

# Anomali Threat Stream

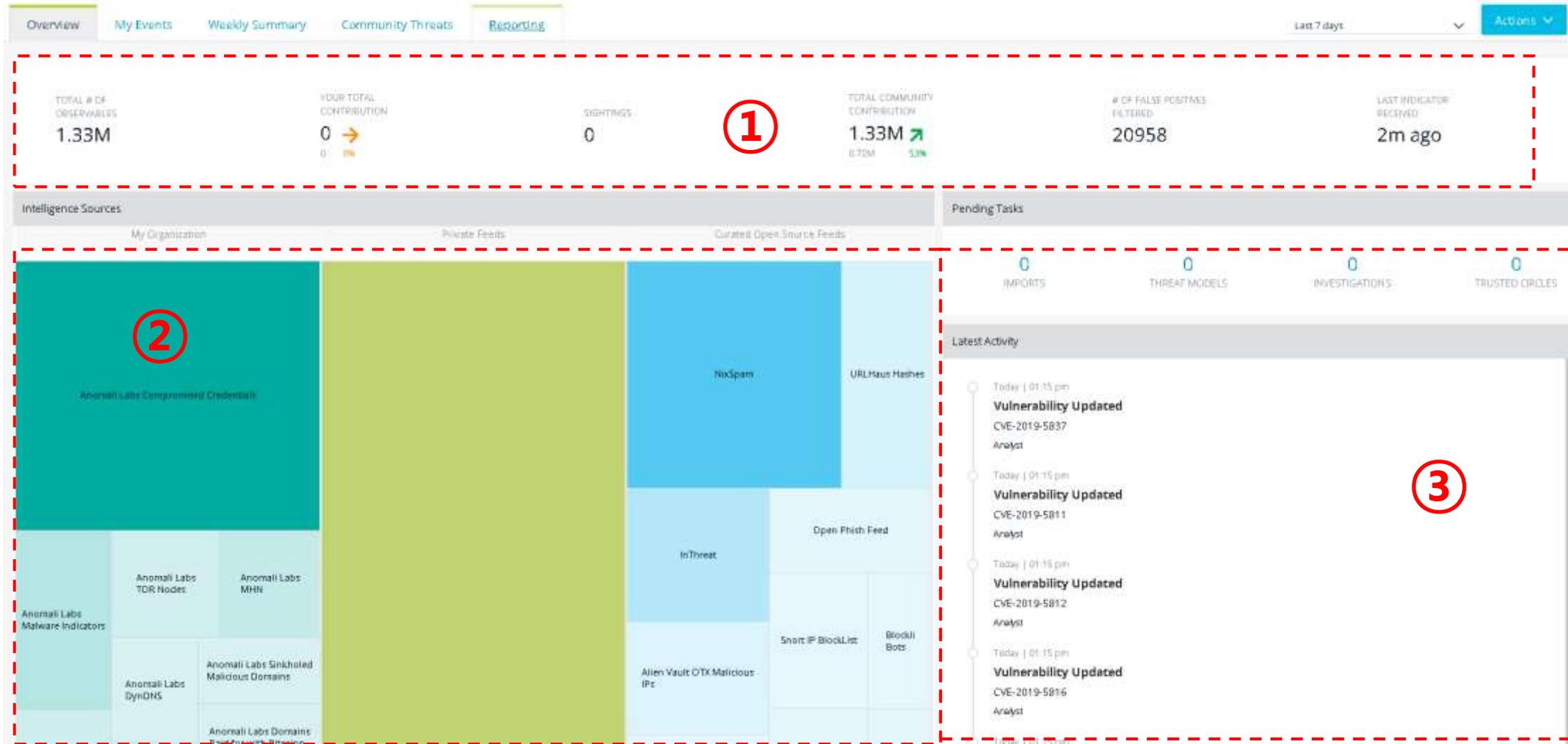
## Detail Function

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

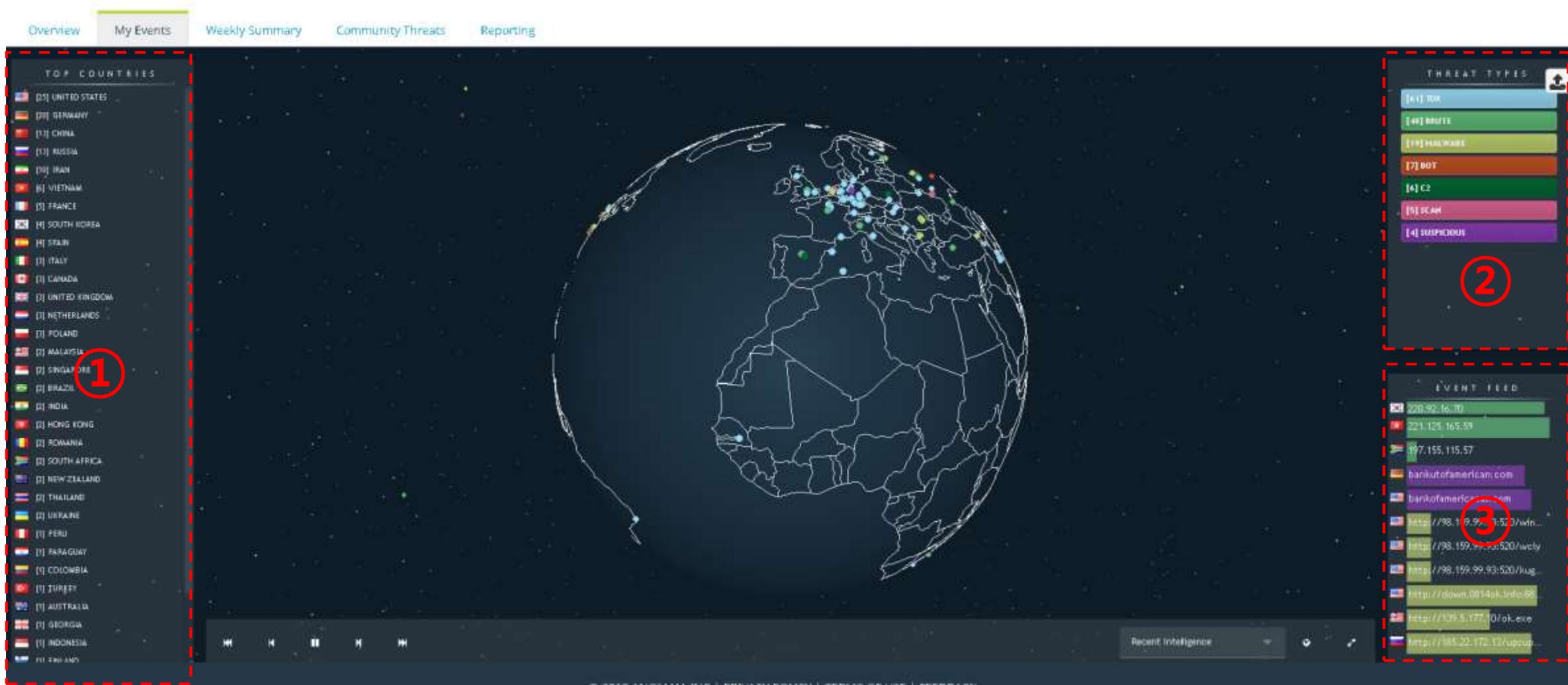
- ① TI source 별 수집 현황
- ② 실시간 취약점 수집 현황
- ③ My Feeds 현황



# 1. Threat Intelligence 정보 제공

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

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

The screenshot displays the 'Observables' interface with various filter options on the left and a table of items on the right. The filter options are categorized into Date Added, Status, Visibility, TLP, and Minimum Confidence. The table columns include Date First, iType, Indicator, Confidence, Country, Streams/Source, Visibility, and Tags. Red dashed boxes and circled numbers 1, 2, and 3 highlight specific filter options: 1 for Status (Active/Inactive), 2 for Visibility (Anomali Community/My Organization), and 3 for Minimum Confidence (slider).

Date First	iType	Indicator	Confidence	Country	Streams/Source	Visibility	Tags
2019-07-25 20:05:27	Malware URL	<a href="http://185.22.172.13/upsupx.exe">http://185.22.172.13/upsupx.exe</a>	82	RU	URLHaus	Anomali CU...	date...
2019-07-25 20:05:26	Malware URL	<a href="http://139.5.177.10/ok.exe">http://139.5.177.10/ok.exe</a>	59	MY	URLHaus	Anomali CU...	date...
2019-07-25 20:05:26	Malware URL	<a href="http://down.0814ok.info:8888/ok...">http://down.0814ok.info:8888/ok...</a>	85	US	URLHaus	Anomali CU...	batch
2019-07-25 20:05:26	Malware URL	<a href="http://98.159.99.93:520/kugbu">http://98.159.99.93:520/kugbu</a>	27	US	URLHaus	Anomali CU...	date...
2019-07-25 20:05:25	Malware URL	<a href="http://98.159.99.93:520/wcly">http://98.159.99.93:520/wcly</a>	27	US	URLHaus	Anomali CU...	aesdd...
2019-07-25 20:05:25	Malware URL	<a href="http://98.159.99.93:520/winseen...">http://98.159.99.93:520/winseen...</a>	27	US	URLHaus	Anomali CU...	ccatt...
2019-07-25 19:45:51	Suspicious Domain	<a href="http://bankofamericaas.com">bankofamericaas.com</a>	82	US	Analyst	Anomali Comm...	bank
2019-07-25 19:45:51	Suspicious Domain	<a href="http://bankoutofamerican.com">bankoutofamerican.com</a>	20		Analyst	Anomali Comm...	bank
2019-07-25 19:45:51	Suspicious Domain	<a href="http://bankoutofamerican.com">bankoutofamerican.com</a>	78	DE	Analyst	Anomali Comm...	bank
2019-07-25 19:43:20	Brute Force IP	<a href="http://197.155.115.57">197.155.115.57</a>	19	ZA	Charles Haley SSH BruteForcer IP...	Anomali Comm...	No Tags
2019-07-25 19:43:15	Brute Force IP	<a href="http://221.125.165.59">221.125.165.59</a>	92	HK	Charles Haley SSH BruteForcer IP...	Anomali Comm...	No Tags
2019-07-25 19:43:13	Brute Force IP	<a href="http://220.92.16.70">220.92.16.70</a>	89	KR	Charles Haley SSH BruteForcer IP...	Anomali Comm...	No Tags
2019-07-25 19:43:12	Brute Force IP	<a href="http://218.150.220.206">218.150.220.206</a>	89	KR	Charles Haley SSH BruteForcer IP...	Anomali Comm...	No Tags

## 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

The screenshot displays the ThreatStream interface. The top navigation bar includes 'DASHBOARD', 'MANAGE', 'ANALYZE', 'RESEARCH', and 'APP STORE'. The main content area is titled 'Observables' and features a search bar with the IP address '45.124.94.245'. Below the search bar, there are filter options for 'Status' (ACTIVE, Inactive, False Positive) and 'Date Added' (Last 24 hours, Last 30 Days, Last 90 Days, This year, Custom Date Range). The search results are displayed in a table with columns: Date First, iType, Indicator, Confidence, Country, Streams..., Visibility, and Tags. The table shows several entries for Malware and Suspicious activity, with indicators like 'http://18...', 'http://13...', 'http://do...', 'http://98...', and 'bankofa...'. The interface also includes a 'FILTER OPTIONS' sidebar on the left and a 'Date Added' filter section at the bottom.

Date First	iType	Indicator	Confidence	Country	Streams...	Visibility	Tags
2019-07-25 20:05:27	Malware...	http://18...	82	RU	URLHaus	Anomali Cu...	date_...
2019-07-25 20:05:26	Malware...	http://13...	59	MY	URLHaus	Anomali Cu...	date_...
2019-07-25 20:05:26	Malware...	http://do...	85	US	URLHaus	Anomali Cu...	batch >>
2019-07-25 20:05:26	Malware...	http://98...	27	US	URLHaus	Anomali Cu...	date_...
2019-07-25 20:05:25	Malware...	http://98...	27	US	URLHaus	Anomali Cu...	aesdd...
2019-07-25 20:05:25	Malware...	http://98...	27	US	URLHaus	Anomali Cu...	ccatt... >
2019-07-25 19:45:51	Suspicio...	bankofa...	82	US	Analyst	Anomali Comm...	bank >>
2019-07-25 19:45:51	Suspicio...	bankout...	20		Analyst	Anomali Comm...	bank >>

## 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

Details for 45.124.94.245

Severity: **LOW** Confidence: **84**

Status: **Active**

Type: IP (Infected DoI)

Process: 45.124.94.245

Tags: **@badguys=poor** **AlienVault** **OTX**

Last Modified: 2019-07-23 20:34:44

Score: 7

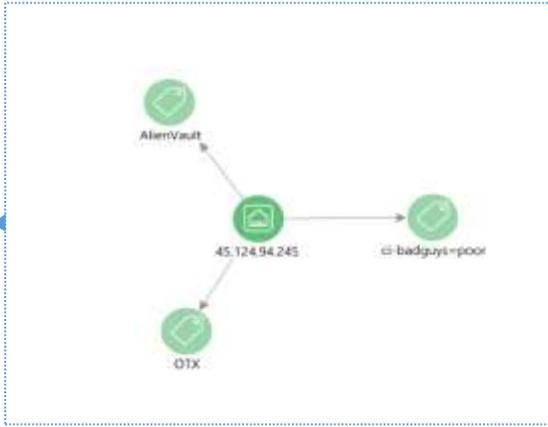
Country: **VN**

Organization: VCCorp Corporation

Insights: DSField has observed IP 45.124.94.245 scanning 25 targets, resulting in 37 reports from 2018-07-19 to 2019-07-21.

Analysis Links: [Google Safe Browsing](#) [IPVirt](#) [Shodan](#) [VirusTotal](#) [IPIntelligence](#)

Export: [CSV](#) [Smart](#) [DBExport](#) [STIX 1.1.1](#) [STIX 1.2](#) [STIX 2](#) [Report as false positive](#)



45.124.94.245

Domain Tools: None

GeoIP

- Continent Code: AS
- Continent Name: Asia
- Country Code: VN
- Country Name: Vietnam
- IP Organization: VCCorp Corporation
- IP Organization Name: VCCorp Corporation
- ISP Country Code: VN
- ISP Country Name: Vietnam
- Latitude: 16
- Longitude: 106
- Result: true
- Time Zone: Asia/Ho\_Chi\_Minh

Google Safe Browsing

- Classification: Not Listed

IPWhois

- Classification: Not Listed
- Status: Listed

IPVirt

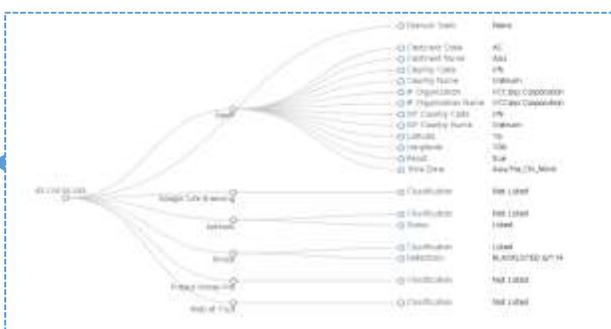
- Classification: Listed
- Detectors: BLACKLISTED 6/114

Project Honey Pot

- Classification: Not Listed

Web of Trust

- Classification: Not Listed



Item Test	Last Visited	Type	Address	Country	Source	Severity	TLP	Confidence	Score Reported Confidence	Status	Import ID	Tags
2019-07-23 20:34:44	2019-07-23 20:34:44	Infected DoI IP	45.124.94.245	VN	@Army	Normal-Curated OSINT	FAK	84	75	Active		
2019-07-21 00:02:39	2019-07-21 00:02:39	Scanning IP	45.124.94.245	VN	@osintand-badguys-DONT	Normal-Curated OSINT	FAK	84	70	Active		@badguys=poor
2019-07-20 19:44:00	2019-07-20 19:44:00	Scanning IP	45.124.94.245	VN	AlienVault OTX Malicious IP	Normal-Curated OSINT	FAK	84	75	Active		AlienVault OTX

## 2. Threat Intelligence 정보 검색

- Threat Model에서 아래 각종 정보를 한번에 검색 가능

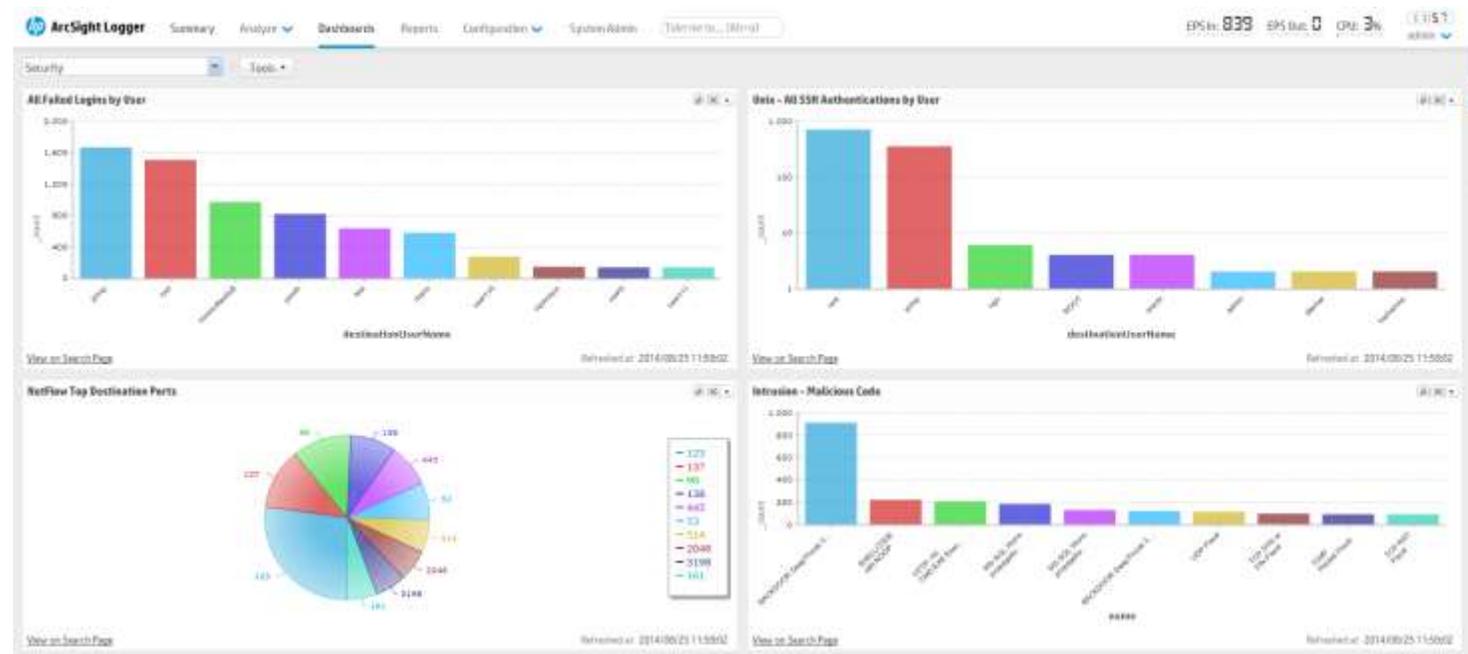
- ① Threat Bulletines
- ② Actors
- ③ Campaign
- ④ TTP (Tactics, Techniques and Procedure)
- ⑤ Incidents
- ⑥ Signatures
- ⑦ Vulnerabilities

The screenshot displays the Threat Model interface with an 'Import STIX' button in the top right corner. The interface is divided into seven panels, each showing a list of items with columns for Name and Last Updated. Each panel includes a dropdown menu for the number of items displayed (set to 10) and a link to 'See more in [Category Name]'.

- Threat Bulletines:** 1 - 10 of 5,907 items. Items include 'Anomali Community Threat Briefing: 2018-07-22', 'CVE-2019-11707 Firefox zero-day exploited to infect...', 'Burned by Firefox part III: a Firefox 6day drops anot...', 'Yorak: Anti-Debugging Techniques from a Complex...', and 'Hard Pass: Declining APT34's Invite to join Their Prof...'.
- Actors:** 1 - 10 of 200 items. Items include 'APT33', 'Silence', 'Cobalt Group', 'APT3', and 'APT39'.
- Campaigns:** 1 - 10 of 42 items. Items include 'Bad Tidings Campaign', 'Adwind DDEInjection Campaign', 'Tax Refund Phishing campaign against Canadian Cl...', 'CISA, DHS Issue Emergency Directive on DHS Tampa...', and 'GRIZZLY STEPPE'.
- TTP:** 1 - 10 of 1,338 items. Items include 'CVE-2019-0888 POC', 'Bypassing Electronic Locks and Access Controls (CA...', '[MITRE PRE-ATT&CK] Domain Generation Algorithm...', '[MITRE PRE-ATT&CK] Acquire or compromise 3rd pa...', and '[MITRE PRE-ATT&CK] Acquire or compromise 3rd pa...'.
- Incidents:** 1 - 10 of 139 items. Items include 'Chinese Security Department Breach', 'Oregon DHS Breach', 'Desjardins Data Leak', 'Mandiant Senior Researcher Hacked #LeakTheAnaly...', and 'Silence Threat Group Targets Dutch-Bangla Bank'.
- Signatures:** 1 - 10 of 12,381 items. Items include 'eChDrax Ransomware Yara Signature', 'RTF\_Equation\_Editor\_CVE\_2018\_0798', 'Nanocore Surveillance Plugin', 'Nanocore RAT', and 'IPStorm Yara'.
- Vulnerabilities:** 1 - 10 of 125,493 items. Items include 'CVE-2018-14645' and 'CVE-2019-12221'.

### 3. SIEM 과의 연동

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

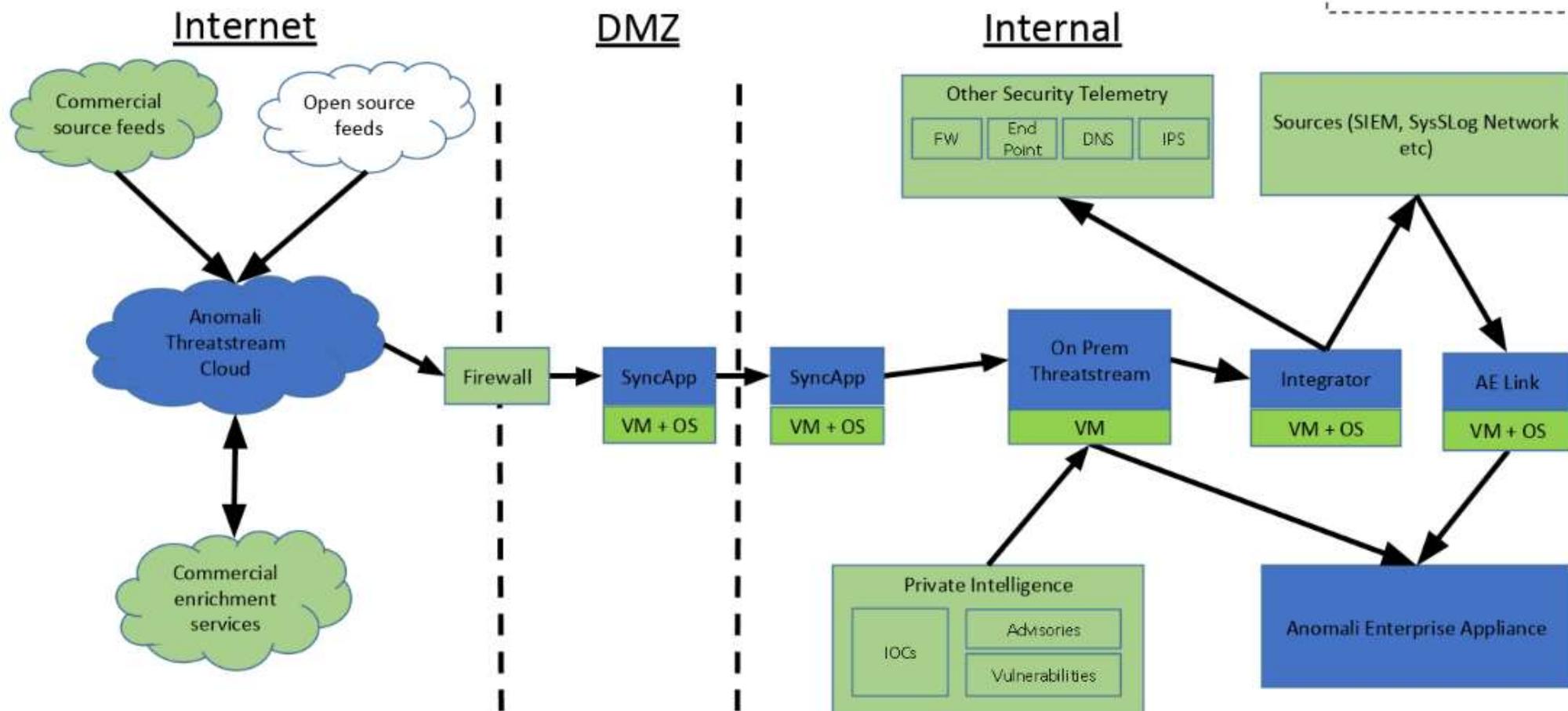


#### 4. Offline 용 TI 정보 제공 시스템(Air gap)

① 망분리 시스템을 위한 TI 제공 시스템

### Use-case: Defense Department

### Threat Platform Architecture (air-gapped full onPrem)



## 5. 추가 제공 서비스

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



### Group IB Financial

Everything in the Enterprise package plus compromised accounts and cards, money mule cash out accounts, malware, hacktivism, DDoS attacks, and much more.

[Request a Trial](#)



### CSIS Financial Threat Intelligence

Malware IOCs targeting the global financial sector, and including sinkhole domains, email names, drive-by websites, malware hashes, C&C, web inject and drop servers.

[Request a Trial](#)



### Cofense

High fidelity, human-verified phishing threat intelligence service provides accurate and timely alerts to strengthen your organization's ability to identify and respond to phishing attacks

[Request a Trial](#)



### CrowdStrike Falcon Intel Premium - E-Crime

Premium eCrime subscription includes reporting and analysis of criminal actors, their campaigns and ecosystems. These actors are motivated by profit.

[Request a Trial](#)



### Sixgill Financial Threat Intelligence

Automatic monitoring of financial cybercrime, providing actionable intelligence from exclusive clear, deep and dark web forums and markets. Detect, analyze and mitigate financial fraud in near real time.

[Request a Trial](#)



### Cisco Threat Grid

Advanced malware analysis platform providing global threat intelligence

[Request a Trial](#)

## 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.

### Sandbox

**Introducing Joe Sandbox**  
Now you have the option to use Joe Sandbox or continue using the ThreatStream Sandbox.  
[Use Joe Sandbox](#)

[New Sandbox Detonation](#)

### Shared With Your Organization

25 ▾ 1 - 25 of 14,434 items

<input type="checkbox"/>	Date	Submits	Extracted File	Platform	Visibility	Status	Report	⚙
<input type="checkbox"/>	2019-07-24 22:00:27	d4a81f7e3c15c9ad64...		Windows 7	Anomali Community	Malicious	<a href="#">Show Report</a>	
<input type="checkbox"/>	2019-07-24 22:00:25	d4a81f7e3c15c9ad64...		Windows 7 (Office 20...	Anomali Community	Malicious	<a href="#">Show Report</a>	
<input type="checkbox"/>	2019-07-24 22:00:21	71a643e25f79aa89b1...		Windows 7	Anomali Community	Malicious	<a href="#">Show Report</a>	
<input type="checkbox"/>	2019-07-24 22:00:19	71a643e25f79aa89b1...		Windows 7 (Office 20...	Anomali Community	Malicious	<a href="#">Show Report</a>	
<input type="checkbox"/>	2019-07-24 14:12:30	http://jobs-datastax....		Windows 7 (Office 20...	Anomali Community	Benign	<a href="#">Show Report</a>	
<input type="checkbox"/>	2019-07-24 05:35:00	cb54e258084ebda32...		Windows 7	Anomali Community	Malicious	<a href="#">Show Report</a>	
<input type="checkbox"/>	2019-07-24 05:34:58	4e54e258084ebda32...		Windows 7 (Office 20...	Anomali Community	Malicious	<a href="#">Show Report</a>	

**파일첨부**

## 5. 추가 제공 서비스

### ③ Investigation

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

<input type="checkbox"/>	Date Created	Name	Status	Investigation Type	Owner	
<input type="checkbox"/>	20 Jul 2019 07:08	<a href="#">new_incident_98_last</a>	Unassigned	User Created	srinivas challa	
<input type="checkbox"/>	21 Jun 2019 22:57	<a href="#">SVDCNET001</a>	Unassigned	User Created	Symantec User	
<input type="checkbox"/>	29 Mar 2019 03:28	<a href="#">WannaCry_Research</a>	In Progress	User Created	Fatima Rodriguez	

## 5. 추가 제공 서비스

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

The image shows a web browser window with a 'New Import' page. On the left, a file explorer window is open, showing a folder named '00.Jsubsa' with a file named 'prt-sample-report.pdf'. A blue arrow labeled 'Drag & Drop' points from the file to the 'Drop a file here' area in the 'New Import' form. The 'New Import' form has tabs for 'Observables', 'STIX', 'Email / Phishing', and 'Threat Model'. The 'Upload' section is selected, and it contains a 'Drop a file here' area with a '+ 복사' button. Below this are 'Paste Intelligence' and 'Paste URL' sections. The '2. SET DEFINITIONS' section includes fields for 'Intelligence Source', 'Threat Type' (set to 'Malware'), and a 'Confidence' slider set to 50. The 'Confidence' section also has an 'Override System Confidence' checkbox.

## 5. 추가 제공 서비스

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

[Anomali ThreatStream] Your daily Threat Model digest 받은편지함 x

Anomali ThreatStream <info@anomali.com>

나에게 ▾

2019. 7. 28. 오전 6:06 (2일 전)

☆ ↶ ⋮

🗨️ 영어 ▾ > 한국어 ▾ [메일 번역](#)

[영어 번역 안함](#) x

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 x

Anomali ThreatStream <info@anomali.com>

나에게 ▾

오전 1:44 (19시간 전)

☆ ↶ ⋮

🗨️ 영어 ▾ > 한국어 ▾ [메일 번역](#)

[영어 번역 안함](#) x

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 [Winnit](#)
- **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.

