| **Datasource** | **Type** | **Why Useful** | **Small Description** | **Download Sources** | **Update Frequency** |
| --- | --- | --- | --- | --- | --- |
| **MITRE D3FEND** | Defensive Techniques Framework | Maps security controls to adversary techniques | Knowledge base linking mitigations to MITRE ATT&CK tactics | [https://d3fend.mitre.org](https://d3fend.mitre.org/) | Occasional updates |
| **CAPEC** | Attack Pattern Database | Identifies known attack techniques | Common Attack Pattern Enumeration and Classification from MITRE | [https://capec.mitre.org](https://capec.mitre.org/) | Periodic |
| **VulnCheck** | Vulnerability Intelligence | Speeds up remediation prioritization | Commercial & free vulnerability intelligence with exploit info | [https://vulncheck.com](https://vulncheck.com/) | Daily |
| **VulDB** | Vulnerability Database | Broad CVE coverage with exploit data | Global vulnerability knowledge base with threat scoring | [https://vuldb.com](https://vuldb.com/) | Daily |
| **Snyk Vulnerability DB** | Open Source Vulnerability Feed | Helps secure dependencies | Maintains open source library security issues | [https://security.snyk.io](https://security.snyk.io/) | Continuous |
| **Snort Rules** | IDS/IPS Detection Rules | Detects intrusions on networks | Rule sets for Snort intrusion detection/prevention systems | <https://www.snort.org/downloads> | Weekly |
| **Suricata Rules** | IDS/IPS Rules | Blocks known malicious traffic | Community & vendor rule feeds for Suricata | <https://suricata.io/rules> | Weekly |
| **Elastic Detection Rules** | SIEM Detection Content | Enables threat hunting in Elastic Security | Open detection rules for Elastic SIEM | <https://github.com/elastic/detection-rules> | Weekly |
| **Splunk Security Content** | SIEM Detection Rules | Improves Splunk threat detection | Prebuilt correlation rules and analytics for Splunk Enterprise Security | [https://research.splunk.com](https://research.splunk.com/) | Weekly |
| **VX Underground** | Malware Samples | Malware analysis & research | Archive of malware source code, binaries, and reports | [https://vx-underground.org](https://vx-underground.org/) | Irregular |
| **AlienVault OTX** | Threat Intelligence Platform | Shares community-driven threat indicators | Open Threat Exchange for IOCs, IPs, domains, hashes | [https://otx.alienvault.com](https://otx.alienvault.com/) | Continuous |
| **MISP Threat Sharing** | Threat Sharing Platform | Enables structured IOC sharing | Open source platform for storing & sharing threat indicators | [https://www.misp-project.org](https://www.misp-project.org/) | Continuous |
| **ThreatFox** | Malware IOC Feed | Tracks malicious indicators globally | IOC feed from Abuse.ch for malware campaigns | [https://threatfox.abuse.ch](https://threatfox.abuse.ch/) | Hourly |
| **PhishTank** | Phishing Database | Community-reported phishing detection | Verified phishing URLs & domains | [https://phishtank.org](https://phishtank.org/) | Continuous |
| **URLhaus** | Malware URL Feed | Detects malware distribution points | Malware-hosting URLs from Abuse.ch | [https://urlhaus.abuse.ch](https://urlhaus.abuse.ch/) | 5 min |
| **Feodo Tracker** | Botnet C2 Tracker | Detects banking trojan C2 servers | Tracks botnet command-and-control servers (Abuse.ch) | [https://feodotracker.abuse.ch](https://feodotracker.abuse.ch/) | Hourly |
| **CyberGreen** | Global Internet Risk Data | Measures global cyber hygiene | Data on risky internet behavior and vulnerable hosts | [https://www.cybergreen.net](https://www.cybergreen.net/) | Periodic |
| **MITRE Engenuity ATT&CK Evaluations** | Security Product Testing Data | Tests EDR tools against known techniques | Evaluations of vendor security products using ATT&CK | [https://attackevals.mitre-engenuity.org](https://attackevals.mitre-engenuity.org/) | Annual |
| **CERT Reports** | Security Incident Reports | Incident data from national CERTs | Official security advisories & breach reports | [https://www.us-cert.gov](https://www.us-cert.gov/) | Weekly |
| **Mandiant Reports** | Threat Intel Reports | High-quality APT & breach reports | Research and case studies from Mandiant | <https://www.mandiant.com/resources> | Irregular |
| **Kaspersky Threat Intelligence** | Threat Intelligence Service | Rich IOC & malware data | Commercial + free intelligence portal | [https://opentip.kaspersky.com](https://opentip.kaspersky.com/) | Continuous |
| **DarkNet Scan Feeds** | Dark Web Data | Monitors dark markets & forums | Aggregated intelligence from darknet scanning | Vendor-specific | Variable |
| **DDoSecrets** | Data Leak Repository | Investigates leaked datasets | Distributed Denial of Secrets publishes hacked/leaked data | [https://ddosecrets.com](https://ddosecrets.com/) | Irregular |
| **GreyNoise** | Internet Background Noise Data | Distinguishes benign scanning from malicious | Classifies internet scanning activity | [https://viz.greynoise.io](https://viz.greynoise.io/) | Continuous |
| **Shodan** | Internet Asset Search Engine | Finds exposed devices & services | Search engine for internet-connected systems | [https://www.shodan.io](https://www.shodan.io/) | Continuous |
| **Censys** | Internet Scanning Platform | Detects vulnerable internet assets | Searchable inventory of internet hosts | [https://censys.io](https://censys.io/) | Continuous |
| **RiskIQ Community Edition** | Threat Surface Discovery | Maps attack surface | Asset and threat discovery tools | [https://community.riskiq.com](https://community.riskiq.com/) | Continuous |
| **PhishStats** | Phishing Intelligence Feed | Tracks phishing campaigns | URLs, hosting, and WHOIS data on phishing | [https://phishstats.info](https://phishstats.info/) | Near real-time |
| **OpenPhish** | Phishing Feed | Detects active phishing threats | Validated phishing URLs from automated collection | [https://openphish.com](https://openphish.com/) | Hourly |
| **Spamhaus DBL** | Domain Block List | Blocks known malicious domains | Lists phishing, malware, botnet-related domains | <https://www.spamhaus.org/dbl/> | Daily |
| **PhishFort via Spamhaus** | Phishing Detection Feed | Brand protection & phishing defense | Detects phishing targeting brands | [https://www.spamhaus.org](https://www.spamhaus.org/) | Continuous |
| **Scam-Blocklist** | Scam & Fraud Blocklist | Blocks scam sites & IPs | Covers fraud, investment scams, tech scams | <https://github.com/mitchellkrogza/Scam-Blocklist> | Daily |
| **MITRE ATT&CK** | Adversary Tactics & Techniques | Models attacker behaviors | Knowledge base of TTPs | [https://attack.mitre.org](https://attack.mitre.org/) | Continuous |
| **ExploitDB** | Exploit Repository | Helps identify exploit PoCs | Archive of public exploits & shellcode | [https://www.exploit-db.com](https://www.exploit-db.com/) | Daily |
| **CISA KEV** | Vulnerability Catalog | Prioritizes patching | Known exploited vulnerabilities from CISA | <https://www.cisa.gov/kev> | Ongoing |
| **Sigma Rules** | Generic Detection Rules | Transforms detection logic across SIEMs | Sigma rule format repository | <https://github.com/SigmaHQ/sigma> | Weekly |
| **MalwareBazaar** | Malware Sample Feed | Threat hunting and analysis | Malware samples from Abuse.ch | [https://bazaar.abuse.ch](https://bazaar.abuse.ch/) | Continuous |
| **VirusTotal** | Malware & URL Scanning | Enriches IOC analysis | Aggregates antivirus scan results | [https://www.virustotal.com](https://www.virustotal.com/) | Continuous |
| **AnyRun** | Malware Sandbox | Behavioral malware analysis | Interactive sandbox for malware samples | [https://any.run](https://any.run/) | Continuous |