Tenable.ad 제품소개서

tenable 공식 총판

ROLTECH

tenable.ad

격

I. 2023 보안 동향

II. Tenable.ad로 시작하는 AD보안

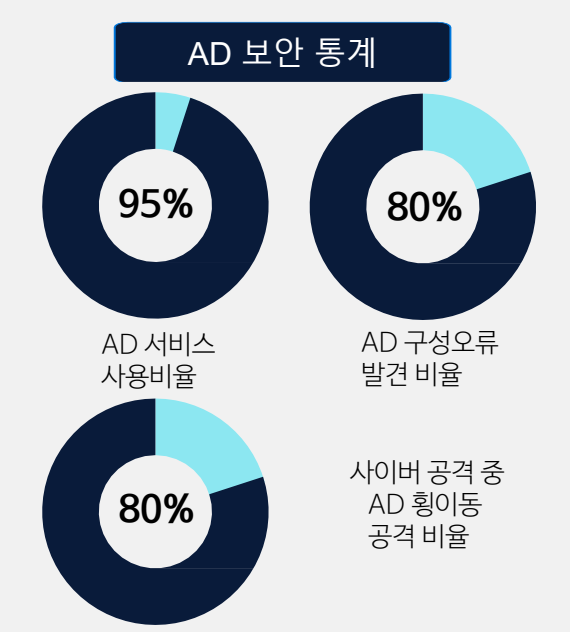
III. Tenable.ad 차별점

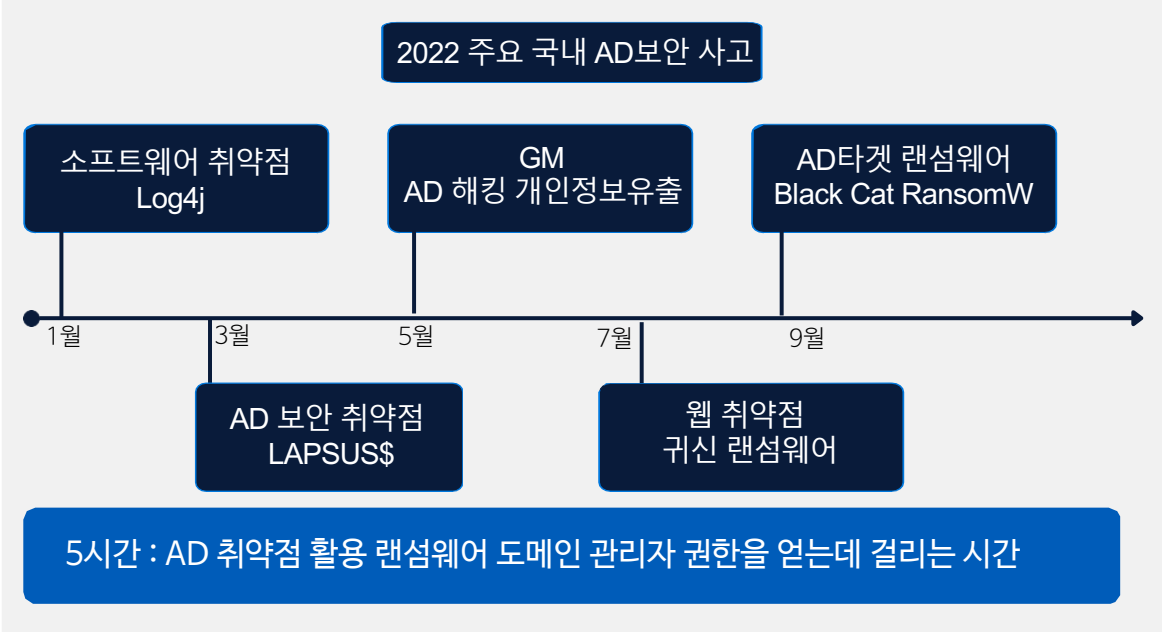
IV. Tenable.ad 도입 효과

V. Tenable 위험노출관리 솔루션 소개

침해 사고의 원인, 보안 취약 Active Directory

2019년 이후 Active Directory 침해 공격이 증가, 보안 사고 발생이 늘어남
AD 보안사고는 2019년 큰 피해를 후 2020년 말부터 다시 크게 증가하는 양상을 보임
2023년 내부 직원 계정, 권한 탈취 공격 사고사례가 증가하고 있음. (2023 KISA 사이버 위협전망)





1) Active Directory 침해 추이 : 한국인터넷 진흥원 2022, TTPs#4: AD 환경을 위협하는 공격 패턴 분석
2) AD 보안통계 : Crowdstrike 2023 global Threat Report

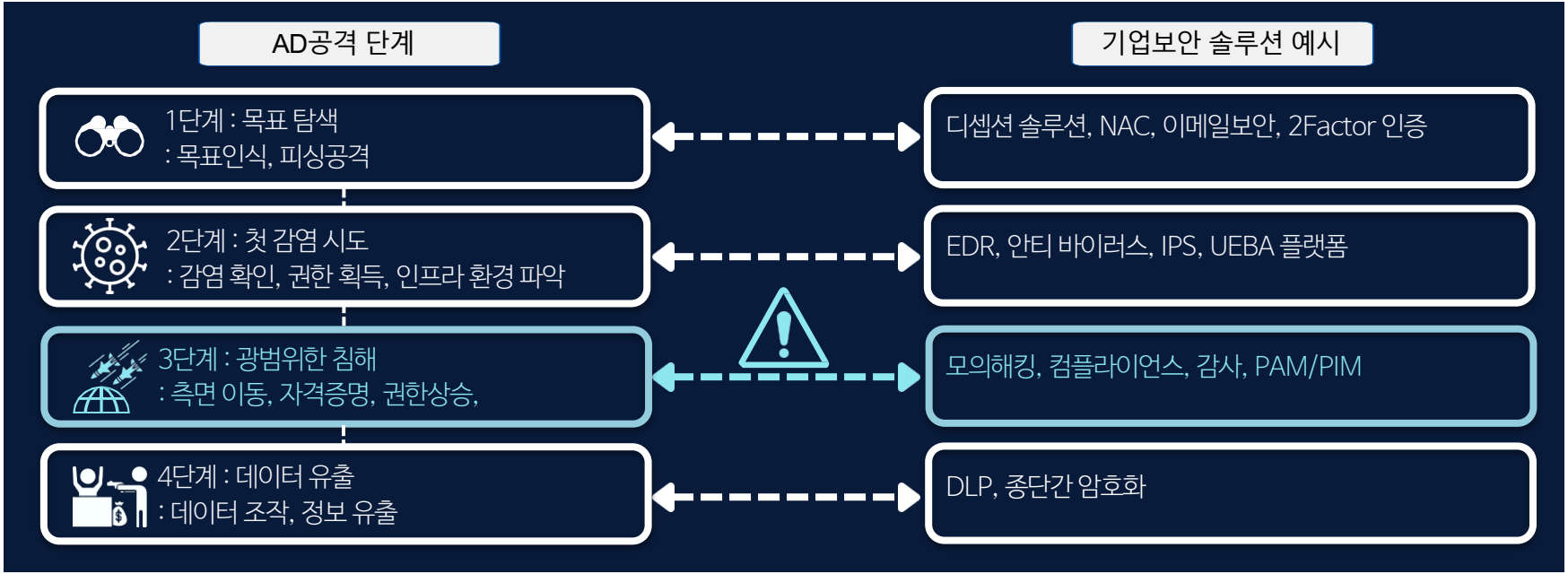
Active Directory (AD) 란?

AD란 마이크로소프트사의 윈도우 환경용 LDAP 디렉토리 서비스로 구축형 AD-DS와 클라우드형 Azure-AD가 있음.
윈도우 환경에서 다양한 중앙 관리 서비스를 사용할 수 있도록 지원함
모든 기업 IT 자산의 열쇠 역할을 하므로, AD 보안 실패는 전체 시스템에 큰 타격을 줄 수 있음.

	AD 대표적기능 예시	AD 공격 예시
계정	잘못된 반복 로그인 시도 시 계정 차단	무제한 계정 비밀번호 추정 시도 허용
접근	원격 컴퓨터 미확인 사용자 네트워크 공유차단 NTLM v1인증 (취약 프로토콜)비활성화	원격 컴퓨터 미확인 사용자 네트워크 공유 NTLM v1인증 활성화
권한	기밀 정보 접근 권한제한 사용자 컴퓨터 명령 프롬프트 제한	기밀 정보 접근 허용 사용자 컴퓨터 명령 프롬프트 활성화
DRM	표준 북마크 집합을 통한 중요 리소스 접근	악성 사이트 링크로 북마크 대체
중앙관리	모든 도메인 컨트롤러에 동일 소프트웨어 설치	악성 소프트웨어 도메인 컨트롤러 설치
운영	윈도우 업데이트 적용	윈도우 업데이트 적용 중지

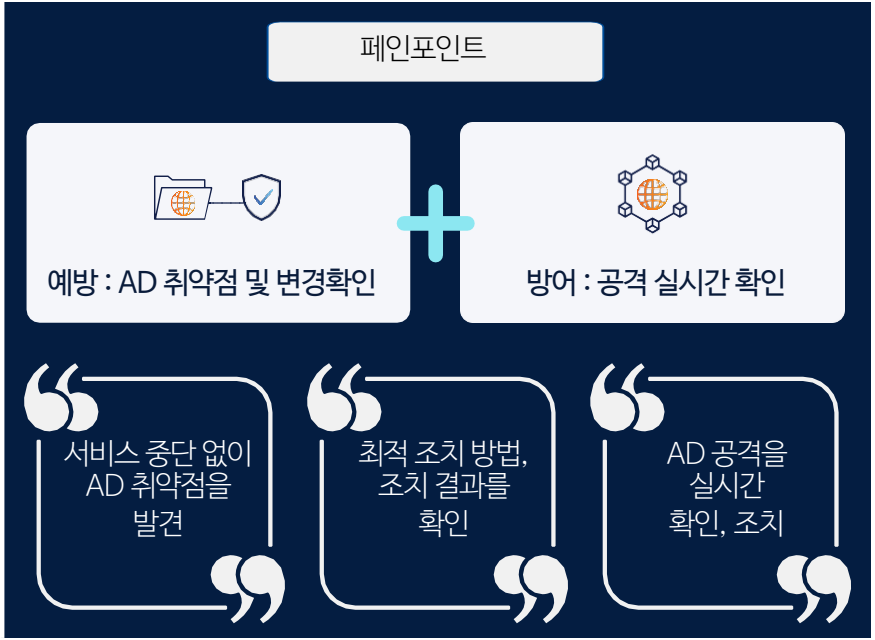
AD 공격의 특징 : 측면 이동

측면 이동(Lateral Movement)이란 정상 사용자를 가장하여 네트워크 내 시스템을 이동, 권한을 상승시키는 공격기법
해커는 Mimikatz, Kerberoasting, 정상 사용자를 가장 등을 통해 공격 경로를 찾아, 기존 솔루션으로 공격 탐지가 어려움
해커가 가장 관심을 보이는 광범위한 침해 단계에 대한 대응 솔루션이 부족한 상황임



AD 보안이 어려운 이유

AD는 사용 기간이 길어지고 조직 구성이 복잡해질수록 구성 및 연계 솔루션 관리 등의 복잡성이 발생함
AD는 24/7 운영되어야 하고, 보안보다 실행에 중점을 두는 인사 담당자나 IT 팀이 관리하는 경우가 많음
이로 인해 변경 이력을 관리하는데 그치고 보안을 위한 취약점 관리는 하지 않는 경우가 많음



노출 지표 : 취약점 예방보안

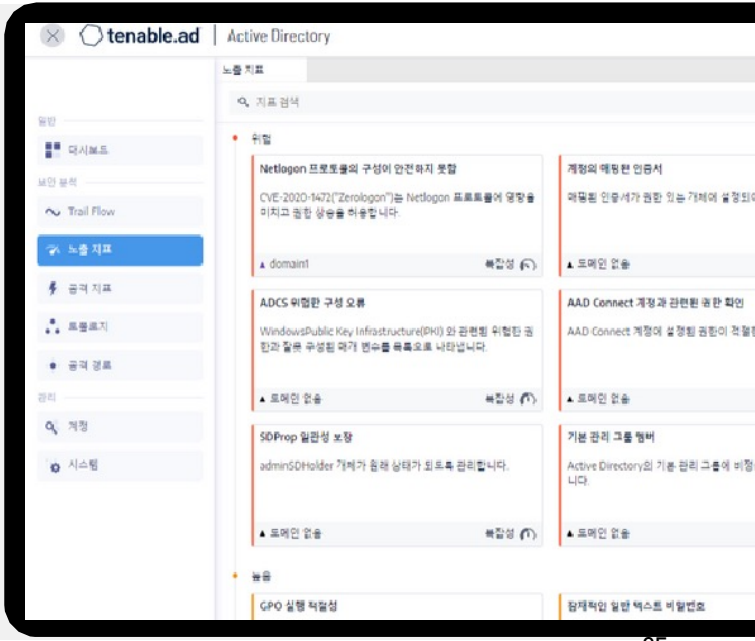
Tenable.ad는 노출 지표 (Indicator of Exposure)를 통해 AD 인프라의 보안 성숙도를 측정, 모니터링
취약점 데이터, 위협 인텔리전스(TI), 데이터 과학을 결합하여 심각도와 복잡도에 따른 취약점 우선순위 제공
비정상적 이벤트, 관련 오브젝트, 권고 조치방안 및 참조 문서 등을 상세 제공

IoE | 토폴로지 | 공격경로 | Trail Flow | IoA

Tenable.ad 는 AD 취약점을 발견하고 심각도, 복잡도 수준에 따른 요약 및 상세 화면을 제공합니다. 취약점 조치에 대한 상세 조치 방안도 함께 제공하여 빠르게 보안 성숙도를 관리할 수 있습니다.

주요기능

- AD 취약점을 심각도에 따라 위험, 높음, 중간, 낮음으로 분류
- AD 취약점 조치의 복잡도에 따라 분류
- 각 취약점에 대한 상세 정보, 관련 오브젝트, 권고 조치 방안 제공



토폴로지 : AD 인프라 구조 분석

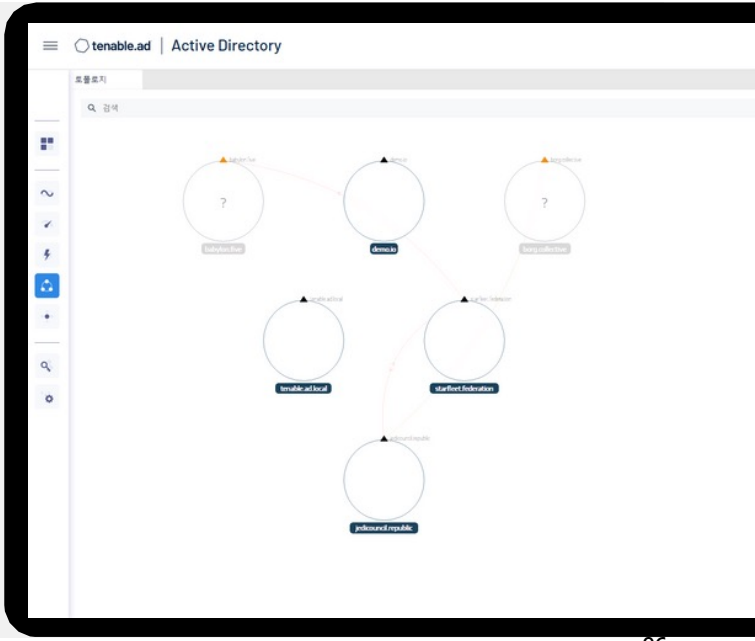
AD와 연동된 서비스를 맵 형태로 형상화하여 도메인, 포레스트간 관계를 시각적으로 제공.
각 트러스트 관계의 위험에 대한 상세 정보 제공

IoE | 토폴로지 | 공격경로 | Trail Flow | IoA

Tenable.ad 는 AD 인프라에 대한 반응형 맵을 제공합니다. 이를 통해 포레스트, 도메인과 트러스트 관계를 한눈에 파악할 수 있습니다.

주요기능

- AD 환경의 도메인, 포레스트 간 트러스트 관계 시각화
- 도메인 트러스트 관계의 위험 사유 가시화



공격 경로 : 다양한 AD 공격 경로 시각화

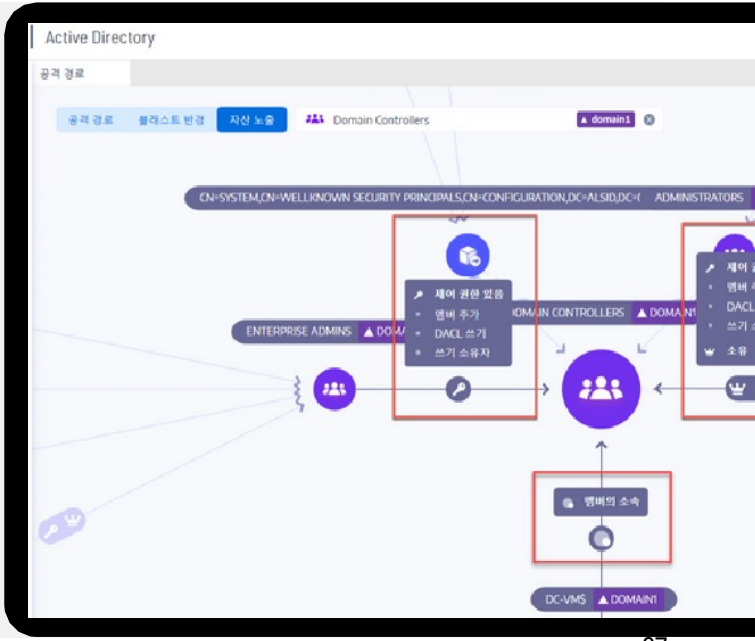
AD오브젝트간 권한/관계를 시각화하여 특정 포인트에 대한 접근, 침해 가능성 및 잠재적 취약점을 시각화
공격 경로, 블래스트 반경, 자산 노출을 시각화하여 표현

IoE | 토폴로지 | 공격경로 | Trail Flow | IoA

AD오브젝트간 권한/관계를 시각화하여 특정 포인트에 대한 접근, 침해 가능성 및 잠재적 취약점을 시각화
공격 경로, 블래스트 반경, 자산 노출을 시각화하여 표현

주요기능

- 공격 경로: 해커가 특정 포인트에서 특정 자산을 공격할 수 있는 경로 표시
- 블래스트 반경 : AD로 측면 이동 가능성 표시
- 자산 노출: 자산을 제어할 수 있는 모든 잠재적 경로 표시
- 티어 0 자산: 최중요 자산에 대한 공격경로 및 계정 표시



Trail Flow : 이벤트 모니터링 분석

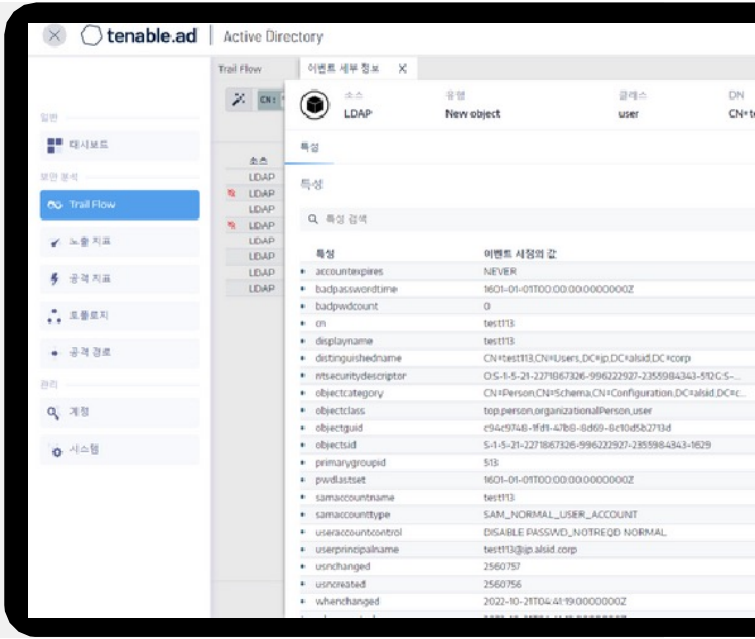
Tenable.ad는 AD 인프라에 영향을 미치는 변경 이벤트(패스워드, 계정추가 등)를 실시간 모니터링하고 분석
과거 이벤트의 간편 검색 및 쿼리 검색 제공

IoE | 토폴로지 | 공격경로 | **Trail Flow** | IoA

Tenable.ad 는 변경 이벤트의 실시간 모니터링 및 분석을 표시합니다. 시간을 거슬러 되돌아가 이전 이벤트를 로드하거나 특정 이벤트를 검 색할 수 있으며, 위협에 따라 악성패턴을 탐지할 수 있습니다.

주요기능

- AD 환경의 모든 이벤트를 다양한 조건에 따라 조회 및 검색(쿼리)
- 주요이벤트 예시 : UAC 변경, 멤버 추가, 비밀번호 변경



공격 지표 : AD 공격 실시간 모니터링

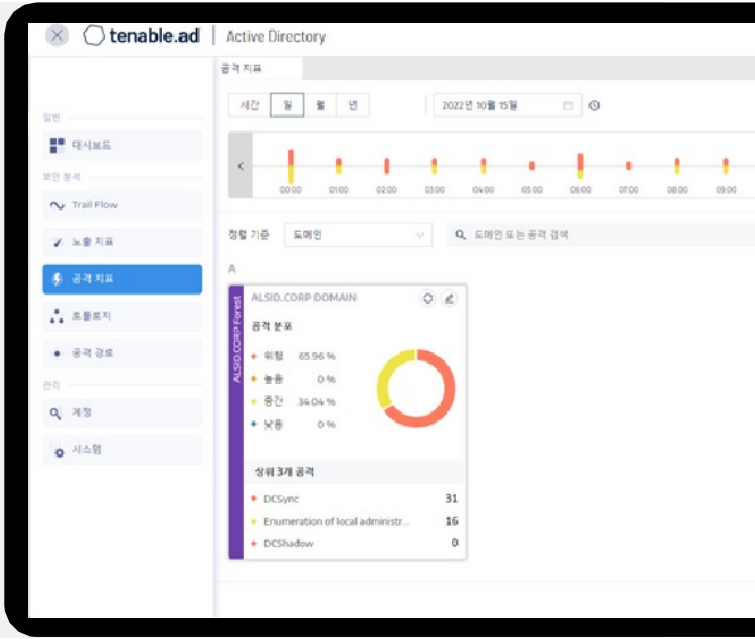
공격이 발생했을 때 실시간 알림 및 타임라인 제공
공격에 대한 요약 정보 및 MITRE ATT&K 정보 등 심층 정보 문서 제공

IoE → 토폴로지 → 공격경로 → Trail Flow → IoA

Tenable.ad는 AD에 대한 공격 징후를 실시간 감지하여 공격 지표로 타임라인과 함께 제공합니다. 또한 공격에 대한 요약 및 심층 정보를 제공합니다.

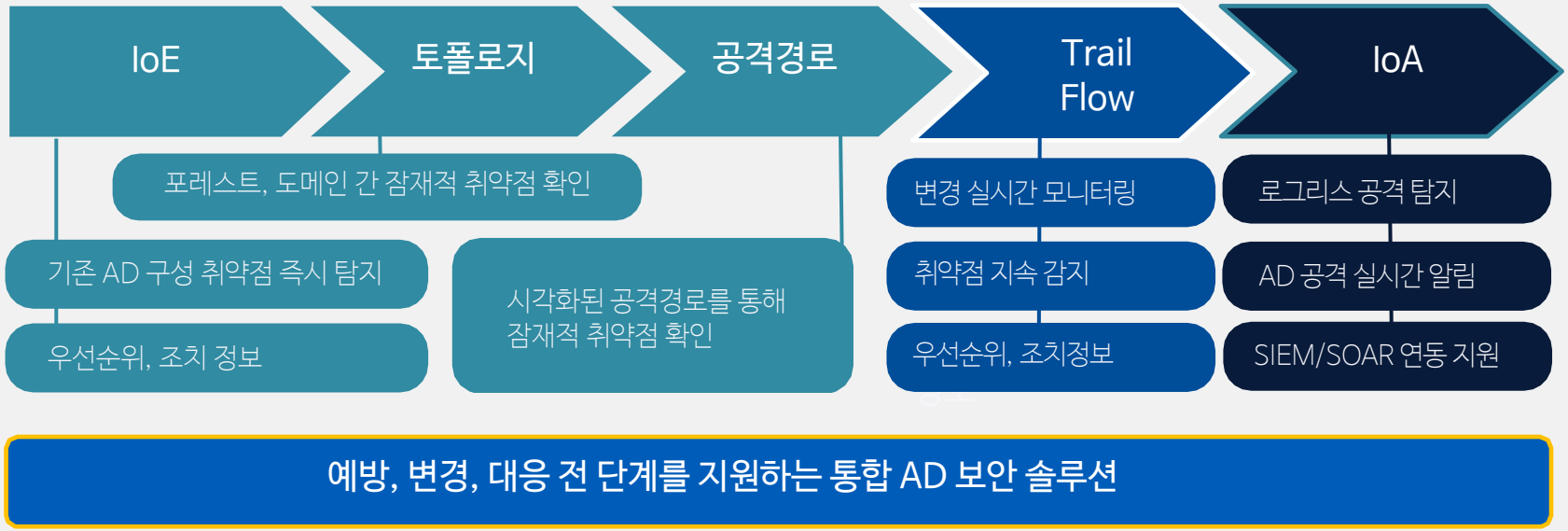
주요기능

- 공격 지표 발생내역 : 시간, 일, 월, 년 단위 조회
- 공격 지표 발생 도메인 표시
- 각 공격지표에 대한 심층 정보 제공



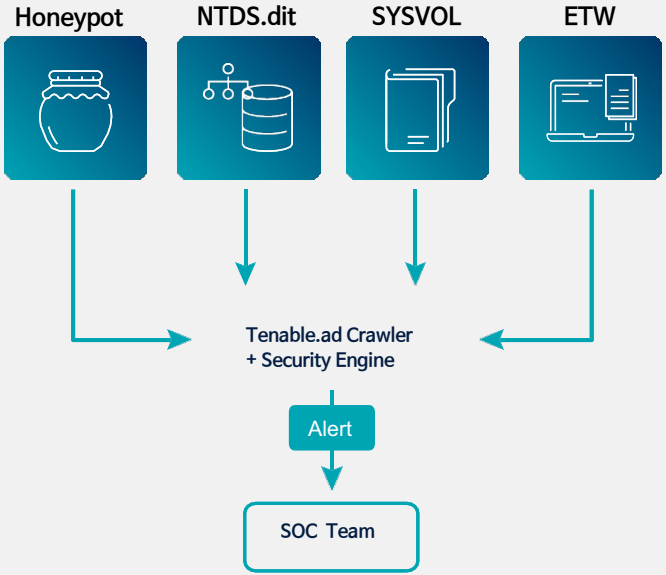
예방, 변경, 대응의 통합 AD 보안 솔루션

Tenable.ad는 예방, 변경, 대응에 이르는 모든 기능을 갖춘 AD 보안 솔루션
현재 구축된 AD 환경의 취약점을 초기 스캔을 통해 즉각 탐지하고 변경 사항의 취약점을 실시간 감지
AD 공격에 대한 실시간 알림을 제공하며 조치를 위한 상세정보 제공



AD 네이티브 기술 적용, 우수한 탐지능력

Tenable.ad는 자체 보유 네서스 기술력에 AD 보안 분야 세계 1위 기업 ALSID 솔루션을 융합
로그리스 AD 네이티브 공격에 대한 탐지, 대응 네트워크를 제공함



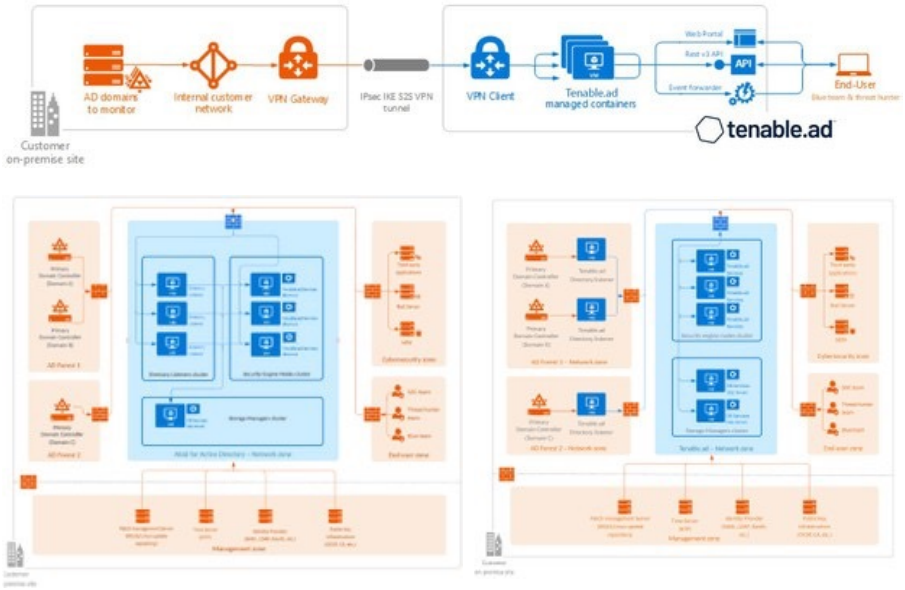
Tenable.ad 공격감지 소스

ETW	윈도우 이벤트 트레이싱 (커널 레벨 트레이싱)
NTDS.dit	DC간 복제 API를 활용한 AD 데이터베이스 변경사항
SYSVOL	GPT (General Policy Template)를 포함하는 System Volume 디렉토리
Honeypot	Honeypot 사용을 통해 ETW 정보 고도화

흔적을 남기지 않는 AD 공격 탐지

유연한 설치환경

Tenable.ad는 에이전트 설치나 추가 권한 설정이 필요하지 않음
구축형 (On-Prem) 및 클라우드 환경 하이브리드 설치 지원



Tenable.ad 구축형 구성요소

Directory Listner
AD DC 모니터링, 실시간 AD 플로우 수집
CPU 2 Core | RAM 12GB | DISK 30GB

Security Engine Node
핵심 서비스, 관리 콘솔, 분산가능
CPU 8 Core | RAM 16GB | DISK 200GB

Storage Manager
데이터 저장
CPU 8 Core | RAM 16GB | DISK 600GB

우선순위 및 편리한 사용성

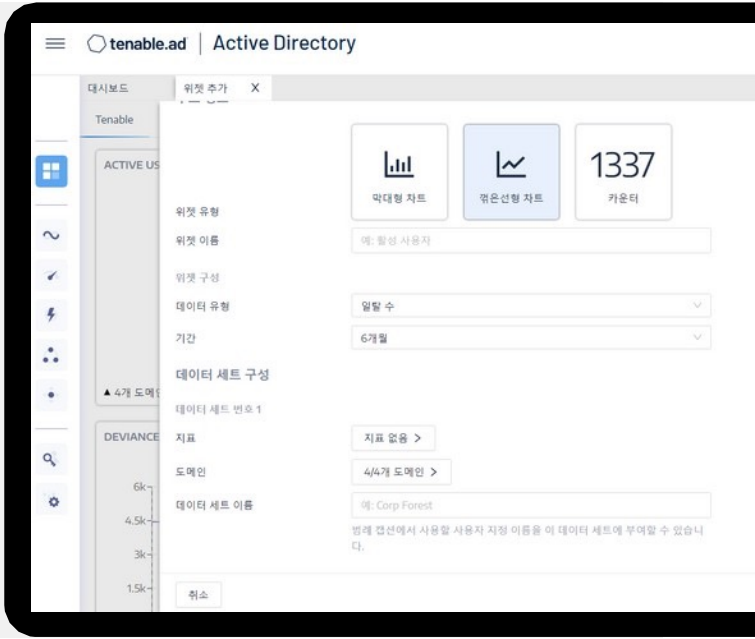
Tenable.ad는 AD 관련 취약점을 심각도에 따라 4등급으로 나누어 분류하여 조치 우선순위 전달
취약점, 설정오류, 도메인 별 컴라이언스 준수 현황 등의 정보를 위젯 형태로 제공
손쉽게 사용자 맞춤 대시보드를 생성, 삭제 지원

Tenable.ad 취약점 우선순위

위험 (14)	높음 (13)	중간 (13)	낮음 (4)
ADCS 설정, 구성 오류 SDPorp 일관성 AD PKI 암호화 알고리즘 DCSync 유사공격 허용 루트 주요 GPO 개체 및 파일 권한 비밀번호 정책 사용자 주 그룹, 관리그룹 케르베로스 위임, 권한 AAD 커넥터 계정 권한	위험 트러스트 KDC 비밀번호 변경 SID History 위험계정 비사용 OS 실행 컴퓨터 AD 스키마 위험권한 AAD SSO 비밀번호 변경 Protected User 그룹 미사용 권한 사용자 로그온 제한 GPO 실행적절성	만료없는 비밀번호 휴면계정 AdminCouont 특성 남용 GPO 해독가능한 비밀번호 기본관리자 계정 최근 사용 사용자 계정 Kerberos 구성 로컬 관리계정 관리 도메인 내 오래된 기능 컴퓨터강화 GPO	미연결, 미사용 GPO 권한있는 그룹의 사용중지계 정 위험한 이전버전 호환성 취약 Credential Roaming

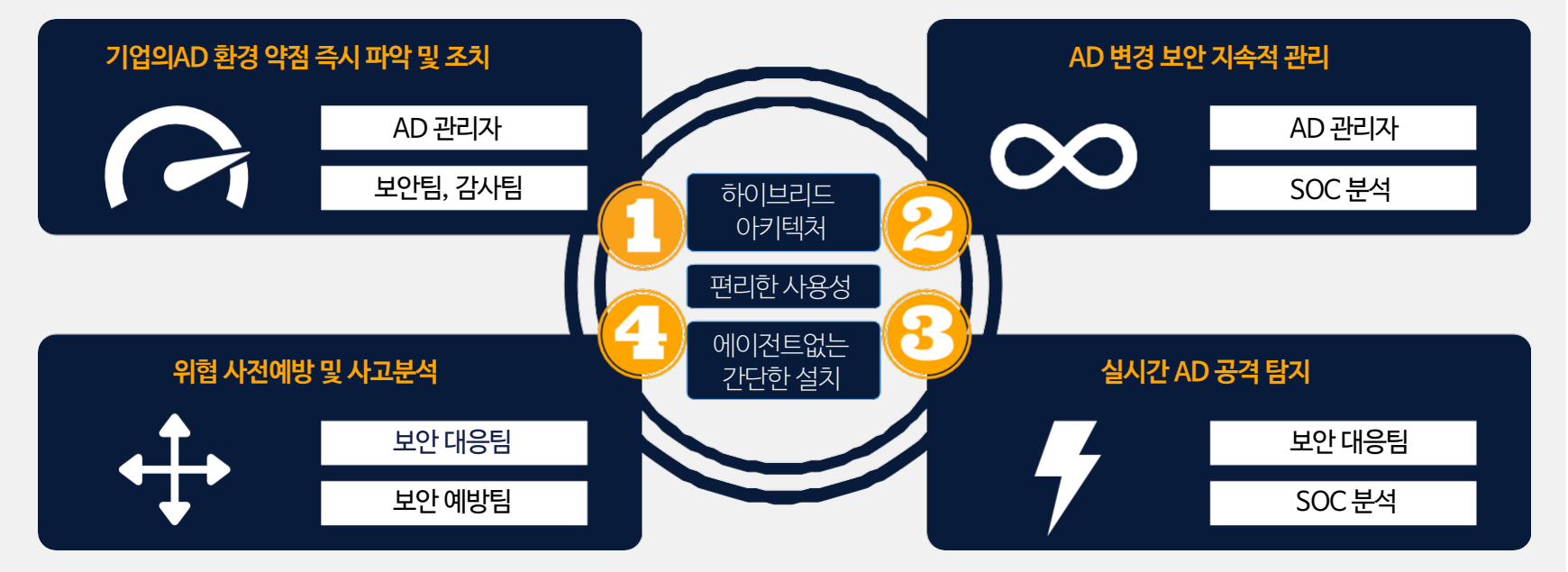
Tenable.ad 위젯 생성정보

위젯타입	바차트, 라인차트, 카운터
데이터	유저 수, 취약점의 컴플라이언스 스코어 (테너블 우선순위), 기간
지표	노출지표
도메인필터	도메인, 포레스트

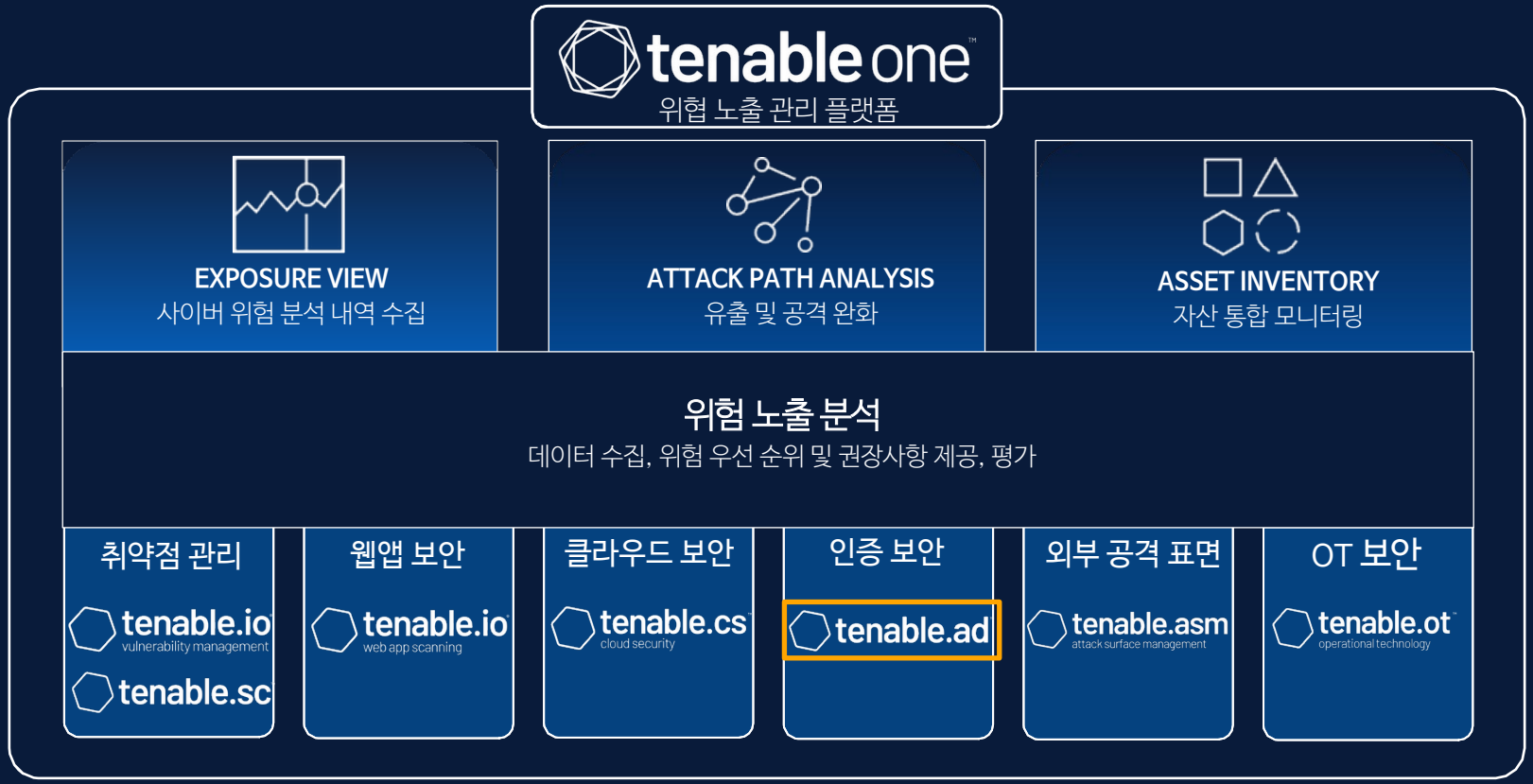


Tenable.ad 도입효과

Tenable.ad는 AD의 보안을 통해 측면이동과 권한 상승을 통해 내부에서 확산하는 공격을 방지
구축형과 클라우드 환경 모두 지원하며, 에이전트 설치 없이 간단하게 실행 가능



Tenable 위협 노출 관리 솔루션



Tenable.ad
위협 노출 관리, 지금 시작하세요

테너블 공식 총판 (주) 롤텍
E-mail : sales@roltech.co.kr
문의처 : 031-711-7108

tenable 공식 총판
ROLTECH