Endpoint · Server · Asset Security

V-Seeker

Windows·Linux 통합 보안 점검 솔루션

Security Operations · Current Reality

점검·점검·또 점검, 그래도 남는 빈틈

PC와 서버가 늘어난 만큼 보안 점검 업무도 늘었습니다. 하지만 인력은 그대로, 점검 결과와 실제 조치 사이의 간극은 커지고 있습니다.

P01 · 현장의 목소리

Issue 01

수백 대 PC·서버를 매번 수기로 점검해야 합니다 .

Issue 02

Windows와 Linux의 점검 체계가 분리되어 있습니다 .

Issue 03

점검 결과는 끝, 실제 조치는 다음으로 미뤄집니다 .

P02 · V-Seeker 응답

Response 01 · 자동화

한 번 설치, 자동으로 진단

에이전트가 상시 진단·정기 점검을 자동화하여 **소수 인력이 수백 대를 관리**할 수 있습니다.

Response 02 · 통합

한 콘솔에서 Windows·Linux 동시

분리되어 있던 점검 체계를 **하나의 화면**으로 통합, 운영 부담과 혼선을 줄입니다.

Response 03 · 진단·강화

위험 등급과 조치 방향까지 함께

취약점 발견에 그치지 않고 **우선순위·조치 방향**을 함께 제시해 즉시 대응을 돕습니다.

Why V-Seeker

한 솔루션, 7가지 핵심 장점

단순한 점검 도구를 넘어, 보안 운영·IT 자산·규제 대응을 동시에 해결하는 통합 플랫폼.

POINT 01

OS 통합 진단

Windows와 Linux가 섞인 환경도 한 콘솔에서 통합 관리

POINT 02

진단 → 강화

위험 등급과 조치 방향까지 함께 제시, 즉시 대응 지원

POINT 03

보안 + IT 관리

보안 점검·자산 관리·자원 관리를 한 콘솔에서 동시 수행

POINT 04

자동화 → 공수 절감

정기 점검과 실시간 관제 자동화로 소수 인력의 대규모 운영

POINT 05

국내 규제 대응

주요정보통신기반시설 (**KISA**) 취약점 점검 기본 제공

POINT 06

대규모 운영

수백 대 대량 배포·중앙 관제·원격 제어 지원

POINT 07 · 신뢰의 기반

안전한 운영 · 위·변조 차단

암호화 통신 · 관리자 2차 인증 · 에이전트 자가 보호까지, 외부·내부 위협에 모두 강한 보안 운영 환경

Solution Architecture

두 개의 엔진, 하나의 콘솔

각 장비의 **에이전트**가 진단을 수행하고, 중앙 서버의 **콘솔**이 전체를 통합 관제합니다.

壹 Endpoint · Agent

에이전트

- 각 PC·서버에 설치되어 자체 점검 수행
- 자산·하드웨어 자원 자동 수집
- 변경 사항 실시간 중앙 서버 전송

貳 Central · Console

중앙 서버 · 웹 콘솔

- 전체 장비 보안 상태 통합 대시보드
- 원격 점검 명령 · 보고서 자동 생성
- 자산 · 자원 · 위협 · 점검의 단일 창구

叁 Audit Layer

점검 레이어

- **기본 점검** · 자체 보안 기준
- **KISA 점검** · 주요정보통신기반시설
- 위협 탐지 / 이벤트 분석

점검 카테고리

⊞ Windows OS (PC · Server)

🎯 기본 보안 설정 분석 (Default Security Audit)

운영체제 전 영역의 보안 무결성 상태 자동 스캐닝

계정·권한 통제 | 시스템 정책 | 네트워크 보안 | 공유 폴더 | 소프트웨어 | 로그 정책

🔍 KISA 주요기반시설 기술 취약점 점검 (W-01 ~ W-64)

KISA 가이드라인에 따른 윈도우 5개 특화 영역

계정 | 서비스 | 패치 | 로그 | 보안

⌬ Linux OS (RHEL · Rocky · Ubuntu)

🎯 기본 보안 설정 분석 (Default Security Audit)

리눅스 커널 수준 보안 설정 및 시스템 권한 탐지

커널·권한 | SELinux | SSH 강화 | 방화벽 정책 | 무결성 분석 | 소프트웨어 | 프로세스

🔍 KISA 주요기반시설 기술 취약점 점검 (U-01 ~ U-67)

KISA 가이드라인에 대응하는 리눅스 5개 특화 영역

계정 | 파일·디렉토리 | 서비스 | 패치 | 로그

Solution Architecture

대규모 엔터프라이즈 환경을 위한 고성능 초경량 아키텍처

가벼운 에이전트와 비동기 고성능 서버의 결합으로 지연 없는 보안 통제 실현.

Key Features · 핵심 특징

- ✓ 자동 점검
- 🔒 암호화 통신
- 통합 관제
- 폐쇄망 대응

Threat · Event Analysis

위협 탐지 · 이벤트 분석, 숨은 징후를 가시화

점검 점수만 보는 것이 아닙니다. Windows와 Linux 양쪽에서 외부 침입 징후와 이상 이벤트를 카테고리 단위로 분석하고, 위협 여부를 분류합니다.

盂 내부 시스템 위협

소프트웨어 · 프로세스 점검

- 설치 프로그램의 신뢰도 · 위험도 평가
- CVE 연계 취약점 정보 자동 매칭
- 위장·악성 프로그램 징후 분석
- 정상 도구의 악용 정황 (정당 도구 오용) 탐지

Windows · Linux 양쪽 지원

孟 외부 침입 위협

외부 침입 직결 항목 점검

- 방화벽 · 원격 접속(RDP) · 위험 포트
- 취약 프로토콜 · 스크립트 실행 정책
- 업데이트 최신성 · 백신 위협 탐지 이력
- 위협 이력 관리로 재발 방지 근거 확보

실시간 모니터링

益 Windows 이벤트 분석

로그온 · 권한 · 정책 변경 이벤트

- 최근 로그온 성공/실패 이력 분석
- 권한 상승 · 계정·정책 변경 이벤트
- 접속 IP의 위치(국가) 확인 및 위협 분류

Windows · 이벤트 분석

嵩 Linux 침입 징후 탐지

SSH 무차별 대입 · 권한 상승 정황

- SSH 무차별 대입(brute-force) 자동 탐지
- 외부 IP 로그인 성공/실패 분석
- 신규 계정 생성 · sudo 권한 상승 정황
- 외부 접속 IP 국가 위치 · 위협 여부 분류

Linux · 침입 징후

Coverage Matrix

Windows·Linux 기본 점검 · KISA 점검

어느 OS든, 어느 규제 프레임도 동일한 체계로 진단. 환경이 혼합되어도 일관된 보안 기준을 유지합니다.

↓ OS · 점검 기준

OS · 01
Windows
PC · Server

OS · 02
Linux
RHEL · CentOS · Rocky · Ubuntu

기본 보안 점검

Default Security

- 기본 보안 설정 점검
- 외부 침입 위협 점검
- S/W 및 프로세스 위험성 진단
- 보안 이벤트 분석 및 침입 징후 탐지
- 실시간 위협 탐지

자체 보안 기준에 따라 계정·시스템·네트워크·공유·감사·고급 보호까지 카테고리 단위로 진단

KISA 기준 점검

KISA Compliance · 5 Areas · W-01 ~ W-67

주요정보통신기반시설 점검

계정 / 서비스 / 패치 / 로그 / 보안

KISA Compliance · 5 Areas · U-01 ~ U-67

주요정보통신기반시설 점검

계정 / 파일·디렉토리 / 서비스 / 패치 / 로그

Windows · Comprehensive Audit

Windows 점검

기본 보안 · KISA 기준 · 위협 탐지 · 이벤트 분석까지 카테고리 통합 점검.
PC·서버 모두 동일 체계로 커버합니다.

A · 기본 점검 · KISA 6 영역

운영체제 보안 설정 + KISA 주요정보통신기반시설

계정 · 시스템 · 네트워크 · 공유 · 감사 · 개인정보 · / 계정·서비스·패치·로그·보안·DB

B · 외부 침입 위협 점검

외부 침입 직결 항목 + 위협 탐지 이력

방화벽 / 원격 접속 / 위험 포트 · 프로토콜 / 스크립트 정책 / 업데이트

C · 소프트웨어 · 프로세스 점검

신뢰도·위험도 평가 (CVE 연계)

화이트리스트 기반 위장/악성 프로그램 징후 · 정상 도구 악용 정황 분석

D · 보안 이벤트 분석

로그온 · 권한 · 정책 변경 이벤트

접속 IP 위치(국가) 확인 · 위협 여부 분류 · 이벤트 이력 관리

E · 시스템 상태

업데이트 · 백신 · 방화벽 · 네트워크 종합

현 시점 보안 상태 종합 스냅샷

핵심 점검 리스트 (10 Key Checkpoints)

- 시스템 정보 (OS/CPU/RAM/Disk)
- 윈도우 업데이트 누락
- 레지스트리 보안 설정
- 방화벽 규칙 점검
- 비정상 공유 폴더
- 네트워크 포트 (TCP/UDP/LISTENING)
- 윈도우 감사 정책
- 사용자 계정
- 설치 소프트웨어 (라이선스/버전)
- KISA 보안 가이드 (주요/권고/선택)

Linux · Comprehensive Audit

Linux 점검

RHEL 계열(CentOS · Rocky · RHEL) 서버에 동일한 기본·KISA 점검 체계를 적용.

A · Linux 기본 점검

운영체제 보안 설정 점검

SELinux · SSH · 패키지 무결성 · CVE 연계 · auditd

B · KISA 5 영역 · U-01 ~ U-67

주요정보통신기반시설 리눅스 점검

계정 / 파일·디렉토리 / 서비스 / 패치 / 로그 관리

C · 보안 이벤트 분석 · 침입 징후

SSH 무차별 대입 · 권한 상승 정황 탐지

외부 IP 로그 · 신규 계정 · sudo 권한 · 외부 접속 IP 위치 분석

D · 시스템 상태

업데이트 · 백신 · 방화벽 · 네트워크 통합

현 시점 Linux 서버 보안 상태 종합 스냅샷

핵심 점검 리스트 (10 Key Checkpoints)

- 시스템 정보 (OS·커널·EOL·패치)
- 서비스·프로세스(데몬·예약·악성코드)
- 계정·인증 (root·sudo·암호정책)
- 네트워크·방화벽 (포트·정책)
- 파일·권한 (핵심파일·SUID·무결성)
- 네트워크 포트 & SSH 보안 (TCP/UDP/LISTENING)
- 로그·감사 (auditd·로그보호)
- 침입 탐지 (브루트포스·이상행위)
- 서비스 보안 (웹·DB·암호화)
- KISA 보안 가이드 (주요/권고/선택)

Central Server · Unified Console

중앙 서버, 보안 운영의 단일 창구

점검·자산·자원·위협·보고서까지 한 콘솔에서. 대시보드 한 장으로 전체 보안 상태를 파악하고 즉시 대응합니다.

300+
대 단위 에이전트 통합관제

2종
기본 + KISA 점검 자동 동시 실행

1콘솔
보안 · 자산 · 자원 · 위협 통합

Console · Function Modules

중앙 명령 컨트롤 타워 기능

📊 통합 대시보드 및 점검 매트릭스

전체 위험도 및 준수율 수치 시각화, OS(Windows/Linux) 간의 취약점 비교 분석, 점검 결과 로우 데이터 CSV/Excel 다운로드.

⚙️ 강력한 점검 명령 센터 (Command Center)

즉시 점검, 전체 일괄 스캔, 위협 탐지 이력 및 진행 상황 추적, 정기점검 및 일지 엑셀 자동 생성 배포 제어.

🌐 에이전트 무중단 원격 배포 및 예외 관리

관리 예외 처리 및 탐지 화이트리스트 정책의 원격 일괄 갱신, 에이전트 데몬 무중단 시작/종료/삭제 통제.

🔒 .report 전용 보안 보고서 생성

AES 256 강력 암호화가 적용된 원클릭 취약점 진단 점검 결과서 자동 생성 및 보고 증빙용 PDF 출력 기능.

대시보드 화면 샘플

※ 실 화면 예시 · 통합 보안 대시보드

Business Outcomes

도입 효과, 고객이 얻는 가치

규제 대응 · 운영 효율 · 위험 가시화 · 대규모 관리 — 임원이 보고할 수 있는 가치로 요약합니다.

REGULATORY

KISA 기본 제공

주요정보통신기반시설 점검 자동화로 규제 대응 부담 감소

VISIBILITY

위험 가시화

숨은 취약점을 등급으로 드러내 사고 예방

EFFICIENCY

자동화 공수 절감

수기·개별 점검 자동화, 소수 인력이 다수 장비 관리

UNIFIED CONSOLE

보안+ 자산+ 자원

세 가지 운영 영역을 하나의 콘솔에서 통합 관리

SCALE

300+ 대 운영

혼합 환경 동일 흐름 일원화

Value · 안전

혼합 환경의 일원화

Windows와 Linux가 섞여도 각각 기본·KISA 점검을 일관되게 수행. 운영 환경이 다르다는 이유로 생기는 사각지대를 제거합니다.

Value · 전문성

엔터프라이즈 운영에 적합한 진단 깊이

자체 보안 기준 + KISA 주요정보통신기반시설 기준 점검을 동시에 제공, 점검 결과를 보고서 형태로 자동 생성합니다.

Value · 신뢰성

안전한 운영을 위한 보호 장치

암호화 통신 · 관리자 2차 인증 · 에이전트 자가 보호로 위·변조에 강한 보안 운영 환경을 제공합니다.

Value · 확장

로드맵 : 웹 취약점 점검 고도화

Web 취약점 진단 모듈을 순차 확장, 오늘의 점검 범위에서 내일의 점검 범위까지 자연스럽게 이어집니다.