DELL Technologies

사이버 보안 강화 및 제로 트러스트 성숙도 향상

혁신의 걸림돌인 보안 위험 해결

사이버 보안의 현재 위치 파악

나아갈 방향을 파악

오늘날의 복잡하고 빠르게 발전하는 환경에서는 조직이 강력한 사이버 보안 관행을 유지하려 시도하더라도 종종 리소스와 지식의 한계에 직면합니다. 사이버 보안 및 제로 트러스트 성숙도 향상은 진화하는 사이버 위협에 맞서 혁신을 위협하지 않고 환경을 안전하게 유지하는 데 필수적입니다.

이 체크리스트를 사용하여 현재의 사이버 보안 성숙도를 진단하십시오. 강점과 취약점을 파악하면 사이버 보안 성숙도를 높일 수 있는 올바른 다음 단계를 수행할 수 있습니다.

목차

자세히 보기

사이버 보안 및 제로 트러스트 성숙도 향상에 대해 자세히 알아보기

체크리스트:

공격 노출 지점 축소

공격 노출 지점은 환경에서 사이버 공격자가 공격하거나 악용할 수 있는 모든 지점 또는 영역을 가리킵니다. 이러한 지점에는 소프트웨어 취약점, 구성 오류, 취약한 인증 메커니즘, 패치가 적용되지 않은 시스템, 과도한 사용자 권한, 오픈 네트워크 포트, 열악한 물리적 보안 등이 포함됩니다. 다음 질문을 통해 악의적 행위자가 악용할 수 있는 취약점 및 진입 지점을 최소화할 수 있는 방법을 확인할 수 있습니다.

예	아니오	
☐	☐	정기적으로 평가, 침투 테스트 또는 침해 공격 시뮬레이션을 수행하여 시스템 및 네트워크의 취약점과 약점을 파악함으로써 시기 적절하게 문제 해결 및 개선 작업을 수행하고 있습니까?
☐	☐	직원을 대상으로 정기적으로 보안 교육을 실시합니까?
☐	☐	MFA(Multifactor Authentication) 및 RBAC(Roles Based Access Controls)를 활용합니까?
☐	☐	중요 자산을 격리하고 네트워크의 다른 부분 간의 액세스를 제한하기 위해 네트워크 세분화를 구현했습니까?
☐	☐	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 사용하고 있습니까?
☐	☐	공급망 보안을 위해 프로세스 및 절차를 증명할 수 있는 IT 공급업체를 선정했습니까?
☐	☐	기존의 경계 기반 보안을 대체하기 위해 제로 트러스트 원칙을 구현하고 있습니까?
☐	☐	최소 권한 원칙을 활용하여 사용자 및 시스템 계정이 작업 수행에 필요한 최소 액세스 권한만 갖도록 제한합니까?
☐	☐	정기적으로 시스템 및 소프트웨어를 패치합니까?
☐	☐	이용 중인 보안 툴이 AI/ML 기능을 활용하여 사전 예방적으로 취약점을 식별합니까?

체크리스트:

위협 탐지 및 대응

사이버 위협을 탐지하고 대응하는 것은 보안 전략의 필수 구성 요소입니다. 여기에는 네트워크 트래픽, 시스템 로그 및 기타 영역을 모니터링 및 분석하고, 보안 데이터를 분석하여 무단 액세스, 침입, 멀웨어 감염, 데이터 침해 또는 기타 사이버 위협의 징후를 식별하는 것이 포함됩니다. 이러한 질문은 컴퓨터 네트워크, 시스템 또는 내부의 잠재적인 보안 인시던트 및 악의적 활동을 사전 예방적으로 식별하고 적극적으로 해결하는 방법을 확인하는 데 도움이 됩니다.

예	아니오	
☐	☐	XDR(Extended Detection and Response), IDS(Intrusion Detection System), IPS(Intrusion Prevention System), SIEM 및 로그 분석과 같은 보안 툴 및 기술을 사용하여 네트워크 및 시스템 활동을 지속적으로 모니터링합니까?
☐	☐	수집된 데이터를 분석하여 잠재적인 사이버 위협을 나타낼 수 있는 패턴, 이상 징후, IoC(Indicators of Compromise) 및 IOA(Indicators of Attack)를 파악합니까?
☐	☐	잠재적인 위험을 신속하게 감지하고 경고하기 위한 최신 가시성 및 모니터링 툴을 배포했습니까?
☐	☐	진행 중인 사이버 공격을 나타낼 수 있는 비정상적인 패턴이나 의심스러운 활동을 감지하도록 네트워크 트래픽을 모니터링하고 있습니까?
☐	☐	비정상적 데이터 패턴이나 행동에 대한 실시간 분석을 통해 사이버 위협을 탐지하는 데 도움이 되는 AI/ML 툴을 구현했습니까?
☐	☐	보안 알림을 보다 효과적으로 관리하고 IT 생태계 전체에서 보안 이벤트 데이터의 상관 관계를 근본적으로 파악할 수 있는 차세대 SIEM 솔루션의 구현을 고려했습니까?
☐	☐	기존 취약점의 우선 순위를 지정하고 해결하는 것은 물론 새로운 취약점에 효율적으로 대응하기 위해 취약점 테스트 및 관리를 수행하고 있습니까?
☐	☐	확인된 보안 인시던트를 조사하고 완화하기 위한 인시던트 대응 계획이 마련되어 있습니까?
☐	☐	사이버 공격의 확산을 줄일 수 있는 인시던트 대응 조치를 가속화하기 위해 SOAR(Security Orchestration, Automation and Response) 툴을 통합하고 있습니까?
☐	☐	인시던트 대응 계획에 방지 정책, 커뮤니케이션 계획, 규정 준수 요건, 포렌식 분석 및 복구 프로세스가 포함되어 있습니까?

체크리스트:

사이버 공격으로부터 복구

사이버 공격으로부터 복구란 보안 인시던트가 발생한 후 영향을 받은 시스템, 네트워크 및 데이터를 안전한 운영 상태로 복원하는 프로세스를 의미합니다. 여기에는 공격으로 인한 손상을 최소화하는 조치를 취하고 손상되거나 중단된 서비스 및 디바이스를 재구축하고, 인시던트 분석을 통해 향후 공격을 방지하고 운영 상태를 정상으로 되돌리는 등의 활동이 포함됩니다. 이러한 질문은 조직이 사이버 공격으로부터 효과적으로 복구되고 있는지 파악하는 데 도움이 될 수 있습니다.

예	아니오	
☐	☐	사이버 공격을 격리하고 억제하기 위한 인시던트 방지 조치를 시행하고 있습니까?
☐	☐	인시던트 방어 후 시스템 또는 디바이스를 복원하는 프로세스가 마련되어 있습니까?
☐	☐	데이터 보호 시 데이터 격리, 변경 불가 기능 또는 사이버 볼트 등을 활용합니까?
☐	☐	데이터가 손상, 암호화 또는 삭제된 경우 데이터를 깔끔하게 복구하기 위한 절차를 수립했습니까?
☐	☐	사이버 공격으로부터 복구를 자동화하거나 신속하게 처리할 수 있도록 AI/ML 기술을 활용합니까?
☐	☐	지속적으로 인시던트를 평가하고 공격 및 복구 이후 개선할 영역을 식별합니까?
☐	☐	공격 방법을 이해하고, 침해 정도를 판단하며, 영향을 받는 시스템과 데이터를 식별하고, 증거를 수집하여 보다 안전하게 보호하고 법적 또는 징계 조치를 취할 수 있도록 포렌식 분석을 실시했습니까?
☐	☐	고객, 파트너, 공급업체 등 관련 당사자에게 사이버 공격과 데이터 또는 운영에 미치는 잠재적 영향에 대해 알려야 한다는 사실을 인식하고 있습니까?
☐	☐	비즈니스를 복원하고 SLA를 충족할 수 있도록 매년 여러 차례 복구 전략을 연습하고 있습니까?
☐	☐	서비스 제공업체와 협력하여 복구 지원 서비스를 제공합니까?

사이버 보안 강화 및 제로 트러스트 성숙도 향상

IT 조직은 사이버 보안에 대해 최악의 시나리오에 대비하는 계획을 세우고 여러 단계의 방어 체계를 구축해야 합니다. 끊임없이 진화하는 사이버 보안의 위협 환경에서는 보안 관행을 지속적으로 발전시키고 제로 트러스트 원칙을 도입하는 것이 중요합니다. 여기에는 다음이 포함됩니다.

공격 노출 지점 축소

환경을 손상시키는 데 악용될 수 있는 취약성과 진입점을 최소화합니다.

사이버 위협 탐지 및 대응

잠재적인 보안 인시던트와 악의적인 활동을 적극적으로 식별하고 해결합니다.

사이버 공격으로부터 복구

보안 인시던트가 발생한 조직을 이전의 알려진 안전한 운영 상태로 복원합니다.

Dell은 전문 서비스의 전문 지식을 활용하고 신뢰할 수 있는 비즈니스 파트너와 협력함으로써 진화하는 사이버 위협으로부터 보호하는 포괄적인 보안 태세를 갖출 수 있도록 지원합니다. 기술이 발전함에 따라, 디지털 인프라를 보호하고 디지털 영역에 대한 신뢰를 유지할 수 있도록 사이버 보안에 대한 접근 방식도 진화해야 합니다.

DELL Technologies

Dell Technologies 소개

Dell Technologies는 조직 및 개인이 디지털 미래를 구축하고 업무 처리와 생활 방식은 물론 여가 시간을 보내는 방식도 혁신하도록 지원합니다. Dell Technologies는 데이터 시대를 맞이하여 업계에서 가장 광범위하고 혁신적인 수준의 기술 및 서비스 포트폴리오를 제공합니다.

자세한 정보: www.dell.com/securitysolutions