데이터 시트

Active Directory 보안 평가

Active Directory의 잘못된 구성, 프로세스 취약점 및 악용 방법 완화

이점

- 조직 Active Directory 환경의 현재 상태에 대한 가시성을 확보합니다.
- 일반적으로 악용되는 Active Directory의 잘못된 구성 및 설정의 위험을 선제적으로 완화합니다.
- 일반적인 공격 경로를 강화하여 보안 사고의 위험과 영향을 줄입니다.
- 권한 있는 액세스를 최소화하기 위해 더 엄격한 정책을 구현합니다.
- Active Directory 환경 내에서 가시성 및 탐지를 증대합니다.
- Active Directory 인프라의 전반적인 보안 태세를 전략적으로 개선합니다.

FireEye Mandiant를 선택해야 하는 이유

FireEye Mandiant는 2004년부터 사이버 보안 및 사이버 위협 인텔리전스를 선도해 왔습니다. Mandiant의 사고 대응 팀은 전 세계에서 가장 복잡한 침해 사건을 일선에서 처리하고 있습니다. 당사는 공격자, 기계 및 피해자 인텔리전스 소스를 조합해서 활용하여 위협 공격자와 그들의 급변하는 전술, 기법 및 절차(TTP)를 심층적으로 이해하고 있습니다.

당사의 Active Directory Security Assessment(ADSA)는 광범위한 사고 대응 경험, 글로벌 격리 및 복구 서비스, 그리고 새롭게 등장하는 위협 인텔리전스에 기반하여 개발되었습니다.

이 평가에서 도출된 실제 지침 및 권장 사항은 고객 환경에서 공격자를 성공적으로 퇴치하고 위협으로부터 복구하는 테스트 및 검증을 거친 기법을 반영합니다.

이러한 사전 예방적 방법을 사용하여 조직은 Active Directory 보안 태세를 강화하고 Active Directory 환경에서 일반적인 약점을 악용하는 사고를 방지할 수 있습니다.

개요

Active Directory는 특히 기술과 조직이 발전함에 따라 관리하기가 복잡하고 성가실 수 있습니다. 조직은 종종 구성을 적절히 유지하고 Active Directory의 최신 보안 기능을 최신 상태로 유지하는 데 어려움을 겪고 있습니다.

ADSA 기간 동안, Mandiant는 귀하의 조직이 Active Directory 환경과 지원 인프라를 효과적으로 보호하는 데 필요한 주요 프로세스, 구성 표준, 보안 및 모니터링 제어를 개선할 수 있도록 지원합니다.

접근 방식

Mandiant 전문가들은 고객 조직의 주요 이해관계자들과 협력하여 일련의 현장 워크샵을 수행하여 기존 기술과 프로세스에 기반한 데이터 수집 및 스크립트 출력 분석을 수행합니다. 당사의 전문가들은 이 정보를 사용하여 아키텍처(온프레미스 및 클라우드 기반 환경 포함)를 평가하고 Active Directory 인프라 내에서 가능한 공격 경로를 식별합니다.

Mandiant 컨설턴트들은 권한 있는 사용자 액세스 및 권한 있는 액세스 관리를 강화하고, Active Directory에서 악의적인 이벤트를 가시화하고 탐지하며, 클라이언트의 Active Directory 인프라의 전반적인 보안 태세를 개선하기 위한 전략적 권장 로드맵을 제공합니다.

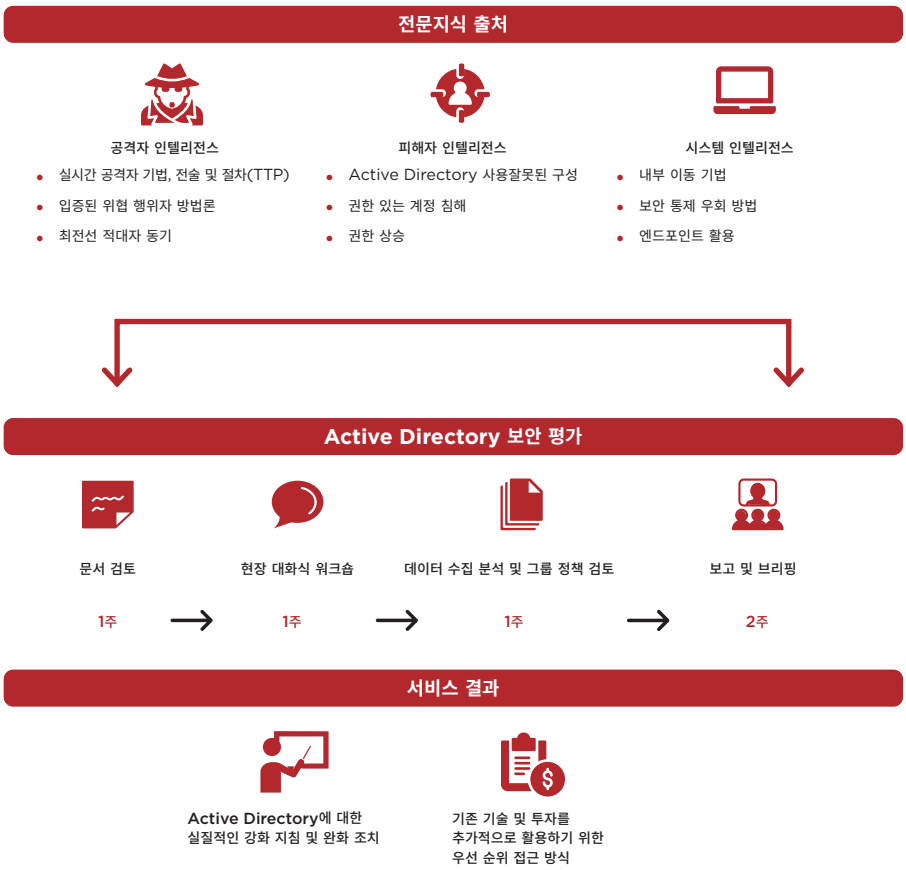

그림 1. 서비스 수명 주기

ADSA 중점 영역

- 포리스트 아키텍처 및 트러스트
- 운영 프로세스
- 모니터링 및 대응
- 권한 있는 계정 및 액세스 관리
- 그룹 정책 통제 및 집행
- 권한 위임
- 서비스 계정 및 서비스 사용자 이름(SPN)
- 원격 액세스 통제 및 강화
- 엔드포인트 구성 및 강화
- Microsoft Azure 및 Microsoft Office 365와의 통합

결과물

평가는 다음 사항을 포함하는 상세한 보고서로 마무리됩니다.

- 환경에 대한 기존 Active Directory 보안 구성의 스냅샷
- 현재 기술과 운영 프로세스에 맞는 특정 Active Directory 보안 모범 사례
- 환경 내에서 특권 사용자 액세스 및 계정을 제한, 관리 및 모니터링하기 위한 실질적인 권장 사항
- Active Directory 인프라의 보안 태세를 더욱 강화하기 위한 자세한 권장 사항

FireEye에 대한 자세한 정보: **www.FireEye.com/services**

FireEye Korea
서울특별시 강남구 테헤란로 534 글라스타워 20층
02.2092.6580
korea.info@fireeye.com

FireEye, Inc. 소개
FireEye는 인텔리전스 기반의 보안 회사입니다. FireEye는 혁신적인 보안 기술, 국가 수준의 위협 인텔리전스 및 세계적으로 유명한 Mandiant® 컨설팅을 결합한 단일 플랫폼을 제공하여 고객 보안 운영플랫폼을 완벽하게 확장합니다. 이를 통해 FireEye는 사이버 공격에 대비하고 이를 방어 및 대응하고자 노력하는 조직의 사이버 보안 부담을 줄이고 간소화합니다.