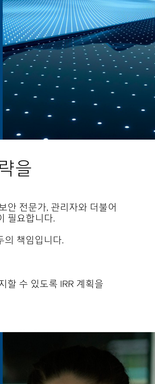
# 10가지 사이버 보안 권장 사항

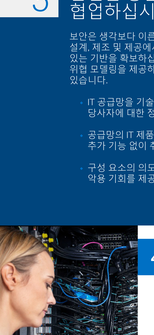
기술은 빠른 속도로 발전하고 있으며, 기능을 강화하는 새로운 툴과 시스템을 도입함에 따라 취약점을 악용하려는 사이버 위협의 새로운 기회도 동시에 창출되고 있습니다. 이러한 환경에서는 새로운 위협으로부터 보호하는 강력한 사이버 보안 조치를 구현하여 혁신이 안전한 환경에서 이뤄질 수 있도록 해야 합니다. 기업과 조직이 새로운 위협에 적응함에 따라 Dell Technologies의 사이버 보안 전문가는 사이버 보안 성숙도를 높이기 위한 10가지 기본 조치를 권장합니다.

## 1 위협적인 위험 환경을 파악하십시오.

숙련된 사이버 보안 파트너는 빠르게 변화하는 위협 환경을 탐색하는 데 도움이 되는 귀중한 전문 지식과 리소스를 제공할 수 있습니다.

- 취약성 진단과 침투 테스트를 꼼꼼하게 수행하여 보완해야 할 잠재적 약점을 파악하고 보안 전략에 존재하는 모든 격차를 파악합니다.
- 새로운 위협에 대한 통찰력, 고급 공격 기법, 최신 보안 전략 및 모범 사례 등 사내에서 제공할 수 없는 전문 기술과 지식을 활용해 보십시오.
- 액세스 권한과 근거를 정의하면 비즈니스 제어 및 거버넌스를 구현하기 위한 적절한 보안 프레임워크를 설정할 수 있습니다.





## 2 포괄적인 사이버 보안 전략을 수립하십시오.

사이버 회복탄력성을 보장하려면 IT 팀, 사이버 보안 전문가, 관리자와 더불어 외부 사이버 전문가가 참여하는 체계적인 노력이 필요합니다.

- 전사적인 노력을 장려하십시오. 보안은 모두의 책임입니다.
- 가급적 자동화를 활용하십시오.
- 사이버 공격이 발생할 때 모든 관계자가 인지할 수 있도록 IRR 계획을 충분히 연습하십시오.

## 3 안전한 공급망을 갖춘 공급업체와 협업하십시오.

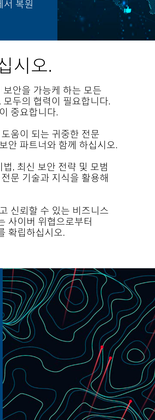
보안은 생각보다 이른 단계에서 시작됩니다. 디바이스와 인프라스트럭처의 설계, 제조 및 제공에서 보안을 우선시하는 공급업체와 협력하여 신뢰할 수 있는 기반을 확보하십시오. 안전한 공급망, 안전한 개발 수명 주기 및 알려한 위협 모델링을 제공하는 공급업체는 위협 요소에 선제적으로 대응할 수 있습니다.

- IT 공급망을 기술하거나 통과하는 정보와 IT 공급망에 참여하는 당사자에 대한 정보에 대해 기밀성, 무결성 및 가용성을 제공합니다.
- 공급망의 IT 제품 또는 서비스가 정품이고 변경되지 않았으며 원치 않는 추가 기능 없이 취득자의 사양을 충족하도록 합니다.
- 구성 요소의 의도된 기능을 제한하거나 구성 요소 장애를 유발하거나 악용 기회를 제공할 수 있는 취약성을 줄입니다.

## 4 제로 트러스트(zero trust) 원칙을 도입하십시오.

제로 트러스트는 회사 안팎의 무엇도 자동으로 신뢰해서는 안 되며, 액세스 권한을 부여하기 전에 시스템에 연결하려는 모든 요소를 검증해야 한다는 신념을 중심으로 하는 보안 개념입니다.

- 경계 기반 보안 모델에서 벗어나 제로 트러스트 원칙을 도입하십시오.
- 최소 권한 원칙을 구현하여 사용자 및 시스템 계정에 작업에 필요한 최소한의 액세스 권한만 부여합니다. 이러한 접근 방식은 공격 노출 지점과 공격자의 무단 액세스에 대한 잠재적인 영향을 줄여줍니다.
- 마이크로 세분화, IAM(Identity and Access Management), MFA(Multifactor Authentication), 보안 분석 등의 솔루션을 통합하십시오.



## 5 공격 노출 지점을 축소하십시오.

공격 노출 지점은 악의적인 행위자가 악용할 수 있는 잠재적 취약성과 진입 지점을 나타냅니다. 보안 태세를 강화하려면 공격 노출 지점을 최소화하고 위험을 완화하여 새로운 위협에 대한 전반적인 사이버 방어 체계를 강화해야 합니다.

- 직원과 사용자에게 잠재적인 보안 위협, 피싱 시도, 소셜 엔지니어링 전략을 인식하고 보고하도록 교육하여 인간의 취약성을 악용하는 공격이 성공할 위험을 최소화하십시오.
- 포괄적인 네트워크 세분화, 중요 데이터 격리, 엄격한 액세스 제어 적용, 시스템과 애플리케이션의 정기 업데이트 및 패치 적용 등의 예방 조치를 실시하십시오.
- 시스템, 네트워크 및 디바이스가 불필요한 서비스 비활성화, 강력한 비밀번호 사용, 액세스 제어 적용 등의 보안 모범 사례로 적절하게 구성되어 있는지 확인하십시오.

## 6 사이버 위협을 탐지하고 대응하십시오.

점고한 위협에 직면한 상황에서 기존의 보안 수단만으로는 더 이상 충분하지 않습니다. 조직은 지능형 공격 탐지 기술과 방법론을 활용하여 알려진 위협과 알려지지 않은 위협을 효과적으로 식별하고 대응해야 합니다.

- 네트워크 트래픽, 시스템 로그 및 기타 영역을 모니터링하고 분석하여 무단 액세스 침입, 맬웨어 감염, 데이터 침해 또는 기타 사이버 위협의 징후를 사전에 식별하십시오.
- 확인된 보안 인시던트를 즉시 조사하고 완화하기 위한 대응 계획을 시작하십시오. 여기에는 영향을 억제하고 근본 원인을 식별하며 시스템을 복원하고 추가 손상을 방지하는 데 필요한 조치를 구현하는 작업이 포함됩니다.
- AI/ML을 활용하여 비정상적인 데이터 패턴이나 행동에 대한 실시간 분석을 통해 사이버 위협을 신속하게 탐지할 수 있습니다. 또한 이러한 기술은 위협 심각도를 평가하고, 영향을 예측하며, 특정 방어 조치를 자동화하고, 보안 관행을 확장하여 잠재적인 손상을 최소화함으로써 신속한 대응을 촉진합니다.

## 7 사이버 공격으로부터 복구하십시오.

중요한 사전 예방 조치를 취했더라도 공격을 당했을 가능성을 항상 염두에 둬야 하며, 회복탄력성 역량을 자주 테스트하여 사이버 공격에서 효과적으로 복구할 수 있는 상태를 유지해야 합니다.

- 사이버 공격으로 인한 피해를 줄일 수 있도록 영향을 분리하고 억제하는 조치를 즉시 취하십시오.
- 영향을 받은 시스템을 네트워크에서 연결 해제하고, 손상된 계정을 비활성화하며, 추가 확산 또는 손상을 방지하기 위한 조치를 구현하십시오.
- AI/ML을 사용하면 영향을 받은 시스템과 데이터를 신속하게 식별하고 백업에서 복원 프로세스를 자동화하여 복구 속도를 높일 수 있습니다.



## 8 숙련된 파트너를 활용하십시오.

사람, 프로세스 또는 기술을 아우르는 포괄적인 보안을 가능케 하는 모든 기능은 단일 공급업체에서 제공할 수 없습니다. 모두의 협력이 필요합니다. 따라서 숙련된 파트너 네트워크와 협력하는 것이 중요합니다.

- 빠르게 변화하는 위협 환경을 탐색하는 데 도움이 되는 귀중한 전문 지식과 리소스를 제공하는 숙련된 사이버 보안 파트너와 함께 하십시오.
- 새로운 위협에 대한 통찰력, 지능형 공격 기법, 최신 보안 전략 및 모범 사례를 포함하여 사내에서 제공할 수 없는 전문 기술과 지식을 활용해 보십시오.
- 숙련된 전문 서비스의 전문 지식을 활용하고 신뢰할 수 있는 비즈니스 파트너와의 협력 관계를 구축하여 진화하는 사이버 위협으로부터 효과적으로 보호하는 포괄적인 보안 태세를 확립하십시오.



## 9 사이버 보안을 엣지 및 클라우드 환경으로 확장하십시오.

네트워크가 코어에서 엣지, 클라우드로 확산됨에 따라 모든 환경이 중대한 취약점이 되었습니다. 애플리케이션 배포 방식에 관계없이 애플리케이션 사용자와 경영진 모두에 대해 일관성을 보장하도록 통합한 수준의 보안 적용과 비즈니스 정책 조정이 필요합니다.

- 제로 트러스트 원칙이 엣지 및 클라우드 환경에 적용되도록 확장하여 강력한 액세스 제어, 지속적인 인증, 네트워크 트래픽에 대한 포괄적인 가시성 및 제어 기능의 제공을 보장하십시오.
- 핵심 네트워크와 클라우드 환경에서 모두 네트워크 분할, 암호화, 연속 모니터링 등의 보안 조치를 구현하여 잠재적인 위협으로부터 보호하십시오.
- 엣지, 코어, 클라우드 보안을 전문으로 하는 숙련된 전문 서비스와 협력하면 모든 측면에서 조직을 보호하는 효과적 조치를 가능케 하는 전문 지식을 활용할 수 있습니다.



## 10 사전 예방적으로 관리하고 포괄적으로 회복탄력성을 향상하십시오.

위협 인텔리전스, 인시던트, 대응 및 보안 운영을 관리하면 사이버 위협 감지 및 대응 역량을 강화할 수 있습니다.

- 역할과 책임을 명확하게 요약하여 팀 구성원 간의 원활한 커뮤니케이션과 조정을 보장하는 사전 예방적인 인시던트 대응 및 복구 프로토콜을 수립하십시오.
- 네트워크 내 위협을 사전 예방적으로 모니터링하고 대응하여 필요할 때 복구를 위한 알림을 제공할 수 있도록 환경에 대한 가시성을 개선하십시오.
- 지능형 공격 인텔리전스, SIEM(Security Information and Event Management), 엔드포인트 보호 솔루션 및 행동 분석을 활용하여 사이버 위협을 사전 예방적으로 탐지하고 대응 능력을 강화하십시오.

보안 위협이 혁신의 걸림돌이 되지 않도록 대비하십시오.
dell.com/SecuritySolutions에서 사이버 보안 및 제로 트러스트 성숙도를 높일 수 있는 방법을 알아보십시오.

DELL Technologies