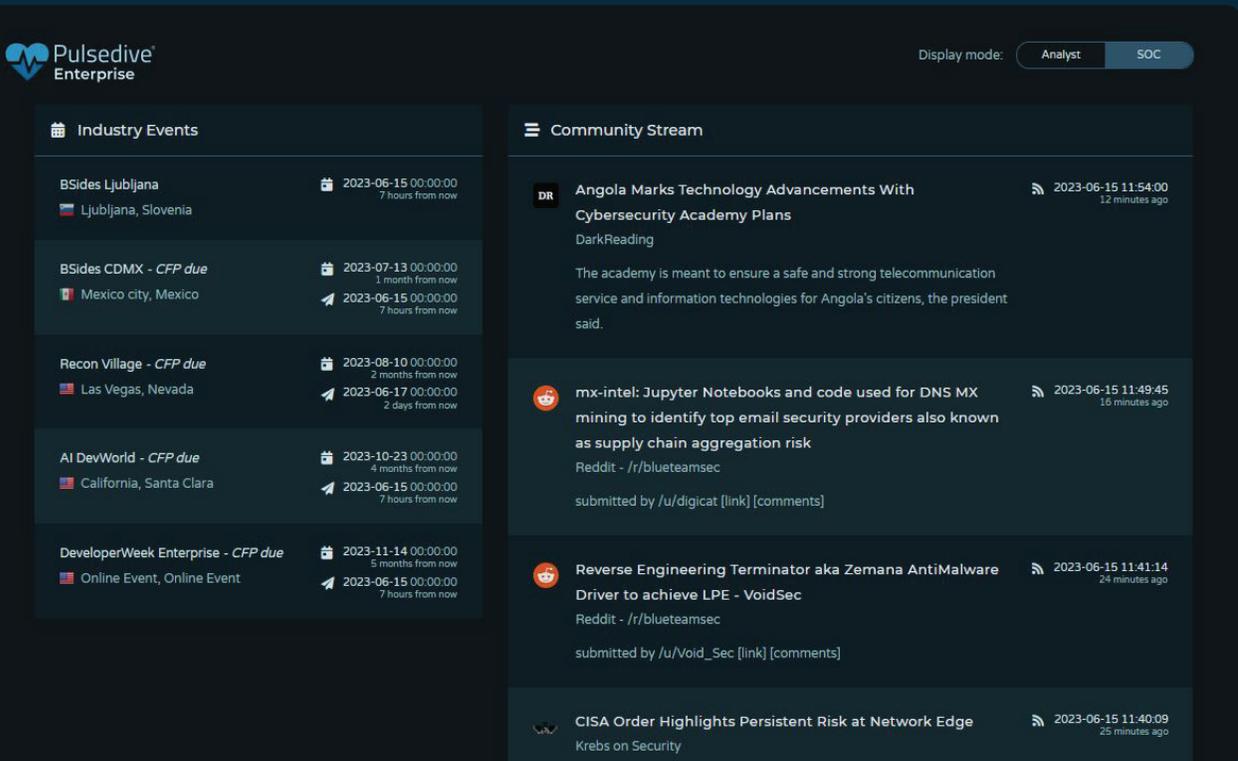




Pulsedive[®]
Enterprise

Threat Intelligence Platform

pulsedive.com



Pulsedive Enterprise

Display mode: Analyst SOC

Industry Events

- BSides Ljubljana**
Ljubljana, Slovenia
2023-06-15 00:00:00
7 hours from now
- BSides CDMX - CFP due**
Mexico city, Mexico
2023-07-13 00:00:00
1 month from now
2023-06-15 00:00:00
7 hours from now
- Recon Village - CFP due**
Las Vegas, Nevada
2023-08-10 00:00:00
2 months from now
2023-06-17 00:00:00
2 days from now
- AI DevWorld - CFP due**
California, Santa Clara
2023-10-23 00:00:00
4 months from now
2023-06-15 00:00:00
7 hours from now
- DeveloperWeek Enterprise - CFP due**
Online Event, Online Event
2023-11-14 00:00:00
5 months from now
2023-06-15 00:00:00
7 hours from now

Community Stream

- DR** Angola Marks Technology Advancements With Cybersecurity Academy Plans
DarkReading
2023-06-15 11:54:00
12 minutes ago
The academy is meant to ensure a safe and strong telecommunication service and information technologies for Angola's citizens, the president said.
- mx-intel**: Jupyter Notebooks and code used for DNS MX mining to identify top email security providers also known as supply chain aggregation risk
Reddit - /r/blueteamsec
2023-06-15 11:49:45
16 minutes ago
submitted by /u/digicat [link] [comments]
- Reverse Engineering Terminator aka Zemana AntiMalware Driver to achieve LPE - VoidSec**
Reddit - /r/blueteamsec
2023-06-15 11:41:14
24 minutes ago
submitted by /u/Void_Sec [link] [comments]
- CISA Order Highlights Persistent Risk at Network Edge**
Krebs on Security
2023-06-15 11:40:09
25 minutes ago

Pulsedive Dashboard in SOC mode with events and news stream

Address key questions like:

- How can we maximize the time and talents of the team for high-value research, analysis, and response?
- What current threats are impacting our organization?
- How can we collect and curate a single source of knowledge – for both internal and external intelligence?
- How can we safely disseminate intelligence across our organization and with trusted partners?
- What information do we need to facilitate decision-making and create priorities to protect and prevent attacks?

How Teams Use Pulsedive Enterprise



IMPORT

Easily ingest and de-dupe new data in a centralized database for evaluation and tracking



CURATE

Create and maintain a curated repository of automated and human-enriched indicators, threats, and data sources



QUERY

Flexibly query across the entire dataset to uncover patterns and correlations



INTEGRATE

Seamlessly integrate and export data for further analysis, enrichment, collaboration, and blocking



Example Enterprise Integration



Bring Data In

Ingest feeds, code-free

Configure third-party feeds in CSV or STIX 2.x formats in less than a minute

Customize each new data source, with advanced identification, extraction, and feed details

Add and edit data in bulk

Process and submit hundreds of thousands of indicators via UI or API

Flexible bulk analysis with IOC filtering, file uploads, expanded CIDR ranges, and parsing exclusions

Retain indicator context with risk scores, user comments, ports, technologies, tactics, and more

Contribute new threats and associated aliases on demand

Analyze

Input

Paste text or upload files containing IPs, URLs, and domains. Large pasted text will be added as a virtual file. Pulsedive will parse, refang, and deduplicate indicators automatically.

Include

All IPv4 IPv6 Domains URLs MD5 SHA-1 SHA-256

Text Input

```
e3d6a5b6jxyz
ebayshow.com
http-www-1cloud-com.us
178[.]128[.]23[.]9
104.248.178.90
204.174.223.210
192.99.150.39
128.199.232.159
159.65.3.147
cfff08f19174f63ca45cd1e2d3ba73d3
380ce030edf017e1a348682b487d4049
```

Upload Files

premiumfull.csv
393.6 KB - application/vnd.m...

Select File(s)

Parsing Options

IPv4 CIDR expansion Email domains

Parsing Exclusions

Hit enter to add.

Reset Submit Analyze

Queue Download

Showing 1000 indicators out of 2020.

```
e3d6a5b6.xyz
ebayshow.com
http-www-1cloud-com.us
178.128.23.9
104.248.178.90
204.174.223.210
192.99.150.39
128.199.232.159
159.65.3.147
cfff08f19174f63ca45cd1e2d3ba73d3
380ce030edf017e1a348682b487d4049
157.90.148.23
https://ec89.
/indicator/
https://157.90
http://157.90
http://117.21
/Mozi.m
http://115.56
http://222.24
http://117.15
/Mozi.m
http://182.11
```

Feed Configuration

Access Details

Start by entering access details for this data source. You can click Test Access to view raw response data and confirm the access details.

Access URL Required

https://urlhaus.abuse.ch/downloads/text/

HTTP Method

GET POST

Enter parameters as key-value pairs separated by a colon. Hit enter to add each parameter. Example: fid:123

URL Parameters

key:value

Basic Auth Optional

Username

Password

200 OK

Test Access Next

```
#####
# abuse.ch URLhaus Plain-Text URL
# Last updated: 2023-06-15 16:01:2
#
# Terms Of Use: https://urlhaus.ab
# For questions please contact url
#####
# url
http://182.119.206.69:50799/bin.sh
https://audit.njc.gov.ng/ifa/?0984
https://savannahplains.ac.tz/mon/?
http://151.236.14.86/gF1sH2v/CD745
http://218.202.197.14:33028/Mozi.m
http://180.116.47.193:38778/Mozi.m
http://117.208.136.39:60349/Mozi.m
http://117.211.40.145:43834/Mozi.m
https://revistas.upp.edu.pe/te/?87
http://59.88.225.221:41942/bin.sh
http://117.215.247.4:49506/bin.sh
http://182.117.0.22:44333/bin.sh
http://117.219.114.188:59272/Mozi.
```



Track and Manage Indicators

The screenshot displays a security tool interface for tracking and managing indicators. The main indicator is **195.201.226.88**. The interface includes a 'Screenshots' section with a 'Latest' tab and a 'Historical' tab. Below this is a 'jupyterhub' screenshot showing a login form with fields for 'Sign In', 'Username', and 'Password', and a 'Sign In' button. The indicator details section shows a 'Critical risk' status and a list of risk factors: 'Self-signed SSL certificate', 'Suspicious SSL certificate', 'Found in threat feeds', 'Hosted on common ISP', and 'Returns PTR record'. An 'Integrations' section lists 'VirusTotal' (2/64), 'Shodan' (4 ports, 0 CVEs), and 'AbuseIPDB' (0 reports). Below this are 'Auto-Fetch' and 'Manual' buttons. The interface also features an 'Actions' bar with options like 'Copy Summary', 'Seen', 'Rescan', 'Comment', 'Export', 'Share', and 'Manage'. The 'Highlights' section lists: '200 HTTP status', 'static 88.226.201.195.clie... your-server.de Reverse DNS', 'text/html Content-type', 'SSL certificate found: 8c1314345590086f48dd7eb599 ... raefik.default', 'Gunzenhausen, Germany, Hetzner Online GmbH', and 'TornadoServer Technologies'. The 'Events' section lists: 'Added 2020-10-15 10:32:38 2 years ago', 'Cert. issued 2023-06-01 13:13:35 1 week ago', 'Scanned 2023-06-04 07:42:41 1 week ago', 'Seen 2023-06-04 07:42:42 1 week ago', 'Updated 2023-06-06 10:40:23 1 week ago', and 'Cert. expires 2024-05-31 13:13:35 1 year from now'. The 'Attributes' section shows 'Port' (# 22, # 443, # 80), 'Protocol' (# HTTP, # HTTPS, # SSH), and 'Technology' (# TornadoServer). The 'Threats' section shows 'Tor Proxy Tool' (2020-10-15 10:32:38 2 years ago) and 'Tor IPs Data.mz.uk' (2020-10-15 10:32:38 2 years ago). The 'Feeds' section shows 'Tor IPs Data.mz.uk' (2020-10-15 10:32:38 2 years ago).

Reduce false positives

Automated and manual risk scoring and retiring to help prioritize real threats

Automated enrichment and scanning in a single click

Edit thousands of indicators at a time

Pulsedive collects

- Risk scores and risk factors
- Registration timestamps
- WHOIS registration info
- Location
- DNS records
- Ports and protocols
- Query strings
- HTTP headers
- SSL certificate info
- Redirects
- Cookies
- Meta tags
- Web technologies
- File names and file types
- Screenshots



Research Threats

Bumblebee

Critical risk

Actions | Indicators | Comment | Export | Share

Highlights

- Malware Category
- 161 indicators
- MITRE ATT&CK Enterprise, Feodo Tracker Feeds
- Windows Technologies
- Collection, Command and Control, Defense Evasion, Discovery, Execution, Exfiltration, Initial Access, Privilege Escalation Tactics

Events

- Added 2022-12-04 22:34:15 (6 months ago)
- Seen 2023-06-06 13:36:36 (1 week ago)
- Updated 2023-06-14 15:23:46 (21 hours ago)

Description

Bumblebee is a custom loader written in C++ that has been used by multiple threat actors, including... download and execute additional payloads since at least March 2022. Bumblebee has been linked to... Quantum, and Mountlocker and derived its name from the appearance of "bumblebee" in the user-agent... [Google EXOTIC LILY March 2022] [Proofpoint Bumblebee April 2022] [Symantec Bumblebee June 2022]

Attributes

- Tactics and Techniques
 - Collection
 - Archive Collected Data
 - Data from Local System
 - Command and Control
 - Defense Evasion
 - Discovery
 - Execution
 - Exfiltration
 - Initial Access
 - Persistence
 - Privilege Escalation
 - Reconnaissance
- Country Code
 - CN
- Technology
 - Windows

Feeds

- MITRE ATT&CK Enterprise (0 indicators)
- MITRE
- Feodo Tracker (161 indicators)
- Abuse.ch

Indicators

View Indicators

Risk Breakdown

161 indicators

Explore Indicators

threat=Bumblebee

Shared Indicator Attributes

| | | |
|----------|---------------|--------|
| Port | 12 indicators | # 22 |
| | 4 indicators | # 80 |
| | 40 indicators | # 443 |
| Protocol | 4 indicators | # HTTP |

Investigate threat infrastructure

- Manually and automatically link IOCs to threats
- Build a comprehensive summary of threat activity, tactics, techniques, screenshots
- Manage and merge threat aliases from different data sources under a single profile
- Stay on top of the latest news and add your own references



Query Across Your Dataset

The screenshot displays a search interface with the following components:

- Your Queries:** A list of recent queries on the left side.
- Search mode:** A toggle between 'Indicators' (selected) and 'Threats'.
- Explore:** The main search area with a query input field containing: `risk=high+ seen=month type=ip,ipv6,domain threat=phishing active=true`.
- Results:** A list of 127 indicators, showing the first six results with details like domain names, locations, and timestamps.
- Right Panel:** A detailed view of the IP address `112.213.89.135`, including risk levels (Critical risk), associated certificates, content types, and registrant information.

| Indicator | Location | Timestamp | Age |
|---|--|---------------------|-------------|
| www.hydropointme.com | REDACTED FOR PRIVACY, United Arab Emirates | 2023-06-02 09:46:39 | 1 week ago |
| paypal-account.binbogabali.net | Adana, Turkey | 2023-05-29 12:00:00 | 2 weeks ago |
| paypal.co.uk.userjcgw75avdau.gospite.com | Orem, Utah | 2023-05-29 12:00:00 | 2 weeks ago |
| evergreen.v6.afraid.org | REDACTED FOR PRIVACY, CA | 2023-06-02 01:09:30 | 1 week ago |
| paypal-account-confirmation.erikahaas.com | KIRKLAND, WA | 2023-05-29 12:00:00 | 2 weeks ago |
| paypal.com.helpdesk-legal-agreement.com | | 2023-05-29 12:00:01 | 2 weeks ago |

Investigate deeper and wider

Search IOCs and threats by almost any data point

Dynamic querying using boolean logic and wildcards

Use real-time autocomplete suggestions to enhance your search

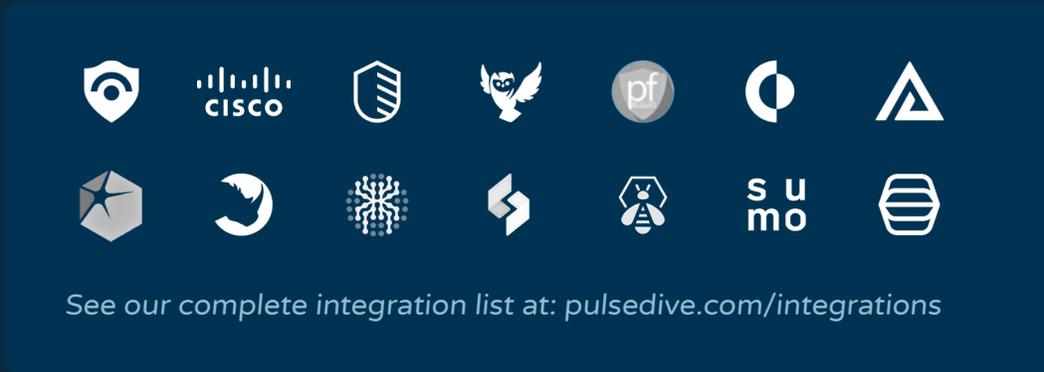
Quickly preview and pivot IOCs and threats without leaving your search

Export results in CSV, JSON, or STIX 2.1 format

Update, retire, and activate IOCs in bulk

Get Data Out

Pulsedive's native data integration and sharing services are included with no limits at no additional cost with an Enterprise license, making it simpler than ever to put your threat intelligence to work.



```
POST request to /api/submit.php with parameters:
{
  "action": "submit",
  "type": "indicator",
  "pretty": "1",
  "data": "{ \"value\": \"https://pulsedive.com/\", \"type\": \"host\", \"acti...
  \"threat\": [], \"attributes\": { \"port\": [ \"443\" ], \"protocol\": [ \"HTT...
  \"activate\": \"1\", \"comment\": \"Testing API submissions\" },
  \"key\": \"193b0bc9691b140f2048214f82dde487a21161a53a3e484cf272e548553...
}

Raw submission data, JSON-encoded in the request above:
{
  \"value\": \"https://pulsedive.com/\",
  \"type\": \"host\",
  \"action\": \"submit\",
  \"risk\": \"recommended\",
  \"threat\": [],
  \"attributes\": {
    \"port\": [
      \"443\"
    ]
  }
}

Send request Test with the command line:
curl -d 'action=submit&type=indicator&pretty=1&data=78922value92283A8229...
2283A822host92292CK22action%2283A822s...'

200 OK
{
  \"success\": \"Added request to queue.\",
  \"aid\": 28713722
}
```

API

JSON and STIX 2.1 formats supported

Automate real-time enrichment

Pull threat data and news

Automate custom reports with
Explore queries

CSV fields: All, Indicator ID, Type, Risk, Threats, Feeds, User Submission Count, Risk Factors, Reference URL

Header row: Print, None

Indicator types: All, Domain, IP, IPv6, MD5, SHA-1, SHA-256, URL

Indicator risk: All, Unknown, Very Low, Low, Medium, High, Critical

Timestamp: Last seen, First added

Time period: All time, Last Day, Last Week, Last Month, Last Year

Retired indicators: Include, Active only

Direct URL: `https://.../?key=00ee98163...&header=true&fields=id,type,risk,threats,feeds,usersubmissions,riskfactors,reference&types=domain,ip,ipv6,md5,sha1,sha256,url&risk=medium,high&retired=true&added=month`

Bulk Export

CSV format and STIX 2.1 export via TAXII 2.1 supported

Integrate with SIEM, SOAR and other technologies

Alert, detect, and block



Customize It

With Rules, track what you need, how you want

Create custom attribute types, with regex validation

Set custom aging rules for retiring indicators

Modify STIX input mapping

Create new threat categories

Malware Delete Category

| | |
|--------------|--|
| Raw Value | malware |
| Display | Malware |
| STIX Output | malware |
| Threat Count | 799 threats |
| Explore | >> category=malware |
| Examples | Zeus Shiotob Bedep Beebone Dromedan Matsnu Nymaim Pizd Proslikefan Pykspa |

⌚ Aging Rules + Create Aging Rule

Age Threshold ↓

Not seen in 14 days IP IPv6 High Critical

Not seen in 3 months All indicator types All risk scores

Attribute Types + Create attribute type

| | | |
|--------------|--|---|
| Country Code | <input type="checkbox"/> countrycode <input checked="" type="checkbox"/> Regex validation <input checked="" type="checkbox"/> Native support | <input type="checkbox"/> Threat |
| File Name | <input type="checkbox"/> filename <input type="checkbox"/> Default validation <input checked="" type="checkbox"/> Native support | <input type="checkbox"/> Artifact <input type="checkbox"/> MD5 <input type="checkbox"/> SHA-1 <input type="checkbox"/> SHA-256 |
| File Type | <input type="checkbox"/> filetype <input type="checkbox"/> Default validation <input checked="" type="checkbox"/> Native support | <input type="checkbox"/> Artifact <input type="checkbox"/> MD5 <input type="checkbox"/> SHA-1 <input type="checkbox"/> SHA-256 |
| Host Type | <input type="checkbox"/> hosttype <input type="checkbox"/> Default validation | <input type="checkbox"/> Domain <input type="checkbox"/> IP <input type="checkbox"/> IPv6 |



| Function | Details |
|--|--|
| Deployment | Cloud |
| Indicator management | Support for IPv4, IPv6, URL, domain, MD5, SHA-1, SHA-256 Capabilities include: bulk or single record editing, commenting, risk adjustment, retiring, association with threats, tactics, technologies, and more |
| Enrichment | Passive and active scanning |
| Indicator normalization and de-duplication | Indicators have 1 dedicated page with normalized and structured data Data includes: screenshots, risk score & factors, registration data, threats, tactics, techniques, ports, protocols, WHOIS, location data, web technologies, DNS records, query strings, HTTP headers, SSL certificate metadata, cookies, meta tags, mail servers, redirects, related domains and URLs |
| Threat management | Add Threats and aliases; data includes: summary, description, references, news, comments, shared attributes, tactics & techniques, linked indicators |
| Pre-configured feeds | 5-20 available out-of-the-box, can be adjusted during POC |
| News tracking | RSS feeds and industry blogs, MITRE ATT&CK references, Twitter, Reddit |
| Search/querying | Explore enables searching across indicator and threat datasets with boolean logic and wildcards; available via GUI and API |
| Dashboard | Upcoming events and CFP schedule; community stream of news and trends; recent user submissions |
| Importing data | Unlimited; Feed Wizard supports CSV and STIX 2.x formats; API bulk submit via JSON; bulk and individual submissions via GUI |
| Source feed management | Set individual source feed risk scores, associated threats, enrichment type, ingestion schedule, publisher data, and more |
| Configuration rules | Create custom aging rules, STIX input mapping, threat categories, and attribute types with regex validation |
| Exporting | Unlimited; configurable CSV and STIX 2.x format; API queries |
| User roles | Unlimited admin, engineer, analyst seats |
| User access | IP range allow-listing |
| SIEM, SOAR integrations | Unlimited integrations may be added – Pulsedive supports many pre-built and any new custom integrations |
| Price | \$80K/year, multi-year discounts available |



Procurement Process

The Pulsedive Enterprise TIP procurement and onboarding process is transparent, straightforward, and fast.

Interested?



Intro

- Align on requirements and timeline
- Share product resources
- Determine key contacts, including TIP admin



POC

- 2-4 weeks free, with access to full product
- 2 optional support meetings
- Dedicated, private Slack support channel



Purchase

- Multi-year discounts available
- Complete customer procurement process
- Purchase order and invoice



Onboarding

- Your POC instance rolls right into production, no re-administration needed
- 2 optional onboarding meetings
- Continuous support via email and Slack





Get In Touch

pulsedive.com
sales@pulsedive.com

