감	밀	하
기	리	태	스	정	안	위	응	보	나	다	사	위	결	이
속	메	책	공	책	터	관	주	리	자	데	경	마	서	리

십자말풀이 정답



십자말풀이 정답 교사용 안내

가로

1 가로: 보안정책 조직이 정보를 지키기 위해 정해 둔 규칙 (4 글자)

4 가로: 기기상태 접속하는 기기가 보안 기준에 맞는지를 나타내는 상태 (4 글자)

6 가로: 사용자인증 접속하는 사람이 본인이 맞는지 확인하는 일 (5 글자)

세로

1 세로: 보안상태 기기와 시스템이 얼마나 안전한 상태인지를 나타내는 정도 (4 글자)

2 세로: 정책엔진 접근을 허용할지 판단하는 규칙을 적용하는 시스템 (4 글자)

3 세로: 보안감사 접근 기록을 살펴 보안 규칙이 지켜지는지 점검하는 일 (4 글자)

5 세로: 상시검증 사용자와 기기를 접속하는 동안 계속 확인하는 일 (4 글자)

뒤섞인 단어 및 암호 해독 답안

어휘 단어 맞추기 활동과 비밀 암호 도전의 채점 기준.

단어 맞추기 정답

1. 검상증시 — **상시검증**
2. 정엔진책 — **정책엔진**
3. 안경보계 — **경계보안**
4. 태상기기 — **기기상태**
5. 책보정안 — **보안정책**
6. 인사자증용 — **사용자인증**
7. 상보태안 — **보안상태**
8. 보사감안 — **보안감사**

비밀 암호 도전 정답

"제로 트러스트로 항상 확인하세요"

사례 연구 답안

A 사례 연구 1: 제로 트러스트 네트워크 아키텍처로 전환하기

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 상황 분석: 한 대기업이 현재 로컬 네트워크의 어떤 기기든 모든 회사 서버와 데이터베이스에 접근할 수 있는 평면 내부 네트워크를 사용합니다.
- 권장 전략 및 해결책: 평면 네트워크를 부서별로 격리된 영역으로 분리하세요. 내부 방화벽을 설치해 영역 간 트래픽을 통제하고, 모든 접근에 연결 토큰 검증을 의무화합니다.

B 사례 연구 2: 최소 권한 접근 제어 적용하기

교사용 풀이

채점 기준

학생 답안에는 다음 사항이 포함되어야 합니다.

- 시나리오 분석: 감사 로그를 보니 임시 데이터베이스 사용자와 하위 직원들이 핵심 회계 데이터베이스에 대한 전체 읽기 및 쓰기 권한을 가지고 있습니다.
- 권장 전략 및 해결책: 모든 전역 관리자 권한을 회수하세요. 실제 직무에 맞게 역할 기반 접근 제어(RBAC)를 도입하고, 매주 자동으로 권한을 검토하도록 하세요.