LOGPRESSO | TANIUM

엔드포인트 위협 대응 자동화

개요

- 태니엄은 엔드포인트 플랫폼을 기반으로 다수의 모듈화된 보안 관리 기능 제공
- 태니엄 REST API를 통해 엔드포인트 관리 기능을 로그프레소 플랫폼에 통합
- 엔드포인트 센서 쿼리, 파일시스템 탐색, 원격 파일 수집 및 다운로드, 작업 생성, 행위 이벤트 조회 쿼리 지원
- 탐지 시나리오 및 플레이북에 따른 엔드포인트 실시간 쿼리, 의심 파일 수집 지원

로그프레소 + 태니엄

대규모 엔드포인트를 관리하는 환경에서 보안팀의 분석가가 악성코드 감염 등 침해 정황, 내부자의 정보 유출과 같은 조사를 수행할 때 사용자 단말에 직접 접근하는 것은 매우 어렵습니다.

태니엄 플랫폼은 중앙에서 엔드포인트 보안 기능을 배포하고 관리할 수 있게 함으로써 이러한 문제를 해결해줍니다. 태니엄 관리 콘솔에서 모든 엔드포인트 관리 작업을 수행할 수 있을 뿐 아니라, 태니엄 REST API를 이용하면 단순한 업무를 상당수 자동화할 수 있습니다.

로그프레소 플랫폼은 태니엄 콘솔에서 수행하던 엔드포인트 질의뿐만 아니라, 엔드포인트에 대해 프로세스 실행이나 네트워크 통신 등의 행위 이벤트 조회, 파일 시스템 탐색, 증거 파일 수집과 다운로드를 지원합니다.

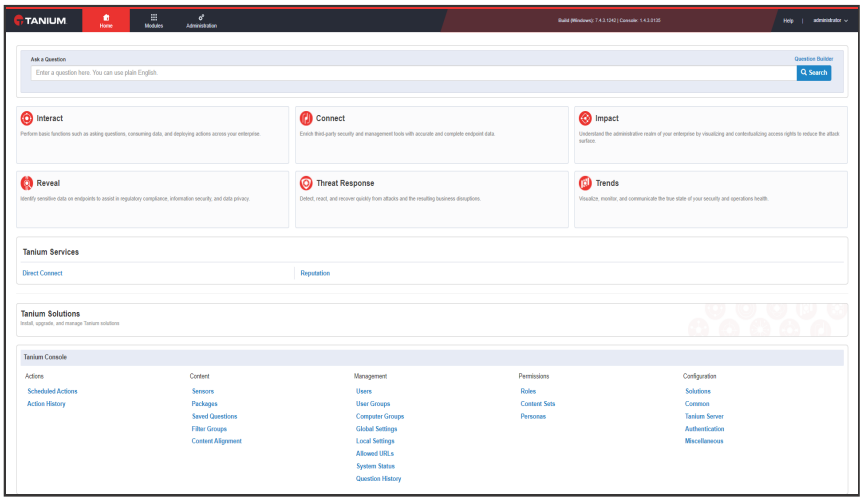
태니엄 플랫폼을 로그프레소가 제공하는 다양한 위협 인텔리전스 및 보안 제품 연동 기능, 플레이북과 통합하여 편리한 보안 운영 환경을 경험해보세요.

지원 플랫폼

- 로그프레소 소나
- 로그프레소 마에스트로

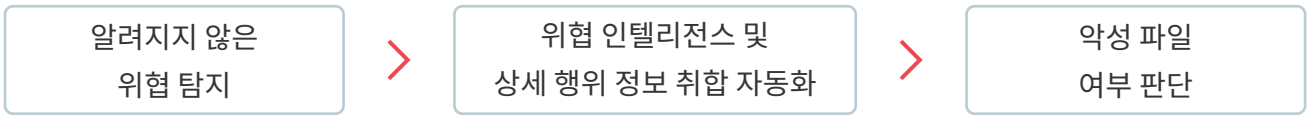
연계 제품

- 태니엄 플랫폼 7.4.3.1242 이상



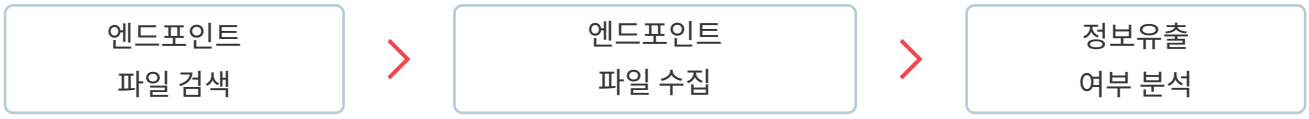
악성코드 정보 자동 취합

알려지지 않은 실행 파일이 발견되면 바이러스토탈과 같은 위협 인텔리전스에서 파일 해시를 조회하거나, 샌드박스 솔루션에 파일을 업로드하는 등 악성 여부를 판단하기 위한 정보를 수작업으로 취합해야 했습니다. 이제 엔드포인트 위협 탐지 시점에 분석 정보를 자동으로 취합할 수 있으므로 악성 여부 판단만 수행하는 수준으로 업무량을 줄일 수 있습니다.



의심 파일 수집 및 분석 요청

엔드포인트에 직접 접근해 의심 파일을 확보하거나 태니엄 콘솔에서 파일을 탐색/수집할 필요없이, 정보 유출 징후가 의심되면 즉시 엔드포인트에서 파일을 수집하여 자동으로 티켓에 첨부하고, 알려진 문서 유형은 내부 정보와 대조하여 정보 유출 여부를 자동으로 분석할 수 있습니다.



17종의 전용 쿼리 확장

로그프레소 플랫폼에서 태니엄 API를 통해 엔드포인트 원격 관리를 지원합니다. 다음은 대표적인 명령어들입니다.

명 령 어	기 능
tanium-question	엔드포인트 센서 질의
tanium-connections	엔드포인트 실시간 연결 목록 조회
tanium-evidences	저장된 증거 파일 목록 조회
tanium-create-evidence	지정된 엔드포인트의 파일 수집
tanium-download-evidence	증거 파일을 로그프레소 서버에 다운로드
tanium-browse-files	엔드포인트 파일 목록 실시간 조회
tanium-process-events	프로세스 실행, 종료 이벤트 조회
tanium-network-events	네트워크 접속, 해제 이벤트 조회
tanium-dns-events	DNS 쿼리 이벤트 조회
tanium-file-events	파일 생성, 기록, 이동, 삭제 이벤트 조회
tanium-registry-events	레지스트리 이벤트 조회
tanium-driver-events	드라이버 이벤트 조회

※표에 있는 명령어들은 전체 명령어 중 일부이며 지속적으로 추가됩니다.