

IOC Feed Integration Guide

Open threat-intelligence feed · Firewalls · EDR/XDR · SIEM/SOAR

Critical 90–100

High 75–89

Medium 50–74

Base URL: <https://mhearsh.github.io/threat-intel-feed/feeds> · Refresh: every 2 h · Expiry: 30 days · ● available now.
Legacy latest/ URLs remain as a compatibility mirror.

Firewalls — Palo Alto NGFW

External Dynamic Lists (pull, HTTPS).

1. Objects → External Dynamic Lists → Add. Create one list per type: IP, Domain, URL.
2. Paste the source URL below and set Repeat to Hourly.
3. Reference the EDL in a Security policy with action Deny or Drop.
4. Commit, then check List Capacities.

● IP	.../feeds/firewall/paloalto/edl-ip.txt
● Domain	.../feeds/firewall/paloalto/edl-domain.txt
● URL	.../feeds/firewall/paloalto/edl-url.txt

Firewalls — Fortinet FortiGate

Security Fabric → External Connectors → Threat Feeds.

1. Create an IP Address, Domain Name, URL, or Malware Hash feed.
2. Enter the URL below. Set refresh to 60 min.
3. Use the feed in a firewall policy, DNS filter, web filter, or AV profile.
4. Use one hash algorithm per feed.

● IP	.../feeds/firewall/fortinet/ip.txt
● Domain	.../feeds/firewall/fortinet/domain.txt
● SHA-256	.../feeds/firewall/fortinet/hash-sha256.txt

Firewalls — Check Point · Cisco · Sophos · pfSense

Plain-text pull feeds. Check Point uses its native CSV.

1. Check Point: `ioc_feeds add --feed_name tif --transport https --resource <URL>`, or add it in SmartConsole → Custom Intelligence Feeds.
2. Cisco FMC: Objects → Security Intelligence → Network/URL feed. Add the .md5 URL for intervals of 30 min or less.
3. Sophos XGS: Active Threat Response → Third-party threat feeds. Create one feed per type.
4. pfSense/OPNsense: URL Table alias or a pfBlockerNG list.

● Check Point CSV	.../feeds/firewall/checkpoint/ioc-feed.csv
● Generic IP	.../feeds/generic/txt/ip.txt
● Generic URL	.../feeds/generic/txt/url.txt

EDR — Microsoft Defender for Endpoint

Settings → Endpoints → Indicators → Import. Maximum 500 rows per file. SHA-1 and SHA-256 only.

1. Download the file CSV below.
2. Select the matching tab (File hashes, or IP addresses / URLs).
3. Import → Choose file → Import.
4. Review the actions (Audit or Block) and the expiration date.

● File hashes	.../feeds/edr/microsoft-defender/files-001.csv
● Network	.../feeds/edr/microsoft-defender/network-001.csv

EDR — CrowdStrike · SentinelOne · ESET

Import through the API, or paste the hashes.

1. CrowdStrike: import the CSV with FalconPy or PSFalcon (IOC API).
2. SentinelOne: POST the JSON to /web/api/v2.1/threat-intelligence/iocs.
3. ESET PROTECT: Blocked hashes → Add hashes. Paste the SHA-256 or SHA-1 list.

- | | |
|-----------------------|--|
| ● CrowdStrike | .../feeds/edr/crowdstrike/iocs-api.csv |
| ● SentinelOne | .../feeds/edr/sentinelone/iocs.json |
| ● ESET SHA-256 | .../feeds/edr/eset/sha256.txt |

EDR — Trend Vision One · Cortex XDR

CSV import.

1. Trend: Threat Intelligence → Suspicious Object Management → Import (max 2,000 objects / 1 MB).
2. Cortex XDR: Detection Rules → IOC → Import CSV.

- | | |
|---------------------------|---|
| ● Trend Vision One | .../feeds/edr/trendmicro/suspicious-objects.csv |
| ● Cortex XDR | .../feeds/edr/cortex-xdr/iocs.csv |

SIEM / SOAR

STIX 2.1 for TI platforms. Typed CSV for Splunk.

1. Microsoft Sentinel: Threat intelligence → Import → Import using a file → JSON. Use the array file (Sentinel JSON template); the STIX bundle stays available for other tools.
2. Splunk ES: Threat intelligence → Data sources → URL. Use the ip_intel, domain_intel, http_intel and file_intel CSVs.
3. MISP / OpenCTI / XSOAR: add the STIX file or the generic CSV as a feed.
4. QRadar / Wazuh: load the generic txt into a reference set or CDB list.

- | | |
|--------------------------|--|
| ● Sentinel JSON | .../feeds/siem-soar/microsoft-sentinel/stix21-objects.json |
| ● STIX 2.1 | .../feeds/generic/stix/stix21.json |
| ● Splunk ip_intel | .../feeds/siem-soar/splunk/ip_intel.csv |
| ● Generic CSV | .../feeds/generic/csv/iocs.csv |

Eliran Emuna

CYBER SECURITY

Threat Intelligence Feed · github.com/mhearsh/threat-intel-feed · 2026