tenable

제로트러스트 구현을 위한 세계 1위 취약점 관리 솔루션

tenable.io
vulnerability management

tenable 공식 총판
ROLTECH

tenable.io
vulnerability management

I. 2023 보안 동향

II. Tenable 소개

III. Tenable.io 로 시작하는 위협 노출 관리

IV. Tenable.io 차별점

V. Tenable.io 기대효과

2022년 국내 사이버 침해사고 전년대비 1.6배 증가

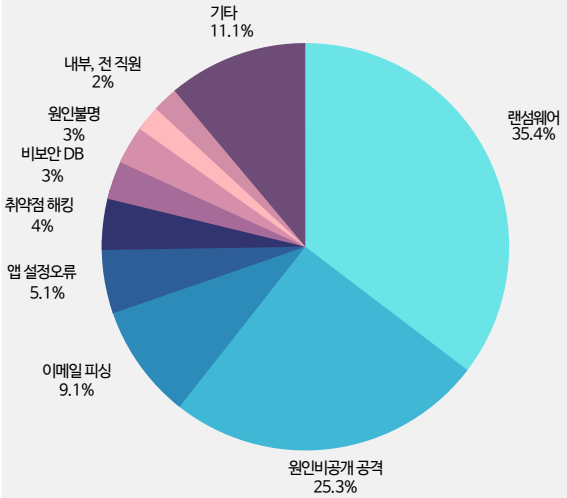
2022년 국내 사이버 침해사고는 전년대비 1.6배 증가 (국내 1.6배, 글로벌 1.4배)
침해사고 원인 1위는 랜섬웨어 등 악성코드 공격 (국내 47.7%,글로벌 35.4%)

2022 주요 국내 보안 사고

- **1월** — 소프트웨어 취약점 Log4j
  - -주요기반 시설 20% 취약점 노출, 공격 발생
- **3월** — AD 보안 취약점 LAPSUS$
  - -S사 190GB 소스코드유출
  - -L사 직원계정정보 등 9만건 탈취
- **5월** — 접근 제어 미설정 개인정보 해킹
  - -구독플랫폼 M사 개인정보 13,000 건 해킹, 과징금 7억
- **7월** — 웹 취약점 악성코드 귀신 랜섬웨어
  - -헬스케어A사 랜섬 지급 40억
  - -콜택시시스템 랜섬웨어감염
- **9월** — AD보안 취약점 LockBit 3.0
  - -S사 내부문건 공개
- **10월** — 클라우드 취약점 DB 설정 오류
  - -M사 2억 5000만 B2B 고객 데이터 유출

2022년 국내 데이터유출 기업 평균 피해 금액 43억 3400만원

2022 년 침해사고 원인



1) 침해사고 증가율 (국내 KISA 2022년 사이버 보안 위협분석, 국제 Checkpoint Research) 2) 주요 국내 보안사고 : 한국재정정보원, 2022년 주요 사이버 보안 사고 리뷰 / IBM, 2022 데이터 유출 비용 연구 보고서 3) 침해사고 원인분석 : 2022, Tenable Research Threat Landscape Report , 과학기술정보통신부 2021년 정보보호 실태조사

트렌드 변화 : 공격 표면의 급격한 확장

공격 표면(Attack Surface)이란 공격받을 수 있는 취약점이 있는 부분을 의미
코로나 19 이후 재택 근무 확산, 클라우드 전환, IoT 도입, 컨테이너 개발 환경 등 새로운 기술을 급격히 도입한 회사가 많음
급격히 확장된 공격표면은 서로 연결되어 한 부분의 취약점이 전체 시스템을 위협하며, 변경사항이 잦아 취약점 관리가 어려워짐

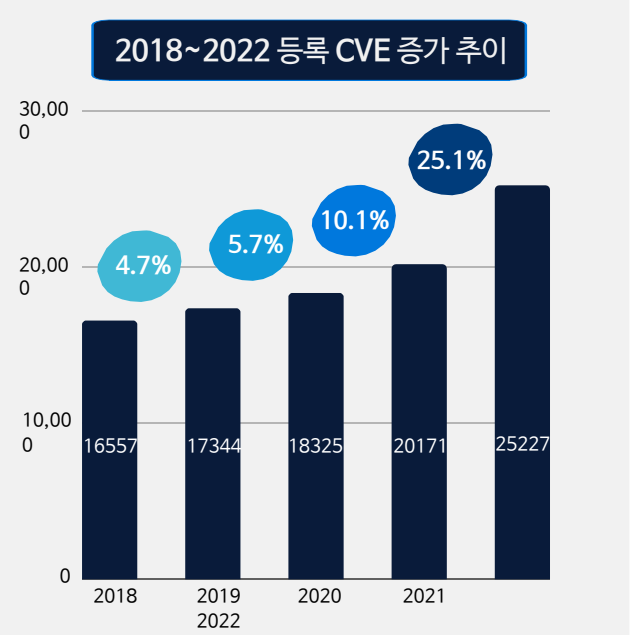
- 원격 IT — 소프트웨어 취약점
- 클라우드 — 클라우드 설정 오류
- 산업 인프라 — IT-OT 융합
- 웹 앱 API — 웹 애플리케이션 결함
- ID 인증 — 인증 설정 오류

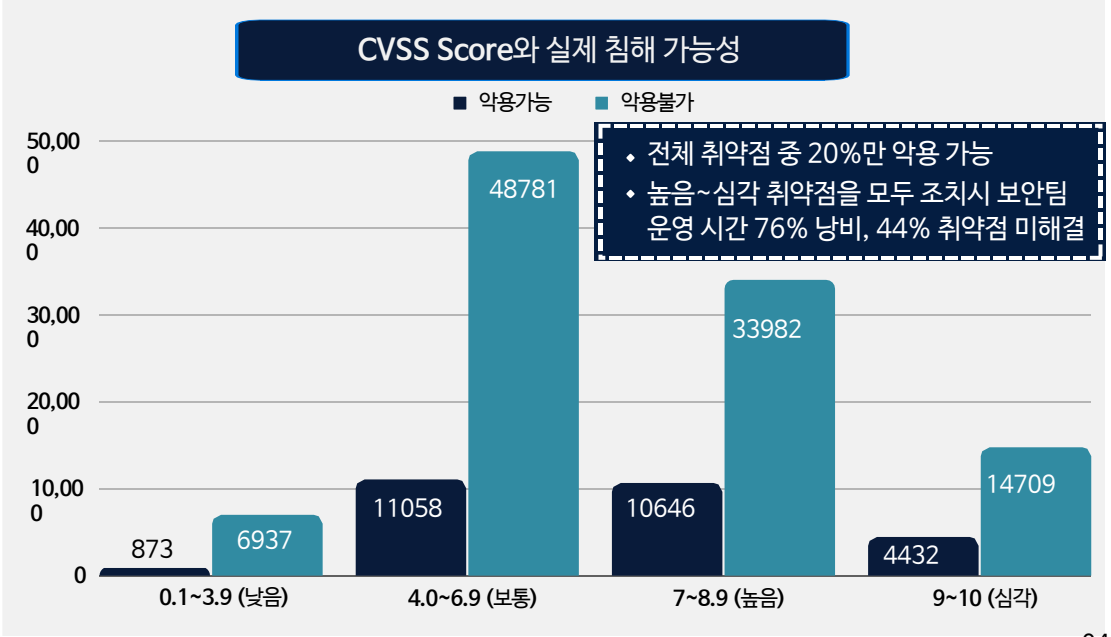
74% 코로나 19 시기 도입 자산에 대한 타겟 공격 비율

1) 코로나 도입자산에 대한 공격 비율 : Forrester 2021, Beyond Boundaries of cyber security in the new world of work

어려워진 취약점 관리 1 : 취약점의 폭발적 증가

2022년 전년대비 신규 CVE 개수 약 25%증가, CVSS (Common Vulnerability Scoring System) 상 "높음"이상 취약점이 56% (2021)
일반적 기업의 보안 자원으로 모두 관리하는 것이 불가능할 정도로 취약점의 개수가 늘어남
CVE (Common Vunurablities & Exposure)란 MITRE Corp.이 운영하는 전세계 통합 보안 취약점 리스트

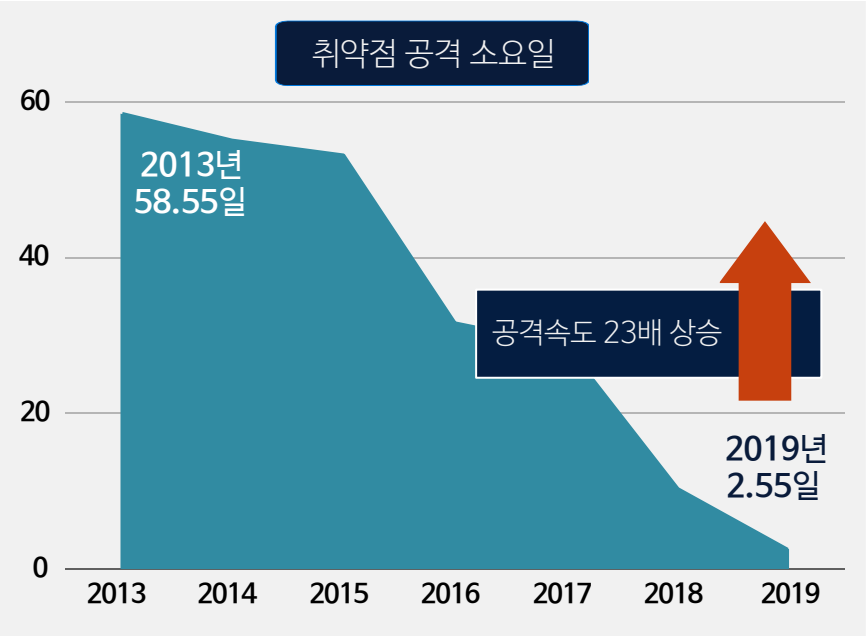


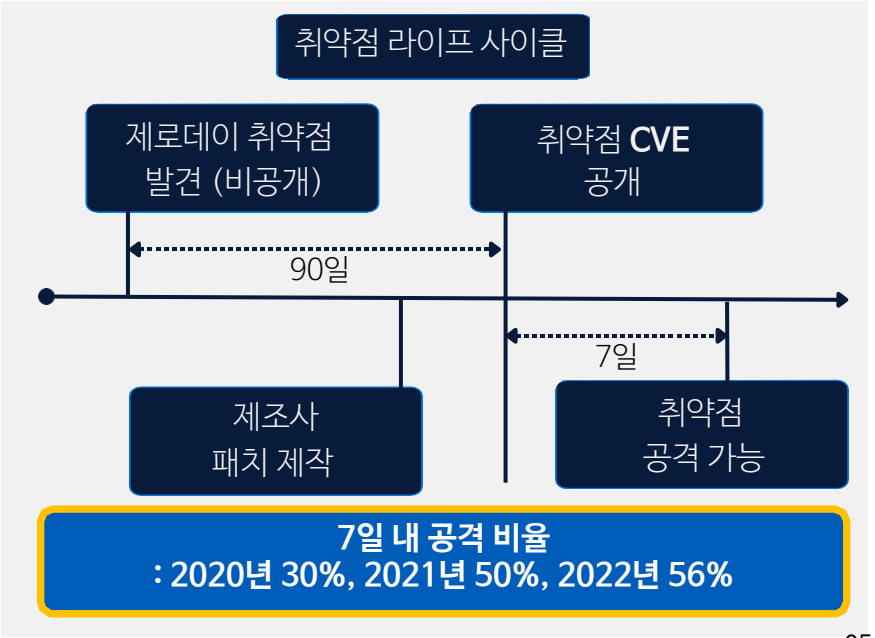


1) 2018~2022 등록 CVE개수 : cve.org
2) CVSS 실제침해확률 : Tenable Research, 2020, Why You Need to Stop Using CVSS for Vulnerability Prioritization

어려워진 취약점 관리 2: 빨라진 공격 속도

2021년 11월 ~ 2022년 10월까지 최소 31개의 기업형 랜섬웨어 그룹 발견
취약점 공격 속도가 23배 빨라지고 갈취 방법이 데이터 암호화, 데이터 유출, 서비스 중단, 데이터 파괴 등 다양화 취약점을 빠르게 발견하는 것이 취약점을 관리를 통한 공격 예방의 중요 지표가 됨





1) 랜섬웨어 그룹 : Tenable, 2022 Threat landscape report
2) 취약점 공격 소요일 : Gartner, 2020, Gartner's Strategic Vision for Vulnerability Management, 취약점 7일내 공격 비율 : Rapid7, 2022 Vulnerability Intelligence Report

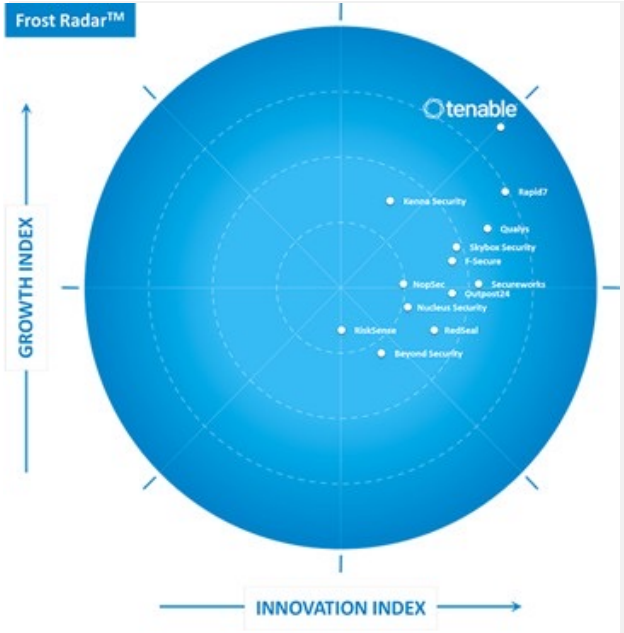
기존 취약점 관리의 한계

대부분의 기업은 정보보호 컨설팅 또는 취약점 진단 스캐너를 통해 취약점을 관리하고 있음
정보보호 컨설팅을 통한 진단은 스크립트를 통한 샘플링 1회성 진단으로 진단 방식과 진단 대상, 진단 품질에 문제가 발생
취약점 진단 스캐너는 자산과 취약점의 변화를 관리하기 어려움

분류	정보보호 컨설팅	취약점 진단 스캐너	대안
진단 주기	1년에 1~2회	사용자 정의	상시 모니터링
진단 방식	컴플라이언스 체크 스크립트	특정 시각 스캔 진행	다중 센서를 통한 진단
진단 대상	중요자산 표본	지정 범위 자산	기업의 모든 자산 및 변동사항
진단 품질	컨설턴트 역량 의존	특정 시각의 취약점 발견	지속적 취약점 발견

취약점 관리 점유율 1위 Tenable

Tenable은 2002년 설립된 취약점 관리 전문 기업으로 분야 전세계 점유율 1위를 차지하고 있는 마켓리
더 네서스 기술을 기반으로 위협 노출 관리를 통한 사이버 위험 감소를 위한 플랫폼 개발
광범위한 네서스 TI에 전세계 TI (위협 인텔리전스)를 통합하여 취약점 전문 서비스를 제공



취약점 관리 시장 점유율 세계 1위
27.5% 점유율 1위, 국내 100개 이상 기업 사용

취약점 진단 범위 세계 1위
경쟁사 대비 20% 많은 CVE 진단 기준 적용

제로 데이 연구분야 테너블 리서치 운영
141/167 제로데이 취약점 발견 (2020/2021)
24시간내 신규 취약점 업데이트

40000+ 전세계고객사 4만개 이상

60% FORTUNE 500 기업 사용률

40% GLOBAL 2000 기업 사용률

CyberSecAsia Best VM 2022

GartnerPeerInsights Choice for VA 2019~2022

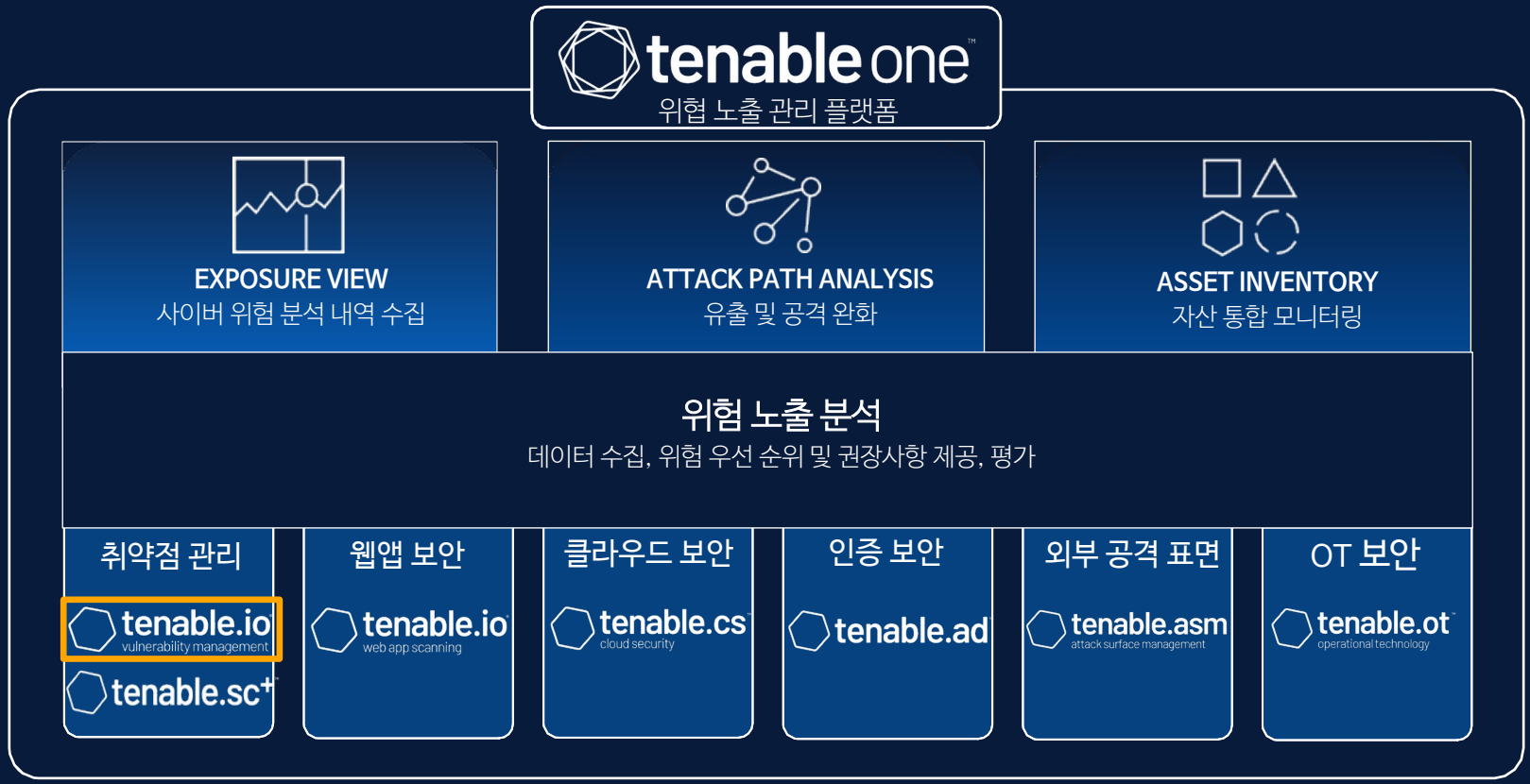
Frost&Sullivan VM leader 2021

IDC Worldwide VM market 점유율 1위(2020~2022)

Forrester Wave Vulnerability Risk Management leader

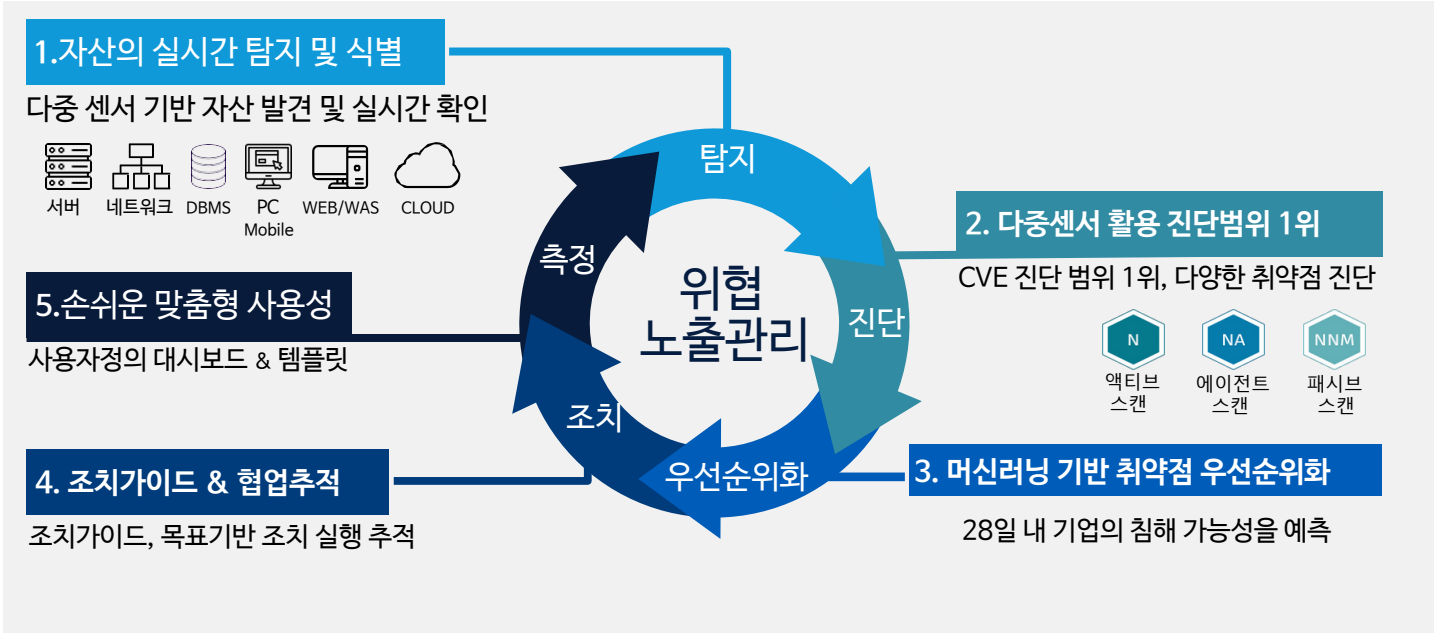
1) 점유율 1위: Worldwide Device Vulnerability Management Market Shares, 2021: “The Stakes Are High”

Tenable 위협 노출 관리 솔루션



Solution : No.1 취약점 관리 솔루션 Tenable.io

위협 노출 관리 (Continuous Threat Exposure Management)란 실제 위험을 기반으로 노출 공격 표면 취약점을 감소시키는 과정
위협 노출 관리는 취약점 관리의 새로운 패러다임으로 떠오름
Tenable.io는 탐지, 진단, 우선순위화, 조치, 결과 측정에 이르는 전 과정을 아우르는 통합 취약점 관리 솔루션



위협 노출 관리를 도입하는 조직은 2026년까지 보안침해 확률이 1/3로 감소할 것이다

Gartner

1)전 세계 1위 CVE 커버리지 : Principled Technologies Report 2019 – Comparing vulnerability and security configuration assessment coverage of leading VM vendors
2) GARTNER 2022, Implement a Continuous Threat Exposure Managemet Program

STEP 1 : 자산의 실시간 탐지

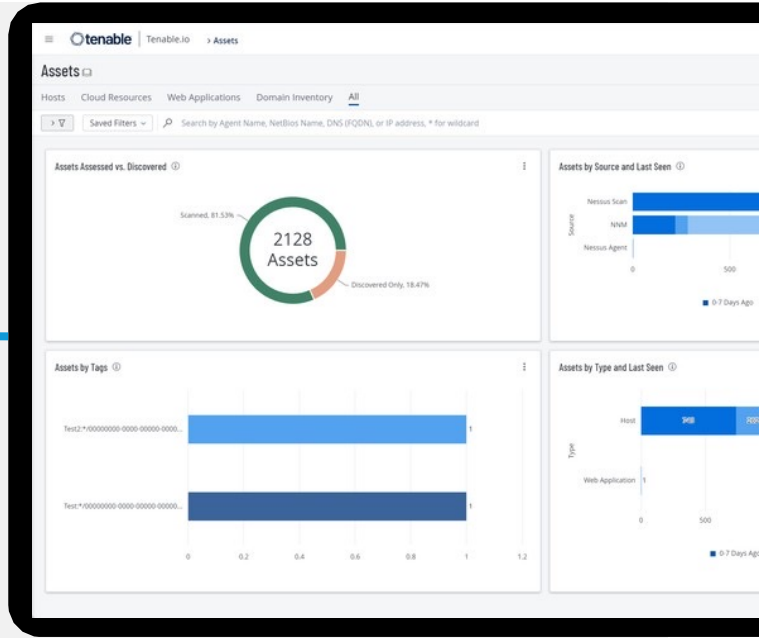
갖고 있는 자산을 실시간으로 파악하지 못하면, 취약점을 파악하는 것은 불가능함
변화하는 다양한 IT 자산 식별은 위협 노출 관리의 첫번째 단계
새로운 자산이 네트워크 상 탐지되거나, 변경이 발생했을 때 Tenable.io는 신속하게 식별 가능

탐지 → 진단 → 우선순위화 → 조치 → 측정

Tenable io는 다양한 네서스 센서 (액티브 스캔, 에이전트 스캔, 패시브 네트워크 모니터링, 클라우드 커넥터 등)를 활용한 다중 스캔을 통해, 다양한 자산을 파악하고 변경 사항을 신속하게 식별합니다

주요기능

- 호스트 자산 정보 식별 및 변경 사항 식별 (IP 주소, FQDN, 운영 체제, etc.)
- 클라우드 자산 정보 자동 식별 및 실시간 모니터링 (AWS,Azure,GCP)
- 웹 애플리케이션 식별
- 모바일 기기 (Microsoft Exchange, MDM) 식별
- NNM(Nessus Network Monitring) 통해 미확인 자산 식별
- 자동 태그 부여를 통한 쉽고 빠른 자산 검색
- 고급 자산식별 알고리즘 : 자산 추적



STEP 2 :다중센서 활용 탐지범위 1 위

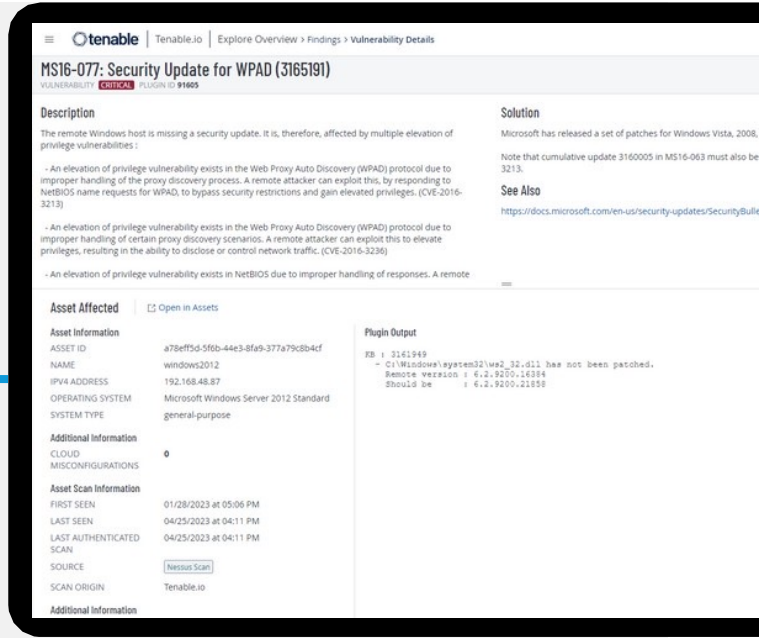
취약점 진단은 CVE 뿐만 아니라 클라우드 설정 오류, 웹 애플리케이션 취약점 등 폭넓은 취약점을 평가해야 함
Tenable.io는 76,000 개 이상의 취약점을 탐지하며 다양한 설정 취약점을 맞춤 가능한 템플릿을 통해 빠르게 평가
제로데이 취약점 연구소 Tenable Research에서 CVE공개 24시간 내 신속하게 진단 플러그인 자동 배포

탐지 | **진단** | 우선순위화 | 조치 | 측정

연 1~2회 진행하는 취약점 스캔만으로는 더이상 빨라진 공격 속도에 대응할 수 없습니다. Tenable.io는 패시브 스캔을 통해 자산별 취약점을 지속적으로 모니터링합니다.

주요기능

- 네트워크 스캔, 미패치 스캔, 다양한 설정 스캔 템플릿
- PCI DSS 인증을 위한 ASV 스캔 애드온
- 취약점 발행 후 24시간 내 최신 플러그인 자동 적용 취약점
- 이해를 위한 상세 정보 및 레퍼런스 제공

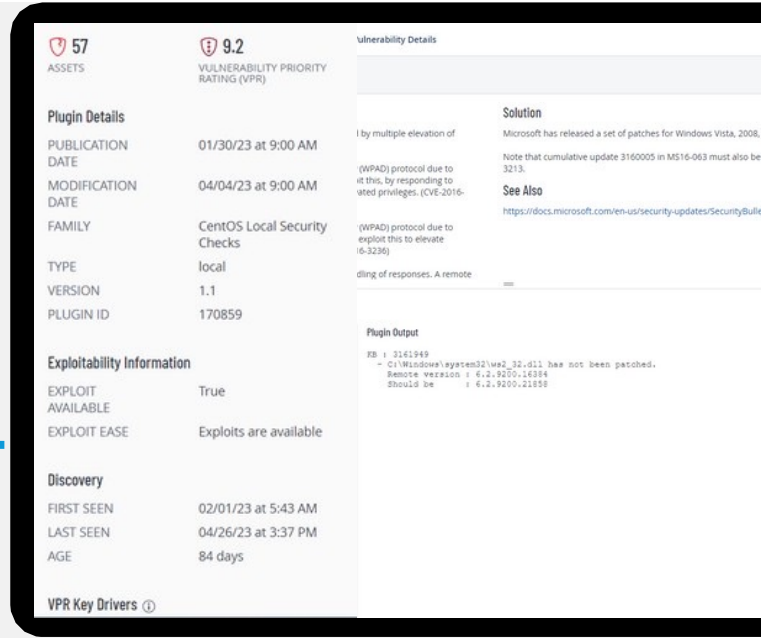


STEP 3 : 머신러닝 기반 취약점 우선순위

IT 자산 1개당 월 평균 발견되는 취약점은 평균 7개로 실제 관리를 위해 우선순위 조치가 필수적
CVSS는 최신 TI와 자산 영향도를 고려하지 않아 실무에서 보안 조치 우선순위로 활용할 수 없음
TI와 기업 자산을 토대로 기업맞춤형 예측적 우선순위 제공을 통해 취약점 관리 효율 증대

탐지 → 진단 → **우선순위화** → 조치 → 측정

Tenable. io는 선제적 보안을 위해 28일 내 침해 가능성을 예측하는 VPR(Vulnerability Priority Rating) 기반 우선순위와 기업의 자산별 파급 영향력 ACR(Asset Critical Rating)을 통해 실제 위험을 평가하는 우선순위를 제공합니다.



주요기능

- 예측적 우선순위 : 취약점 나이, CVSS, 악용코드 성숙도, 제품 영향력, 위협 인텔리전스 (TI), 스캔 데이터를 위협 모델링 머신러닝을 통해 28일 내 침해 가능성을 예측하여 우선순위 도출
- 기업 맞춤형 우선순위 : 기업 자산 상태 반영 우선순위 자동 도출

STEP 4 : 조치 가이드 & 협업 추적

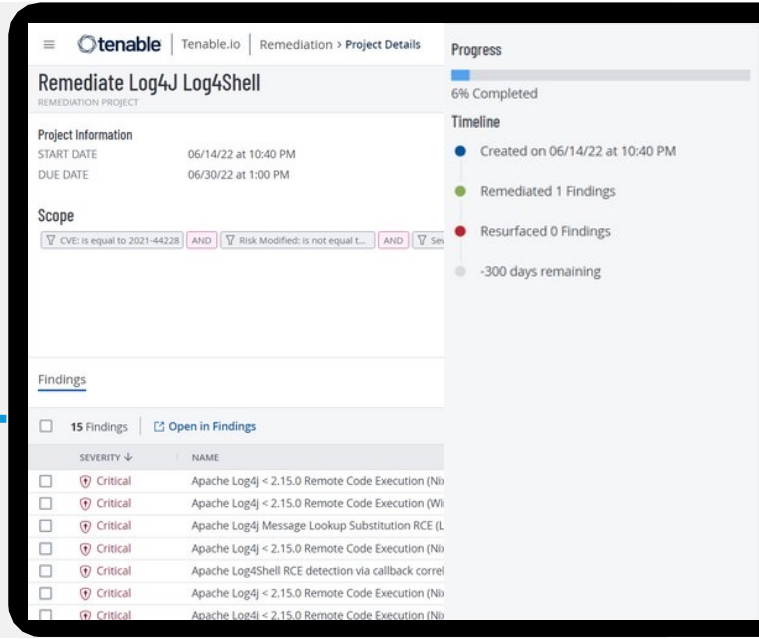
최적의 조치 방안을 찾아내고 우선순위에 따라 실행자에게 정보를 제공하는 과정의 신속함과 신뢰도 필수
Tenable.io는 취약점의 최적 조치 방법을 제공하여 보안 조치 효율을 높임
발견된 취약점 조치 작업에 대한 진행상황을 추적하여 조치 현황을 빠르게 확인 가능

탐지 → 진단 → 우선순위화 → **조치** → 측정

Tenable. io는 취약점 조치 방법을 제공하고, 조치 작업에 대한 협업을 원활하게 도와줍니다.

주요기능

- 조치 가이드 제공 : 최적의 조치 방법을 제공합니다.
- 목표 기반 조치 실행 추적 : 조치 목표를 세우고 작업을 배분하고 추적할 수 있습니다.
- SIEM, SOAR,티켓팅 시스템, 기타 보안 솔루션 플러그인 사전구축 통합 기능을 통해 쉽게 취약성 관리 프로세스의 완성도를 높일 수 있습니다.

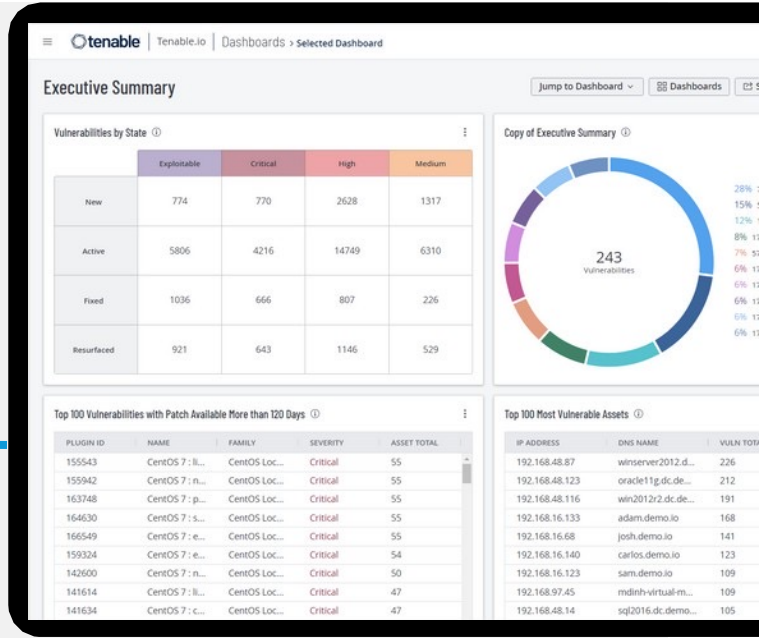


STEP 5 : 손쉬운 맞춤형 사용성

Tenable.io는 맞춤형 보고서 및 실시간 대시보드를 통해 취약점 현황 및 추세를 쉽게 확인 가능
다양한 사전정의 템플릿을 통해 간단하게 스캔 구성, 평가 실행, 결과 분석을 정리할 수 있음

탐지 → 진단 → 우선순위화 → 조치 → 측정

Tenable. io는 자산, 취약점, 조치 과정에 대해 가시성을 제공합니다.
최신 뉴스 피드를 통해 사이버 노출 경고를 제공합니다.

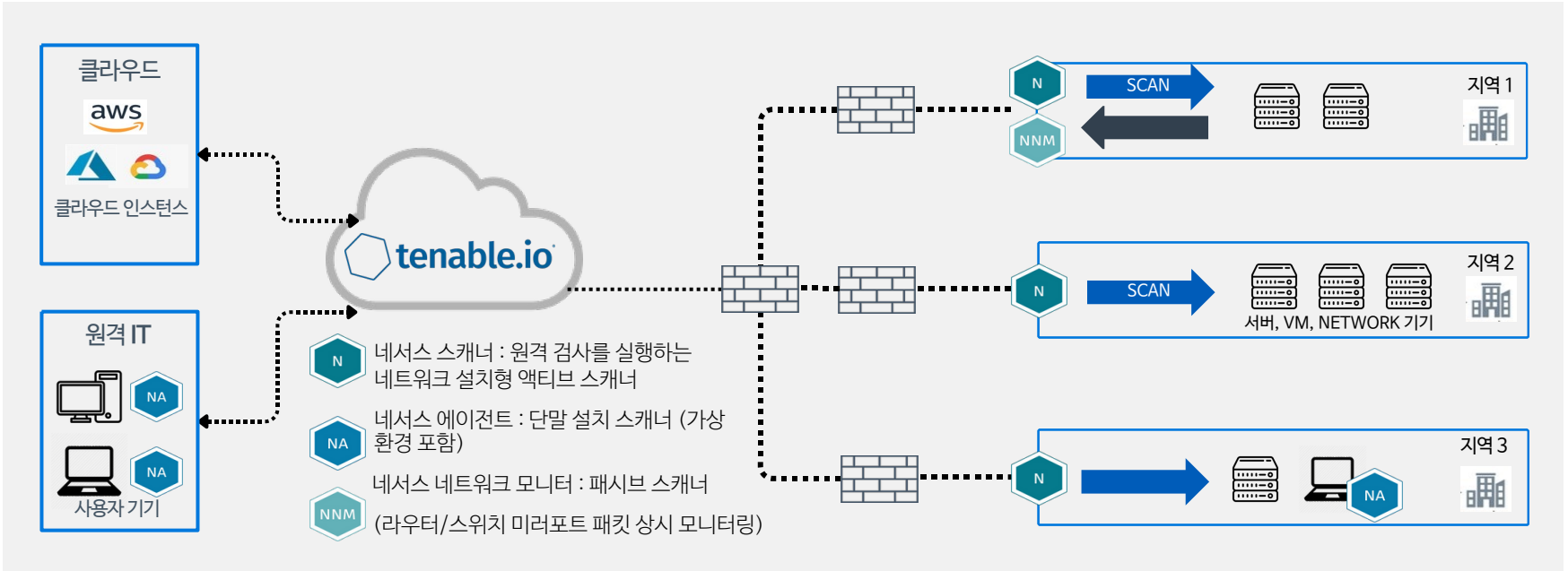


주요기능

- 맞춤형 대시보드 및 보고서 : 취약점 현황 및 추세 가시성
- 사전 정의 대시보드 및 보고서 템플릿 제공

다중 센서를 활용한 사각지대 제거

Tenable.io는 클라우드 기반으로, 취약점 탐지 세계 1위의 Nessus 기술을 활용하여 위험 노출 관리 체계를 실현
네서스 네트워크 스캐너, 에이전트 스캐너, 네서스 네트워크 모니터링 (패시브 스캔)을 활용하며 그외 클라우드 커넥터 등을 통해 다양한 센서와 연결되어 자산과 취약점의 사각지대를 제거하고 완전한 가시성을 확보



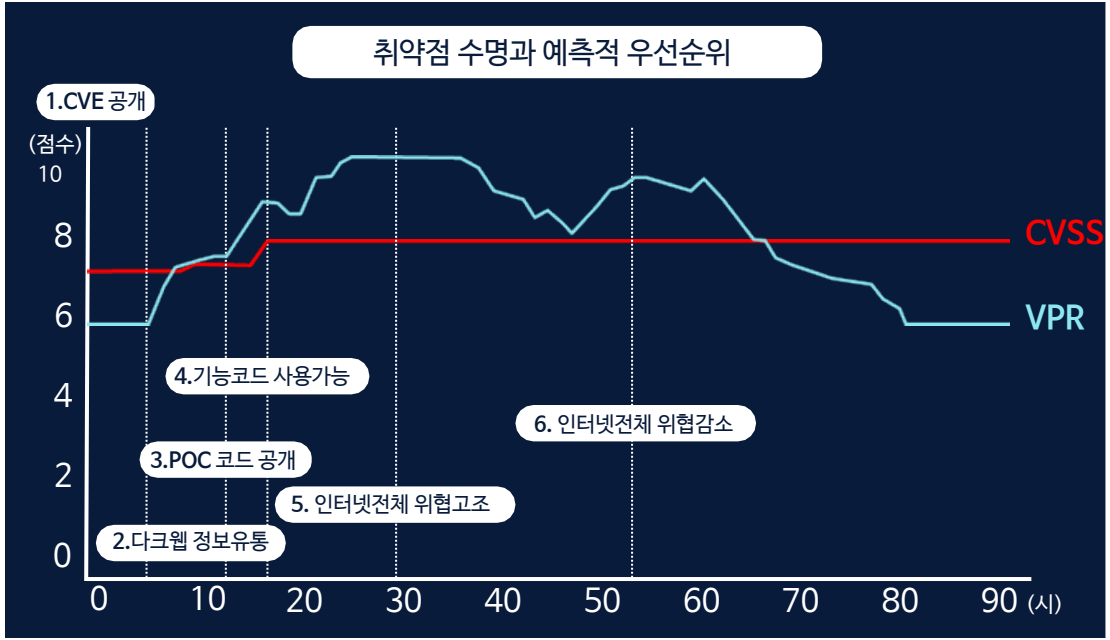
패시브 스캔을 통한 24/7 모니터링

네서스 네트워크 모니터는 사용자가 직접 스캔을 수행하지 않고 지속적으로 자산과 취약점을 모니터링 하는 테너블 특허기술
SPAN 포트 / TAP 장비로 트래픽 미러링을 통해 수집 정보를 분석, 미확인 자산, OS/어플리케이션/프로토콜/세션 정보 등을 모니터링
각 기기나 네트워크에 부하 없이 **실시간으로 지속적 탐지 가능**

24/7 지속 모니터링	실시간 정보 파악	IPv4/IPv6 모니터링
특정 시점 기반 액티브 스캔 공백 보안	시스템 간 연결내역 확인	IoT / 모바일 기기 모니터링
주요 시스템 보안 취약점 점검	비 표준포트 애플리케이션 점검	점검패턴 사용자 정의 가능

28일 공격 가능성 예측 우선순위 VPR

기존 우선순위 기준인 CVSS는 취약점의 수명과 기업의 자산 중요도를 반영하지 못해 실제 적용하기 위험
머신러닝을 통해 150개 이상 다양한 위협 인텔리전스 소스를 분석, 긴급한 취약점의 수를 97% 감소



VPR과 CVSS 실제 침해율 비교

With IoC	False	True
VPR		
1-Low	26889	1
2-Medium	28398	63
3-High	1259	263
4-Critical	289	102

With IoC	False	True
CVSSv3		
1-Low	937	5
2-Medium	22252	49
3-High	24892	278
4-Critical	8760	98

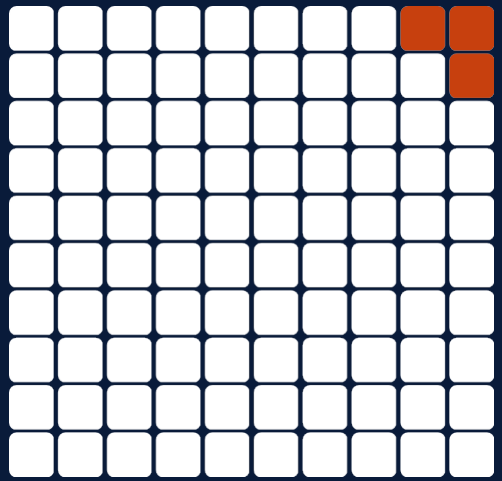
VPR 알고리즘 Key Driver

- 취약점 수명
- CVSS3 Impact Score
- Exploit Code 성숙도
- 취약점이 영향을 미치는 제품 범위
- 다크웹 등을 통한 위협 정보 소스
- 최근 위협 이벤트 발생 빈도
- 위협 이벤트 발생 현황

기업 맞춤형 보안 지표 AES

Tenable.io는 기업의 환경에 최적화된 보안지표를 통해 기업 맞춤형 우선순위를 제공
VPR(Vulnerability Priority Rating), ACR(Asset Critical Rating)을 통해 자산별 AES(Asset Exposure Scoring)를 도출
자산별로 취약점과 보안 상태를 한눈에 확인할 수 있음

공격자가 악용하는 취약점의 비율 3%



VPR 예측적 우선순위
: 머신러닝과 TI 활용
공격 가능성 예측

+

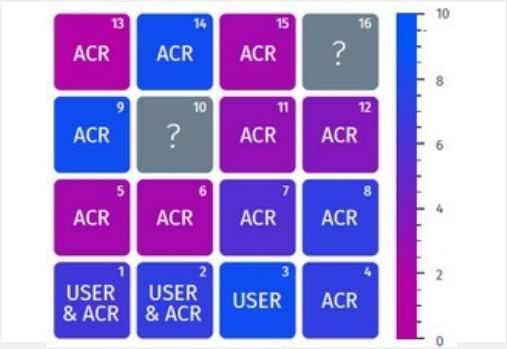
ACR 자산 중요도
: 자산의 기업가치와
영향도 측정

=

AES 자산 노출점수
: 각 자산별
보안 상태 지표

자동 ACR의 Key Driver

- 기기 타입
- 기기의 사용 목적 (Capability)
- 인터넷 노출 정도 사용자
- 입력 지원



다양한 확장 기능 – WAS, Container

Tenable.io 는 확장 프로그램을 통해 추가기능을 쉽게 추가할 수 있음
웹 애플리케이션에 대한 보다 상세한 취약성 검색을 제공하는 Tenable.io WAS
컨테이너 보안을 위한 Tenable.io Container Security 애드온

tenable.io web app scanning

DAST (Dynamic Application Security Testing) 기술을 기반으로 웹 애플리케이션 전용 스캐닝 운영의 다양한 방법을 제공합니다

주요기능

- JavaScript, HTML 5, AJAX 또는 SPA(단일 페이지 애플리케이 션) 등 최신 웹 애플리케이션 프레임워크 지원
- 다수 웹 애플리케이션 점검 동시 수행
- 성능 지연 , 중단 방지를 위한 제어기능, 자동점검기능
- 웹애플리케이션 특정 부분 예외 처리 기능
- 구축형 (On-Prem), 클라우드 기반 점검 가능

tenable.io container security

개발 운영중인 컨테이너의 보안을 위해 네트워크 외부로 컨테이너 이미지를 전송하지 않고 스캔하는 기능을 제공합니다

주요기능

- 개발 중 컨테이너 이미지의 취약점 분석하여 위험 노출 가능성을 사전 제거
- 계층별 취약점 분석 : 오탐 최소화
- 새로운 취약점 발생 시 자동 점검
- 사용자 정의 악성코드 탐지

Tenable.io 기대효과

자산 리스트 작성

숨겨진 자산을
찾아내는
패시브 디스커버리

다중센서 실시간 취약점 모니터링

다중 센서 기반
CVE 범위 세계 1위
실시간 취약점 감시

공격 확률 예측 맞춤형 우선순위

TI기반 머신러닝
공격 확률 예측
기업별 자산 중요
도

전사적 보안조치 속도 향상

조치가이드 제공
목표기반 실행추적
SIEM, SOAR 연동

보안 의사결정 속도 상승

실시간 대시보드 맞
춤형 보고서를 통한
의사소통 가속

Tenable.io
위협 노출 관리, 지금 시작하세요

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

tenable 공식 총판
ROLTECH