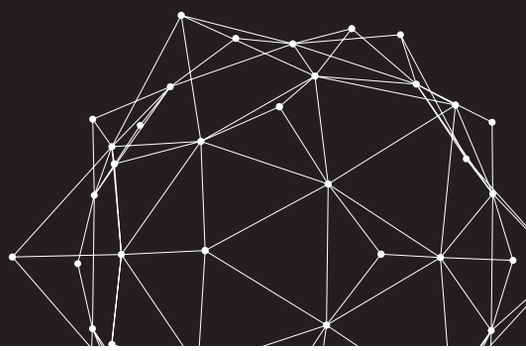
CYBERONE
주 식 회 사 · 싸 이 버 원

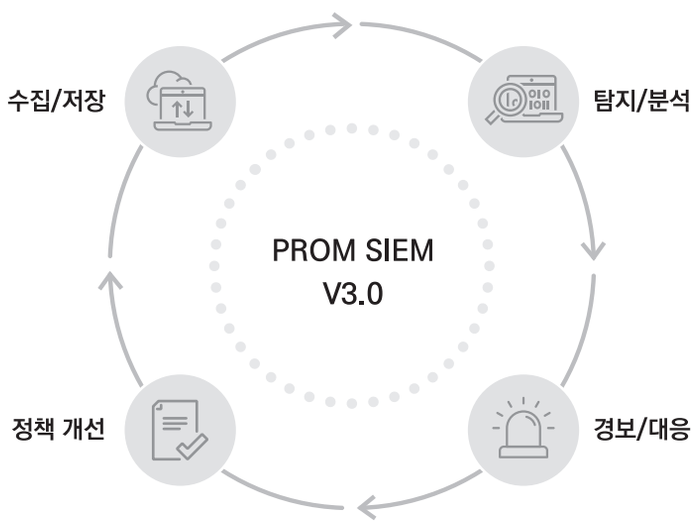
보안정보 및 이벤트 관리 시스템

PROM SIEM V3.0



제품 개요

PROM SIEM V3.0은 기업이 보안 경고를 효과적으로 모니터링하고, 분석하며, 대응할 수 있도록 설계된 중요한 보안 제품입니다. PROM SIEM V3.0은 다양한 IT 자산 및 보안 데이터를 수집하고 분석하여 실시간으로 보안 위협을 탐지하고 경고하는 역할을 합니다. PROM SIEM V3.0은 조직의 IT 인프라를 보호하는데 필수적인 역할을 하며, 복잡한 보안 환경에서의 위협 관리를 단순화합니다.



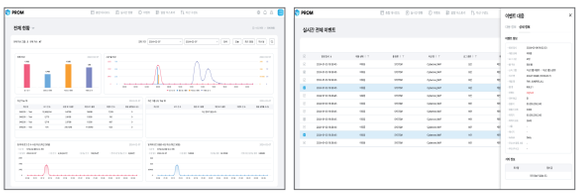
특장점

최적화된 통합 보안 관리	· 이기종 보안 시스템 및 IT 자산 통합관리 · 정형/비정형 데이터 관리
CEP 분석 및 빅데이터 처리	· 실시간 이벤트 탐지 · NoSQL 적용한 빅데이터 처리
사용자 중심의 UI	· 사용자 정의 대시보드 · 복잡한 쿼리가 아닌 UI 기반 로그 검색
효율적인 로그 관리	· 70% 이상 로그 압축 · 로그 수집부터 삭제까지 로그 라이프 관리

주요 기능

실시간 이벤트 탐지

- In-Memory 기반의 실시간 이벤트 탐지 엔진 적용
- 시나리오 기반 상관 이벤트 탐지

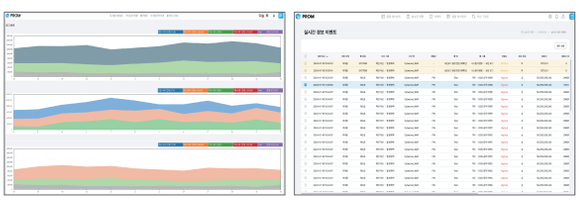


위협 분석 대시보드 제공

- 공격유형 기반의 보안 위협현황
- GeoIP 기반의 공격 맵
- 고객환경에 맞는 대시보드 제공

다양한 분석 기능

- 추이차트/단일분석/복합분석
- 시계열 분석 기능



도입 효과

PROM SIEM은 싸이버원의 축적된 관제 경험을 바탕으로 특화된 관제 서비스를 제공하기 위해 만들어진 제품이며 최적화된 기능 체계를 제공합니다. PROM SIEM의 도입으로 사이버 보안 위협에 신속하게 대응하고, 조직의 사이버 보안 태세를 종합적으로 강화할 수 있습니다.

위협탐지 및 대응

- 보안 이벤트와 로그 데이터를 실시간으로 수집하고 분석
- 알려진 위협뿐만 아니라 비정상적인 행동 패턴을 식별하여 미리 위협을 탐지

준법 및 규정준수

- SIEM을 통해 필요한 로그를 자동으로 수집, 보관하여 감사 준비 지원으로 규정 준수 가능
- 보안 사고 발생 시 SIEM을 통한 로그 및 기록을 기반으로 사고 조사 및 보고 과정 간소화

비용 절감

- SIEM을 통한 효과적인 위협 탐지 및 대응을 통한 비용 절감 가능
- 자동화와 효율성 향상으로 인력 비용과 기타 관련 비용 절감 효과

효율적인 보안 운영

- 자동화된 경보 및 보고 기능을 통한 수동 작업량 감소
- 다양한 대시보드를 통한 가시성 제공으로 즉각적인 상황 인식

CYBERONE
주 식 회 사 · 싸 이 버 원
서울시 서초구 효령로 39 (방배동, 싸이버원 빌딩) TEL. 02-3475-4900 www.cyberone.kr