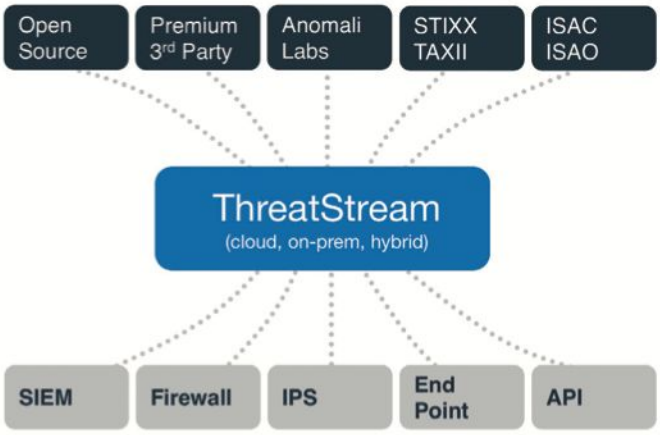
ANOMALI®

ThreatStream

가장 널리 보급된 위협 인텔리전스 플랫폼

위협 인텔리전스 과부하

보안관제실(SOC)의 보안 분석가, 사고 대응팀 그리고 연구원들은 과도하게 많은 양의 위협 데이터에 허덕이고 있다. 포네몬(Ponemon)이 보안 관계자들을 상대로 실시한 조사에 따르면 78%의 응답자가 위협 인텔리전스는 강력한 보안 포스처 운영에 매우 중요하다고 답변했으며 70%의 응답자는 과도하게 많은 위협 정보의 관리가 운영상의 큰 애로점이라고 답변했다.
Anomali는 ThreatStream을 통해 보안팀에게 완전한 위협 인텔리전스를 제공한다. ThreatStream은 위협 정보의 수집, 관리 및 통합에 필요한 모든 절차를 자동화하고 보안 분석가가 필요로 하는 각종 도구와 자원을 적시에 제공하여 활성 위협에 신속하게 대응할 수 있도록 도와준다.



포네몬(Ponemon) 연구 자료:
State of Threat Intelligence:
anomali.com/ponemon

수집(Collect)

ThreatStream은 다양한 원천으로부터 인텔리전스 정보를 수집한다.

- STIX/TAXII 피드
- 오픈소스 위협 피드
- 유료/상용 위협 인텔리전스
- 비정형 인텔리전스: PDF 파일, CSV 포맷, 이메일
- ISAC/ISAO 공유 위협 인텔리전스

관리(Manage)

ThreatStream은 원시 위협 데이터를 강력하고 활용이 용이한 인텔리전스로 변환한다.

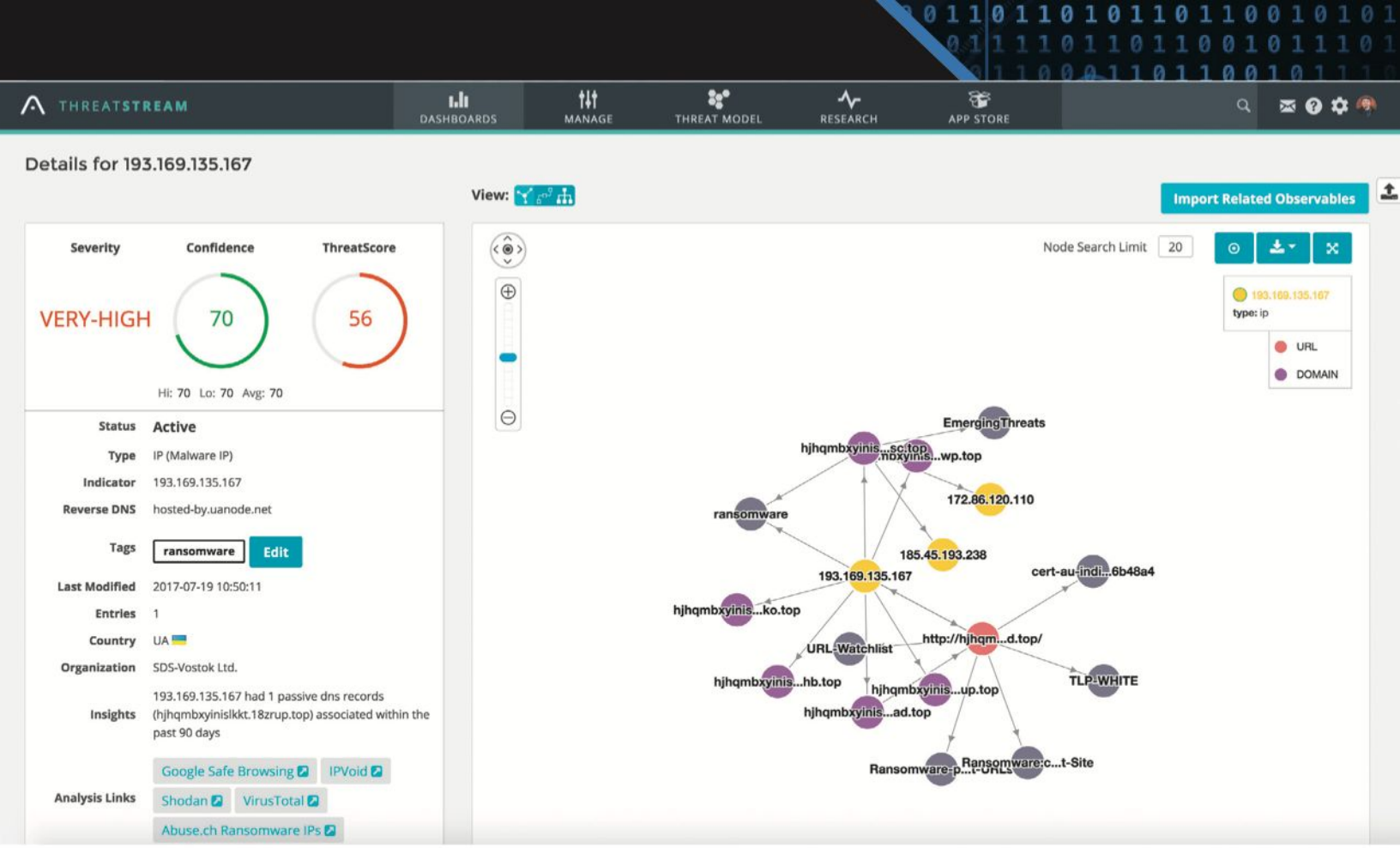
- 수많은 피드의 정규화, 통일된 형식으로 분류
- 중복 데이터의 제거
- 거짓 긍정 정보의 제거
- 액터(Actor), 캠페인, TTP를 이용한 데이터 강화
- 관련 위협 지표와 연결

통합(Integrate)

ThreatStream은 위협 인텔리전스 정보가 즉시 적용될 수 있도록 내부 보안 시스템과 통합한다.

- SIEM, 방화벽, 침입탐지 시스템, 엔드포인드 통합
- 수백만 이상의 보안 지표를 처리할 수 있는 확장 능력
- 기계학습을 통한 위협에 대한 위험 점수 생성
- Anomali Lab을 통한 위협 브리핑 제공
- Trusted Circle과의 안전한 양방향 공유

ANOMALI™
808 Winslow Street, Redwood City, CA 94063 USA
1-844-4-THREATS | info@anomali.com | www.anomali.com



보안 분석가 능력 극대화

Anomali ThreatStream은 보안 분석가의 업무 효율을 극대화하는 각종 도구를 제공하며 그들로 하여금 위협 인텔리전스의 활용 효과를 향상시킬 수 있게 도와주며 분석가 친화적인 다음과 같은 기능들을 제공한다.

- 내장 샌드박스를 통한 의심스러운 파일 조사
- 위협 지표를 사이버 액터 연결
- 상황 인지 정보: WHOIS, PassiveDNS 등 제공
- 분석 워크플로우를 통한 위협 조사 엔진
- 위협 인텔리전스의 손쉬운 생성 및 공유
- 브랜드 모니터링: 브랜드 오용 탐지
- Trusted Circle을 통한 협업

도입 효과

ThreatStream은 위협 인텔리전스 운영성을 향상시키고 기존 보안 도구를 하나의 플랫폼으로 통합하여 탐지 및 대응 시간을 획기적으로 줄여준다.

- 모든 위협 인텔 정보를 한 곳으로 통합
- 원시 지표를 즉시 사용할 수 있는 인텔리전스로 변환
- 기본 보안 투자 자산과 쉽게 통합
- 사고 대응 시간 감소
- 보안 분석가 업무 효율 증가

Anomali ThreatStream에 대한 보다 상세한 정보는 www.anomali.com/threatstream 사이트를 방문하거나 이메일 주소 info@anomali.com를 통해 받아볼 수 있다.

ANOMALI™
808 Winslow Street, Redwood City, CA 94063 USA
1-844-4-THREATS | info@anomali.com | www.anomali.com