Anomali Threat Stream

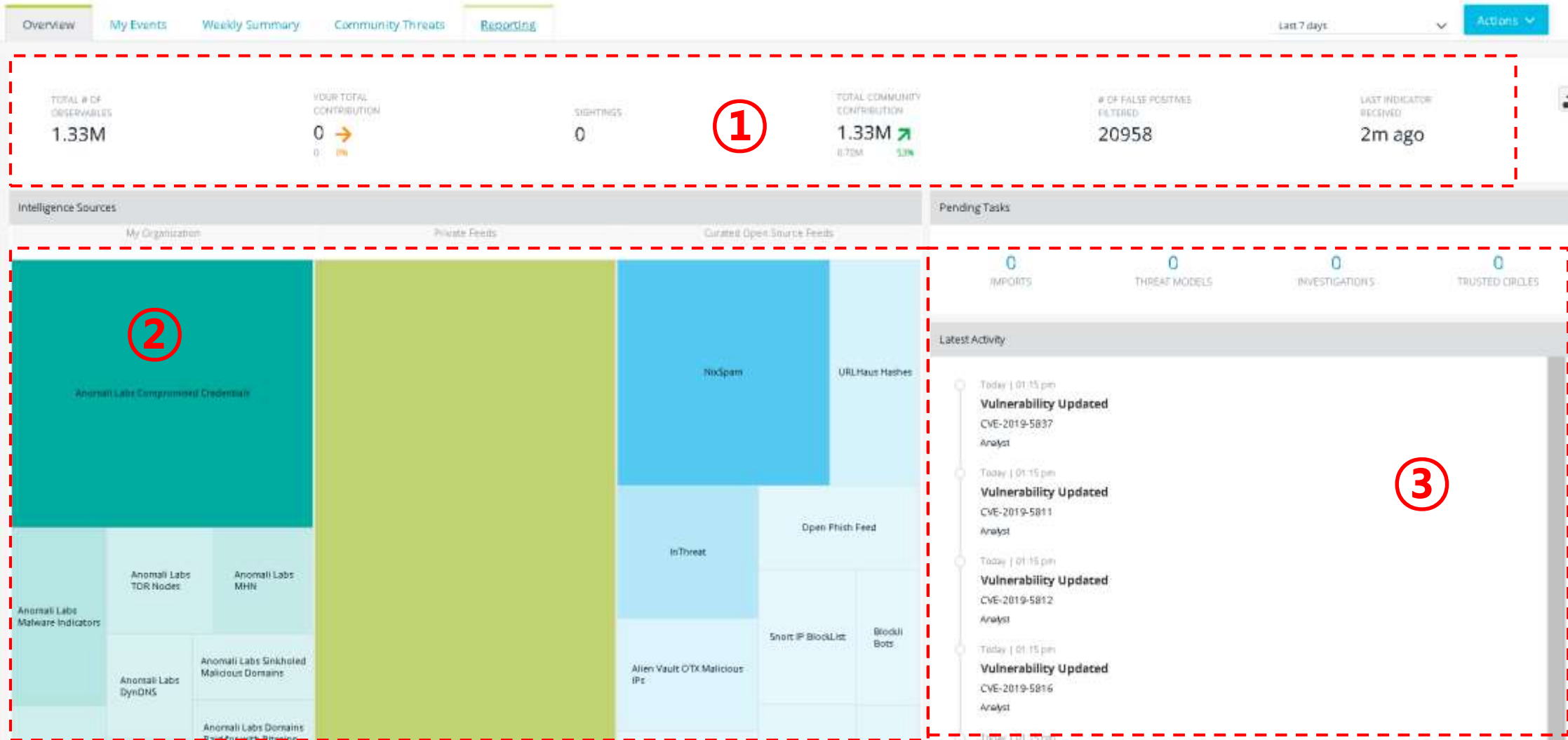
Detail Function

1. Threat Intelligence 정보 제공
2. Threat Intelligence 정보 검색
3. SIEM 과의 연동
4. Offline 용 TI 정보 제공 플랫폼(Air gap)
5. 기타 제공 서비스

1. Threat Intelligence 정보 제공

- TI source 수집 현황 및 각종 신규 취약점 정보 실시간 업데이트

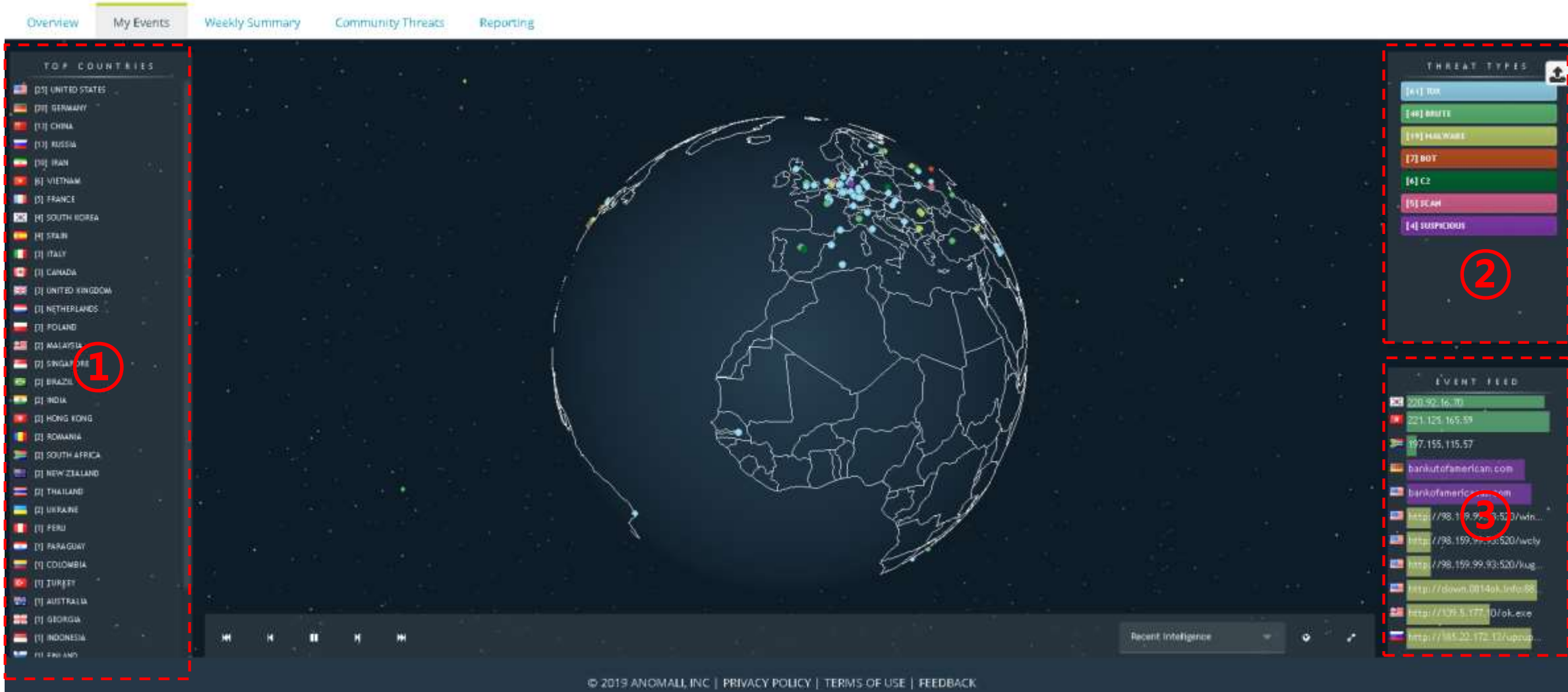
①TI source 별 수집 현황
②실시간 취약점 수집 현황
③My Feeds 현황



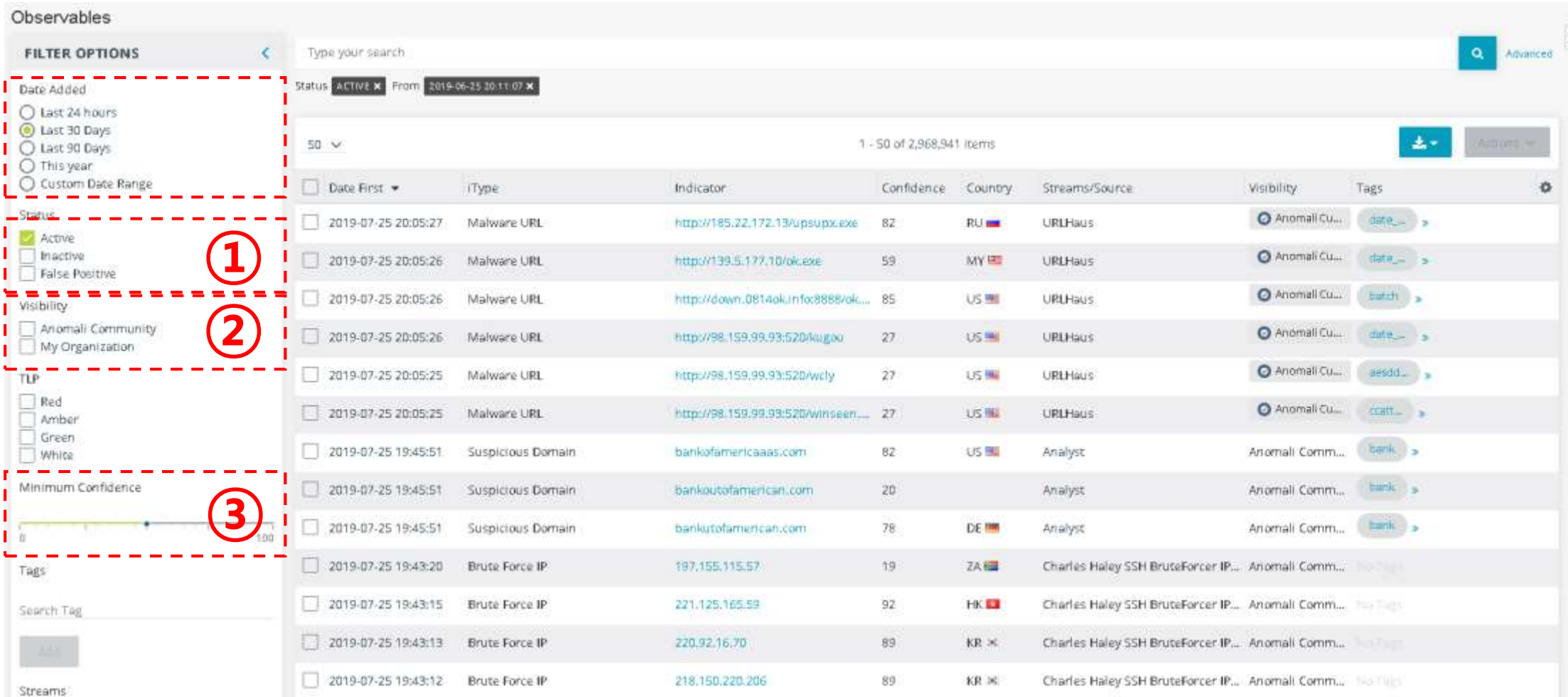
1. Threat Intelligence 정보 제공

- TI source 수집 현황 및 각종 신규 취약점 정보 실시간 업데이트

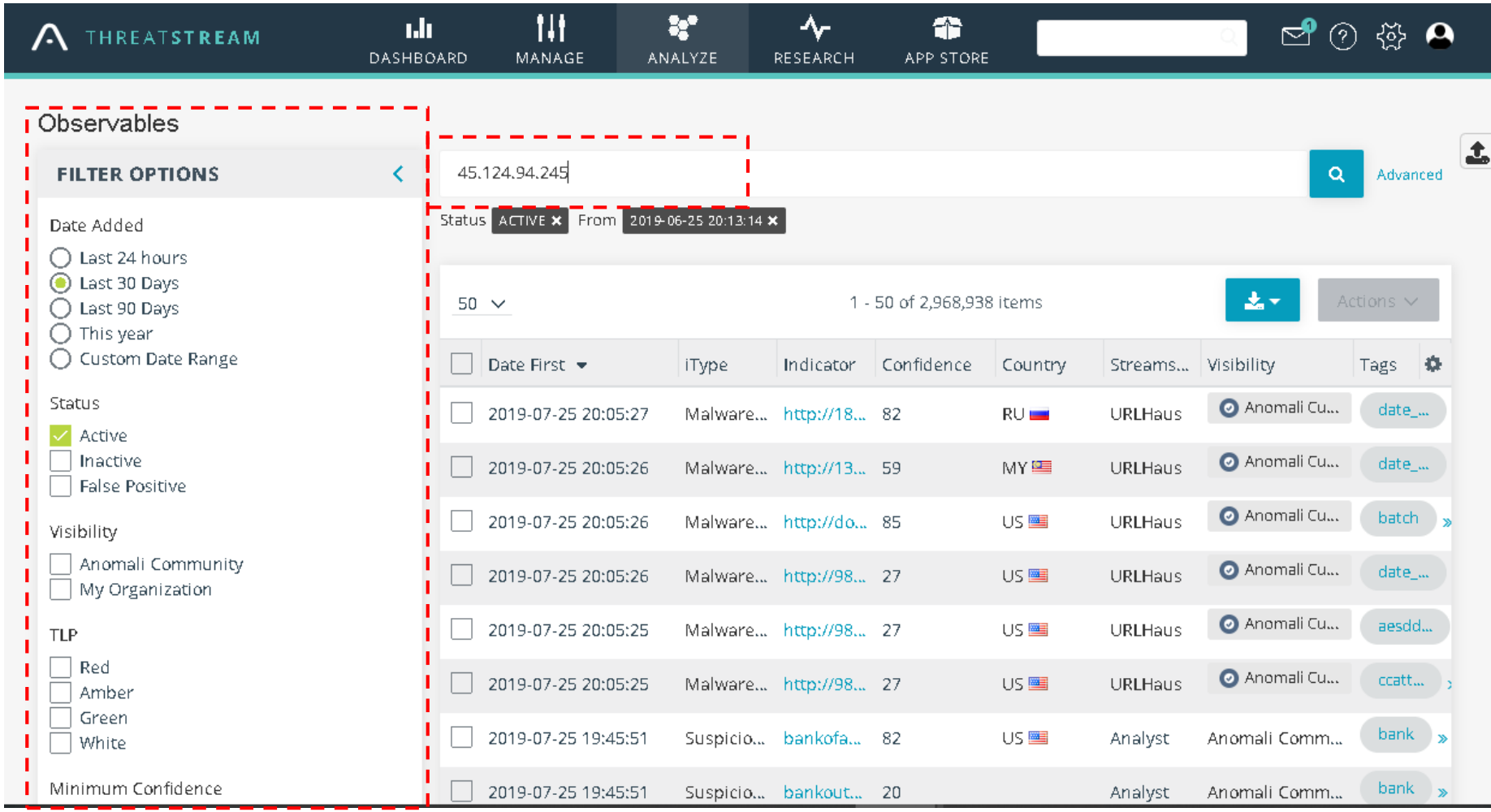
①국가별 TI source 수집 현황
②Threat Type별 수집 현황
③국가별 Threat Event 수집 현황



1. Threat Intelligence 정보 제공
   - TI source 수집 현황 및 각종 신규 취약점 정보 실시간 업데이트
     ① Active OR Non-Active
     ② TI source 별 검색
     ③ Confidence 별 검색 조건
     ④ URL, IP 등 다양한 TI정보 및 source 별 검색

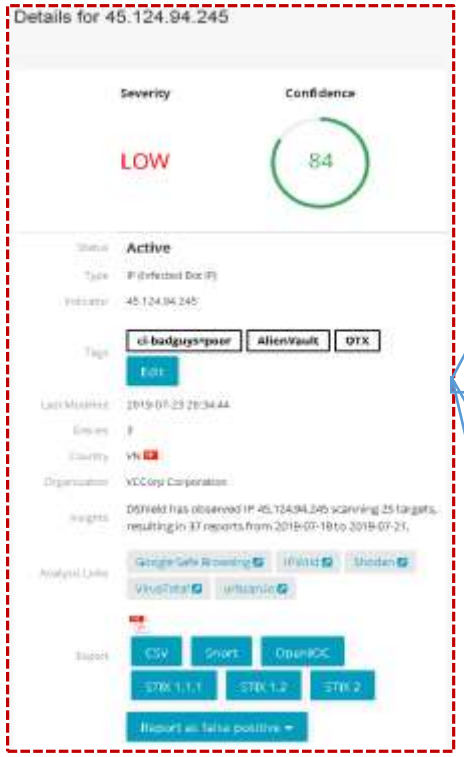


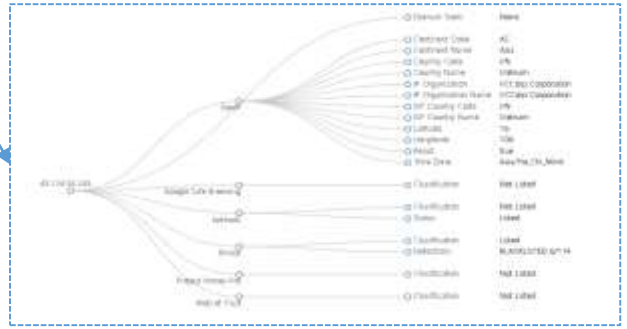
2. Threat Intelligence 정보 검색
   - 실시간 업데이트되는 TI정보 검색
   ① 기간별 조건
   ② Active OR Non-Active 조건
   ③ TI source 별 조건
   ④ Confidence 별 조건
   ⑤ URL, IP 등 다양한 TI정보 및 source 별 조건
   ⑥ 이 외 다양한 조건으로 검색

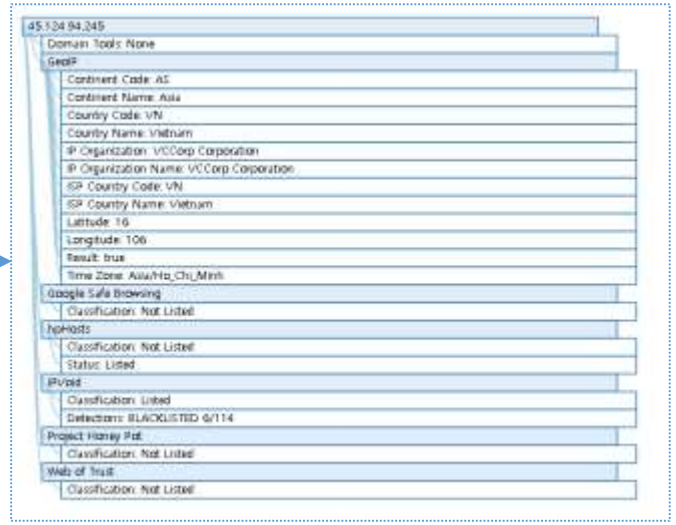


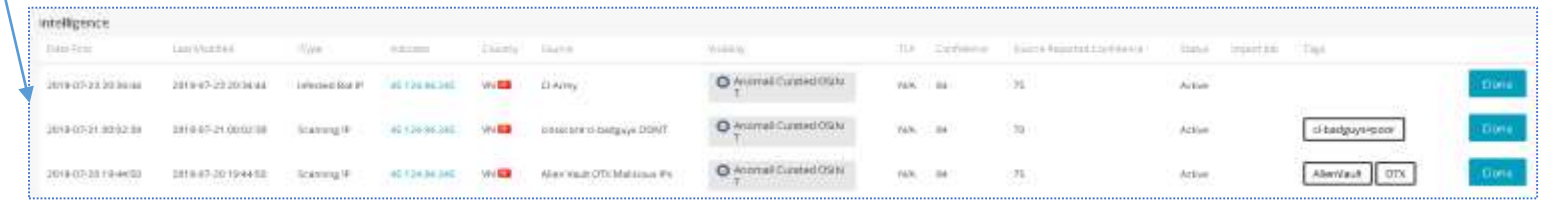
2. Threat Intelligence 정보 검색

① Active OR Non-Active 확인 가능
② Threat 기법 확인 가능
③ TI source 확인 가능
④ Confidence 확인 가능
⑤ Threat Timeline(언제부터 Active했는지 혹은 언제부터 non-active 했는지 등 확인)
⑥ IP 혹은 Domein information



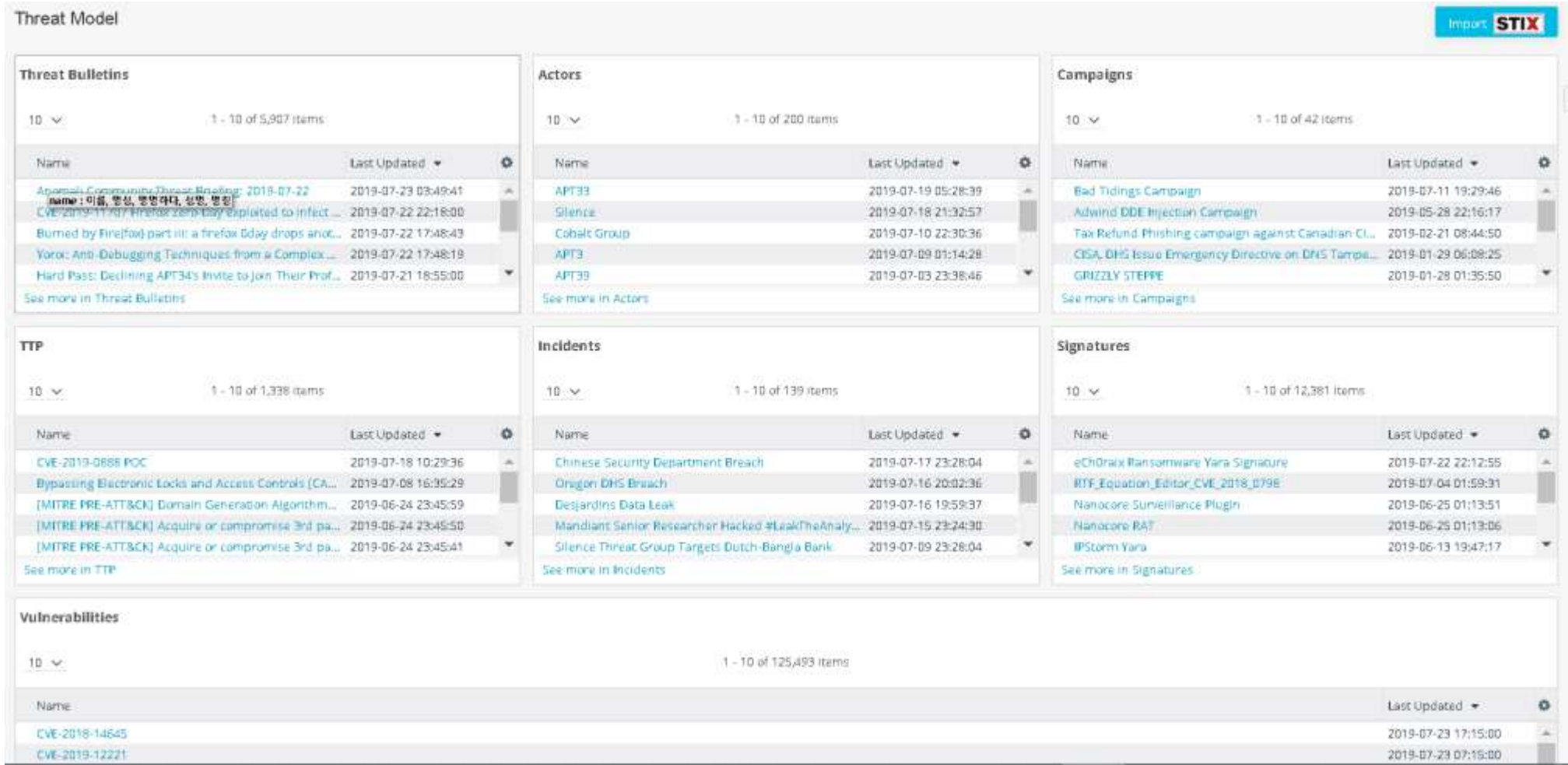






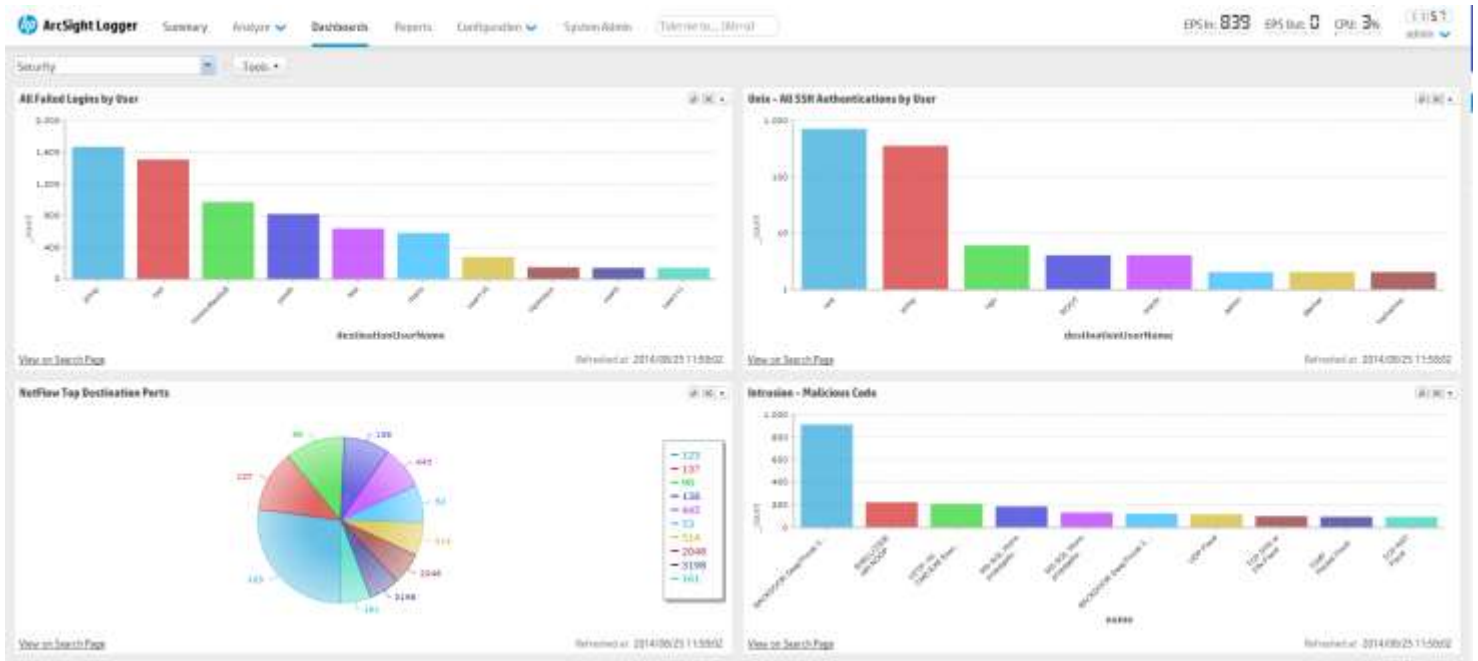
2. Threat Intelligence 정보 검색
   - Threat Model에서 아래 각종 정보를 한번에 검색 가능

① Threat Bulletines
② Actors
③ Campaign
④ TTP (Tactics, Techniques and Procedure)
⑤ Incidents
⑥ Signatures
⑦ Vulnerabilities



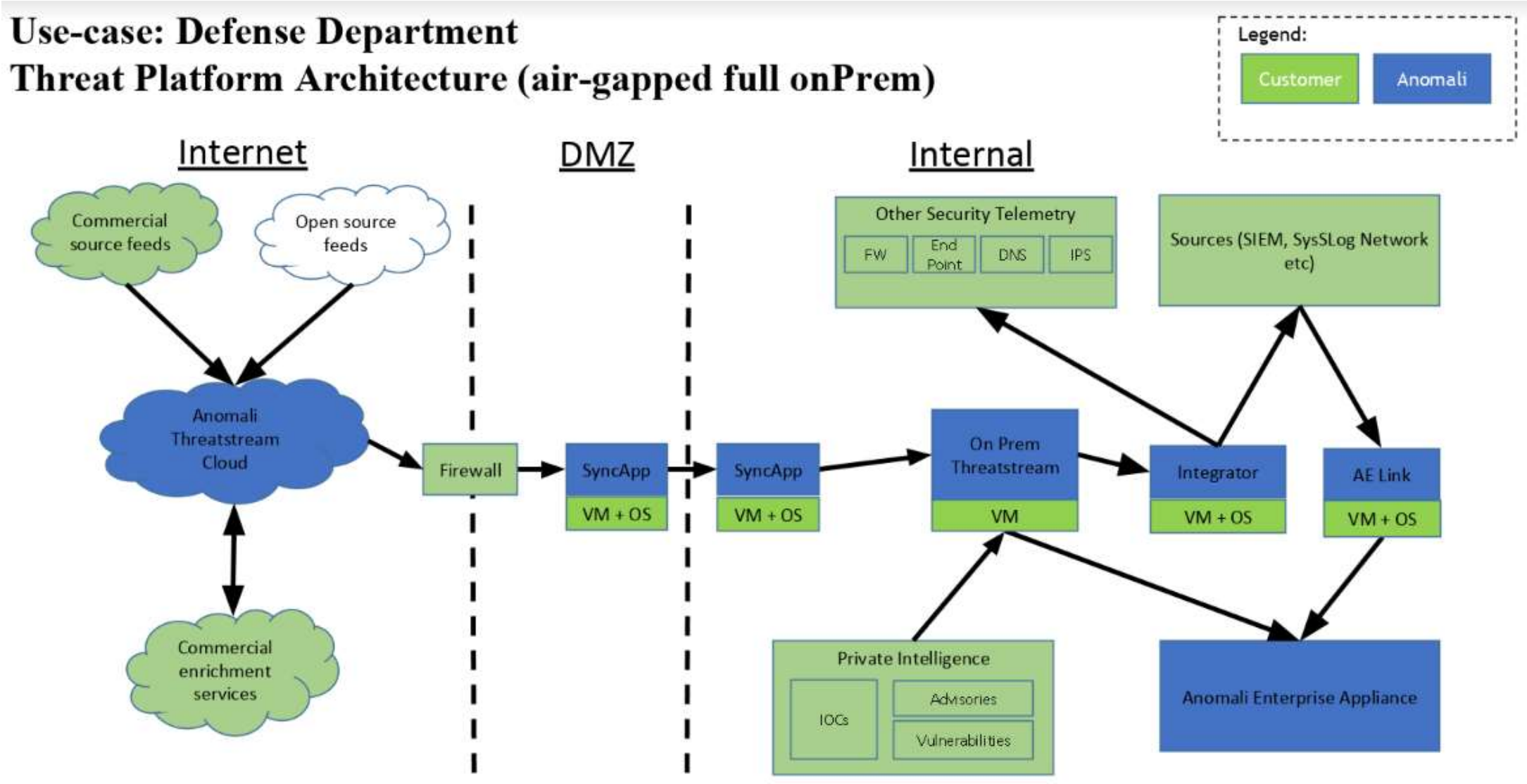
3. SIEM 과의 연동

① with Archsight
② with Q-Rader
③ with Splunk
④ with Firewall
⑤ etc



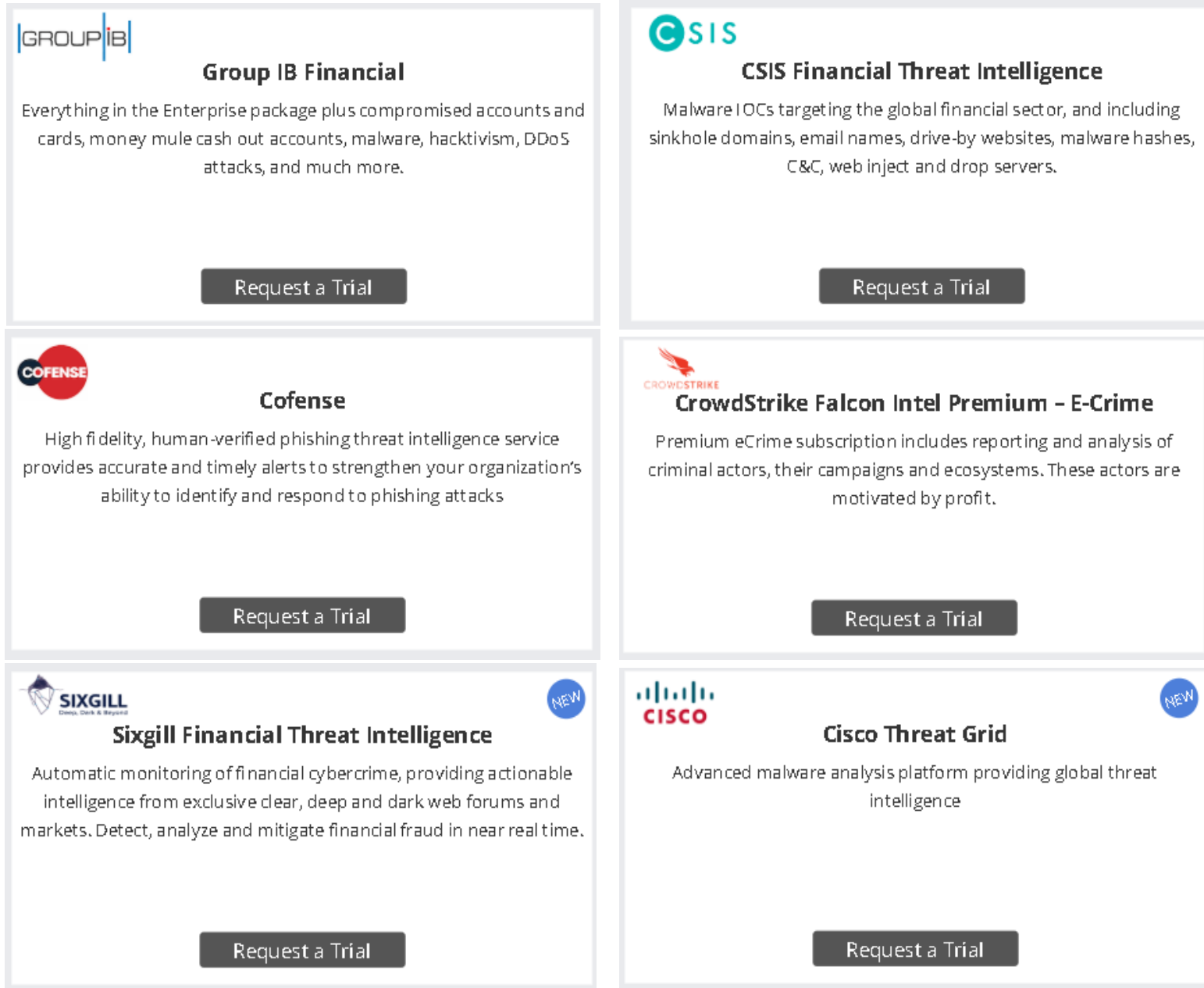
4. Offline 용 TI 정보 제공 시스템(Air gap)

① 망분리 시스템을 위한 TI 제공 시스템



5. 추가 제공 서비스

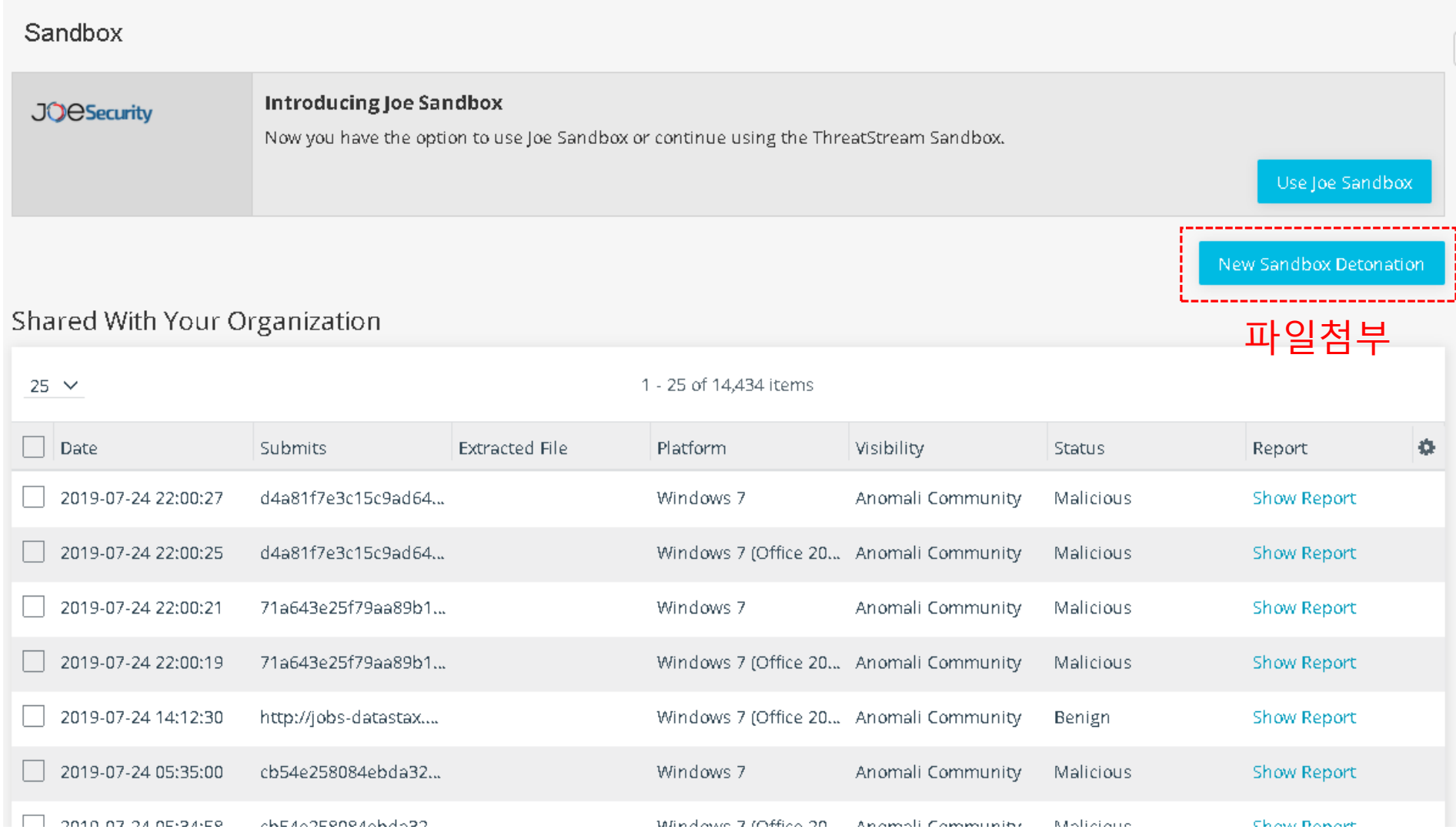
① 현재 66개 이상의 Threat Intelligence Alience(지속적으로 신규 Alience 생성 중)



5. 추가 제공 서비스

② Sand Box

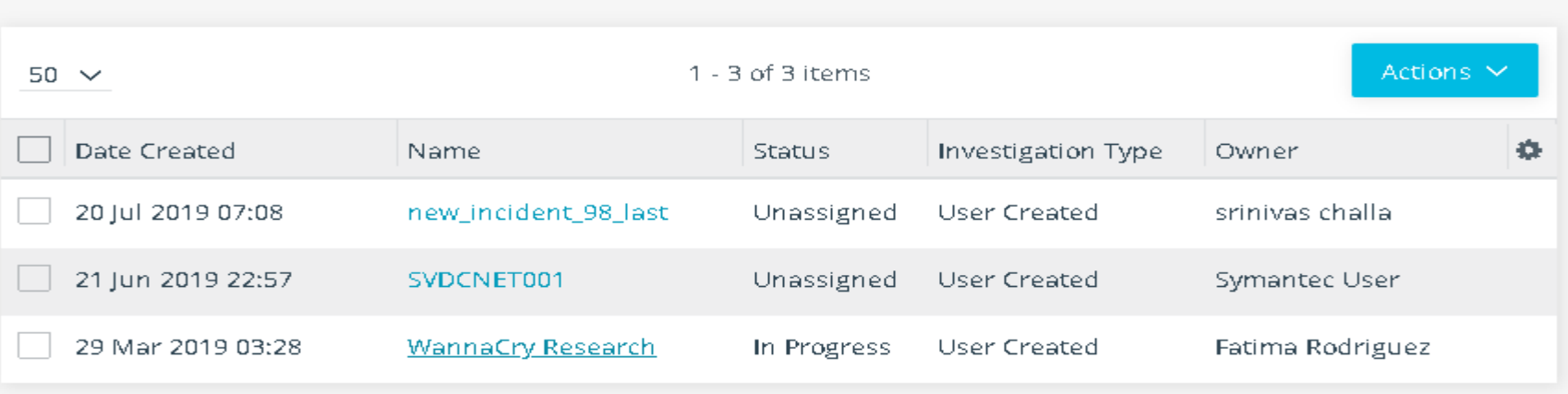
샌드박스(SandBox) : 외부로부터 받은 파일을 바로 실행하지 않고, 보호된 영역에서 실행시켜 봄으로써 외부로부터 들어오는 파일과 프로그램이 내부 시스템에 악영향을 주는 것을 미연에 방지.



5. 추가 제공 서비스

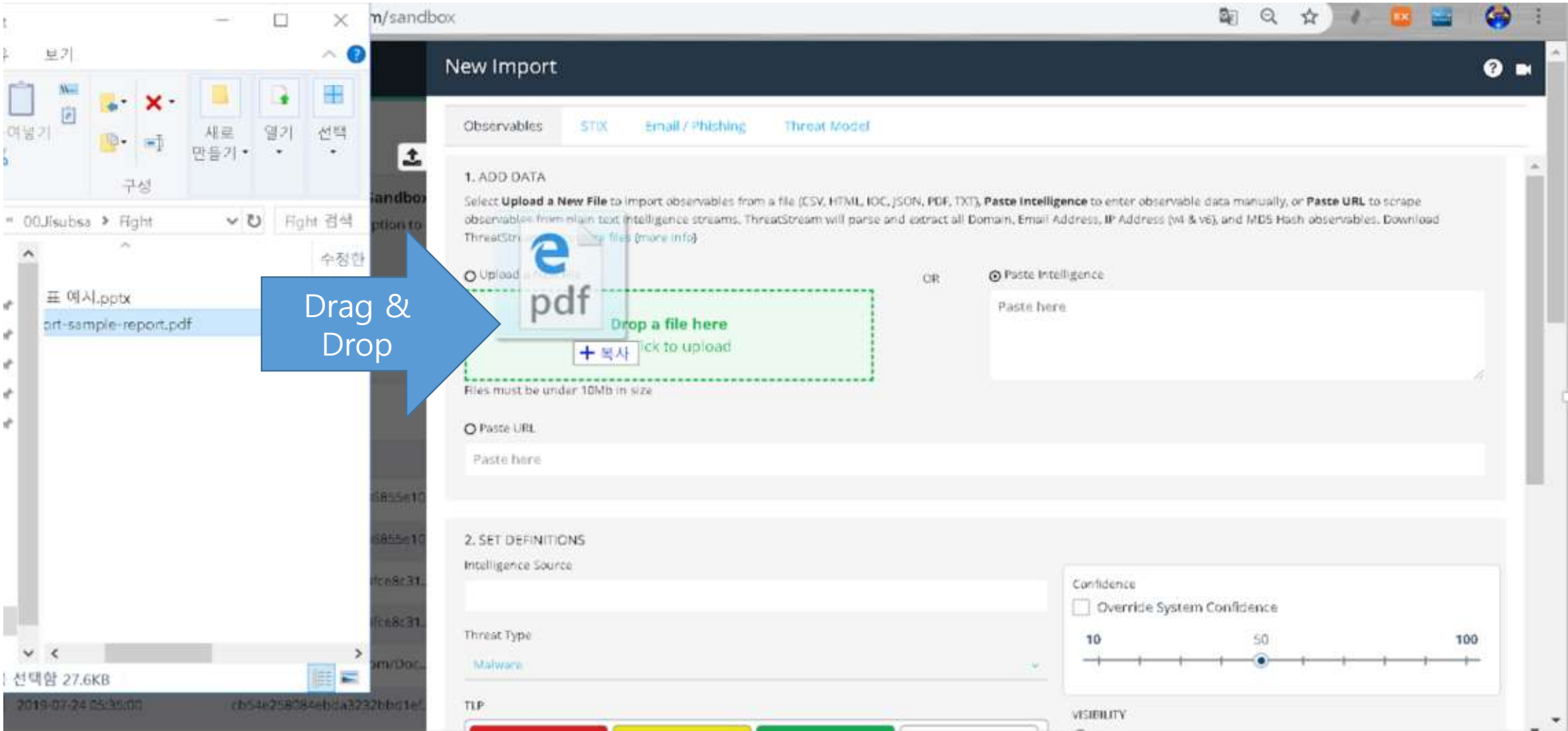
③ Investigation

- Trust Circle 간 Investigaton 진행
- 심층 분석을 위한 부서 이관
- 타 Alliance와의 공조



5. 추가 제공 서비스

⑤ 메일로 수신하는 위협 정보 넣기(PDF파일 원본 그대로 Import)



5. 추가 제공 서비스

⑥ Threat Model Daily Digest : 일일 Anomali TI 업데이트 정보 제공

[Anomali ThreatStream] Your daily Threat Model digest 받은편지함 ×

Anomali ThreatStream <info@anomali.com>
나에게

2019. 7. 28. 오전 6:06 (2일 전)

영어 › 한국어 메일 번역 영어 번역 안함 ×

ANOMALI THREATSTREAM

Threat Model Daily Digest (July 27)

- New Threat Bulletin 2 updates: 이스트시큐리티 알약 블로그 – [if lt IE 9]><script src="https:
- New Threat Bulletin 1 update: 이스트시큐리티 알약 블로그 – (function() {... created by kenn
- Threat Bulletin 1 update: REMCOS Backdoor Tool Tip – Summary... created by Anomali Labs
- Threat Bulletin 1 update: Mirai Tool TIP – Summary... created by Aaron Shelmire LABS
- Threat Bulletin 1 update: Hawkeye Tool Tip – Summary... created by Luis Mendieta

To unsubscribe from these notifications, go to https://ui.threatstream.com/settings.

Thank you!

Copyright 2019 Anomali, Inc.

[Anomali ThreatStream] Your daily Threat Model digest 받은편지함 ×

Anomali ThreatStream <info@anomali.com>
나에게

오전 1:44 (19시간 전)

영어 › 한국어 메일 번역 영어 번역 안함 ×

ANOMALI THREATSTREAM

Threat Model Daily Digest (July 29)

- 1 updates CVE-2019-0708
- Actor 1 updates FIN4
- Actor 1 updates Energetic Bear
- Actor 1 updates Silent Librarian
- Actor 1 updates Orangeworm
- Actor 1 updates APT10
- Actor 1 updates Winnti
- New Threat Bulletin 1 update: bark_2907_9 – my tip desc test created by Hema.Halliyal@demisto.com
- New Threat Bulletin 1 update: bark_2907_3 – my desc test created by Hema.Halliyal@demisto.com
- New Threat Bulletin 1 update: bark_2907 created by Hema.Halliyal@demisto.com
- New Threat Bulletin 1 update: bark_2907 created by Hema.Halliyal@demisto.com
- Threat Bulletin 1 update: REMCOS Backdoor Tool Tip – Summary... created by Anomali Labs
- Threat Bulletin 1 update: Bozok Tool Tip – Summary... created by Luis Mendieta
- Threat Bulletin 1 update: Pony Tool Tip – Summary... created by Luis Mendieta
- Threat Bulletin 1 update: Hawkeye Tool Tip – Summary... created by Luis Mendieta

To unsubscribe from these notifications, go to https://ui.threatstream.com/settings.

Thank you!

Copyright 2019 Anomali, Inc.

고맙습니다.


CROWDSTRIKE
VISA
ANOMALI
paloalto NETWORKS
OpenDNS
CISCO OpenDNS is now part of Cisco.
INTEL471
iDefense
Part of Accenture Security
CARBON BLACK
IBM QRadar
Symantec
FORSIGHT SECURITY
McAfee
FireEye
FLASHPOINT
COFENSE
splunk>
LogRhythm