

1 0 1
1 0 0
0 1
1 0 0
1 1 0
1 0 1
1 1 0
1 1 0
1 1 0
1 1 0
1 0 1
1 0 1
1 0 1
1 0 0
1 1 0
0 1
1 1 0
1 1 0
1 1 0

ANOMALI[®]

“위협 인텔리전스 플랫폼”

(주)한국밸런스

회사 소개

위협 인텔리전스와 분석 플랫폼을 제공하는 사이버보안 회사

- 본사: 미국, 캘리포니아 레드우드
- 직원: 300명 이상
- 설립: 2013년
- 투자: \$100M

ANOMALI

귀사에 가해지는 사이버 위협을 신속히 찾고 대응할 수 있도록 도와드리는 것이 저희의 임무입니다. 저희는 귀사의 보안팀에 없는 것 한가지, 바로 외부 컨텍스트 정보를 제공해드립니다. Anomali와 함께하시면 의심스러운 악성 트래픽이 귀사의 네트워크에 도달하기 전에 미리 식별하실 수 있습니다. 거대한 위협 인텔리전스를 귀사만의 핵심 목록으로 정제하고 이를 내부 보안 시스템 및 IT 시스템과 유기적으로 통합하실 수 있도록 도와드립니다.

수상 이력

- 사이버 시큐리티 엑셀런스 어워드 수상
- CRN 시큐리티 상위 100대 보안 기업
- 사이버 디펜스 “위협 인텔” 부문 최고 제품
- SC미디어 리뷰 별 5개 “Best Buy” 제품 선정
- CRN 선정 가장 뜨는 보안 스타트업



위협 인텔리전스 개요



위협 인텔리전스 개요

- IOC (Indicator of Compromise)
 - IP, 도메인, URL 뿐만 아니라
 - 파일 해시, 이메일, URL, 서비스, 프로세스, 레지스트리, 인증서도 중요
- 종류도 많고 그 개수는 수백/수천만건 이상
- 유/무료 피드도 많지만

많을수록
좋은가?

활동하는 최신
정보인가?

내 업종/지역과
유관한가?

관리는 어떻게
할 것인가?

위협 정보를 어떻게 잘 관리하고 활용할지가 관건!

제품 소개

두 가지 제품으로 구성

ANOMALI®

ThreatStream

The Most Widely Adopted Threat Intelligence Platform

Anomali Enterprise

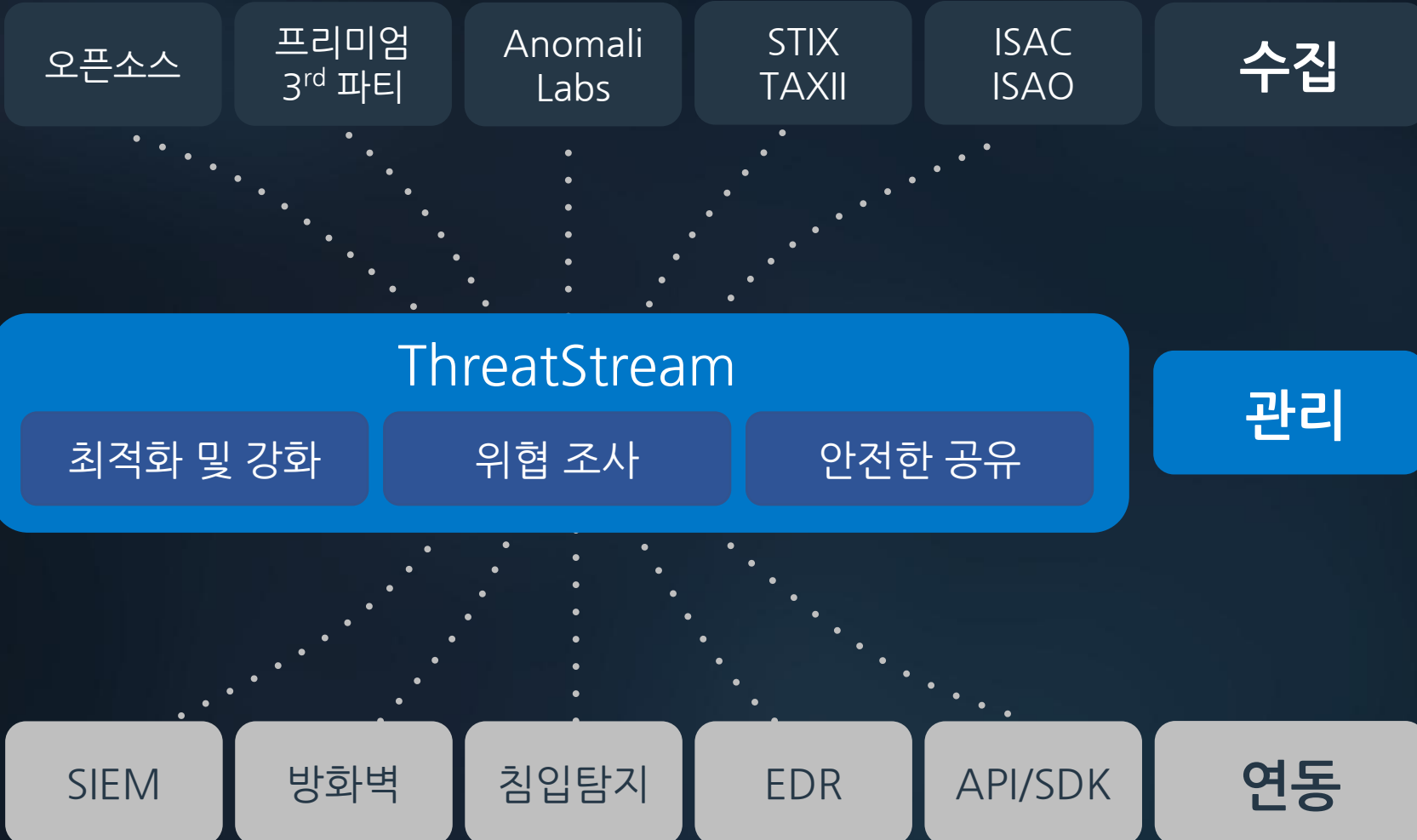
“위협 인텔리전스 플랫폼”

수많은 내/외부 위협 인텔 정보를 수집, 통합, 정제, 강화, 정렬, 필터링하며 각각의 인텔을 점수화하여 나에게 특화된 정보에 집중, 보안 분석가의 인텔 정보 활용 효율을 극대화하고 위협 분석 활동을 적극적으로 수행할 수 있는 환경 제공.

“위협 추적 엔진”

SIEM 또는 로그 시스템과 통합되어 데이터를 중복으로 저장하지 않고도 일년 이상 지속되는 공격을 탐지하고 이에 대한 가시성을 제공. 신규 인텔 정보를 지속적으로 매칭하는 위협 추적 엔진. 실시간 포렌직으로 발견 즉시 알려주며 별도의 분석 도구 제공으로 보안 대응 능력 향상.

1. ThreatStream 소개



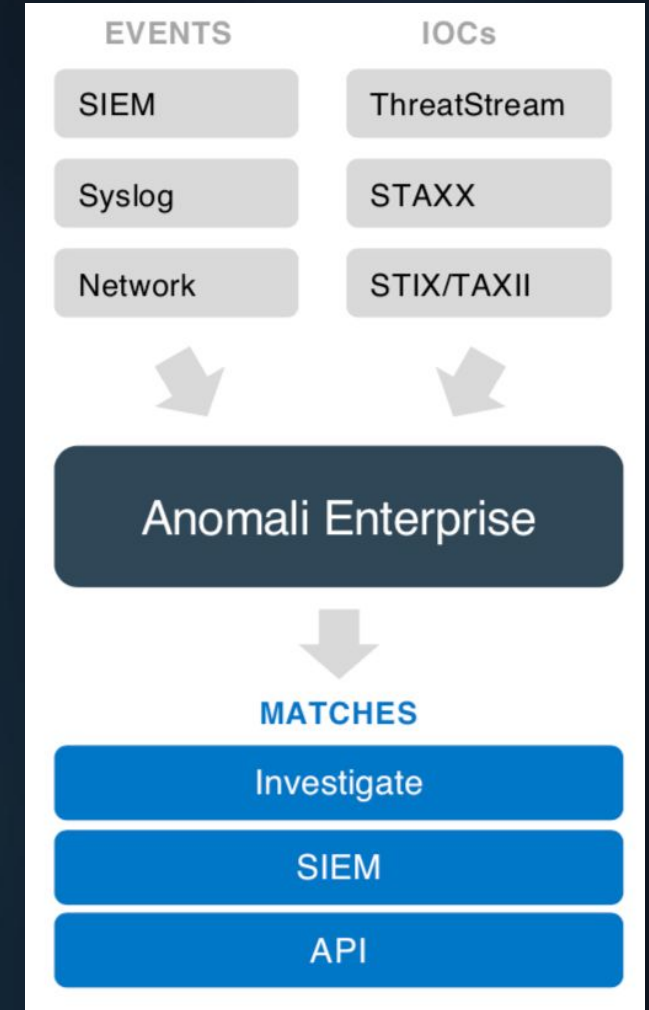
- 모든 소스로 부터 인텔 수집
- STIX/TAXII 포맷 지원
- 완전한 양방향 IOC 공유

- 다수 소스의 중복된 IOC 정제
- 액터, 캠페인, TTP로 강화
- 중복 제거, 거짓 긍정 탐지

- 지표 내려받기
- 내부 시스템과 연동
- API/SDK를 통한 커스텀 연동

2. Anomali Enterprise 소개

- 네트워크의 활성 위협 탐지
- 365일 이력 데이터 검색
- 별도의 로그 데이터 저장소 불필요
- DGA 도메인 탐지
- 중요 IOC에 대해 필터링/우선 순위 분류/추정 불필요
- 탐지 결과를 SIEM 또는 대시보드에 전송
- 내장된 위협 조사 도구 및 워크플로우



제공 서비스

고객 만족을 위한 후방 지원 체계

- 운영** • SIEM & Anomali 솔루션 전문가
- 기술 지원** • 티어 1, 2, 3 고객 기술 지원
- 솔루션 엔지니어링** • 커스텀 연동, 피드 또는 기능 개발
- 프로페셔널 서비스** • 인텔 지원 서비스의 설계 및 실행
- 위협 분석 팀** • 정보 및 위협에 대한 연구 요청
- Anomali Lab** • 위협 피드 큐레이션, 주간 위협 브리핑
- 교육** • Anomali 유니버시티, Anomali 포럼
- 이벤트** • Anomali Detect Conference + Threat Briefing Days

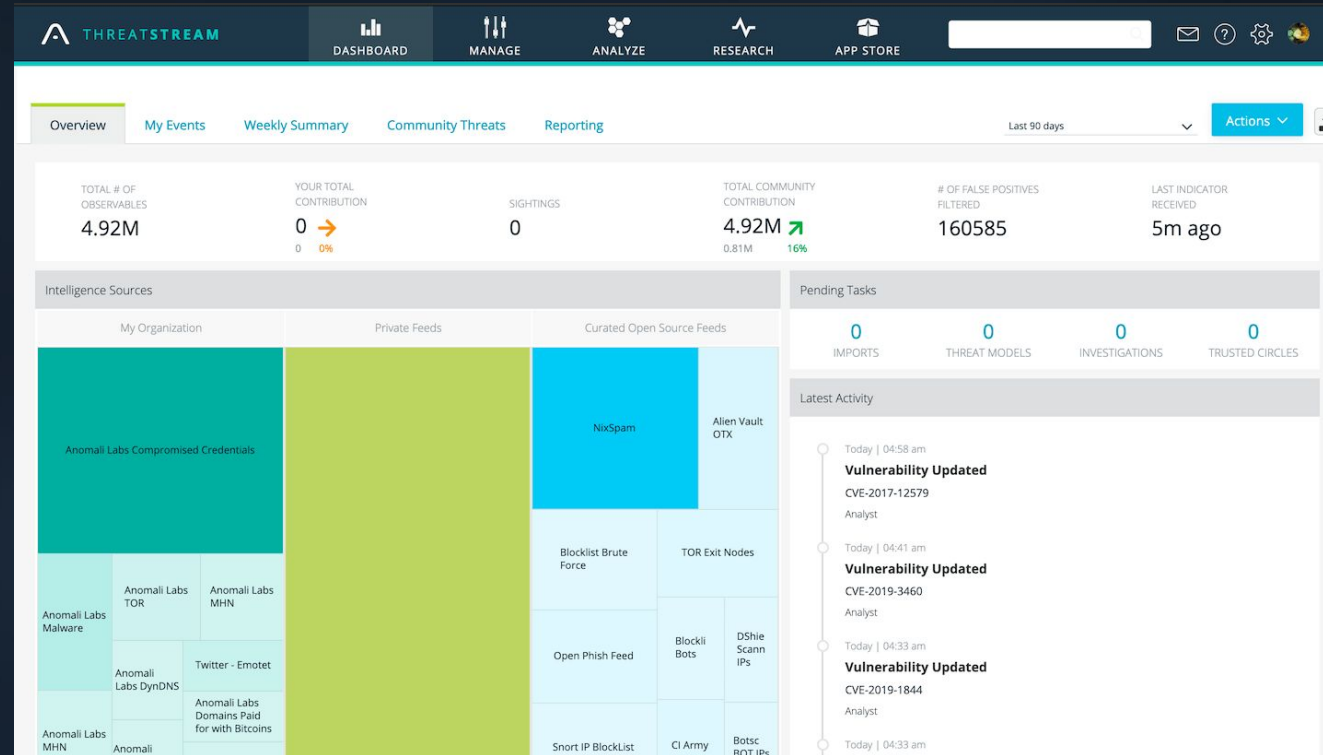
ANOMALI®



- **Comprehensive:** 위협 인텔리전스 + 위협 탐지 + 위협 조사
- **Proven:** 포춘 100대 기업 35%가 도입, 상위 은행 5곳 중 4곳 도입
- **Trusted:** 대부분의 ISAC과 위협 인텔 공동체와 협력
- **Research:** Anomali Labs, 위협 보고서, 주간 위협 브리핑 제공
- **Global:** 6개 대륙 운영, 글로벌 서포트

Anomali ThreatStream 예시

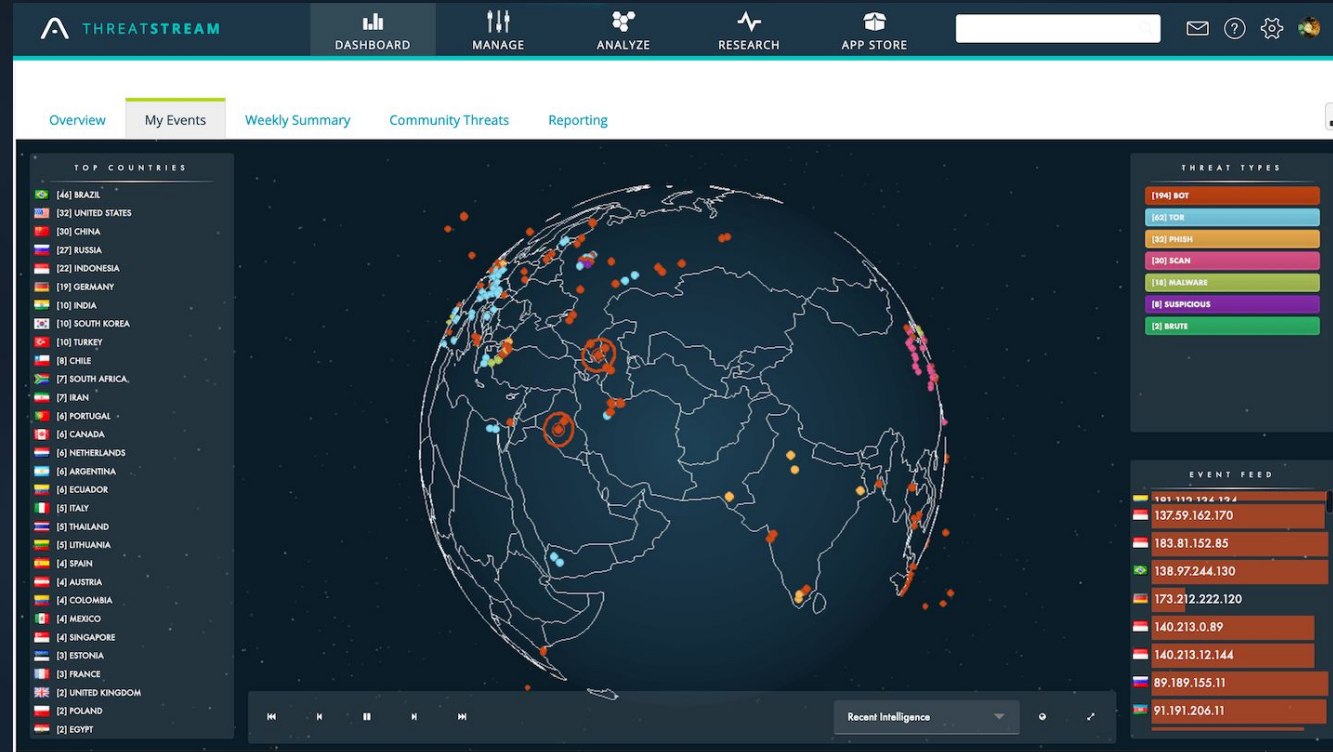
인텔리전스 현황 대시보드



Anomali ThreatStream 대시보드는 위협 인텔리전스의 수집 및 활용 현황을 한눈에 보여주며 현재 사용 중인 인텔 목록, 기업 내부 인텔 목록, 정제된 오픈소스 피드 등을 체계적으로 정리해줄 뿐 아니라 각종 위협 인텔 관련 활동 기록과 나의 관심 태그에 해당하는 위협 인텔의 현황을 보여줍니다.

Anomali ThreatStream 예시

이벤트 활동



위협 인텔리전스의 활동 이벤트를 지도 상에 동적으로 표시합니다. 이를 통해 어느 지역에서 어떤 종류의 위협 인텔리전스들이 발생하고 등록되고 있는지 실시간으로 확인할 수 있습니다.

Anomali ThreatStream 예시

위협 정보 업로드

자체적으로 관리하는 위협 정보를 직접 Anomali ThreatStream으로 업로드하여 관리할 수 있습니다. 자체적으로 관리 시스템을 개발/운영할 필요없이 ThreatStream의 프라이빗 영역에서 관리합니다.

직접 입력하거나 JSON, CSV, PDF 등 정형, 비정형 파일로 업로드 할 수 있고, 이메일을 등록하여 자동으로 등록되도록 설정할 수 있습니다.

New Import

Observables **STIX** **Email / Phishing**

1. ADD DATA

Import observables from files, web page, emails, or select paste intelligence to manually enter observables. Accepted document types are: JSON, CSV, PDF or Text File. The following IOCs will be extracted: IP Address (v4 & v6), Domain, URL, Email, & MD5 Hash. Download ThreatStream's [structure files](#) (more info)

Upload a New File OR Paste Intelligence

Drop a file here
Or click to upload

187.99.88.105
167.298.8.11
209.110.228.29

2. SET DEFINITIONS

Intelligence Source: ANOMALI_TEST

Threat Type: Adware

Tags: Test1, TLP:WHITE, ADD, ADD KILL CHAIN PHASE

Expiration Date *: 90 Days, 60 Days, 30 Days, Never, Custom

Visibility: Public, Trusted Circles, Private

Shared with only your organization. Setting the confidence below will set confidence for all items except IPs and Domains

Confidence: 10, 50, 100

Override system Confidence

3. ASSOCIATE WITH THREAT MODELS (OPTIONAL)

Bulletin

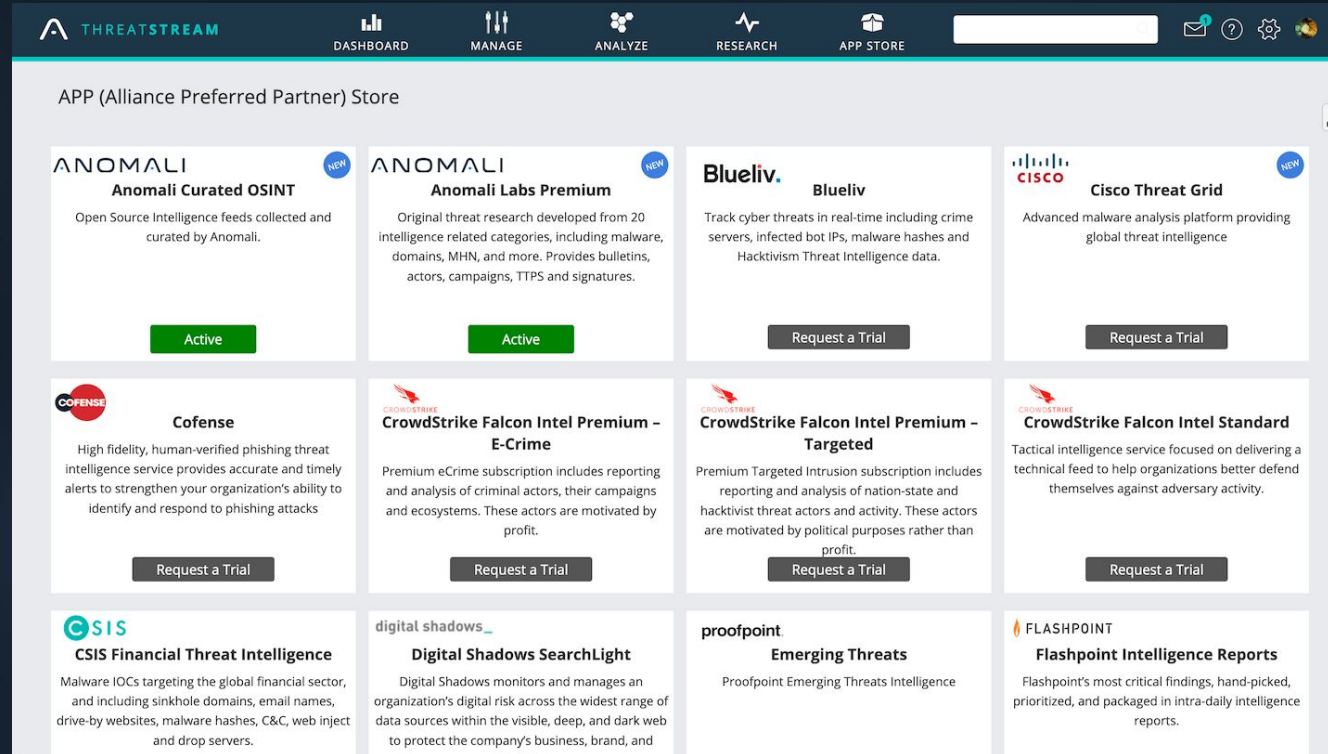
Actor, Bulletin, Campaign, Incident, TTP

Selected Associations: TTPs: Dictionary-based Password Attack [CAPEC 16]

IMPORT

Anomali ThreatStream 예시

외부 인텔리전스 연동 앱스토어



Anomali ThreatStream에는 자체 앱스토어가 있어, 유료 위협 인텔리전스 제공사와 즉시 연동할 수 있고, 내 환경에 맞게 정제된 위협 인텔 정보를 SIEM, 방화벽, 침입탐지시스템 등으로 자동 전송 및 적용할 수 있습니다.

Anomali ThreatStream 예시

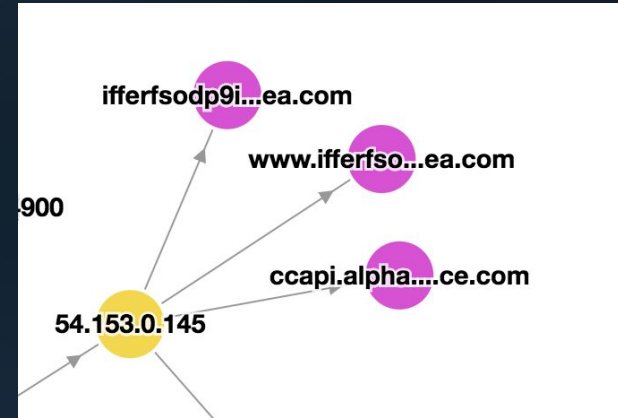
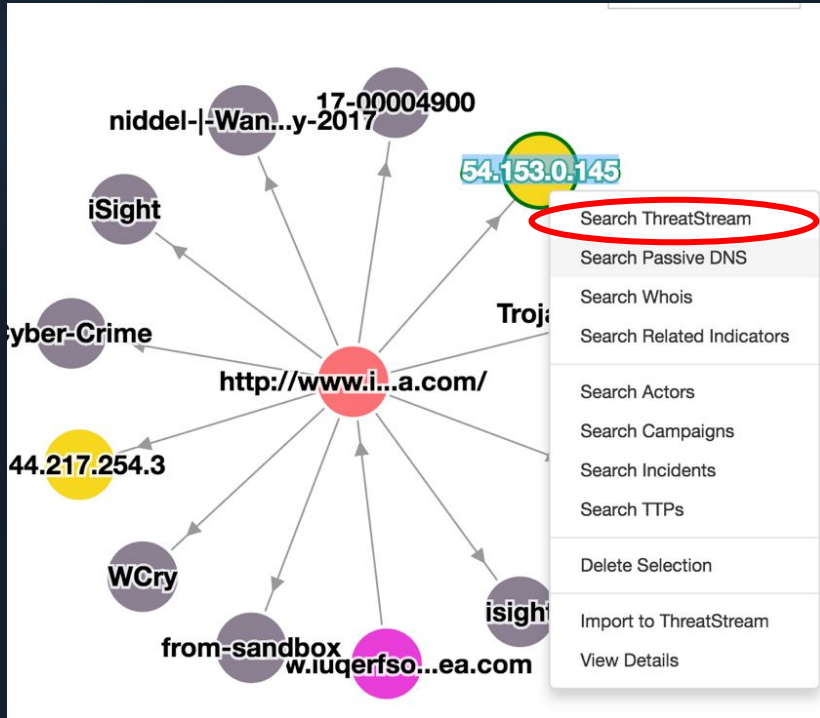
위협 인텔리전스 분석

The screenshot displays the Anomali ThreatStream interface. On the left, the 'Observables' section shows a search filter: '(status="active") and (stream_id=445) and (created_ts>=2018-04-29T23:44:07)'. Below this is a table of search results with columns for Date First, iType, Indicator, Confidence, Country, Streams/Source, Visibility, and Tags. The table lists several 'Compromised A...' indicators with a confidence of 100, all from 'Anomali Labs Co...'. On the right, the 'Details for microsoft-log.com' page is shown. It features a 'Severity' of HIGH and a 'Confidence' of 100. The status is 'Active' and the type is 'Domain (Suspicious Domain)'. The indicator is 'microsoft-log.com' and the IP is '87.242.73.75'. A network diagram shows connections between '87.242.73.75', 'microsoft-log.com', 'TSLABS', and 'victim-Hi-Tech'. The organization is identified as 'Masterhost is a hosting and technical support orga'.

위협 인텔리전스 분석 기능은 클라우드상의 방대한 인텔 정보를 대상으로 다양한 조건으로 검색하고 SIEM에서 매칭된 특정 인텔 정보에 대한 상세한 내용(심각도, 신뢰도, 액터, 침해 보고서, 관련 위협 정보, 활동 상태, 활동 이력 등)을 조회하여 관심 지표로 등록하거나 태깅하여 즉시 활용할 수 있습니다.

Anomali ThreatStream 예시

위협 인텔리전스 분석



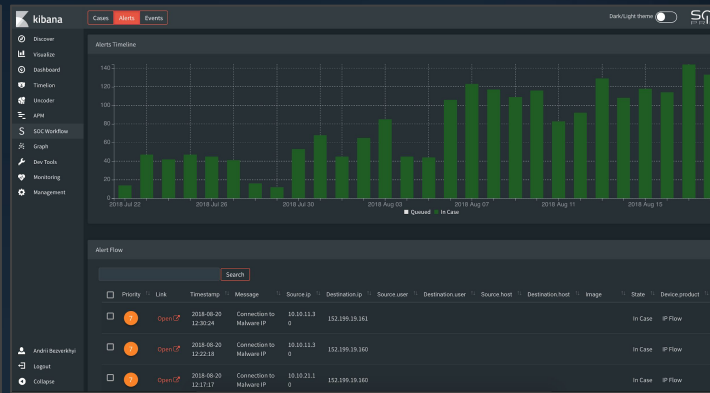
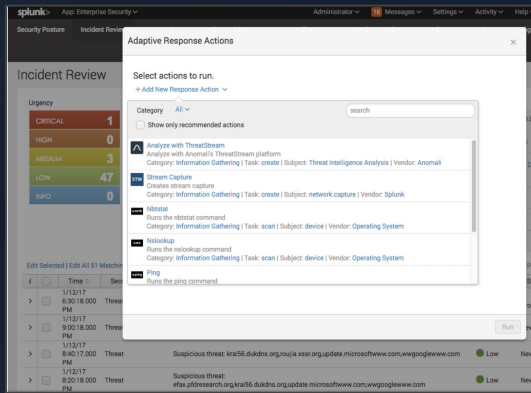
하나의 침해지표를 선택하면 이와 연관된 모든 관련 지표들을 그래프 형식으로 한눈에 표시해주며, 이어서 관련 지표 선택시 컨텍스트 메뉴를 통해 그 속성에 따라 추가 검색, 후이즈 록업, 액터 검색 등의 여러가지 추가 분석 기능을 제공하며 특정 침해지표의 완전한 분석을 가능하도록 도와줍니다.

Anomali ThreatStream 예시

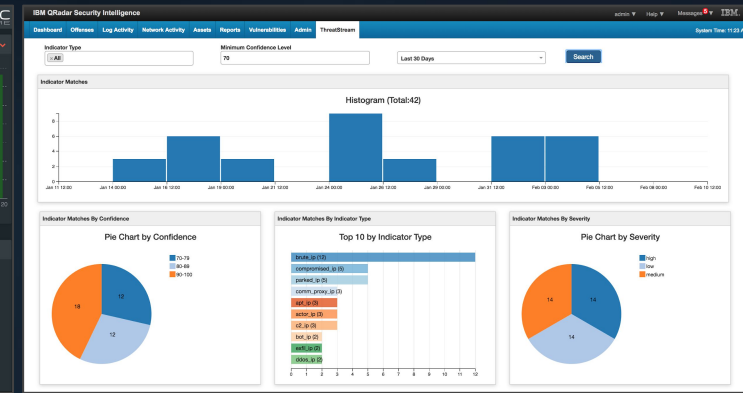
SIEM 연동 예시



스플링크 ES 대시보드



Elasticsearch 연동



Qradar 연동

Anomali는 주요 SIEM 제품(Splunk, ELK, Qradar 등)용 전용 앱을 제공하여 매우 쉽게 기존 SIEM에 Anomali가 제공하는 정제된 위협 인텔리전스 정보를 즉시 적용할 수 있습니다.

Anomali ThreatStream 예시

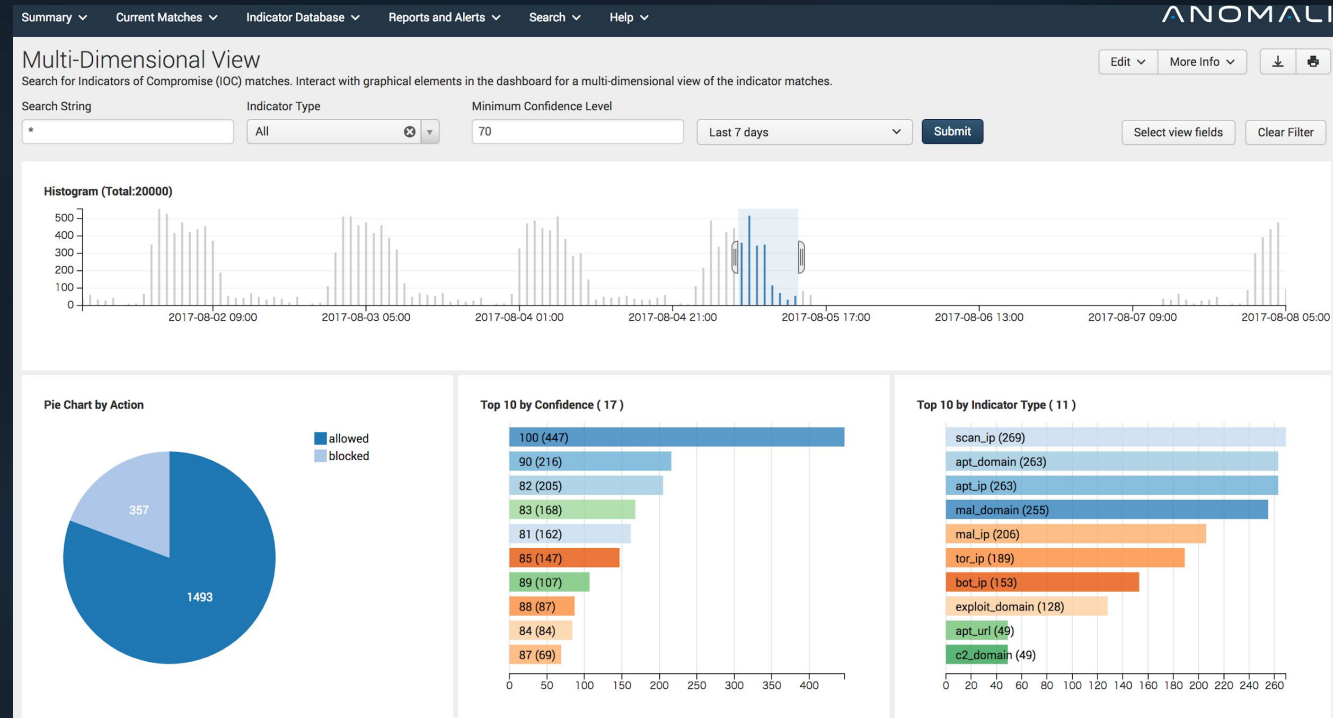
SIEM 연동 예시

The screenshot displays the 'CHOOSE DESTINATION' dialog in the Anomali ThreatStream interface. It is divided into two main sections: 'FEATURED DESTINATIONS' and 'OTHER DESTINATIONS'. The 'FEATURED DESTINATIONS' section contains a grid of logos for various security products, including Accellera, ArcSight, Blue Coat, The Bro Network Security Monitor, Bit9 + Carbon Black, CEF, Cloudera, CrowdStrike, CSV, FireEye, HIVE, Infoblox, LogRhythm, McAfee, Palo Alto Networks, Radar, RSA Security Analytics, **splunk** (highlighted with a red circle), Syslog, and Tanium. The 'OTHER DESTINATIONS' section contains a text box stating: 'We can send threat intelligence to any product that allows for file based integration. We do not currently support API integrations.' Below this text is a link: 'Click to set up Custom Destination'. The 'CREATE NEW DESTINATION' dialog is open, showing the following fields: Name* (splunk_1502177980252), Destination Filter* (confidence>80 AND itype=c2_domain), Splunk version (6.5), Splunk ThreatStream integration* (Add-on selected, App selected), Splunk ThreatStream absolute path* (/opt/splunk/etc/apps/threatstream), and Splunk deployment server* (localhost). There are 'CANCEL' and 'SAVE' buttons at the bottom right of the dialog.

연동 방법은 UI에서 대상 제품을 선택하고 기본 정보 몇 가지만 입력하면 바로 동작합니다.

Anomali ThreatStream 예시

SIEM에서의 활용



ThreatStream과 연동된 SIEM 제품에서 내부 보안 로그와 매칭된 결과를 다차원 분석합니다. 예시는 스플링크에서 사용하는 예이며 매칭 빈도에 대한 히스토그램과 탐지 형태 등의 정보를 보여줍니다.

감사합니다.

Contact :

(주)한국밸런스

김형덕 영업대표

Mobile : 010-7138-8889

Email : hdkim@valence.co.kr