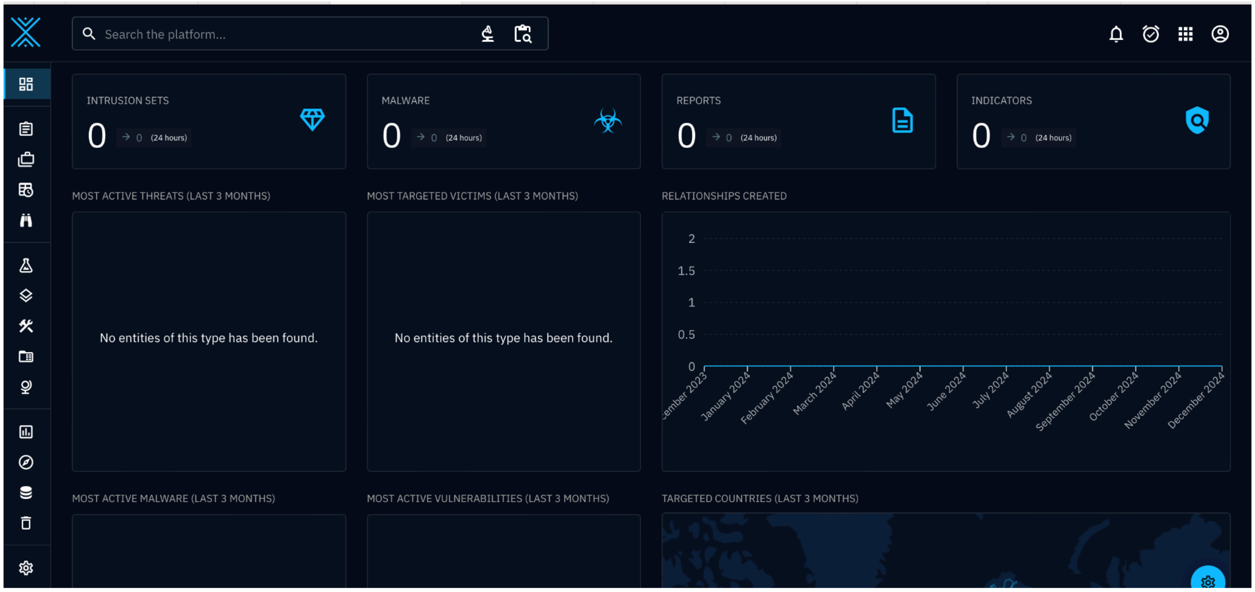
Indicators of Compromise:

1. **IP Address is linked to attackers**
    a. **Threat Intelligence Feeds & Blacklists**
        i. Firewalls and IDS/IPS monitor incoming and outgoing network traffic.
        ii. Tools: Snort, Suricata, Zeek (formerly Bro).
    b. **Log Analysis & SIEM Systems**
        i. Security Information and Event Management (SIEM) solutions aggregate logs from different network devices and analyze traffic patterns.
        ii. Tools: Splunk, IBM QRadar, Elastic Security.
    c. **How It Indicates Threats**
        i. An IP associated with previous attacks may be attempting unauthorized access to a system.
        ii. A spike in connections from a single suspicious IP suggests a DDoS attack or reconnaissance scanning.
        iii. Communication with a malicious IP post-breach may mean a command and control (C2) server is directing malware inside the network.
2. **Host based indicators**
    a. **File Integrity Monitoring (FIM)**
        i. Tracks changes in critical system files, configuration settings, or registry entries.
        ii. Tools: Tripwire, OSSEC, Wazuh.
    b. **Endpoint Detection & Response (EDR) Solutions**
        i. EDR solutions continuously monitor processes, memory usage, and system behavior.
        ii. Tools: CrowdStrike Falcon, Microsoft Defender ATP, SentinelOne.
    c. **How It Indicates Threats**
        i. New or modified startup items (registry keys, scheduled tasks) could mean persistence mechanisms are in place.
        ii. Unusual process behavior (e.g., LSASS memory dumping) suggests credential theft attempts.
        iii. Unauthorized file changes (e.g., system file tampering) may indicate rootkit or malware installation.

What OpenCTI dashboard looked like before adding connectors:



Search the platform...

INTRUSION SETS
0 → 0 (24 hours)

MALWARE
0 → 0 (24 hours)

REPORTS
0 → 0 (24 hours)

INDICATORS
0 → 0 (24 hours)

MOST ACTIVE THREATS (LAST 3 MONTHS)

No entities of this type has been found.

MOST TARGETED VICTIMS (LAST 3 MONTHS)

No entities of this type has been found.

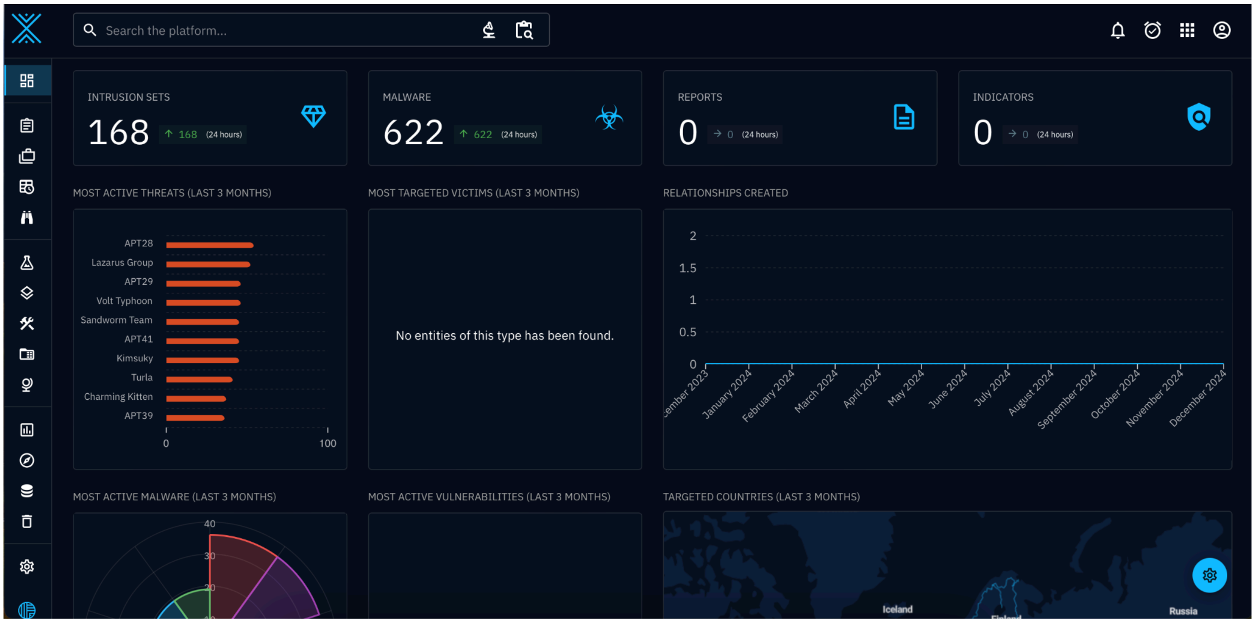
RELATIONSHIPS CREATED

MOST ACTIVE MALWARE (LAST 3 MONTHS)

MOST ACTIVE VULNERABILITIES (LAST 3 MONTHS)

TARGETED COUNTRIES (LAST 3 MONTHS)

What OpenCTI dashboard looked like after adding connectors:



Search the platform...

INTRUSION SETS
168 ↑ 168 (24 hours)

MALWARE
622 ↑ 622 (24 hours)

REPORTS
0 → 0 (24 hours)

INDICATORS
0 → 0 (24 hours)

MOST ACTIVE THREATS (LAST 3 MONTHS)

MOST TARGETED VICTIMS (LAST 3 MONTHS)

No entities of this type has been found.

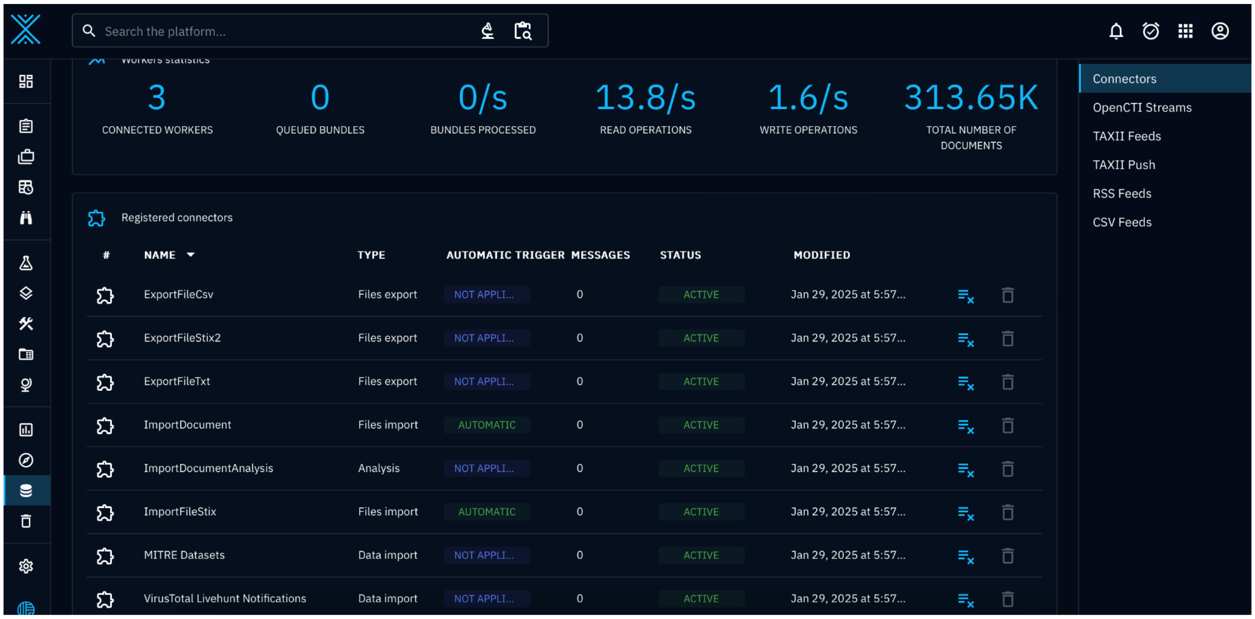
RELATIONSHIPS CREATED

MOST ACTIVE MALWARE (LAST 3 MONTHS)

MOST ACTIVE VULNERABILITIES (LAST 3 MONTHS)

TARGETED COUNTRIES (LAST 3 MONTHS)

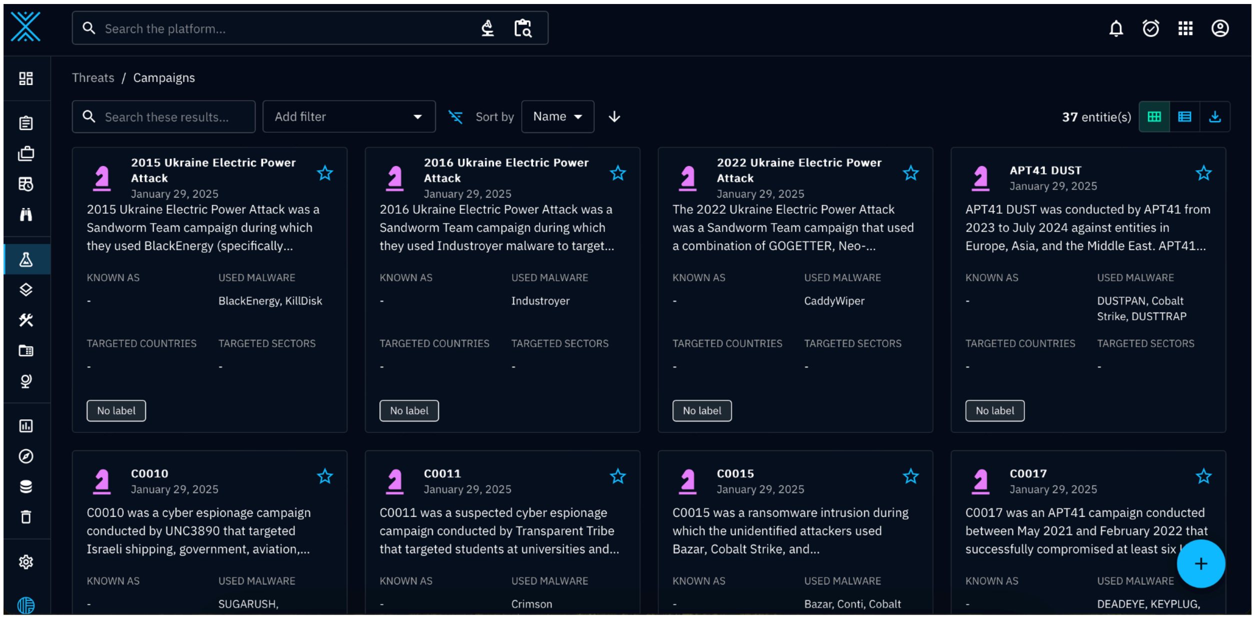
List of connectors:



3	0	0/s	13.8/s	1.6/s	313.65K
CONNECTED WORKERS	QUEUED BUNDLES	BUNDLES PROCESSED	READ OPERATIONS	WRITE OPERATIONS	TOTAL NUMBER OF DOCUMENTS

Registered connectors

#	NAME	TYPE	AUTOMATIC TRIGGER	MESSAGES	STATUS	MODIFIED
	ExportFileCsv	Files export	NOT APPLI...	0	ACTIVE	Jan 29, 2025 at 5:57...
	ExportFileStix2	Files export	NOT APPLI...	0	ACTIVE	Jan 29, 2025 at 5:57...
	ExportFileTxt	Files export	NOT APPLI...	0	ACTIVE	Jan 29, 2025 at 5:57...
	ImportDocument	Files import	AUTOMATIC	0	ACTIVE	Jan 29, 2025 at 5:57...
	ImportDocumentAnalysis	Analysis	NOT APPLI...	0	ACTIVE	Jan 29, 2025 at 5:57...
	ImportFileStix	Files import	AUTOMATIC	0	ACTIVE	Jan 29, 2025 at 5:57...
	MITRE Datasets	Data import	NOT APPLI...	0	ACTIVE	Jan 29, 2025 at 5:57...
	VirusTotal Livehunt Notifications	Data import	NOT APPLI...	0	ACTIVE	Jan 29, 2025 at 5:57...



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

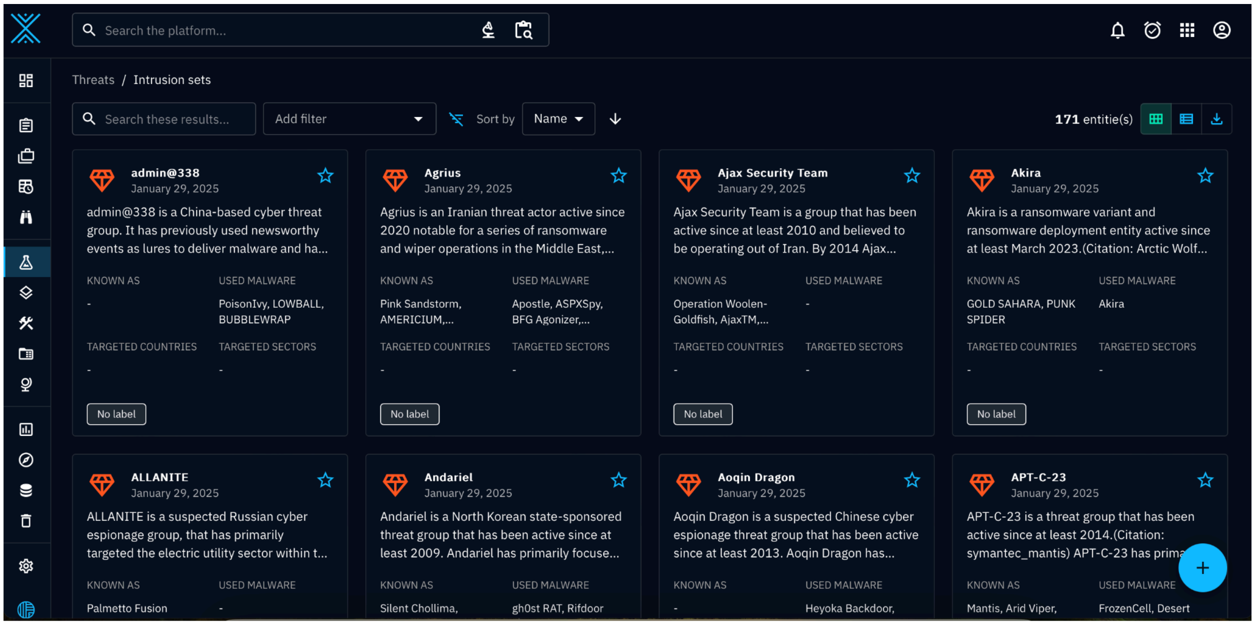
APT41 DUST
January 29, 2025
APT41 DUST was conducted by APT41 from 2023 to July 2024 against entities in Europe, Asia, and the Middle East. APT41...
KNOWN AS: -
USED MALWARE: DUSTPAN, Cobalt Strike, DUSTTRAP
TARGETED COUNTRIES: -
TARGETED SECTORS: -
No label

C0010
January 29, 2025
C0010 was a cyber espionage campaign conducted by UNC3890 that targeted Israeli shipping, government, aviation,...
KNOWN AS: -
USED MALWARE: SUGARUSH,

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

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

C0017
January 29, 2025
C0017 was an APT41 campaign conducted between May 2021 and February 2022 that successfully compromised at least six
KNOWN AS: -
USED MALWARE: DEADEYE, KEYPLUG,



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: Pink Sandstorm, AMERICIUM,...
USED MALWARE: 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: Operation Woolen-Goldfish, AjaxTM,...
USED MALWARE: -
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: GOLD SAHARA, PUNK SPIDER
USED MALWARE: 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: Palmetto Fusion
USED MALWARE: -

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: Silent Chollima,
USED MALWARE: gh0st RAT, Rifdoor

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,

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 prima

KNOWN AS: Mantis, Arid Viper,
USED MALWARE: FrozenCell, Desert