보안 취약점 진단 솔루션

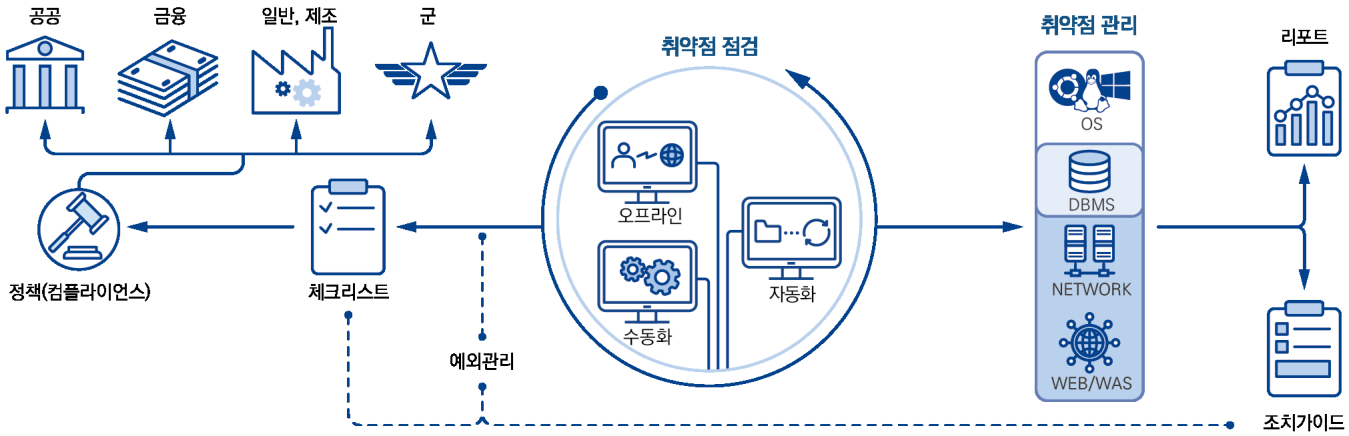
Vulnerability Assessment Management Solution

SecuMS

GS1등급

나라장터 국가종합전자조달

SecuMS는 인프라 시스템 보안 취약점을 자동으로 점검하고 발견된 문제들에 대한 해결 방법을 제공합니다. 또한 취약점 현황을 일괄 파악하여 보안 수준을 높이고 상시 모니터링을 지원하는 보안 취약점 진단 솔루션입니다.



Overview

취약점 관리 범위 확대

- 감독기관이 요구 하는 취약점 점검 항목의 추가 대응
- OS, DBMS, WEB/WAS, NW 등 관리 시스템의 증가
- 신규 취약점의 지속적인 발생

통합 관리 필요성 대두

- 다양한 플렛폼 및 신규버전으로 관리범위 증가
- IT 인프라 장비의 상시 취약점 점검 및 이력관리 미흡
- 감독기관의 '금융 IT 자율체계 및 상시 감시체계 강화' 요구

대내외 정보보안 위협의 증가

- 개인 정보 유출 등 취약점 사고의 증가
- 자산 및 취약점의 증가로 지속적 관리와 보안 위협에 대한 꾸준한 대응 필요
- 오픈SSL의 HeartBleed, 랜섬웨어, 스피어 피싱 등 보안 이슈

법률 및 규제 요구사항 준수 및 감사 대응 필요

- 非 금융 전산시스템까지 취약점 점검·보안관제 확대 (금융 전산 보안강화 종합대책)
- 정기적으로 기술적 취약점 점검을 수행하고 발견된 취약점들은 조치 (정보보호관리체계 ISMS)
- 주요정보통신기반시설에 대한 취약점 분석·평가를 매년 실시

SecuMS 기대효과

1일 보안진단 체제 구현 → 진단 프로세스 개선 → IT보안 지수화 → 보안감사 안정적 경영활동 → 보안 생활화

LSware 엘에스웨어(주) 08504 서울특별시 금천구 서부샛길 606 대성디폴리스 A동 18층 TEL +82-2-6919-0321 FAX +82-2-6919-0329

SecuMS 주요기능

취약점 점검

- 국내/외 컴플라이언스 기준 만족
- 정기적인 취약점 자동 점검
- 수동·포터블(오프라인) 점검
- 사용자 정의 스크립트 지원

예외 관리

- 진단 항목 예외 설정
- 예외 현황 및 이력 제공
- 개별/일괄 예외 적용
- 예외 기간 만료 시 재 탐지

취약점 관리

- 취약점 관리 프로세스 제공
- 취약점 조치 내용 및 결과 확인
- 조치 이행 이력 관리
- 점검수행 히스토리 제공
- 취약점 등급 변경 및 설정 지원

보고서

- 상세 보고서 제공
- 취약점 현황에 대한 일일 보고서 제공
- 취약점 변화 추이 및 통계 자료 제공
- 리포팅 툴을 활용한 보고서 제공
- 포터블(오프라인) 점검 시 대상시스템에서 자체 리포트 생성 기능 제공

SecuMS 특장점

Consulting

- 산업 별 규제에 따른 Checklist 반영(금융, 공공, 기업, 군 기관 등)
- 기존 고객사 보안 정책 유지 및 필수 정책 업데이트
- 과학기술정보통신부, 금융보안원 등 취약점 점검 기준 반영

Process

- 결재시스템·메일시스템·RMS·ESM 등 과의 연동 지원
- 취약점 진단 프로세스의 시스템화로 업무의 효율성 향상
- 커스터마이징을 통한 맞춤형 고객 지원

Safety

- 리소스 제어 기능으로 시스템 영향을 최소화
- 서버 부하 및 장애를 방지할 수 있는 매커니즘 적용
- 대형 인프라 환경에서 검증된 안정성

Different

- 중복 설정이 가능한 다중 스케줄링 기능 제공
- 취약점 조치 이력관리 기능 제공
- 취약점 점검의 예외 기간 설정 기능 지원
- 한글화된 상세 조치 가이드 제공

핵심 요소와 법규, 지침 매핑

핵심요소	주요 인증지침
전자금융거래법	- 제 21조의 3(전자금융기반시설의 취약점 분석·평가) ① 금융회사 및 전자 금융 업자는 전자 금융 거래의 안전성과 신뢰성을 확보하기 위하여 전자 금융 기반시설에 대한 다음 각 호의 사항을 분석·평가 하고 그 결과를 금융위원회에 보고하여야 한다. 4 ②금융회사 및 전자 금융 업자는 제1항에 따른 전자금융기반시설의 취약점 분석·평가 결과에 따른 필요한 보완조치의 이행계획을 수립·시행하여야 한다.
금융 전산 보안 강화 종합 대책	- CEO 책임하에 취약점 점검 및 보완조치 이행 철저 취약점 점검 결과에 대한 이행절차 마련 등 취약점 보완조치를 철저히 이행토록 제도 마련 - 非 금융 전산시스템까지 취약점 점검·보안관제 확대 전자금융기반시설 이외의 교육·홍보용 홈페이지, 그룹웨어 등 내부 업무 지원 시스템에 대해 취약점 점검 의무화
주요정보통신 기반시설 보호지침	- 제 13조(취약점 분석·평가) ① 관리기관의 장은 법 제9조에 따라 소관 주요정보통신기반시설에 대한 최초 취약점 분석·평가를 실시한 때에는 1년을 주기로 실시하여야 한다. ③ 관리기관의 장은 법 제9조제4항에 따른 취약점 분석·평가에 관한 기준을 고려하여 취약점 분석·평가의 대상, 기간, 절차, 방법, 소요예산 편성 및 집행 등 취약점 분석·평가를 구체적으로 시행하기 위하여 필요한 계획을 수립·시행하여야 한다.
정보보호 관리체계 ISMS	- 정보통신망의 안전성 확보를 위하여 수립·운영하고 있는 기술적·물리적 보호조치 등 종합적인 관리체계에 대한 인증제도 - 제 18조의 11(운영보안) 정보시스템이 알려진 취약점에 노출되어 있는 지 여부를 확인하기 위하여 정기적으로 기술적 취약점 점검을 수행하고 발견된 취약점들은 조치하여야 한다.

※ 관련 법적 근거

금융위원회 「전자금융거래법」, 「금융 전산 보안 강화 종합 대책」 **과학기술정보통신부**(전 미래창조과학부) 「주요정보통신 기반시설 보호지침」, 「정보보호 관리체계 인증 등에 관한 고시」