DELL Technologies

대화형 사이버 보안 시나리오 EBOOK

실제 시나리오. 더 스마트한 의사 결정. 더욱 강력한 방어.

보안에 대한 Dell의 노력은 Dell Technologies가 하는 모든 일의 핵심입니다. 이 eBook은 통찰력, 모범 사례 및 혁신적인 기술을 공유하여 새로운 사이버 위협에 미리 대비하는 데 필요한 툴과 지식을 제공하는 것을 목표로 합니다.

공격 시나리오 선택

사이버 보안 위협은 끊임없이 진화하고 있으며, 조직은 데이터를 보호하기 위해 효과적으로 대응해야 합니다. 조직이 가장 효과적으로 준비 태세를 갖추도록 하려면, 사이버 공격에 대처하기 위한 사이버 보안 전략을 안내하는 실제 시뮬레이션 연습에 몰입하십시오.

연방, 주, 지방 정부, 금융 서비스, 의료 등 다양한 부문에서 다양한 공격 유형과 산업별 당면 과제를 살펴보십시오. 이 과정에서 노트북 및 데스크탑에서 엔터프라이즈 시스템에 이르기까지 Dell의 통합 보안 솔루션이 이러한 위협으로부터 보호하도록 어떻게 구축되었는지 알아볼 수 있습니다.

- 백업 침투 →
- 랜섬웨어 →
- DDoS(Distributed Denial of Service) →
- 공급망 하드웨어 →
- 악의적인 내부자 →
- 공급망 소프트웨어 →
- MITM(Man-in-the-Middle) →
- 제로 데이 →
- 프롬프트/SQL 삽입 →

공격 유형: 백업 침투

클라우드 백업 서비스 공급업체의 관리자로서, 어느 날 저녁 손실된 일부 데이터를 복원하려고 하는 고객으로부터 전화를 받습니다.

클라우드에서 복구를 여러 번 시도했지만, 복구가 항상 실패했습니다.

사무실에 가보니 컴퓨터 화면에 모든 데이터가 암호화됐다고 표시되어 있었고, 필요한 데이터에 다시 접근하려면 랜섬을 지불해야 했습니다.

이해도 테스트 →

공격 유형: 백업 침투

1: 공격 노출 지점 최소화 — 2 — 3 — 4

어떤 백업 시스템 또는 고객이 영향을 받았는지 확실하지 않습니다. 가장 먼저 무엇을 해야 합니까?

- [ ] 관련 당국에 알림
- [ ] 모든 시스템 종료
- [ ] 위협을 억제하고 격리 시도
- [ ] 복원할 수 있는 안전한 백업이 있는지 확인

정답 확인하기 →

공격 유형: 백업 침투

1: 공격 노출 지점 최소화 — 2 — 3 — 4

어떤 백업 시스템 또는 고객이 영향을 받았는지 확실하지 않습니다. 가장 먼저 무엇을 해야 합니까?

- ✗ 관련 당국에 알림
- ✗ 모든 시스템 종료
- ✓ 위협을 억제하고 격리 시도
- ✗ 복원할 수 있는 안전한 백업이 있는지 확인

위협을 즉시 억제하고 격리하면 추가 확산이나 피해를 방지하고 인시던트 범위를 평가할 시간을 확보할 수 있으며, AI를 포함한 모든 유형의 사이버 공격에 미치는 영향을 최소화할 수 있습니다.

다음 질문 →

공격 유형: 백업 침투

1 — 2: 사이버 위협 탐지 및 대응 — 3 — 4

고객의 데이터를 신속하게 사용할 수 있도록 하는 것이 최우선 과제입니다. 이를 어떻게 달성하시겠습니까?

- [ ] 랜섬 비용 지불
- [ ] 랜섬웨어 유형 파악
- [ ] 관련 당국에 알림
- [ ] 손상된 데이터 식별

정답 확인하기 →

공격 유형: 백업 침투

1 — 2: 사이버 위협 탐지 및 대응 — 3 — 4

고객의 데이터를 신속하게 사용할 수 있도록 하는 것이 최우선 과제입니다. 이를 어떻게 달성하시겠습니까?

- ✗ 랜섬 비용 지불
- ✗ 랜섬웨어 유형 파악
- ✗ 관련 당국에 알림
- ✓ 손상된 데이터 식별

손상된 데이터를 식별하면 가장 중요한 고객 정보를 복원하는 데 복구 노력을 집중하고, 더 빠른 데이터 가용성을 보장하며, 영향을 받지 않는 시스템에서 불필요한 작업을 방지하는 데 도움이 됩니다.

다음 질문 →

공격 유형: 백업 침투

1 2 3: 사이버 공격으로부터 복구 4

복구할 백업이 있는지 파악했습니다. 프로세스의 첫 번째 단계는 무엇입니까?

- [ ] 중요한 시스템 복구 우선순위 지정
- [ ] 포렌식 분석을 사용하여 공격이 완전히 억제되었는지 확인
- [ ] 모든 비밀번호를 변경하고 손상된 자격 증명 해지
- [ ] 제로 트러스트(zero trust) 원칙 구현

정답 확인하기 →

공격 유형: 백업 침투

1 2 3: 사이버 공격으로부터 복구 4

복구할 백업이 있는지 파악했습니다. 프로세스의 첫 번째 단계는 무엇입니까?

- ✗ 중요한 시스템 복구 우선순위 지정
- ✓ 포렌식 분석을 사용하여 공격이 완전히 억제되었는지 확인
- ✗ 모든 비밀번호를 변경하고 손상된 자격 증명 해지
- ✗ 제로 트러스트(zero trust) 원칙 구현

시스템을 복원하기 전에 사용자 환경 내에서 위협이 악화되거나 확산되지 않도록 하기 위해 공격이 완전히 억제되었는지 확인하여 우발적 재감염 및 추가 손상이 방지되도록 해야 합니다.

다음 질문 →

공격 유형: 백업 침투

1 2 3 4: 전반적인 모범 사례

향후 이러한 상황이 발생할 위험을 완화할 수 있는 방법은 무엇입니까?

- [ ] 제로 트러스트(zero trust) 원칙 활용
- [ ] EDR(Endpoint Detection and Response) 기능 활성화
- [ ] 변경 불가능한 에어 갭 백업 구현
- [ ] 모두 해당

정답 확인하기 →

공격 유형: 백업 침투

1 2 3 4: 전반적인 모범 사례

향후 이러한 상황이 발생할 위험을 완화할 수 있는 방법은 무엇입니까?

- [x] 제로 트러스트(zero trust) 원칙 활용
- [x] EDR(Endpoint Detection and Response) 기능 활성화
- [x] 변경 불가능한 에어 갭 백업 구현
- [x] 모두 해당

단일 조치만으로는 충분하지 않기 때문에 다중 계층 방어 전략을 사용하면 위험을 줄이고, 피해를 최소화하며, 조직의 회복탄력성을 높일 수 있습니다.

솔루션 보기 →

공격 유형: 백업 침투

요약

백업 침투는 사이버 범죄자가 백업 시스템의 취약성을 악용하여 중요한 복구 데이터를 손상, 파괴 또는 암호화할 때 발생합니다. 이러한 정교한 공격은 랜섬웨어나 멀웨어 배포와 같은 다른 사고와 동시에 발생하거나 후속적으로 발생할 수 있으며, 이는 운영 및 재정적 피해를 증폭시킵니다.

Dell Technologies는 조직들이 진화하는 사이버 위협에 맞서 회복탄력성을 유지할 수 있도록 지원하는 것을 중요하게 생각합니다. Dell Technologies는 최첨단 솔루션, 전문가 서비스 및 신뢰할 수 있는 파트너십을 통해 가장 중요한 것을 보호할 수 있도록 도와드립니다.

Dell Technologies의 솔루션과 오늘날의 가장 까다로운 사이버 당면 과제를 해결하는 방법에 대해 자세히 알아보십시오.

백업 침투 브리프 살펴보기 →

⌂ 시나리오로 돌아가기

PowerProtect 포트폴리오 ›

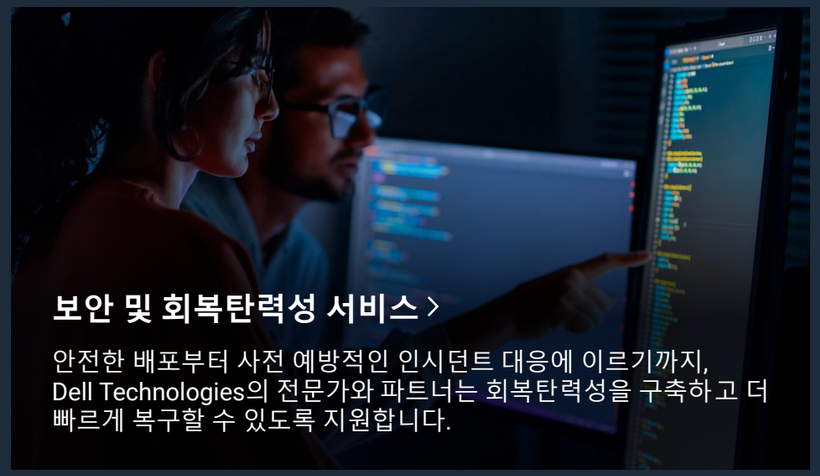
Dell Technologies의 AI 기반 CyberSense 분석 기반의 변경 불가능한 에어 갭 암호화 백업 볼트는 회복탄력성을 유지할 수 있도록 신속한 탐지 및 복구를 보장합니다.

PowerEdge 서버 ›

Dell Technologies는 보안 부팅, 하드웨어 RoT(Root of Trust) 및 시스템 잠금 기능을 통해 백업 데이터를 보호할 수 있는 믿을 만한 인프라스트럭처를 제공합니다.

신뢰할 수 있는 작업 공간 ›

SafeBIOS 및 SafeData 보호 기능은 위험을 최소화하여 백업 시스템이 훼손되지 않고 필요할 때 바로 사용할 수 있도록 합니다.



보안 및 회복탄력성 서비스 ›

안전한 배포부터 사전 예방적인 인시던트 대응에 이르기까지, Dell Technologies의 전문가와 파트너는 회복탄력성을 구축하고 더 빠르게 복구할 수 있도록 지원합니다.

네트워킹 솔루션 ›

Dell은 네트워크 세분화, MFA(Multi-Factor Authentication) 및 최소 권한 구성을 통해 접근을 차단하고 중요한 데이터를 보호할 수 있도록 지원합니다.

공격 유형: DDoS(Distributed Denial of Service)

큰 눈보라가 예상되는 화요일 오후, 어느 주 정부 기관의 사무실입니다.

다음과 같은 업무를 위해 시스템에 접속해야 하는데 접속이 불가능하다는 상담원의 전화가 교통부 IT 팀에 빗발칩니다.

- 운전면허증 갱신
- 도로 통행 허가서 받기
- 세금 납부
- 도로 상태 점검
- 비상 대응 시스템을 가동하여 도로 작업 팀의 눈/빙판 제거 작업을 늦추게 함

이 모든 것이 시스템 시간 초과로 인해 발생했습니다.

이해도 테스트 →

공격 유형: DDoS(Distributed Denial of Service)

1: 공격 노출 지점 최소화 2 3 4

어떤 일이 일어날 수 있는지 가장 먼저 확인할 곳은 어디입니까?

- [ ] 네트워크 디바이스에서 원인 불명의 인바운드 트래픽이 갑자기 증가하고 있는지 확인
- [ ] 네트워크 디바이스에 단일 또는 제한된 수의 IP 주소에서 발생하는 비정상적인 트래픽이 있는지 확인
- [ ] 방화벽 또는 네트워크 가시성 툴 로그에서 과도한 연결 실패 또는 트래픽 차단 이벤트가 있는지 확인
- [ ] 모두 해당

정답 확인하기 →

공격 유형: DDoS(Distributed Denial of Service)

1: 공격 노출 지점 최소화 — 2 — 3 — 4

어떤 일이 일어날 수 있는지 가장 먼저 확인할 곳은 어디입니까?

- [x] 네트워크 디바이스에서 원인 불명의 인바운드 트래픽이 갑자기 증가하고 있는지 확인
- [x] 네트워크 디바이스에 단일 또는 제한된 수의 IP 주소에서 발생하는 비정상적인 트래픽이 있는지 확인
- [x] 방화벽 또는 네트워크 가시성 툴 로그에서 과도한 연결 실패 또는 트래픽 차단 이벤트가 있는지 확인
- [x] 모두 해당

광범위한 시스템 운영 중단을 올바르게 진단하려면 네트워크 디바이스 활동과 방화벽 또는 가시성 툴 로그를 동시에 검토하여 비정상적인 패턴이나 차단 이벤트를 신속하게 찾아내야 합니다. 이를 통해 사이버 인시던트와 인프라스트럭처 문제를 구분할 수 있으므로 더 빠르고 정확한 인시던트 대응이 가능합니다.

다음 질문 →

공격 유형: DDoS(Distributed Denial of Service)

1 — 2: 사이버 위협 탐지 및 대응 — 3 — 4

DDoS 공격으로 의심되는 상황이 발생했습니다. 가장 먼저 할 일은 무엇입니까?

- [ ] DDOS 완화 서비스를 통해 모든 네트워크 트래픽 리디렉션
- [ ] WAF(Web Application Firewall) 규칙을 활성화하여 악의적인 패턴 필터링
- [ ] 트래픽 급증이 정상적인 소스에서 발생한 것인지 확인
- [ ] 내부적으로 그리고 외부적으로 현재 상황을 보고

정답 확인하기 →

공격 유형: DDoS(Distributed Denial of Service)

1 — 2: 사이버 위협 탐지 및 대응 — 3 — 4

DDoS 공격으로 의심되는 상황이 발생했습니다. 가장 먼저 할 일은 무엇입니까?

- ✗ DDOS 완화 서비스를 통해 모든 네트워크 트래픽 리디렉션
- ✗ WAF(Web Application Firewall) 규칙을 활성화하여 악의적인 패턴 필터링
- ✓ 트래픽 급증이 정상적인 소스에서 발생한 것인지 확인
- ✗ 내부적으로 그리고 외부적으로 현재 상황을 보고

DDoS 대응 조치를 활성화하기 전에 트래픽 급증의 진위를 확인하는 것이 중요합니다. 이를 통해 실수로 정품 사용자를 차단하는 것을 방지하고, 중요한 이해 관계자들의 운영 중단을 방지하며, 추가적인 보호 조치가 적절하고 정확하게 타겟팅되도록 하여 공공 운영과 전반적인 비즈니스 연속성에 부정적인 영향이 미치는 것을 최소화할 수 있습니다.

다음 질문 →

공격 유형: DDoS(Distributed Denial of Service)

1 — 2 — 3: 사이버 공격으로부터 복구 — 4

향후 DDoS 공격을 방지하기 위해 어떤 조치를 취할 수 있습니까?

- [ ] 문제가 되는 IP 주소 차단
- [ ] DDoS 시뮬레이션을 통한 정기적인 침투 테스트 수행
- [ ] 클라우드 공급업체는 일반적으로 DDoS 공격을 받지 않으므로 모든 애플리케이션을 클라우드로 이동
- [ ] 제로 트러스트 원칙 구현

정답 확인하기 →

공격 유형: DDoS(Distributed Denial of Service)

1 — 2 — 3: 사이버 공격으로부터 복구 — 4

향후 DDoS 공격을 방지하기 위해 어떤 조치를 취할 수 있습니까?

- ✗ 문제가 되는 IP 주소 차단
- ✓ DDoS 시뮬레이션을 통한 정기적인 침투 테스트 수행
- ✗ 클라우드 공급업체는 일반적으로 DDoS 공격을 받지 않으므로 모든 애플리케이션을 클라우드로 이동
- ✓ 제로 트러스트 원칙 구현

DDOS 시뮬레이션을 통한 사전 예방적 침투 테스트는 보안상의 취약점을 식별하여 보강하며, 제로 트러스트 원칙은 항상 최소 권한 액세스를 적용하여 위험을 최소화하는 데 중점을 둡니다. 이를 통해 공격 중에도 기능을 유지해야 하는 긴급 대응 조정 또는 실시간 교통 신호 제어와 같은 필수 시스템이 중단될 위험을 줄일 수 있습니다.

다음 질문 →

공격 유형: DDoS(Distributed Denial of Service)

1 2 3 4: 전반적인 모범 사례

전반적인 IRR(Incident Response and Recovery Plan)의 일환으로 누구에게 알려야 합니까?

- [ ] 법무 팀
- [ ] 사이버 보험 공급업체
- [ ] CISA(Cybersecurity and Infrastructure Security Agency), FBI, MS-ISAC(Multi-State Information Sharing & Analysis Center)
- [ ] 모두 해당

정답 확인하기 →

공격 유형: DDoS(Distributed Denial of Service)

1 2 3 4: 전반적인 모범 사례

전반적인 IRR(Incident Response and Recovery Plan)의 일환으로 누구에게 알려야 합니까?

- [x] 법무 팀
- [x] 사이버 보험 공급업체
- [x] CISA(Cybersecurity and Infrastructure Security Agency), FBI, MS-ISAC(Multi-State Information Sharing & Analysis Center)
- [x] 모두 해당

대규모 사이버 사고 발생 시에는 규정 준수, 손해 배상 청구 및 법 집행과 관련하여 법률, 보험 및 정부 기관과 협력하는 것을 고려해야 합니다. 모든 규제 요건이 충족되었는지 확인한 후에는 조직에서 인시던트를 효과적으로 억제, 해결 및 복구할 수 있습니다.

솔루션 보기 →

공격 유형: DDOS(DISTRIBUTED DENIAL OF SERVICE)

요약

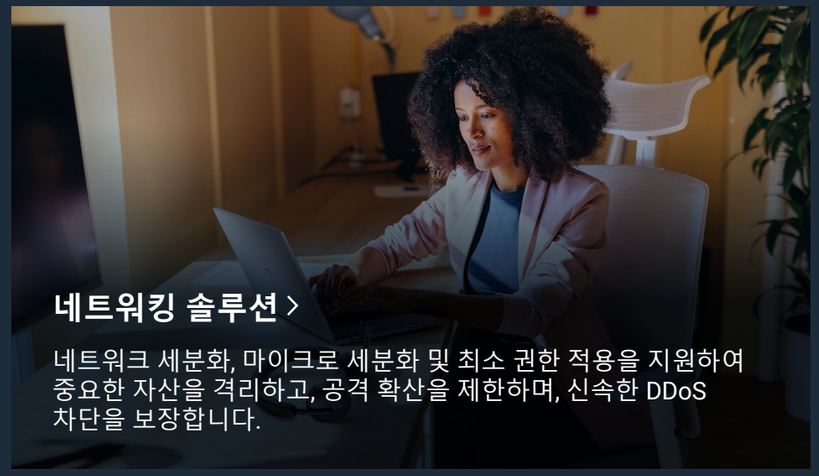
DDoS 공격은 여러 소스에서 발생하는 방대한 양의 트래픽으로 네트워크, 서비스 또는 서버에 과부하를 발생시켜 정상적인 작동을 방해하는 것을 목적으로 합니다. 이러한 공격은 공격자가 원격으로 제어하는 감염된 디바이스 네트워크인 봇넷을 악용하여 실행됩니다.

Dell Technologies는 고급 탐지 및 완화 기술과 전문가 서비스 및 제로 트러스트 접근 방식을 결합하여 조직이 DDoS 공격에 대한 회복탄력성을 유지하도록 지원함으로써 신속한 대응, 운영 중단 최소화, 강화된 방어 체계를 보장합니다.

고급 사이버 회복탄력성 전략에 대해 자세히 알아보고 DDoS 로부터 조직을 보호하는 데 Dell Technologies가 어떤 도움을 줄 수 있는지 자세히 알아보십시오.

DDoS 브리프 살펴보기 →

⌂ 시나리오로 돌아가기



네트워킹 솔루션 >

네트워크 세분화, 마이크로 세분화 및 최소 권한 적용을 지원하여 중요한 자산을 격리하고, 공격 확산을 제한하며, 신속한 DDoS 차단을 보장합니다.

PowerEdge 서버 >

Dell Technologies는 하드웨어 RoT(Root of Trust), 보안 부팅, 시스템 잠금 및 실시간 변조 방지 기능을 통해 회복탄력성이 뛰어난 고성능 DDoS 보호 및 신속한 복구를 제공합니다.

신뢰할 수 있는 디바이스 >

통합된 SafeBIOS, SecureData, 자동화된 탐지 및 대응 기능은 엔드포인트 공격 노출 지점을 최대 70%까지 줄여 DDoS로 인한 주의 분산이 보안 침해로 이어지지 않게 해줍니다.

PowerProtect 포트폴리오 >

AI 기반 위협 분석을 기반으로 하는 암호화되고 변경 불가능한 에어 갭 백업 환경은 DDoS 중단 시 신속하고 검증된 복원을 보장하며 비즈니스 연속성을 유지합니다.

보안 및 회복탄력성 서비스 >

MDR(Manage Detection and Response), IRR(Incident Response and Recovery), 위협 추적 및 회복탄력성이 뛰어난 아키텍처 설계 지침은 DDoS 대비를 강화하고 방어 역량을 강화합니다.

공격 유형: 악의적인 내부자

화요일 오전 8시입니다. 미국 의료 회사 직원들의 업무가 이제 막 시작되었습니다.

매우 민감한 환자 데이터를 다루는 한 고위급 직원이 야근 후에 로그인을 합니다.

전날 밤에 작업하던 폴더에서 변경 사항을 발견합니다. 그녀는 팀과 상의한 후 IT 팀에 문의를 합니다.

조사 결과, 범죄 조직에 연루된 한 하급 IT 직원이 고위급 직원을 속여 USB 해킹 장치를 디바이스에 꽂게 한 사실을 발견했는데, 이렇게 되면 BIOS(Basic Input/Output System)가 취약한 버전으로 다운그레이드되어 시스템이 손상됩니다.

이해도 테스트 →

공격 유형: 악의적인 내부자

1: 공격 노출 지점 최소화 — 2 — 3 — 4 — 5

악의적인 내부자는 MITRE ATT&CK 프레임워크(MITRE Adversarial Tactics, Techniques, and Common Knowledge)로 추적되는 두 가지 방법을 사용하여 이 공격을 시작했습니다. 어떤 기능일까요?

- [ ] 신뢰할 수 있는 관계 + 이동식 미디어를 통한 복제
- [ ] 소셜 엔지니어링 + 이동식 미디어를 통한 복제
- [ ] 소셜 엔지니어링 + 외부 원격 서비스
- [ ] 신뢰할 수 있는 관계 + 하드웨어 추가

정답 확인하기 →

공격 유형: 악의적인 내부자

1: 공격 노출 지점 최소화 — 2 — 3 — 4 — 5

악의적인 내부자는 MITRE ATT&CK 프레임워크(MITRE Adversarial Tactics, Techniques, and Common Knowledge)로 추적되는 두 가지 방법을 사용하여 이 공격을 시작했습니다. 어떤 기능일까요?

- ✗ 신뢰할 수 있는 관계 + 이동식 미디어를 통한 복제
- ✓ 소셜 엔지니어링 + 이동식 미디어를 통한 복제
- ✗ 소셜 엔지니어링 + 외부 원격 서비스
- ✗ 신뢰할 수 있는 관계 + 하드웨어 추가

공격자는 사람의 조작과 휴대용 스토리지를 통한 복제 둘 다를 위해 MITRE ATT&CK 기법들을 활용함으로써, 소셜 엔지니어링을 활용하여 고위급 직원을 속여 USB 해킹 장치를 연결하게 만들어서 이동식 미디어를 통해 손상된 데이터를 전달했습니다.

다음 질문 →

공격 유형: 악의적인 내부자

1 — 2: 사이버 위협 탐지 및 대응 — 3 — 4 — 5

공격자가 두 가지 방법을 모두 사용해야 했던 이유는 무엇입니까?

- [ ] 글로벌 관리자로 네트워크에 접속하여 BIOS(Basic Input/Output System)를 다운그레이드하기 위해
- [ ] 관리자에게 피싱 공격을 하여 BIOS가 다운그레이드되도록 하기 위해
- [ ] 디바이스의 DNS(Domain Name System) 공급업체를 변경하여 일회성 네트워크 액세스에 필요한 자격 증명을 얻기 위해
- [ ] 지속적인 네트워크 액세스에 필요한 자격 증명을 얻기 위해 디바이스에 멀웨어를 설치하기 위해

정답 확인하기 →

공격 유형: 악의적인 내부자

1 — 2: 사이버 위협 탐지 및 대응 — 3 — 4 — 5

공격자가 두 가지 방법을 모두 사용해야 했던 이유는 무엇입니까?

- ✗ 글로벌 관리자로 네트워크에 접속하여 BIOS(Basic Input/Output System)를 다운그레이드하기 위해
- ✗ 관리자에게 피싱 공격을 하여 BIOS가 다운그레이드되도록 하기 위해
- ✗ 디바이스의 DNS(Domain Name System) 공급업체를 변경하여 일회성 네트워크 액세스에 필요한 자격 증명을 얻기 위해
- ✓ 지속적인 네트워크 액세스에 필요한 자격 증명을 얻기 위해 디바이스에 멀웨어를 설치하기 위해

공격자는 대상 환경에 대한 지속적인 무단 제어 권한을 확보하기 위해, USB 해킹 장치를 통해 멀웨어를 설치하여 디바이스를 손상시키고 자격 증명을 사용하여 지속적인 네트워크 액세스를 가능하게 하는 두 가지 방법이 모두 필요했습니다.

다음 질문 →

공격 유형: 악의적인 내부자

1 2 3: 사이버 위협 탐지 및 대응 4 5

비정상적인 네트워크 활동을 탐지하는 한 가지 방법은 무엇입니까?

- [ ] 애플리케이션 제어
- [ ] XDR(Extended Detection and Response)
- [ ] NGAV(Next-Gen Antivirus)
- [ ] 엔드포인트 지오펜싱

정답 확인하기 →

공격 유형: 악의적인 내부자

1 2 3: 사이버 위협 탐지 및 대응 4 5

비정상적인 네트워크 활동을 탐지하는 한 가지 방법은 무엇입니까?

- ✗ 애플리케이션 제어
- ✓ XDR(Extended Detection and Response)
- ✗ NGAV(Next-Gen Antivirus)
- ✗ 엔드포인트 지오펜싱

위협을 신속하게 탐지할 수 있는 광범위한 상관관계 가시성을 제공한다는 측면에서, XDR은 엔드포인트, 네트워크 및 클라우드 환경 전반에서 일어나는 활동을 지속적으로 모니터링하고 분석하기 때문에 의심스러운 네트워크 활동을 탐지하는 데 가장 적합합니다.

다음 질문 →

공격 유형: 악의적인 내부자

1 2 3 4: 사이버 공격으로부터 복구 5

킬 체인 초기에 의심스러운 활동을 탐지할 수 있는 내장형 PC 보안 기능은 무엇입니까?

- [ ] SIEM(Security Information and Event Management)
- [ ] XDR(Extended Detection and Response)
- [ ] IOA(Indicators of Attack)
- [ ] RBAC(Role-Based Access Control)

정답 확인하기 →

공격 유형: 악의적인 내부자

1 2 3 4: 사이버 공격으로부터 복구 5

킬 체인 초기에 의심스러운 활동을 탐지할 수 있는 내장형 PC 보안 기능은 무엇입니까?

- ✗ SIEM(Security Information and Event Management)
- ✗ XDR(Extended Detection and Response)
- ✓ IOA(Indicators of Attack)
- ✗ RBAC(Role-Based Access Control)

IOA는 공격자의 행동과 의심스러운 활동 패턴을 실시간으로 탐지하여 보안 팀이 서명 기반 방법보다 먼저 위협을 식별하고 심각한 피해가 발생하기 전에 개입할 수 있도록 합니다.

다음 질문 →

공격 유형: 악의적인 내부자

1 2 3 4 5: 전반적인 모범 사례

초기 액세스 방법을 파악한 후, 유사한 향후 침해를 복구하고 방지하기 위해 취할 수 있는 조치는 무엇입니까?

- [ ] BIOS를 최신 버전으로 업데이트합니다.
- [ ] BIOS 다운그레이드 옵션 비활성화
- [ ] USB 포트 비활성화
- [ ] 세분화된 제어를 구현하여 안전한 USB 디바이스 사용을 지원하고 멀웨어 확산 방지
- [ ] 모두 해당

정답 확인하기 →

공격 유형: 악의적인 내부자

1 2 3 4 5: 전반적인 모범 사례

초기 액세스 방법을 파악한 후, 유사한 향후 침해를 복구하고 방지하기 위해 취할 수 있는 조치는 무엇입니까?

- ✓ BIOS를 최신 버전으로 업데이트합니다.
- ✓ BIOS 다운그레이드 옵션 비활성화
- ✓ USB 포트 비활성화
- ✓ 세분화된 제어를 구현하여 안전한 USB 디바이스 사용을 지원하고 멀웨어 확산 방지
- ✓ 모두 해당

하드웨어를 안전하게 보호하고 다운그레이드를 차단하기 위해 다양한 공격 벡터를 처리함으로써 USB 기반 위협을 억제하고 여러 지점에서 멀웨어 확산을 차단하여 영향을 받은 시스템을 복구하고 향후 침해로부터 보호하는 포괄적인 계층형 방어 체계를 구축할 수 있습니다.

솔루션 보기 →

공격 유형: 악의적인 내부자

요약

악의적인 내부자 공격은 조직 내의 개인들이 자신의 액세스 권한을 악용하여 데이터를 손상시키거나 운영을 중단시키거나 개인, 재무 또는 경쟁 목표를 위해 기밀 정보를 추출할 때 발생합니다. 이러한 개인은 직원, 계약자, 파트너 또는 회사 시스템과 네트워크에 합법적으로 액세스할 수 있는 사람일 수 있습니다.

Dell은 고급 기술과 엄격한 보안 프로토콜을 결합하여 악의적인 내부자 사이버 공격을 방어합니다.

고급 사이버 회복탄력성 전략에 대해 자세히 알아보고 악의적인 내부자 공격으로부터 조직을 보호하는 데 Dell Technologies가 어떤 도움을 줄 수 있는지 자세히 알아보십시오.

악의적인 내부자 브리프 살펴보기 →

⌂ 시나리오로 돌아가기

신뢰할 수 있는 디바이스 및 인프라스트럭처 ›

내장된 최소 권한, MFA(Multi-Factor Authentication), RBAC(Role-Based Access Control), 이중 인증 및 제로 트러스트 보호 기능은 엔드포인트와 인프라스트럭처를 보호하여 내부자 위협의 위험을 줄입니다.

PowerEdge 서버 ›

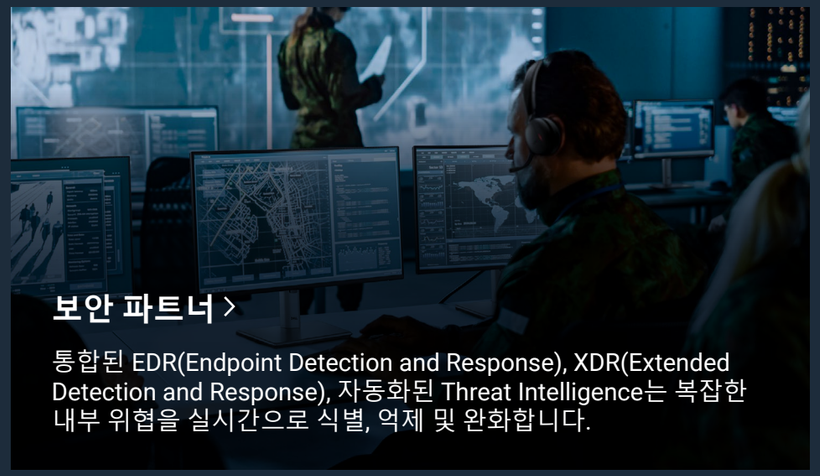
하드웨어 RoT(Root of Trust), 보안 부팅, 동적 USB 포트 관리 및 시스템 잠금 기능은 변조를 방지하고 물리적 또는 펌웨어 기반 내부 공격을 차단합니다.

PowerProtect 포트폴리오 ›

수정할 수 없고 격리된 백업은 데이터 무결성, 신속한 복원 및 데이터 조작 시도의 조기 탐지를 보장하여 내부자 인시던트로부터 복구할 수 있게 해줍니다.

보안 및 회복탄력성 서비스 ›

전문가 주도 교육, 침투 테스트, 위협 추적, 인시던트 대응 및 침해 복구 서비스는 내부자에 의한 이벤트에 대비하는 역량과 회복탄력성을 강화합니다.



보안 파트너 ›

통합된 EDR(Endpoint Detection and Response), XDR(Extended Detection and Response), 자동화된 Threat Intelligence는 복잡한 내부 위협을 실시간으로 식별, 억제 및 완화합니다.

공격 유형: MITM(Man-in-the-Middle)

경계심 없는 한 고객이 커피숍에서 안전하지 않은 무료 Wi-Fi에 연결하여 공유된 팀 문서의 최종 업데이트를 마무리합니다.

잠시 후 회사의 IT 팀은 직원 계정에서 비정상적인 로그인 시도와 전 세계 여러 위치에서 무단 데이터 접근이 발생했다는 알림을 받습니다.

조사 후 IT 팀은 공격자가 무선 연결을 가로채고 조작하여 기밀 정보에 접근한 것을 확인했습니다.

이해도 테스트 →

공격 유형: MITM(Man-in-the-Middle)

1: 공격 노출 지점 최소화 2 3 4

비정상적인 로그인 시도를 탐지한 후 IT 팀이 가장 먼저 조사해야 하는 위치는 어디입니까?

- [ ] 방화벽, IDS(Intrusion Detection System), IPS(Intrusion Prevention System) 로그 및 XDR(Extended Detection Response)
- [ ] 영향을 받는 직원의 노트북
- [ ] 커피숍의 안전하지 않은 Wi-Fi의 네트워크 트래픽
- [ ] 회사 시스템의 인증 로그

정답 확인하기 →

공격 유형: MITM(Man-in-the-Middle)

1: 공격 노출 지점 최소화 — 2 — 3 — 4

비정상적인 로그인 시도를 탐지한 후 IT 팀이 가장 먼저 조사해야 하는 위치는 어디입니까?

- ✓ 방화벽, IDS(Intrusion Detection System), IPS(Intrusion Prevention System) 로그 및 XDR(Extended Detection Response)
- ✗ 영향을 받는 직원의 노트북
- ✗ 커피숍의 안전하지 않은 Wi-Fi의 네트워크 트래픽
- ✓ 회사 시스템의 인증 로그

IT 팀은 이러한 방화벽 및 IDS/IPS 및 인증 로그를 분석하여 무단 접근 시도를 추적하고, 손상된 계정을 평가하며, 인시던트의 범위를 더 잘 이해할 수 있습니다.

다음 질문 →

공격 유형: MITM(Man-in-the-Middle)

1 — 2: 사이버 위협 탐지 및 대응 — 3 — 4

MITM 공격을 확인한 후 IT 팀은 어떤 즉각적인 조치를 취해야 합니까?

- [ ] 손상된 직원의 디바이스를 네트워크에서 즉시 분리하고 분석을 위해 격리
- [ ] 방화벽 규칙 및 네트워크 구성을 업데이트하여 추가 무단 접근을 차단
- [ ] 모든 직원 계정의 비밀번호 재설정
- [ ] 영향을 받는 시스템을 비활성화하여 데이터 유출 방지

정답 확인하기 →

공격 유형: MITM(Man-in-the-Middle)

1 — 2: 사이버 위협 탐지 및 대응 — 3 — 4

MITM 공격을 확인한 후 IT 팀은 어떤 즉각적인 조치를 취해야 합니까?

- ✓ 손상된 직원의 디바이스를 네트워크에서 즉시 분리하고 분석을 위해 격리
- ✓ 방화벽 규칙 및 네트워크 구성을 업데이트하여 추가 무단 접근을 차단
- ✗ 모든 직원 계정의 비밀번호 재설정
- ✗ 영향을 받는 시스템을 비활성화하여 데이터 유출 방지

손상된 디바이스를 즉시 연결 해제하고 격리하면 공격자의 접근이 차단되고 포렌식 증거가 보존되며, 방화벽 및 네트워크 규칙을 업데이트하면 더 이상의 악의적인 연결이 차단되고 광범위한 네트워크가 지속적인 손상으로부터 보호됩니다.

다음 질문 →

공격 유형: MITM(Man-in-the-Middle)

1 — 2 — 3: 사이버 공격으로부터 복구 — 4

MITM 공격에 대한 취약성을 줄일 수 있는 예방 조치는 무엇입니까?

- [ ] 모든 직원에게 VPN(Virtual Private Network) 사용 적용
- [ ] MFA(Multi-Factor Authentication)와 같은 제로 트러스트 보안 원칙 구현
- [ ] 공용 Wi-Fi 이용 피하기
- [ ] 이메일을 통해 공유되는 기밀 파일 암호화

정답 확인하기 →

공격 유형: MITM(Man-in-the-Middle)

1 2 3: 사이버 공격으로부터 복구 4

MITM 공격에 대한 취약성을 줄일 수 있는 예방 조치는 무엇입니까?

- ✓ 모든 직원에게 VPN(Virtual Private Network) 사용 적용
- ✓ MFA(Multi-Factor Authentication)와 같은 제로 트러스트 보안 원칙 구현
- ✗ 공용 Wi-Fi 이용 피하기
- ✗ 이메일을 통해 공유되는 기밀 파일 암호화

안전하지 않은 네트워크에서 VPN 사용을 시행하면 직원 인터넷 트래픽이 암호화되어 가로채기가 방지되고, 제로 트러스트 보안과 MFA를 구현하면 모든 액세스 요청이 지속적으로 검증됩니다.

다음 질문 →

공격 유형: MITM(Man-in-the-Middle)

1 2 3 4: 전반적인 모범 사례

보안 침해를 해결한 후 조직에서 구현해야 하는 장기적인 전략은 무엇입니까?

- [ ] 정기적인 감사 및 시스템 패치
- [ ] 네트워크 세분화를 늘려 기밀 데이터 및 시스템 격리
- [ ] EDR(Endpoint Detection and Response) 및 MDR(Managed Detection and Response) 솔루션 배포
- [ ] 직원을 위한 강력하고 정기적인 교육 이행
- [ ] 모두 해당

정답 확인하기 →

공격 유형: MITM(Man-in-the-Middle)

1 2 3 4: 전반적인 모범 사례

보안 침해를 해결한 후 조직에서 구현해야 하는 장기적인 전략은 무엇입니까?

- [x] 정기적인 감사 및 시스템 패치
- [x] 네트워크 세분화를 늘려 기밀 데이터 및 시스템 격리
- [x] EDR(Endpoint Detection and Response) 및 MDR(Managed Detection and Response) 솔루션 배포
- [x] 직원을 위한 강력하고 정기적인 교육 이행
- [x] 모두 해당

다양한 위협으로부터 보호하기 위한 이러한 장기적인 전략들이 결합되어 공격자가 취약점을 악용하는 것을 차단하고 침해에 대한 신속하고 효과적인 대응을 보장하는 포괄적이고 회복탄력성이 뛰어난 보안 태세가 구축됩니다.

솔루션 보기 →

공격 유형: MITM(MAN-IN-THE-MIDDLE)

요약

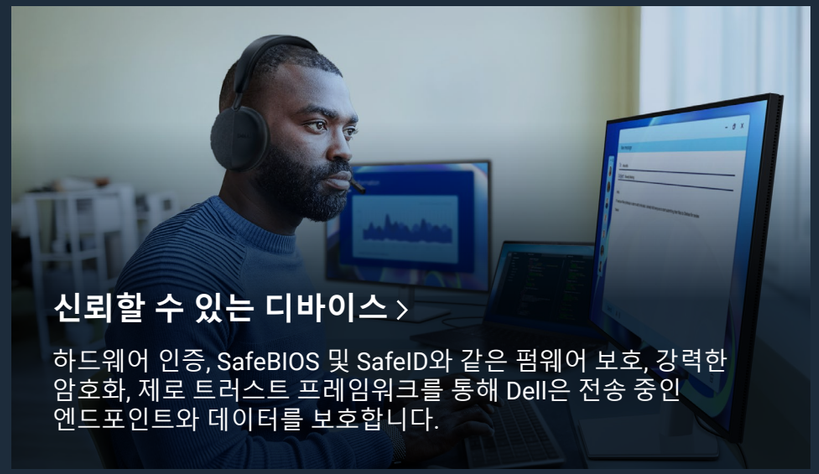
MITM 공격은 사이버 범죄자가 직원과 기업 서버 사이에서 또는 고객과 비즈니스 웹사이트 사이에서와 같이 두 당사자 사이의 통신을 비밀리에 가로챌 때 발생합니다. 공격자의 목표는 다를 수 있지만 결과는 동일합니다. 즉, 신뢰와 보안 침해입니다.

Dell Technologies는 혁신적이고 확장 가능한 보안 솔루션을 제공하여 조직이 안심하고 탐지, 대응 및 복구하는 데 필요한 툴과 전문 지식을 통해 MITM 위협을 무력화하고 자산을 보호하며 비즈니스 무결성을 유지할 수 있도록 지원합니다.

고급 사이버 회복탄력성 전략에 대해 자세히 알아보고 MITM 공격으로부터 조직을 보호하는 데 Dell Technologies가 어떤 도움을 줄 수 있는지 자세히 알아보십시오.

MITM 공격 브리프 읽기 →

⌂ 시나리오로 돌아가기



신뢰할 수 있는 디바이스 ›

하드웨어 인증, SafeBIOS 및 SafeID와 같은 펌웨어 보호, 강력한 암호화, 제로 트러스트 프레임워크를 통해 Dell은 전송 중인 엔드포인트와 데이터를 보호합니다.

PowerEdge 서버 ›

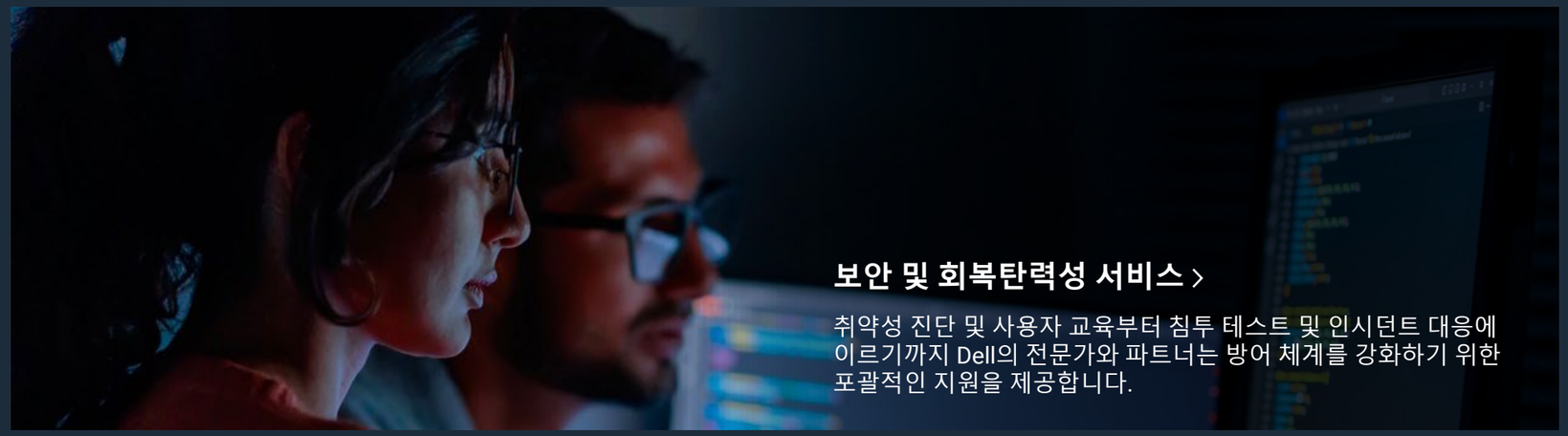
보안 부팅, 칩 내장형 RoT(Root of Trust), 동적 USB 포트 관리 및 시스템 잠금 기능은 하드웨어 무결성을 보장하고 중요한 워크로드를 네트워크 기반 위협으로부터 보호합니다.

스토리지 솔루션 ›

저장 상태 데이터와 전송 중인 데이터를 암호화하고, 격리된 스냅샷과 신속한 복구 기능을 결합되면 파일이 안전하게 유지되어 MITM 공격 후에도 신속하게 복원할 수 있습니다.

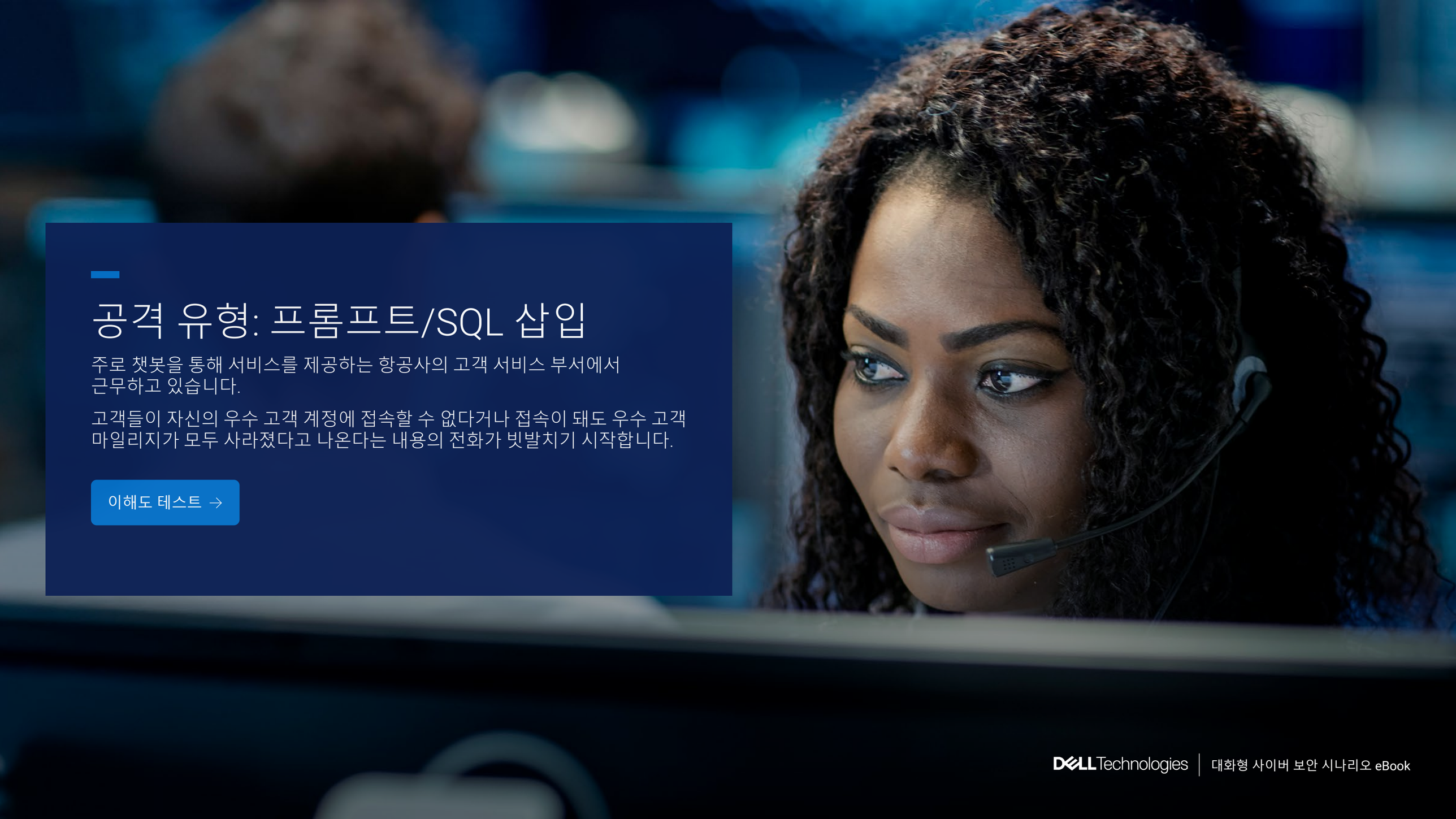
PowerProtect 포트폴리오 ›

수정할 수 없고 격리된 백업과 AI 기반 CyberSense 분석을 통해 MITM 공격 발생 시 신속한 복구와 신뢰할 수 있는 데이터 복원을 지원합니다.



보안 및 회복탄력성 서비스 ›

취약성 진단 및 사용자 교육부터 침투 테스트 및 인시던트 대응에 이르기까지 Dell의 전문가와 파트너는 방어 체계를 강화하기 위한 포괄적인 지원을 제공합니다.



공격 유형: 프롬프트/SQL 삽입

주로 챗봇을 통해 서비스를 제공하는 항공사의 고객 서비스 부서에서 근무하고 있습니다.

고객들이 자신의 우수 고객 계정에 접속할 수 없다거나 접속이 돼도 우수 고객 마일리지가 모두 사라졌다고 나온다는 내용의 전화가 빗발치기 시작합니다.

이해도 테스트 →

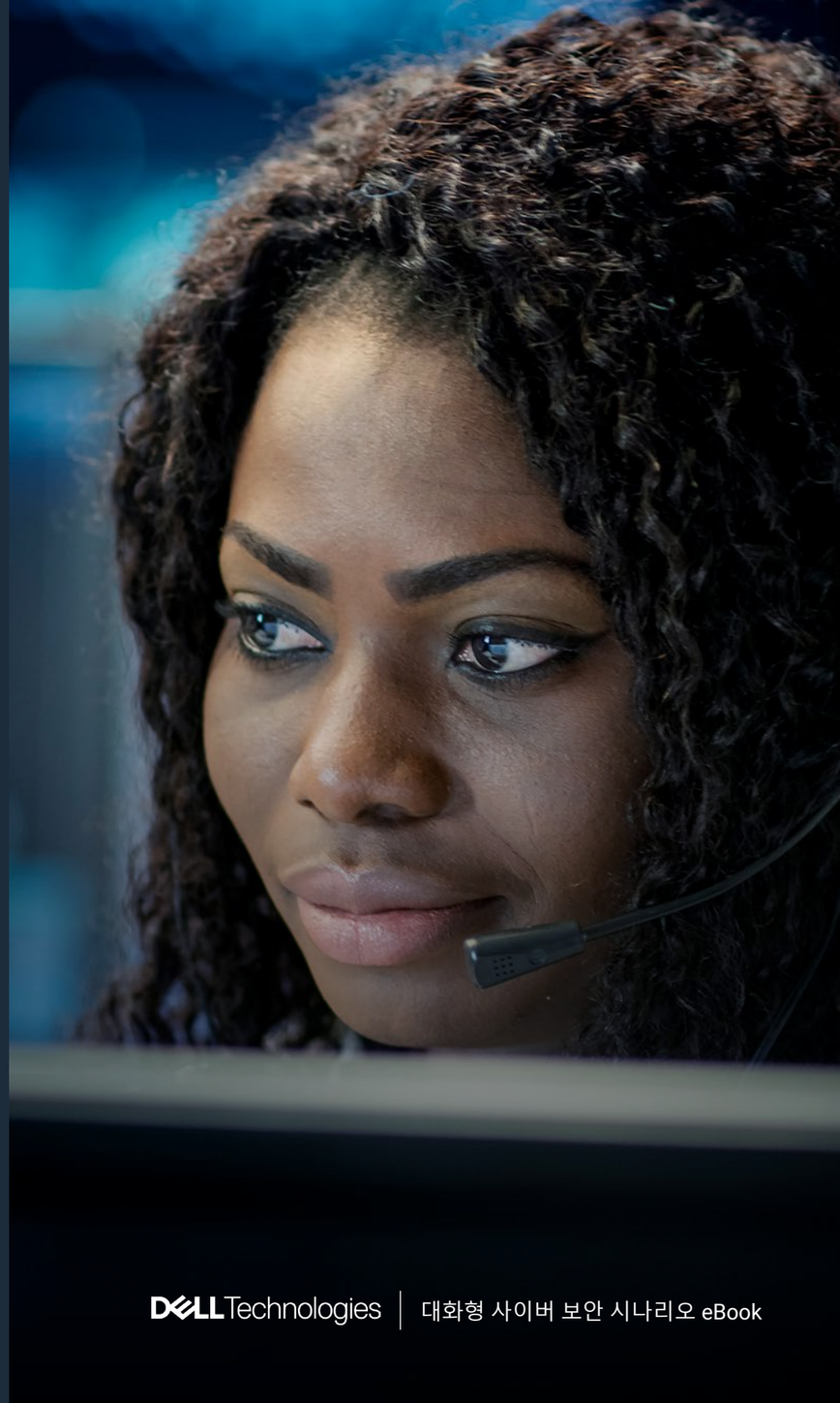
공격 유형: 프롬프트/SQL 삽입

1: 공격 노출 지점 최소화 — 2 — 3 — 4

조사 결과 로그에 몇 가지 오류가 있는 것을 확인합니다(*SQL(Structured Query Language) 구문의 구문 오류 또는 'admin'이라는 잘못된 열 이름*). 이 사건은 어떤 유형의 사이버 인시던트입니까?

- [ ] 자격 증명 도난
- [ ] 프롬프트 또는 SQL 삽입
- [ ] MITM(Man-in-the-Middle) 공격
- [ ] 피싱

정답 확인하기 →



공격 유형: 프롬프트/SQL 삽입

1: 공격 노출 지점 최소화 — 2 — 3 — 4

조사 결과 로그에 몇 가지 오류가 있는 것을 확인합니다(*SQL(Structured Query Language) 구문의 구문 오류 또는 'admin'이라는 잘못된 열 이름*). 이 사건은 어떤 유형의 사이버 인시던트입니까?

- ✗ 자격 증명 도난
- ✓ 프롬프트 또는 SQL 삽입
- ✗ MITM(Man-in-the-Middle) 공격
- ✗ 피싱

"SQL 구문의 구문 오류" 또는 "잘못된 열 이름 'admin'"과 같은 로그 오류는 공격자가 고객 계정 데이터에 접근하거나 이를 변경하기 위해 악의적인 SQL 코드로 챗봇의 입력 필드를 악용하였음을 의미하는 것이며, 이는 위에서 설명한 의심스러운 활동과 일치하는 SQL 삽입 공격의 명확한 기술적 지표이기 때문에 '프롬프트 또는 SQL 삽입'이 정답입니다.

다음 질문 →

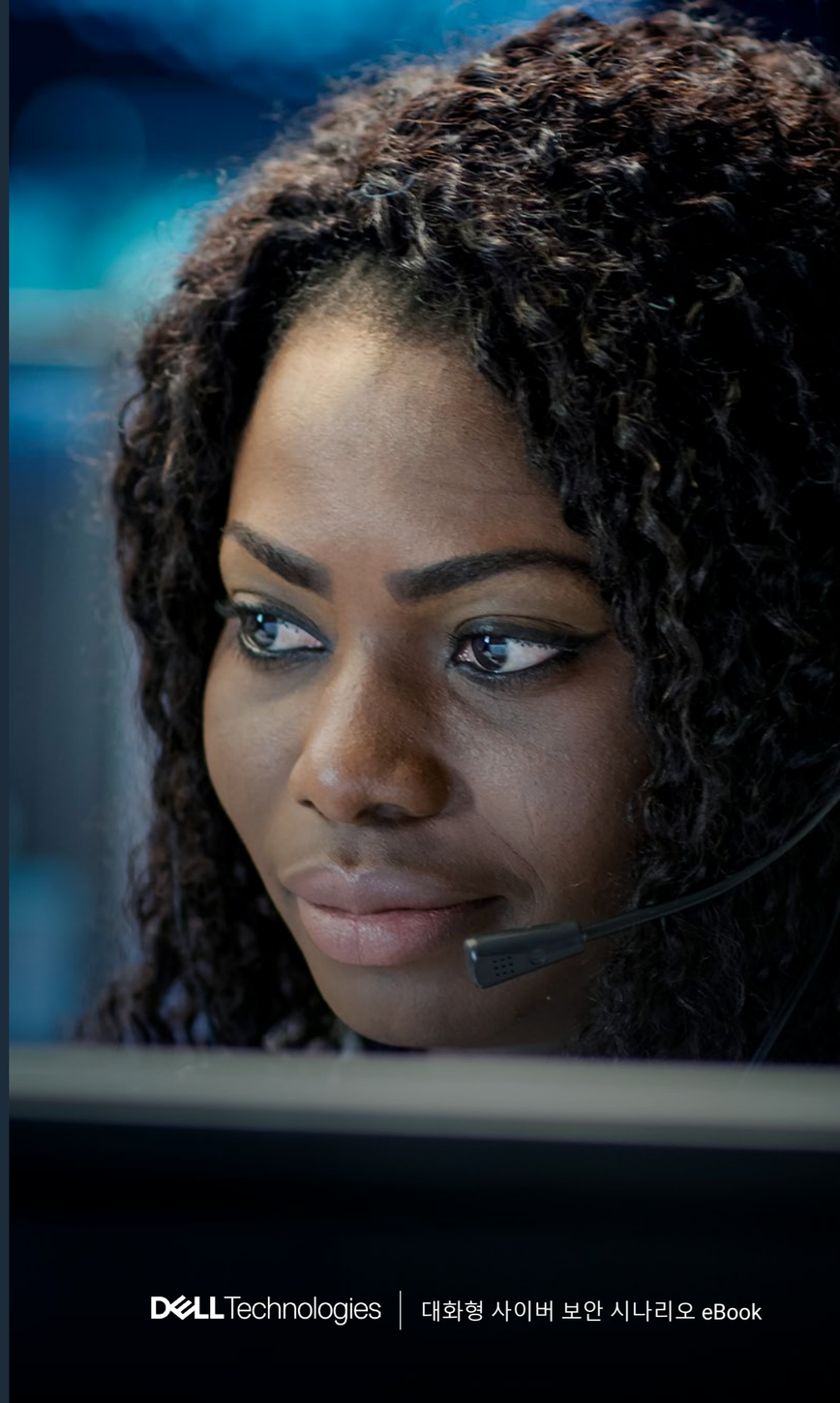
공격 유형: 프롬프트/SQL 삽입

1 — 2: 사이버 위협 탐지 및 대응 — 3 — 4

고객 서비스 챗봇을 통해 프롬프트/SQL 삽입 공격을 받았다는 사실을 알게 되었습니다. 어떻게 해야 합니까?

- [ ] 챗봇을 오프라인으로 전환
- [ ] 데이터베이스 로그를 조사하여 무단 접근 및 도난, 수정 또는 삭제된 데이터가 있는지 확인
- [ ] 모든 데이터 침해 공개 관련 법률 준수
- [ ] 모두 해당

정답 확인하기 →



공격 유형: 프롬프트/SQL 삽입

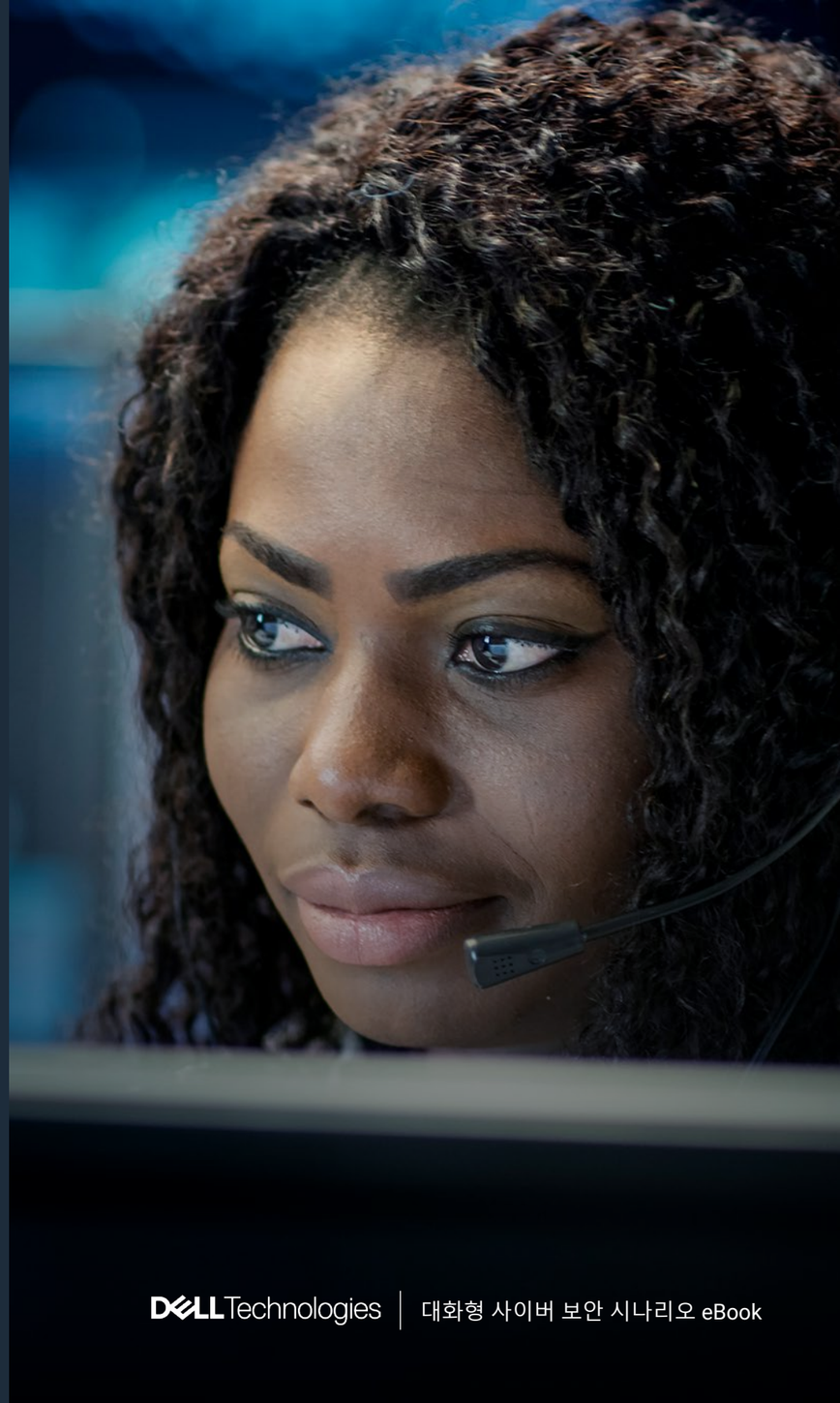
1 — 2: 사이버 위협 탐지 및 대응 — 3 — 4

고객 서비스 챗봇을 통해 프롬프트/SQL 삽입 공격을 받았다는 사실을 알게 되었습니다. 어떻게 해야 합니까?

- [x] 챗봇을 오프라인으로 전환
- [x] 데이터베이스 로그를 조사하여 무단 접근 및 도난, 수정 또는 삭제된 데이터가 있는지 확인
- [x] 모든 데이터 침해 공개 관련 법률 준수
- [x] 모두 해당

프롬프트/SQL 삽입 공격에 대응하려면 챗봇을 오프라인으로 전환하고, 데이터베이스 로그를 조사하여 무단 접근 여부를 확인하고, 공개 관련 법률을 준수하도록 해야 합니다. 이러한 단계는 악용을 차단하고, 피해를 평가하고, 규제 및 윤리적 의무를 충족하는 데 필수적입니다.

다음 질문 →



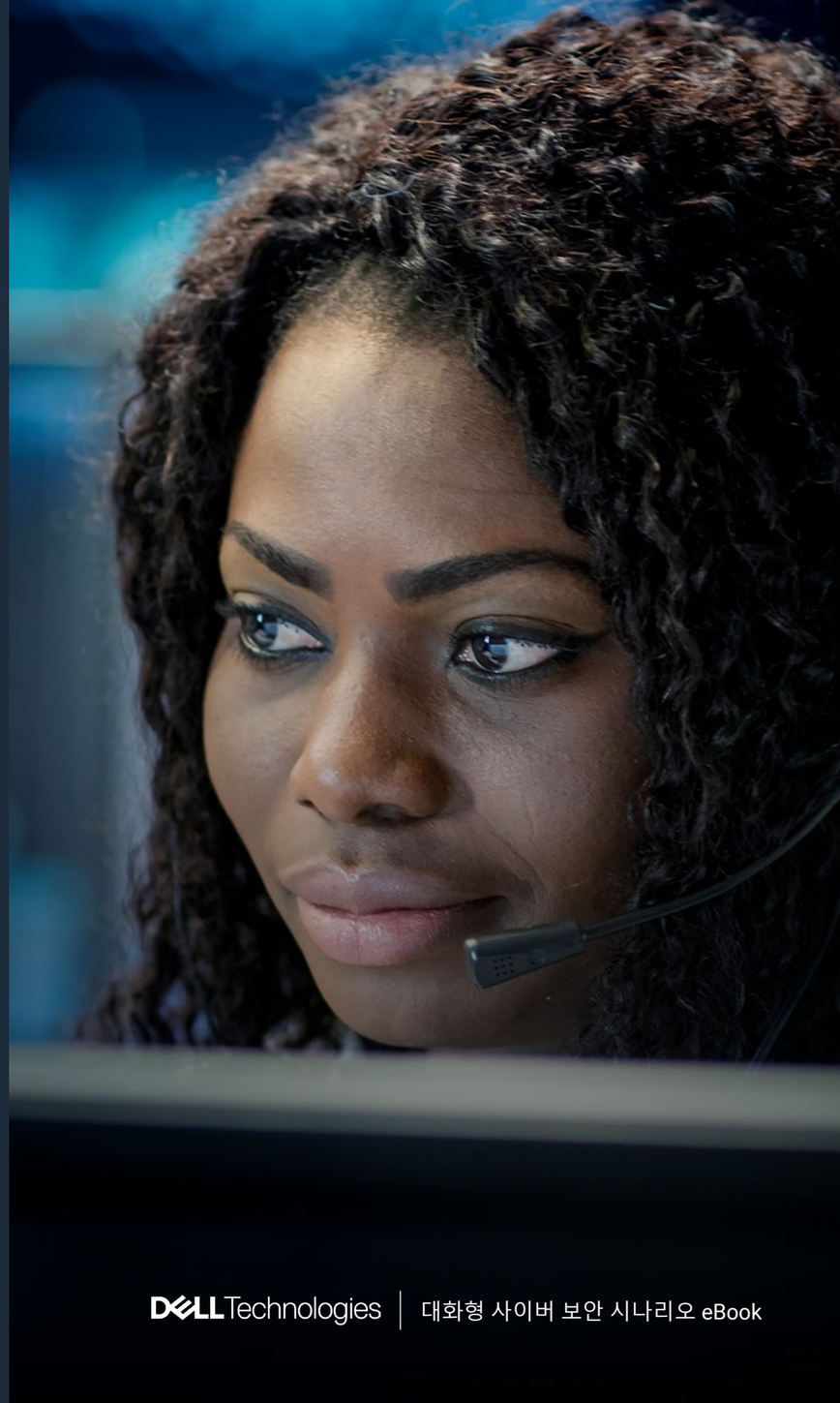
공격 유형: 프롬프트/SQL 삽입

1 2 3: 사이버 공격으로부터 복구 4

프롬프트/SQL 삽입을 차단하려면 어떤 기능을 구현해야 합니까?

- [ ] 개발 팀이 코딩 실무로서 준비된 구문과 매개변수화된 쿼리를 사용하도록 교육
- [ ] MDR(Managed Detection and Response) 툴
- [ ] MFA(Multi-Factor Authentication), RBAC(Role-Based Access Control), WAF(Web Application Firewall) 등과 같은 최소 권한 액세스 구현
- [ ] 백엔드 데이터베이스/기술 자료 세분화

정답 확인하기 →



공격 유형: 프롬프트/SQL 삽입

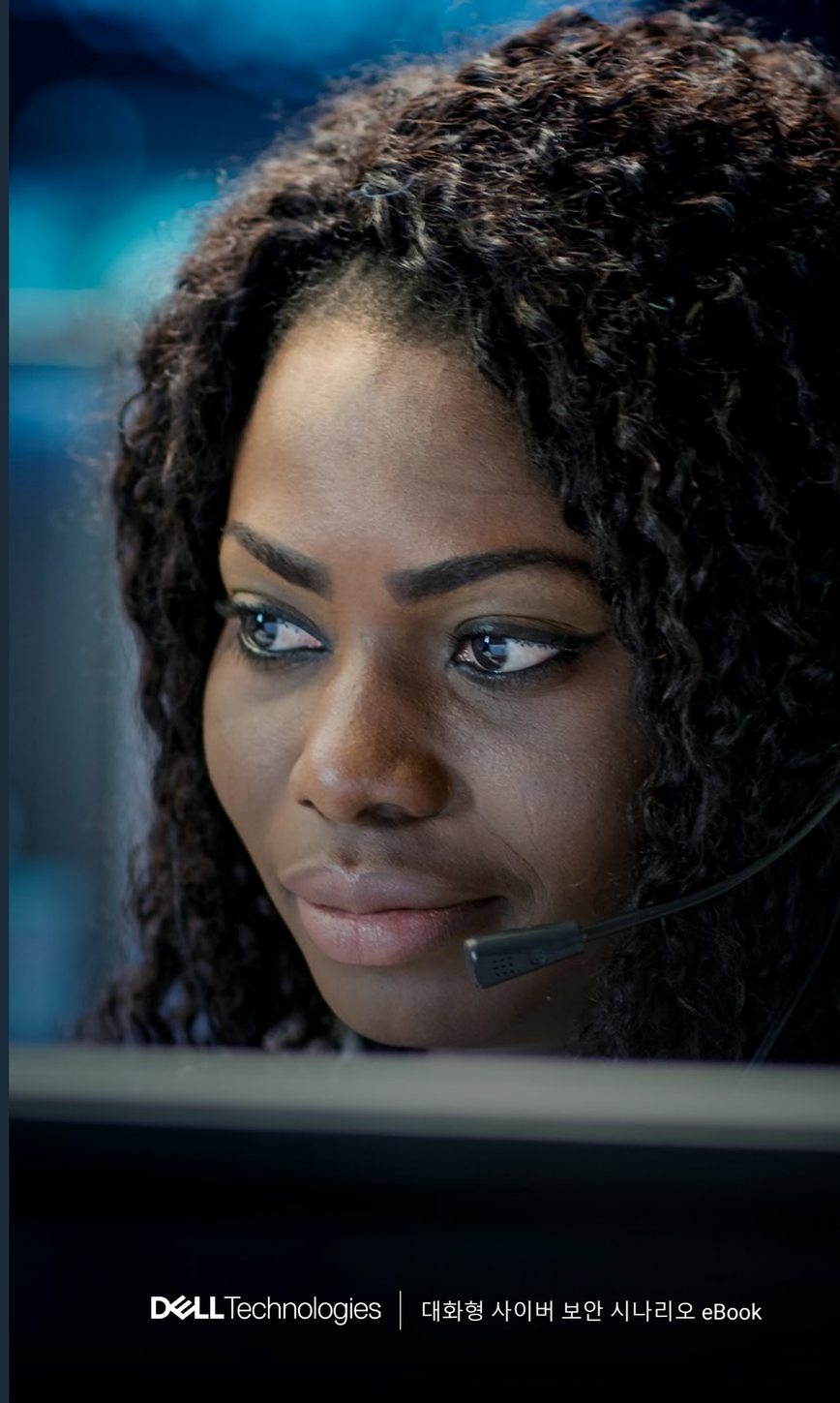
1 — 2 — 3: 사이버 공격으로부터 복구 — 4

프롬프트/SQL 삽입을 차단하려면 어떤 기능을 구현해야 합니까?

- ✓ 개발 팀이 코딩 실무로서 준비된 구문과 매개변수화된 쿼리를 사용하도록 교육
- ✗ MDR(Managed Detection and Response) 툴
- ✓ MFA(Multi-Factor Authentication), RBAC(Role-Based Access Control), WAF(Web Application Firewall) 등과 같은 최소 권한 액세스 구현
- ✗ 백엔드 데이터베이스/기술 자료 세분화

준비된 구문과 매개변수화된 쿼리를 사용하도록 개발 팀을 교육하면 SQL 삽입 공격이 원천적으로 차단되고, MFA, RBAC 및 WAF와 같은 최소 권한 액세스 제어를 적용하면 공격자가 권한을 확대하거나 내부로 이동하지 못하도록 하여 삽입 시도에 따른 영향이 제한됩니다.

다음 질문 →



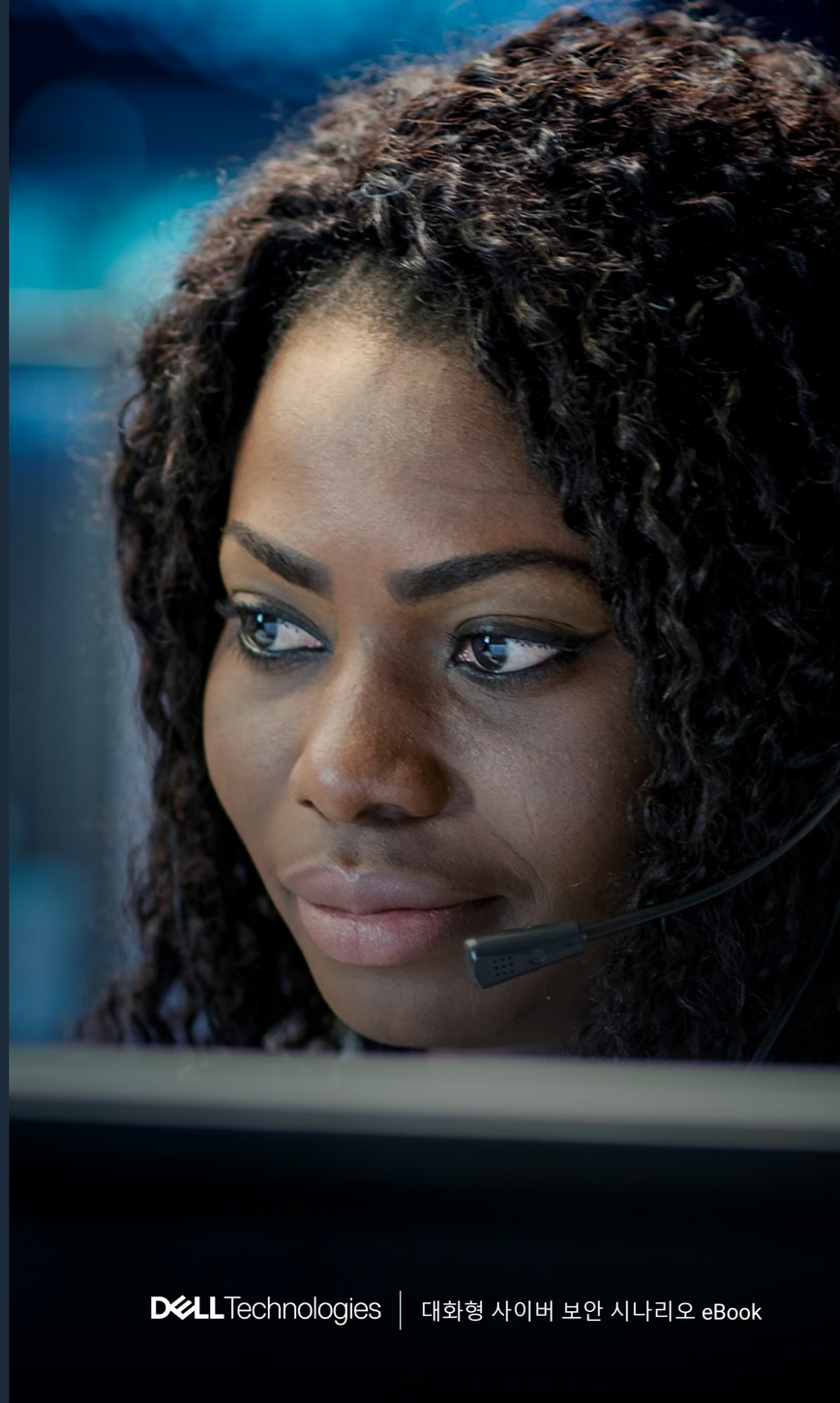
공격 유형: 프롬프트/SQL 삽입

1 2 3 4: 전반적인 모범 사례

항공사 고객 데이터를 복구하기 위해 어떤 조치를 취하시겠습니까?

- [ ] 도난당한 데이터 추적
- [ ] 고객이 프로파일을 재구축하도록 권유
- [ ] 사이버 공격자에게 데이터를 다시 구매
- [ ] 손상되지 않은 최신 백업을 통해 복원하여 항공사 마일리지를 복구하고 고객에게 비밀번호를 변경하고 신용 카드를 확인하는 것이 좋다고 알립니다.

정답 확인하기 →



공격 유형: 프롬프트/SQL 삽입

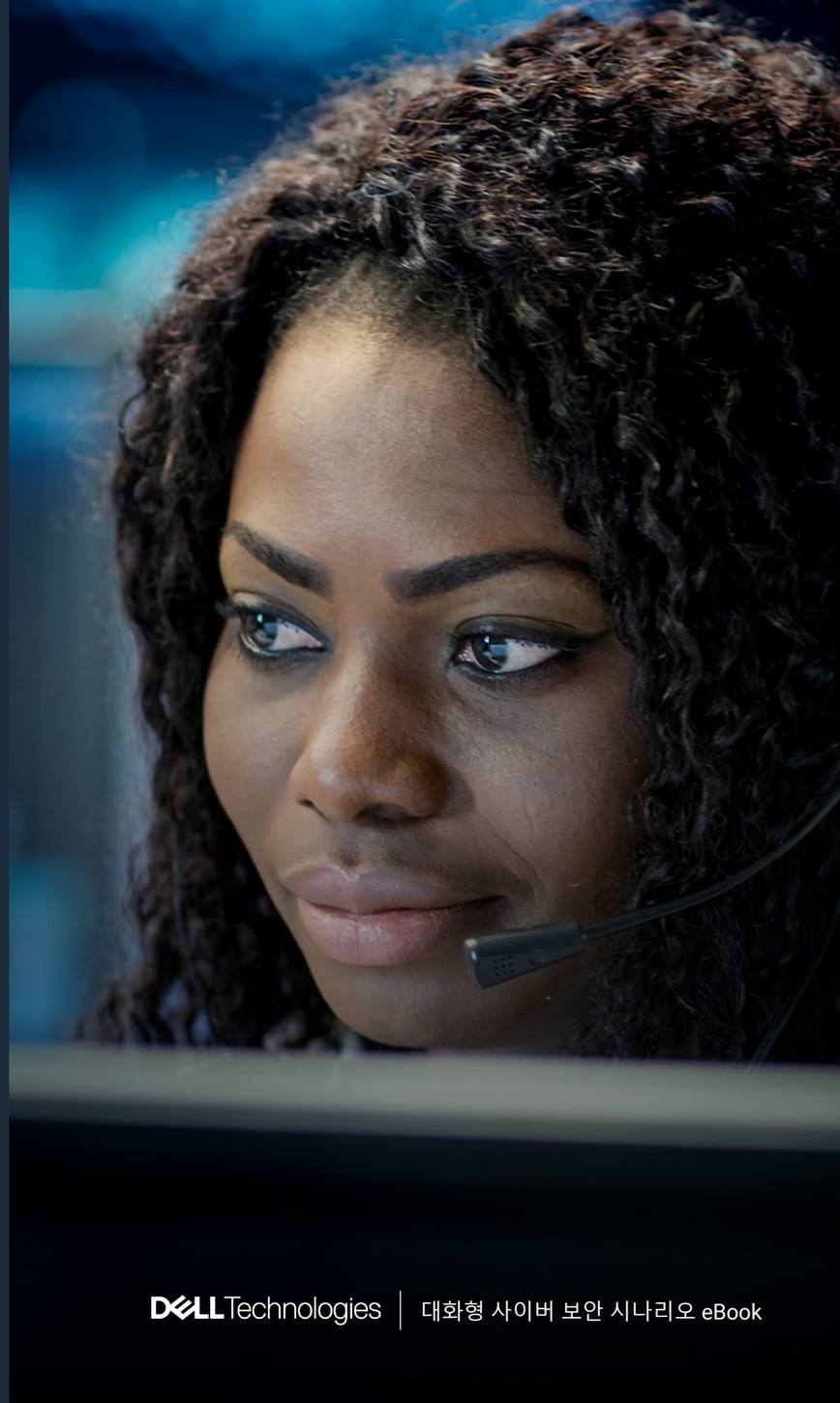
1 2 3 4: 전반적인 모범 사례

항공사 고객 데이터를 복구하기 위해 어떤 조치를 취하시겠습니까?

- ✗ 도난당한 데이터 추적
- ✗ 고객이 프로파일을 재구축하도록 권유
- ✗ 사이버 공격자에게 데이터를 다시 구매
- ✓ 손상되지 않은 최신 백업을 통해 복원하여 항공사 마일리지를 복구하고 고객에게 비밀번호를 변경하고 신용 카드를 확인하는 것이 좋다고 알립니다.

손상되지 않은 최신 백업에서 손실된 계정 데이터를 복구하면 데이터 무결성을 유지하고 다운타임을 줄일 수 있습니다. 파괴적 삽입 공격 발생 시 고객에게 비밀번호를 재설정하고 신용카드 활동을 모니터링하도록 즉시 알리면 규정 준수를 더욱 강화할 수 있습니다.

솔루션 보기 →



공격 유형: 프롬프트/SQL 삽입

요약

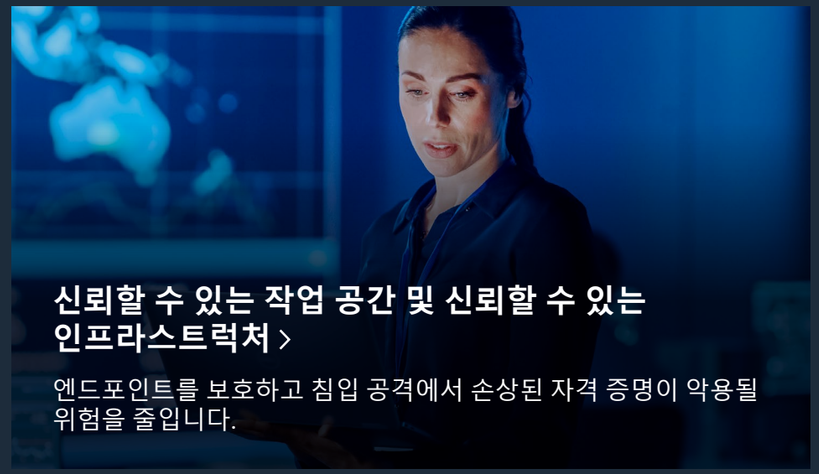
프롬프트 및 SQL 삽입 공격은 사이버 범죄자가 이용하는 가장 위험하고 보편적인 사이버 공격 방법 중 하나임이 반복적으로 입증되었습니다. 이러한 공격은 사용자 쿼리 또는 데이터베이스 시스템의 취약성을 악용하여 악의적인 행위자가 서버를 조작하거나 데이터를 탈취하거나 워크플로를 중단시킬 수 있도록 합니다.

점점 더 진화하는 프롬프트/SQL 삽입 위협 및 공격으로부터 조직을 보호하는 것은 사이버 보안에 대한 Dell의 지속적인 노력의 일환으로, 탐지, 대응 및 복구에 필요한 툴과 전문 지식을 제공합니다.

고급 사이버 회복탄력성 전략에 대해 자세히 알아보고 조직이 프롬프트 및 SQL 삽입 공격을 방어할 수 있도록 Dell Technologies가 어떻게 도울 수 있는지 알아보십시오.

프롬프트/SQL 삽입 브리프 살펴보기 →

⌂ 시나리오로 돌아가기



신뢰할 수 있는 작업 공간 및 신뢰할 수 있는 인프라스트럭처 ›

엔드포인트를 보호하고 침입 공격에서 손상된 자격 증명이 악용될 위험을 줄입니다.

PowerEdge 서버 ›

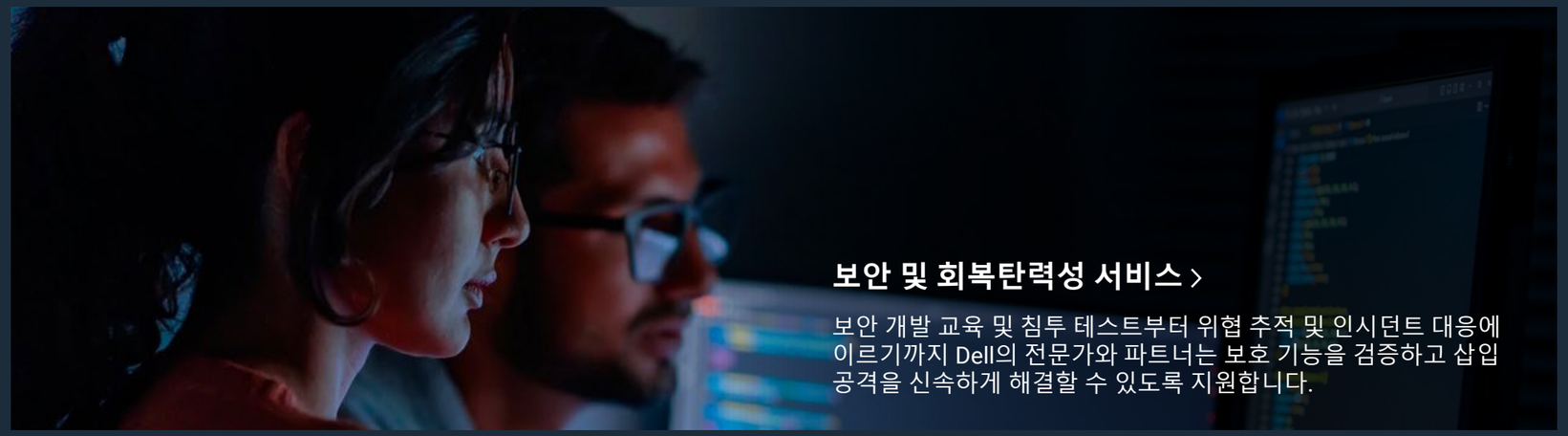
하드웨어 RoT(Root of Trust), 보안 부팅, 칩 기반 보안 및 실시간 구성 검증을 갖춘 Dell PowerEdge 서버는 신뢰할 수 있는 코드만 실행하는 변조 방지 인프라스트럭처를 보장합니다.

보안 파트너 ›

Dell 보안 파트너는 세분화된 액세스 제어, 고급 Threat Intelligence, 외부 탐지 및 대응 기능을 통해 SQL 및 프롬프트 삽입 시도를 식별하고 완화할 수 있도록 지원합니다.

PowerProtect 포트폴리오 ›

Dell의 수정할 수 없는 에어 갭 백업과 고급 Cyber Recovery 분석 기능은 신뢰할 수 있는 복원 지점을 제공하여 데이터 손상이나 유출로부터 신속하게 복구할 수 있도록 지원합니다.



보안 및 회복탄력성 서비스 ›

보안 개발 교육 및 침투 테스트부터 위협 추적 및 인시던트 대응에 이르기까지 Dell의 전문가와 파트너는 보호 기능을 검증하고 삽입 공격을 신속하게 해결할 수 있도록 지원합니다.

공격 유형: 랜섬웨어

EHR(Electronic Health Record), 스마트 주입 펌프, 방사선 영상 등 모든 것이 중앙 집중식 네트워크에 연결된 의료 시스템으로 유명한 한 지역 병원의 IT 전문가입니다.

어젯밤, 여러 시스템이 동시에 작동 중단되기 시작했습니다. 아침이 되자 의료진은 환자 기록에 접근할 수 없다고 보고했습니다.

다음과 같은 랜섬웨어 메모가 여러 단말기에 나타났습니다.

"파일이 암호화되었습니다. 72시간 이내에 20비트코인을 지불하지 않으면 환자 데이터가 공개됩니다."

이해도 테스트 →

공격 유형: 랜섬웨어

1: 공격 노출 지점 최소화 — 2 — 3 — 4

헬프 데스크에 파일 암호화 및 애플리케이션 오류에 대한 신고가 100건 이상 접수되었습니다. 보안 로그에 내부 도메인 계정의 비정상적인 파일 이름 변경 활동이 표시됩니다. 가장 먼저 할 일은 무엇입니까?

- [ ] 중요한 서비스를 복원하기 위해 즉시 랜섬 비용 지불
- [ ] 법 집행 기관 및 법률 고문에 알림
- [ ] 영향을 받는 모든 엔드포인트 이미지 재작성 시작
- [ ] 감염된 시스템을 네트워크에서 분리

정답 확인하기 →

공격 유형: 랜섬웨어

1: 공격 노출 지점 최소화 — 2 — 3 — 4

헬프 데스크에 파일 암호화 및 애플리케이션 오류에 대한 신고가 100건 이상 접수되었습니다. 보안 로그에 내부 도메인 계정의 비정상적인 파일 이름 변경 활동이 표시됩니다. 가장 먼저 할 일은 무엇입니까?

- ✗ 중요한 서비스를 복원하기 위해 즉시 랜섬 비용 지불
- ✗ 법 집행 기관 및 법률 고문에 알림
- ✗ 영향을 받는 모든 엔드포인트 이미지 재작성 시작
- ✓ 감염된 시스템을 네트워크에서 분리

감염된 병원 시스템을 즉시 분리하고 격리하면 랜섬웨어가 확산되지 않고 중요한 의료 디바이스와 민감한 환자 데이터를 보호하며, 조사를 위한 증거를 보존하고, 조율된 대응 및 복구를 위해 중요한 시간을 확보할 수 있습니다.

다음 질문 →

공격 유형: 랜섬웨어

1 — 2: 사이버 위협 탐지 및 대응 — 3 — 4

인시던트 대응 팀은 MFA(Multi-Factor Authentication) 없이 서버에 접근하는 데 사용된 손상된 계정에서 공격이 시작되었을 가능성이 있음을 발견합니다. 다음 중 공격에 가장 직접적으로 기여한 요인은 무엇입니까?

- [ ] 오래된 안티바이러스 정의 파일
- [ ] 노출된 EHR(Electronic Health Record) 데이터베이스
- [ ] 원격 액세스 시 MFA 미적용
- [ ] 취약한 이메일 필터링

정답 확인하기 →

공격 유형: 랜섬웨어

1 — 2: 사이버 위협 탐지 및 대응 — 3 — 4

인시던트 대응 팀은 MFA(Multi-Factor Authentication) 없이 서버에 접근하는 데 사용된 손상된 계정에서 공격이 시작되었을 가능성이 있음을 발견합니다. 다음 중 공격에 가장 직접적으로 기여한 요인은 무엇입니까?

- ✗ 오래된 안티바이러스 정의 파일
- ✗ 노출된 EHR(Electronic Health Record) 데이터베이스
- ✓ 원격 액세스 시 MFA 미적용
- ✗ 취약한 이메일 필터링

원격 액세스 시 MFA의 부재로 인해 공격자가 훔쳤거나 추측으로 알아낸 자격 증명으로 추가 확인 단계 없이 로그인할 수 있게 되어 서버 침해가 발생했습니다. MFA를 사용하면, 손상된 계정이라 할지라도 두 번째 인증 수단이 필요하므로 무단 접근 위험이 크게 줄어듭니다.

다음 질문 →

공격 유형: 랜섬웨어

1 2 3: 사이버 공격으로부터 복구 4

의료 직원은 이제 종이 기반 워크플로를 사용합니다. 오늘 수술이 예정된 환자는 시스템에서 확인할 수 없습니다. 병원 운영을 지원하기 위한 최선의 단기 조치는 무엇입니까?

- [ ] 코어 데이터베이스 서버를 재부팅하여 재초기화를 시도
- [ ] 6개월이 지난 백업도 모두 활성화
- [ ] 병원의 수동 비상 절차를 발동하고 비상 대응 팀에 보고
- [ ] 직원이 케이스별로 진행 방법을 결정하도록 허용

정답 확인하기 →

공격 유형: 랜섬웨어

1 — 2 — 3: 사이버 공격으로부터 복구 — 4

의료 직원은 이제 종이 기반 워크플로를 사용합니다. 오늘 수술이 예정된 환자는 시스템에서 확인할 수 없습니다. 병원 운영을 지원하기 위한 최선의 단기 조치는 무엇입니까?

- ✗ 코어 데이터베이스 서버를 재부팅하여 재초기화를 시도
- ✗ 6개월이 지난 백업도 모두 활성화
- ✓ 병원의 수동 비상 절차를 발동하고 비상 대응 팀에 보고
- ✗ 직원이 케이스별로 진행 방법을 결정하도록 허용

수동 비상 절차를 발동하고 비상 대응 팀에 보고하면 필수 의료 워크플로의 즉각적인 연속성이 보장되고, 환자의 안전이 보호되며, 진료를 확인하고 문서화하는 표준화된 프로세스가 확립됩니다. 이 접근 방식은 오류를 최소화하고, 위험과 리소스를 효율적으로 관리하며, 전문가가 디지털 시스템을 안전하게 복원하도록 지원합니다.

다음 질문 →

공격 유형: 랜섬웨어

1 2 3 4: 전반적인 모범 사례

지역 언론이 이 소식을 보도했습니다. 경영진은 공개 성명서를 발표해야 하는지 알고 싶어 하며, 법무 팀은 HIPAA(Health Insurance Portability and Accountability Act) 의무에 대해 질문하고 있습니다. 다음 중 가장 적절한 다음 조치는 무엇입니까?

- [ ] 추가 정보가 확보될 때까지 사건을 공개적으로 부인
- [ ] 타사 IT 공급업체를 비난하는 보도 자료 발표
- [ ] 규제 기관에 통보 및 내부 침해 신고 절차 시작
- [ ] 즉시 랜섬 비용을 지불하고 대중의 관심을 피함

정답 확인하기 →

공격 유형: 랜섬웨어

1 2 3 4: 전반적인 모범 사례

지역 언론이 이 소식을 보도했습니다. 경영진은 공개 성명서를 발표해야 하는지 알고 싶어 하며, 법무 팀은 HIPAA(Health Insurance Portability and Accountability Act) 의무에 대해 질문하고 있습니다. 다음 중 가장 적절한 다음 조치는 무엇입니까?

- ✗ 추가 정보가 확보될 때까지 사건을 공개적으로 부인
- ✗ 타사 IT 공급업체를 비난하는 보도 자료 발표
- ✓ 규제 기관에 통보 및 내부 침해 신고 절차 시작
- ✗ 즉시 랜섬 비용을 지불하고 대중의 관심을 피함

HIPAA 및 주 법률에 따라 보호되는 건강 정보 침해 사실을 당국 및 관련 개인에게 신속하게 보고함으로써 규정 준수, 법적 보호, 모범 사례 투명성을 확보하여 법적 책임과 평판 훼손을 방지하고, 의무 공개 의무를 이행하며, 환자, 직원 및 이해 관계자와 적절한 커뮤니케이션을 확립할 수 있습니다.

솔루션 보기 →

공격 유형: 랜섬웨어

요약

랜섬웨어는 랜섬 비용을 지불할 때까지 컴퓨터 시스템이나 데이터에 대한 접근을 차단하는 멀웨어의 일종입니다. 가장 파괴적인 사이버 공격 유형 중 하나입니다. 전 세계 조직의 50%가 작년 한 해 동안 한 번 이상 랜섬웨어 공격을 받았으며, 랜섬웨어 공격 후 평균 다운타임은 3주에 달하여 심각한 운영 중단을 초래합니다.

Dell Technologies는 제로 트러스트 프레임워크, 엔드포인트 보호 및 네트워크 세분화로 조직을 보호하는 것을 우선시하여 랜섬웨어 진입을 차단하고 확산을 제한합니다. 전문가가 주도하는 인시던트 대응 계획을 통해 회복탄력성을 유지하고 공격으로부터 신속하게 복구할 수 있도록 지원합니다.

고급 사이버 회복탄력성 전략에 대해 자세히 알아보고 랜섬웨어 공격으로부터 조직을 보호하는 데 Dell Technologies가 어떤 도움을 줄 수 있는지 자세히 알아보십시오.

랜섬웨어 공격 브리프 살펴보기 →

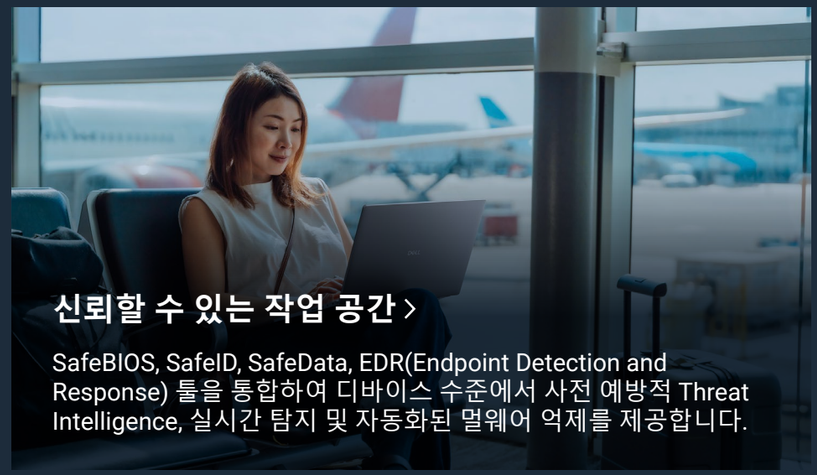
시나리오로 돌아가기

신뢰할 수 있는 인프라스트럭처 ›

하드웨어 인증, MFA(Multi-Factor Authentication), RBAC(Role-Based Access Control) 및 제로 트러스트 프레임워크를 통해 인프라스트럭처 수준에서 랜섬웨어를 차단합니다.

네트워킹 및 PowerEdge 서버 ›

랜섬웨어 이동을 제한합니다. 네트워크 세분화, 보안 부팅, 칩 내장형 RoT(Root of Trust), 동적 USB 포트 관리 및 시스템 잠금 기능을 제공합니다.

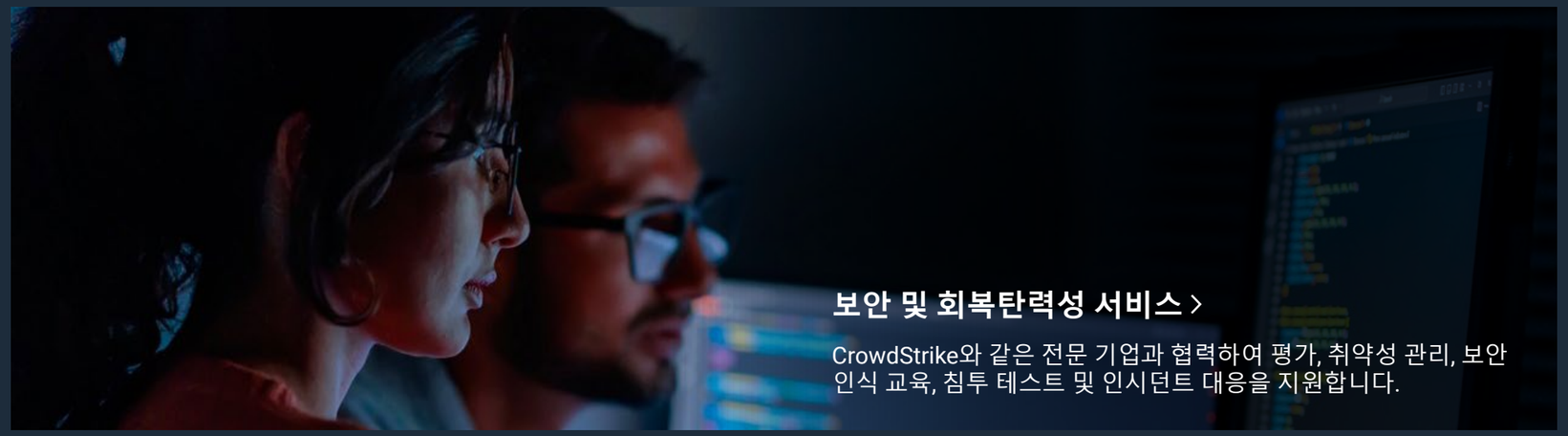


신뢰할 수 있는 작업 공간 ›

SafeBIOS, SafeID, SafeData, EDR(Endpoint Detection and Response) 툴을 통합하여 디바이스 수준에서 사전 예방적 Threat Intelligence, 실시간 탐지 및 자동화된 멀웨어 억제를 제공합니다.

PowerProtect 포트폴리오 ›

수정할 수 없는 에어 갭 백업, 지능형 Cyber Recovery 분석 및 신속한 복원 기능으로 중요한 데이터를 보호하여 갈취를 방지하고 회복탄력성을 지원합니다.



보안 및 회복탄력성 서비스 ›

CrowdStrike와 같은 전문 기업과 협력하여 평가, 취약성 관리, 보안 인식 교육, 침투 테스트 및 인시던트 대응을 지원합니다.

공격 유형: 공급망 하드웨어

귀사는 전 세계 지사에서 500대의 새 노트북을 출시했습니다. 작업 속도를 높이기 위해 이미징 및 하드웨어 준비를 타사 IT 물류 공급업체에 아웃소싱했습니다. 해당 업체는 사전 구성된 시스템을 직원들에게 직접 배송합니다.

며칠 후, 현장에서 다음과 같은 내용의 전화가 여러 통 걸려옵니다.

- MFA(Multi-Factor Authentication) 요청이 우회되고 제대로 작동하지 않는 문제가 발생하고 있습니다.
- 보안 팀에서 평소와 다른 시간대에 무단 관리자 로그인이 여러 번 발생한 것을 확인합니다.
- 또한 오프라인 상태인 것으로 추정되는 사용자의 VPN(Virtual Private Network) 트래픽도 확인합니다.

이해도 테스트 →

공격 유형: 공급망 하드웨어

1: 공격 노출 지점 최소화 2 3 4

한 직원이 로그인을 시도하지도 않았는데 MFA(Multi-Factor Authentication) 푸시 알림이 온다고 보고합니다. 회사에서 발급한 자산 태그가 있는 디바이스에서 로그인이 되었다고 회사 보안 대시보드에 표시됩니다. 논리적으로 생각할 때 SOC(Security Operations Center) 팀에서 가장 먼저 해야 할 일은 무엇입니까?

- [ ] 사용자의 계정을 비활성화하고 노트북을 원격으로 삭제
- [ ] 로그인 IP와 디바이스 지문을 공격을 받은 다른 사용자들과 비교
- [ ] 사용자의 과실을 전제로 HR 팀에 보고
- [ ] 회사 차원의 알림을 보내 비밀번호를 즉시 변경

정답 확인하기 →

공격 유형: 공급망 하드웨어

1: 공격 노출 지점 최소화 — 2 — 3 — 4

한 직원이 로그인을 시도하지도 않았는데 MFA(Multi-Factor Authentication) 푸시 알림이 온다고 보고합니다. 회사에서 발급한 자산 태그가 있는 디바이스에서 로그인이 되었다고 회사 보안 대시보드에 표시됩니다. 논리적으로 생각할 때 SOC(Security Operations Center) 팀에서 가장 먼저 해야 할 일은 무엇입니까?

- ✗ 사용자의 계정을 비활성화하고 노트북을 원격으로 삭제
- ✓ 로그인 IP와 디바이스 지문을 공격을 받은 다른 사용자들과 비교
- ✗ 사용자의 과실을 전제로 HR 팀에 보고
- ✗ 회사 차원의 알림을 보내 비밀번호를 즉시 변경

SOC 팀에서 의심스러운 활동이 더 광범위한 공격의 일부인지 아니면 신속한 패턴 인식을 가능하게 하기 위한 독립된 공격인지 판단할 때, 공급망 하드웨어 공격을 식별함에 있어서 대상 인시던트 대응 및 추가 위험 억제가 논리적인 첫 번째 단계입니다.

다음 질문 →

공격 유형: 공급망 하드웨어

1 — 2: 사이버 위협 탐지 및 대응 — 3 — 4

인시던트 대응 팀은 영향을 받은 여러 노트북에서 공식 공급업체 릴리스 노트와 일치하지 않는 SSD 펌웨어 버전을 실행하고 있음을 발견했습니다. EDR(Endpoint Detection Response)에 악성 프로세스가 표시되지 않습니다. 이는 무엇을 나타낼 가능성이 가장 높습니까?

- [ ] IT 공급업체의 구성 오류
- [ ] 스스로 삭제를 수행하는 새로운 유형의 랜섬웨어
- [ ] 펌웨어 수준의 공급망 손상
- [ ] 이미징 중 정상적인 동작

정답 확인하기 →

공격 유형: 공급망 하드웨어

1 — 2: 사이버 위협 탐지 및 대응 — 3 — 4

인시던트 대응 팀은 영향을 받은 여러 노트북에서 공식 공급업체 릴리스 노트와 일치하지 않는 SSD 펌웨어 버전을 실행하고 있음을 발견했습니다. EDR(Endpoint Detection Response)에 악성 프로세스가 표시되지 않습니다. 이는 무엇을 나타낼 가능성이 가장 높습니까?

- ✗ IT 공급업체의 구성 오류
- ✗ 스스로 삭제를 수행하는 새로운 유형의 랜섬웨어
- ✓ 펌웨어 수준의 공급망 손상
- ✗ 이미징 중 정상적인 동작

EDR로 감지되지 않고 공식 릴리스와 일치하지 않는 무단 SSD 펌웨어가 여러 노트북에서 발견된다는 것은 의도적인 하드웨어 또는 펌웨어 변조를 의미하며, 이는 펌웨어 수준 공급망 손상의 특징입니다.

다음 질문 →

공격 유형: 공급망 하드웨어

1 2 3: 사이버 공격으로부터 복구 4

악성 SSD 펌웨어가 있는 100개의 의심되는 디바이스를 격리했습니다. 원격 액세스 권한이 있을 수 있는 공격자를 차단하지 않고 어떻게 조치를 취할지 결정해야 합니다. 가장 좋은 다음 조치는 무엇입니까?

- [ ] 모든 디바이스의 전원을 끄고 포렌식 팀에 전달
- [ ] 메모리 덤프를 실시간으로 수행하고 시스템이 실행되는 동안 조사
- [ ] 타사 공급업체에 침해 사실을 알림
- [ ] 모든 디바이스를 삭제하고 전 세계 모든 사용자에게 새 노트북을 재배송

정답 확인하기 →

공격 유형: 공급망 하드웨어

1 2 3: 사이버 공격으로부터 복구 4

악성 SSD 펌웨어가 있는 100개의 의심되는 디바이스를 격리했습니다. 원격 액세스 권한이 있을 수 있는 공격자를 차단하지 않고 어떻게 조치를 취할지 결정해야 합니다. 가장 좋은 다음 조치는 무엇입니까?

- ✗ 모든 디바이스의 전원을 끄고 포렌식 팀에 전달
- ✓ 메모리 덤프를 실시간으로 수행하고 시스템이 실행되는 동안 조사
- ✗ 타사 공급업체에 침해 사실을 알림
- ✗ 모든 디바이스를 삭제하고 전 세계 모든 사용자에게 새 노트북을 재배송

실시간 메모리 덤프는 활성 멀웨어 및 루트킷과 같은 휘발성 증거를 보존하는 데 매우 중요합니다. 즉, 숨겨진 위협과 액세스 포인트가 사라지거나 공격자가 알림을 받기 전에 이를 탐지하여 대상 인시던트 대응을 가능하게 해줍니다.

다음 질문 →

공격 유형: 공급망 하드웨어

1 2 3 4: 전반적인 모범 사례

최고 정보 보안 책임자는 이 공격이 어떻게 환경에 침투했는지에 대한 요약을 요청합니다. 경영진에게 간결한 설명을 제시해야 합니다. 공격을 어떻게 설명해야 합니까?

- [ ] 피싱 링크에서 실수로 바이러스 다운로드
- [ ] 외부 액세스를 허용하는 네트워크 구성 오류 발생
- [ ] 노트북 프로비저닝 도중에 공격받은 하드웨어 공급업체를 통해 악성 펌웨어가 유입
- [ ] 개발자 중 한 명이 안전하지 않은 코드를 프로덕션 환경에 배포

정답 확인하기 →

공격 유형: 공급망 하드웨어

1 2 3 4: 전반적인 모범 사례

최고 정보 보안 책임자는 이 공격이 어떻게 환경에 침투했는지에 대한 요약을 요청합니다. 경영진에게 간결한 설명을 제시해야 합니다. 공격을 어떻게 설명해야 합니까?

- ✗ 피싱 링크에서 실수로 바이러스 다운로드
- ✗ 외부 액세스를 허용하는 네트워크 구성 오류 발생
- ✓ 노트북 프로비저닝 도중에 공격받은 하드웨어 공급업체를 통해 악성 펌웨어가 유입
- ✗ 개발자 중 한 명이 안전하지 않은 코드를 프로덕션 환경에 배포

펌웨어 버전이 일치하지 않고 활성 멀웨어가 없다는 것은 이것이 사용자의 실수나 구성 오류가 아니라 공급업체에서 발생한 펌웨어 수준 공격임을 확인해 줍니다.

솔루션 보기 →

공격 유형: 공급망 하드웨어

요약

공급망 공격은 최근 몇 년 동안 크게 증가했습니다. 운영, 배송 또는 배포 중에 물리적 디바이스를 변조하거나 소프트웨어 공급업체의 약점을 발견하면 공격자는 악성 구성 요소 또는 코드를 주입하거나, 시스템을 손상시키거나, 기밀 데이터를 유출할 수 있는 수단을 얻게 됩니다. 피해자는 소규모 기업부터 글로벌 대기업까지 다양하며, 심각한 재정적 손실, 고객 신뢰 훼손, 법적 후속 조치 등의 결과가 초래됩니다.

Dell Technologies는 엄격한 공급업체 위험 진단과 제로 트러스트 원칙을 통합하여 지속적인 디바이스 검증과 독립적인 무결성 검사를 통해 공급망 하드웨어 공격을 완화합니다. Dell Technologies는 전체 수명주기에 걸쳐 하드웨어 무결성을 강화합니다.

고급 사이버 회복탄력성 전략에 대해 자세히 알아보고 공급망 하드웨어 공격으로부터 조직을 보호하는 데 Dell Technologies가 어떤 도움을 줄 수 있는지 자세히 알아보십시오.

공급망 하드웨어 공격 브리프 살펴보기 →

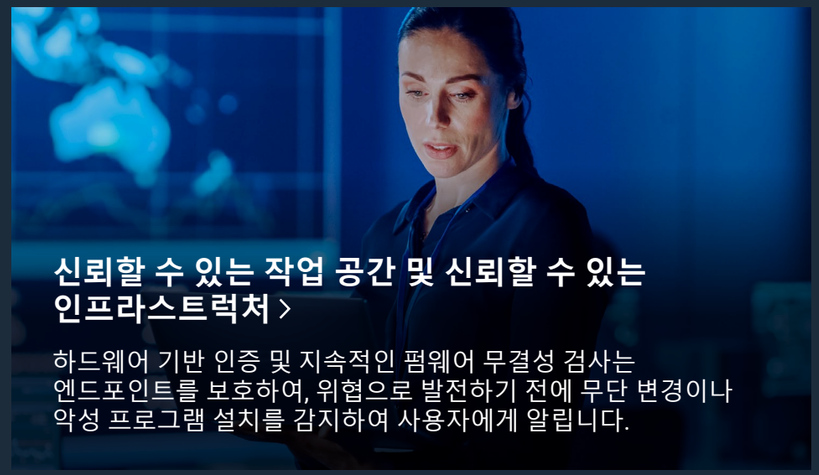
시나리오로 돌아가기

공급망 보증 ›

Dell Technologies의 공급망은 고급 출처 관리, 변조 방지 물류 및 투명한 조달을 통해 하드웨어, 펌웨어 및 공급업체를 조직에 도달하기 전에 철저히 검증합니다.

SCV(Secure Component Verification) ›

출고 시 및 설치 중에 PC 구성 요소의 암호화 검증을 통해 신뢰성을 보장하고, 숨겨진 변경 사항을 탐지하며, 공급망 변조 위험을 완화합니다.



신뢰할 수 있는 작업 공간 및 신뢰할 수 있는 인프라스트럭처 ›

하드웨어 기반 인증 및 지속적인 펌웨어 무결성 검사는 엔드포인트를 보호하여, 위협으로 발전하기 전에 무단 변경이나 악성 프로그램 설치를 감지하여 사용자에게 알립니다.

자산 추적 및 ProSupport Suite (SupportAssist 포함) ›

포괄적인 자산 추적, 디바이스 출처에 대한 실시간 모니터링, 사전 예방적 무결성 검증을 통해 신속한 이상 징후 탐지 및 전체 시스템 보안을 보장합니다.

보안 파트너: AI 기반 탐지 및 대응 ›

AI 기반 보안 툴은 지속적인 모니터링, 포렌식 조사, 그리고 변조 또는 비정상적인 디바이스 행동의 자동화된 억제를 가능하게 하여 공급망 위협에 대한 신속한 조치를 보장합니다.

공격 유형: 공급망 소프트웨어

귀사는 병원에서 사용하는 클라우드 기반 분석 소프트웨어를 제공합니다. 백엔드 서비스는 GitHub에서 신뢰할 수 있는 타사 개발자가 유지 관리하는 널리 사용되는 오픈 소스 로깅 라이브러리를 사용합니다.

귀사의 개발 팀이 모르게 공격자가 GitHub 계정을 손상시키고 다음을 위해 설계된 숨겨진 코드가 포함된 악성 업데이트를 삽입했습니다.

- API(Application Programing Interface) 키 및 JWT(JavaScript Object Notation Web Token) 암호를 포함한 환경 변수 유출
- 특정 IP가 요청할 때 역방향 셸 생성
- 원격으로 트리거되지 않는 한 휴면 상태 유지

이해도 테스트 →

공격 유형: 공급망 소프트웨어

1: 공격 노출 지점 최소화 2 3 4

API가 갑자기 주요 클라이언트에 500 오류를 반환하기 시작합니다. 귀사의 컨테이너화된 서비스에서 이전에 볼 수 없었던 도메인으로의 아웃바운드 연결이 클라우드 모니터링을 통해 탐지되었습니다. 첫 번째 대응은 무엇입니까?

- [ ] 컨테이너에서 모든 아웃바운드 네트워크 트래픽 비활성화
- [ ] 영향을 받는 서비스를 재부팅하여 메모리 문제를 해결
- [ ] GitHub 리포지토리에서 최근 코드 커밋을 확인
- [ ] 도메인의 호스팅 공급업체에 문의

정답 확인하기 →

공격 유형: 공급망 소프트웨어

1: 공격 노출 지점 최소화 — 2 — 3 — 4

API가 갑자기 주요 클라이언트에 500 오류를 반환하기 시작합니다. 귀사의 컨테이너화된 서비스에서 이전에 볼 수 없었던 도메인으로의 아웃바운드 연결이 클라우드 모니터링을 통해 탐지되었습니다. 첫 번째 대응은 무엇입니까?

- ✓ 컨테이너에서 모든 아웃바운드 네트워크 트래픽 비활성화
- ✗ 영향을 받는 서비스를 재부팅하여 메모리 문제를 해결
- ✗ GitHub 리포지토리에서 최근 코드 커밋을 확인
- ✗ 도메인의 호스팅 공급업체에 문의

컨테이너에서 모든 아웃바운드 네트워크 트래픽을 비활성화하면 공격자가 기밀 데이터를 유출하거나 손상된 로깅 라이브러리를 통해 원격 액세스를 설정하지 못하도록 즉시 차단하여 환경을 실시간으로 격리하고, 조사할 시간을 확보하여, API 키와 비밀 정보를 보호하고, 잠복 공격 메커니즘의 활성화를 방지할 수 있습니다.

다음 질문 →

공격 유형: 공급망 소프트웨어

1 — 2: 사이버 위협 탐지 및 대응 — 3 — 4

엔지니어링 책임자는 문제가 발생하기 3일 전에 해당 애플리케이션이 GitHub에서 코드를 자동으로 가져왔다는 사실을 확인합니다. 해당 버전은 아직 공개 데이터베이스에 악성으로 표시되지 않았습니다. 가장 책임감 있는 즉각적인 조치는 무엇입니까?

- [ ] GitHub를 통해 라이브러리 유지 관리자에게 직접 문의
- [ ] 모든 로컬 프로젝트 종속성 삭제 및 재구축
- [ ] 추가 조치를 취하기 전에 CVE(Common Vulnerabilities and Exposures)를 기다림
- [ ] 최종적으로 검증된 안전한 코드 버전으로 롤백

정답 확인하기 →

공격 유형: 공급망 소프트웨어

1 — 2: 사이버 위협 탐지 및 대응 — 3 — 4

엔지니어링 책임자는 문제가 발생하기 3일 전에 해당 애플리케이션이 GitHub에서 코드를 자동으로 가져왔다는 사실을 확인합니다. 해당 버전은 아직 공개 데이터베이스에 악성으로 표시되지 않았습니다. 가장 책임감 있는 즉각적인 조치는 무엇입니까?

- ✗ GitHub를 통해 라이브러리 유지 관리자에게 직접 문의
- ✗ 모든 로컬 프로젝트 종속성 삭제 및 재구축
- ✗ 추가 조치를 취하기 전에 CVE(Common Vulnerabilities and Exposures)를 기다림
- ✓ 최종적으로 검증된 안전한 코드 버전으로 롤백

최종적으로 검증된 안전한 코드 버전으로 롤백하면 손상된 업데이트가 즉시 제거되고, 공격자의 거점이 제거되며, 운영 무결성이 복원되어 위험을 사전에 억제하고 기밀 데이터를 보호할 수 있습니다.

다음 질문 →

공격 유형: 공급망 소프트웨어

1 — 2 — 3: 사이버 공격으로부터 복구 — 4

분석 결과 라이브러리가 API 키 및 클라우드 자격 증명을 유출하고 있었음이 확인되었습니다. 손상된 버전으로 구축된 여러 컨테이너를 식별했습니다. 억제 전략에서 가장 중요한 조치는 무엇입니까?

- [ ] 영향을 받은 환경의 모든 자격 증명을 무효화하고 재발급함
- [ ] 업데이트된 OS(Operating System) 이미지를 사용하여 컨테이너 이미지 재작성
- [ ] 개발 팀의 노트북 삭제
- [ ] GitHub 리포지토리에 대한 삭제 알림 제출

정답 확인하기 →

공격 유형: 공급망 소프트웨어

1 — 2 — 3: 사이버 공격으로부터 복구 — 4

분석 결과 라이브러리가 API 키 및 클라우드 자격 증명을 유출하고 있었음이 확인되었습니다. 손상된 버전으로 구축된 여러 컨테이너를 식별했습니다. 억제 전략에서 가장 중요한 조치는 무엇입니까?

- ✓ 영향을 받은 환경의 모든 자격 증명을 무효화하고 재발급함
- ✗ 업데이트된 OS(Operating System) 이미지를 사용하여 컨테이너 이미지 재작성
- ✗ 개발 팀의 노트북 삭제
- ✗ GitHub 리포지토리에 대한 삭제 알림 제출

자격 증명을 무효화하고 재발급하는 것은 클라우드 침해 발생 후 공격자가 서비스에 접근하지 못하도록 차단하고, 데이터 도난을 방지하며, 침해 범위에 관계없이 시스템을 보호하기 위한 첫 번째 중요한 절차입니다.

다음 질문 →

공격 유형: 공급망 소프트웨어

1 2 3 4: 전반적인 모범 사례

최고 기술 책임자와 법률/규정 준수 팀에서 무슨 일이 일어났는지 설명해 달라는 요청을 받습니다. 가장 정확하고 명확한 설명은 무엇입니까? 인시던트를 어떻게 요약하시겠습니까?

- [ ] 내부 CI/CD(Continuous Integration and Continuous Deployment/Delivery) 툴에 문제가 발생하여 오류 코드 배포
- [ ] 타사 소프트웨어 종속성이 공격으로 손상되었고 자동화 과정에서 해당 코드가 실제 운영 환경에 배포
- [ ] 개발자가 테스트되지 않은 코드를 급하게 출시한 릴리스에 포함
- [ ] 공격자가 GitHub 리포지토리에 무차별 대입 공격을 가함

정답 확인하기 →

공격 유형: 공급망 소프트웨어

1 2 3 4: 전반적인 모범 사례

최고 기술 책임자와 법률/규정 준수 팀에서 무슨 일이 일어났는지 설명해 달라는 요청을 받습니다. 가장 정확하고 명확한 설명은 무엇입니까? 인시던트를 어떻게 요약하시겠습니까?

- ✗ 내부 CI/CD(Continuous Integration and Continuous Deployment/Delivery) 툴에 문제가 발생하여 오류 코드 배포
- ✓ 타사 소프트웨어 종속성이 공격으로 손상되었고 자동화 과정에서 해당 코드가 실제 운영 환경에 배포
- ✗ 개발자가 테스트되지 않은 코드를 급하게 출시한 릴리스에 포함
- ✗ 공격자가 GitHub 리포지토리에 무차별 대입 공격을 가함

근본 원인은 공급망 공격이었습니다. 공격자가 타사 소프트웨어 종속성을 손상시켰고, 자동화된 빌드 프로세스가 악성 업데이트를 운영 환경에 직접 가져와 애플리케이션 무결성과 민감한 환경에 영향을 미쳤고 신뢰할 수 있는 외부 종속성에서 악의적인 업데이트 위험이 부각되었습니다.

솔루션 보기 →

공격 유형: 공급망 소프트웨어

요약

공급망 소프트웨어 사이버 공격은 소프트웨어 업데이트, 타사 통합 및 개발 환경 내의 취약성을 악용하여 네트워크 전체에 확산되는 악성 코드를 심습니다. 이러한 공격은 광범위한 데이터 침해, 운영 중단을 초래하고 전체 생태계를 손상시켜 모든 규모의 비즈니스에 영향을 미칠 수 있습니다.

Dell Technologies는 사이버 회복탄력성을 위해 투명성, 보안 개발 및 지속적인 모니터링을 강조하는 동시에 신속한 복구와 이해 관계자와의 커뮤니케이션을 보장하기 위해 강력한 인시던트 대응 계획을 유지하고 있습니다.

고급 사이버 회복탄력성 전략에 대해 자세히 알아보고 공급망 소프트웨어 공격으로부터 조직을 보호하는 데 Dell Technologies가 어떤 도움을 줄 수 있는지 자세히 알아보십시오.

공급망 소프트웨어 공격 브리프 살펴보기 →

시나리오로 돌아가기

공급망 보증 ›

Dell Technologies의 공급망은 고급 출처 관리, 변조 방지 물류 및 투명한 조달을 통해 하드웨어, 펌웨어 및 공급업체를 조직에 도달하기 전에 철저히 검증합니다.

SDL(Security Development Lifecycle) ›

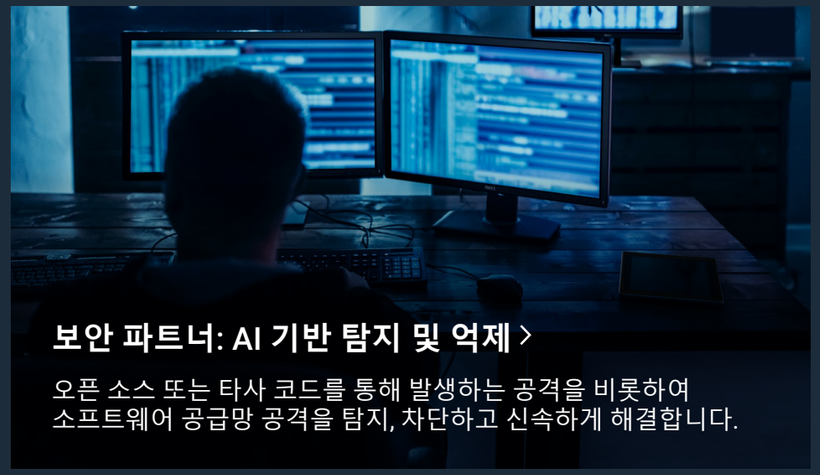
업계를 선도하는 보안 개발 방식 운영을 구현하여 타사 종속성으로 인한 위험을 줄이고 제공되는 솔루션에서 소프트웨어 기반 공격을 방지합니다.

신뢰할 수 있는 작업 공간 및 신뢰할 수 있는 인프라스트럭처 ›

SafeBIOS, SafeID 및 SafeData 하드웨어 인증은 엔드포인트가 신뢰할 수 있는 코드만 실행하도록 보장하고 무단 또는 악성 소프트웨어 수정을 신속하게 탐지하는 데 도움이 됩니다.

자산 추적 및 ProSupport Suite (SupportAssist 포함) ›

디바이스 및 소프트웨어의 실시간 모니터링으로 공급망을 통해 발생하는 이상 징후를 신속하게 탐지하고 대응할 수 있습니다.



보안 파트너: AI 기반 탐지 및 억제 ›

오픈 소스 또는 타사 코드를 통해 발생하는 공격을 비롯하여 소프트웨어 공급망 공격을 탐지, 차단하고 신속하게 해결합니다.

공격 유형: 제로 데이

회사의 인증 로그를 모니터링하는 보안 분석가입니다. 최근 사용자들이 자신의 자격 증명을 다른 사람과 공유하지 않았음에도 불구하고 계정에 대한 무단 액세스가 발생했다고 보고했습니다.

로그를 조사한 결과, 다음과 같은 활동이 발견되었습니다.

```
[INFO] 2025-04-02 14:05:12 - User Login - UserID: 1023 - IP: 192.168.1.15 - JWT Token Issued
[INFO] 2025-04-02 14:07:35 - User Login - UserID: 1023 - IP: 5.62.60.12 - JWT Token Reused
[INFO] 2025-04-02 14:08:00 - User Login - UserID: 1023 - IP: 203.0.113.45 - JWT Token Reused
```

동시에 보안 연구원이 API(Application Programming Interface)의 취약성을 발견했습니다.

- JWT(JavaScript Object Notation Web Token)는 만료되지 않습니다.
- 토큰은 HTTP 전용 쿠키 대신 로컬 스토리지에 저장됩니다.
- MFA(Multi-Factor Authentication)는 적용되지 않습니다.

이해도 테스트 →

공격 유형: 제로 데이

1: 공격 노출 지점 최소화 — 2 — 3 — 4

보안 팀으로서, 경고가 울리지 않았으므로 제로 데이 공격으로 의심되는 경우, 이를 확인하기 위해 어떤 절차를 밟으시겠습니까?

- [ ] 모든 사용자를 시스템에서 로그오프
- [ ] 로그에서 주요 비정상적인 인증 동작 식별
- [ ] 다른 회사의 친구에게 전화를 걸어 동일한 문제가 있는지 확인
- [ ] 다른 보안 비정상 활동과 상관관계 파악

정답 확인하기 →

공격 유형: 제로 데이

1: 공격 노출 지점 최소화 — 2 — 3 — 4

보안 팀으로서, 경고가 울리지 않았으므로 제로 데이 공격으로 의심되는 경우, 이를 확인하기 위해 어떤 절차를 밟으시겠습니까?

- ✗ 모든 사용자를 시스템에서 로그오프
- ✓ 로그에서 주요 비정상적인 인증 동작 식별
- ✗ 다른 회사의 친구에게 전화를 걸어 동일한 문제가 있는지 확인
- ✓ 다른 보안 비정상 활동과 상관관계 파악

평소와 다른 로그인 시간, 자격 증명 재사용 또는 비정형 디바이스에서의 액세스 등과 같은 비정상적인 인증 동작을 정확히 파악하고, 이를 데이터 액세스 이상 또는 권한 상승과 같은 다른 비정상적인 보안 활동과 연관시키면 조직적 제로 데이 공격이 확인됩니다.

다음 질문 →

공격 유형: 제로 데이

1 — 2: 사이버 위협 탐지 및 대응 — 3 — 4

취약성을 알 수 없으므로 보안 팀은 조사 중에 피해를 최소화해야 합니다. 어떻게 하시겠습니까?

- [ ] 시스템 전체의 모든 인증 세션 무효화
- [ ] 모든 리소스를 공격 진입 지점에 집중
- [ ] MFA(Multi-Factor Authentication) 로그인만 적용
- [ ] 현재 정적 방화벽 또는 WAF(Web Application Firewall) 규칙 사용

정답 확인하기 →

공격 유형: 제로 데이

1 — 2: 사이버 위협 탐지 및 대응 — 3 — 4

취약성을 알 수 없으므로 보안 팀은 조사 중에 피해를 최소화해야 합니다. 어떻게 하시겠습니까?

- ✓ 시스템 전체의 모든 인증 세션 무효화
- ✗ 모든 리소스를 공격 진입 지점에 집중
- ✓ MFA(Multi-Factor Authentication) 로그인만 적용
- ✗ 현재 정적 방화벽 또는 WAF(Web Application Firewall) 규칙 사용

이러한 조치를 함께 적용하면 보안이 강화되고 위험이 최소화되는 동시에 공격자의 접근이 차단되어 보안 팀이 근본적인 취약성을 조사하고 해결할 수 있습니다.

다음 질문 →

공격 유형: 제로 데이

1 2 3: 사이버 공격으로부터 복구 4

Dell PC에는 보안 부팅, TPM(Trusted Platform Modules), BIOS(Basic Input/Output System) 비밀번호 보호 및 SafeBIOS와 같은 기술이 있습니다. 제로 데이 공격에 어떻게 도움이 될 수 있습니까?

- [ ] API(Application Programming Interface) 토큰을 훔치는 자격 증명 덤핑 공격으로부터 보호
- [ ] 물리적 액세스 권한이 있는 공격자가 OS(Operating System) 보안을 우회하여 인증 토큰을 훔치는 멀웨어를 설치하지 못하도록 방지
- [ ] 공격자가 BIOS 설정을 조작해서 OS 보안을 약화시킬 수 없도록 하여 API 세션 하이재킹으로 이어지지 않게 함
- [ ] 모두 해당

정답 확인하기 →

공격 유형: 제로 데이

1 — 2 — 3: 사이버 공격으로부터 복구 — 4

Dell PC에는 보안 부팅, TPM(Trusted Platform Modules), BIOS(Basic Input/Output System) 비밀번호 보호 및 SafeBIOS와 같은 기술이 있습니다. 제로 데이 공격에 어떻게 도움이 될 수 있습니까?

- API(Application Programming Interface) 토큰을 훔치는 자격 증명 덤핑 공격으로부터 보호
- 물리적 액세스 권한이 있는 공격자가 OS(Operating System) 보안을 우회하여 인증 토큰을 훔치는 멀웨어를 설치하지 못하도록 방지
- 공격자가 BIOS 설정을 조작해서 OS 보안을 약화시킬 수 없도록 하여 API 세션 하이재킹으로 이어지지 않게 함
- 모두 해당

이 계층화된 접근 방식은 BIOS, 펌웨어, 자격 증명 및 시스템 구성을 대상으로 하는 제로 데이 공격에 대한 포괄적인 보호 기능을 제공합니다. 이러한 기술은 조작, 무단 액세스 및 자격 증명 도난을 방지하여 공격자가 새로운 취약성을 발견하더라도 효과를 유지합니다.

다음 질문 →

공격 유형: 제로 데이

1 2 3 4: 전반적인 모범 사례

제로 데이 공격을 예방하는 가장 좋은 방법은 무엇입니까?

- [ ] 오픈 소스 소프트웨어를 사용하지 않음
- [ ] 제로 트러스트 원칙 적용
- [ ] OS(Operating System), 펌웨어, API(Application Programming Interface), 라이브러리, 컨테이너를 포함한 모든 항목에 패치를 적용
- [ ] 위협 행위자를 차단하기 위해 회사 주변에 전기를 공급하는 관문 설치

정답 확인하기 →

공격 유형: 제로 데이

1 — 2 — 3 — 4: 전반적인 모범 사례

제로 데이 공격을 예방하는 가장 좋은 방법은 무엇입니까?

- ✗ 오픈 소스 소프트웨어를 사용하지 않음
- ✓ 제로 트러스트 원칙 적용
- ✗ OS(Operating System), 펌웨어, API(Application Programming Interface), 라이브러리, 컨테이너를 포함한 모든 항목에 패치를 적용
- ✗ 위협 행위자를 차단하기 위해 회사 주변에 전기를 공급하는 관문 설치

알려지지 않은 취약성이나 패치가 적용되지 않은 시스템이 있는 경우, 제로 트러스트 원칙은 사용자와 디바이스에 대한 암묵적 신뢰를 없애고, 지속적인 인증을 시행하고, 필수 정보에 대해서만 액세스를 허용하고, 공격자의 움직임을 억제하여 제로 데이 공격을 예방함으로써 조직이 발견되지 않은 위협에 의해 위험에 처할 가능성을 크게 줄여줍니다.

솔루션 보기 →

공격 유형: 제로 데이

요약

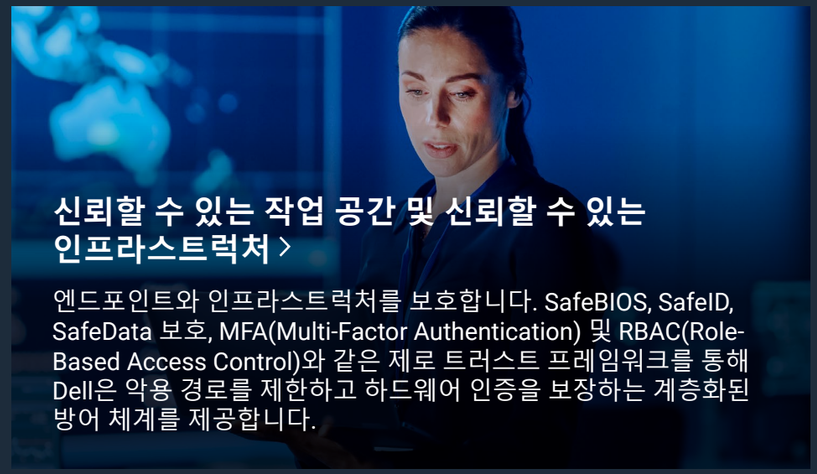
제로 데이 공격은 패치 또는 수정 사항이 제공되기 전에 소프트웨어 또는 하드웨어의 공개되지 않은 보안 취약성을 악용하는 공격입니다. 공격자들은 취약성이 발견되고 해결되기 전에 이를 활용하여 광범위한 혼란을 일으키는 경우가 많습니다.

Dell Technologies는 제로 트러스트 제어, 네트워크 세분화, 신속한 억제 및 사용자 교육을 통해 새로운 위협에 대한 방어 체계를 더욱 강화하여 제로 데이 공격에 대응합니다.

고급 사이버 회복탄력성 전략에 대해 자세히 알아보고 제로 데이 공격으로부터 조직을 보호하는 데 Dell Technologies가 어떤 도움을 줄 수 있는지 자세히 알아보십시오.

제로 데이 공격 브리프 살펴보기 →

시나리오로 돌아가기

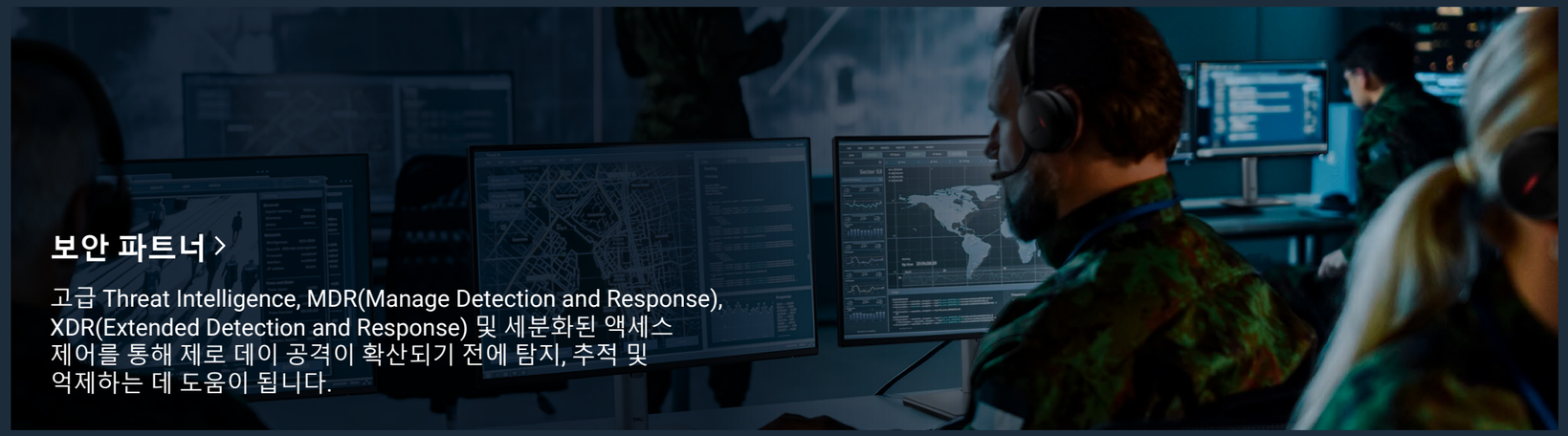


신뢰할 수 있는 작업 공간 및 신뢰할 수 있는 인프라스트럭처 ›

엔드포인트와 인프라스트럭처를 보호합니다. SafeBIOS, SafeID, SafeData 보호, MFA(Multi-Factor Authentication) 및 RBAC(Role-Based Access Control)와 같은 제로 트러스트 프레임워크를 통해 Dell은 악용 경로를 제한하고 하드웨어 인증을 보장하는 계층화된 방어 체계를 제공합니다.

PowerEdge 서버 ›

보안 부팅, 칩 내장형 RoT(Root of Trust) 및 SmartFabric 네트워크 세분화는 공격자의 내부 이동을 제한하고 인프라스트럭처에서 신뢰할 수 있는 코드만 실행되도록 합니다.



보안 파트너 ›

고급 Threat Intelligence, MDR(Manage Detection and Response), XDR(Extended Detection and Response) 및 세분화된 액세스 제어를 통해 제로 데이 공격이 확산되기 전에 탐지, 추적 및 억제하는 데 도움이 됩니다.

PowerProtect 포트폴리오 ›

변경 불가능한 백업, 격리된 Cyber Recovery 볼트, AI 기반 CyberSense 분석은 제로 데이 공격 후 빠른 복구와 회복탄력성을 보장합니다.

보안 및 회복탄력성 서비스 ›

Dell Technologies의 전문가들은 패치 관리에서 인시던트 대응에 이르기까지 신속한 억제, 포렌식 조사 및 회복탄력성 계획 수립을 통해 제로 데이 위협에 대응합니다.


DELL Technologies