OIXLY

Threat Intelligence Platform

SOC Team Field Guide

How to use OIXLY in daily security operations —
what each category means and how to act on it

1. What Is OIXLY and Why Should a SOC Team Care?

OIXLY is a free, automated threat intelligence dashboard that pulls data from 10 of the most trusted security sources on the internet — every 6 hours, automatically, with no manual work required. It aggregates CVEs, malware hashes, phishing URLs, botnet IPs, ransomware indicators, and more into one single screen that any analyst can open in a browser right now.

Most organisations either pay thousands of dollars for commercial threat intel feeds, or they have analysts manually checking 10 different websites every morning. OIXLY eliminates both problems. It is not a SIEM, not an EDR, not a scanner — it is a daily intelligence layer that tells your team what threats are active in the wild right now, so you can act before those threats reach you.

The core value for a SOC team in one sentence:

OIXLY answers the question your team asks every morning: "What is being actively exploited, distributed, or attacked right now — and what should we block, patch, or hunt for today?"

How the data stays fresh

A GitHub Actions workflow runs automatically at 00:00, 06:00, 12:00 and 18:00 UTC every day. It fetches all 10 feeds, processes and deduplicates the results, and publishes an updated JSON file. The dashboard header shows the exact time of the last update so analysts always know how fresh the data is. There is no server to manage, no subscription to renew — it runs entirely on GitHub infrastructure at zero cost.

2. The 7 Threat Categories — What They Mean and How to Use Each One

Every threat in OIXLY is tagged with one of seven categories. Understanding what each category represents and which team action it triggers is the foundation of using OIXLY effectively.

🔓 CVE / Zero-Day

This category shows vulnerabilities that are being actively exploited in the wild, sourced from CISA's Known Exploited Vulnerabilities (KEV) list. Every entry here is a confirmed, real-world attack — not a theoretical risk. If a CVE appears in this tab, threat actors are already using it.

What it tells your team:

- Which software vulnerabilities are being weaponised right now
- Which ones are linked to ransomware gangs (the Ransomware Use flag)
- When you must patch by (the CISA Remediation Due Date)
- Which vendor and product is affected

Daily SOC actions:

- Open CVE/Zero-Day tab every morning as the first check of the day
- Filter by Severity: Critical — these are the must-patch items for the day
- Check the "Ransomware Use: Known" entries — escalate these immediately to the patching team
- Cross-reference CVE IDs against your asset inventory to find exposed systems
- Raise a patch ticket in your ITSM tool for each critical KEV entry
- Export as CSV and attach to the morning standup report

Real example: CVE-2024-3400 (Palo Alto PAN-OS) appears in this tab with Ransomware Use: Known. Your team knows within hours of CISA publishing it — before most commercial feeds update.

NVD CVEs

While the CVE/KEV tab shows vulnerabilities already being exploited, the NVD tab shows the broader universe of newly published CVEs from NIST's National Vulnerability Database — including ones that have not yet been weaponised. These are early warnings. Today's NVD entry can become tomorrow's KEV entry.

What it tells your team:

- Newly disclosed vulnerabilities with CVSS scores for risk ranking

- Full technical descriptions of what is vulnerable and how
- Whether a fix is available yet

Daily SOC actions:

- Check NVD tab daily for critical (CVSS 9.0+) and high (CVSS 7.0+) scores
- Filter by Severity: Critical to find the highest-risk new CVEs
- Cross-reference against your tech stack — if affected software is in your environment, escalate immediately
- Use NVD entries to brief vulnerability management teams before the CVE appears in KEV
- Feed CVE IDs into your vulnerability scanner as custom scan targets

Pro tip: Think of NVD as your 72-hour early warning system. Patch teams should review NVD Critical entries even before exploitation is confirmed — the average time from NVD publication to active exploitation is shrinking.

☢ Malware

This category aggregates confirmed malware samples from MalwareBazaar and IOCs from ThreatFox. Each entry includes file hashes (SHA-256), malware family names, and file details. These are samples that have been submitted, analysed and verified as malicious.

What it tells your team:

- SHA-256 hashes of active malware samples in the wild right now
- The malware family — Emotet, AgentTesla, RedLine, AsyncRAT, etc.
- File names that malware disguises itself as
- Tags like "stealer", "loader", "ransomware", "RAT"

Daily SOC actions:

- Export hash list daily → import into EDR platform (CrowdStrike, Defender for Endpoint, SentinelOne) as custom IOC block rules
- Search for the malware family name in your SIEM to check if any alerts have already fired
- Check file names against recent email quarantine logs — malware often arrives as fake invoice PDFs or shipping notifications
- Add SHA-256 hashes to your threat hunting queries
- If a family like "Emotet" or "QakBot" appears, brief the team — these spread laterally fast

Real example: MalwareBazaar shows a new AgentTesla sample (info-stealer). Your EDR import blocks the hash. You search SIEM for the filename "invoice_scan.exe" — two endpoints flagged in the last 48 hours. Incident response starts before users even report anything.

⚠ Phishing

Phishing entries come from OpenPhish and PhishTank — two of the most widely used phishing feed providers. Every URL in this category is a live or recently-active credential harvesting page impersonating a real brand: Microsoft, PayPal, banking portals, Google, and more. OIXLY automatically detects which brand is being targeted.

What it tells your team:

- Active phishing URLs with the targeted brand identified (Microsoft, PayPal, banking, etc.)
- PhishTank entries are human-verified — higher confidence than automated-only feeds
- Whether the URL is currently online or has been taken down
- The hosting domain — useful for blocking entire domains, not just single URLs

Daily SOC actions:

- Export phishing URL list daily → import into web proxy / Secure Web Gateway blocklist (Zscaler, Cisco Umbrella, Bluecoat)
- If your organisation uses Microsoft 365: check the targeted brand filter — Microsoft phishing campaigns directly target your users
- Search email gateway logs for any messages containing the phishing domains
- Alert the awareness team when a major campaign is active so they can send a user warning
- Add phishing domains to DNS sinkhole or firewall category overrides

How to integrate: Most SWG/proxy platforms support custom URL category feeds. Schedule a daily export from OIXLY as CSV, extract the URL column, and feed it into your proxy's custom block list via API or file import.

⛓ Ransomware

This is the highest-priority category for most SOC teams. It combines two things: (1) CVEs from CISA KEV that have confirmed use by ransomware groups, and (2) malware IOCs specifically linked to ransomware campaigns. If something appears in this tab, a ransomware group is actively using it right now.

What it tells your team:

- Which CVEs ransomware gangs are currently exploiting for initial access
- Hashes and IOCs linked to active ransomware payloads
- The specific ransomware family — LockBit, BlackCat, Cl0p, Play, etc.

Daily SOC actions:

- Check this tab FIRST — ransomware entries are the highest-urgency items
- Any CVE in this tab with Ransomware Use: Known = immediate patch escalation, no waiting for the next patch cycle
- Run the associated CVE through your vulnerability scanner against all internet-facing and RDP-exposed assets
- Block associated hashes in EDR immediately

- If a known ransomware family's C2 IP appears in Botnets, block it at the firewall and search SIEM logs for prior connections
- Use as briefing material for management — ransomware entries justify emergency patching requests

Why this matters: The average time between a vulnerability being published and ransomware groups exploiting it has dropped to under 5 days in 2024. OIXLY updates every 6 hours — giving your team a fighting chance to patch before the attack arrives.

◉ Botnets

Botnet entries cover two things: Command & Control (C2) server IPs from Feodo Tracker (used by banking trojans like Emotet, Dridex, TrickBot, QakBot), and general attack IPs from Blocklist.de reported for SSH brute force, DDoS, and spam. These are network-level IOCs — any connection from your network to a C2 IP is a near-certain sign of compromise.

What it tells your team:

- Live C2 server IPs that infected machines phone home to
- The malware family using each C2 — tells you what you are dealing with
- IPs conducting active SSH brute force, web attacks, and DDoS from Blocklist.de
- Port numbers for C2 communications — useful for firewall rules

Daily SOC actions:

- Export Botnet IP list daily → add to firewall outbound deny rules
- Search SIEM / firewall logs for any existing connections to C2 IPs — a hit is an active incident
- Add C2 IPs to SIEM threat intel lookup tables for automatic alerting
- If Feodo shows a banking trojan C2 is online, proactively block and alert finance/banking staff
- Check DHCP/NAT logs for which internal IPs tried to reach C2 servers

Critical indicator: If any internal host in your environment has an outbound connection to a Feodo Tracker C2 IP, that host is infected. Do not just block the IP — isolate the host and start incident response immediately.

🔴 Zero-Day (within CVE/KEV tab)

Zero-Day entries are a sub-classification within the CVE category. OIXLY marks a CVE as Zero-Day when CISA notes it as a zero-day exploitation or when it is linked to a known ransomware campaign. These represent the most dangerous class of vulnerability — actively exploited before or shortly after a patch is available.

Daily SOC actions:

- Zero-Day entries = immediate escalation, same day, no patch cycle exceptions
- If no patch is available: apply vendor mitigations or temporarily disable the affected service
- Notify CISO directly for any zero-day affecting internet-facing systems
- Check vendor advisory pages linked in the sourceUrl field for workarounds

3. How to Implement OIXLY in Your SOC — Step by Step

OIXLY requires zero infrastructure to run. It is already deployed and live. Implementation for a SOC team is purely about building it into your existing daily routines and tooling. Below is a practical guide from Day 1 to fully integrated.

Day 1 — Access & Familiarise (30 minutes)

- Open OIXLY in your browser — bookmark it for all analysts
- Read the stats bar: Total threats, Critical count, High count, Added today
- Click through each category tab (CVE, NVD, Malware, Phishing, Ransomware, Botnets)
- Try the search bar — type a vendor name, CVE ID, or IP address you recognise
- Do a test export (JSON and CSV) to understand the data structure
- Note the Last Updated timestamp — understand the 6-hour update cycle

Week 1 — Build into Daily Routine

Morning Shift Start (10 minutes):

- Open OIXLY → Time filter: Last 24 Hours
- Check Critical count — if non-zero, filter Severity: Critical immediately
- Check Ransomware tab — any new entries = top priority for the day
- Note any CVE/KEV entries affecting software your organisation uses
- Export daily critical list as CSV → paste into shift handover notes or ITSM ticket

Afternoon Review (5 minutes):

- Quick refresh — OIXLY updates every 6 hours so new threats may have appeared since morning
- Check Phishing tab for any new campaigns targeting your organisation's common tools (Microsoft, Google, banking)
- Check Botnets tab for any new C2 IPs → run a quick SIEM search for those IPs against your network logs

Week 2 — Integrate with Your Tools

Tool / Platform	How to Integrate with OIXLY
Firewall / Next-Gen Firewall	Export Botnet + Phishing IPs/URLs daily as CSV. Import to custom block rules or threat feed. Most NGFWs (Palo Alto, Fortinet, Check Point) support custom threat feeds via URL or file.
SIEM (Splunk, Sentinel,	Schedule daily export of IOC indicators as JSON. Import into threat

QRadar)	intelligence lookup tables. Set up automated alerts when any internal host communicates with a known C2 IP.
EDR (CrowdStrike, Defender, SentinelOne)	Export Malware SHA-256 hashes daily. Import as custom IOC block list. Most EDR platforms support bulk hash import via API or CSV upload.
Web Proxy / SWG (Zscaler, Umbrella)	Export Phishing and Malware URL lists. Add to custom URL category or block list. Update daily on a schedule.
Vulnerability Management (Tenable, Qualys)	Use CVE IDs from KEV tab as priority targets for scanning. Feed CISA KEV CVE list into your scanner's priority queue.
Ticketing / ITSM (Jira, ServiceNow)	For each new Critical KEV entry, raise a patch ticket automatically. Export daily critical list and use it as input to your patch management workflow.
Email Gateway	Extract domains from Phishing tab. Add to sender block list or custom threat category in your email security platform.

Month 1 — Build Weekly Reporting Workflow

- Every Friday: Set Time filter to Last 7 Days, export full CSV
- The CSV has 17 pre-structured columns — open in Excel, no cleanup needed
- Use the category breakdown bars in the dashboard to write your weekly threat landscape summary
- Track which categories had the highest volume — helps identify trend shifts week over week
- Include OIXLY stats in monthly security reports to management: "X critical CVEs were being actively exploited this month, Y of which were linked to ransomware"

4. SOC Playbooks — What to Do When You See Each Type of Alert

These are practical step-by-step responses for the most common scenarios OIXLY surfaces. Share these with your Level 1 and Level 2 analysts as reference cards.

Playbook A — New Critical CVE in KEV Tab

Step 1	Note the CVE ID, vendor, and product from the threat card
Step 2	Check if affected software exists in your environment (CMDB, asset inventory)
Step 3	If yes: raise an emergency patch ticket. Set due date to CISA Remediation Due date
Step 4	If ransomwareUse = Known: escalate to L3 / Incident Response team immediately
Step 5	Check vendor advisory (sourceUrl link) for patches or workarounds
Step 6	If no patch: apply vendor mitigation or isolate the service from the internet
Step 7	Add CVE ID to vulnerability scanner as an immediate scan target
Step 8	Document in shift log and brief incoming shift

Playbook B — New Malware Hash in Malware Tab

Step 1	Copy the SHA-256 hash from the threat card (click JSON to get full data)
Step 2	Import hash into EDR platform as custom block IOC
Step 3	Search SIEM for the hash across endpoint telemetry — last 7 days
Step 4	Search for the malware filename in email gateway quarantine logs
Step 5	If a hit is found: isolate the endpoint and escalate to IR
Step 6	Brief security awareness team if the malware is spreading via phishing email
Step 7	Add malware family name to threat hunting backlog

Playbook C — New C2 IP in Botnets Tab

Step 1	Note the IP, port, and malware family from the threat card
Step 2	Search firewall/proxy logs for any outbound connections to this IP — last 30 days
Step 3	If hit found: the connecting host is likely infected — isolate immediately
Step 4	Add the IP:Port to outbound deny rules on perimeter firewall
Step 5	Add IP to SIEM threat intel lookup for ongoing alerting
Step 6	If malware family is a banking trojan (Emotet, QakBot, Dridex): alert finance team
Step 7	Document the block and check for lateral movement from any infected host

Playbook D — Phishing Campaign Targeting Your Tools

Step 1	Note the targeted brand (Microsoft, PayPal, banking, etc.)
Step 2	Add the phishing URL/domain to web proxy block list
Step 3	Search email gateway for inbound messages containing the phishing domain
Step 4	Add domain to email gateway block list / sender policy
Step 5	If Microsoft 365 targeted: check Azure AD sign-in logs for any suspicious logins from the past 24 hours
Step 6	Send user awareness alert if a major campaign is active ("We are aware of a Microsoft phishing campaign, do not click links in unexpected emails")
Step 7	Document in daily report

5. Quick Reference — Category to Action Mapping

Use this table as a wall reference or shift handover card.

Category	What It Means	Who Acts	Action
CVE / Zero-Day	Actively exploited vulnerability (CISA KEV)	Patch team	Raise patch ticket. Check asset exposure. If ransomware-linked: escalate immediately.
NVD CVEs	Newly published vulnerability (not yet exploited)	Vulnerability Mgmt	Add to scanner priority queue. Monitor for exploitation signs.
Malware	Confirmed malware hash or IOC	EDR / Endpoint team	Import hash to EDR block list. Search SIEM for prior hits.
Phishing	Live credential-harvesting URL	Email / Proxy team	Block URL in proxy. Search email gateway. Warn users if major campaign.
Ransomware	CVE or IOC used by ransomware groups	All teams / CISO	Highest priority. Emergency patch or isolate. Management notification.
Botnets	C2 server IP or attack IP	Firewall / Network team	Block at firewall. Search logs for existing connections. Isolate if hit found.
Zero-Day	Zero-day exploitation confirmed	IR / All teams	Same day response. Apply mitigation if no patch. Notify CISO.

6. Using the Export Feature for Reporting

OIXLY can export any filtered view as CSV or JSON with a single click. This makes it easy to feed data into other tools and generate reports without any manual work.

Daily Shift Report

- Filter: Last 24 Hours → Severity: Critical + High
- Export CSV → attach to shift handover document or ITSM ticket
- Takes under 2 minutes, gives the incoming shift a complete picture

Weekly Threat Report

- Filter: Last 7 Days → Category: All → Severity: All
- Export CSV → open in Excel
- The 17 structured columns (ID, severity, category, vendor, indicators, action required, timestamp) are ready to use — no data cleaning
- Add the category breakdown totals from the OIXLY sidebar as a summary chart

Patch Management Input

- Filter: Category = CVE/KEV → Severity: Critical
- Export CSV → import into your vulnerability management platform
- The Vendor, Product and Remediation Due Date columns map directly to patch ticket fields

IOC Feed for SIEM / Firewall

- Filter: Category = Botnets OR Malware → Export JSON
- Parse the indicators array from each threat object
- Import IPs and hashes into your SIEM threat intel lookup or firewall custom feed
- Schedule this as a daily automated task for hands-off IOC management

7. Practical Tips for Your Team

► Always check Last Updated

The timestamp in the header shows when data was last fetched. If it is more than 7 hours old, something may have gone wrong with the pipeline. Manually trigger a refresh via GitHub Actions if needed.

► Use the search bar for live incidents

During an active incident, type the suspicious IP, domain, hash, or CVE ID into the search bar. If it appears in OIXLY, you have instant context: what malware family, what source, how severe, what action to take.

► The Ransomware tab is not optional

Some teams skip this thinking it only applies if they are already under attack. Wrong — it shows which CVEs ransomware groups are actively exploiting for initial access. This is pre-breach intelligence.

► Copy JSON for instant SOAR integration

Every threat card has a "Copy JSON" button. The copied object has all fields in structured format. Paste directly into a SOAR playbook, incident ticket, or automation script.

► Set filters before exporting

Exports respect the current filter state. Set category + severity + time window before clicking export to get exactly the data slice you need — not the entire 6000-entry dataset.

► Brief your L1 analysts with the playbooks

Level 1 analysts should have the Category to Action table (Section 5) printed or pinned. It tells them exactly who to escalate to and what action to take for each category without needing L2 guidance every time.

► Use the auto-refresh during incidents

Enable the auto-refresh toggle in the dashboard when monitoring an active incident or during a threat campaign. OIXLY will poll for new data every 5 minutes automatically.

► NVD is a 72-hour early warning

A CVE appears in NVD first, then moves to CISA KEV when exploitation is confirmed. Treating high-CVSS NVD entries seriously before they reach KEV gives your patch team a head start.

OIXLY — Free. Automated. Always Current.

Updates every 6 hours · 10 authoritative sources · No login required · Export-ready