Building a Threat Intelligence Capability with OpenCTI: A Case Study from Exke Corporation

Introduction

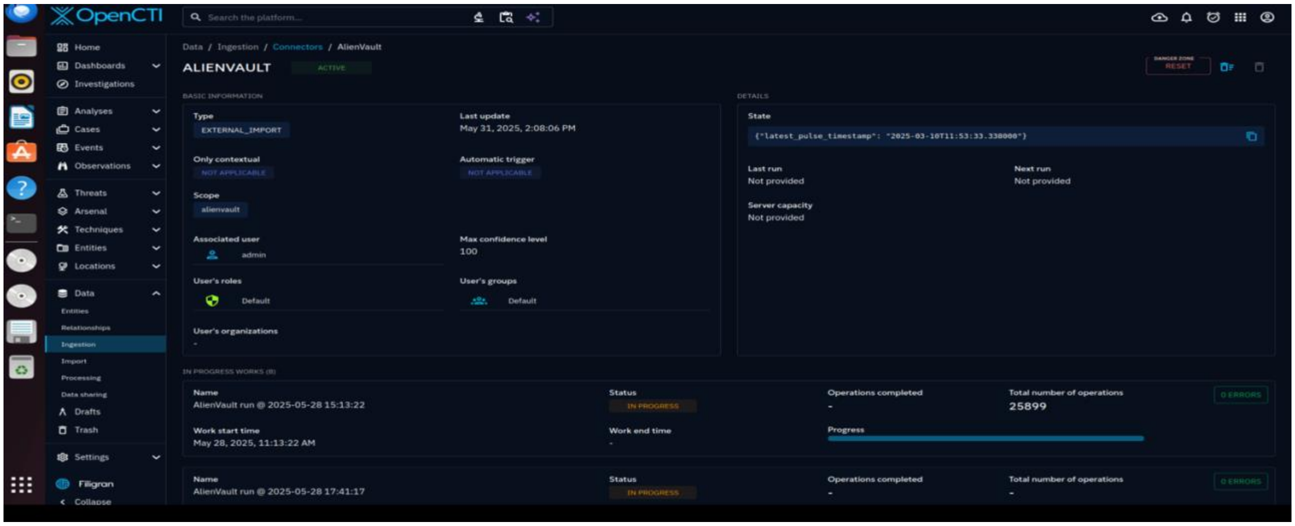
This report presents a case study on building a foundational threat intelligence capability at Exke Corporation using the Open Cyber Threat Intelligence (OpenCTI) platform. As part of our ongoing efforts to strengthen cybersecurity posture and enhance proactive threat detection, we successfully integrated the AlienVault OTX connector into our OpenCTI instance. The integration enabled the automated ingestion and enrichment of Indicators of Compromise (IOCs) with real-time threat intelligence sourced from AlienVault's Open Threat Exchange (OTX). This setup allowed for improved situational awareness, more accurate threat attribution, and streamlined incident response processes.

This case study outlines the architecture, configuration process, challenges encountered, and the resulting operational benefits. It is intended to serve as both documentation of the implementation and a guide for similar organizations aiming to leverage OpenCTI for cyber threat intelligence.

Contributions

1. Installation, Data Collection and Analysis

One of my primary responsibilities involved installing the OpenCTI in my Linux(Ubuntu), Connecting the AlienVault for data collection , open-source intelligence (OSINT), internal logs, and third-party threat feeds. I ensured the data was organized, validated, and analyzed to identify patterns and anomalies indicative of emerging threats. My thorough approach resulted in the identification of actionable intelligence that informed decision-making.



Data / Ingestion / Connectors / AlienVault

ALIENVAULT ACTIVE

BASIC INFORMATION

Type
EXTERNAL_IMPORT

Last update
May 31, 2025, 2:08:06 PM

Only contextual
NOT APPLICABLE

Automatic trigger
NOT APPLICABLE

Scope
alienvault

Associated user
admin

Max confidence level
100

User's roles
Default

User's groups
Default

User's organizations
-

DETAILS

State

```
{"latest_pulse_timestamp": "2025-03-10T11:53:33.338000"}
```

Last run
Not provided

Next run
Not provided

Server capacity
Not provided

IN PROGRESS WORKS (8)

Name
AlienVault run @ 2025-05-28 15:13:22

Status
IN PROGRESS

Operations completed
-

Total number of operations
25899

0 ERRORS

Work start time
May 28, 2025, 11:13:22 AM

Work end time
-

Progress

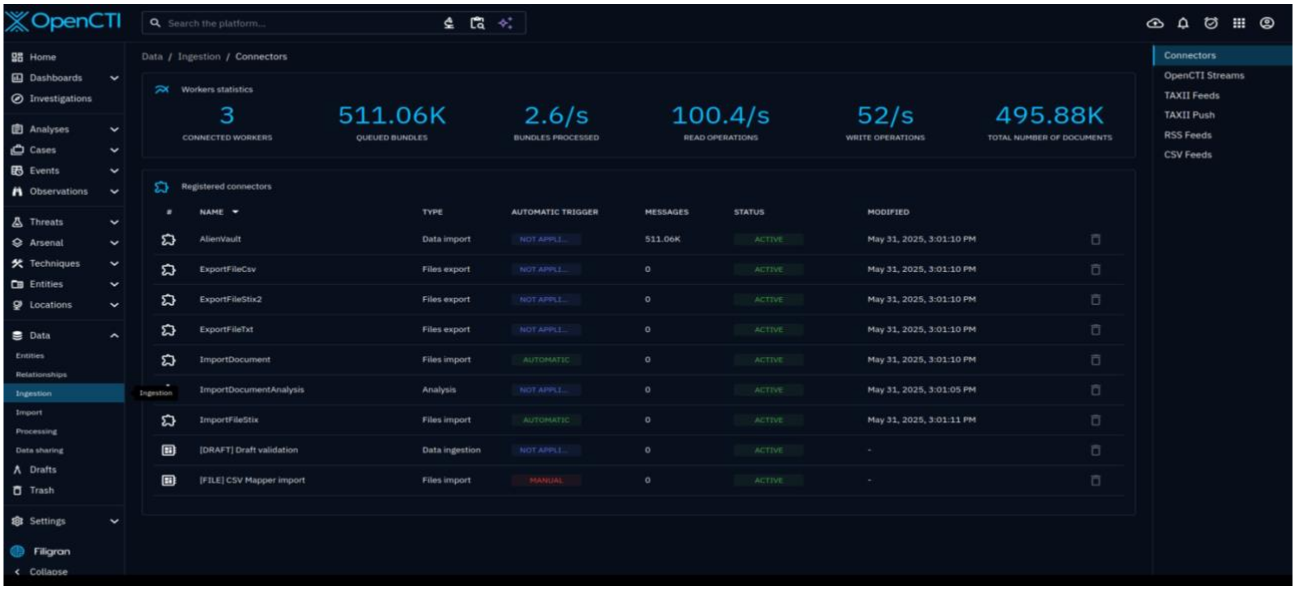
Name
AlienVault run @ 2025-05-28 17:41:17

Status
IN PROGRESS

Operations completed
-

Total number of operations
-

0 ERRORS



Workers statistics

3	511.06K	2.6/s	100.4/s	52/s	495.88K
CONNECTED WORKERS	QUEUED BUNDLES	BUNDLES PROCESSED	READ OPERATIONS	WRITE OPERATIONS	TOTAL NUMBER OF DOCUMENTS

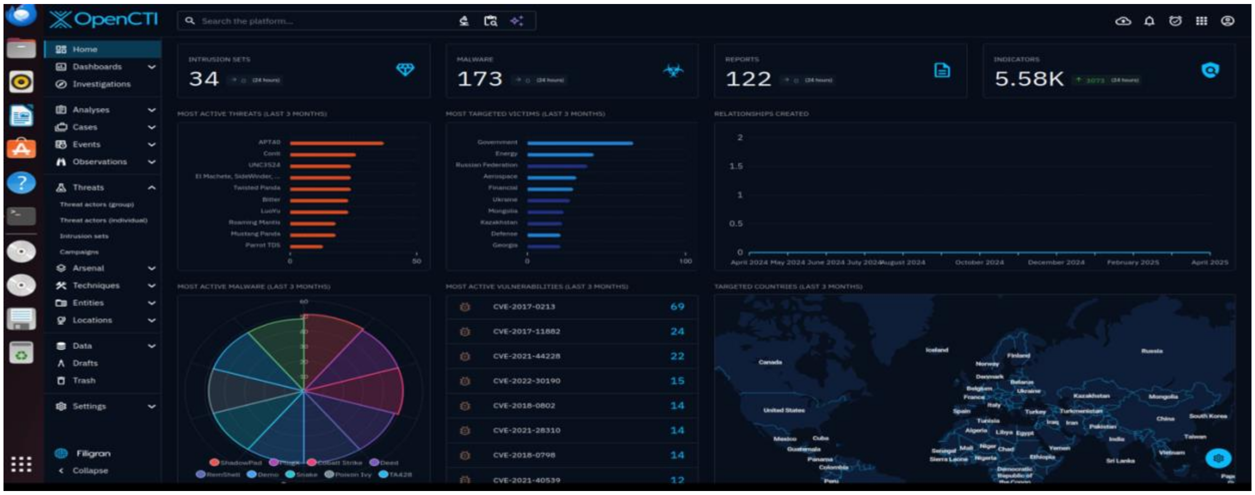
Registered connectors

#	NAME	TYPE	AUTOMATIC TRIGGER	MESSAGES	STATUS	MODIFIED
	AlienVault	Data import	NOT APPLI...	511.06K	ACTIVE	May 31, 2025, 3:01:10 PM
	ExportFileCsv	Files export	NOT APPLI...	0	ACTIVE	May 31, 2025, 3:01:10 PM
	ExportFileStix2	Files export	NOT APPLI...	0	ACTIVE	May 31, 2025, 3:01:10 PM
	ExportFileTxt	Files export	NOT APPLI...	0	ACTIVE	May 31, 2025, 3:01:10 PM
	ImportDocument	Files import	AUTOMATIC	0	ACTIVE	May 31, 2025, 3:01:10 PM
	ImportDocumentAnalysis	Analysis	NOT APPLI...	0	ACTIVE	May 31, 2025, 3:01:05 PM
	ImportFileStix	Files import	AUTOMATIC	0	ACTIVE	May 31, 2025, 3:01:11 PM
	[DRAFT] Draft validation	Data ingestion	NOT APPLI...	0	ACTIVE	-
	[FILE] CSV Mapper import	Files import	MANUAL	0	ACTIVE	-

A screenshot showing the AlienVault-otx connector is active and pulling data

2. Threat Identification and Analysis

I contributed to the development of the task by identifying the top 3 most recently targeted victims within the last 3 months. Collaborating with my team member, I helped made research that streamlined the process of identifying the victims involved, the threat actors, malware/tools used, campaign involved. Also, I was able to breakdown the threat using the Diamond model(Adversary, Capability, Infrastructure, Victim). Added was the timeline of the attack as well as the Global Kill Chain.



CVE-2017-0213	69
CVE-2017-11882	24
CVE-2021-44228	22
CVE-2022-30190	15
CVE-2018-0802	14
CVE-2021-28310	14
CVE-2018-0798	14
CVE-2021-40539	12

Graphical representation from OpenCTI displaying the most active threats and most targeted victims in the last 3 months

3. Collaboration and Communication

Effective threat intelligence relies heavily on communication across teams and organizations. I played a key role by installing the OpenCTI and AlienVault, sharing findings, and contributing to the team strategic discussions. My ability to translate technical insights into actionable recommendations ensured that all team members had vast knowledge of what it was all about.

4. Development of Threat Intelligence Reports

I crafted detailed threat intelligence reports using the results I got from OpenCTI and other intelligence sources which summarized findings, recommended mitigation strategies, and highlighted emerging trends. These reports were distributed to other members of the team, hereby fostering a culture of cybersecurity awareness and preparedness.

Lessons Learned

1. Importance of Collaboration

One of the most significant lessons I learned is the value of teamwork in threat intelligence. The phase demonstrated how diverse perspectives and expertise contribute to a more comprehensive understanding of threats and enable more robust mitigation strategies.

2. Adaptability in a Dynamic Environment

The threat landscape is constantly evolving, requiring professionals to adapt their methodologies and tools. Through this experience, I gained insights into the importance of using OpenCTI and other threat intelligence sources to make findings and research. Also, with the use of Linux, I learned more about using the command line interface.

3. Challenges Faced

The challenges I faced was with the installation of the OpenCTI, I have an 8gb RAM MacBook Pro laptop which isn't enough to run the OpenCTI if I have to allocate 4gb RAM to keep my pc running. The craziest thing I did was to allocate 7gb out of 8gb RAM before I was able to install both the OpenCTI and AlienVault.

4. Critical Thinking and Decision-Making

Analyzing threats and determining appropriate responses honed my critical thinking skills. I learned to evaluate risks from multiple angles and make informed decisions under pressure, which will undoubtedly benefit my future endeavors.

5. Value of Proactive Measures

Another key takeaway was the importance of proactive measures in preventing security incidents. Investing time in identifying vulnerabilities and anticipating threats proved instrumental in reducing the organization's risk exposure.

Conclusion

My contributions to the threat intelligence phase not only bolstered the team's cybersecurity posture but also provided me with invaluable learning experiences that have shaped my professional growth. The skills and insights I developed during this phase will continue to guide my approach to cybersecurity challenges, enabling me to contribute effectively to future projects and initiatives.

Recommendations

To maximize the value of threat intelligence processes, I recommend the following:

- Enhancing collaboration by fostering interdepartmental communication.
- Investing in advanced tools for real-time threat monitoring.
- Providing continuous training to stay abreast of emerging threats and technologies.

This report serves as a reflection of my contributions and lessons learned, underscoring the importance of threat intelligence in safeguarding organizational assets.