AhnLab

White Paper

# AhnLab SOAR Basic으로 구현하는 보안 운영 최적화

위협의 고도화로 통합 보안의 중요성 증대
대응 역량 강화, 운영 자동화 고민하는 기업 늘고 있어

## 개요

SOAR(Security Orchestration, Automation and Response) 플랫폼은 보안 운영 시 유입되는 다양한 보안 위협에 대해 대응 수준을 자동으로 분류하고, 표준화된 업무 프로세스에 따라 사람과 기계가 유기적으로 협력할 수 있도록 지원하는 솔루션을 의미한다.

AhnLab SOAR Basic은 ▲안랩 솔루션 연계로 자동화된 대응을 지원하는 전용 '플레이북(Playbook)' ▲탐지·대응 현황 대시보드 ▲대응 결과 보고서 등의 기능을 제공하는 안랩 솔루션 전용 SOAR 플랫폼이다. 이번 백서에서는 AhnLab SOAR Basic의 기능과 특장점, 구체적인 활용 방안을 살펴본다.

## AhnLab SOAR Basic의 주요 기능 및 특징

AhnLab SOAR Basic은 안랩 솔루션 전용 플레이북을 통해 위협에 대한 통합 대응 역량과 보안 담당자의 업무 효율성을 높인 점이 특징이다. 여기서 플레이북은 다년간 축적된 안랩의 위협 대응 시나리오를 기반으로 위협 종류, 상황 별 통합 대응 프로세스를 표준화한 일종의 대응 절차서로 이해하면 된다.

일반적으로 위협이 탐지되면 보안 담당자가 분석/알림/네트워크 차단 등의 복잡한 대응 절차를 개별적으로 실행해야 한다. 하지만 AhnLab SOAR Basic을 이용하면 내장된 플레이북이 사전에 정의한 '위협 대응', '보안 강화', '운영 관리' 등 목적별 시나리오에 따라 안랩의

AhnLab SOAR Basic의 핵심:
안랩의 다양한
엔드포인트·네트워크 보안
솔루션 연계를 통한 위협 대응
수준 강화 및 보안 관리 부담
최소화 달성

엔드포인트와 네트워크 보안 솔루션의 다양한 기능을 연계해 통합적이고 자동화된 대응이 가능하다.


[그림 1] AhnLab SOAR Basic 개념도

안랩은 지속적으로 플레이북을 비롯한 기능 업데이트를 제공해 보안 담당자의 관리 부담도 최소화했다. AhnLab SOAR Basic은 써드파티(3rd party) 보안 솔루션 연계를 위한 구축 과정 없이 안랩 솔루션만 있다면 설치 방식으로 손쉽게 사용할 수 있기 때문에 안랩 제품을 사용하는 고객들은 구축에 소요되는 비용과 시간을 줄일 수 있다.

## AhnLab SOAR Basic과 기존 SOAR의 차이

기존 SOAR 플랫폼의 경우 SIEM(Security Information & Event Management)과의 연계를 바탕으로 이기종 솔루션 간 연동, 프로세스 및 정책 실행, 리포팅 등을 통해 보안 관제 자동화를 구현해왔다. 또한, SOC(Security Operation Center) 조직을 보유한 중대형 공공기관 또는 기업에서 활용하는 것이 일반적이었다.

반면, AhnLab SOAR Basic은 이기종 솔루션 간 연계는 제공하지 않지만, 안랩 솔루션을 사용 중인 고객사 환경에서 엔드포인트와 네트워크 영역을 융합 및 연계해 자동화된 대응과 리포팅 등을 지원한다.

### AhnLab SOAR Basic의 차별점

안랩 제품 간 연계를 통한 실시간 및 자동화된 위협 대응, 최신 위협 시나리오 기반 플레이북 제공으로 보안 업무 효율성 향상

| 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** |

[그림 2] AhnLab SOAR Basic과 기존 SOAR 비교

기존 SOAR 대비 AhnLab SOAR Basic이 갖는 주요 장점은 아래와 같이 3가지 정도로 요약할 수 있다.

① 안랩 제품 간 연계 및 자동화를 통한 실시간 위협 대응 효과
② 설치형으로 쉬운 연동 제공
③ 업데이트 방식의 최신 위협 시나리오 기반 플레이북 제공

## 기본적으로 제공되는 플레이북과 제품 연계 활용 방안

AhnLab SOAR Basic을 통해 기본적으로 제공되는 플레이북은 크게 ▲위협 대응 ▲보안 강화 ▲운영 관리 3가지 카테고리에 걸쳐 총 30여 개의 케이스로 세분화돼 있다.

| 구분 | Playbook명 | 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 |

## AhnLab SOAR Basic 플레이북 기능 (1) : 조직 내부 서버에 접근하는 취약한 단말 탐지 및 조치

| | | | |
|---|---|---|---|
| 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 |

[표 1] AhnLab SOAR Basic 플레이북 케이스 중 일부

[표 1]과 같이 기본적으로 내장되어 있는 30여 개 플레이북 시나리오 중 카테고리 별로 대표적인 사례들을 소개한다. 이를 통해, 실제 환경에서 해당 플레이북들이 어떻게 동작하고 실행되는지 알아보도록 하자.

### 1. 위협 대응 – 내부서버 접근 취약 단말 관리

내부서버 접근 취약 단말 관리 시나리오는 EDR(V3), ESA, TrusGaurd(TG) 제품에 대한 연계 기반으로 구성됐다. 플레이북은 취약한 단말을 대상으로 초기 침투 후 이루어지는 내부 이동(lateral movement)과 취약한 단말이 조직 내부 주요 서버에 접근하는 위협을 사전에 탐지해 경보를 생성하도록 제작됐다.

| 연계 제품 | 시나리오 | 수행 제품 | 수행 항목 | 상세 설명 |
|---|---|---|---|---|
| TG<br>ESA<br>EDR<br>V3 | 내부 주요 서버에 접속하는 단말 중 ESA 점검 점수 미달, 악성코드 감염 이력 존재, EDR 위협 정보 이력이 존재하는 경우 공지사항 발송 후 ESA 점검 및 자동 조치 | TG | 단말 정보 수집 | 내부 주요 서버 접속 단말 중 보안 점검 점수가 낮은 단말, 윈도우 계정 취약점 단말, 악성코드 감염 이력 단말 정보(호스트 명, IP정보) 수집 |
| | | ESA/V3/ EDR | 상세 정보 수집 | ESA 점수 및 보안 점검 결과, 권한 상승, 계정 탈취 EDR이력 정보, 악성코드 감염 이력 등 정보 수집 |
| | | SOAR | 관리자 메일 발송 | 분석 템플릿 생성 후 관리자 대상 메일 발송 |
| | | EPP | 공지사항 보내기 | 사용자에 결과 알림 |
| | | SOAR | 알림 메일 발송 | 관리자에게 알림 메일 발송 / 처리현황 |
| | | EPP/ESA | 공지사항 발송 및 점검 수행 | 사용자 대상 공지사항 발송 및 보안 점검 및 자동 조치 수행 |
| | | TG | 네트워크 격리 | 보안 점검 점수 기준 미달 시 네트워크 격리 / 만족 시 해제 |
| | | SOAR | 보고서 생성 | 처리 결과 리포트 |

[표 2] AhnLab SOAR Basic 플레이북 구동 프로세스 (1)

## AhnLab SOAR Basic 플레이북 기능 (2) :

피싱 사이트 URL 정보 추출, 네트워크 기반 자동 차단을 통한 보안 강화

최근 대다수의 지능형 지속 위협(APT)은 내부이동 과정을 통해 주요 서버에 접근하고, 권한을 탈취해 랜섬웨어를 전사적으로 배포하거나 중요 데이터를 탈취하는 행위를 수행한다. 따라서 취약한 단말에 대한 주요 서버 접근 이력 관리는 위협 대응 관점에서 매우 중요하다. AhnLab SOAR Basic을 활용하면 제품 간 연계를 통해 이를 효과적·효율적으로 구현할 수 있다.

### 2. 보안 강화 – 타겟형 피싱 사이트 자동 대응

타겟형 피싱 사이트 자동 대응 시나리오는 MDS, TrusGuard, V3 제품에 대한 연계 기반으로 구성돼 있다. 플레이북은 악성코드의 초기 침투 유형으로 가장 많이 발생하는 스피어 피싱 메일에 포함된 피싱 사이트 URL 정보를 추출해 네트워크 기반 자동 차단을 수행하도록 제작됐다.

| 연계 제품 | 시나리오 | 수행 제품 | 수행 항목 | 상세 설명 |
|---|---|---|---|---|
| MDS<br>TG<br>V3 | MDS에서 탐지된 피싱 사이트를 TG 및 V3 방화벽 모듈로 차단하고 기존 이력 리포팅 | MDS | 이벤트 트리거 | 메일 본문 또는 첨부 문서에 포함된 URL 분석 결과 중 피싱 URL 진단명 트리거 |
| | | SOAR | 데이터 추출 | 진단 로그 중 피싱 관련 도메인 정보 추출 |
| | | TG | 접속 이력 조회 | 네트워크 접속 로그 중 과거 피싱 사이트 도메인 접속기록 조회 |
| | | V3 | 차단 룰셋 등록 | V3 방화벽 모듈 사용 시 차단 룰셋 자동 등록 |
| | | TG | 차단 룰셋 등록 | TG Blacklist IP 자동 등록 |
| | | SOAR | 보고서 생성 | 처리 결과 리포트 |

[표 3] AhnLab SOAR Basic 플레이북 구동 프로세스 (2)

AhnLab SOAR Basic의 플레이북을 활용하면 위협 정보를 기반으로 네트워크 장비에 차단 정책을 수작업으로 추가할 필요가 없어 업무 효율성이 높아진다. 보안 강화 관점에서도 추가적으로 발생할 수 있는 동일한 공격을 사전에 차단함으로써 견고한 보안 운영 환경을 유지할 수 있다.

### 3. 운영 관리 – PC 보안 점검 취약 사용자 대응

PC 보안 점검 취약 사용자 대응 시나리오는 ESA 제품에 대한 연계 기반으로 구성됐다.

플레이북은 AhnLab ESA를 통한 보안점검 점수 기준 초과, 취약항목 기준 초과, 보안진단 미실행 기간 초과 단말을 선별하여 사용자에게 경고 알림을 보내고 관리자가 처리 현황 리포팅을 자동으로 수행할 수 있도록 제작됐다.

AhnLab SOAR Basic 플레이북 기능 (3) :

보안 규칙을 위배한 단말 및 사용자 대상 경고 발송, 자동 리포팅을 통한 보안 운영 최적화

| 연계 제품 | 시나리오 | 수행 제품 | 수행 항목 | 상세 설명 |
|---|---|---|---|---|
| ESA<br>EPP | ESA 보안 점검 점수 미달 사용자 대상 관리 | ESA | PC 보안 점검 조회 | 메일 본문 또는 첨부 문서에 포함된 URL 분석 결과 중 피싱 URL 진단명 트리거 |
| | | EPP | 공지사항 보내기 | 보안 점검 점수 미달인 단말 PC가 발견되었습니다.<br>보안 점검 취약 항목 다수가 존재하는 단말 PC가 발견되었습니다.<br>'장기간 보안 점검이 미 실행된 단말 PC가 발견되었습니다.' |
| | | ESA | PC보안 점검 실행 | 기준 점수 초과 시 다음 스텝 진행 |
| | | EPP | 공지사항 보내기 | 사용자에 결과 알림 |
| | | SOAR | 알림 메일 발송 | 관리자에게 알림 메일 발송 / 처리현황 |

[표 4] AhnLab SOAR Basic 플레이북 구동 프로세스 (3)

대다수 보안 솔루션은 로그를 확인할 수 있는 콘솔을 제공하는데, 보안 관제를 수행하는 조직을 제외하면 해당 콘솔을 실행한 상태로 업무 시간 내내 모니터링하는 보안 담당자들은 사실상 거의 없다. 하지만 이 플레이북을 활용하면 사람이 실시간 모니터링을 하지 않아도 보안 규칙에 위배되는 단말 및 사용자들에게 자동 경고 알림을 보낸다. 또한, 관리자도 결과에 대해 자동으로 리포팅을 받을 수 있기 때문에 보안 운영 최적화 관점에서 매우 유용하게 활용될 수 있다.

AhnLab SOAR Basic 도입 시 효과 :

· 보안 업무 프로세스 간소화
· 소수의 보안 인력으로 시나리오 기반 실시간 위협 대응

## 맺음말

AhnLab SOAR Basic은 플레이북 시나리오에 대한 지속적인 업데이트를 통해 최신 위협 트렌드를 반영한 위협 대응 역량을 강화하고 고객이 보안을 강화해 나갈 수 있도록 지원할 예정이다.

따라서 전사적인 보안 업무 프로세스를 최적화하거나, 소수의 보안 인력 운영만으로도 안랩 솔루션 간 연계를 통해 다양한 위협에 맞서 시나리오 기반의 실시간 대응을 수행하고자 한다면, AhnLab SOAR Basic을 통해 해당 도전과제를 효과적으로 해결할 수 있을 것으로 기대된다.

AhnLab

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