AhnLab
CONNECT PLUS

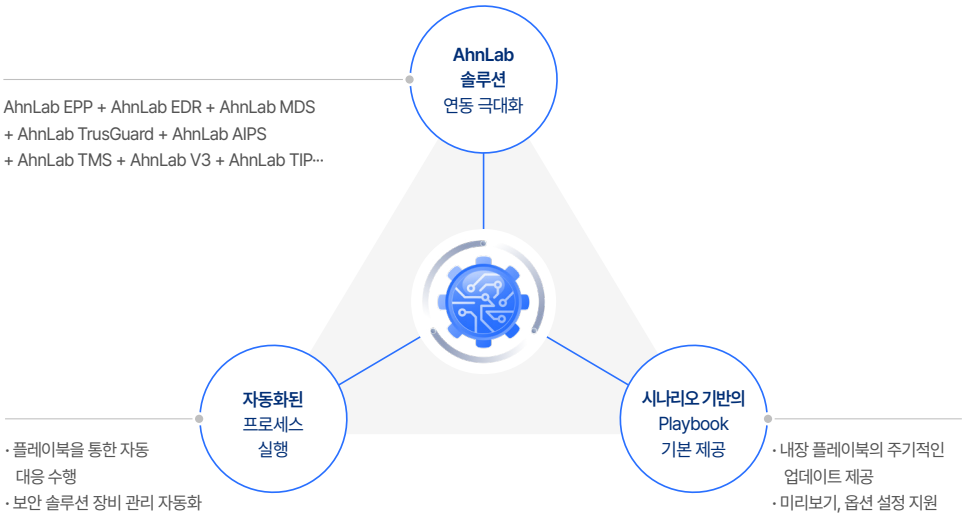
AhnLab SOAR Basic

Streamline Your Security Operations

AhnLab SOAR Basic은 자사 솔루션을 사용하는 환경에서 엔드포인트와 네트워크 영역을
융합하고 연계하여 자동화된 대응 및 운영 자동화 구현할 수 있어 업무 효율성 증대에 기여합니다.

제품 개요

AhnLab SOAR Basic은 안랩 제품 간 연동 및 내장된 전용 플레이북을 통해 위협에 대한 통합 대응 및 운영의 자동화를 구현 할 수 있습니다.이를 통해 IT 현업 업무 부하를 감소시킬 수 있으며, 리스크를 최소화하여 조직의 안정성과 보안성을 강화할 수 있습니다.



주요 기능

AhnLab SOAR Basic은 안랩 솔루션 연계로 통합적이고 자동화된 대응을 제공하는 전용 플레이북(Playbook), 탐지·대응 현황 대시보드, 대응 결과 보고서 등 위협 대응 수준 강화와 업무 자동화를 위한 주요 기능을 제공합니다.

전용 플레이북 제공

AhnLab SOAR Basic은 다양한 시나리오에 대응하기 위해 사전에 정의된 플레이북을 제공하고 있습니다. 이를 활용하여 보안 인시던트에 대한 신속하고 정확한 대응 절차를 실행할 수 있으며, 플레이북의 미리보기와 옵션 설정을 지원합니다.

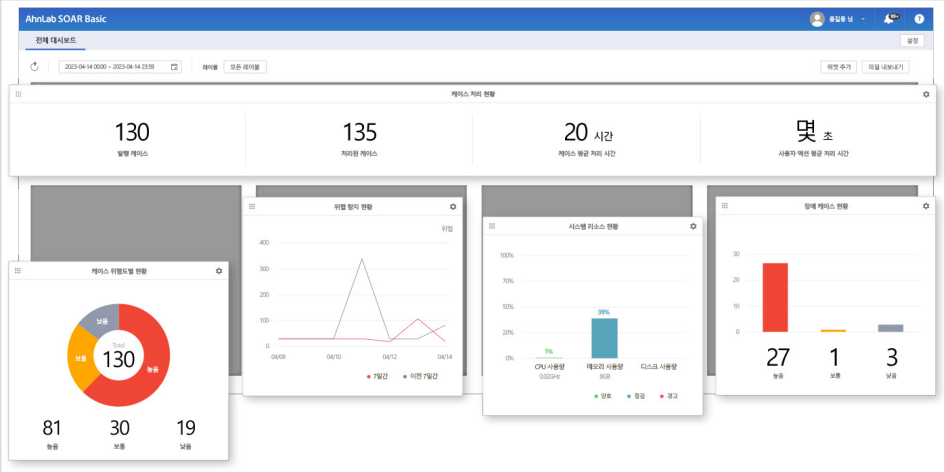
구분	Playbook 명	활용 솔루션	시나리오 개요
위협 대응	이상 트래픽 발생 호스트 탐지 및 차단	TG + TMS + MDS + EDR	대상 단말에서 발생하는 이상 트래픽 원인 분석 및 재발 방지
	의심되는 APT 공격 대응	V3 + EPP + TG + EDR + MDS	APT로 의심되는 공격에 대한 근거 데이터 분석
	유해 사이트 접근 탐지	AIPS/TG + V3 + ESA + EPM + EPrM + EDR	유해사이트 접속 단말에 대한 자동 대응
	외부 위협 정보의 조직 대응 현황 관리	TI + MDS + EDR	수집된 IOC 정보를 활용하여 조직 대응 현황 관리
	내부서버 접근 취약 호스트 관리 1, 2, 3	EDR + ESA + TG	중요 서버에 접근하는 대상 단말의 취약점 관리
	AIPS 탐지한 공격자 대응 1, 2	AIPS + TIP + TG + V3 + EDR	AIPS에서 탐지된 Top5 공격자에 대한 대응
보안 강화	피싱 사이트 자동 대응	MDS + TG + V3	타겟형 피싱사이트 자동 대응
운영 관리	악성코드 감염대응	V3 + EDR (TG)	악성코드에 감염된 단말에 대한 자동 대응
	보안 취약점 대응	EPM + EDR (TG)	대상 단말에 대한 보안 취약점 패치 관리
	네트워크 침입 대응	V3 + EDR (TG)	네트워크 침입이 발생 시 단말의 PC상태 점검
	개인정보 유출 대응 1, 2	EPRM + V3	개인정보 유출이 의심되는 상황에 대한 대응
	PC 보안 점검에 따른 취약 사용자 대응 1, 2, 3	ESA	단말의 보안 점검 및 취약점 관리
	보안 수준 평가에 따른 취약 사용자 대응 1, 2	ESA	단말의 보안 수준평가 관리
	장기 미접속자 확인	V3	장기 미 접속 단말에 관리
	V3 업데이트 장기 미 실행자 관리	V3	V3 엔진 업데이트 장기 미실행자에 대한 자동 조치

* (예시) AhnLab SOAR Basic에서 지원하는 플레이북 일부 내역 발췌

주요 기능

탐지 대응 현황 대시보드

AhnLab SOAR Basic은 조직내 발생한 케이스에 대한 다양한 현황 정보를 제공합니다. 이를 통해 관리자는 한눈에 보안 상황을 파악할 수 있습니다. 특히, 위젯 형태로 제공하기 때문에 사용자의 선택에 따라 유연한 구성이 가능합니다.



다양한 보고서 지원

AhnLab SOAR Basic은 각각의 플레이북 별로 편집이 가능한 형태의 결과 보고서를 제공하여 상세한 분석과 의사 결정을 지원합니다.

특장점 및 기대 효과

AhnLab SOAR Basic은 별도의 SIEM 구축이 필요 없는 설치형 자동화 플랫폼이므로 구축 및 유지 보수 비용을 절감할 수 있습니다. 또한 안랩 솔루션 전용 플레이북으로 위협에 대한 통합 대응 역량과 보안담당자의 업무 효율성을 높여주는 것이 특징입니다.

특장점

- 별도의 구축 과정이 없는 설치형 자동화 플랫폼
- 안랩 제품들을 활용한 다양한 시나리오 기반의 전용 플레이북 탑재
- 콘텐츠 팩을(플레이북, app, adapter, 보고서 등) 통한 다양한 업데이트 제공

기대 효과

- 안랩 제품간 연계 연동을 통한 다층적 통합 대응 가능
- 자동으로 실행되는 플레이북을 통한 대응 품질 향상
- 자동화를 통해 업무의 효율성 증대

SOAR vs. AhnLab SOAR Basic

SOAR(Security Orchestration, Automation and Response, 보안 오케스트레이션·자동화·대응)는 보안 운영 시 유입되는 다양한 보안위협에 대해 대응 수준을 자동으로 분류하고, 표준화된 업무 프로세스에 따라 사람과 기계가 유기적으로 협력할 수 있도록 지원하는 플랫폼입니다. 전통적인 SOAR는 써드파트(3rd Party) 솔루션 연계하여 운영 업무의 자동화와 표준화를 지원합니다. 이에 비해 AhnLab SOAR Basic은 안랩 솔루션만 있다면 간단한 설치와 저렴한 가격으로 손쉽게 사용할 수 있습니다.

전통적인 SOAR	구분	AhnLab SOAR Basic
구축형 (3 - 6개월 소요)	도입 방식	**설치형**
SIEM 또는 ESM 필요	연동 방식	**안랩의 솔루션**
3rd Party 솔루션 지원 하지만 개발 필요 할 수 있음	연동 App	**안랩의 솔루션**
기존 대응 프로세스 분석 후 사용자 또는 벤더 지원 형태의 구현 필요	플레이북 구현	**사전 정의된 시나리오 기반 플레이북 제공**
지원	플레이북 편집	**지원 X**
사용자 또는 벤더 지원 형태의 관리 필요	플레이북 업데이트	**콘텐츠 업데이트 방식**
고가의 도입 비용	도입 비용	**구독형, 월과금 형태의 과금 지불 방식**

운영 환경

구분	내용
운영 체제	Linux Rocky OS 8.7
CPU	Intel Xeon 6 Core
RAM	32GB 또는 이상
HDD	960GB 이상

경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901

AhnLab