Introduction ThreatStream

위협 행위자는 끊임없이 진화하고 공격을 진행하고 있습니다.
조직이 사이버 위협으로부터 효과적으로 자신을 방어할 수 있는 유일한 방법은 이러한 공격에 대한 상황을 파악하고 사후 대응 방식에서 사전 대응 방식으로 전환하는 것입니다.
이는 위협 인텔리전스를 활용해야만 가능합니다. 위협 인텔리전스는 공격자와 그들의 전술, 기법 및 절차 (TTP)에 대한 실행 가능한 정보입니다.

Anomali ThreatStream 은 위협 인텔리전스 분석의 수작업을 자동화하고 분석가가 고립된 환경으로부터 통합된 환경에서 사이버 위협을 조사하고 대응할 수 있도록 하는 솔루션입니다.
또한 대규모 조직의 경우 ThreatStream 은 작업 할당 및 팀 협업을 지원합니다.

ThreatStream 은 조직의 요구와 환경을 충족시키기 위해 직접 선택할 수 있는 여러 소스로부터 인텔리전스를 모아서 종합합니다.

다음과 호환됩니다.

- 시장에서의 공개 소스 및 최고의 프리미엄 타사 피드
- 구조화 / 비구조화 파일
- STIX / TAXII
- 오픈 소스분석 플랫폼
- 위협 공유 그룹
- MITRE ATT & CK 프레임워크 같은 커뮤니티 기술 자료

또한 우리의 제품으로 고객이 최상의 경험을 얻을 수 있도록 수상 경력에 빛나는 Anomali Labs 팀은 관련 IOC(Indicators of Compromise)와 함께 주간 위협 브리핑 및 위협 게시판을 게시합니다.

그런 다음 IOC 는 사이버 위협과 관련 있는 다중 요인들을 기반으로 한 개별 Observable 의 가중치와 정보를 정렬하기 위해 자체 머신 러닝 알고리즘으로 분석됩니다.

선별된 지표는 빠른 식별을 위한 태그 및 위협 모델 연계를 포함한 연계된 인텔리전스와 위험 점수를 읽기 쉬운 형식으로 제공됩니다.

마지막으로, 이 인텔리전스 저장소는 팀이 신뢰할 수 있는 조직 및 Anomali 커뮤니티와 공유하고 조사하는 것을 가능하도록 합니다.

또한 ThreatStream 은 기존 보안 투자와 완벽하게 통합되므로 사고 대응이 신속하고 자동화되며 효과적입니다.

Anomali의 ThreatStream은 정확하고 빠른 응답 시간과 이미 구축되어 있는 보안 자산들을 통합하여 한 곳에서 모든 위협 인텔 데이터를 집중화하는 Threat Intelligence Platform(TIP)입니다.

정보는 어디에서 가져옵니까?

Anomali ThreatStream은 인텔 정보를 아래에서 가져옵니다.

- OSINT(Open Source INTelligence) 피드.
- Trusted Circles.
- STIX/TAXII 피드.
- 상용 공급 업체의 프리미엄 피드
- CSV 파일의 구조화된 인텔리전스
- 구조화되지 않은 인텔리전스 : PDF, CSV, 이메일, 원시 텍스트

받은 정보는 어떻게 처리됩니까?

귀하의 원시 위협 데이터는 다음과 같이 ThratStream에 의해 정교하게 처리됩니다.

- 피드는 일반적인 분류 체계로 정규화됩니다.
- 피드 간 중복 데이터가 제거됩니다.
- 오탐이 제거됩니다.
- 데이터는 액터, 캠페인, TTP 정보로 향상됩니다.
- 위협 지표 인텔리전스 간의 연계가 생성됩니다.

강화된 위협 데이터는 어떻게 사용됩니까?

IOC(Indicator of Compromise)라고도 하는 Observable은 분석가가 공격 네트워크 구축을 위해 검토, 강화 및 연계를 위해 사용할 수 있습니다. 이 데이터는 인텔리전스 공유 및 공격 방지를 위해 내부 또는 외부에 게시될 수 있습니다.

또한 규칙과 태깅을 사용하면 TreatStream과 내부 보안 시스템을 쉽게 통합하여 위협 인텔리전스를 여러 가지 방법으로 실행할 수 있습니다.

- SIEM, Firewall, IPS 및 EDR과의 통합을 강화하십시오
- 머신런닝을 통해 위협의 위험 순위가 나타납니다.
- 위협 게시판 생성.
- 신뢰할 수 있는 서클과의 양방향 공유.

<ThreatStream 배포 다이어그램 상 용어 설명>

- Threat Feed Source
  ThreatStream은 수백 개의 소스에서 인텔리전스 데이터를 수집합니다. 사용자는 Anomali APP Store에서 직접 타사 프리미엄 피드를 검토하고 구입할 수 있습니다.
  위협 인텔리전스 소스는 다음과 같습니다.
  - STIX / TAXII 피드
  - 오픈 소스 위협 피드

    - 상업용 위협정보 제공 업체
    - 구조화 / 비구조화 인텔리전스
    - ISAC / ISAO 공유 위협 인텔리전스
- ThreatStream

  Anomali ThreatStream은 데이터를 정교화한 후 Integrator로 전송하여 최종 사용자가 사용할 수 있게 합니다.
- Integrator

  ThreatStream Integrator는 ThreatStream 플랫폼 또는 ThreatStream 어플라이언스에 연결하여 풍부한 사이버 위협 인텔리전스 피드를 기존 도구 및 인프라로 가져와서 기존 보안 솔루션에 실시간 인텔리전스를 제공하는 소프트웨어입니다.
- SIEM

  Integrator는 다음의 SIEM 솔루션과 호환됩니다.
    - ArcSight ESM
    - Splunk
    - QRader
    - McAfee ESM (NitriSecurity)
    - LogRhythm
    - AccelOps
    - RSA NetWitness
    - Bro_intel
- IDS

  침입탐지시스템은 악의적인 활동이나 정책 위반에 대해 네트워크를 모니터링하는 장치 또는 소프트웨어 응용 프로그램입니다.

  ThreatStream은 BroIDS와 같은 서비스와 통신할 수 있습니다.
- Hadoop

  다음과 같은 하둡 솔루션이 지원됩니다.
    - Cloudera Impala
    - 하둡 하이브
- DNS

  ThreatStream은 Infoblox와 즉시 통합할 수 있습니다.
- Firewall

  Integrator는 다음 방화벽과 호환됩니다.
    - Palo Alto Networks
    - Blue Coat Proxy SG
    - Check Point
    - Cisco ASA
- Endpoint Security

  ThreatStream은 다음 Endpoint Security 솔루션과 통합할 수 있습니다.
    - Carbon Black

    - Tanium
    - CrowdStrike
    - FireEye HX
- SDK

  Integrator SDK (Software Development Kit)는 ThreatStream Integrator가 기본적으로 지원하지 않는 네트워크 및 보안제품에 대한 통합을 생성할 수 있는 유연성을 제공합니다.
  통합을 만든 후에는 SDK 기반 통합이 이미 사용 가능한 기본 제공 통합과 동일하게 작동합니다.
- ThreatStream Analyst Interface

  ThreatStream 사용자 인터페이스는 웹브라우저를 통해 시작됩니다.

Why ThreatStream?

웹브라우저를 통해 사용 가능한 ThreatStream은 내장 위젯을 통해 의미 있고 읽기 쉬운 보고서를 제공합니다. 보안팀은 다음을 수행할 수 있습니다.

위협 데이터 수집 간소화

ThreatStream은 여러 이종 소스의 대량 정보 수집을 관리합니다. 수동으로 수행하는 경우 분석가에게 많은 시간과 노력이 필요한 작업입니다.

데이터 품질 향상

ThreatStream은 원시 위협 데이터를 수집하여 다음과 같은 방법으로 이를 풍부하고 유용한 인텔리전스로 전환합니다.

- 무제한의 IOC 수집 및 관리
- 무제한 볼륨의 로그에 대한 IOC 일치
- 로그에서 IOC 활동에 대한 경보를 자동으로 작성합니다.
- Integrator를 통해 Feeding indicator를 SIEM 및 기타 시스템과 일치합니다.

조사 수행

위협 데이터는 서로 연결되어 쉽게 분석할 수 있습니다. ThreatStream에는 ThreatStream 인터페이스 내에서 공격 맵을 구축하고 조사를 관리할 수 있는 탐색 기능이 포함되어 있습니다.
Anomali에서 Workflow Service를 구매하여 ThreatStream 플랫폼 내에서 분석가의 성능을 향상시킬 수도 있습니다.

보안 조치 자동화에 사전 대응

ThreatStream Integrator는 네트워크 및 보안 서비스를 통해 위협 데이터가 운영되게 하고 인텔리전스를 실행 가능하게 합니다.

DASHBOARD

대시보드는 ThreatStream에 액세스할 때 (특히 Overview Dashboard) 기본 방문 페이지입니다. 데이터를 한 눈에 볼 수 있는 전체 위젯 세트가 표시됩니다.

- Overview
  조직과 관련된 Observable(IOC)에 대한 실시간 개요를 얻고 즉각적인 조치가 필요한 경고를 봅니다.
- My Events
  전 세계 위협의 지리적 위치를 시각화합니다.
- Weekly Summary
  조직에 인텔리전스를 제공하는 다양한 피드를 통해 제공되는 데이터의 품질을 시각화합니다.
- Community Threats
  지난 30일 동안 커뮤니티에서 가장 많이 본, 별표 표시된, 좋아요 및 댓글이 있는 Observable 및 위협 모델 항목을 봅니다.
- Reporting
  보고 대시보드를 사용하면 최대 1년의 사용자 활동에 대한 임시 보고서를 생성할 수 있습니다. ThreatStream의 모든 사용자는 사용자 활동 보고서를 생성할 수 있지만 조직 관리자만 조직의 모든 사용자 활동에 대한 보고서를 생성할 수 있습니다. 관리자가 아닌 사용자는 자신의 활동에 대해서만 보고서를 생성할 수 있습니다.

MANAGE

- Imports
  조직과 관련된 모든 가져오기 작업의 목록을 표시합니다.
- Trusted Circles
  조직이 현재 속한 신뢰할 수 있는 서클을 표시합니다. 사용 가능한 공개 서클 목록을 보고 새 서클을 만들 수도 있습니다.
  조직과 관련된 모든 가져오기 작업의 목록을 표시합니다.
- Streams
  - 현재 위협 정보를 제공하는 스트림을 봅니다.
  - 조직에서 액세스할 수 있는 새 스트림을 선택할 수 있습니다.
  - 이전에 제출된 스트림을 편집할 수 있습니다.
- Rules
  ThreatStream에서 구성된 규칙을 보고 관리하여 특정 키워드가 인텔리전스에 나타날 때 자동 작업을 수행할 수 있습니다.
- Source Optimizer
  오픈 소스 인텔리전스와 조직의 관련성에 대한 중요한 지표를 제공합니다.

ANALYZE

- Overview
  TreatStream에서 업데이트된 가장 최근의 5가지 행위자, 캠페인, 사건, 멀웨어 개체, 서명, 위협 게시판, TTP 및 취약점이 포함된 위협 모델 대시보드를 표시합니다. 또한 STIX 가져오기 페이지에 액세스할 수 있으며 최근에 가져온 STIX 데이터의 상태를 제공합니다.
- Observables
  현재 데이터베이스에 있는Observable을 표시하여 사용자가 기본 및 고급 Observable 검색을 수행할 수 있습니다.
- Threat Models
  위협 모델 목록 보기 페이지가 열립니다. 이 페이지에서 새 개체를 만들고 개체를 삭제하며 조사에 개체를 추가할 수 있습니다.

RESEARCH

- Investigations
  조사 대시보드에는 ThreatStream에서 액세스할 수 있는 조사가 표시됩니다. 조사는 일상적인 작업을 수행하는데 사용할 수 있는 협업적이고 유연한 작업 공간입니다.
- Sandbox
  샌드박스 목록 보기 화면에서 샌드박스 보고서에 액세스하면 다음을 수행할 수 있습니다.
  - 새로운 폭발을 만듭니다.
  - 조사 시작/계속
  - 선택한 샌드박스 보고서를 삭제하십시오.
- Explore
  함께 관련된 것으로 알려진 Observable을 추가하여 공격 인프라를 매핑할 수 있는 그래픽 도구를 시작합니다.

APP STORE

APP (Alliance Preferred Partner)은 OSINT (Open Source INTelligence feeds)를 활성화할 뿐만 아니라 Anomali 파트너들에 의해 제공되는 프리미엄 위협 인텔리전스 스트림을 평가하고 구매할 수 있는 마켓플레이스입니다.

Observable and Intelligence

ThreatStream에서는 프리미엄 피드, OSINT, STIX/TAXII, ISAC으로부터 인텔리전스를 수집하고 Import Assistant를 사용하여 사용자가 수동으로 가져오기를 만들 수 있도록 합니다.

Observable은 ThreatStream 컨택스트에서 악의적인 활동을 식별하는 인위적 산물입니다.
본 제품에서 Observable이 선호되는 용어이지만 Indicator / IOC / Observable은 서로 바꿔 사용할 수 있습니다.

Observable

가져오기를 할 때 ThreatStream은 Severity(심각도)와 Confidence(신뢰도) 수준을 자동으로 할당합니다.

Severity(심각도)는 Observable과 관련된 지표 유형의 잠재적 영향을 측정합니다.

지표 유형은 다음 4가지 심각도 중 하나에 매핑됩니다.

- Low
- Medium
- High
- Very-High

예를 들어 명령 및 제어 지표 유형은 심각도 값이 높음에 매핑되는 반면 TOR 관련 Observable은 낮음에 매핑됩니다.
따라서 심각도는 분석된 Observable과 동일한 범주의 다른 Observable들을 비교하는 것이 아니라 iType을 기반으로 지정됩니다.

Confidence(신뢰도)는 Observable의 측정 정확도입니다. ThreatStream의 기계 학습 알고리즘은 할당된 지표 유형의 정확도를 포함하여 많은 요소를 고려하여 신뢰도를 계산합니다.
다양한 위협 인텔리전스 소스에 의해 보고된 단일 Observable의 모든 유용한 사례에 의해 신뢰도가 계산됩니다. 활성 상태에서 사용 가능한 사례 중 가장 높은 ThreatStream 계산 신뢰도 점수는 Observable 상세 페이지 맨 위에 표시됩니다.
ThreatStream의 기계 학습 알고리즘은 이메일, 해시, String Observable Type과 사용자가 "Override System Confidence"를 선택한 경우 신뢰 점수를 계산하지 않습니다.

Analyst Tip: Confidence Scores
기본적으로 동일한 Observable이 여러 소스에 의해 보고되면 Overview 섹션에는 사용 가능한 경우의 최고 신뢰도 점수가 활성 상태로 표시됩니다.
신뢰도 그래프 위로 마우스를 가져가면 신뢰도의 가장 높은 값과 가장 낮은 값 및 평균 값을 확인할 수 있습니다.

iTypes

하나의 iType은 Observable로 심각도 수준을 할당하고 데이터를 분류하기 위해 TreatStream에 의해 각 Observable에 연결됩니다.

- actor_ip
  심각도: 낮음
  악성 활동이 포함된 시스템과 관련된 IP 주소입니다.
- apt_domain
  심각도: 매우 높음
  명령 및 제어, 익스플로잇 실행 또는 데이터 탈취에 사용되는 알려진 APT (Advanced

Persistent Threat) 행위자와 관련된 도메인 이름입니다.

- c2_domain
  심각도: 높음
  명령 및 제어 통신을 위해 멀웨어가 사용하는 도메인 이름입니다.
- cryto_hash
  심각도: 높음
  암호화폐 마이닝 소프트웨어의 파일 해시
- exploit_domain
  심각도: 매우 높음
  익스플로잇 키트를 호스팅하거나 웹 기반 익스플로잇을 시작하는 웹 서버와 관련된 도메인 이름입니다.
- mal_domain
  심각도: 매우 높음
  멀웨어 코드에 접속된 도메인: 명령 및 제어 명령일 수도 있고 클라이언트가 온라인인지 확인할 수도 있습니다.
- phish_domain
  심각도: 매우 높음
  피싱 또는 스피어 피싱 이메일을 피해자에게 보내는 것과 관련된 이메일 주소입니다.
- suspicious_ip
  심각도: 보통
  의심스러운 이유로 등록된 것으로 보이지만 아직 알려진 악의적인 활동과 관련이 없는 IP 주소입니다.
- tor_ip
  심각도: 낮음
  TOR(The Onion Router) 네트워크의 일부로 작동하는 IP 주소이며 TOR exit node라고도 합니다.

Tags

ThreatStream은 짧은 자유 형식의 조각 정보인 태그 개념을 지원하여 Observable (indicator)과 위협 모델 개체 모두에 컨텍스트를 추가할 수 있습니다. 태그는 공개 또는 비공개 표시로 추가할 수 있습니다.

Import Assistant Overview

ThreatStream의 Import Assistant는 다음의 구조화/비구조화 데이터 데이터를 구문 분석할 수 있습니다.

- 파일 (CSV, HTML, IOC, PDF, TXT, XML)
- 원시 텍스트
- 일반 텍스트 인텔리전스 스트림
- 파일에 직접 연결

- 이메일

Intelligence Streams

ThreatStream에는 사용자가 인텔리전스 스트림이라는 Observable의 정보 수집을 위한 사용자 지정 피드를 생성할 수 있는 기능이 포함되어 있습니다.

STIX TAXII

STIX 및 TAXII는 사이버 공격의 예방 및 완화를 증진하기 위해 개발된 표준입니다.

APP STORE

APP(Alliance Preferred Partner) Store는 조직에서 Anomlai 파트너가 제공하는 프리미엄 위협 정보 스트림을 평가하고 구매할 수 있는 마켓플레이스입니다.

Reviewing an Observable in ThreatStream

인텔리전스를 연구하고 Observable을 검토하는 것은 단순하지 않으며 기술, 지식 및 경험이 필요하지만 일부 단계는 항상 수행해야 합니다.
여기에서 미숙련 분석가가 Observable 세부 사항 페이지에 포함된 정보를 이해하도록 돕기 위해 이러한 단계를 표준화된 프로세스로 통합하려고 시도했습니다.

- Look at Severity and Confidence
  Severity는 iType의 위협에 대한 잠재적 영향력을 나타내고 Confidence는 주어진 iType의 정확성에 대한 ThreatStream의 신뢰도를 나타냅니다.
- Review Existing Tag
  kill-chain: c2는 Observable이 Command & Control임을 나타냅니다.
  Malware-family: cobalt-strike는 Cobalt Strike 제품군의 C2 멀웨어임을 확인합니다.
- Relationships
  Observable간의 또는 위협 모델 개체 간의 관계를 그래픽적 관계로 만들고 보여줍니다,
- Intelligence Table
  Malware C&C IP 및 지리적 위치를 확인하는 여러 소스
- Enrichments
  강화를 통해 현재 ThreatStream에는 없지만 파트너가 제공하는 정보를 찾을 수 있습니다.
  Settings page의 Integrations Tab에서 구성 및 활성화할 수 있습니다.
  이 예에서는 VirusTotal에서 나오는 인텔리전스를 볼 수 있습니다.
- Associations
  Observable이 ThreatStream의 기존 위협 모델 개체 중 하나에 이미 연결되어 있으면 연결이 자동으로 이루어집니다.
- What Do We Do Next?
  우리는 이제 악의적인 Observable을 고려하기에 충분한 세부 정보를 얻었습니다. 다음에 수행할 작업은 내부 워크플로우 및 절차에 따라 달라지지만 복제된 Observable에서 시작하여 조사를 생성할 가능성이 높습니다. 그러나 조사 과정으로 안내하기 전에 여러 가지

ThreatStream 기능을 계속 다루어야 합니다.

Why Is the Observable Interesting for Us?

Observable 세부 정보 페이지는 우리 PC 중 하나가 C&C IP와 통신 중이므로 네트워크가 손상되었음을 나타냅니다.
강화된 기능 덕분에 우리는 Observable이 침투 테스터가 사용할 수 있는 가장 강력한 네트워크 공격 키트 중 하나를 사용하여 현대 기업에 대한 표적 공격을 실행하는 위협 에뮬레이션 소프트웨어인 Cobalt Strike와 연결되어 있음을 알았습니다.
이제 그룹 및 위협 행위자가 Cobalt Strike를 사용하여 우리 및 해당 분야와 유사한 조직을 적극적으로 대상으로 하는지 여부를 식별해야 합니다.

Review

- TRAFFIC LIGHT PROTOCAL (TLP)
  TLP 색상은 Observable 및 기타 공유 가능한 정보(위협 모델 개체, 위협 게시판, 사건)와 연관될 수 있습니다.
  TLP 색상은 이러한 정보의 추가 배포를 허용할 것인지 만약 허용한다면 얼마나 자유롭게 배포할 것인지에 대해 정보 사용자와의 통신 메커니즘을 제공합니다.
    White: 공개적으로 공유
    Green: 커뮤니티로 제한
    Amber: 제한된 공개. 참가자 조직만 해당.
    Red: 조직 내에서
  TLP 설정은 외부 조직과 정보를 공유할 때 필터 정보를 사용합니다.
- TAG
  태그는 개체를 검색 및 식별하는데 사용할 수 있는 용어입니다.
  태그는 비공개일 수 있습니다 (조직에서만 볼 수 있음)
  태깅은 위협 인텔리전스에 메타 데이터를 추가하는 빠르고 쉬운 방법입니다. 예를 들면 위협 인텔리전스가 연결된 산업을 나타내는 태그 또는 킬 체인 단계를 나타내는 태그를 추가할 수 있습니다. 또한 태깅은 Integrator를 사용하여 보안 장치에 대한 정보 배포를 자동화하는 방법일 수 있습니다.
- ENRICHMENTS
  ThreatStream 은 타사 데이터와의 통합으로 Observable 상세 페이지 또는 탐색 피벗 도구에 컨텍스트 데이터를 추가할 수 있는 강화 서비스를 제공합니다.
  설정의 통합 탭을 통해 조직 관리자가 Enrichments 를 활성화해야 합니다.
- STATUS
  Observable 은 **Active**, **Inactive** 또는 **False Positive** 상태를 갖습니다.
  ThreatStream 이 15 이하의 신뢰점수를 할당한 피드를 통해 가져온 Observable 은 자동으로 오탐으로 표시되며 반면에 ThreatStream 사용자 인터페이스를 통해 가져오고 승인된 Observable 은 ThreatStream 에서 절대 오탐으로 자동 표시되지 않습니다.

Observable을 복제하면 Observable의 개별 인스턴스가 생성됩니다.
복제된 Observable은 원래 Observable과 완전히 독립적입니다. 복제된 Observable을 가져와서 위협 인텔리전스에 추가하면 ThreatStream에 있는 다른 Observable 처럼 처리됩니다.

Analyst Tip : Why Clone Observables?

- 내부 사용을 위한 개인 복사본 Observable을 원할 수 있습니다. 복제된 Observable의 가시성은 항상 My Organization에서 설정합니다.
- 다른 조직에서 가져오기(Importing)한 비활성 Observable이 나타나고 이를 복제하면 새로운 활성화된 Observable이 생성됩니다. (정규 가져오기 프로세스를 성공적으로 이동한 후)

개인 태그를 사용하면 사용자는 Observable의 개인 복제본을 만들지 않고도 개인 정보를 Trusted Circle Observables 또는 Anomali 커뮤니티에 추가할 수 있습니다.

독점 정보가 포함된 태그를 공개 Observable에 추가하려는 경우 태그를 개인용으로 만들면 됩니다. Observable이 공개적으로 사용 가능하지만 태그는 조직의 사용자에게만 표시됩니다.

Reporting False Positives

ThreatStream에서 오탐으로 나타나고 양성이라고 생각되는 것을 리포트 할 수 있습니다.
My Organization과 Anomali Community 또는 Trusted Circle Observable 모두에 대해 수행할 수 있지만 프로세스는 약간 다릅니다. 차이점을 살펴 봅니다.

Reporting My Organization Observables as False Positive

My Organization Observables는 사용자 조직에 포함되어 Anomali의 승인이 필요하지 않으므로 My Organization Observables을 오탐으로 만들기 위해서는 Observable을 편집하고 상태를 False Positive로 변경하면 됩니다.
My Organization Observable의 상태를 False Positive로 변경하면 다운 스트림 통합에서 제거되지만 가져오기 화이트리스트에는 추가되지 않습니다.

Reporting Anomali Community or Trusted Circle Observables as False Positives

Anomali Community Observable 또는 Trusted Circle을 통해 조직과 공유된 것을 False Positive로 보고할 때는 Anomali의 승인이 필요합니다.

Analyst Tip: Communicating with Your Active Integrations

오탐에 대한 Observable Reporting은 다운 스트림 통합에서 신속하고 쉽게 제거할 수 있는 방법입니다.

- My Organization observable을 리포팅하면 이들은 화이트리스트 가져오기로 추가되지 않습니다.
- Anomali Community observable 또는 Trusted Circle을 통해 조직과 공유된 것을 리포팅하면 이들은 즉각 화이트리스트 가져오기로 추가되고 승인을 위해 Anomali로 보내집니다.

만약 오탐이 Anomali에 의해 거부되면 그것은 사용자 화이트리스트 가져오기에는 유지되나 ThreatStream에는 Active 상태로 남습니다.

Deleting Observables

ThreatStream에서 조직이 소유하고 My Organization 가시성 설정이 할당된 Observable을 삭제할 수 있습니다. 그러나 Observable을 삭제하려면 가져오기 승인 권한이 있어야 합니다.

Advanced Observable Search

고급 검색을 사용하면 쿼리에 메타 데이터를 추가하고 검색을 특정 필드로 제한할 수 있습니다. 특정 필드에서 특정 값을 검색할 때 고급 검색을 사용하십시오. 고급 검색 쿼리는 구성된 필터로 이루어집니다.

Analyst Tip: 자주 사용하는 고급 검색 쿼리를 필터로 저장

필터를 저장하면 버튼 클릭으로 일반적인 쿼리를 수행할 수 있습니다. 저장된 필터는 고급 검색 창의 검색 필터 메뉴에서 액세스할 수 있습니다.

Threat Model

ThreatStream 의 위협 모델링은 잠재적으로 관련된 위협 정보를 행위자, 캠페인, 사건, 멀웨어 등과 같은 다양한 개체로 분류합니다.
보안 전문가가 인프라에 대한 위협 영향을 방지하거나 완화하기 위한 대책을 마련할 수 있도록 데이터를 수집하고 서로 연결합니다.
특정 캠페인과 관련될 수 있는 Observable 이 특정 액터와 관련될 수도 있습니다.
ThreatStream 에서 이 관계를 확인하면 Observable 뿐만 아니라 액터 및 캠페인에 대한 보안 상태도 강화할 수 있습니다.
Anomali 위협 모델은 STIX 호환 (v1.2, v2.0 및 v2.1)이며 다음 유형의 위협 모델 개체에 대한 상황, 관계 및 워크플로우 정보 추가, 관리, 가져오기 및 내보내기를 지원합니다.

- Actor
  적의 식별 및/또는 특성화. 같은 목표를 달성하기 의해 함께 일하는 악의적인 개인 또는 그룹일 수 있습니다.
- TTP
  TTP (Tactics, Techniques and Procedures)의 약자이며, 위협 행위자가 캠페인 또는 사건을 통해 목표를 달성하기 위해 채택한 도구와 기술을 그룹화합니다.
- Incident
  특정적 행동의 단일 사례
- Campaign
  특정 대상 집합에 대해 일정 기간 동안 발생하는 일련의 악의적 활동 또는 공격을 설명하는 적대적 행동의 그룹입니다.
- Malware

악의적인 코드 및 악의적인 소프트웨어라고도 하는 TTP 유형으로, 피해자의 데이터 또는 시스템의 기밀성, 무결성 또는 가용성을 손상시키는데 사용됩니다.

- Signature
  악의적인 활동을 식별하는데 사용할 수 있는 패턴 또는 규칙 집합입니다.
- Attack Pattern
  위협 행위자가 대상을 손상시키려고 시도하는 방법을 설명하는 TTP 유형입니다.
- Course of Action
  공격을 방지하거나 공격에 대응하기 위해 취한 조치입니다.
- Identity
  개인, 조직 또는 그룹 뿐 만 아니라 개인, 조직 또는 그룹의 클래스.
  STIX 에서 ID 는 무엇보다도 공격 대상, 정보 소스, 개체 생성자 및 위협 행위자 ID 를 나타내는데 사용됩니다.
- Infrastructure
  특정 목적을 지원하기 위한 시스템, 소프트웨어 서비스 및 관련 물리 또는 가상 리소스를 설명하는 TTP 유형(예: 공격의 일부로 사용되는 C2 서버, 방어의 일부인 장치 또는 서버, 공격의 대상이 되는 데이터베이스 서버 등)
- Intrusion Set
  단일 위협 행위자에 의해 조정된 것으로 여겨지는 공통 속성을 가진 일련의 적대적 행동과 자원.
- Bulletin
  사이버 공격 및 이벤트에 대한 정보와 세부 정보를 제공하는 출판.
- Tools
  위협 행위자가 공격을 수행하는 데 사용할 수 있는 합법적인 소프트웨어.
- Vulnerability
  해커가 시스템이나 네트워크에 액세스하기 위해 직접 사용될 수 있는 소프트웨어 오류입니다.
- Hash
  멀웨어 위협 모델 개체와 관련될 수 있는 멀웨어 변종에 대한 파일 해시

위협 모델은 두 가지 방법으로 시각화될 수 있습니다.

1. **위협 모델 목록 보기** : 사용 가능한 모든 개체가 필터링 옵션과 함께 테이블에 표시됩니다.
2. **위협 모델 대시보드** : 항목은 다른 테이블에 표시되고 항목 유형별로 그룹화되어 각 유형에 대해 생성된 마지막 5 개의 개체만 표시됩니다.

Analyst Tip : 위협 모델 대시보드를 자주 방문하십시오.
대시보드는 ThreatStream 에서 가장 최근에 업데이트된 위협 모델 개체를 표시합니다. 이러한 개체에 대한 업데이트는 최근 활동을 의미하므로 해당 개체에 관심이 있을 수 있습니다.

ThreatStream 을 사용하면 고유한 위협 모델 개체를 만들 수 있습니다.
ThreatStream 의 다른 모든 데이터 유형(예: Observable, 조사 또는 샌드박스 보고서)과 마찬가지로 위협 모델 개체는 조직에 비공개로 유지하거나 회원이 속한 특정 Trusted Circles 과 공유하거나 Anomali 커뮤니티에 전부에 개체를 게시하는 3 가지 가시성 설정 중 하나를 선택할 수 있습니다. 게시되지 않은 개체는 조직 내 사용자만 볼 수 있습니다.

Analyst Tip: 위협 모델 템플릿으로 시간 절약 및 일관성 유지
조직은 여러 설명 템플릿을 설정하고 하나를 기본값으로 선택할 수 있으며 모든 위협 모델 개체 유형에 사용할 수 있습니다.

Threat Bulletin

위협 게시판은 하나의 위협 모델 개체이고 사이버 공격과 이벤트, 진화 활동 그리고 채택된 TTP 에 대한 상세한 내용과 정보를 제공하는 간행물입니다. 여기에는 연구 대상 공격자로부터 조직을 방어하는 방법에 대한 제안이 포함됩니다.

아래는 위협 게시판의 구성에 대한 예입니다.

- Intelligence Actions
    - Watch
      인텔리전스가 업데이트될 때 알림을 받습니다.
    - Star
      인텔리전스를 북마크하면 별표시 인텔리전스가 My Threats 페이지의 별표시 항목에 나타납니다.
    - Like
      해당 정보에 대한 생각을 Anomali 커뮤니티에 나타냅니다.
    - Share
      다른 ThreatStream 사용자에게 인텔리전스를 보냅니다. 인텔리전스가 공유되면 사용자는 인앱 알림을 받습니다. My Threats 페이지에서 댓글을 달거나 보거나 별표마음에 드는 인텔리전스를 추적할 수 있습니다.
- Actions
  위협 게시판에서 수행할 수 있는 작업.
- Summary
  요약에는 위협 게시판 제목, 작성자(로고 오른쪽), 상태, 날짜 및 TLP 설정과 같은 고급 정보가 포함됩니다.
- Tags
  속성에는 태그, 가시성, 캠페인, 소스, 및 TTP 가 포함될 수 있습니다.
- Description
  이 스크린샷에 표시된 위협 게시판의 전체 텍스트
- Associations

위협 게시판과 관련된 행위자, 캠페인, 가져오기 세션, 사건, 멀웨어, Observable, 샌드박스 보고서, 서명, 위협 게시판, TTP 및 취약점.

- Attachments
  위협 게시판과 관련된 외부 참조
- History
  위협 게시판을 변경하면 나중에 참조할 수 있도록 이 섹션에 변경 로그 항목이 생성됩니다.
- Comments
  위협 게시판을 보고 의견을 추가하십시오. 조직에서만 볼 수 있는 개인 설명을 추가하려면 TLP 색상을 빨간색으로 지정하십시오. TLP 색상이 흰색으로 지정된 주석은 위협 게시판에 액세스할 수 있는 모든 사용자에게 표시됩니다.

Threat Model Associations

Anomali 위협 모델은 동일한 위협 모델 유형의 개체를 포함하여 모든 위협 모델 유형의 개체 간에 **양방향** 연결을 제공합니다

Analyst Tips: 연계는 자동으로 생성되지 않음

위협 모델 개체를 서로 연결하려면 분석가(조직, Anomali 커뮤니티 또는 신뢰할 수 있는 서클 중 어느 누구든)는 둘 이상의 개체를 서로 연결해야 합니다.

Creating Threat Model Associations

위협 모델 연계는 두 가지 방법으로 달성할 수 있으며 동일한 결과를 얻습니다.

1. Import job view 로부터
2. Threat Model edit window 로부터

Importing STIX Data into the Anomali Threat Model

Import Assistant 를 사용하여 STIX 호환 데이터를 파일에서 위협 모델로 가져올 수 있습니다. ThreatStream 은 STIX 1.2, 2.0 또는 2.1 데이터 모델을 따르는 파일을 지원합니다.

Associating Observables to the MITRE ATT&CK Framework TTPs

행동 기반 위협 모델인 MITRE ATT&CK 프레임워크는 공격적인 에뮬레이션을 사용하여 관련 방어 센서를 식별하고 행동 기반 분석 탐지 기능을 구축, 테스트 및 개선하는데 사용됩니다.

이 방법론은 현재 **TTP 위협 모델**로 ThreatStream 에 통합되어 있습니다.

Exporting Threat Model Entities

Anomali 위협 모델 데이터를 다음 형식으로 내보낼 수 있습니다.

- PDF
- STIX 버전 1.2 XML

- STIX 버전 2.0 JSON
- STIX 버전 2.1 JSON

Importing Observables

What is the Import Assistant?

ThreatStream 은 다양한 소스에서 인텔리전스를 플랫폼으로 가져올 수 있는 사용하기 쉬운 마법사를 제공합니다.

Import Assistant 를 통해 **New Import** 를 시작할 수 있습니다.

New Import 페이지에서 다음 소스로부터 Observable 을 가져올 수 있습니다.
CSV, HTML, IOC, JSON, PDF, TXT, XML

가져온 데이터는 ThreatStream 의 위협 인텔리전스 일부가 되기 전에 검토되고 승인을 받아야 합니다. "가져오기 승인" 권한이 있는 사용자가 승인하면 ThreatStream 은 추가로 이를 분석하고, 주어진 지표 유형에 연계되어 있는 Observable 에 있는 신뢰성과 같은 추가 컨텍스트를 제공합니다.

사용자 계정에 승인 권한이 부여된 경우 가져오기 작업을 자동 승인할 수 있습니다.

Raw Text

데이터가 구조화되지 않은 형식인 경우 ThreatStream 플랫폼은 원시 데이터를 구문 분석하고 Observable 데이터를 추출합니다.

- ✧ **Paste Intelligence**
  187.76.140.163 robaczek@konto.pl217.228.187.74
  위의 원본 텍스트에서 하나의 이메일 주소와 두 개의 IP 주소로 세 개의 Observable 을 가져옵니다.

Plain-Text Intelligence Stream

가져오기 도우미를 사용하면 일반 텍스트 인텔리전스 스트림을 한번에 스크랩할 수 있습니다. 인텔리전스 스트림의 URL 을 제공하십시오. ThreatStream 은 URL 에 연결하고 Observable 데이터에 대한 코드를 구문 분석합니다.

Direct Links to Files

파일 업로드 외에도 온라인으로 호스팅되는 CSV, HTML, IOC, JSON, PDF, TXT 또는 XML 파일에서 가져오기 지원을 사용하여 데이터를 수집할 수 있습니다.
파일의 URL 을 제공하십시오. ThreatStream 은 URL 에 연결하고 파일을 다운로드 한 후 Observable 데이터를 구문 분석합니다. 위에 나열된 파일 형식만 지원됩니다.

STIX 1.2 Data Model XML Files

XML 파일을 가져오면 ThreatStream 은 Observable 과 위협 모델 개체 및 연계 항목을 추출합니다. 그런 다음 STIX 가져오기 프로세스는 모든 Observable 에 대해 Observable 가져오기 세션을 생성합니다.

Emails

ThreatStream 은 또한 자유 형식 이메일에서 Observable 을 가져올 수 있습니다. 하나 이상의 Observable 이 포함된 이메일을 ThreatStream 에서 제공한 지정된 이메일 주소로 전달하기만 하면 됩니다. ThreatStream 은 수신된 이메일을 구문 분석하고 이메일에서 Observable 을 추출한 다음 가져오기 작업을 생성합니다.

Importing Observables from an Email

이메일을 통해 Observable 을 배포하는 것은 서로를 신뢰하지만 현재 공식적인 공유 방법이 없는 팀과 조직 (예: 신뢰할 수 있는 서클) 간에 인텔을 공유하는 가장 빠르고 쉬운 방법입니다.

ThreatStream 은 이메일 본문에 포함된 Observable 을 수집할 수 있으며 가장 중요한 것은 ThreatStream 에 연결하거나 로그인할 필요가 없다는 것입니다.

ThreatStream 에서 제공하는 이메일 및 이메일 주소가(수신자로 작동) 필요합니다.

- ✓ 또한 PDF, TXT 또는 CSV 첨부 파일로 Observable 을 이메일로 보낼 수도 있습니다.

ThreatStream 메일박스에서 이메일을 받으면 본문에 포함된 Observable 을 ThreatStream 에서 검증하고 구문 분석합니다.
프로세스가 성공하면 유효한 모든 IOC 를 포함하는 Import Job 이 생성됩니다.

- ✓ 프라이버시가 걱정됩니까?
  Observable 가져오기를 위해 ThreatStream 에 수신된 이메일은 플랫폼에 저장되지 않습니다. Observable 이 추출되면 이메일이 삭제됩니다.

Using Streams

스트림 페이지를 사용하면 다음을 할 수 있습니다:

- 현재 피딩되는 위협 인텔리전스를 봅니다.
- 조직에서 액세스 할 수 있는 새 스트림을 제출합니다.
- 이전에 제출된 스트림을 편집합니다.

Analyst Tip: **효과적인 검색 필터링을 위해 인텔리전스 소스 사용을 시작하십시오.**
import_source 필드를 사용하여 조직에서 가져온 Observable 에 대한 인텔리전스 소스를 기반으로 고급 검색 필터를 생성할 수 있습니다.

Analyzing Suspicious Data

분석가 및 조직에 대한 ThreatStreams 의 장점 중 하나는 사용의 용이성, 파일, URL, 이메일과 IOC 의 빠른 분석 및 상관 관계입니다.

Viewing Attacks with Sightings

Sightings 은 ThreatStream 에서 구성한 통합 대상의 공격 데이터를 표시하는 그래픽 위젯 입니다. Sightings 을 사용하면 인프라에 영향을 주는 Observable 과 ThreatStream 커뮤니티의 다른 조직과 비교하는 방법을 명확하게 이해할 수 있습니다.

ThreatStream 에서 통합 대상의 데이터를 Observable 에 사용할 수 있으면 Observable 세부 정보 페이지에 Sightings 가 표시됩니다. Observable 에 대한 Sightings 데이터를 수동으로 추가할 수도 있습니다. 위젯은 Observable 에서 이전 30 일 동안의 데이터를 표시합니다.

Sightings 에 표시되는 Observable 일치 항목은 **세가지** 범주로 분류됩니다.

1. Other Organizations
   내 조직이 아닌 다른 ThreatStream 조직이 보고한 Observable 일치 항목입니다. 다른 조직의 데이터는 익명이며 개인 식별 정보가 제거됩니다.
2. My Organization
   내 조직과 다른 ThreatStream 조직에서 보고한 Observable 일치 항목입니다.
3. Unique to my Organization
   내 조직에서만 보고한 Observable 일치 항목입니다.

Sending Attack Data to ThreatStream

Sightings 는 통합 대상에서 ThreatStream 으로 전송된 데이터를 사용합니다.
ThreatStream 에서 데이터를 수신할 수 있게 하려면 통합 대상에서 다음 설정을 구성해야 합니다.

- ArcSight ESM
  ThreatStream Integrator 에서 **Enable My Attacks** 설정이 되어야 합니다.
- Splunk - via ThreatStream Integrator
  ThreatStream Integrator 를 통해 ThreatStream 에서 데이터를 받는 사용자는 Splunk 에서 **ThreatStream Autotune Report** 를 활성화해야 합니다.
- Splunk App
  Splunk App 에 의해 ThreatStream 에서 직접 데이터를 받는 사용자는 추가 구성이 필요 없습니다. ThreatStream Autotune Report 가 기본으로 활성화되어 있습니다.

Analyzing Suspicious Files and URLs Using a Sandbox

멀웨어 분석은 수동으로 수행할 때 시간이 오래 걸리고 리소스 집약적인 프로세스일 수 있습니다. 또한 기본 시스템에서 소프트웨어 및 데이터를 보유하는 멀웨어를 분석하면 해당

시스템을 손상시킬 수 있습니다. 샌드박스는 기본 시스템을 손상시키지 않으면서 멀웨어를 실행하고 결과를 검토할 수 있는 외딴 환경을 제공합니다.

ThreatStream 은 멀웨어(파일 또는 URL)를 자동으로 분석하고 결과에 대한 자세한 보고서를 생성할 수 있는 **호스팅된 샌드박스**를 제공합니다 . 이 보고서를 사용하여 조직에 대한 특정 멀웨어의 심각성과 영향을 확인할 수 있습니다. 위협 분석에 샌드박스를 사용하면 조직에 심각한 영향을 줄 수 있는 멀웨어 샘플에만 노력을 집중할 수 있으므로 시간과 리소스가 절약됩니다.

Joe Sandbox

ThreatStream 은 **추가 비용** 없이 모든 **프리미엄** 고객에게 Joe Sandbox 를 제공합니다.

이 설정은 **조직 관리자**가 활성화해야 하며 CSM 은 조직에 액세스 권한이 있는지 확인할 수 있습니다. 활성화되면 Joe Sandbox 를 사용하여 모든 Sandbox 폭발이 수행됩니다.

비밀번호로 보호된 아카이브 파일(예: **.zip**, **.rar** 또는 **.7z)**을 제출할 수 있습니다. 비밀번호는 문자를 포함하고 제출 시 사용자 인터페이스에서 비밀번호를 지정하여 Joe Sandbox 에 전달하십시오.

또한 Joe Sandbox 는 사용자가 ThreatStream 에 비밀번호를 입력하지 않을 때 제출되는 비밀번호로 보호된 아카이브에 대해 **감염된** 기본 비밀번호를 사용합니다.

Joe Sandbox via Individual Subscription

별도의 Joe Sandbox 구독을 이미 보유한 경우 **조직 관리자**는 **Integrations Tabs 을** 통해 ThreatStream 에서 활성화할 수 있습니다.
이 경우 ThreatStream 사용자는 Joe Sandbox(제공된 자격 증명 사용) 또는 기본 ThreatStream Sandbox 중 하나를 사용하여 폭발을 수행하는데 사용할 샌드박스를 선택할 수 있습니다.

Default ThreatStream Sandbox

또한 ThreatStream 은 멀웨어 폭발을 위해 **Windows XP** 및 **Windows 7** 플랫폼을 지원하는 기본 샌드박스 서비스와 통합되어 있습니다.

이 샌드박스 서비스는 모든 고객이 사용할 수 있지만 기본 샌드박스의 현재 Windows XP 시스템에는 Microsoft Office 가 설치되어 있지 않습니다.

- ✓ **NOTE**: 샌드박스 폭발이 완료되고 검토 준비가 완료되는 데 최대 20 분이 소요될 수 있습니다.

Using the Sandbox to Analyze Phishing Emails

귀하(또는 귀하의 조직의 구성원)가 의심스러운 이메일을 받았으며 이에 대해 더 자세히 알고 싶다고 생각합니다. 아마도 대량 피싱 캠페인의 희생자 중 한 명일 것입니다. 액터가 조직을 목표로 하고 있습니다.

컴퓨터를 감염시킬 위험 없이 이메일을 검사하기 위해 무엇을 할 수 있습니까?

ThreatStream 은 메일박스 설정에 의해 피싱 이메일을 수집하고 분석을 위해 샌드박스로 링크하고 첨부하여 보낼 수 있습니다.

Working with Sandbox Detonation Reports

ThreatStream 에 대한 일반적인 샌드박스 분석 보고서는 다음 정보를 제공합니다.

- 멀웨어를 폭파하기 위해 취한 단계의 슬라이드 쇼
- 악성 코드의 세부 사항 및 서명.
- 악성 코드의 네트워크 및 행동 분석.
- 보고서가 Anomali 커뮤니티인지 또는 내 조직인지와 같은 샌드박스 작업에 대한 기타 세부 사항.
- 악성 코드를 폭파하는데 사용된 샌드박스 사이트에서 분석 보고서를 얻을 수 있는 링크입니다.

✓ 멀웨어를 폭파할 때 Import Indicators 를 선택하면 "Suspicious"또는 "Malicious"으로 표시된 멀웨어에 대한 가져오기 세션이 자동으로 생성됩니다.
이 세션을 사용하여 악성 감시 대상을 ThreatStream 으로 가져올 수 있습니다.
"Benign"으로 분류된 멀웨어의 경우 가져오기 세션이 생성되지 않습니다.

Understanding a Sandbox Report

샌드박스 폭발 보고서를 읽고 완전히 이해하려면 네트워킹, 사이버 보안, 운영 체제에 대한 지식이 있어야 하며 리버스 멀웨어에 대한 경험이 있으면 도움이 됩니다.

그러나 ThreatStream 에서 사용할 수 있는 보고서를 익히기 위한 몇 가지 기본 단계를 다음과 같이 설명할 수 있습니다.

- Step 1: Malicious?
  제출된 **파일**, **URL** 또는 **이메일**이 왼쪽 상단에서 악성으로 발견된 경우 모든 샌드박스 보고서에 표시됩니다.
  여기서부터 시작하는 것이 좋습니다.
- Step 2: Look at the Dropped Files
  컴퓨터에서 어떤 파일이 다운로드(시도)되었는지 이해하는 것은 멀웨어 동작 및 동작을 이해하기 위한 두 번째 단계입니다.
  삭제된 파일 영역에서 다운로드된 파일에 연결된 해시를 검색할 수도 있습니다.
- Step 3: Review the Step-By-Step Screenshots

파일이 다운로드 및 실행되었는지 확인하는 또 다른 방법은 샌드박스가 촬영하고 사용할 수 있는 단계별 스크린샷을 보는 것입니다.

- Step 4: Signatures
  시그니처는 색상으로 구분되어 있으며 (녹색=안전, 파란색=의심, 빨간색=악성) 멀웨어의 동작에 대한 자세한 정보를 제공합니다.
  멀웨어가 실행되면 Windows 폴더 내에 자체 복사본을 생성하고 원래 다운로드 한 파일을 삭제합니다.
- Step 5: Network Analysis
  DNS 가 해결되는 위치와 HTTP 요청이 있는지 확인하는데 유용합니다.
  PCAP (Packet Capture)를 열고 분석하기 위하여 다운로드 하는 것도 유용합니다.
- Step 6: Behavior Analysis
  동작 분석 탭에는 파일, 레지스트리 키 편집 및 뮤텍스와 관련된 멀웨어가 수행하는 모든 작업에 대한 자세한 정보가 표시됩니다.

Analysis Tip:
링크나 파일이 악의적이라는 사실을 알고 있더라도 샌드박스 분석을 제출하면 악성 프로그램의 행위를 수동으로 분석하는 대신 네트워킹 표시 및 삭제된 파일의 획득을 가속화하므로 여전히 유용할 수 있습니다.

Building out an Attack Infrastructure Map Using Explore

ThreatStream 에는 분석가가 IOC 를 수동으로 교차하지 않고도 분석가가 Observable 개체 간의 관계를 파악하여 인프라를 공격하는 적에 대한 종합적인 맵을 생성할 수 있는 탐색이라고 불리는 도구가 제공됩니다.
ThreatStream 의 **탐색** 기능을 사용하면 행위자, 기타 Observable 과 같이 관련이 있는 것으로 알려진 데이터와의 관계를 **시각적으로 표현**하고 플랫폼을 벗어나 수동으로 작업할 필요 없이 파트너의 데이터로 ThreatStream 인텔리전스를 강화할 수 있습니다.
탐색을 통해 사용자는 적의 공격 인프라에 대한 포괄적인 맵을 구축할 수 있습니다.

Investigations in ThreatStream

인프라에서 악성 IP 주소를 찾았으므로 이제 사건을 조사할 차례입니다.

ThreatStream 의 조사 기능은 협력적이고 유연한 작업 공간으로 일상의 작업을 수행하여 적의 공격을 조사하고 대응할 수 있습니다.

조사를 통해 다음을 수행할 수 있습니다.

- 데이터를 피봇하여 연계를 이해합니다.
- 사용자 또는 작업 그룹에 작업을 할당하고 완료를 추적합니다.
- 위협 모델 개체로 조사내용을 컴파일 합니다.

Creating a New Investigation

조사는 여러 가지 방법으로 만들 수 있습니다..

- User Created
- Fishing Ingest
- Rules Generated Investigations

Already Imported Observables vs Not Imported Observables

업로드된 파일에서 구문 분석되었거나 단순히 탐색 그래픽 도구에 추가된 모든 Observable 이 새로운 조사에 포함됩니다.

- IOC 가 ThreatStream 에 이미 있는 경우, Already Imported Observables 로서 조사에 추가됩니다.
- Observable 이 처음인 경우 사용자는 사용자 인터페이스를 통해 가져올 수 있습니다.

Graphical Tool

조사 UI 에는 온 보드 버전의 탐색 피벗 도구가 장착되어 있습니다.

데이터(노드)가 탐색 차트에 추가되면 해당 데이터도 조사에 추가되고 개체 테이블 보기에서 사용할 수 있게 됩니다.

탐색 모음에서 직접 액세스할 수 있는 탐색 도구와 비교하여 이 버전에서는 다음을 수행할 수 있습니다.

- Browse Observable
  포괄적인 검색 기능을 사용하여 **Observables** 또는 위협 모델 개체를 조사에 추가합니다.
- Add All
  검색 결과에 표시된 모든 개체를 조사에 추가합니다.

The Table View

개체 관리에 사용되며 조사에 포함된 모든 개체를 표시합니다.

Analysis

알려진 데이터의 경우 분석 탭에서 아이콘을 클릭하여 분석으로 개체에 컨택스트 정보를 추가할 수 있습니다.

Models

ThreatStream 의 조사 UI 를 통해 사용자는 조사에 추가된 개체를 표로 시각화하거나 침입 분석에 사용 가능한 세 가지 모델 중 하나를 사용하여 지능을 컨택스트화 할 수 있습니다.

TIP 에서 지표 및 기타 개체가 소비되면 퍼즐 조각과 같습니다. 이것들은 다른 지표나 개체(위협 리포트를 제외한)들과 항상 상호 연결되어 있지는 않습니다. 지표들과 개체들 사이의 연결을 보여주기 위해 이 조각들을 한데 모으는 작업이 분석가들의 작업입니다.

최종 결과는 잠재적 또는 실제 위협 또는 적의 전반적인 상황을 보여줍니다.

Diamond Model

알려진 인프라에서 희생자를 대상으로 사용되는 공격자와 알려진 기능을 설명하는 간단한 모델입니다.

STIX Model

STIX 는 TAXII (Trusted Automated Exchange of Intelligence)를 통해 공유될 수 있는 위협 인텔리전스를 구조화하기 위해 사용되는 산업 표준입니다.

Kill Chain Model

"사이버 킬 체인" (Cyber Kill Chain)은 공격자가 조직에 해를 입히는데 필요한 활동을 수행하는 방법을 이해하기 위해 업계에서 인정된 방법입니다.

- ✓ ThreatStream 에서 개체는 STIX 모델에 자동으로 지정됩니다.
  다이아몬드 또는 킬 체인 모델에서 개체를 보려면 킬 체인 단계 또는 다이아몬드 특성을 할당해야 합니다.

Tasks

ThreatStream 의 조사는 특정 사용자 및 작업 그룹에 작업을 할당할 수 있도록 지원하며 마감일 및 알람과 연계될 수 있습니다.

Exporting Investigations

조사가 완료되면 ThreatStream 커뮤니티에 다음 중 하나로 내보내서 배포할 수 있습니다.

- 액터
- 캠페인
- 사건
- 멀웨어
- 위협 게시판
- TTP
- 취약성

조사를 내보내면 모든 첨부 파일과 연계된 개체가 위협 모델 개체 결과에 포함됩니다. 분석에 첨부된 파일은 포함되지 않습니다.
내보내기 후 개체 결과는 하나의 연계로 조사에 추가됩니다.

또한 조사에 가져오지 않은 Observable 로 나열된 모든 Observable 에 대해 가져오기 세션이 시작됩니다. 조사에 할당된 TLP 색상은 가져오기 세션에 자동으로 적용됩니다.

Automation with Rules

ThreatStream 에 규칙을 구성하면 새로 생성된 인텔리전스에 특정 키워드가 나타날 때 자동 작업을 수행할 수 있습니다.

Rules Dashboard

- Filters
  다음과 같은 목록의 규칙을 필터링합니다.
  - Matched within
  - 조사
  - 업데이트 날짜
  - 생성 날짜
- Search Rules Bar
  키워드로 규칙을 검색하는데 사용합니다.
  - Rule Name
  - Description
  - Tags
- Actions Button
  사용자가 할 수 있는 작업
  - 새로 만들기: 새 규칙을 구성합니다.
  - 편집: 선택한 규칙을 편집합니다.
  - 선택한 항목 제거: 선택한 규칙을 제거합니다.
  - 내보내기: 구성된 규칙을 CSV 형태로 내보냅니다.

  선택된 편집 및 제거는 사용자가 하나 이상의 규칙을 선택한 경우에만 표시됩니다.
- Rules
  조직의 모든 현재 규칙에 대한 표 보기

Configuring Rules

ThreatStream 에 규칙을 구성하면 새로 생성된 위협 게시판, 샌드박스 보고서, 서명, 취약성 또는 최근에 가져온 Observable 에 특정 키워드가 나타날 때 자동 작업을 수행할 수 있습니다.

- ✓ 단일 규칙은 최대 100 개의 고유 키워드를 포함할 수 있으며 조직은 최대 300 개의 규칙을 구성할 수 있습니다.

- **Enable Email Domain Monitoring**
  전제 조건: 조직 소유 이메일 도메인 목록을 수집하십시오.
- **Enable Compromised VIP Email Monitoring**
  전제 조건: 조직의 VIP 이메일 주소 목록을 수집하십시오.
- **Industry Specific Keywords**
  전제 조건: 조직의 자체 식별 산업 수직계열 키워드 목록을 수집하십시오.
- **Enable Partner and Supplier Domain Monitoring**
  전제 조건: 조직 파트너 및 공급 업체 이메일 도메인 목록을 수집하십시오.

The Power of Intel Sharing

사이버 보안에서 동료 및 산업 그룹 간의 협력을 촉진하는 것이 표준이 되었습니다. 매일 엄청난 양의 데이터를 처리하고 세계 곳곳에서 새롭게 등장하는 위협이 발견되면서 인텔을 공유하면 조직의 시간과 궁극적으로 많은 돈을 절약할 수 있습니다.

Unidirectional vs. Bidirectional Sharing

위협 인텔리전스 공유는 여러 가지 형태로 제공됩니다.
가장 일반적인 버전은 단 방향 위협 인텔리전스 공유입니다. 여기서 한 기업은 다른 기업이 소비하는 위협 인텔리전스를 생성하고 공유합니다. 정보를 "푸시"하는 메커니즘이 없기 때문에 정보를 소비하는 사람들은 그 대가로 기여하지 않습니다. 단 방향 위협 인텔리전스 공유의 예는 다음과 같습니다.

- **공개 소스** 인텔리전스. 여기에는 사용된 지표 및 방법이 포함된 최근 공격에 대한 공개 보고서를 다운로드 하거나 공개 소스 인텔리전스 피드를 수집하는 것이 포함될 수 있습니다.
- **비공개 소스** 보고서 및 피드

조직의 다른 옵션은 **양방향** 위협 인텔리전스 공유에 참여하는 것입니다. 대부분의 조직에서 이러한 종류의 공유에 대한 초기 경험은 업계 **ISAC 또는 정부 공유 프로그램에** 참여했을 때 나타났습니다.

이러한 상태에서 정보는 소비되기 위해 내려 보내지는 것만이 아니라 회원 조직에서 수집될 수도 있습니다.

이러한 프로그램에서 공유가 허용되고 권장되지만 모든 조직이 이전에 언급한 것처럼 공유한다는 보장은 없습니다.
이들은 소비자이지만 위협 인텔리전스의 공유자는 아닙니다.

Where to Start or Expand Intelligence Sharing

조직에서 이미 적극적으로 인텔리전스를 공유하고 있거나 아직 시작하지 않은 경우 아래에서 시작하는 위치 또는 이미 진행중인 공유를 향상시키는 방법에 대한 몇 가지 팁을 찾을 수 있습니다.

- TOOLS AND COMMUNITIES

  이메일은 가장 쉬운 시작이지만 **STIX** 및 **TAXII** 와 같은 표준을 활용할 수 있는 도구를 통해 보다 공식적인 공유 방법으로 이동하는데 중점을 둡니다..

  ISAC 및 기타 산업 조직은 인텔리전스 공유를 시작하기에 완벽한 **커뮤니티**이며 일반적으로 그렇게 하는 메커니즘을 갖추고 있습니다.

  다른 산업 분야의 현지 기관 또는 파트너와의 임시 공유는 처음에는 공식적이지 않지만 표준 도구와 공유 메커니즘을 활용하기 위해 노력합니다.

  Anomali ThreatStream 사용자는 이미 다른 조직과 지표 및 기타 인텔리전스를 공유하거나 자체 공유 커뮤니티를 만들 수 있는 매우 강력한 솔루션을 보유하고 있습니다.

- SHARE AND CONTRIBUTE

  이것은 분명한 것처럼 들릴 수 있지만 공유 파트너쉽이 확립되면 실제로 공유에 기여해야 합니다.

  다른 당사자와 공유한 인텔리전스에 컨텍스트를 추가하고, 관찰된 적의 행동, 공격 또는 사건 대응의 세부 정보를 공유하십시오.

- SHARE OUTSIDE YOUR VERTICAL

  ISAC, 법률 및 이 주제에 대한 정부의 노력 덕분에 외부 단체와의 공유 아이디어가 조직에서 점점 더 수용되고 있습니다. 이러한 수용을 활용하여 업계의 수직 및 정부 외부의 기관과 신뢰를 구축하고 관계를 공유하면 성공을 거둘 수 있습니다.

  현지화된 개체를 포함하여 업종 외부의 조직과 공유할 기회를 찾으십시오.

- SHARING WITH VENDOR

  인텔리전스을 공유하고 그들에게 다가가는데 도움이 될 수 있는 일부 잠재적 벤더를 고려하십시오. 조직에서 정보를 수집할 수 있는 메커니즘이 반드시 필요한 것은 아니지만 공유 계약에 도달할 경우 무엇을 시작해야 하는지 알 수 있습니다.

- SHARE DEFENCE TECHNIQUES

  지금까지 인텔리전스는 정보 공유에 중점을 두었지만 다른 항목도 공유할 것을 고려하십시오.

  유용하고 가치 있는 특정 로그 항목으로 입증된 검색 및 기타 관련 세부 정보와 같은 위협 사냥 세부 정보는 다른 조직의 사냥 노력에서 지름길로 바뀔 수 있습니다. 또한 YARA 규칙, 스너트 서명, Bro 규칙, 스크립트 및 조직 간에 쉽게 복제할 수 있는 모든 항목과 같은 성공적인 방어 기술 또는 규칙을 공유합니다.

- SHARE BREACH DETAIL

  이것이 제공하는 것은 관련된 모든 당사자에게 다양한 잠재적 혜택입니다.

  위반 세부 정보를 신속하게 공개하면 다른 사람이 위반을 미리 막을 수 있습니다. 또한 다른 조직의 기술과 전문 지식을 이벤트에 추가함으로써 추가 인텔리전스 측면에서 많은 지원을 제공하고 사고 대응 문제에 대한 빠른 답변을 얻을 수 있습니다.

✓ "The Definitive Guide to Sharing Threat Intelligence"에서 발췌

Participating in the Anomali Community

ThreatStream 을 사용하면 조직 외부의 사용자를 포함하여 더 넓은 Anomali 커뮤니티와 교류하고 최신 상태를 유지할 수 있습니다.
고유한 사용자 프로필을 만든 후 다음을 수행할 수 있습니다.

1. 위협 모델 개체 및 샌드박스 보고서를 보고 별표시합니다.
2. 위협 모델 개체 및 샌드박스 보고서를 추적합니다.
3. 개별 ThreatStream 사용자와 정보를 공유하십시오.
4. Anomali 커뮤니티의 인텔리전스 트랜드를 보십시오.

Watch, Star, and Like Threat Model entities and Sandbox Reports.

ThreatStream 는 폭넓은 Anomali 커뮤니티와 인텔리전스를 추적, 평가 및 공유할 목적으로 위협 모델 개체, 샌드박스 보고서에 **Watch, Star, Like** 및 **Share** 를 할 수 있게 합니다.

내 위협 페이지에서 위협 모델 개체 및 샌드박스 보고서를 추적하십시오.

커뮤니티 위협 페이지에서 Anomali 커뮤니티의 인텔리전스 트랜드를 보십시오.

Trusted Circles

신뢰할 수 있는 서클은 표준화된 형식으로 위협 인텔리전스를 공유하고 수신할 수 있습니다. 이는 한 가지 형식의 위협 인텔리전스로 표준화된 조직에 유연성을 제공합니다.

신뢰할 수 있는 서클은 ThreatStream 내의 커뮤니티로, 참여하여 위협 인텔리전스를 실시간으로 공유하고 다른 사람이 공유한 정보에 액세스할 수 있습니다.

풍부한 정보를 공유하려는 최종 목표를 달성하기 위해 다음과 같은 유사한 배경을 가진 조직을 포함하는 신뢰할 수 있는 서클을 만드는 것이 좋습니다.
산업, 위치, 공급체인, 정치적 적대세력

And, How Does It Work?

신뢰할 수 있는 서클은 독립적인 데이터 피드 역할을 합니다. ThreatStream 은 두 종류의 신뢰할 수 있는 서클을 허용합니다.

- Public
  이 신뢰할 수 있는 써클의 이름은 모든 조직에서 볼 수 있습니다. 모든 조직은 이 서클에 초대를 요청할 수 있습니다.
  조직이 해당 서클에 참여하려면 먼저 Trusted Circle 소유자가 요청을 승인해야 합니다.
  공개 신뢰할 수 있는 서클은 ThreatStream 내의 Public Trusted Circles 표에 나열됩니다.
- Non-Public

비공개 신뢰할 수 있는 서클의 이름은 모든 조직에 표시되지는 않지만 서클을 만든 조직의 구성원과 명시적으로 초대된 다른 조직만 볼 수 있습니다. 조직이 이러한 서클에 참여하는 경우 신뢰할 수 있는 서클 표에 나열됩니다.

STIX TAXII

ThreatStream 과 TAXII 서버 간의 양방향 데이터 교환을 활용하여 ThreatStream 에서 인텔리전스를 다운로드(**폴링**이라고도 함)하고 기존 TAXII 서버 사이트로 수집물을 **푸시**할 수 있습니다.

또한 ThreatStream 은 TAXII 서버로 작동할 수도 있습니다. TreatStream 의 내장된 이중 기능을 통해 TAXII 서버 및 클라이언트 역할을 동시에 수행합니다.

STIX TAXII 를 사용하여 몇 가지 방법으로 보안 방안을 개선하는 것을 목표로 합니다.

- 현재 위협 인텔리전스 공유 역량을 확장하십시오.
- 사전 탐지 기능으로 균형 잡힌 반응.
- 위협 인텔리전스에 대한 전체적인 접근 방식을 권장하십시오.

TAXII 클라이언트와 서버는 요청-응답 모델로 정보를 교환합니다.

Using ThreatStream as a TAXII Client

ThreatStream 을 TAXII 클라이언트로 사용하면 TAXII 서버에서 TAXII 데이터를 집계하여 ThreatStream 에서 이미 수신중인 인텔리전스에 추가하고 TAXII 데이터를 서버로 푸시할 수 있습니다.

간단히 말해서, ThreatStream 은 TAXII 서버로(또는 서버로부터) 정보를 요청(또는 푸시)합니다. 정보는 STIX 형식이어야 합니다.

TAXII 서버는 보통 인텔리전스를 컬렉션으로 체계화합니다. 컬렉션은 생산자가 소비자에 의해 요청될 수 있는 CTI 데이터 세트를 호스트할 수 있도록 하는 TAXII 서버에 의해 제공되는 CTI 오브젝트의 논리 저장소에 대한 인터페이스입니다.

서버는 컬렉션을 사용하여 특정 신뢰 그룹의 요구를 지원하기 위해 인텔리전스를 그룹화합니다.

Using ThreatStream as a TAXII Server

ThreatStream 을 TAXII Server 로 사용하면 당신의 플랫폼에서 TAXII 클라이언트로 데이터를 폴링하여 선택한 인텔리전스를 빠르고 쉽고 안전하게 공유할 수 있습니다.

ThreatStream 은 TAXII 클라이언트에서 ThreatStream 에 연결하는데 사용할 수 있는 두 개의 TAXII Discovery URL (TAXII v1.x 형식의 데이터를 푸시하기 위한 URL 과 TAXII v2.0 용)을 제공합니다.

TAXII 클라이언트에서 UR 에 연결하면 ThreatStream TAXII 피드(TAXII 데이터 교환을 위한 전용 채널)가 폴링 데이터에 사용 가능한 콜렉션으로 나타납니다.

끝

본 자료는 Anomali University 의 Course 1 ThreatStream End User 101 의 내용을 요약한 것으로써 더 자세한 내용을 알고 싶으신 경우는 아래로 연락하여 주시기 바랍니다.

연락처 : ㈜한국밸런스 영업대표 김 형덕 (010-7138-8889, hdkim@valence.co.kr)