DELL Technologies

사이버 보안을 강화하고 제로 트러스트 성숙도를 높이십시오.

리소스와 지식의 격차를 줄여 사이버 공격에 대한 방어력을 강화합니다.

운영

인프라스트럭처 및 디바이스

클라우드

애플리케이션

데이터

특히 GenAI의 등장과 함께 오늘날 빠르게 진화하는 위협으로 인해 가장 경험 많은 사이버 보안 전문가도 어려워하는 예상치 못한 새로운 문제가 발생합니다. 숙련된 보안 전문가와 협력하여 사이버 공격을 방지하고 강력한 보안 관행을 유지하는 방법을 알아보십시오.

소풍 중에 마주한 개미처럼 성가신 사이버 위협

한 가지 위협에 대응하면 또 다른 위협이 뒤따라 등장합니다.

상호연결성이 갈수록 심화되는 세상에서는 조직이 디지털 인프라스트럭처에 크게 의존하고 데이터가 광범위한 필수품으로 거듭나고 있으며, 정교한 공격자가 이미 귀하의 IT 환경을 침해했다고 가정하는 것이 좋습니다.

하지만 다행인 점은 기술과 사이버 보안이 만나는 교차점에 특화된 숙련된 파트너인 Dell Technologies가 있다는 것입니다.

Dell Technologies는 끊임없이 진화하는 위협 환경을 탐색하기 위해 사내에서 구현할 수 없는 혁신적인 솔루션과 귀중한 전문 지식을 제공합니다.

- 하드웨어 및 소프트웨어 보안
- 새로운 위험에 대한 통찰력
- 지능형 공격 기법 이해
- 빠르게 변화하는 위협에 대응하는 AIOps
- 새로운 보안 전략 및 모범 사례

보안 관행을 지속적으로 발전시키고 제로 트러스트 접근 방식을 수용하는 방어 계층을 구축하십시오.

Dell Technologies는 포괄적인 전문 서비스와 하드웨어 및 소프트웨어 솔루션, 강력한 파트너 생태계를 제공하는 사이버 보안 파트너입니다.

Dell Technologies 파트너 생태계는 공격 기회를 제한하고 취약성을 식별 및 최소화하며 비즈니스 운영을 신속하게 복원할 수 있도록 지원합니다.

공격 노출 지점 축소 →

사이버 위협 탐지 및 대응 →

공격으로부터 신속한 복구 →

엣지 **코어** **멀티클라우드**

전문 서비스

비즈니스/기술 파트너 생태계 **안전한 공급망**

DELL Technologies

공격 노출 지점 축소

사이버 범죄자들이 악용하기 쉬운 경로를 줄여 방어력을 높이고 표적으로 삼기 어렵게 만들 수 있습니다.

보안 태세를 강화하려면 엣지, 코어, 클라우드를 비롯한 다양한 도메인에서 애플리케이션, 시스템 또는 네트워크를 손상시킬 수 있는 취약성과 진입점을 식별하고 최소화해야 합니다.

취약점 파악

- 소프트웨어 취약성
- 잘못된 구성
- 취약한 인증 메커니즘
- 패치되지 않은 시스템
- 과도한 사용자 권한
- 오픈 네트워크 포트
- 열악한 물리적 보안

예방적 조치 구현

- 안전한 공급업체와 협력
- 포괄적인 네트워크 세분화 적용
- 중요한 데이터 분리
- 엄격한 액세스 제어 적용
- 시스템과 애플리케이션 업데이트 및 패치
- AI, 정기적인 진단 및 테스트를 통해 취약성 식별 및 해결

제로 트러스트 접근 방식 수용

제로 트러스트 아키텍처는 조직의 경계 내부 또는 외부의 그 무엇도 자동으로 신뢰하지 않습니다. 대신 액세스 권한을 부여하기 전에 시스템에 연결하려는 모든 것을 검증합니다. 이 아키텍처는 미국 국방부에서 확립하고 규정한 모델로, 상호 연관된 7가지 핵심 요소를 통합하여 성숙도를 체계적으로 구축합니다.

1. 사용자 신뢰
2. 디바이스 신뢰
3. 데이터 신뢰
4. 애플리케이션 및 워크로드
5. 네트워크 및 환경
6. 가시성 및 분석
7. 자동화 및 오케스트레이션

DELL Technologies

공격 노출 지점 축소

문제가 발생하기 전에 시스템을 약화시키는 약점을 파악할 수 있습니다.

사이버 보안은 일회성 작업이 아닌 지속적인 프로세스입니다. 숙련된 보안 서비스 파트너의 도움을 받아 정기적인 감사, 침투 테스트 및 취약성 진단을 수행하면 격차를 식별하고 해소하여 위험을 줄일 수 있습니다.

 안전한 공급망 운영	보안은 생각보다 이른 단계에서 시작됩니다. 안전한 공급망, 안전한 개발 수명주기 및 엄격한 위협 모델링을 사용하여 설계, 제조 및 제공된 디바이스와 인프라스트럭처를 사용하여 신뢰할 수 있는 기반을 구축하십시오.
 내장된 보안 기능	공격으로 피해를 입기 전에 이를 포착하고 해결하도록 설계된 하드웨어 기반 보안 기능이 내장된 디바이스 및 인프라스트럭처로 작업할 수 있습니다.
 정기적인 패치 및 업데이트	최신 보안 패치로 애플리케이션, 펌웨어 및 운영 체제를 최신 상태로 유지하여 알려진 취약성을 해결하고 악용 위험을 최소화할 수 있습니다.
 최소 권한	사용자 및 시스템 계정이 작업을 수행하는 데 필요한 최소 액세스 권한만을 보유하도록 제한합니다. 이 접근 방식은 공격자가 무단 액세스 권한을 얻는 경우 발생할 수 있는 잠재적인 영향을 제한합니다.
 네트워크 세분화	중요 데이터와 비즈니스 그룹 및 애플리케이션에 최신 네트워크 세분화를 사용하여 네트워크 액세스가 제한되도록 중요 자산을 격리할 수 있습니다. 여기에는 내부 이동을 방지하는 공격이 포함됩니다.
 애플리케이션 보안	보안 코딩 관행을 구현하고, 정기적인 보안 테스트 및 코드 검토를 수행하며, 일반적인 애플리케이션 수준 공격으로부터 보호하고 웹 애플리케이션의 공격 노출 지점을 축소하는 데 도움이 되는 WAF(Web Application Firewall)를 사용할 수 있습니다.
 전문 서비스 및 파트너십	사이버 보안 서비스 공급업체와 협력하고 비즈니스 및 기술 파트너와 파트너십을 맺어 사내에서 실현할 수 없는 전문 지식과 솔루션을 제공합니다.
 사용자 교육과 인식	직원과 사용자에게 잠재적인 보안 위협, 피싱 시도, 소셜 엔지니어링 전략을 인식하고 보고하도록 교육하여 인간의 취약성을 악용하는 위험을 최소화합니다.

DELL Technologies

사이버 위협 탐지 및 대응

오늘날의 까다로운 환경에서 오래된 보안 관행은 전화 접속 인터넷처럼 너무 느리고 비효율적입니다.

정교한 사이버 위협에 대처하려면 더 나은 보안 요령이 필요합니다. 알려진 위협과 알려지지 않은 위협을 식별하고 대응하는 애플리케이션 및 방법론에 내장된 AI 및 ML이 대표적으로 도움이 될 수 있습니다.

강력한 침입 탐지 및 예방 시스템 구현

AI 및 ML을 활용한 이상 징후 탐지

네트워크 트래픽 및 사용자 동작에 대한 실시간 모니터링 확립

숙련된 전문 서비스를 적극 활용하여 전문 지식을 습득하고 회복탄력성을 높이십시오.

Dell Technologies는 숙련된 기술 파트너로서 역할과 책임을 간략하게 설명하고 구성원 간의 원활한 커뮤니케이션과 조율을 보장하는 사전 예방적인 인시던트 대응 및 복구 프로토콜을 수립하도록 도와드립니다.

사이버 위협을 사전 예방적으로 탐지하고 대응하는 능력을 강화하는 고급 기능

- Threat intelligence
- 인시던트 대응
- Security Information and Event Management
- 엔드포인트 보호
- 동작 분석

신속하고 효율적인 복구를 촉진하고 데이터 손실을 최소화하는 기능

- 잘 정의된 인시던트 대응 계획 및 협업
- 중요한 데이터 및 시스템의 정규 백업
- 안전한 오프사이트 스토리지 솔루션 및 데이터 암호화

DELL Technologies

사이버 위협 탐지 및 대응

경계를 늦추지 말고 신속하게 조치를 취하십시오.

사이버 위협을 탐지하고 대응한다는 것은 최악의 시나리오에 대해 경계를 유지하고 계획을 수립하는 것을 의미합니다. 조직 전체가 공격의 영향을 줄이는 방법을 알 수 있도록 지속적으로 업데이트되고 일상적으로 실행되는 대응 및 복구 계획을 수립합니다. 이는 기술, 숙련된 인력, 잘 정의된 프로세스 및 팀 협업을 결합해야 하는 지속적이고 반복적인 프로세스입니다.

지속적 모니터링	IDS(Intrusion Detection System), IPS(Intrusion Prevention System), 로그 분석 및 Threat Intelligence와 같은 보안 툴을 사용하면 무단 액세스, 침입, 멀웨어 감염 및 데이터 침해의 징후를 식별할 수 있습니다.
위협 탐지	AI와 ML을 활용하여 데이터를 분석하고 위협을 나타내는 패턴, 이상 징후 및 IOC(Indicators of Compromise)를 식별합니다. 여기에는 알려진 공격 서명을 인식하고 비정상 동작을 식별하는 작업이 포함됩니다.
경고 및 알림	조기 경고를 제공하여 즉각적인 조사 및 대응을 요청합니다. 통합 보안 기능을 통해 신속하게 조치를 취할 수 있도록 버블 경고와 알림을 표면에 표시합니다. 잠재적인 위협 또는 인시던트 탐지 시 위협 탐지 속도를 높이고 보안 담당자 또는 SOC(Security Operations Center)를 활용할 수 있도록 OS 위에 디바이스 레벨 텔레메트리를 제공합니다.
인시던트 대응	확인된 보안 인시던트를 조사하고 완화하기 위한 대응 계획을 시작합니다. 여기에는 영향을 억제하고 근본 원인을 식별하고 시스템을 복원하고 추가 손상을 방지하는 데 필요한 조치를 구현하는 작업이 포함됩니다.
포렌식 분석	인시던트 세부 분석을 수행하여 공격 방법론을 파악하고, 보안 침해의 범위를 확인하며, 영향을 받은 시스템 또는 데이터를 식별하고, 보안 약점을 찾아 해결할 수 있는 증거를 수집합니다.
문제 해결 및 복구	유사한 인시던트를 방지하기 위해 취약성을 해결하고, 시스템에 패치를 적용하며, 멀웨어를 제거하고, 보안 강화 조치를 구현하는 단계를 수행합니다. 영향을 받은 시스템과 데이터를 정상 상태로 복원하여 복구 프로세스를 완료합니다.

DELL Technologies

사이버 공격으로부터 복구

전력을 다해 최대한 빨리 비즈니스를 복구하십시오.

오늘날의 데이터 중심 환경에서는 사이버 회복탄력성이 필요하며 고객과 파트너가 모두 이러한 사이버 회복탄력성을 기대합니다. 성공을 거두려면 중요한 데이터를 안전하게 보호하고 격리하여 공격 후 안심하고 신속하게 복구할 수 있도록 여러 계층의 보호가 필요합니다. 내 사이버 회복탄력성 평가하기 ›

- 사이버 공격으로 인한 피해를 완화하기 위한 조치 수행
- 손상되거나 중단된 서비스 및 디바이스 재구축
- 인시던트 분석으로 향후 공격 방지
- 비즈니스 SLA를 준수하고 운영을 정상으로 되돌림

조직이 효과적이고 효율적으로 복구할 수 있도록 포괄적인 사이버 보안 전략을 수립하십시오.

사이버 공격으로부터 복구하려면 IT 팀, 사이버 보안 전문가, 관리자 그리고 사이버 외부 전문가가 참여하는 조율된 노력이 필요합니다. 복구의 핵심은 중단 및 다운타임을 줄이고, 서비스 및 데이터 무결성을 복원하며, 재무 및 평판에 미치는 영향을 최소화하고, 사이버 보안을 강화하여 향후 유사한 공격을 방지하기 위해 인시던트로부터 학습하는 동시에 시스템과 운영을 신속하게 정상으로 되돌리는 것입니다.

- 공격이 비즈니스 운영에 미치는 영향 평가
- 중요 서비스 우선순위 지정
- 데이터 보호 시스템 배포
- 인시던트 및 복구 진행 상황과 관련된 커뮤니케이션
- 무중단 업무 운영 보장을 위한 계획 수립 및 반복 실천

DELL Technologies

사이버 공격으로부터 복구

인시던트 발생 후 시스템, 네트워크 및 데이터를 복구하여 다시 현장으로 돌아갈 수 있습니다.

사이버 회복탄력성 전략을 달성하려면 인력, 프로세스 및 기술을 전체 조직을 보호하는 전체적인 프레임워크에 통합해야 합니다.

인시던트 억제

첫 번째 단계는 사이버 공격의 영향을 격리하고 억제하는 것입니다. 여기에는 영향을 받은 시스템을 네트워크에서 연결 해제하고, 손상된 계정을 비활성화하고, 추가 확산 또는 손상을 방지하기 위한 조치를 구현하는 작업이 포함됩니다.

시스템 또는 디바이스 복원

인시던트가 억제되면 영향을 받은 시스템과 네트워크가 깨끗하고 안전한 상태로 복원됩니다. 여기에는 손상된 시스템을 재구축하고, 소프트웨어를 재설치하며, 보안 패치 및 업데이트를 적용하는 작업이 포함될 수 있습니다. 자동화와 자가 복구는 다시 운영 상태로 돌아가는 데 중요한 역할을 할 수 있습니다.

데이터 복구

공격 중에 손상되거나, 암호화되거나, 삭제되었을 수 있는 데이터를 복구해야 합니다. 백업에서 데이터를 복원하거나 전문적인 데이터 복구 기법을 사용하여 손실되거나 암호화된 파일을 되찾는 작업이 포함될 수 있습니다.

포렌식 분석

공격 후에는 보안 침해가 어떻게 발생했는지, 어떤 취약성이 악용되었는지, 유사한 공격을 방지하는 단계는 무엇인지 이해하는 것이 중요합니다. SIEM(Security Information and Event Management)과 같은 시스템 및 오프호스트 BIOS 비교와 같은 기능은 유용한 통찰력을 제공합니다.

인시던트 대응 평가

복구 후에는 인시던트 대응 프로세스를 평가하고 개선할 부분을 확인해야 합니다. 공격으로부터 얻은 교훈을 통해 보안 관행을 강화하고 인시던트 대응 계획을 업데이트하며 향후 인시던트에 대한 더 나은 보호를 제공할 수 있습니다.

전문 서비스 및 파트너십

사이버 보안 서비스 공급업체와 기술 파트너는 조직의 복구에 도움을 주는 귀중한 전문 지식과 리소스를 제공하며, 포렌식 분석, 보안 침해 발생 파악 및 향후 인시던트 방지를 위한 조치 권장 등의 작업을 지원할 수 있습니다.

DELL Technologies

사이버 보안을 엣지 및 클라우드 환경으로 확장

네트워크가 코어에서 엣지 그리고 클라우드로 확산됨에 따라 환경은 중대한 취약점이 되었습니다.

조직은 사이버 보안 전략을 발전시키면서 제로 트러스트 원칙을 엣지와 클라우드로 확장하여 엄격한 액세스 제어, 지속적인 인증, 네트워크 트래픽에 대한 포괄적인 가시성 및 제어를 보장해야 합니다. 위협 환경이 진화함에 따라 AI 기능을 1차 방어선으로 배치하는 것이 현명합니다. 또한 핵심 네트워크 및 클라우드 환경에 네트워크 세분화, 암호화 및 지속적인 모니터링과 같은 보안 조치가 있는 경우에만 전략이 완성됩니다.

사이버 보안 전문 서비스는 포괄적인 접근 방식을 취하도록 도와줄 수 있습니다.

다양한 보안 솔루션을 연결하는 것은 어려울 수 있습니다. 엣지, 코어, 클라우드 보안을 전문으로 하는 전문 서비스와 협력하면 모든 각도에서 조직을 보호하는 효과적인 조치를 취할 수 있는 전문 지식을 얻을 수 있습니다.

엣지

엣지, 네트워크, 하드웨어 및 소프트웨어 내에서 여러 보안 계층을 구축합니다.

코어

AI 및 ML, 그리고 자동화를 사용하여 인프라스트럭처를 제로 트러스트 방식과 연계합니다.

멀티클라우드

퍼블릭 클라우드, 컨테이너 및 클라우드 네이티브 워크로드를 비롯한 모든 환경에서 모든 워크로드를 보호합니다.

DELL Technologies

GenAI: 사이버 보안을 위한 양날의 검

차세대 AI는 더욱 빠르게 새로운 위험을 제공하고 있지만 보안도 강화하고 있습니다.

AI의 다음 단계인 GenAI는 다양한 작업에서 지식을 이해, 학습, 조정 및 구현할 수 있는 시스템을 포괄합니다.

한편으로는 위협 탐지 및 대응 개선, 예측 기능 및 운영 효율성 향상을 약속합니다. 다른 한편으로는 새로운 당면 과제를 가져와 강력한 보안 조치, 지속적인 모니터링, 정기적인 업데이트 및 패치 적용, 끊임없이 진화하는 데이터 프라이버시 및 윤리 접근 방식을 통해 위험을 해결하는 진화하는 사이버 보안 전략을 요구합니다.

GenAI를 통한 조직 보호

GenAI는 사이버 보안의 중요한 동맹자가 되어 조직을 보호할 수 있는 새로운 길을 열어주고 있습니다.

- 위협 탐지 및 대응의 효과를 개선합니다.
- 미래의 위협을 예측하거나 잠재적 취약성을 식별합니다.
- 위협 탐지를 자동화하고 효율성을 제공합니다.
- 포렌식 분석을 통해 패턴, 이상 징후 및 손상 지표를 신속하게 식별합니다.
- 맞춤형 보안 인식 교육을 제공합니다.
- 풍부한 통찰력에 더 빠르게 액세스하여 보안 운영을 확장합니다.

GenAI 시스템 보안

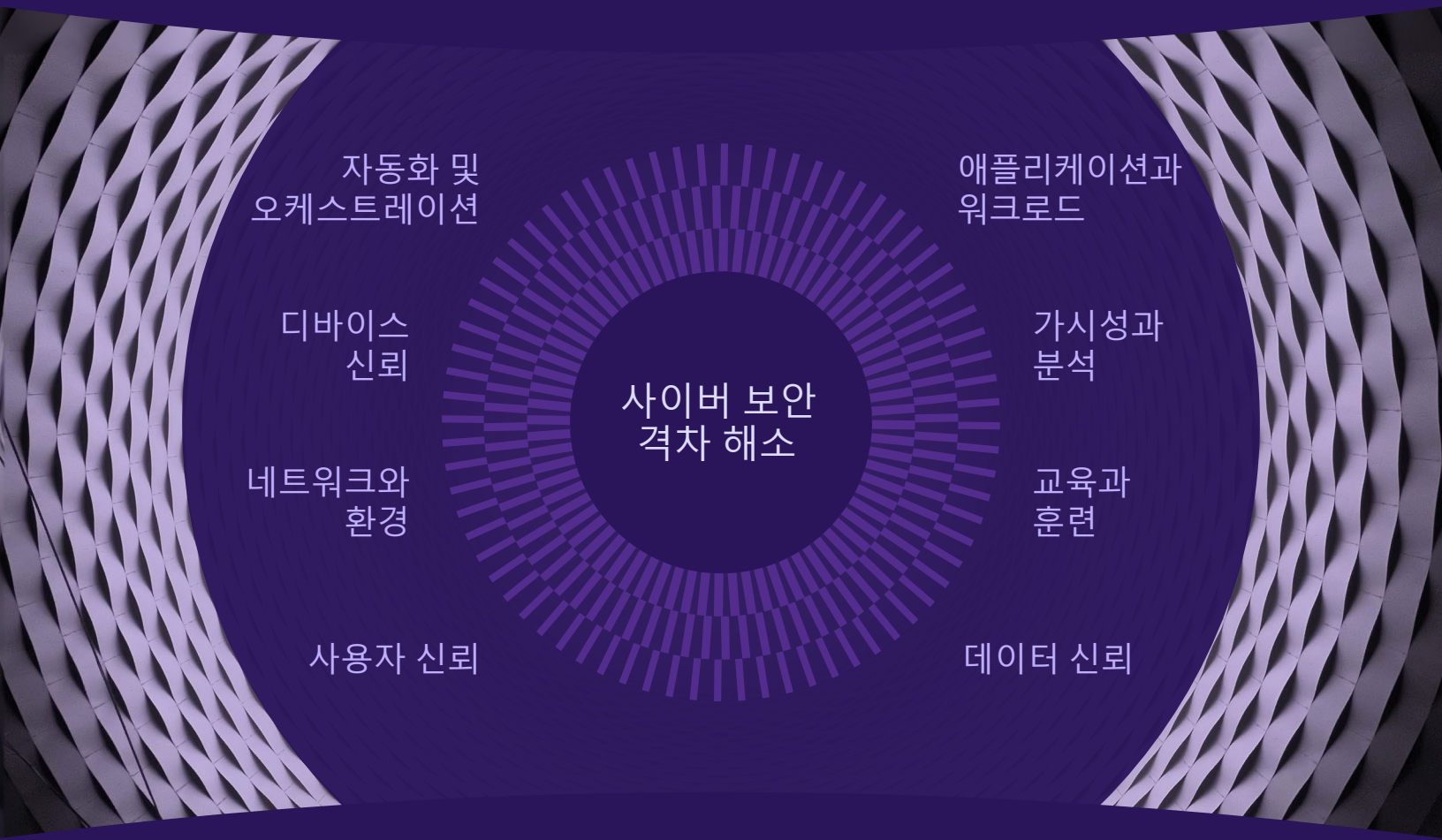
GenAI는 상당한 보안 이점을 제공하지만 적절하게 보호되지 않으면 기능이 악의적으로 사용될 수 있습니다.

- 데이터 프라이버시와 무결성을 보장합니다.
- AI 시스템을 속여 오작동을 일으키도록 설계된 적대적 공격을 완화합니다.
- 악의적인 AI의 시스템 오용을 탐지하고 이에 대응합니다.
- 윤리적 문제와 편견을 감사하고 완화합니다.
- AI 시스템을 위한 강력한 액세스 제어를 구현합니다.
- LLM(Large Language Model)을 안전하게 보호하고 복구합니다.

DELL Technologies

최신 사이버 보안은 지능적이고 확장 가능하며 자동화되어야 합니다

Dell Technologies는 진화하는 사이버 위협으로부터 보호를 제공하는 포괄적인 보안을 수립하는 데 도움을 줄 수 있습니다. 기술이 발전함에 따라 사이버 보안에 대한 Dell Technologies의 접근 방식은 AI와 ML의 힘을 활용하여 디지털 인프라스트럭처를 보호하고 디지털 영역에 대한 신뢰를 유지하면서 한발 앞서 나아가고 있습니다. 사이버 보안 여정의 어느 단계에 있든, 민첩성과 회복탄력성을 유지하기 위한 단계를 통해 단순히 조직을 보호하는 것 이상의 혁신을 실현할 수 있도록 협력할 것입니다.



DELL Technologies

Dell.com/SecuritySolutions

콜백 요청

보안 어드바이저와 채팅 상담

전화 1-800-433-2393