통합 보안관제 솔루션 Splunk

기업의 정보자산을 효과적으로 보호하고 보안 사고에 신속하게 대응할 수 있습니다.

▪ Splunk 솔루션의 장점

주요 이슈를 사전에 예방

Splunk는 디지털 전반의 가시성을 확보하고 위험을 사전에 감지하고 해결합니다.

82%
다운타임 감소

위협과 중단을 더 빠르게 해결

사고 우선순위와 표준 워크플로로 탐지와 대응 시간을 단축하고 영향을 최소화합니다.

80%
더 빠른 평균 수정 시간

새로운 기회를 위한 빠른 적응

포괄적인 가시성을 통해 위험을 최소화하고 환경 변화와 의존성을 이해합니다.

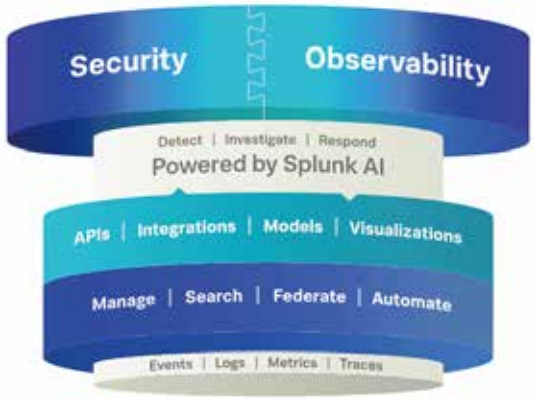
50%
새로운 앱의 출시시간 단축

통합 보안 및 관찰 플랫폼

업계 최고의 보안 및 관측 가능성 솔루션을 제공

Security
통합 위협 탐지, 조사 및 대응을 통해 SOC를 고도화하세요.

Splunk Platform
대규모 실시간 모니터링, 조사 및 대응이 가능합니다.

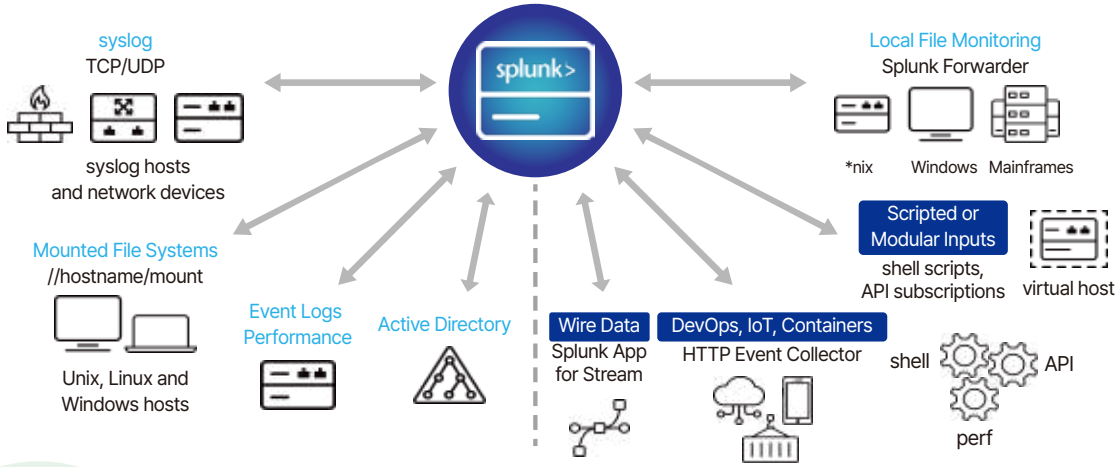


Observability
IT 인적 자원을 최적화하고, 문제를 더 빠르게 해결하세요.

Splunk AI
감지, 조사 및 대응을 가속화하기 위한 인간 참여형 AI입니다.

다양한 이기종 데이터 소스로부터 제약 없는 수집

에이전트 / 에이전트리스 방식 제공으로 유연성과 최적화된 수집 기능 제공



통합 보안관제 솔루션 Splunk

Splunk는 구축형에서부터 클라우드까지 전반에 걸친 솔루션을 보유하고 있습니다.

▪ Splunk Solution 포트폴리오

핵심 플랫폼(Splunk Cloud/Enterprise)을 중심으로 각 사용 사례에 맞는 패키지 솔루션 구성

Splunk Cloud/Enterprise
모든 데이터를 자유롭게 수집, 저장, 분석, 시각화할 수 있는 데이터 플랫폼 서비스입니다.

Data Stream Processor
다양한 데이터 소스와의 연결성과 실시간 데이터 분석 및 배포를 실현하는 스트리밍 플랫폼입니다.

The Splunk Platform

Splunk AI
맞춤형 AI 모델 및 워크플로우 구축, 배포

- **AI Assistant** — 자연어로 SPL 자동 생성
- **AI Toolkit (AITK)** — 머신러닝 기반 이상 탐지, 예측
- **Data Science Deep Learning(DSDL)** — 딥러닝 모델 플랫폼 통합

Observability (DevOps)

- **Synthetic / Real User Monitoring(RUM)** — 최종 사용자가 경험하는 서비스 성능 모니터링, 분석 (디지털 경험 모니터링)
- **Application Performance Monitoring(APM)** — 마이크로 서비스 환경의 트랜잭션을 추적하고 코드 레벨 병목 현상을 분석
- **Infrastructure Monitoring** — 클라우드 네이티브에 특화된 기반 기술의 성능을 모니터링, 분석
- **Log Observer Connect** — 간단한 조작으로 성능 장애와 관련된 모든 로그 분석
- **Splunk On-Call** — 여러 역할이 관련된 팀의 인시던트 대응 효율성
- **OT Intelligence** — 산업 현장 및 제조 설비의 실시간 가시성 확보

IT Operation

- **IT Service Intelligence(ITSI)** — 고급 모니터링 및 분석 알고리즘으로 운영 고도화를 실현하는 차세대 AIOps 플랫폼
- **ContentPacks** — IT 시스템을 구성하는 다양한 기술 요소에 대한 포괄적인 모니터링 기능을 제공하는 확장 기능
- **Splunk On-Call** — 여러 역할이 관련된 팀의 인시던트 대응 효율성

Security

- **Enterprise Security** — 강력한 상관 엔진과 리스크 기반 스코어링 알고리즘을 구현하는 SIEM 플랫폼의 결정판
- **User Behavior Analytics** — 고급 및 정교한 머신러닝 알고리즘을 통한 내부 위협 탐지 엔진
- **Splunk SOAR** — 인시던트 응답과 관련된 조치, 분석 및 조사를 자동화하고 관련 도구를 오케스트레이션
- **TruSTAR(Intel Management)** — 여러 위협 인텔리전스를 통합하고 탐지된 이벤트에 대한 고급 의미를 제공하는 TI 플랫폼
- **Mission Control** — 보안 운영의 통합 인터페이스를 제공하는 플랫폼
- **OT Security** — ICS/SCADA 등의 산업 제어 시스템 보안 위협을 실시간 탐지

IT Operation

IT 서비스 인텔리전스

AI 기반 사고 예측, 감지 및 해결을 한 곳에서 모두 수행

- 서비스 중심 대시보드
- 서비스 심층 분석
- 예측 경보
- 자동화된 이벤트 집계
- KPI 기반 분류 보기
- ITSM과의 통합

OT Intelligence

운영 기술 인텔리전스

산업 현장의 OT 데이터 실시간 가시화 및 보안 체계 구축

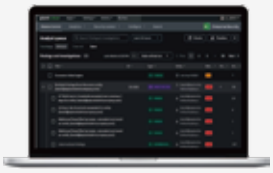
- 산업 설비(ICS/SCADA)와 IT 인프라 데이터를 통합 모니터링
- AI 기반 이상 징후 탐지로 예기치 못한 설비 가동 중단 예방 및 공정 최적화
- OT 전용 프로토콜 분석을 통한 비정상 제어 명령 실시간 탐지 및 위협 대응
- 네트워크 내 연결된 모든 OT 자산의 실시간 식별 및 리스크 관리 자동화

Security

Enterprise Security

분석 중심의 보안운영 솔루션으로 주요 보안 Use Case 제공

- 검증된 SIEM 솔루션
- 안정적이고 확장 가능한 아키텍쳐
- 효율적인 보안 관제 체계
- Advanced 위협탐지 및분석을 위한추가기능
- 신속한 공격 탐지 및 대응



Splunk UBA(User Behavior Analytics)

머신러닝을 통해 알려지지 않은 위협 및 비정상적인 사용자 행동 탐지

- 알려지지 않은 위협과 숨겨진 위협을 탐지 비지도 학습ML을 사용
- 임계치 설정, 룰 생성, 커스텀의 불필요 신속한 공격 탐지 및 대응
- 조사 가속화

SOAR(Security Orchestration, Automation and Response)

OODA[Observe(관찰), Orient(상황판단), Decide(의사결정), Act(실행)] Loop를 통한 빠른 실행으로 보안 향상

- 반복 작업 자동화를 통한 스마트한 업무 환경
- 이벤트 조사, 대응 절차 자동화를 통해 보안 이벤트 대응 속도 개선
- 기존의 보안 인프라(SIEM)와 통합

Mission Control

하나의 현대적인 인터페이스에서 위협을 탐지, 조사하고 대응

- 위협 탐지, 조사 및 대응 기능 통합
- 보안 워크플로우 간소화
- 현대화 및 보안 운영 강화

ITCEN CTS (구 콤텍시스템)

보안 사고 예방, ITCEN CTS와 상의하세요.

안정적인 재무 건전성, Splunk의 보안 솔루션, 보안 전문 인력을 보유하고 있는 ITCEN CTS와 상의하세요.

사이버 공격 기법의 진화로 이를 탐지하거나 대응하기 어렵습니까?
다양한 보안 솔루션과 데이터를 통합 관리하기 어려우십니까?
방대한 보안 관제 데이터를 수집, 저장, 분석하기 어려우십니까?
보안관제 인력이 부족하여 효과적인 보안 관제 운영이 어려우십니까?
보안관제 프로세스가 복잡하고 비체계적인 경우가 많아 신속하게 대응하기 어려우십니까?

ITCEN CTS

(주)아이티센씨티에스 www.itcencts.com
TEL. 02-3289-0114 **EMAIL.** junlee@itcen.com
경기도 과천시 과천대로 12길 117 E동 아이티센빌딩

Splunk + AI

SOC의 자율화: Agentic AI

보안 알림 평가부터
위협 분석 및 대응까지
스스로 판단하고 실행하여
보안 운영의 속도와
자동화 수준을 극대화

Splunk AI Assistant

자연어 기반의 다단계
추론과 검색 쿼리(SPL)
최적화를 통해 복잡한
문법 지식 없이도 신속하고
정밀한 데이터 탐색을 지원

AI 기반 Observability 및 Data Fabric 통합

기업 내 AI 인프라 워크로드를
실시간으로 모니터링하고
머신 데이터를 지능적으로
결합하여 시스템 신뢰성과
사용자 경험을 향상

DSDL* 앱의 RAG 및 LLM 확장

외부 유출 없이 Splunk
내부 환경에서 자체 LLM과
벡터 DB를 구동하여,
안전하고 고도화된 로그 기반
분석 및 RAG 아키텍처 구현

*DSDL:Data Science and Deep Learning

▪ OT Intelligence

splunk>

Manufacturing

- 유지보수 일정 최적화하여 장비 다운타임 최소화
- 보안 사고 및 무단 출입 시도 탐지
- 장비 생산성 측정을 통한 공정 최적화

Logistics

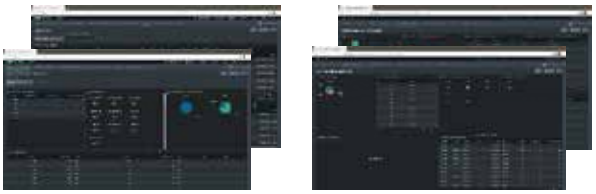
- 실시간 추적으로 경로 최적화
- 정비 주기 예측
- 컨테이너 내 습도 및 온도 측정

Datacenter

- 전력 사용량 측정을 통한 에너지 효율성 증대
- 온도 및 냉각제, 팬 속도 측정을 통한 과열 방
- 전원 상태 측정을 통한 가시성 확보

▪ AICC

AVAYA



CISCO

- CTI 이벤트 캡처
- 실시간 보고서 및 분석 제공
- 포기 및 단기 콜 발신자 식별
- 대기열 고객 및 대기 시간 나열

- 보류 콜의 빈도와 기간 파악
- 먼저 전화를 끊는 상담원 파악