LOGPRESSO | AhnLab

엔드포인트 위협 대응 자동화

개요

- 안랩 EPP는 안티바이러스와 EDR 통합 관리 기능 제공
- 로그프레소는 안랩 EPP REST API를 통해 엔드포인트 관리 기능을 플랫폼에 통합
- 네트워크 격리 및 해제, 파일 검색, 파일 수집, 안리포트 수집, 바이러스 검사, 노드 목록 조회, 의심 프로세스 행위 내역 조회, 파일 예외 처리, 태스크 관리 지원
- 시나리오 탐지 및 플레이북에 따른 엔드포인트 의심 파일 수집, 자동 격리 및 해제 지원

지원 플랫폼

- 로그프레소 소나
- 로그프레소 마에스트로

연계 제품

- 안랩 EPP 1.0.9.20 이상

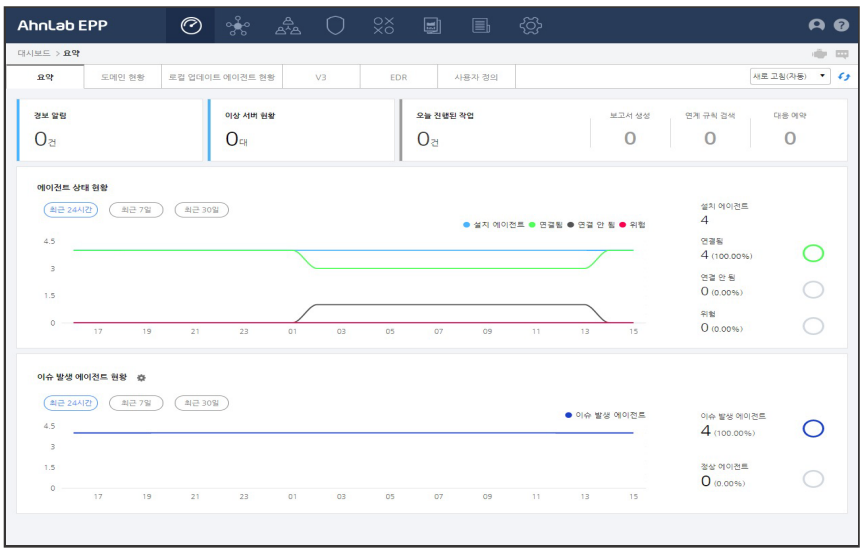
로그프레소 + 안랩 EPP

엔드포인트가 악성코드에 감염되거나 이상 행위를 보이면 보안 담당자는 악성 코드 확보 및 분석, 감염 범위 확인, 악성 코드의 해시값 등록과 같은 차단 조치를 수행하거나, 오탐이 반복되지 않도록 예외 처리 작업을 수행합니다.

이와 같은 과정은 적잖은 시간이 걸리는 반복적인 작업을 포함하고 있음에도 보안 담당자가 직접 EPP 콘솔에 접속하여 대응할 수 밖에 없습니다.

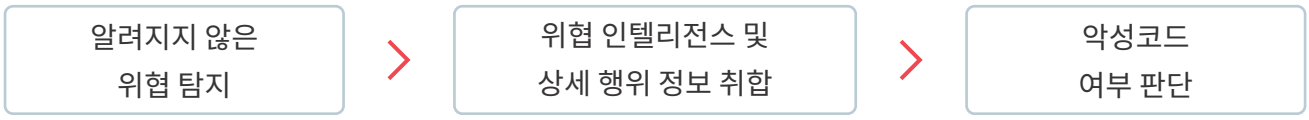
로그프레소 플랫폼은 안랩 EPP에서 제공하는 REST API를 이용하여 엔드포인트 바이러스 검사, 파일 검색, 파일 수집, 네트워크 격리 및 해제, 의심 프로세스의 상세 행위 내역 조회, 관리자 예외 처리를 모두 자동으로 수행할 수 있습니다.

플레이북은 의심 파일에 대한 외부의 위협 인텔리전스 정보까지 취합하여 표시할 수 있으므로, 모든 분석 자료가 준비된 상태에서 보안 담당자가 악성 여부를 판단하기만 하면 차단이나 예외 처리까지 자동화하여 편리한 보안 운영 환경을 구성할 수 있습니다.



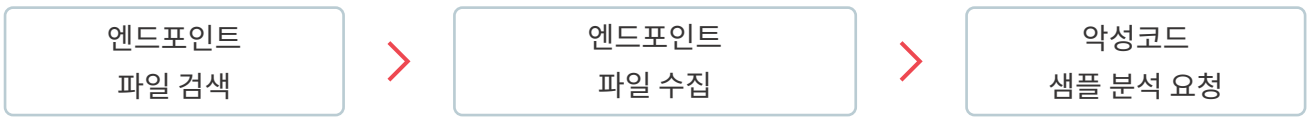
악성코드 정보 자동 취합

지금까지는 알려지지 않은 실행 파일이 발견되면 바이러스토탈과 같은 위협 인텔리전스에 직접 접속하여 해시를 조회하거나, 샌드박스 솔루션에 파일을 업로드하는 등 수작업을 통해 악성 여부 판단에 필요한 정보를 취합해야만 했습니다. 이제 위협 탐지 시점에 분석 정보를 자동으로 취합할 수 있으므로, 가장 중요한 악성 여부 판단만 수행하는 수준으로 업무량을 줄일 수 있습니다.



의심 파일 수집 및 분석 요청

이전에는 직접 엔드포인트에 접속하여 의심 파일을 확보하거나, EPP 콘솔에서 파일 검색 및 수집 명령을 내리고 완료될 때까지 대기해야 했습니다. 이제 파일 검색, 파일 수집, 분석 요청까지 모든 단계를 자동화할 수 있으므로, 불필요한 대기 시간을 제거할 수 있습니다.



19종의 전용 쿼리 확장

로그프레소 플랫폼에서 API를 통해 안랩 EPP 원격 관리를 지원합니다. 다음은 대표적인 명령어들입니다.

명 령 어	기 능
ahnlab-epp-unknowns	알려지지 않은 위협 탐지 목록 조회
ahnlab-epp-unknown-detail	알려지지 않은 위협 탐지 상세 내용 조회
ahnlab-epp-unknown-behaviors	프로세스 실행 및 네트워크 통신 상세 내역 조회
ahnlab-epp-ack-unknown	관리자의 악성 파일 확인 혹은 예외 처리
ahnlab-epp-start-search-file	파일 검색 명령 (파일 이름, 파일 크기 등 조건 지정)
ahnlab-epp-start-collect-file	지정된 파일 수집 명령
ahnlab-epp-start-collect-ahnreport	안리포트 수집 명령
ahnlab-epp-start-v3-scan	V3 악성코드 검사 명령
ahnlab-epp-start-block-network	네트워크 격리 명령
ahnlab-epp-start-unblock-network	네트워크 격리 해제 명령
ahnlab-epp-tasks	엔드포인트 명령 이력 조회

※표에 있는 명령어들은 전체 명령어 중 일부이며 지속적으로 추가됩니다.