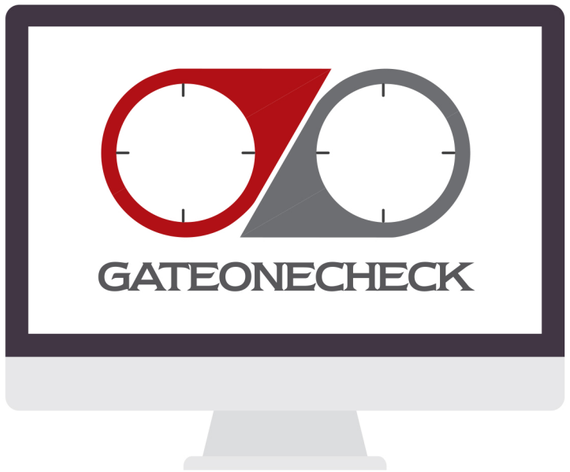
어디에도 Agent가 설치되지 않는 완벽한

“Agent-less”



GATEONE-CHECK는 설정된 보안 취약점 점검 사항을 주기적으로 확인하고 그 결과를 관리자에게 보고서 형식으로 제공합니다. 또한, 수집된 결과를 토대로 취약점 발견 시 해당 시스템 담당자에게 통보하여 취약점 발생 부분의 보안 조치를 필수적으로 수행하고 그 수행 여부를 관리자에게 보고하여, 정보 시스템의 보안 취약점이 발생하지 않도록 관리합니다.

주기 또는 즉시 점검 항목 발생 → 컨설팅 업체 의뢰 → 스크립트 작성 등의 대기 시간 발생 → 결과 보고서 대기

GATEONE-CHECK 의 필요성과 기대효과

필요성

정보 시스템을 구축하고 있는 업체의 경우 보안의 한 부분으로 보안 취약점 검사를 필수로 인지하고 있으며, 현재 대부분 업체의 경우 외부 컨설팅 업체를 통해 짧게는 분기별로 자사의 정보 시스템 취약점 검사를 의뢰합니다. 내부 보안 관리자가 아닌 외부 업체에 의존하여 진행하므로 시간과 비용의 문제가 발생하며 자동화된 분석 Tool이 아닌 스크립트 방식에 의존하여 즉각적인 대처가 어려운 문제점 을 가지고 있습니다.

기대효과

자동화된 보안 취약점 점검 솔루션으로 각 장비에 대한 보안 취약점을 파악하고 예방 관리 함으로써, 위험한 보안 사고 예방 및 해킹 방지, 침해 사고 최소화 등의 안정적이며 효율적인 보안 관리가 기대됩니다.

관리자 맞춤 통계

수행 결과 보고를 통한 각종 통계 자료를 토대로 관리 정보 시스템의 보안 취약점 사전 점검 및 취약점 발생을 미연에 방지하여 관리하도록 합니다.

보안은 항상 철저히

평시 운영 중에도 규칙적인 주기로 보안취약점을 확인하여 취약점 발견 시 즉각적인 조치를 수행합니다.

안정적인 시스템

Agent-less 방식으로 정보시스템에 접근함으로써 정보시스템 구성 및 리소스를 사용하지 않고 정보시스템을 안정적으로 운영할 수 있습니다.

강력한 사후 관리

취약점 점검 → 각 시스템 담당자에게 결과 전송
→ 취약점 발생 부분의 보안 조치 → 완료 보고
→ 취약점 보안 조치 결과 확인

GATEONE-CHECK 의 특장점




- **시스템 접근제어**
  - 각 정보 시스템에 대한 접근제어 기능
  - 점검 후 조치 대상 장비에 대한 권한 부여
  - 대상 장비 조치에 대한 로깅 기능
  - 각 정보 시스템의 접근 권한 회수 기능
  - 관리 시스템의 접속시간 부여 기능
- **시스템 별 책임분담**
  - 업무 플로우 기능 제공
  - 시스템 담당자 설정 기능
  - 담당자 그룹 별 시스템 설정 기능
  - 취약점 점검 결과의 관리자 및 담당자 알림 기능
  - 취약점 문제 발견 시 조치 후 보고 기능
  - 관리자에 의한 담당자 조치 확인 기능
- **취약점 분석 자동화**
  - 항목에 맞는 취약점 항목 업데이트 기능
  - 시스템에 적용하기 위한 취약점 그룹관리
  - 주기 설정 기능
  - 취약점 즉시 확인 기능
  - 취약점 점검 후 보고서 수신기능 (메일, 메시지)
  - 취약점 발견 시 가이드 기능
- **로그 및 감사**
  - 취약점 점검 후 결과 리포트
  - 분기별 또는 설정 주기 별 통계 기능
  - 패치 대상 장비의 접속 로그 조회 기능
  - 다양한 형태의 분석 리포트 제공