

Anomali Threat Stream

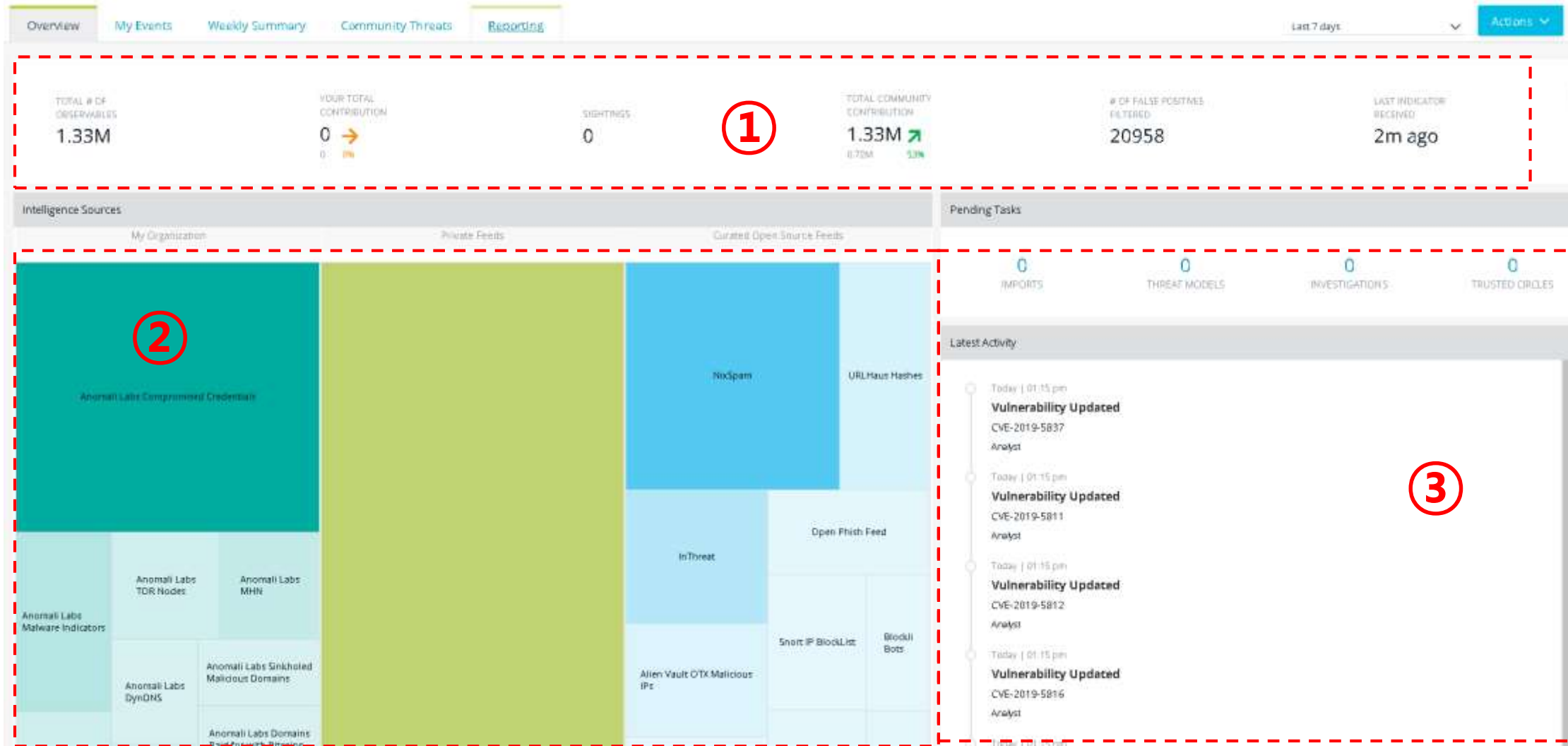
Detail Function

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

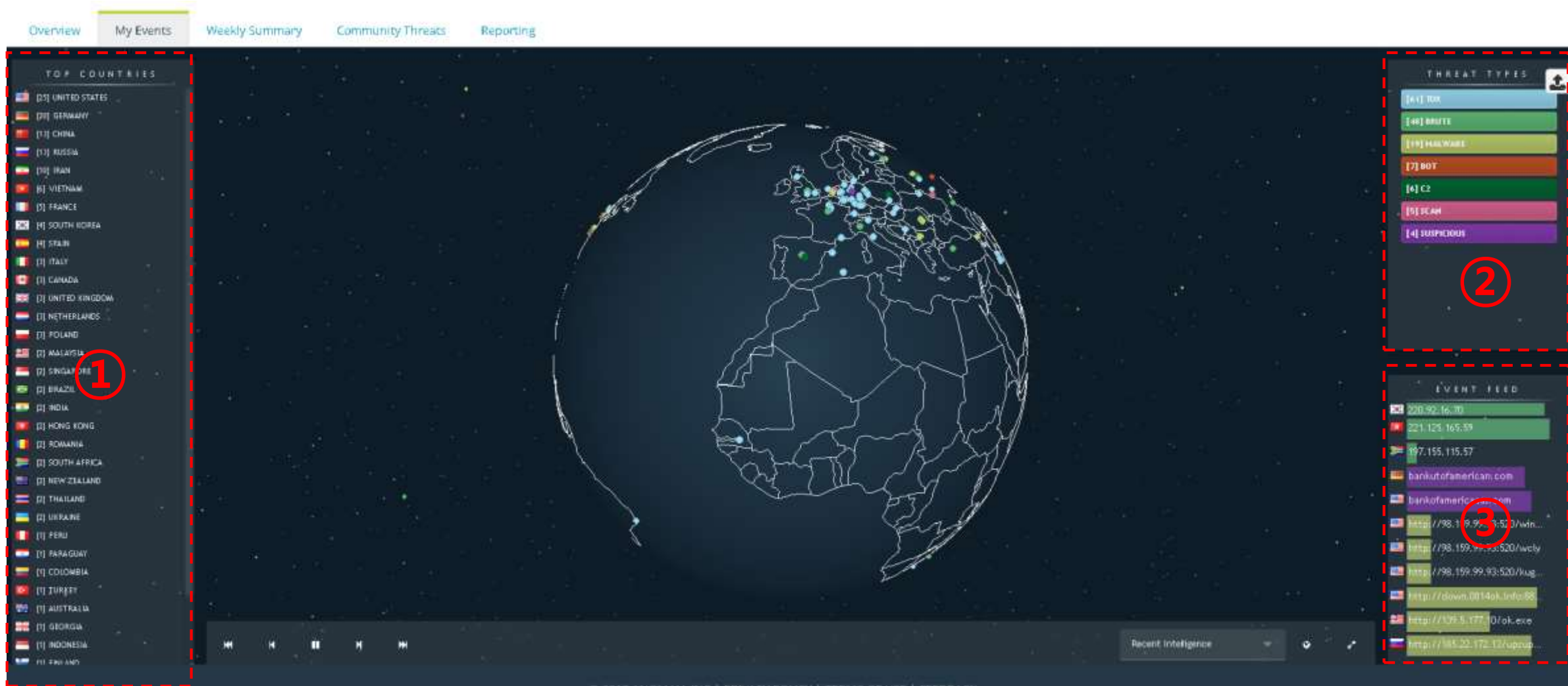
- ① TI source 별 수집 현황
- ② 실시간 취약점 수집 현황
- ③ My Feeds 현황



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 a sidebar on the left containing filter options and a main table of results. The sidebar filters are grouped into three red dashed boxes with numbered callouts:

- Box 1 (Status):** Includes 'Date Added' (Last 24 hours, Last 30 Days, Last 90 Days, This year, Custom Date Range) and 'Status' (Active, Inactive, False Positive). The 'Active' status is selected.
- Box 2 (Visibility):** Includes 'Visibility' (Anomali Community, My Organization) and 'TLP' (Red, Amber, Green, White). The 'Anomali Community' visibility is selected.
- Box 3 (Minimum Confidence):** Includes a 'Minimum Confidence' slider ranging from 0 to 100.

The main table displays 1 - 50 of 2,968,941 items. The columns are: Date First, IType, Indicator, Confidence, Country, Streams/Source, Visibility, and Tags. The table shows various threat intelligence items, including Malware URLs, Suspicious Domains, and Brute Force IPs.

Date First	IType	Indicator	Confidence	Country	Streams/Source	Visibility	Tags
2019-07-25 20:05:27	Malware URL	http://185.22.172.13/upsupx.exe	82	RU	URLHaus	Anomali Cu...	date...
2019-07-25 20:05:26	Malware URL	http://139.5.177.10/ok.exe	59	MY	URLHaus	Anomali Cu...	date...
2019-07-25 20:05:26	Malware URL	http://down.0814ok.info/8888/ok...	85	US	URLHaus	Anomali Cu...	batch
2019-07-25 20:05:26	Malware URL	http://98.159.99.93:520/kuqbu	27	US	URLHaus	Anomali Cu...	date...
2019-07-25 20:05:25	Malware URL	http://98.159.99.93:520/wcly	27	US	URLHaus	Anomali Cu...	aesdd...
2019-07-25 20:05:25	Malware URL	http://98.159.99.93:520/winseen...	27	US	URLHaus	Anomali Cu...	ccatt...
2019-07-25 19:45:51	Suspicious Domain	bankofamericaas.com	82	US	Analyst	Anomali Comm...	bank
2019-07-25 19:45:51	Suspicious Domain	bankoutofamerican.com	20		Analyst	Anomali Comm...	bank
2019-07-25 19:45:51	Suspicious Domain	bankoutofamerican.com	78	DE	Analyst	Anomali Comm...	bank
2019-07-25 19:43:20	Brute Force IP	197.155.115.57	19	ZA	Charles Haley SSH BruteForcer IP...	Anomali Comm...	No Tags
2019-07-25 19:43:15	Brute Force IP	221.125.165.59	92	HK	Charles Haley SSH BruteForcer IP...	Anomali Comm...	No Tags
2019-07-25 19:43:13	Brute Force IP	220.92.16.70	89	KR	Charles Haley SSH BruteForcer IP...	Anomali Comm...	No Tags
2019-07-25 19:43:12	Brute Force IP	218.150.220.206	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 web interface. The top navigation bar includes links for DASHBOARD, MANAGE, ANALYZE, RESEARCH, and APP STORE, along with a search bar and user profile icons. The main content area is titled 'Observables' and features a 'FILTER OPTIONS' sidebar on the left. The sidebar contains filters for Date Added (Last 24 hours, Last 30 Days, Last 90 Days, This year, Custom Date Range), Status (Active, Inactive, False Positive), Visibility (Anomali Community, My Organization), TLP (Red, Amber, Green, White), and Minimum Confidence. The main panel shows a search for '45.124.94.245' with filters for Status (ACTIVE) and From (2019-06-25 20:13:14). Below the filters, a table lists 50 items (1 - 50 of 2,968,938 items). The table columns are Date First, iType, Indicator, Confidence, Country, Streams..., Visibility, and Tags. The table contains several rows of data, including malware indicators and suspicious activity.

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 Domain information

Details for 45.124.94.245

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

Status: **Active**

Type: IP (Detected DoI)

Indicators: 45.124.94.245

Tags: ci-badguys=poor, alienVault, OTX

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

Country: VN

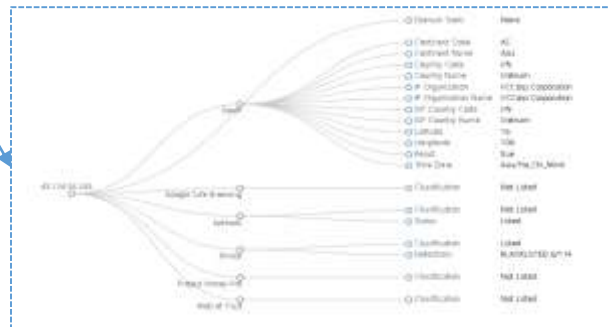
Organization: VCCorp Corporation

Insights: OSINT has observed IP 45.124.94.245 scanning 25 targets, resulting in 37 reports from 2018-07-18 to 2019-07-23.

Analysis Tools: Google Safe Browsing, VirusTotal, IPinfo, Shodan, AlienVault, OTX

Export: CSV, Short, OpenIOC, STIX 1.1.1, STIX 1.2, STIX 2

Report as false positive



45.124.94.245

Domain Tools: None

GeotIP

- 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

Ipinfo

- Classification: Not Listed
- Status: Listed

IPinfo

- Classification: Listed
- Detections: BLACKLISTED 6/114

Project Honey Pot

- Classification: Not Listed

Web of Trust

- Classification: Not Listed

Intelligence											
Date First	Last Modified	Type	Indicator	Country	Source	Severity	TLP	Confidence	Score Reported Confidence	Status	Impact
2019-07-23 20:34:44	2019-07-23 20:34:44	Detected DoI	45.124.94.245	VN	OTX	LOW	PAK	84	75	Active	
2019-07-21 00:02:08	2019-07-21 00:02:08	Scanning IP	45.124.94.245	VN	osint-ci-badguys DONT	LOW	PAK	84	70	Active	ci-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	LOW	PAK	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

Threat Model Import STIX

Threat Bulletines

10 1 - 10 of 5,907 items

Name	Last Updated
Anomali Community Threat Briefing: 2019-07-22	2019-07-23 03:49:41
CVE-2019-11107 Firefox zero-day exploited to infect ...	2019-07-22 22:18:00
Burned by Firefox part III: a Firefox 0day drops anot...	2019-07-22 17:48:43
Yoroi: Anti-Debugging Techniques from a Complex...	2019-07-22 17:48:19
Hard Pass: Declining APT34's Invite to Join Their Prof...	2019-07-21 18:55:00

[See more in Threat Bulletines](#)

Actors

10 1 - 10 of 200 items

Name	Last Updated
APT33	2019-07-19 05:28:39
Silence	2019-07-18 21:32:57
Cobalt Group	2019-07-10 22:30:36
APT3	2019-07-09 01:14:28
APT39	2019-07-03 23:38:46

[See more in Actors](#)

Campaigns

10 1 - 10 of 42 items

Name	Last Updated
Bad Tidings Campaign	2019-07-11 19:29:46
Adwind DDEInjection Campaign	2019-05-28 22:16:17
Tax Refund Phishing campaign against Canadian CI...	2019-02-21 08:44:50
CISA, DHS Issue Emergency Directive on DHS Tampa...	2019-01-29 06:08:25
GRIZZLY STEPPE	2019-01-28 01:35:50

[See more in Campaigns](#)

TTP

10 1 - 10 of 1,338 items

Name	Last Updated
CVE-2019-0888 POC	2019-07-18 10:29:36
Bypassing Electronic Locks and Access Controls (CA...	2019-07-08 16:35:29
[MITRE PRE-ATT&CK] Domain Generation Algorithm...	2019-06-24 23:45:59
[MITRE PRE-ATT&CK] Acquire or compromise 3rd pa...	2019-06-24 23:45:50
[MITRE PRE-ATT&CK] Acquire or compromise 3rd pa...	2019-06-24 23:45:41

[See more in TTP](#)

Incidents

10 1 - 10 of 139 items

Name	Last Updated
Chinese Security Department Breach	2019-07-17 23:28:04
Oregon DHS Breach	2019-07-16 20:02:36
Desjardins Data Leak	2019-07-16 19:59:37
Mandiant Senior Researcher Hacked #LeakTheAnaly...	2019-07-15 23:24:30
Silence Threat Group Targets Dutch-Bangla Bank	2019-07-09 23:28:04

[See more in Incidents](#)

Signatures

10 1 - 10 of 12,381 items

Name	Last Updated
eChDrax Ransomware Yara Signature	2019-07-22 22:12:55
RTF_Equation_Editor_CVE_2018_0798	2019-07-04 01:59:31
Nanocore Surveillance Plugin	2019-06-25 01:13:51
Nanocore RAT	2019-06-25 01:13:06
IPStorm Yara	2019-06-13 19:47:17

[See more in Signatures](#)

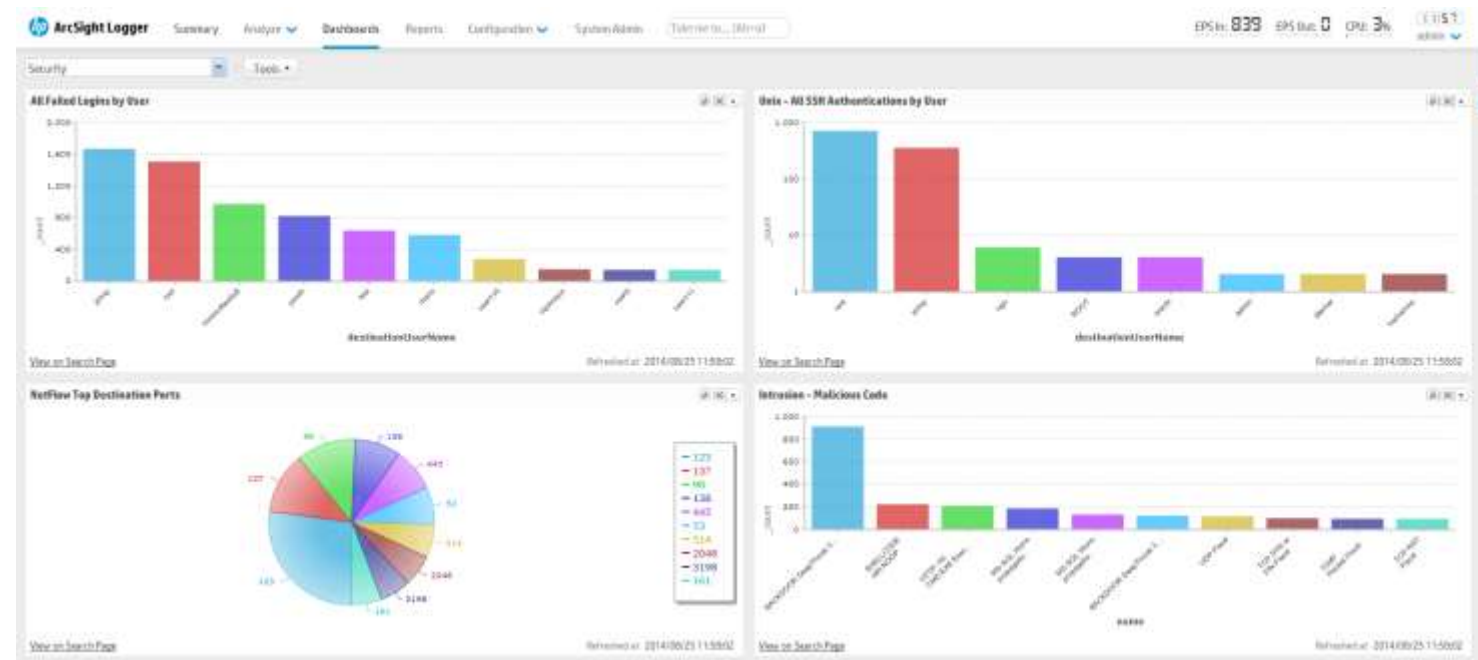
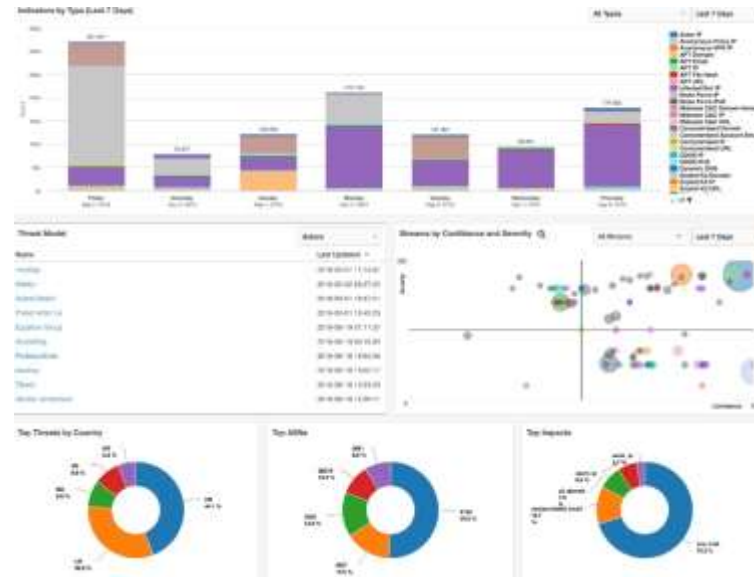
Vulnerabilities

10 1 - 10 of 125,493 items

Name	Last Updated
CVE-2018-14645	2019-07-23 17:15:00
CVE-2019-12221	2019-07-23 07:15:00

3. SIEM 과의 연동

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

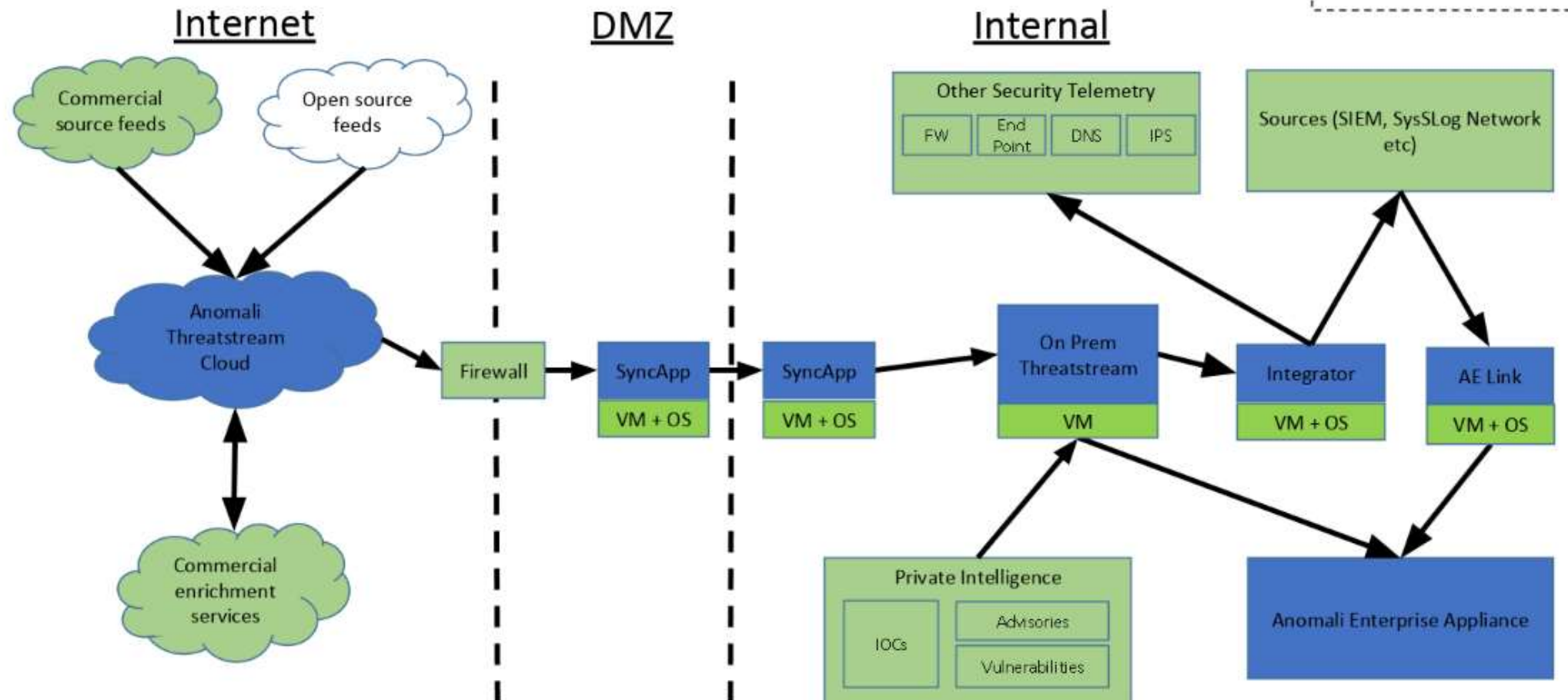


4. Offline 용 TI 정보 제공 시스템(Air gap)

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	Show Report	
<input type="checkbox"/>	2019-07-24 22:00:25	d4a81f7e3c15c9ad64...		Windows 7 (Office 20...	Anomali Community	Malicious	Show Report	
<input type="checkbox"/>	2019-07-24 22:00:21	71a643e25f79aa89b1...		Windows 7	Anomali Community	Malicious	Show Report	
<input type="checkbox"/>	2019-07-24 22:00:19	71a643e25f79aa89b1...		Windows 7 (Office 20...	Anomali Community	Malicious	Show Report	
<input type="checkbox"/>	2019-07-24 14:12:30	http://jobs-datastax....		Windows 7 (Office 20...	Anomali Community	Benign	Show Report	
<input type="checkbox"/>	2019-07-24 05:35:00	cb54e258084ebda32...		Windows 7	Anomali Community	Malicious	Show Report	
<input type="checkbox"/>	2019-07-24 05:34:58	4b54e258084ebda32...		Windows 7 (Office 20...	Anomali Community	Malicious	Show Report	

파일첨부

5. 추가 제공 서비스

③ Investigation

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

50 ▾	1 - 3 of 3 Items					Actions ▾
<input type="checkbox"/>	Date Created	Name	Status	Investigation Type	Owner	⚙
<input type="checkbox"/>	20 Jul 2019 07:08	new_incident_98_last	Unassigned	User Created	srinivas challa	
<input type="checkbox"/>	21 Jun 2019 22:57	SVDCNET001	Unassigned	User Created	Symantec User	
<input type="checkbox"/>	29 Mar 2019 03:28	WannaCry_Research	In Progress	User Created	Fatima Rodriguez	

5. 추가 제공 서비스

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

The screenshot illustrates the process of importing a PDF file into the ThreatStream interface. On the left, a Windows File Explorer window shows a folder named '00.Jisubsa' containing a file named 'ort-sample-report.pdf'. A blue arrow labeled 'Drag & Drop' points from this file to the 'New Import' window on the right. The 'New Import' window has a dark header and a light gray body. It features three tabs: 'Observables', 'STIX', and 'Email / Phishing'. The 'Observables' tab is selected. Under the heading '1. ADD DATA', there are three options: 'Upload a New File', 'Paste Intelligence', and 'Paste URL'. The 'Upload a New File' option is selected, and a green dashed box labeled 'Drop a file here' is visible. Below this box, it says 'Files must be under 10Mb in size'. The 'Paste Intelligence' option has a text area labeled 'Paste here'. The 'Paste URL' option also has a text area labeled 'Paste here'. At the bottom of the window, there are sections for '2. SET DEFINITIONS', including 'Intelligence Source', 'Threat Type' (set to 'Malware'), and 'TLP'. A 'Confidence' slider is also present, ranging from 10 to 100, with a checkbox for 'Override System Confidence'.

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 [Winni](#)
- **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.

