ELLIO

Actionable IP Threat Intel

ELLIO: IP Threat Intel delivers real-time threat intelligence that helps security teams reduce alert fatigue and speed up triage in TIPs, SIEM & SOAR platforms.

Reduce alert fatigue.

Accelerate Triage.

Boost teams' Performance.

Gain critical insight.

Enrich SIEM events.

Data delivery that fits your use-case.

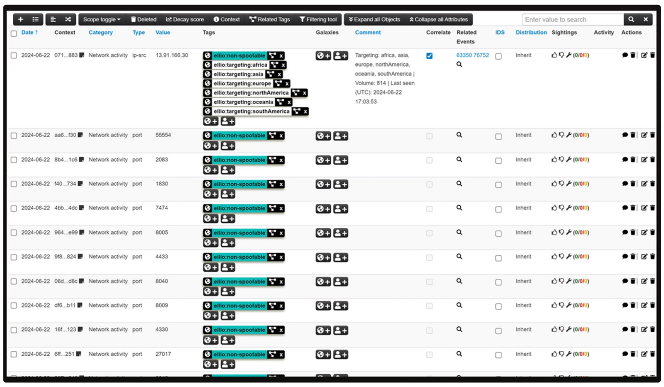
Available as an API for your SIEM/SOAR/TIP or as a local database for most demanding on-premise workloads.

MISP Threat Sharing {json} logstash

MISP Feed

Extended Feed provides detailed information on IP addresses observed in the last 30 days, including ports targeted by an IP.

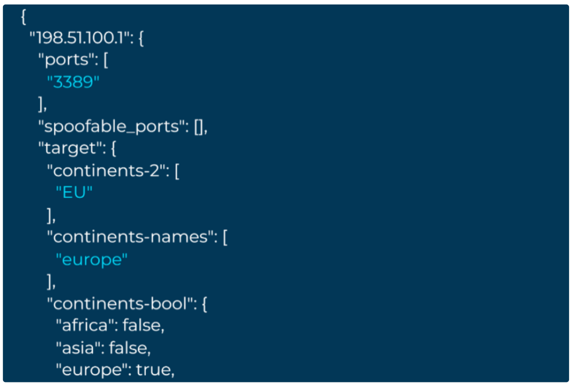
Daily Feed provides a list of all IP addresses observed today.



☐	Date ↑	Context	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	IDS	Distribution	Sightings	Activity	Actions
☐	2024-06-22	071...883	Network activity	ip-src	13.91.166.30	ellio:non-spoofable ellio:targeting:africa ellio:targeting:asia ellio:targeting:europe ellio:targeting:northAmerica ellio:targeting:oceania ellio:targeting:southAmerica		Targeting: africa, asia, europe, northAmerica, oceania, southAmerica | Volume: 814 | Last seen (UTC): 2024-06-22 17:03:53	☑	63350 76752	☐	Inherit	(0/0/0)		
☐	2024-06-22	aa6...f30	Network activity	port	55554	ellio:non-spoofable			☐		☐	Inherit	(0/0/0)		
☐	2024-06-22	8b4...1c6	Network activity	port	2083	ellio:non-spoofable			☐		☐	Inherit	(0/0/0)		
☐	2024-06-22	f40...734	Network activity	port	1830	ellio:non-spoofable			☐		☐	Inherit	(0/0/0)		
☐	2024-06-22	4bb...4dc	Network activity	port	7474	ellio:non-spoofable			☐		☐	Inherit	(0/0/0)		
☐	2024-06-22	964...e99	Network activity	port	8005	ellio:non-spoofable			☐		☐	Inherit	(0/0/0)		
☐	2024-06-22	9f8...824	Network activity	port	4433	ellio:non-spoofable			☐		☐	Inherit	(0/0/0)		
☐	2024-06-22	06d...d8c	Network activity	port	8040	ellio:non-spoofable			☐		☐	Inherit	(0/0/0)		
☐	2024-06-22	df6...b11	Network activity	port	8009	ellio:non-spoofable			☐		☐	Inherit	(0/0/0)		
☐	2024-06-22	16f...123	Network activity	port	4330	ellio:non-spoofable			☐		☐	Inherit	(0/0/0)		
☐	2024-06-22	6ff...251	Network activity	port	27017	ellio:non-spoofable			☐		☐	Inherit	(0/0/0)		

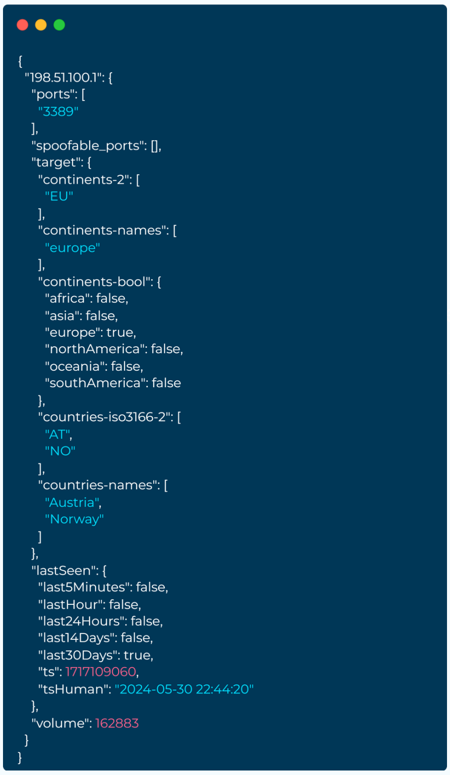
JSON Feed

JSON Feed, updated every 5 minutes, provides an exhaustive list of all IPs detected by ELLIO's advanced deception network over the past 30 days, delivered in a clear and accessible JSON format.



```
{
 "198.51.100.1": {
  "ports": [
   "3389"
  ],
  "spoofable_ports": [],
  "target": {
   "continents-2": [
    "EU"
   ],
   "continents-names": [
    "europe"
   ],
   "continents-bool": {
    "africa": false,
    "asia": false,
    "europe": true,
```

ELLIO Technology | ellio.tech | info@ellio.tech



```
{
  "198.51.100.1": {
    "ports": [
      "3389"
    ],
    "spoofable_ports": [],
    "target": {
      "continents-2": [
        "EU"
      ],
      "continents-names": [
        "europe"
      ],
      "continents-bool": {
        "africa": false,
        "asia": false,
        "europe": true,
        "northAmerica": false,
        "oceania": false,
        "southAmerica": false
      },
      "countries-iso3166-2": [
        "AT",
        "NO"
      ],
      "countries-names": [
        "Austria",
        "Norway"
      ]
    },
    "lastSeen": {
      "last5Minutes": false,
      "lastHour": false,
      "last24Hours": false,
      "last14Days": false,
      "last30Days": true,
      "ts": 1717109060,
      "tsHuman": "2024-05-30 22:44:20"
    },
    "volume": 162883
  }
}
```

JSON Feed

JSON Feed provides an exhaustive list of all IPs detected by ELLIO's advanced deception network over the past 30 days, delivered in a clear and accessible JSON format. **Updated every 5 minutes**, this feed ensures you stay ahead of emerging threats with most up-to-date data available.

With detailed information on IPs, contacted ports, targeted regions, and event volume, ELLIO: IP Threat Intel feed empowers you to **automate your workflow with precision**.

It's designed to meet the needs of customers managing large volumes of events and it's perfect for environments requiring data enrichment, air-gapped systems, and custom workflows. The demand for this high-frequency format has been driven by the critical requirements of government Security Operations Centers and the sensitive workloads of the financial industry.

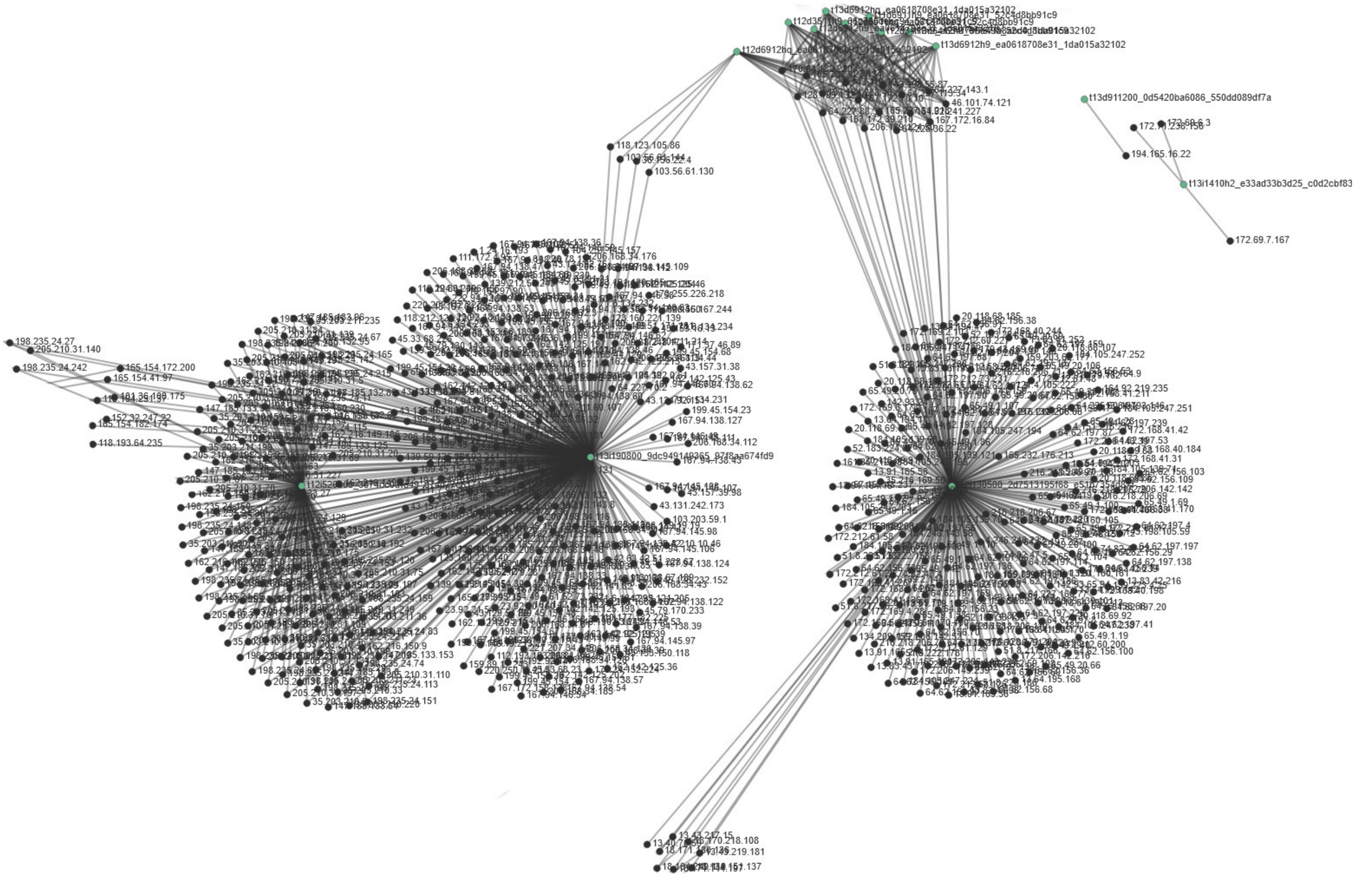
Fingerprints. At your fingertips.

Optional addon that includes fingerprints for all observed IPs during last 30 days.

JA3

NEW! JA4

NEW! JA4+



Try demo samples. See ELLIO in action.

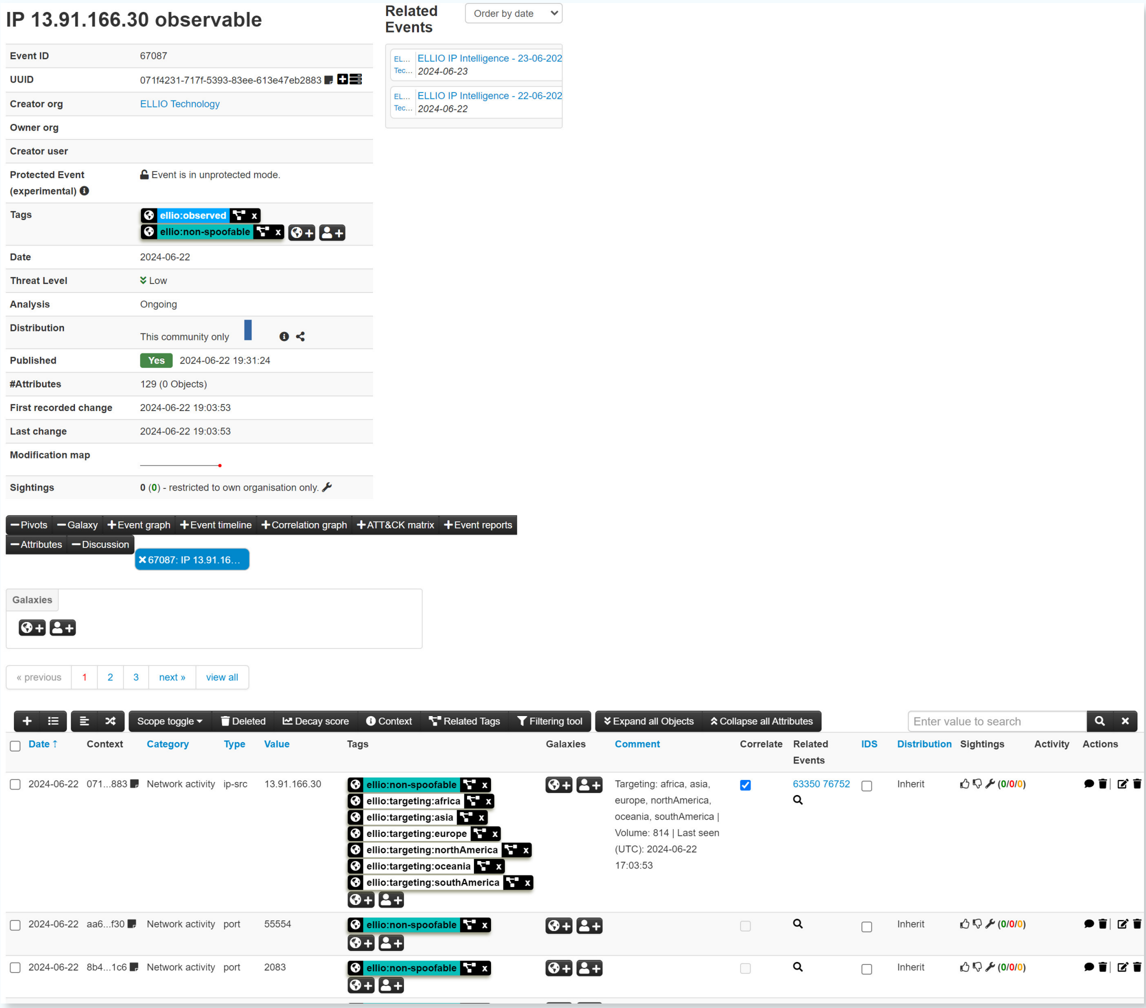
Test ELLIO’s demo samples of the daily and extended feeds in your MISP instance.
For the download link and more information, visit our Demo Space page or contact us.

Visit
Demo Space

Email us
info@ellio.tech.

triage in TIPs, SIEM & SOAR platforms

Demo samples | Extended Feed in your MISP instance:



IP 13.91.166.30 observable

Event ID	67087
UUID	071f4231-717f-5393-83ee-613e47eb2883
Creator org	ELLIO Technology
Owner org	
Creator user	
Protected Event (experimental)	Event is in unprotected mode.
Tags	ellio:observed x ellio:non-spoofable x
Date	2024-06-22
Threat Level	Low
Analysis	Ongoing
Distribution	This community only
Published	Yes 2024-06-22 19:31:24
#Attributes	129 (0 Objects)
First recorded change	2024-06-22 19:03:53
Last change	2024-06-22 19:03:53
Modification map	
Sightings	0 (0) - restricted to own organisation only.

Related Events

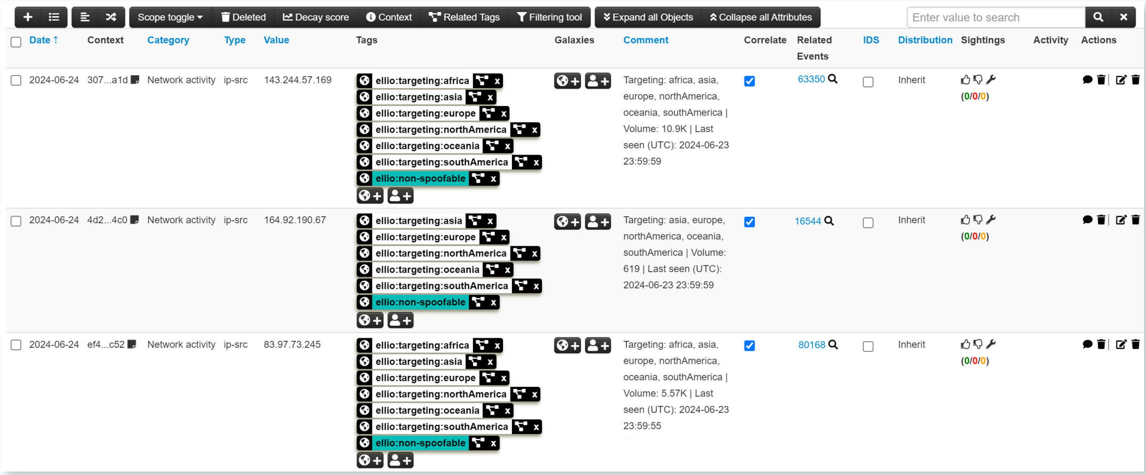
Order by date

EL... Tec...	ELLIO IP Intelligence - 23-06-202 *2024-06-23*
EL... Tec...	ELLIO IP Intelligence - 22-06-202 *2024-06-22*

—Pivots —Galaxy +Event graph +Event timeline +Correlation graph +ATT&CK matrix +Event reports
—Attributes —Discussion
✕67087: IP 13.91.16...
Galaxies
« previous 1 2 3 next » view all
Scope toggle Deleted Decay score Context Related Tags Filtering tool Expand all Objects Collapse all Attributes
Enter value to search

□	Date ↑	Context	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	IDS	Distribution	Sightings	Activity	Actions
□	2024-06-22	071...883	Network activity	ip-src	13.91.166.30	ellio:non-spoofable x ellio:targeting:africa x ellio:targeting:asia x ellio:targeting:europe x ellio:targeting:northAmerica x ellio:targeting:oceania x ellio:targeting:southAmerica x		Targeting: africa, asia, europe, northAmerica, oceania, southAmerica | Volume: 814 | Last seen (UTC): 2024-06-22 17:03:53	☑	63350 76752	□	Inherit	(0/0/0)		
□	2024-06-22	aa6...f30	Network activity	port	55554	ellio:non-spoofable x			□		□	Inherit	(0/0/0)		
□	2024-06-22	8b4...1c6	Network activity	port	2083	ellio:non-spoofable x			□		□	Inherit	(0/0/0)		

Demo samples | Daily Feeds in your MISP instance:



Scope toggle Deleted Decay score Context Related Tags Filtering tool Expand all Objects Collapse all Attributes
Enter value to search

□	Date ↑	Context	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	IDS	Distribution	Sightings	Activity	Actions
□	2024-06-24	307...a1d	Network activity	ip-src	143.244.57.169	ellio:targeting:africa x ellio:targeting:asia x ellio:targeting:europe x ellio:targeting:northAmerica x ellio:targeting:oceania x ellio:targeting:southAmerica x ellio:non-spoofable x		Targeting: africa, asia, europe, northAmerica, oceania, southAmerica | Volume: 10.9K | Last seen (UTC): 2024-06-23 23:59:59	☑	63350	□	Inherit	(0/0/0)		
□	2024-06-24	4d2...4c0	Network activity	ip-src	164.92.190.67	ellio:targeting:asia x ellio:targeting:europe x ellio:targeting:northAmerica x ellio:targeting:oceania x ellio:targeting:southAmerica x ellio:non-spoofable x		Targeting: asia, europe, northAmerica, oceania, southAmerica | Volume: 619 | Last seen (UTC): 2024-06-23 23:59:59	☑	16544	□	Inherit	(0/0/0)		
□	2024-06-24	ef4...c52	Network activity	ip-src	83.97.73.245	ellio:targeting:africa x ellio:targeting:asia x ellio:targeting:europe x ellio:targeting:northAmerica x ellio:targeting:oceania x ellio:targeting:southAmerica x ellio:non-spoofable x		Targeting: africa, asia, europe, northAmerica, oceania, southAmerica | Volume: 5.57K | Last seen (UTC): 2024-06-23 23:59:55	☑	80168	□	Inherit	(0/0/0)		