삼성SDS

보안관제 수준진단

보안관제 체계 진단을 통한 보안관제 수준진단 및 고도화 컨설팅

필요성

보안관제 체계진단의 필요성

웹해킹, 웹쉘, DDoS, 악성코드, APT 등에 대한 위협 지속 증가
침해사고 대응 메뉴얼 등 운영 프로세스 수립 필요
보안위협 대응을 위한 보안관제체계 고도화 및 개선 모델 수립 필요

서비스 개념

검증된 보안관제 진단 Framework를 통해 기 구축된 또는 신규 구축 보안관제 아키텍처에 대한 수준 진단 및 개선 지원 서비스

주요 특징

삼성고유 보안관제 수준진단 서비스

- 관제정책, 조직역량, 관제프로세스, 관제플랫폼 4개영역, 8개 도메인으로 구성된 SMCI[1] 기반 보안관제 아키텍처 체계진단

현장 실사 중심의 수준진단 및 문제점 도출

- 실무자 인터뷰, 로그 샘플링 분석, 보안장비 운영 실사 등을 통한 보안관제 주요 기능별 미흡 사항 도출
- 보안관제 프로세스맵, 보안관제 영역별 구축시 고려사항 등 개선안 제시

목표 수준 정의 및 가이드라인 제시

- 개선안에 따른 세부 목표 및 실행과제 리스트 제시
- 개선과제 이행 경과 점검 및 지원

[1] SMCI (Security Monitoring & Control Index): 국제표준 및 삼성 노하우가 집약된 보안관제 수준 진단 지표

주요 서비스

보안관제 아키텍처 수준진단

관제정책, 수행조직/역량, 운영 프로세스 등 상세 현황파악
보안로그 분석 미흡으로 인한 미탐지 해킹 흔적 유무 조사

보안관제 개선안 수립

Best Practice 대비 Gap 분석 및 도메인간 균형도 분석
구현 용이성, 효과성, 연관성을 고려하여 개선 과제 우선순위 도출

보안관제 역량 전달

방화벽, 침입방지, DDoS, 좀비PC차단 등 기본과정 제공
보안관제의 역할, 이벤트 로그분석, 영역별 모의훈련 등 심화과정 제공

현황 분석	보안관제 진단	개선방안 수립	전문가 Advisory
보안관제 규정/지침	영역별 실사 및 인터뷰	보안시스템 개선방안 • 보안솔루션 • 보안관제 시스템	개선방안 이행점검
관제 Rule	탐지 누락분석	보안관제체계 개선방안 • 정보흐름 분석 • 예상 취약점 도출 • 점검방식 결정	관제 운영 가이드
보안 시스템 로그	보안관제 모의훈련		관제 전문가 양성 교육

기대효과

현 보안관제 수준의 객관적 평가

정책관리, 탐지 Rule 관리, 사고대응 등 도메인간 균형도 및 도메인별 Gap 분석

최적의 보안관제 체계 구성

인력, 역량, 관제 프로세스, 관제 플랫폼 등 TO-BE 모델 제시

신규 보안위협 선제적 대응

최신 침해 공격에 대한 탐지룰 및 대응 프로세스 보유