# OIXLY

## Open-Source Threat Intelligence Platform

**SOC Team Demo & Technical Briefing**

Aggregates real-time threat feeds from 10 authoritative sources into a single, filterable, exportable intelligence dashboard.

# 1. What Is OIXLY?

OIXLY is a fully automated, open-source Cyber Threat Intelligence (CTI) platform hosted on GitHub Pages. It requires zero infrastructure — no servers, no databases, no subscriptions. Every 6 hours a GitHub Actions workflow silently runs in the background, fetching fresh data from 10 authoritative threat intelligence sources, processing and deduplicating entries, then publishing the result as a single JSON file. The web dashboard reads that file and gives any SOC analyst an instantly usable, always-current picture of the threat landscape.

The platform is built around three guiding principles: freshness (automated 6-hourly updates), coverage (10 diverse sources spanning CVEs, malware, phishing, botnets, and network IOCs), and usability (filter, search, and export in seconds without any login or setup).

## Architecture at a Glance

| Layer | Component | Detail |
|---|---|---|
| Data Collection | GitHub Actions Workflow | Cron: every 6 hours — fetches all 10 feeds |
| Processing | Node.js Script (inline) | Deduplication, CVE merging, 90-day retention |
| Storage | data/td_9f3a7e.json | Single flat JSON file, committed to repo |
| Delivery | GitHub Pages CDN | Served globally with cache-busting on every fetch |
| Frontend | Vanilla JS + CSS | api.js · app.js · ui.js · storage.js |

# 2. The 10 Intelligence Sources — Why Each One Matters

Each source was chosen because it is (a) authoritative or community-validated, (b) freely accessible without a paid subscription, and (c) covers a threat category not fully addressed by the others. Together they provide defence-in-depth across every major attack vector a SOC team encounters daily.

### 1. CISA KEV — Known Exploited Vulnerabilities

Published by the US Cybersecurity & Infrastructure Security Agency. Every CVE in this list is confirmed to be actively exploited in the wild — not theoretical, not lab-tested, but seen in real attacks. Federal agencies are legally required to patch KEV entries by their due date. For a SOC team, a KEV entry means: this vulnerability is being weaponised right now.

- Confirms active exploitation — not just a high CVSS score.
- Includes ransomware use flag — immediately visible when ransomware gangs are leveraging a CVE.
- Provides remediation due date — gives SOC a hard deadline for escalation.
- Updated daily by CISA — freshest possible data on in-the-wild exploitation.

## 2. NVD — National Vulnerability Database (Paginated)

The NVD is NIST's comprehensive CVE registry with CVSS scoring. Where CISA KEV gives you the "on fire right now" list, NVD gives the broader universe of published vulnerabilities — including newly disclosed ones before they have been weaponised. The workflow now fetches the full 7-day window using pagination, ensuring not a single CVE is missed regardless of volume.

- Provides CVSS base score and severity — quantitative risk ranking.
- Full description and affected software — enables asset-based prioritisation.
- Captures newly published CVEs within hours of disclosure.
- Pagination fix ensures 100% coverage even on high-volume weeks.

## 3. Feodo Tracker (abuse.ch)

Tracks active Command & Control (C2) servers used by banking trojans (Emotet, Dridex, TrickBot, QakBot). These are live, confirmed C2 IPs that malware on infected endpoints phones home to. Any connection from your network to one of these IPs is a near-certain indicator of compromise.

- IP + Port + Malware family — block at firewall and alert on SIEM.
- Country and ASN information — useful for geo-based detection rules.
- First seen / last online timestamps — helps distinguish active vs dormant C2.

## 4. URLhaus (abuse.ch)

Community-curated list of URLs actively distributing malware. These are live download links used in phishing emails, malvertising, and drive-by downloads. Blocking these at your web proxy stops the malware delivery stage of the attack chain.

- URL + threat type + status — know if the URL is still online.
- Tags (e.g. "Emotet", "AgentTesla") — enables malware-family-specific hunting.
- Domain extraction — block entire domains, not just single URLs.

## 5. OpenPhish

Real-time phishing feed sourced from automated analysis and user submissions. Covers credential harvesting pages targeting major brands (PayPal, Microsoft, Google, banking). OIXLY automatically identifies the targeted brand from the URL, letting analysts filter by campaign.

- Brand detection logic built in — filter all Microsoft phishing in one click.
- Fresh URLs — submitted and verified within hours.
- Complement to PhishTank's more manual, voted verification process.

### 6. PhishTank

Community-verified phishing database where submissions are voted on by the security community. Higher confidence than automated-only feeds since human analysts have reviewed each entry. The "verified: yes" flag in OIXLY lets analysts instantly know the confidence level.

- Human-verified entries — lower false-positive rate than automated-only feeds.
- Target field — directly names the impersonated brand or organisation.
- Complements OpenPhish for double-coverage of active phishing campaigns.

### 7. MalwareBazaar (abuse.ch)

Repository of malware samples with file hashes, type signatures, and tags. Critical for endpoint teams — if a hash appears on MalwareBazaar, it is confirmed malicious and should be blocked immediately across all EDR/AV platforms.

- SHA-256 hash — import directly into EDR blocklists (CrowdStrike, Defender, SentinelOne).
- File name + MIME type — identify disguised executables (e.g., .pdf.exe).
- Malware signature / family — enables threat-actor attribution.
- Tag system — e.g., "ransomware", "stealer", "loader" for triage prioritisation.

### 8. ThreatFox (abuse.ch)

IOC sharing platform covering IPs, domains, URLs, and file hashes linked to specific malware families. ThreatFox entries come with a confidence level (0–100%) — OIXLY maps entries with ≥75 confidence to "critical" severity automatically.

- Multi-type IOCs — one source covering IPs, domains, URLs, and hashes simultaneously.
- Malware family attribution — know which threat actor group is behind the IOC.
- Confidence scoring — built-in quality signal reduces analyst noise.

### 9. SSL Blacklist / SSLBL (abuse.ch)

Blacklist of SSL certificates used by malware for encrypted C2 communications. As more malware uses HTTPS to evade detection, this feed becomes increasingly important. A certificate appearing here means it was observed in confirmed malware traffic.

- SHA-1 fingerprint — block at SSL inspection / firewall level.
- Reason field — identifies the malware family using the certificate.
- Addresses the "encrypted malware traffic" blind spot in many organisations.

### 10. Blocklist.de

Community-aggregated blocklist of IPs reported for SSH brute force, spam, web attacks, and DDoS. Sourced from thousands of honeypots and reporting servers worldwide. Useful for enriching SIEM alerts — if an IP hitting your SSH/RDP appears here, it's a known bad actor.

- Massive scale — hundreds of thousands of IPs from global honeypot network.
- Attack type classification — SSH, spam, DDoS, web attacks.
- Low false-positive rate for inbound attack detection.

# 3. How a SOC Team Uses OIXLY — Daily Workflows

## Morning Threat Briefing (5 Minutes)

- Open OIXLY → Time filter: "Today" → instantly see everything added in the last 24 hours.
- Check the Critical counter in the stats bar — if non-zero, click Severity: Critical.
- Scan CISA KEV entries first (filter: CVE/KEV tab) — these are the must-patch items of the day.
- Export the daily critical list as CSV → paste into the morning standup or ITSM ticket.

## Vulnerability Management / Patch Prioritisation

- Filter by Category: CVE/KEV → sort by severity.
- The "Ransomware Use: YES" flag instantly surfaces CVEs being exploited by ransomware groups — these jump the patching queue.
- Remediation Due Date column gives you the CISA-mandated deadline for federal/compliance environments.
- Cross-reference with NVD tab for CVSS scores on newer CVEs not yet in KEV.
- Export filtered list as CSV → import into vulnerability management tool (Tenable, Qualys, Rapid7).

## Firewall & Proxy Blocklist Updates

- Filter: Category = Botnet → reveals Feodo C2 IPs and Blocklist.de attack IPs.
- Copy indicators (one-click copy button on each threat card) → add to firewall deny rules.
- Filter: Category = Phishing → grab URLhaus and OpenPhish/PhishTank URLs → add to web proxy blocklist.
- Filter: Category = Malware → grab MalwareBazaar hashes → push to EDR/AV platforms.
- Full workflow can be done in under 10 minutes per shift.

## Incident Response — IOC Enrichment

- During an active incident, use the search bar to look up a suspicious IP, domain, hash, or CVE ID.
- OIXLY searches across all fields — title, description, indicators — simultaneously.
- A hit confirms the IOC is in an authoritative threat feed, providing context: malware family, C2 owner, threat type.
- Click the source URL on any card to go directly to the original feed entry for deeper investigation.

- Copy the threat card as JSON (copy button) → attach directly to incident ticket or SOAR playbook.

### Weekly Threat Report Generation

- Set Time filter: Last 7 Days → Category: All → Severity: All.
- Review the category breakdown bars — visualises what types of threats dominated the week.
- Set custom date range if needed (date picker supports precise start/end).
- Click Export CSV → produces a structured spreadsheet with all fields: ID, severity, category, indicators, source, action required, timestamps.
- CSV imports directly into Excel/Sheets — no data cleaning needed, BOM character included for proper encoding.

### Ransomware Campaign Monitoring

- Filter: Category = Ransomware → shows both explicit ransomware IOCs and KEV entries with Known ransomware use.
- The dual-source approach (CISA KEV + dedicated ransomware category) means nothing is missed.
- Indicators include CVE IDs, hashes, and C2 IPs — covering both the initial access vector and the post-compromise infrastructure.

## 4. Key Platform Features

| Feature | Description |
|---|---|
| **Automated 6-Hour Updates** | GitHub Actions cron job runs at 00:00, 06:00, 12:00, 18:00 UTC. No manual intervention needed. The "Last Updated" timestamp in the dashboard header shows exactly how fresh the data is. |
| **10-Source Aggregation** | Single pane of glass across CISA KEV, NVD, Feodo, URLhaus, OpenPhish, PhishTank, MalwareBazaar, ThreatFox, SSL Blacklist, and Blocklist.de. No need to maintain 10 separate bookmark tabs. |
| **Smart CVE Deduplication** | When the same CVE appears in both CISA KEV and NVD, the platform intelligently merges them — CISA data takes priority, NVD data fills in CVSS scores. No duplicate noise. |
| **90-Day Rolling Retention** | Only threats from the last 90 days are shown. Old data is automatically purged, keeping the dashboard focused on actionable |

| | |
|---|---|
| | intelligence rather than historical noise. |
| **Multi-Dimensional Filtering** | Filter simultaneously by category (9 types), severity (critical/high/medium/low), time window (today/3 days/week/month/90 days/custom date range), and free-text search across all fields. |
| **Full-Text Search with Pre-indexing** | The search index is pre-computed on load for performance. Searches hit title, description, category, source, and indicators — find anything in milliseconds. |
| **One-Click JSON Export per Threat** | Every threat card has a copy-as-JSON button. Copy the raw structured data directly into SOAR playbooks, SIEM enrichment pipelines, or incident tickets. |
| **CSV & JSON Bulk Export** | Export the current filtered view (or a custom date range) as CSV (Excel-ready, BOM encoded) or JSON. 17-column CSV includes all actionable fields already parsed from descriptions. |
| **Auto-Refresh Toggle** | Enable auto-polling (every 5 minutes) for shift-watch scenarios — dashboard stays live without manual refresh. |
| **No Login, No Infrastructure** | Entirely static — runs on GitHub Pages CDN. No server to maintain, no credentials to manage, no cost. Works from any browser, including mobile. |
| **Ransomware Use Flag (CISA)** | KEV entries where CISA has confirmed ransomware group involvement are prominently flagged. Ransomware filter surfaces these across both the CVE and Ransomware categories. |
| **Live Status Indicator** | Header shows SYSTEM ACTIVE / SCANNING / CONNECTION ERROR with a coloured dot — operators know at a glance whether the feed is healthy. |

# 5. Data Pipeline — How the Backend Works

Understanding the pipeline helps analysts trust the data. Every 6 hours the following sequence runs automatically:

### Step 1 — Fetch

All 10 sources are fetched in parallel using curl. HTTP status codes are captured — any non-200 response triggers a logged warning and a safe empty fallback rather than crashing the pipeline.

### Step 2 — NVD Pagination

The NVD endpoint now loops using startIndex and resultsPerPage=2000 until fetched count equals totalResults. With an API key (50 req/30s), this completes in seconds. Without a key (5 req/30s), a 7-second sleep is inserted between pages to respect rate limits.

### Step 3 — Parse & Normalise

Each source has a dedicated parser that maps raw feed fields into the unified threat schema: { id, title, description, category, severity, indicators[], source, sourceUrl, timestamp }.

### Step 4 — Smart Deduplication

New threats are merged with the existing dataset using a Map keyed by threat ID. For CVEs, a secondary deduplication pass groups all entries sharing the same CVE ID — CISA KEV entries win over NVD entries for the same CVE.

### Step 5 — 90-Day Retention

Any threat with a timestamp older than 90 days is filtered out. This keeps the dataset focused, fast to load, and free of irrelevant historical noise.

### Step 6 — Publish

The final JSON (threats array + lastUpdated + stats object) is written to data/td_9f3a7e.json and committed to the repo. GitHub Pages CDN propagates the update within seconds.

### Step 7 — Frontend Refresh

The dashboard has an auto-refresh toggle (5-minute interval) and a manual refresh button. On load, it fetches the JSON with a cache-busting timestamp query parameter to always get the latest version.

## Unified Threat Schema

Every threat, regardless of source, is normalised to this structure before storage:

| Field | Type | Description |
|---|---|---|
| **id** | string | Unique identifier. Prefixed by source: cisa-, nvd-, feodo-, uh-, phish-, mb-, tf-, ssl-, bl-, tor-, pt- |
| **title** | string | Human-readable summary. CVE entries include the CVE ID as prefix. |
| **description** | string | Structured multi-line text with emoji section headers. Parsed by export engine into CSV columns. |
| **category** | string | One of: cve, zero-day, ransomware, malware, phishing, botnet, nvd |
| **severity** | string | One of: critical, high, medium, low — mapped from source severity or CVSS score |
| **indicators** | string[] | Array of actionable IOCs: IP addresses, URLs, hashes, CVE IDs, vendor/product names |
| **source** | string | Human-readable source name: CISA KEV, NVD, Feodo Tracker, etc. |
| **sourceUrl** | string | Direct link to the original feed entry for analyst investigation |
| **timestamp** | number | Unix milliseconds. Used for time filtering, retention, and sort ordering. |
| **ransomwareUse** | string | "Known" or "Unknown" — from CISA KEV knownRansomwareCampaignUse field |

## 6. Source Coverage — Attack Vector Matrix

The following matrix shows which attack vectors each source covers, demonstrating why all 10 sources are necessary for complete coverage. A tick indicates primary coverage; a dash indicates partial or indirect coverage.

| Source | Active Exploit | CVE / Vuln | Malware Hash | C2 / Botnet IP | Phishing URL | Malware URL | SSL / Cert | Network IOC |
|---|---|---|---|---|---|---|---|---|
| **CISA KEV** | ✓ Primary | ✓ Primary | – | – | – | – | – | – |
| **NVD** | – Partial | ✓ Primary | – | – | – | – | – | – |
| **Feodo Tracker** | – | – | – | ✓ Primary | – | – | – | ✓ Partial |
| **URLhaus** | – | – | – Partial | – | – Partial | ✓ Primary | – | – |
| **OpenPhish** | – | – | – | – | ✓ Primary | – | – | – |
| **PhishTank** | – | – | – | – | ✓ Primary | – | – | – |
| **MalwareBazaar** | – | – Partial | ✓ Primary | – | – | – | – | – |
| **ThreatFox** | – | – | ✓ Primary | ✓ Primary | – Partial | – Partial | – | ✓ Primary |
| **SSL Blacklist** | – | – | – | – Partial | – | – | ✓ Primary | – |
| **Blocklist.de** | – | – | – | – Partial | – | – | – | ✓ Primary |

## 7. Export Capabilities

OIXLY supports two export formats for integration with downstream security tools and reporting workflows. Exports respect the currently active filters — if you have filtered to "Critical CVEs from the last 7 days", the export contains exactly that subset. A custom date range picker allows precise time-window exports for reports.

## CSV Export — 17 Structured Columns

The CSV export is purpose-built for security teams. The export engine parses the structured description field of each threat to extract specific sub-fields into dedicated columns — no manual data cleaning needed. Excel BOM character is prepended for correct encoding on Windows.

- Threat ID: Unique source-prefixed ID
- Category: cve / malware / phishing / botnet / ransomware / nvd
- Severity: critical / high / medium / low
- Date Added: Formatted timestamp: YYYY-MM-DD HH:MM:SS
- URL / IP / CVE: Primary indicator extracted from title or description
- Host: Hostname/domain for malware/phishing entries
- Target: Impersonated brand for phishing entries
- Vendor: Affected vendor for CVE/KEV entries
- Product: Affected product for CVE/KEV entries
- Threat Type: Specific threat classification
- Status: Active / Verified / Online / Offline
- Ransomware Use: Known / Unknown — from CISA KEV
- Remediation Due: CISA mandated patch deadline
- Action Required: Parsed recommended action
- Tags: Malware family tags
- Source: Origin feed name
- Full Description: Complete raw description for reference

## JSON Export — Machine-Readable Structured Data

JSON export produces a full structured object: { threats: [...], exportedAt, source, count }. Each threat object contains the full schema including the indicators array. Ideal for ingestion into SIEM platforms, SOAR playbooks, threat intelligence platforms (TIPs), or custom automation scripts.

# 8. Current Limitations & Honest Assessment

OIXLY is a powerful lightweight CTI tool, but it is important to understand what it is not. Being transparent about limitations is as important as showcasing strengths.

### Not a SIEM replacement

OIXLY provides threat intelligence context but does not ingest log data, correlate events, or generate alerts. It is a research and enrichment tool, not a detection engine.

### No user authentication

The dashboard is publicly accessible (GitHub Pages). Do not configure it to expose any internal or sensitive data. All data served comes from public feeds.

### Capped feed slice sizes

For performance, each feed is currently capped (e.g., top 80 CISA entries, 50 Feodo IPs). High-volume sources have caps to prevent JSON bloat. The most recent and severe entries are always prioritised.

### No historical trending

90-day rolling window means threats older than 90 days are purged. For long-term trend analysis, export regularly and store externally.

### GitHub Actions dependency

If GitHub Actions is unavailable, the 6-hour update cycle pauses. The dashboard will continue to show the last cached data with the correct timestamp.

### NVD without API key is rate-limited

The NVD rate limit of 5 req/30s means multi-page fetches sleep between pages, potentially extending the NVD portion of the workflow. Adding the free NVD API key eliminates this.

# 9. Recommended Demo Script (10 Minutes)

## 0:00 — Opening

- Open the OIXLY dashboard. Point to the status indicator: "SYSTEM ACTIVE" with a green dot.
- Highlight the "Last Updated" timestamp — show it updated within the last 6 hours.
- Read the stats bar: "X total threats, Y critical, Z high, W added today."

## 1:00 — CVE / Patch Prioritisation

- Click the CVE/KEV category tab.
- Filter: Severity = Critical.
- Open a CISA KEV entry — point to the Ransomware Use flag, Remediation Due date, Required Action.
- Say: "This is a vulnerability being exploited by ransomware groups right now. CISA says patch by [date]."

## 2:30 — Phishing Campaign

- Click the Phishing tab.
- Open an OpenPhish entry — show the targeted brand detection ("Microsoft Credential Theft").
- Say: "This phishing URL was submitted within the last 24 hours. We can block it at the proxy right now."

## 4:00 — Live IOC Search

- In the search bar, type a CVE ID (e.g. "CVE-2024").
- Show results appearing instantly across CISA KEV and NVD simultaneously.
- Type an IP-like string — show matching botnet / C2 results.
- Say: "This is a full-text search across every field — titles, descriptions, indicators."

## 5:30 — Copy for Incident Response

- Open a MalwareBazaar threat card.
- Click the copy JSON button.
- Say: "I can paste this directly into our incident ticket or feed it into the SOAR playbook."

## 6:30 — Export Workflow

- Filter: Last 7 Days, Category: All, Severity: Critical + High.
- Click Export CSV.
- Open the resulting file in Excel — show the 17 pre-structured columns.
- Say: "No data cleaning, no pivot tables — straight into the weekly report."

## 8:00 — Automated Update Demo

- Point to the workflow YAML: "This runs automatically 4 times a day, zero human involvement."
- Mention the NVD pagination fix: "Previously a single API call could miss thousands of CVEs — now we paginate to guarantee 100% coverage."
- Mention the NVD API key: "A free key from NIST raises the rate limit 10x — one-time 30-second setup."

## 9:00 — Closing

- Summarise: 10 sources, 6-hour updates, no infrastructure, no cost, export-ready.
- Open questions from the audience.