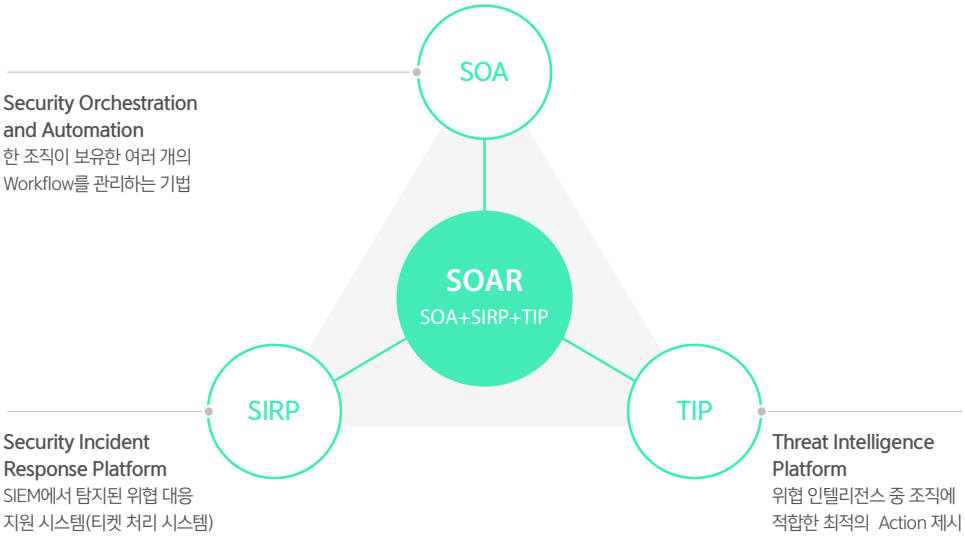
AhnLab SOAR

Automate your Tasks, Orchestrate your Response

AhnLab SOAR는 보안운영 및 위협 대응 분야에서
오랜 기간 축적된 안랩의 기술력과 노하우로 보안 오케스트레이션, 자동화를 구현한 대응 플랫폼입니다.

왜 SOAR인가?

지능적이고 고도화되는 위협으로 인해 증가하는 이벤트와 보안장비는 단순 반복적인 업무의 증가 및 처리자에 따른 대응 품질 차이를 발생시켰습니다. 이러한 문제점을 개선하기 위해 Gartner는 표준화된 업무 프로세스에 따라 사람과 기계의 유기적인 협력을 지원하는 SOAR라는 대응 플랫폼을 정의하였습니다.
AhnLab SOAR는 국내 최초로 SOAR 개념을 도입한 대응 플랫폼으로 분석, 대응, 운영 등의 업무 프로세스에 대한 가시성을 확보하고 자동화와 오케스트레이션을 통한 업무 표준화와 유기적인 대응을 가능하게 합니다.



핵심 기능

- 다양한 솔루션 연동을 통해 대응 프로세스의 효율성을 높여주는 오케스트레이션
- 체계적인 대응 및 보안운영 프로세스 구축을 통한 업무 생산성 향상
- 반복적으로 행해지는 태스크의 자동화
- 다양한 보안 솔루션 및 업무 시스템과의 연동 지원
- 보안 전문가간의 협업 및 커뮤니케이션
- 재사용 가능한 Playbook

특장점

AhnLab SOAR는 다년간 누적된 자사 위협 대응 프로세스를 Playbook 형태로 표준화하여 처리자의 업무 능력에 따른 품질 차이를 최소화시켜 대응 품질을 일관되게 유지하고, 국내외 솔루션과의 연동을 통해 운영 업무의 자동화와 표준화까지 확장할 수 있습니다.

안랩의 보안운영 및 위협 대응 노하우

- 다년간 누적된 안랩의 위협 대응 시나리오를 기반으로 제작된 다양한 Playbook 제공
- 표준 Playbook 제공 및 고객사 업무에 맞는 Playbook 재생산 가능

다양한 솔루션과의 효율적 연동

- 보안 오케스트레이션 구현을 위한 다양한 3rd Party 연동 지원
- 기존 도입된 안랩 보안 솔루션과의 유기적 연동으로 위협 대응의 시너지 향상

머신러닝 기반 분석 모듈 ASA

- 위협 요소 자동 식별 및 식별된 위협에 대한 자동화된 추론
- 유사 위협의 그룹핑, 정오탐 분석 자동화로 분석가의 의사 결정에 도움

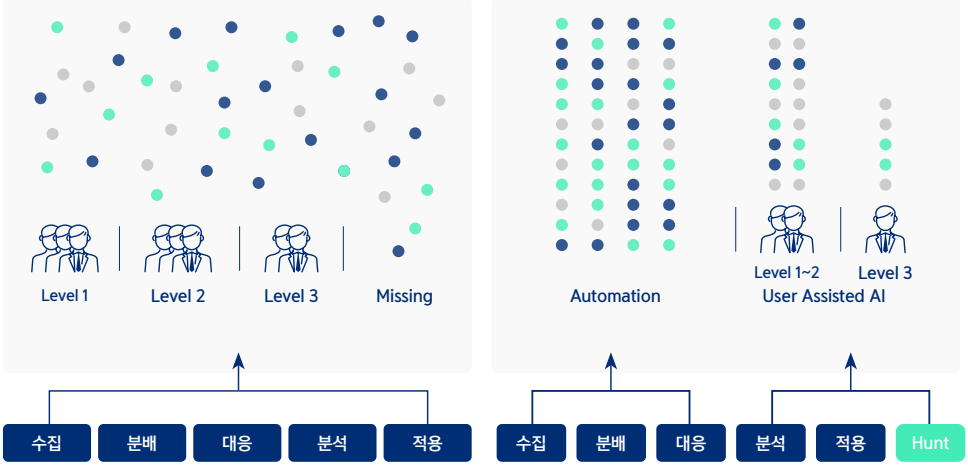
* ASA(AhnLab SOAR AI)는 머신러닝 기반 데이터 분석 엔진으로서 별도 판매 제품입니다.

도입 효과

AhnLab SOAR는 사람에 의해 수동으로 처리되던 단순 반복적인 태스크를 자동화하여 각 Case에 대한 선별 및 대응을 즉각적으로 수행하고 Playbook 기반의 표준화된 대응 체계로 대응 품질을 상향 평준화할 수 있습니다.

또한, 다양한 솔루션 연동으로 통합적이고 유기적인 대응이 실현되어 단순 반복 업무에 대부분 할애되던 업무 시간을 위협 분석과 같은 보다 **전문적이고 가치가 높은 업무에 투자**할 수 있습니다.

기존의 대응 업무	AhnLab SOAR를 이용한 대응 업무
· 긴 대응 시간 · 불규칙적인 대응 품질 · 프로세스 가시성 부족 · 대부분의 인력이 단순 반복 업무에 투입	· 대응 시간 단축 및 신속한 의사 결정 · 대응 품질의 상향 평준화 · 프로세스 가시성 확보 · 사람의 판단이 필요한 분석 업무 등 전문 업무 투입

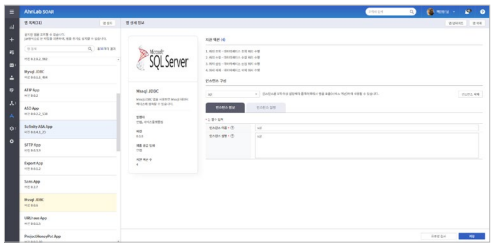


주요 기능

AhnLab SOAR는 표준화된 Playbook 및 자유로운 편집 기능을 제공하며, 다양한 솔루션과의 연동으로 오케스트레이션 개념을 업무에 도입할 수 있습니다. 또한 프로세스 자동화와 머신러닝 기반 분석 모듈을 통해 위협 요소를 자동 식별하고, 식별된 요소로 위협을 추론하여 대응 업무의 효율성을 향상시킬 수 있습니다.

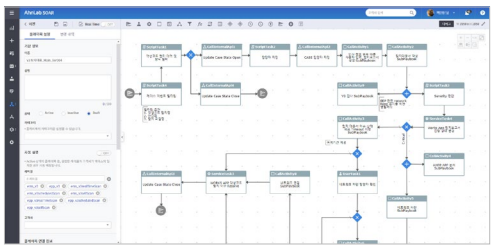
· Multi Task in Single View
· 안랩의 보안운영 및 위협 대응 전문 기업의 기술력이 응집된 SOAR 플랫폼

Orchestration



· 하나의 대응 프로세스에 속해 있는 각 Task의 조율
· 다양한 솔루션과의 연동

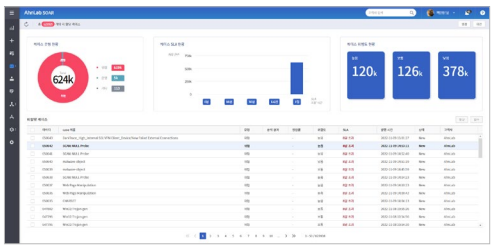
Automation



· Built-in Play book 제공 및 Playbook 제작 지원
· Script 엔진을 이용한 유연한 자동화 액션 지원
· Playbook Simulator 지원 추가

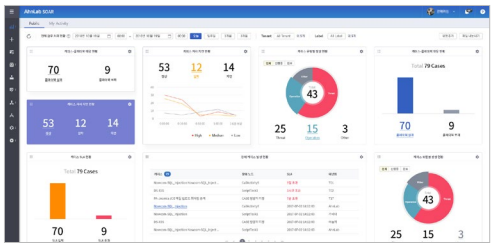
* Playbook은 특정 작업 절차에 속한 개별 업무 단위를 선별하고 태스크로 정의하여 태스크 간의 흐름, 처리 시점, 사용자나 시스템의 개입 여부 등을 정의한 표준화된 작업 절차입니다.

Case Management



· 대응 내역 및 의사결정에 대한 관리 및 근무자 간의 협업 지원
· 위협 대응, 보안 운영, 업무 요청 및 지원 등 유형별 Case 생성 및 관리

Dashboard



· 공용 및 개인 대시보드 지원
–공용 대시보드: 조회 기간 내 선택된 위젯의 정보
–개인 대시보드: 계정 별 조회 조건 내 수행 내역 정보

운영 환경

구분	권장 사양
운영 체제	Linux CentOS 7 이상
지원 브라우저	Chrome
CPU	Intel Xeon CPU E5-2630 x 2 이상
메모리	128 GB 이상
인터페이스	10/100/1000 Base-T x 2
RAID	기본 구성(RAID 5)
HDD 용량	기본형 2 TB(2 TB x 2) 이상

* 권장 사양은 고객사의 환경에 따라 달라질 수 있으므로, 자세한 내용은 개별 상담을 권장합니다.

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

AhnLab