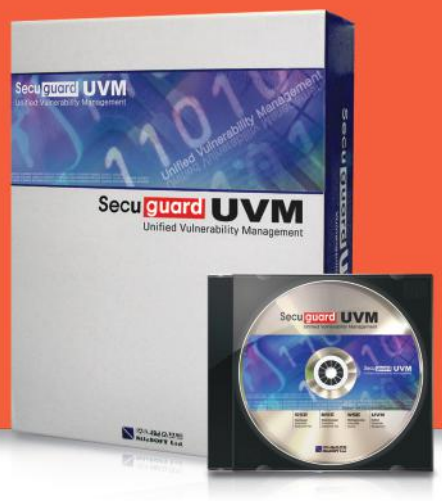
Secuguard UVM

Unified Vulnerability Management system

통합 보안취약점 관리시스템

Secuguard UVM (Unified Vulnerability Management system)은 취약점 점검도구 (호스트 스캐너, 네트워크 스캐너, 웹 스캐너, PC 스캐너 등)와 연계하여 취약점 점검결과를 공유하여 체계적인 취약점 분석업무 체계를 구축합니다. 따라서 전체 및 서버 별 취약점 현황의 일괄 파악을 통한 수준 상시 모니터링과 취약점 분석 및 조치에 대한 현황관리를 할 수 있으며, 고유의 분석 대응 기술을 축적하고 관련자료를 확보하여 보안취약점 분석 및 대응 기술의 상시 적용 및 운영이 가능합니다. 취약점 점검도구의 단순한 운영으로부터 탈피하여 획기적으로 향상된 관리적 취약점분석 업무체계를 구축할 수 있습니다. 담당자의 잦은 교체에 따른 업무 공백과 관련 기술 축적의 어려움 등에 대한 효율적인 대안이 될 수 있습니다.



UVM 상세특징

편리한 사용자 인터페이스
직관적이고 한글화된 사용자 인터페이스

체계적인 자산관리 가능
기업 내 시스템, 네트워크 장비 및 PC 등의 자산을 체계적으로 관리

사용자 이용에 관한 보안 강화
다양한 사용자 권한설정 기능
(수퍼 관리자, 그룹 관리자, 장비 관리자, 일반 사용자)

취약점관련 정보 센터 운영
기술문의, 보안공지, 업데이트정보, 기술자료, 취약점업무절차, 취약점정보 등 제공

보안취약점 관리업무의 중앙 집중화
보안취약점 점검, 조치, 결과의 조회를 중앙에서 수행, 관리 및 통제

보안취약점 점검도구와 연계운영
호스트 점검도구(SSE), 네트워크 점검도구(NSE), 웹 점검도구(WSE), 개인 PC 점검도구(mySSE) 및 타사 취약점 점검도구와 연계운영

효율적이고 편리한 그룹관리
절대그룹(한개 그룹 소속) 및 가상그룹(다수 그룹 소속) 기능

원격 취약점 점검도구 콘솔운영
웹 GUI 상에서 사전 정의된 취약점 점검도구의 원격 콘솔을 수행

mySSE에 의한 개인 PC 취약점 점검 (선택)
UVM을 통해 자신의 PC에 있는 취약점들을 점검, 결과 조회, 발견된 취약점의 조치방안

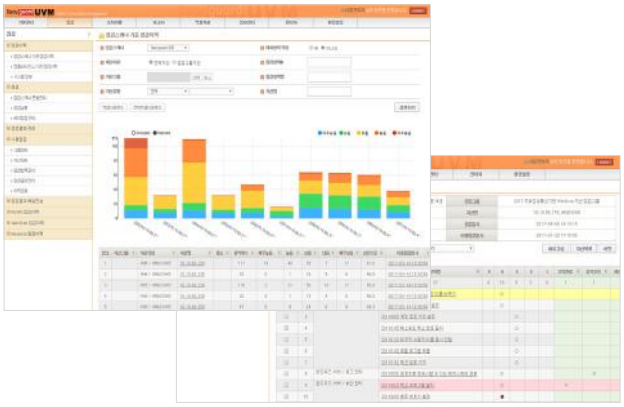
다양한 관리적 통계수치 자동 산출
기간별 최다 취약점항목(TOP 10), 최다 취약점 장비 등 다양한 조건별 통계 검색기능

보안취약점 관리업무의 워크플로우 운영
점검요청, 결과조회, 조치요청, 조치이행, 취약점문의 및 답변처리 업무운영

UVM 실행화면 및 보고서

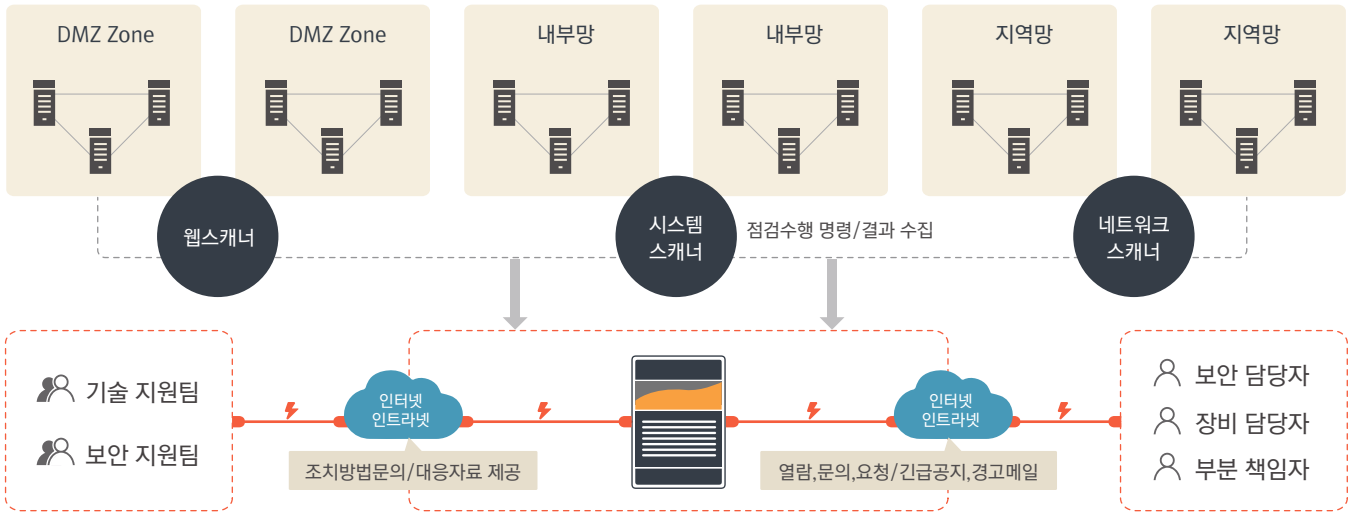
▲ 실행화면 메인

▲ 자산 관리



▲ 조치이행 조회

UVM 구성



기술 지원	주요 기능		업무 내용
	점검이력	· 점검결과조회	· 취약점 분석결과(이력) · 취약점 상세조치내역 검색
	점검통계	· 취약점TOP 10, 최다취약점, 중요취약점 등 · 서버별 취약점추이, 다양한 조건별 통계검색 등	· 취약점 분석통계 검색 · 취약점 조건별통계 검색
메일 접수 및 대응	조치이행	· 조치이행 실적조회	· 기간에 따른 조치 이행 실적조회 · 취약점 조치 및 추가 내역 상세조회
	보 고 서	· 서버별, 기간별, 에이전트별 각종 보고서 · 보고서 설정	· 취약점보고서 검색 및 출력 · 보고서 Export
	환경설정	· 사용자관리, 그룹관리, 장비관리 · 중요취약점, 제외취약점 설정	· 사용자 권한설정, 장비조회 및 그룹핑 · 중요취약점, 제외취약점 설정
취약점 업데이트 공지 관련 자료 수집 및 제공	정보센터	· 기술문의, 보안공지 업데이트 정보, 기술자료 · 취약점 업무절차, 취약점정보, 취약점이란?	· 각종 기술문의 및 게시판 검색 · 취약점 점검 업무 절차열람
	원격점검	· 시스템 및 네트워크 취약점 분석도구 원격 점검	· 통합관리시스템에서 직접 콘솔 운영 가능 · 지역에 관계업시 콘솔운영 가능

UVM 기능 및 구성

구분	설명	구분	설명
취약점 점검수행	· 호스트 점검도구(SSE), 네트워크 점검도구(NSE), 웹서버 및 응용프로그램 점검도구(WSE), 개인 PC 점검도구(mySSE)를 이용하여 취약점 점검 수행	취약점 정보센터	· 보안 공지사항, 취약점 조치문의, FAQ,업데이트정보, 기술자료 공유, 자유게시판, 취약점 업무절차, 취약점 정보
취약점 점검이력	· 점검장비, 점검이력, 취약점 별로 순번, Agent, IP, 운영체제, 총점검개수, 취약개수, 안전개수, 위험도, 최근 점검일시, 취약점 목록, 취약점 설명 등의 정보 검색	원격진단 콘솔	· 호스트 점검도구(SSE), 네트워크 점검도구(NSE), 웹서버 및 응용 프로그램 점검도구 (WSE) 콘솔을 원격에서 수행 · 타사 취약점 점검도구 연계가능
취약점 점검통계	· 전체, 그룹 별, 운영체제 별, 장비 별 점검통계(취약점 개수 변동 현황, 위험지수 변동 현황, 위험도별 취약점 개수 변동 현황, 취약점 점검대상 장비 현황, 취약점 현황, 위험도별 취약점 현황, 취약점 점검 횟수 현황, 최다취약점 발견장비, 최다취약점 증감장비, 최다취약점항목, 미점검 장비, 미업데이트 장비)	취약점 보고서	· 점검결과 요약, 위험도, 장비 별 취약점 목록, 장비 위험도별 취약점 목록, 점검항목별 취약점 목록, 점검항목별 조치결과표, 기간별 통계 보고서, 취약점 분포 통계보고서, 장비 별 취약점 내용, 위험도별 취약점 내용, 장비 취약점 항목별 상세보고서, 장비 위험도별 상세 보고서, 위험도 취약점 취약점 보고서보고서 등
취약점 조치이행	· 취약점 분석대상, 취약점 점검, 조치이행, 조치여부 확인 등 생명주기를 수용 전체, 그룹 별, 장비 별로 기간 및 위험도에 따라 조치이행 여부조회 및 조치내역 관리	메일발송, 업데이트 및 온라인 도움말	· 점검 결과 메일 공지 기능 · 제품 업데이트, 취약점DB 업데이트 · 전체기능에 대해 친절하고 상세한 온라인 도움말
환경설정	· 사용자관리, 그룹관리, 장비관리, 콘솔관리, 사용자정보변경, 패스워드변경, SMTP설정, 보고서LOGO, 취약점DB 업데이트, 취약점 위험도 관리	제외취약점 중요취약점 관리	· 점검이력, 조치이행, 점검통계, 보고서에 적용가능

NileSOFT
서울시 구로구 구로동 디지털로 32길 30, 코오롱디지털타워 빌란트1차 1004호
TEL. 02-783-0961 FAX. 02-783-0963 e-mail. nileman@nilesoft.co.kr
www.nilesoft.co.kr
정보보호의 대중화! 나일소프트가 함께 하겠습니다