

보안취약성 분석! 무엇으로 하시겠습니까?

SecuGuard SSE

보안의 첫 걸음!

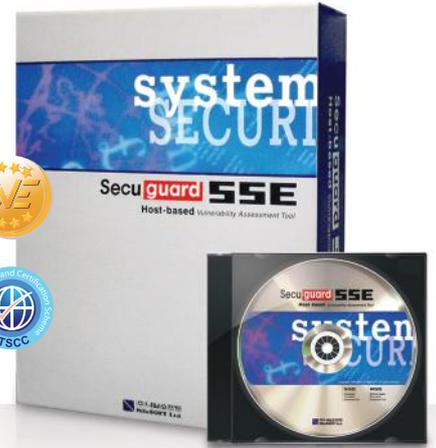
Secuguard SSE로 점검하십시오!

국내기술로 개발된 시스템 취약점 점검도구 SSE는 컴퓨터 시스템들의 다양한 보안 취약점들에 대해서 자동으로 진단하고 발견된 문제들에 대한 해결 방법을 제공하여 해킹과 컴퓨터 범죄들로부터 보호하고 예방할 수 있는 보안 소프트웨어 솔루션입니다.

국내 최초의 CVE 인증마크 획득
CVE(Common Vulnerability Exposure)



CC인증획득
CC인증 EAL2등급 획득
CC(Common Criteria)



SSE 상세 특징

✓ 국내 최초로 CEV Compatibility 인증 획득

· 국제 보안취약점 표준화 단체 MITRE로부터 보안취약점 표준을 준수하는 제품에만 인증하는 CVE(Common Vulnerability Exposure) 인증 획득

✓ 편리한 사용자 인터페이스

· 직관적이고 한글화된 윈도우 탐색기 형태의 사용자 인터페이스
· 모든 기능에 대해 친절하고 자세한 온라인 도움말 제공
· 쉽게 확인되는 점검이력, 진행상황 및 점검결과 보고서

✓ 빠르고 강력한 보안취약점 점검

· Knowledge Base를 이용하여 점검 모듈간 정보공유로 점검시간 대폭 단축
· 강력하고 다양한 패스워드 크래킹 기능
· 개별점검, 일괄점검 및 서버 그룹점검 등 다양한 점검방법 제공
· 운영체제의 보안취약점은 물론 사용자 설정에 의한 보안취약점도 완벽하게 점검
· 운영체제의 중요한 파일들에 대한 접근과 변경을 점검
· 발견된 보안취약점의 위험수준, 내용, 영향 및 조치방안을 제시

✓ 보안취약점 관리의 중앙 집중화

· 하나의 콘솔 운영화면에서 분산된 여러 서버에 대한 보안취약점 점검을 동시에 수행
· 여러 대의 서버에 대해 동시에 보안취약점 점검을 수행하므로 점검시간을 대폭 단축

✓ 상세한 취약점 정보 제공

· 취약점 데이터베이스를 기반으로 다양한 형태의 취약점 정보 제공
· 취약점 그룹별, 운영체제별, 위험도별 취약점 정보 제공

✓ 다양한 운영체제를 지원

· Unixware, Solaris, HP-UX, AIX, Tru64, Linux 등 모든 유닉스계열 운영체제 지원
· Windows 2000, Windows 2003, Windows 2008, Windows 7 등 윈도우계열 운영체제 지원

✓ 온라인 및 오프라인 자동 업데이트

· 최신 콘솔 모듈, 점검 모듈 및 취약점 데이터베이스를 인터넷을 통해 자동 업데이트
· 폐쇄망 사용자를 위한 오프라인 업데이트 기능 제공

✓ 다양한 보고서

· 취약점 목록보고서, 위험도별 취약점 분포 보고서 등 14종 이상의 다양한 보고서
· Crystal Report를 이용하여 작성된 다양한 그래프 및 표 형태 보고서
· HTML, Word, Excel 파일 및 PDF 등 다양한 파일형식으로의 보고서 변환기능 제공

✓ 다양한 부가 기능 제공

· 예약점검 기능
· 점검결과 E-mail 전송 기능
· 에이전트 가동상태의 실시간 모니터링 기능
· 자체 보안팀 운영으로 지속적인 최신 점검모듈 제공
· 취약점 정보 링크 기능
· 서버의 패치 적용여부 점검 기능
· ESM과 연동 기능
· 그룹별 Agent 관리기능
· 보고서 제외취약점 설정기능

✓ 간편한 설치와 손쉬운 확장

· 하나의 콘솔에 서버와 에이전트 설치로 간편
· 부하 분산을 위해 다중 콘솔 운영 가능

✓ 통신 및 자료의 암호화 처리로 보안 강화

· 콘솔과 서버 간의 통신 메시지를 암호화 처리하여 내용이 유출되어도 안전
· 인증된 콘솔과 사용자만이 취약점 점검 실행 및 내용 조회 가능

✓ IPv4 및 IPv6 지원

· IPv4 및 차세대 인터넷체계주소 IPv6 지원

SSE 기대 효과



보안사고 예방활동에 필요

주기적으로 운영중인 정보시스템의 보안 취약점 분석을 통하여 사고를 예방하기 위한 활동을 할 수 있습니다.



보안수준 향상을 기대

수많은 보안취약점을 취약점 분석도구를 통해 이해할 수 있으며, 이를 관리 정책 등에 반영하여 보안 수준 향상을 기대 할 수 있습니다.



보안수준 평가 도구

원하는 시점에서 현재 정보시스템의 보안상태를 파악 할 수 있으며 이를 기반으로 정보시스템의 안전한 운영을 도모 할 수 있습니다.



재해(안전) 대책

평소 보안 취약점 분석 및 조치를 통하여 침입차단, 침입 탐지 시스템의 장애 시 피해를 최소화 할 수 있습니다.

SSE 실행화면 및 기능

▲ 점검진행화면

▲ 온라인 오프라인 업데이트

트리형식으로 에이전트 서버 점검항목을 관리
· 서버별로 별도의 점검항목 관리
· 복수 개의 서버를 동시에 관리

색으로 구별되는 취약성 수준

취약점 점검결과 요약 정보

취약점 영향 정보

취약점에 대한 조치방안 및 대응책 제시

참조 링크 표시

▲ 점검항목 편집 기능

▲ 항목별 점검 및 예약점검 기능

SSE 구조도 및 점검항목



UNIX/Linux 계열 점검항목	Windows 계열 점검항목
<ul style="list-style-type: none"> · Password 관련 취약점 · X Windows 관련 취약점 · FTP 취약점 · 유틸리티 취약점 · 파일 시스템 취약점 · DB 취약점 · 데몬 취약점 · RPC 취약점 · WWW/HTTP와 CGI 취약점 · DNS/BIND 관련 취약점 · 원격접속 명령어 취약점 · 패킷 관련 취약점 · Port 취약점 · NIS/NIS+ 취약점 · 특정 파일 취약점 · 관리자 및 사용자 환경 취약점 · SMTP와 Mail 관련 취약점 · Firewalls/Filters/Proxies 취약점 · 네트워크에 관련된 명령 취약점 · Backdoors 취약점 	<ul style="list-style-type: none"> · Password 관련 취약점 · 패킷 관련 취약점 · DB 취약점 · 특정 파일 취약점 · 기타 서버 서비스 취약점 · 응용 프로그램 취약점 · Registry 취약점 · WWW/HTTP와 CGI 취약점 · SMTP와 Mail 관련 취약점 · Backdoors 취약점 · Internet Explorer 취약점 · 관리자 및 사용자 환경 취약점 · 기타 응용프로그램 취약점 · Exchange server 취약점 · Firewalls/Filters/Proxies 취약점 · Internet Information Server 취약점

SSE 다양한 보고서

▲ 요약 보고서

▲ 상세 보고서