ELLIO: Experts on mass vulnerability exploitation, botnets, and cybernoise.

Real-time detection for highly accurate, customized blocking, data enrichment, and automation processes.

We filter out the noise.
You focus on what really matters.

ELLIO offers advanced network security solutions that provide real-time visibility and context into mass vulnerability exploitation, botnets, cybernoise, and other scanning activities on the Internet.

ELLIO IP Threat Intelligence and IP blocklists help security teams reduce alert fatigue, accelerate triage, enhance automation processes, and improve protection capabilities of next-gen network firewalls, leading to more efficient security operations and better-optimized resource allocation.

ELLIO's solutions integrate with SOAR, SIEM, TIP, and next-gen network firewalls.

info@ellio.tech | ellio.tech

ELLIO IP datasets is

4x larger

15x faster

2x more dynamic

We helps security teams in organisations of all sizes to

SOAR, SIEM, TIP

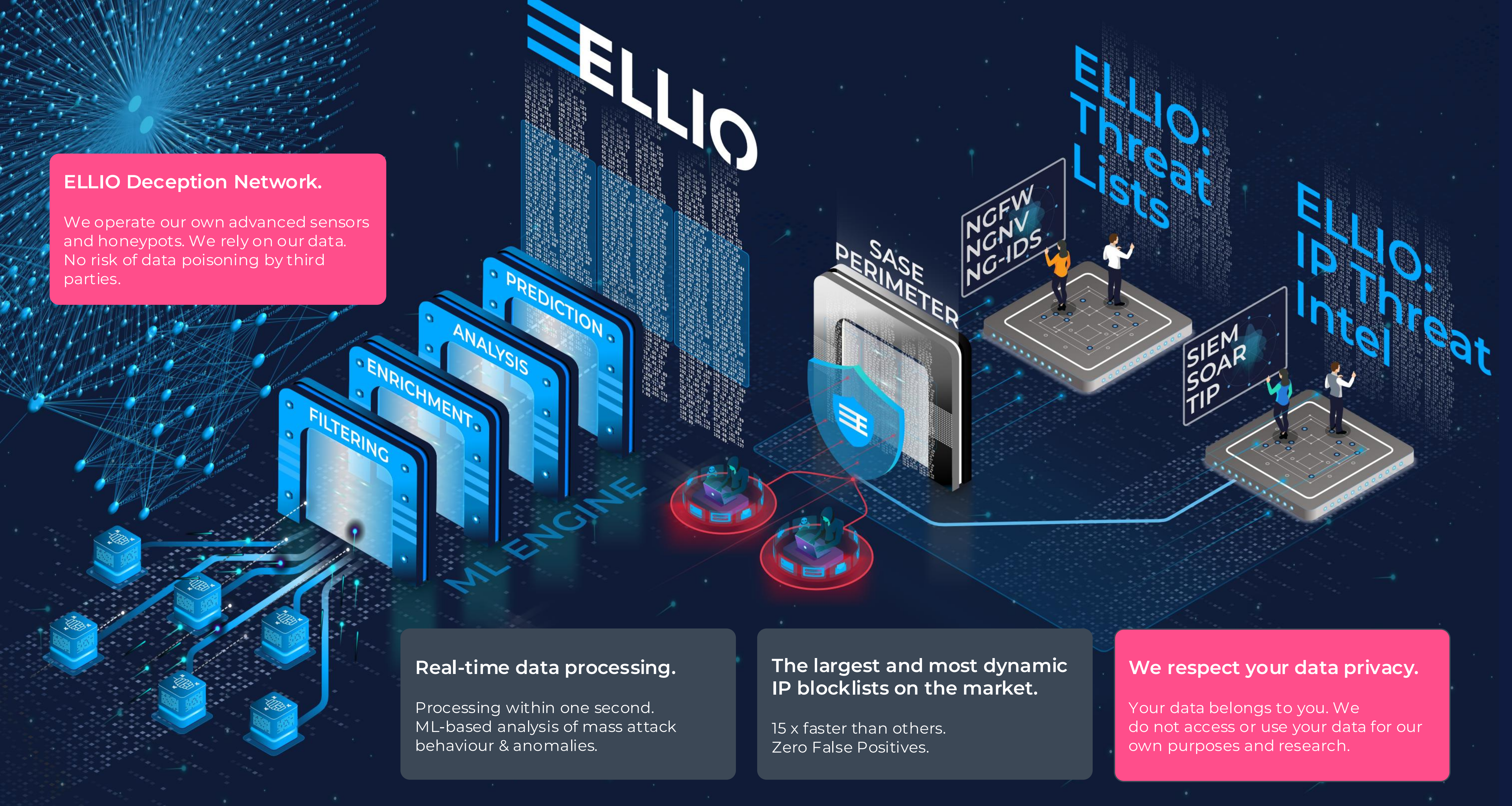
- Reduce alert fatigue.
- Fine-tune automation.
- Enhance prioritization.
- Speed up triage process.
- Enrich SIEM events.

Perimeter Defense

- Block mass exploitation.
- Reduce perimeter footprint.
- Filter out botnets.
- Reduce risk of L7 DDoS.
- Hold off attackers until detection are available.

Traffic Monitoring

- Provide latest information on malicious activities that hits your network.
- Help identify malicious actors that use your services for illicit activities.



ELLIO Deception Network.

We operate our own advanced sensors and honeypots. We rely on our data. No risk of data poisoning by third parties.

Real-time data processing.

Processing within one second.
ML-based analysis of mass attack behaviour & anomalies.

The largest and most dynamic IP blocklists on the market.

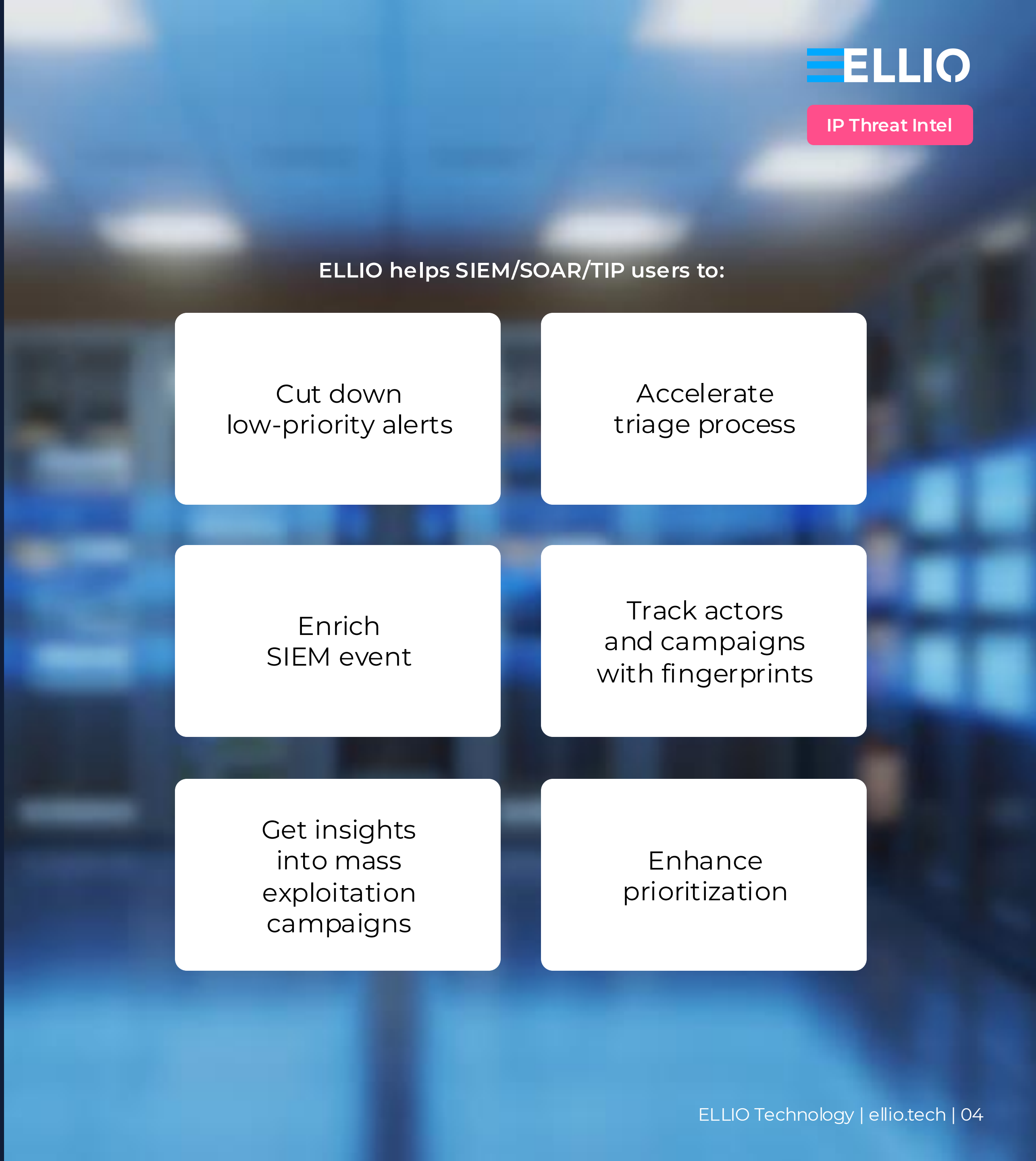
15 x faster than others.
Zero False Positives.

We respect your data privacy.

Your data belongs to you. We do not access or use your data for our own purposes and research.

Actionable IP Threat Intel for higher SOC's performance

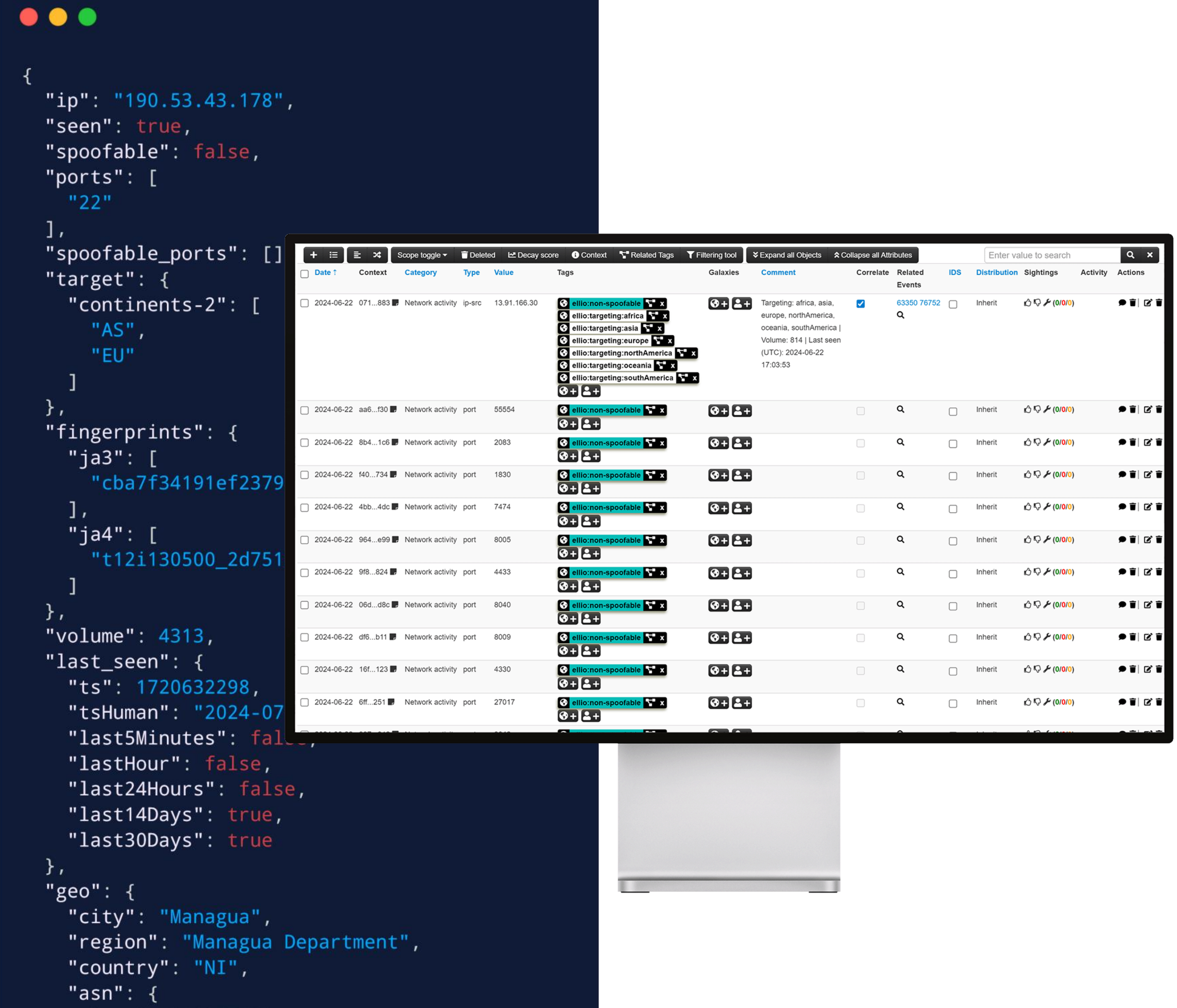
ELLIO: IP Threat Intel is a real-time threat intelligence designed to reduce alert fatigue and speed up triage processes in existing TIP, SIEM & SOAR platforms.



ELLIO helps SIEM/SOAR/TIP users to:

- Cut down low-priority alerts
- Accelerate triage process
- Enrich SIEM event
- Track actors and campaigns with fingerprints
- Get insights into mass exploitation campaigns
- Enhance prioritization

IP Threat Intel



```
{
  "ip": "190.53.43.178",
  "seen": true,
  "spoofable": false,
  "ports": [
    "22"
  ],
  "spoofable_ports": []
  "target": {
    "continents-2": [
      "AS",
      "EU"
    ]
  },
  "fingerprints": {
    "ja3": [
      "cba7f34191ef2379
    ],
    "ja4": [
      "t12i130500_2d751
    ]
  },
  "volume": 4313,
  "last_seen": {
    "ts": 1720632298,
    "tsHuman": "2024-07
    "last5Minutes": fal  ,
    "lastHour": false,
    "last24Hours": false,
    "last14Days": true,
    "last30Days": true
  },
  "geo": {
    "city": "Managua",
    "region": "Managua Department",
    "country": "NI",
    "asn": {
```

☐	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)		
☐	2024-06-22	f40...734	Network activity	port	1830	ellio:non-spoofable x			☐		☐	Inherit	(0/0/0)		
☐	2024-06-22	4bb...4dc	Network activity	port	7474	ellio:non-spoofable x			☐		☐	Inherit	(0/0/0)		
☐	2024-06-22	964...e99	Network activity	port	8005	ellio:non-spoofable x			☐		☐	Inherit	(0/0/0)		
☐	2024-06-22	9f8...824	Network activity	port	4433	ellio:non-spoofable x			☐		☐	Inherit	(0/0/0)		
☐	2024-06-22	06d...d8c	Network activity	port	8040	ellio:non-spoofable x			☐		☐	Inherit	(0/0/0)		
☐	2024-06-22	df6...b11	Network activity	port	8009	ellio:non-spoofable x			☐		☐	Inherit	(0/0/0)		
☐	2024-06-22	16f...123	Network activity	port	4330	ellio:non-spoofable x			☐		☐	Inherit	(0/0/0)		
☐	2024-06-22	6ff...251	Network activity	port	27017	ellio:non-spoofable x			☐		☐	Inherit	(0/0/0)		

Data delivery that **fits your use-case**

ELLIO: IP Threat Intel is available as an API for your SIEM/SOAR/TIP or as a local database for most demanding on-premise workloads.

- **API**
- **Bulk data access / feed**

{json} MISP Threat Sharing logstash

ELLIO IP Blocklists

Your reliable defense against ever increasing cybernoise.

Hold off attackers until detections are available.	Block attackers immediately, giving security vendors and your team time to detect and patch new vulnerabilities before they reach your network.
Block mass exploitation.	Prevent large-scale cyberattacks by automatically blocking traffic from malicious sources, protecting your network from new widespread vulnerabilities.
Reduce perimeter footprint.	Filter out traffic from scanners, making your network and company invisible to search engineers for internet-connected devices like Censys.
Filter out evil bots.	Stop bots that scan, spam, or abuse your network, prevent reconnaissance and potential attacks.

IP Blocklists

ELLIO. Beyond traditional blocklists.

	ELLIO: Threat List **MAX**	ELLIO: Threat List **ONE**
THREAT PROTECTION		
Average Size	175,000 - 400,000 entities	40,000 - 90,000 entities
Update Frequency	• Every minute • Every 5 minutes • Every 30 minutes	• Every 5 minutes • Every 30 minutes • Every 60 minutes
Tailored to network perimeter	Comprehensive coverage, no need for tailoring	Yes
COMPATIBILITY		
ntopng	✓	✓
Palo Alto Networks NGFW	✓	✓
Check Point NGFW	✓	✓
Fortinet NGFW	✓	✓
Cisco NGFW	✓	✓
F5 NGFW	✓	✓
OPNSense	✓	✓
pfSense	✓	✓
TARGET AUDIENCE		
Suitable for backbone network appliances	✓	-
Suitable for medium and large enterprises	✓	-
Recommended for	• Medium and Large Enterprises • ISPs • Data Centers • Government • MSSPs	• Satellite Offices • SMBs • Regional MSPs
FEATURES		
Self-service web portal	-	✓
Multi-tenancy	-	✓
PRICING		
Pricing model	Per corporate entity and use case	Per public perimeter IP address
Price	Starts at $999/month. Pricing	Starts at $99/month per IP address. Pricing

ELLIO IP Blocklists

ELLIO allows your network to disappear from internet-wide scanning services such as Shodan, Censys.io, and BinaryEdge, which are frequently used by malicious actors to locate new targets.

Successful customer story I.

ELLIO for Checkpoint NGFW

CHECK POINT™

3.000.000

ELLIO filtered out more than 3 million unwanted events for the customer in just 45 days.

100.000

Over 100.000 threat lists were automatically downloaded from ELLIO for the customer in just 45 days.

60.000

Each dynamic ELLIO: Threat List ONE contained an average of over 60.000 rules during the given 45-day period.

800%

After activating ELLIO: Threat List ONE, the number of detections increased by more than 800% within the 'New Anti-Virus' blade on Check Point.

Successful customer story II.

ELLIO for Fortinet NGFW

FORTINET®

38.000.000

ELLIO: Threat List filtered out more than 38 million unwanted connections during 30 day period.

270.000

Each dynamic ELLIO: Threat List MAX contained on average over 270.000 IP addresses.

8.640

8.640 different threat lists were automatically downloaded by the customers' NGFW during 30 day period.

0

After activating ELLIO: Threat List MAX, the number of reported False Positives is zero.

Successful customer story III.

ELLIO for pfSense NGFW

15%

The overall traffic to the customers' network dropped by 15% after 2 months. This includes traffic from bots, spray-and-pray attackers and opportunistic exploitations attempts.

75.000

Each dynamic ELLIO: Threat List ONE contained on average over 75.000 rules.

720

720 different 60-minte threat lists were automatically downloaded by the customers' firewall during 30 days.

60 days

After activating ELLIO: Threat List ONE, customers' infrastructure disappeared from services like Shodan and Censys after 60 days.

You might find interesting

Demo Space

Try ELLIO and experience all its benefits with free trials, data samples, or customized pilot programs.

ellio.tech/demo-space

Partners

Become our Partner and gain benefits that drive business growth through innovative highly reliable security offerings.

ellio.tech/partners

Pricing

Choose your pricing plan according your needs and requirements. If you have any questions, feel free to reach out to us at sales@ellio.tech.

ellio.tech/purchasing/pricing

Blog

Find out what's new in our products. In the ELLIO Blog you will find practical tutorials, company updates, or industry insights.

blog.ellio.tech

ELLIO

info@ellio.tech | ellio.tech | Linkedin | X | Mastodon | Discord | ELLIO Community Slack