Threat Intel README

Threat Intelligence Aggregator

Description

Threat Intelligence Aggregator is a Python-driven dashboard that brings together real-time threat intelligence from **VirusTotal, Shodan, and AbuseIPDB** into a single platform. It allows security teams and analysts to rapidly assess the risk level of various IOCs (Indicators of Compromise) such as **IP addresses, domains, URLs, and file hashes**. By integrating multiple established open threat intelligence sources, the tool helps identify, prioritize, and report cyber threats efficiently.

Features

- **Multi-Source Lookup:** Scan **IP addresses, domains, URLs, or file hashes** across VirusTotal, Shodan, and AbuseIPDB APIs.
- **Automated Risk Assessment:** Each IOC is automatically assessed and categorized as *High*, *Medium*, *Low*, or *Legitimate* risk based on intelligence data.
- **Batch Scanning:** Quickly process large lists by uploading CSV files of IOCs for automated scanning and enrichment.
- **Interactive Dashboard:** Visualize findings, trends, and summaries through an intuitive Streamlit web dashboard.
- **Report Generation:** Export comprehensive PDF reports of scan results for sharing and documentation.
- **API Key Management:** Secure interface to input and manage your API keys easily from within the dashboard.
- **Support & Contact:** Built-in section for reaching out if help or feedback is needed.

Technologies Used

- **Python 3.8+** – Core programming language
- **Streamlit** – For building interactive web dashboards
- **pandas** – Data handling and manipulation
- **requests** – HTTP calls to external threat APIs
- **plotly** – Visualization and charts
- **fpdf** – PDF report generation
- **shodan** – Accessing the Shodan threat intelligence database
- **virustotal-python** – VirusTotal API integration
- **AbuseIPDB API (via requests)** – IP reputation lookups
- **CSV** – Bulk data import/export

Setup Instructions

1. **Clone the repository:**

```
bashgit clone https://github.com/yourusername/threat-intel-aggregator.git
cd threat-intel-aggregator
```

2. **Install dependencies:**

```
bashpip install -r requirements.txt
```

3. **Run the app:**

```
bashstreamlit run streamlit_app.py
```

4. **Configure API Keys:**

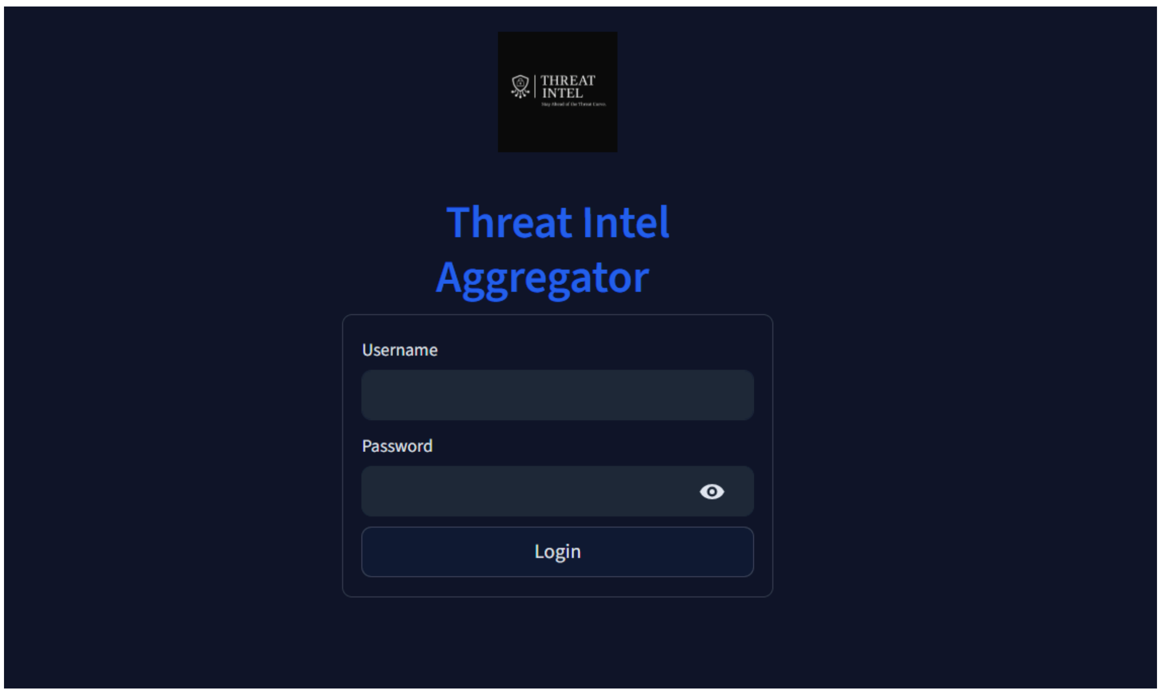
   Go to the **Settings** section of the app's dashboard and add your VirusTotal, Shodan, and AbuseIPDB API keys.

How to Use

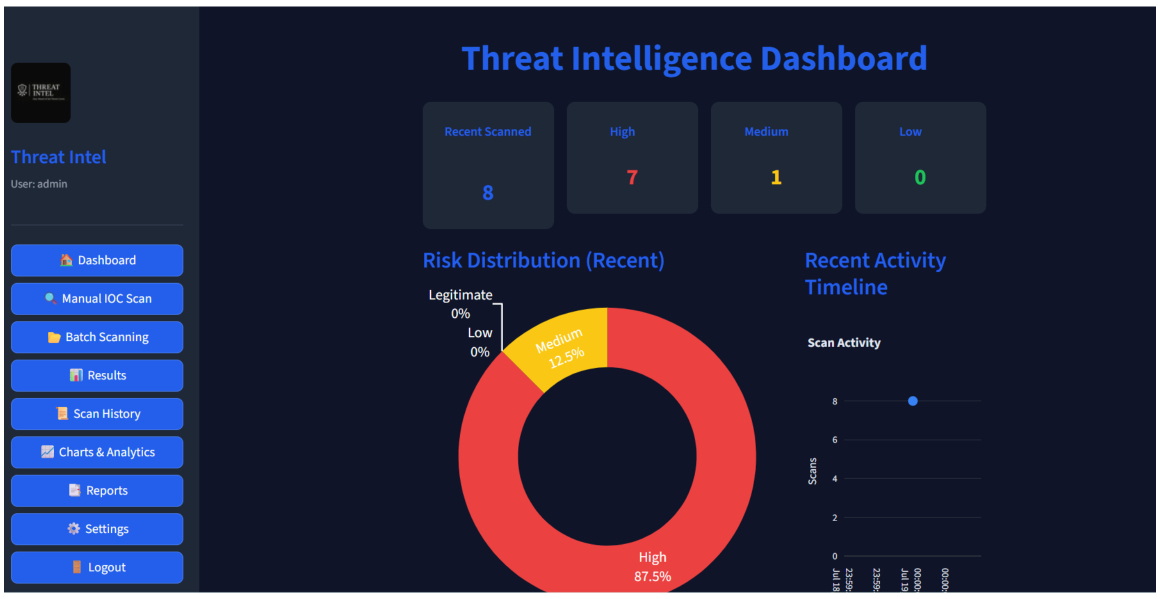
- **Single Scan:** Enter an IP, domain, URL, or file hash into the scan form for immediate threat analysis across all integrated platforms.
- **Batch/CSV Scan:** Upload a `.csv` file containing a list of IOCs (IPs, domains, URLs, hashes) for mass processing. Results will be automatically categorized and displayed.
- **Dashboard Visualization:** Review threats, trends, and flagged items interactively. Apply filters to focus on timeframes, threat types, or individual IOCs (similar to professional SOC dashboards).
- **PDF Reporting:** After scanning, export results to a well-formatted PDF report for sharing (email option) or compliance.
- **Settings:** Update your API credentials at any time within the app.

Screenshots

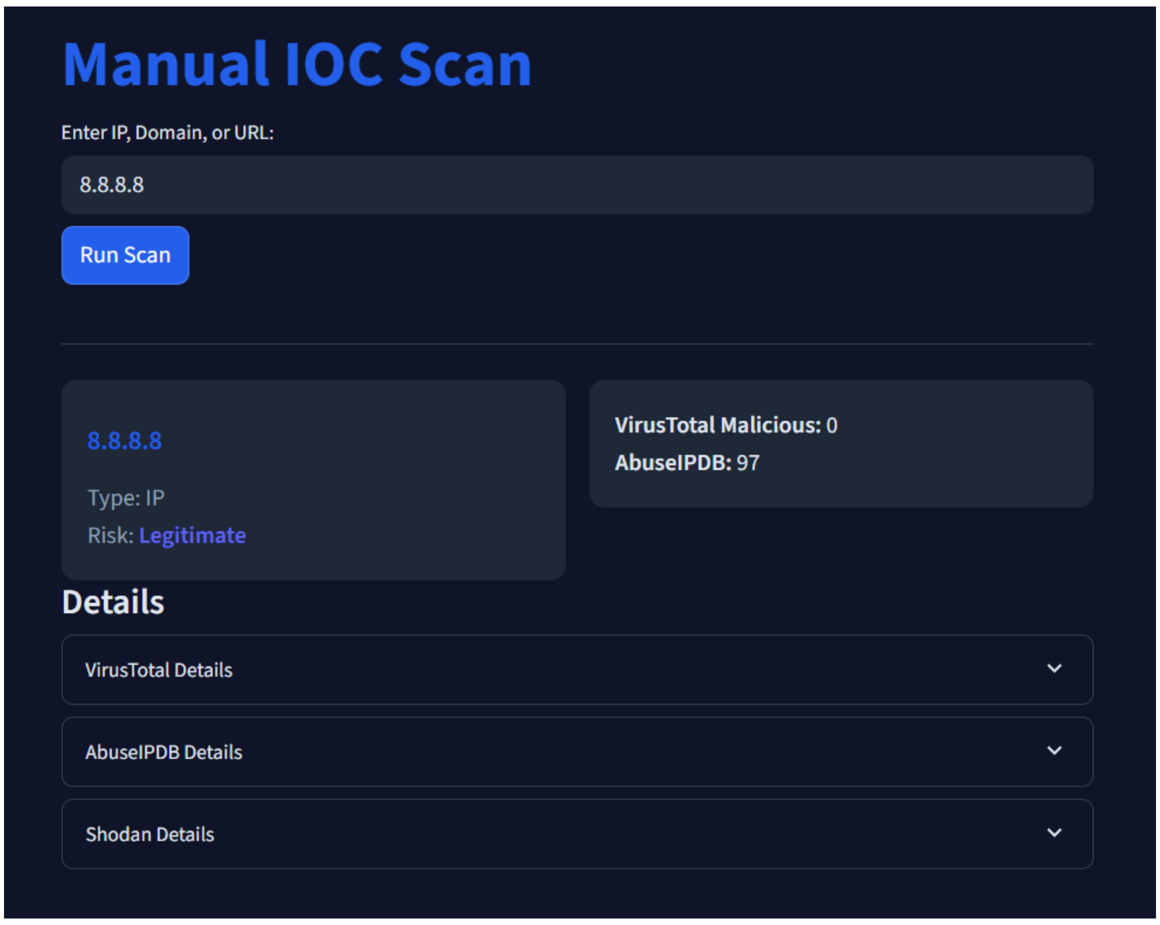
- The login page :



- The dashboard main view :



- Example scan results :
- manual IOC Scan :



Manual IOC Scan

Enter IP, Domain, or URL: 8.8.8.8

8.8.8.8

Type: IP

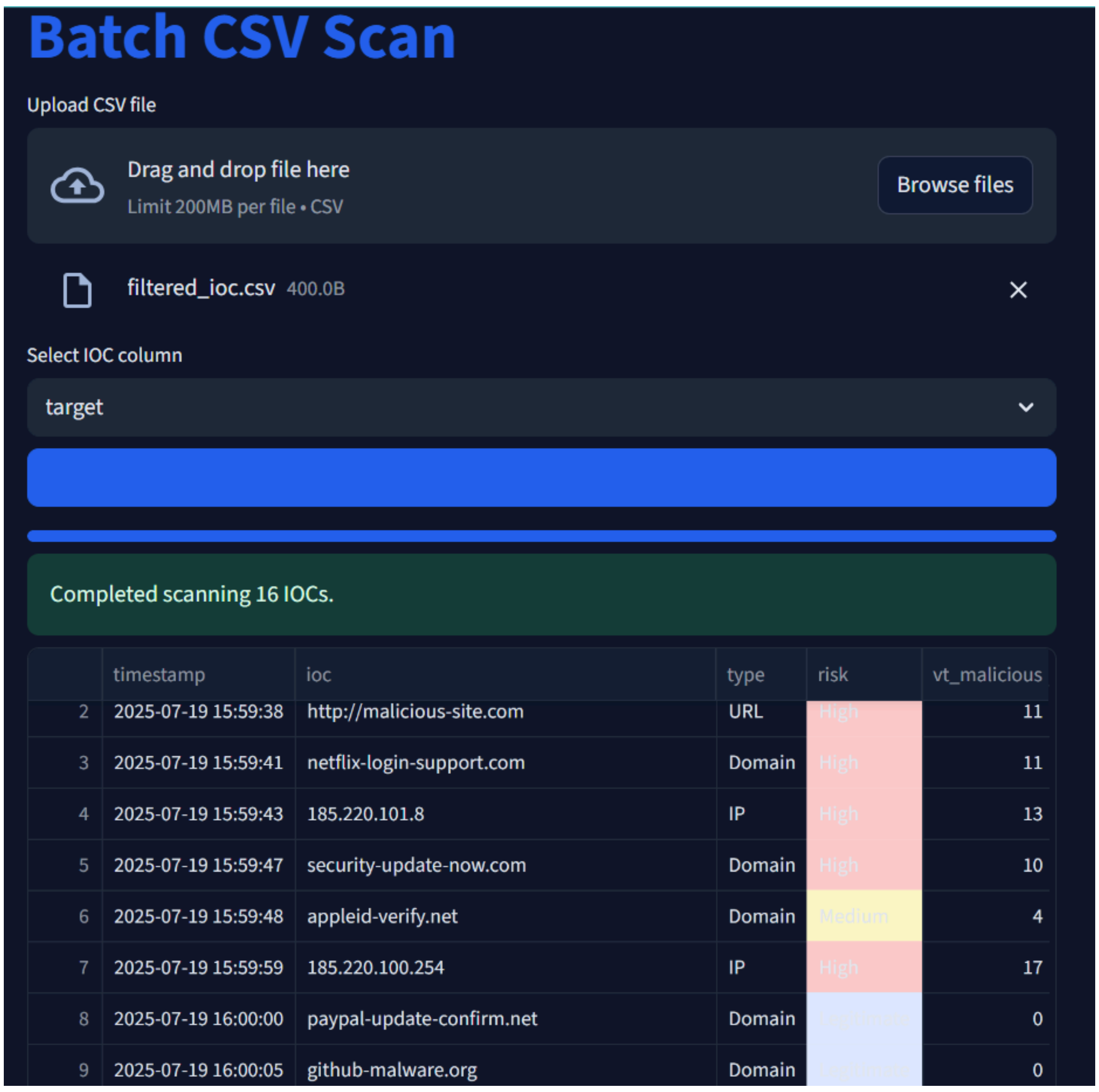
Risk: Legitimate

VirusTotal Malicious: 0

AbuseIPDB: 97

Details

- Batch scan:



Batch CSV Scan

Upload CSV file

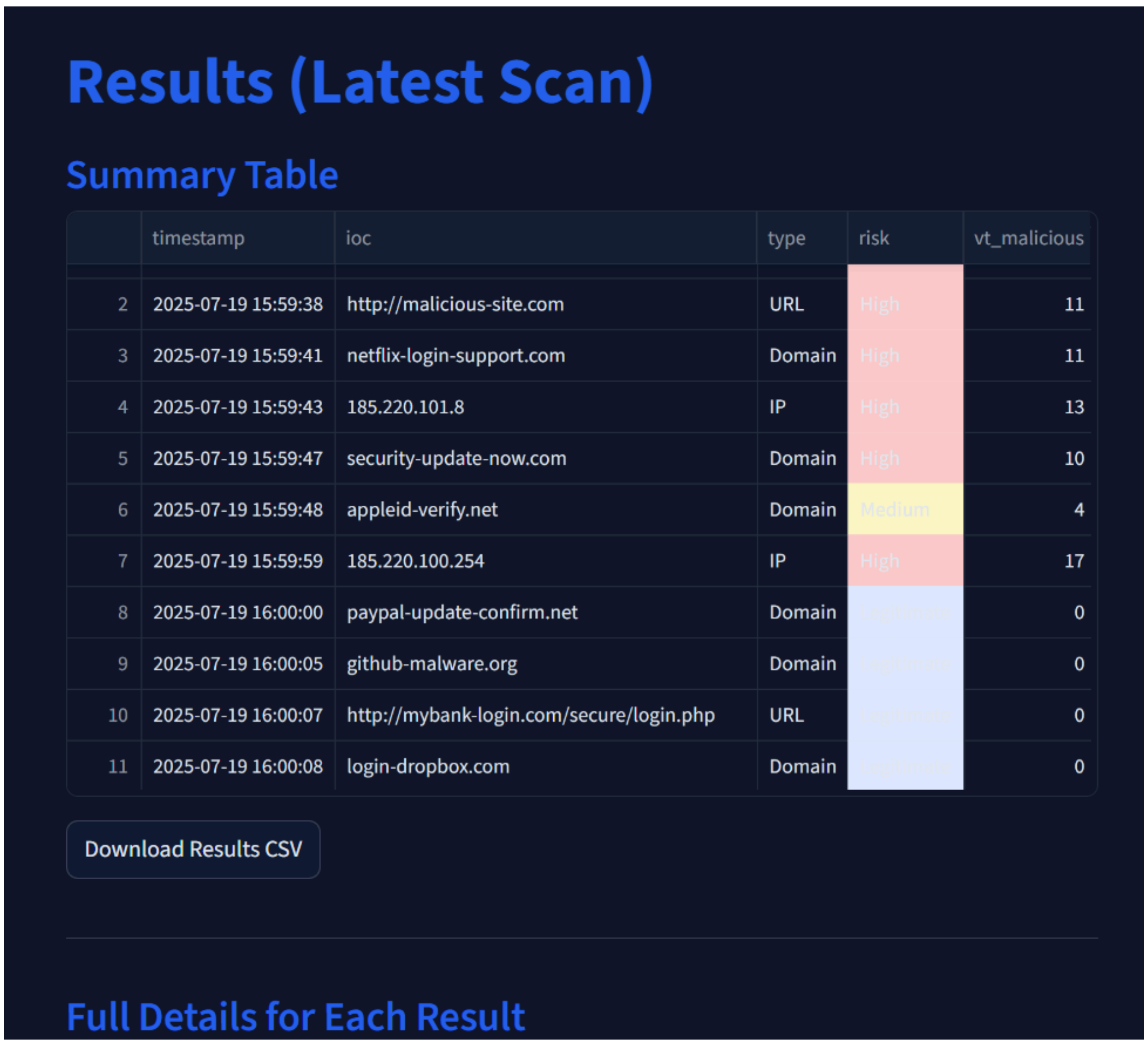
filtered_ioc.csv 400.0B

Select IOC column: target

Completed scanning 16 IOCs.

	timestamp	ioc	type	risk	vt_malicious
2	2025-07-19 15:59:38	http://malicious-site.com	URL	High	11
3	2025-07-19 15:59:41	netflix-login-support.com	Domain	High	11
4	2025-07-19 15:59:43	185.220.101.8	IP	High	13
5	2025-07-19 15:59:47	security-update-now.com	Domain	High	10
6	2025-07-19 15:59:48	appleid-verify.net	Domain	Medium	4
7	2025-07-19 15:59:59	185.220.100.254	IP	High	17
8	2025-07-19 16:00:00	paypal-update-confirm.net	Domain	Legitimate	0
9	2025-07-19 16:00:05	github-malware.org	Domain	Legitimate	0

- Results with more details:



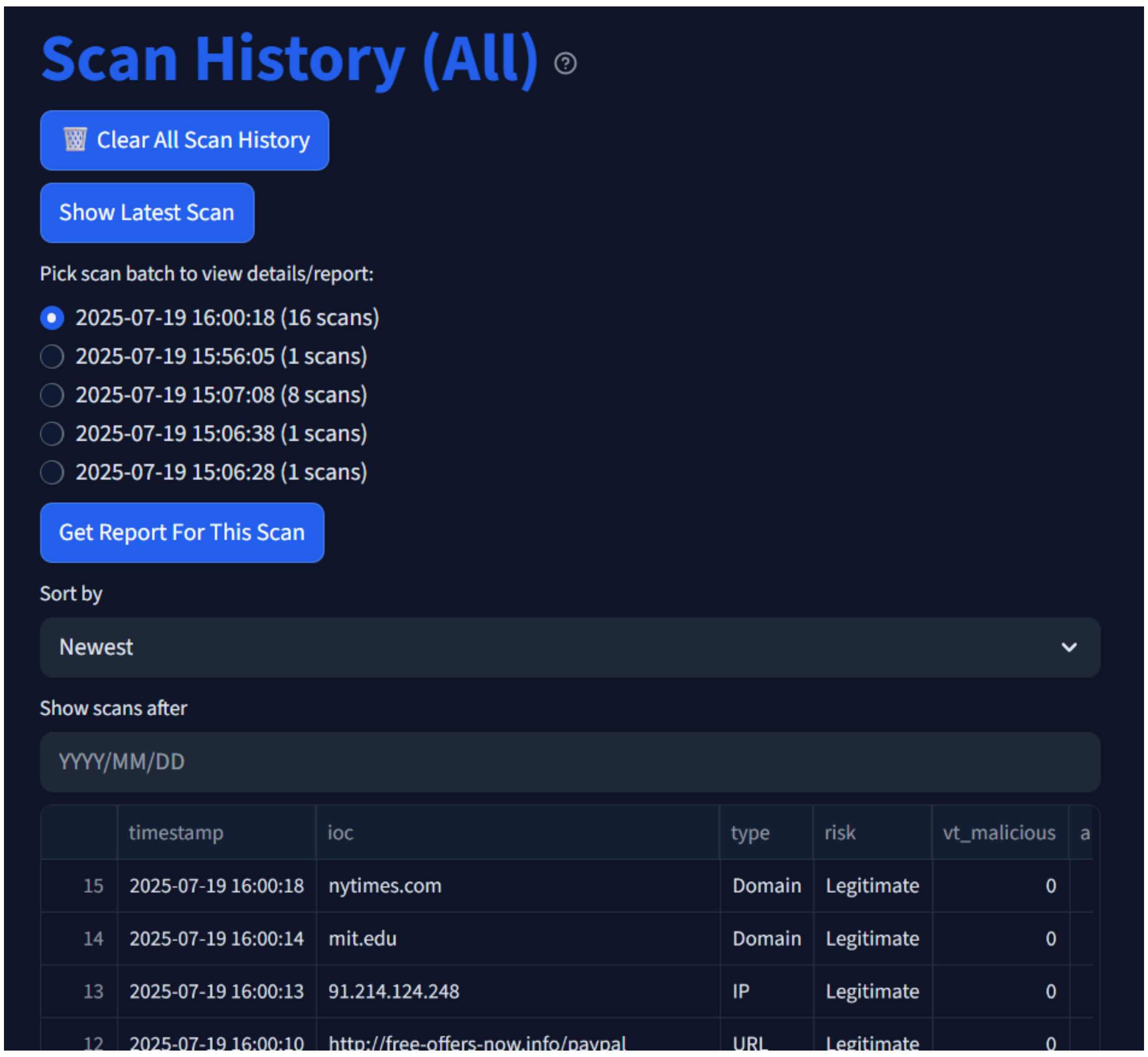
Results (Latest Scan)

Summary Table

	timestamp	ioc	type	risk	vt_malicious
2	2025-07-19 15:59:38	http://malicious-site.com	URL	High	11
3	2025-07-19 15:59:41	netflix-login-support.com	Domain	High	11
4	2025-07-19 15:59:43	185.220.101.8	IP	High	13
5	2025-07-19 15:59:47	security-update-now.com	Domain	High	10
6	2025-07-19 15:59:48	appleid-verify.net	Domain	Medium	4
7	2025-07-19 15:59:59	185.220.100.254	IP	High	17
8	2025-07-19 16:00:00	paypal-update-confirm.net	Domain	Legitimate	0
9	2025-07-19 16:00:05	github-malware.org	Domain	Legitimate	0
10	2025-07-19 16:00:07	http://mybank-login.com/secure/login.php	URL	Legitimate	0
11	2025-07-19 16:00:08	login-dropbox.com	Domain	Legitimate	0

Full Details for Each Result

- Scan History:



Scan History (All)

Pick scan batch to view details/report:

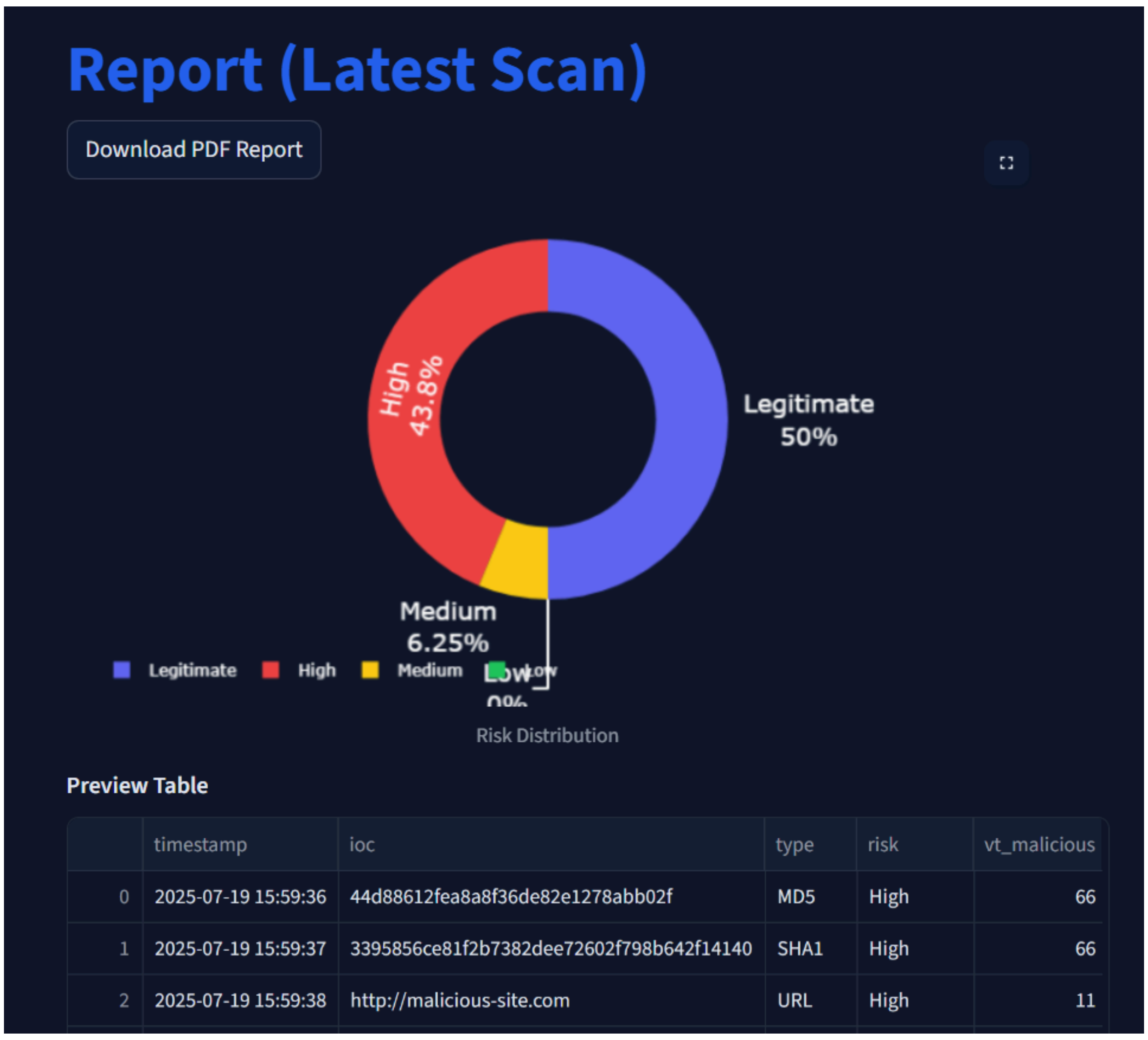
● 2025-07-19 16:00:18 (16 scans)
○ 2025-07-19 15:56:05 (1 scans)
○ 2025-07-19 15:07:08 (8 scans)
○ 2025-07-19 15:06:38 (1 scans)
○ 2025-07-19 15:06:28 (1 scans)

Sort by
Newest

Show scans after
YYYY/MM/DD

	timestamp	ioc	type	risk	vt_malicious	a
15	2025-07-19 16:00:18	nytimes.com	Domain	Legitimate	0	
14	2025-07-19 16:00:14	mit.edu	Domain	Legitimate	0	
13	2025-07-19 16:00:13	91.214.124.248	IP	Legitimate	0	
12	2025-07-19 16:00:10	http://free-offers-now.info/paypal	URL	Legitimate	0	

- PDF report sample (Download option):



Report (Latest Scan)

Preview Table

	timestamp	ioc	type	risk	vt_malicious
0	2025-07-19 15:59:36	44d88612fea8a8f36de82e1278abb02f	MD5	High	66
1	2025-07-19 15:59:37	3395856ce81f2b7382dee72602f798b642f14140	SHA1	High	66
2	2025-07-19 15:59:38	http://malicious-site.com	URL	High	11

- **Live Demo:** https://threat-intel-aggregator-pa9c9rdgja5iqpyh4teskk.streamlit.app/

Demo credentials:

- Username: `Bob`
- Password: `testuser123`

🔑 How to Configure API Keys in the App

If you experience API errors (for example, due to public rate limits), you can set your **own API keys** directly inside the app:

1. **Register and get your free API keys:**
   - VirusTotal – Get API Key
   - AbuseIPDB – Get API Key
   - Shodan – Get API Key
2. **Set your keys inside the app:**
   - Go to the **Settings & Info** page from the sidebar.
   - Enter your VirusTotal, AbuseIPDB, and Shodan API keys in the designated fields.
   - Click **Save Settings**. The app will use your custom keys for all scans.

   > ⚠️ Note for Streamlit Cloud:If you deploy your own copy of the app on Streamlit Cloud, you can also set these keys in the app's Settings > Secrets panel for best security. More about Streamlit secrets management →

3. **Now you're ready!**

   The app will now use **your API keys**, resolving any rate-limit or access issues. You can always return to Settings to update keys as needed.

Conclusion

Thank you for exploring the Threat Intel Aggregator app!

This tool was built to help security analysts and teams quickly scan IOCs, visualize risks, and generate detailed reports with ease. Your feedback and suggestions are welcome—feel free to open issues or contact the developer directly.

If you’d like to run your own copy, see the “Getting Started” section above.

For any problems or questions, check the troubleshooting section or reach out to [your support email].

Happy scanning! 🛡️