Static Data Sources (Offline Uploads)

These are datasets you can download or upload manually for analysis/training.

Category	Source	Description
🔥 Malware / Attack logs	CICIDS2017, CSE-CIC-IDS2018	Network traffic labeled as normal or attack (DDoS, brute force, botnet, etc.)
	NSL-KDD	Classic intrusion detection dataset
	TON_IoT	Real IoT telemetry & network attacks
🧠 Phishing / URLs	PhishTank, OpenPhish, URLHaus	Lists of phishing and malicious URLs
🐍 Malware samples / hashes	VirusShare, MalShare, Malpedia	Malware binaries, hashes, family info
🔒 Endpoint logs	Azure Sentinel Datasets	Simulated enterprise telemetry
🕵️ Sysmon / Windows event logs	Security Datasets Project	Realistic attack simulations with Sysmon and log data
🌐 Network captures (PCAP)	MAWI Traffic Archive, Stratosphere IPS	Real-world traffic dumps for feature extraction
⚡ Darknet / Honeypot	DShield / Honeynet Project, CAIDA Datasets	Anonymized attack telemetry

Live Data Sources (Streaming / APIs)

These sources provide real-time threat feeds or traffic monitoring.

Category	Source / Tool	Description
🌍 Threat Intelligence APIs	[VirusTotal API](), [AlienVault OTX](), [AbuseIPDB](), [GreyNoise](), [Cisco Talos]()	Real-time indicators (IPs, domains, URLs, file hashes)
🧭 SIEM / Log Feeds	Splunk HEC, Elastic Security, IBM QRadar, Wazuh, Azure Sentinel	Stream events from enterprise logs
📊 Network Traffic Stream	Zeek (Bro), Suricata, Snort, NetFlow	Collect and parse live traffic features
🧱 Firewall / IDS Feeds	Palo Alto Cortex XSOAR, FortiGate, Cisco Firepower APIs	Collect block events, alerts
⚙️ System Monitoring	Sysmon, osquery, Auditd	Local host telemetry
☁️ Cloud Logs	AWS CloudTrail, GuardDuty, Azure Security Center, GCP SCC	Security events and alerts
🕸️ Social / News Streams	Twitter/X (cyber threat intel accounts), Reddit (r/cybersecurity)	Open source intel (OSINT) feeds
🧠 Custom IoT / Sensor Feeds	MQTT, Kafka, WebSocket	For custom security sensors or internal telemetry