Implement Threat Intelligence Principles

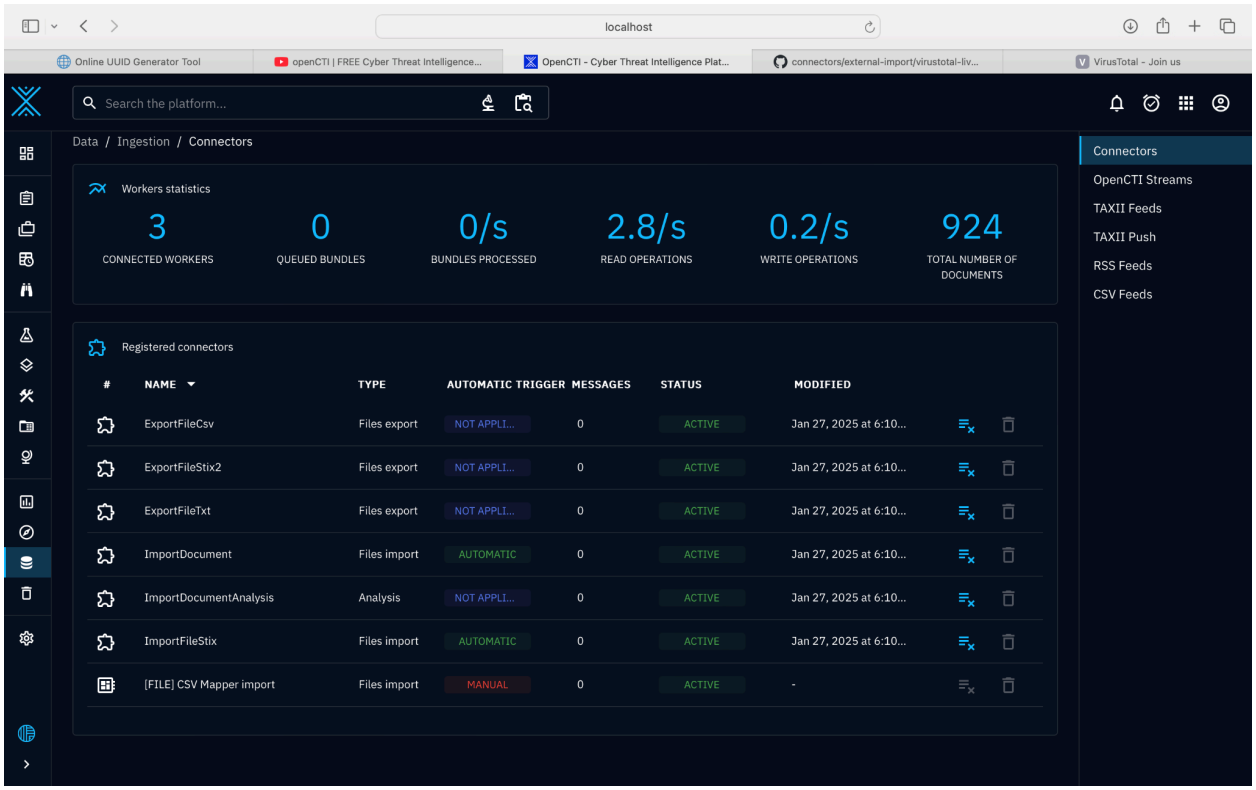
Indicators of Compromise (IoCs) and Detection Methods

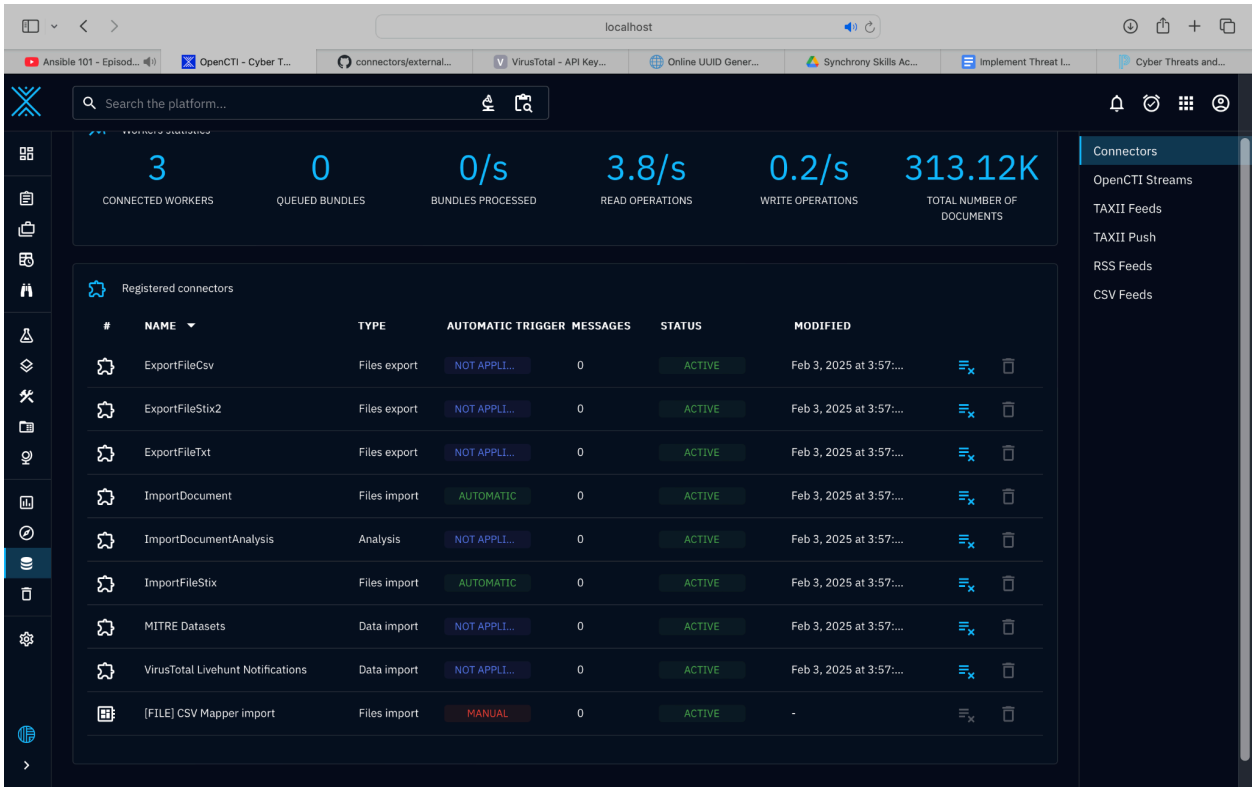
1. **Suspicious IP Addresses**

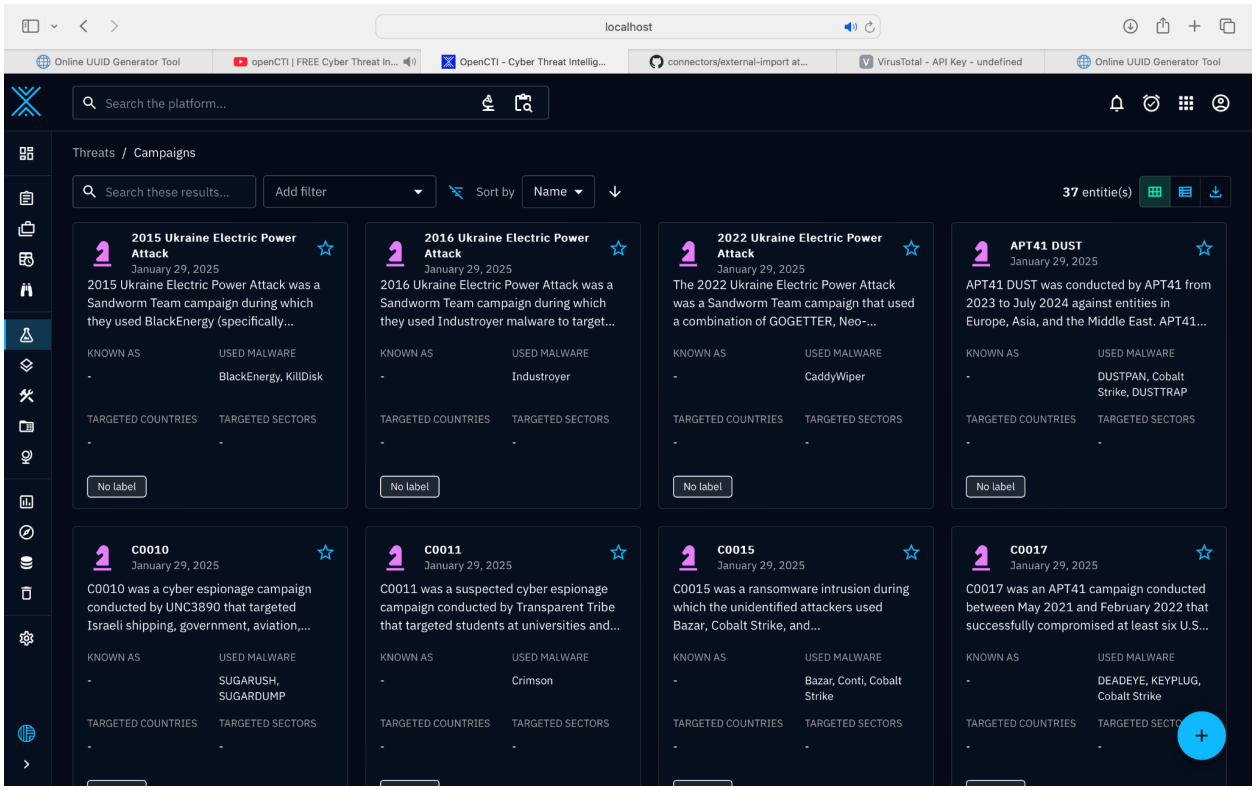
- Detection Methods:
    - Network traffic monitoring tools (e.g., Wireshark, Snort) can flag and analyze incoming/outgoing packets for connections with blacklisted or unusual IPs.
    - Threat intelligence feeds maintain databases of malicious IPs, which security software cross-references in real-time.
- How It Indicates Threats:
    - Frequent connections to a known malicious IP address could indicate botnet activity, data exfiltration, or unauthorized remote control by attackers.
    - Unusual spikes in traffic to obscure regions suggest potential communication with command-and-control servers.

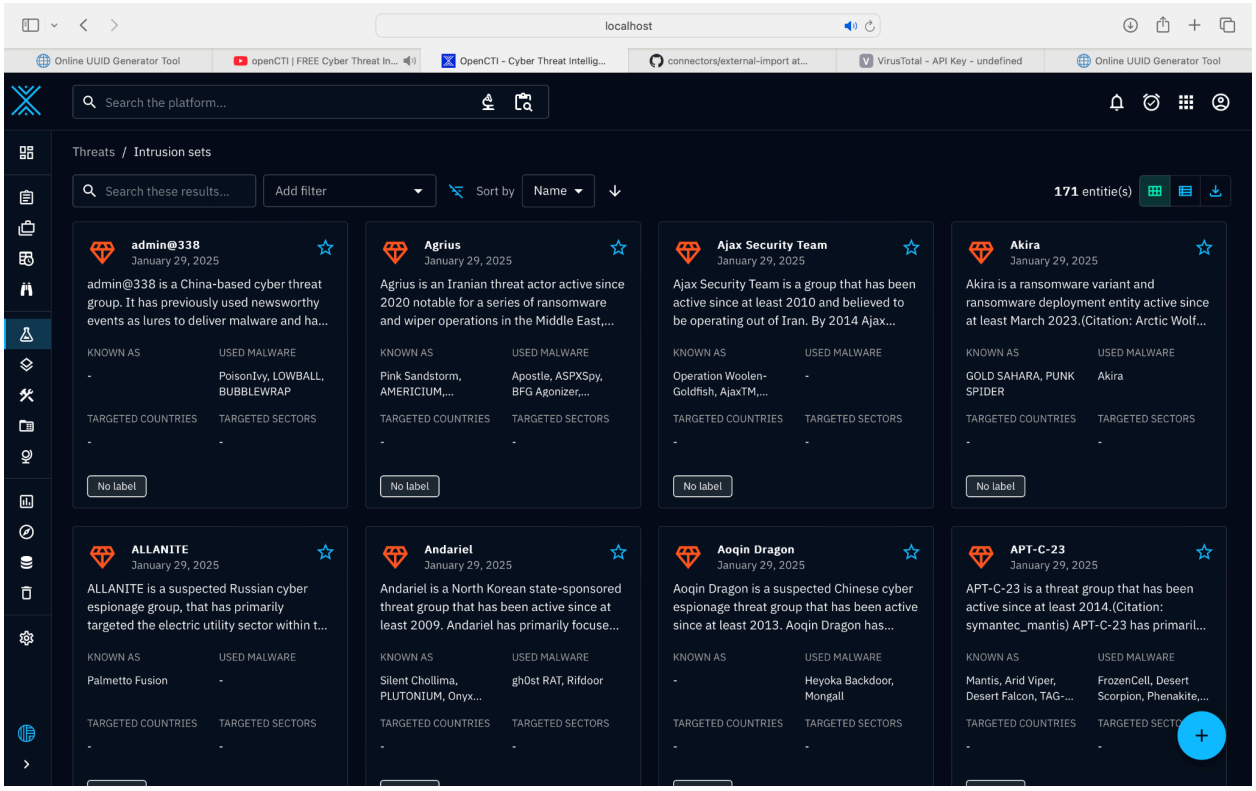
2. **Abnormal File Hashes (Malicious Executables)**

- Detection Methods:
    - Endpoint security solutions like antivirus and EDR systems scan files for signature-based matches against known malware hashes
    - Tools such as VirusTotal and SHA256 checks help validate the integrity of files.
- How It Indicates Threats:
    - If a file's hash matches that of a known malicious payload, it may point to ransomware, trojans, or backdoors on the system.
    - Files with uncommon hashes may indicate polymorphic malware that changes slightly to evade signature-based detection.


localhost
Online UUID Generator Tool
openCTI | FREE Cyber Threat Intelligence...
OpenCTI - Cyber Threat Intelligence Plat...
connectors/external-import/virustotal-liv...
VirusTotal - Join us
Search the platform...
Data / Ingestion / Connectors
Connectors
OpenCTI Streams
TAXII Feeds
TAXII Push
RSS Feeds
CSV Feeds
Workers statistics
3 CONNECTED WORKERS
0 QUEUED BUNDLES
0/s BUNDLES PROCESSED
2.8/s READ OPERATIONS
0.2/s WRITE OPERATIONS
924 TOTAL NUMBER OF DOCUMENTS
Registered connectors
NAME TYPE AUTOMATIC TRIGGER MESSAGES STATUS MODIFIED
ExportFileCsv Files export NOT APPLI... 0 ACTIVE Jan 27, 2025 at 6:10...
ExportFileStix2 Files export NOT APPLI... 0 ACTIVE Jan 27, 2025 at 6:10...
ExportFileTxt Files export NOT APPLI... 0 ACTIVE Jan 27, 2025 at 6:10...
ImportDocument Files import AUTOMATIC 0 ACTIVE Jan 27, 2025 at 6:10...
ImportDocumentAnalysis Analysis NOT APPLI... 0 ACTIVE Jan 27, 2025 at 6:10...
ImportFileStix Files import AUTOMATIC 0 ACTIVE Jan 27, 2025 at 6:10...
[FILE] CSV Mapper import Files import MANUAL 0 ACTIVE -


localhost
Ansible 101 - Episod...
OpenCTI - Cyber T...
connectors/external...
VirusTotal - API Key...
Online UUID Gener...
Synchrony Skills Ac...
Implement Threat I...
Cyber Threats and...
Search the platform...
Connectors
OpenCTI Streams
TAXII Feeds
TAXII Push
RSS Feeds
CSV Feeds
3 CONNECTED WORKERS
0 QUEUED BUNDLES
0/s BUNDLES PROCESSED
3.8/s READ OPERATIONS
0.2/s WRITE OPERATIONS
313.12K TOTAL NUMBER OF DOCUMENTS
Registered connectors
NAME TYPE AUTOMATIC TRIGGER MESSAGES STATUS MODIFIED
ExportFileCsv Files export NOT APPLI... 0 ACTIVE Feb 3, 2025 at 3:57:...
ExportFileStix2 Files export NOT APPLI... 0 ACTIVE Feb 3, 2025 at 3:57:...
ExportFileTxt Files export NOT APPLI... 0 ACTIVE Feb 3, 2025 at 3:57:...
ImportDocument Files import AUTOMATIC 0 ACTIVE Feb 3, 2025 at 3:57:...
ImportDocumentAnalysis Analysis NOT APPLI... 0 ACTIVE Feb 3, 2025 at 3:57:...
ImportFileStix Files import AUTOMATIC 0 ACTIVE Feb 3, 2025 at 3:57:...
MITRE Datasets Data import NOT APPLI... 0 ACTIVE Feb 3, 2025 at 3:57:...
VirusTotal Livehunt Notifications Data import NOT APPLI... 0 ACTIVE Feb 3, 2025 at 3:57:...
[FILE] CSV Mapper import Files import MANUAL 0 ACTIVE -


localhost
Online UUID Generator Tool
openCTI | FREE Cyber Threat In...
OpenCTI - Cyber Threat Intellig...
connectors/external-import at...
VirusTotal - API Key - undefined
Online UUID Generator Tool
Search the platform...
Threats / Campaigns
Search these results...
Add filter
Sort by
Name
37 entitie(s)
2015 Ukraine Electric Power Attack
January 29, 2025
2015 Ukraine Electric Power Attack was a Sandworm Team campaign during which they used BlackEnergy (specifically...
KNOWN AS
USED MALWARE
-
BlackEnergy, KillDisk
TARGETED COUNTRIES
TARGETED SECTORS
-
-
No label
2016 Ukraine Electric Power Attack
January 29, 2025
2016 Ukraine Electric Power Attack was a Sandworm Team campaign during which they used Industroyer malware to target...
KNOWN AS
USED MALWARE
-
Industroyer
TARGETED COUNTRIES
TARGETED SECTORS
-
-
No label
2022 Ukraine Electric Power Attack
January 29, 2025
The 2022 Ukraine Electric Power Attack was a Sandworm Team campaign that used a combination of GOGETTER, Neo-...
KNOWN AS
USED MALWARE
-
CaddyWiper
TARGETED COUNTRIES
TARGETED SECTORS
-
-
No label
APT41 DUST
January 29, 2025
APT41 DUST was conducted by APT41 from 2023 to July 2024 against entities in Europe, Asia, and the Middle East. APT41...
KNOWN AS
USED MALWARE
-
DUSTPAN, Cobalt Strike, DUSTTRAP
TARGETED COUNTRIES
TARGETED SECTORS
-
-
No label
C0010
January 29, 2025
C0010 was a cyber espionage campaign conducted by UNC3890 that targeted Israeli shipping, government, aviation,...
KNOWN AS
USED MALWARE
-
SUGARUSH, SUGARDUMP
TARGETED COUNTRIES
TARGETED SECTORS
-
-
C0011
January 29, 2025
C0011 was a suspected cyber espionage campaign conducted by Transparent Tribe that targeted students at universities and...
KNOWN AS
USED MALWARE
-
Crimson
TARGETED COUNTRIES
TARGETED SECTORS
-
-
C0015
January 29, 2025
C0015 was a ransomware intrusion during which the unidentified attackers used Bazar, Cobalt Strike, and...
KNOWN AS
USED MALWARE
-
Bazar, Conti, Cobalt Strike
TARGETED COUNTRIES
TARGETED SECTORS
-
-
C0017
January 29, 2025
C0017 was an APT41 campaign conducted between May 2021 and February 2022 that successfully compromised at least six U.S...
KNOWN AS
USED MALWARE
-
DEADEYE, KEYPLUG, Cobalt Strike
TARGETED COUNTRIES
-


localhost
Online UUID Generator Tool
openCTI | FREE Cyber Threat In...
OpenCTI - Cyber Threat Intellig...
connectors/external-import at...
VirusTotal - API Key - undefined
Online UUID Generator Tool
Search the platform...
Threats / Intrusion sets
Search these results...
Add filter
Sort by
Name
171 entitie(s)
admin@338
January 29, 2025
admin@338 is a China-based cyber threat group. It has previously used newsworthy events as lures to deliver malware and ha...
KNOWN AS
USED MALWARE
-
PoisonIvy, LOWBALL, BUBBLEWRAP
TARGETED COUNTRIES
TARGETED SECTORS
-
-
No label
Agrius
January 29, 2025
Agrius is an Iranian threat actor active since 2020 notable for a series of ransomware and wiper operations in the Middle East,...
KNOWN AS
USED MALWARE
Pink Sandstorm, AMERICIUM,...
Apostle, ASPXSpy, BFG Agonizer,...
TARGETED COUNTRIES
TARGETED SECTORS
-
-
No label
Ajax Security Team
January 29, 2025
Ajax Security Team is a group that has been active since at least 2010 and believed to be operating out of Iran. By 2014 Ajax...
KNOWN AS
USED MALWARE
Operation Woolen-Goldfish, AjaxTM,...
-
TARGETED COUNTRIES
TARGETED SECTORS
-
-
No label
Akira
January 29, 2025
Akira is a ransomware variant and ransomware deployment entity active since at least March 2023.(Citation: Arctic Wolf...
KNOWN AS
USED MALWARE
GOLD SAHARA, PUNK SPIDER
Akira
TARGETED COUNTRIES
TARGETED SECTORS
-
-
No label
ALLANITE
January 29, 2025
ALLANITE is a suspected Russian cyber espionage group, that has primarily targeted the electric utility sector within t...
KNOWN AS
USED MALWARE
Palmetto Fusion
-
TARGETED COUNTRIES
TARGETED SECTORS
-
-
Andariel
January 29, 2025
Andariel is a North Korean state-sponsored threat group that has been active since at least 2009. Andariel has primarily focuse...
KNOWN AS
USED MALWARE
Silent Chollima, PLUTONIUM, Onyx...
gh0st RAT, Rifdoor
TARGETED COUNTRIES
TARGETED SECTORS
-
-
Aoqin Dragon
January 29, 2025
Aoqin Dragon is a suspected Chinese cyber espionage threat group that has been active since at least 2013. Aoqin Dragon has...
KNOWN AS
USED MALWARE
-
Heyoka Backdoor, Mongall
TARGETED COUNTRIES
TARGETED SECTORS
-
-
APT-C-23
January 29, 2025
APT-C-23 is a threat group that has been active since at least 2014.(Citation: symantec_mantis) APT-C-23 has primaril...
KNOWN AS
USED MALWARE
Mantis, Arid Viper, Desert Falcon, TAG-...
FrozenCell, Desert Scorpion, Phenakite,...
TARGETED COUNTRIES
-

MITRE and VirusTotal Connectors Integration

Connector Analysis:

Connector Name	Type	Automatic Trigger	Messages	Status	Modified
MITRE Datasets	Data Import	Not Applicable	0	Active	Feb 3, 2025
VirusTotal Livehunt Notifications	Data Import	Not Applicable	0	Active	Feb 3, 2025

Expected Data After Integration:

1. MITRE Datasets Connector:
    - You'll see structured threat intelligence data aligned with the MITRE ATT&CK framework.
    - Entities such as techniques, tactics, software, tools, groups (threat actors), and mitigation strategies will populate the database.
    - Enhanced attack pattern relationships, tactic graphs, and visualizations showing connections between threat actors and techniques.
    - Rich metadata on threat vectors, adversarial campaigns, and defensive recommendations.
2. VirusTotal Livehunt Notifications Connector:
    - Import and display data on the latest malware indicators (e.g., file hashes, URLs, domains).
    - Behavioral analysis and malware relationships tied to threat reports.
    - Alerts about malicious files or threat campaigns sourced from the VirusTotal community.
    - Integration with OpenCTI graphs to track evolving malware trends and enhance detection strategies.

Findings and Observations:

1. Operational Status: Both MITRE Datasets and VirusTotal Livehunt Notifications connectors are currently active, indicating that they are properly integrated and functional.
2. Trigger Configuration: Neither connector is configured for automatic triggers, suggesting that manual or scheduled processes may be required to fetch data.
3. Data Import Roles:
    - MITRE Datasets: Provides essential information about attack techniques, threat actor tactics, and procedural details aligned with MITRE ATT&CK framework data.
    - VirusTotal Livehunt Notifications: Enables the import of critical malware detection and behavioral analysis data for enhanced threat monitoring.

Recommendations:

1. **Trigger Automation**: Consider configuring automated triggers for these connectors to ensure regular and timely data imports without manual intervention.
2. **Data Verification**: Periodically review the incoming data from MITRE and VirusTotal to validate its relevance and integrity for ongoing threat analysis.
3. **Operational Monitoring**: Maintain continuous health checks of these connectors to ensure uninterrupted import of key threat intelligence feeds.