OpenCTI TryHackMe Walkthrough

8 min read · Dec 15, 2023

Kryptologyst

This room will cover the concepts and usage of OpenCTI, an open-source threat intelligence platform. The room will help you understand and answer the following questions:

- What is OpenCTI and how is it used?
- How would I navigate through the platform?
- What functionalities will be important during a security threat analysis?

Cyber Threat Intelligence is typically a managerial mystery to handle, with organisations battling with how to input, digest, analyse and present threat data in a way that will make sense. From the rooms that have been linked on the overview, it is clear that there are numerous platforms that have been developed to tackle the

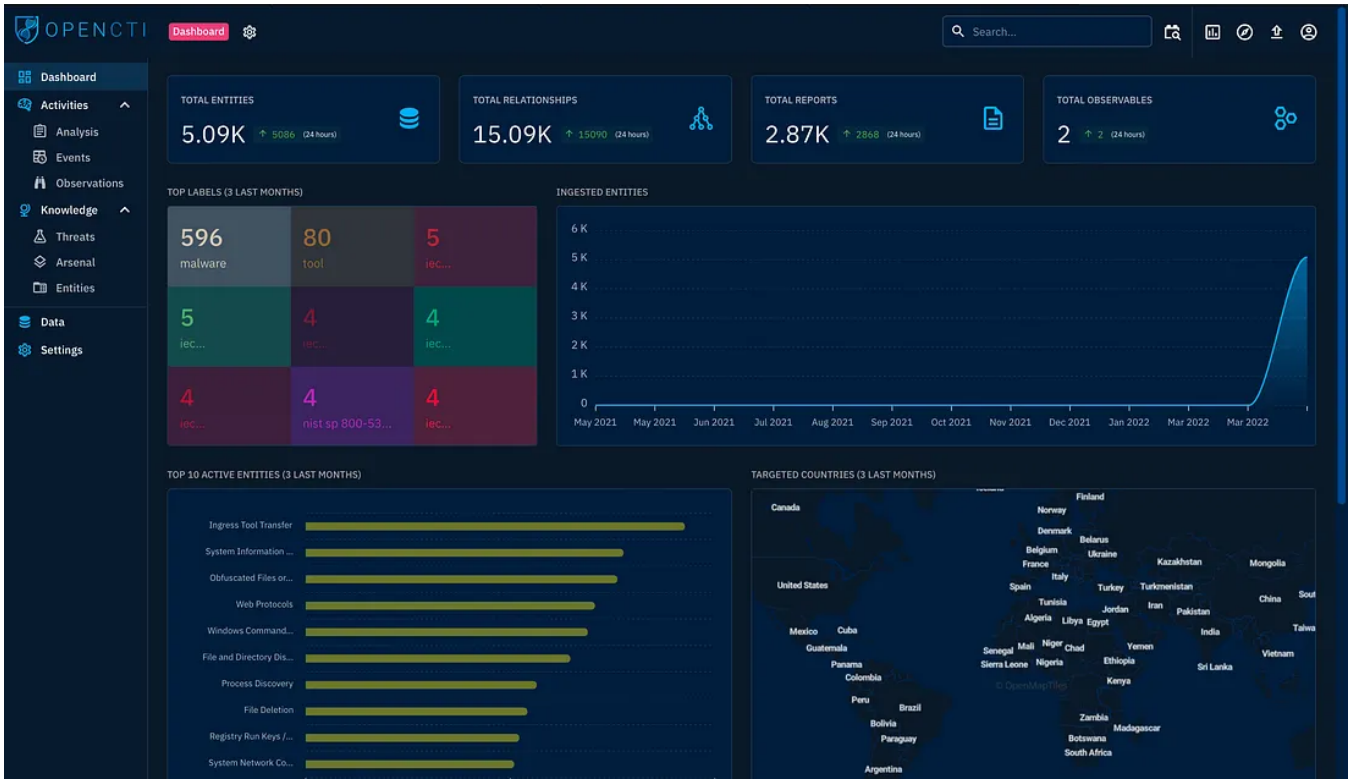
juggernaut that is Threat Intelligence.

OpenCTI

OpenCTI is another open-sourced platform designed to provide organisations with the means to manage CTI through the storage, analysis, visualisation and presentation of threat campaigns, malware and IOCs.

Objective

Developed by the collaboration of the French National cybersecurity agency (ANSSI), the platform's main objective is to create a comprehensive tool that allows users to capitalise on technical and non-technical information while developing relationships between each piece of information and its primary source. The platform can use the MITRE ATT&CK framework to structure the data. Additionally, it can be integrated with other threat intel tools such as MISP and TheHive. Rooms to these tools have been linked in the overview.

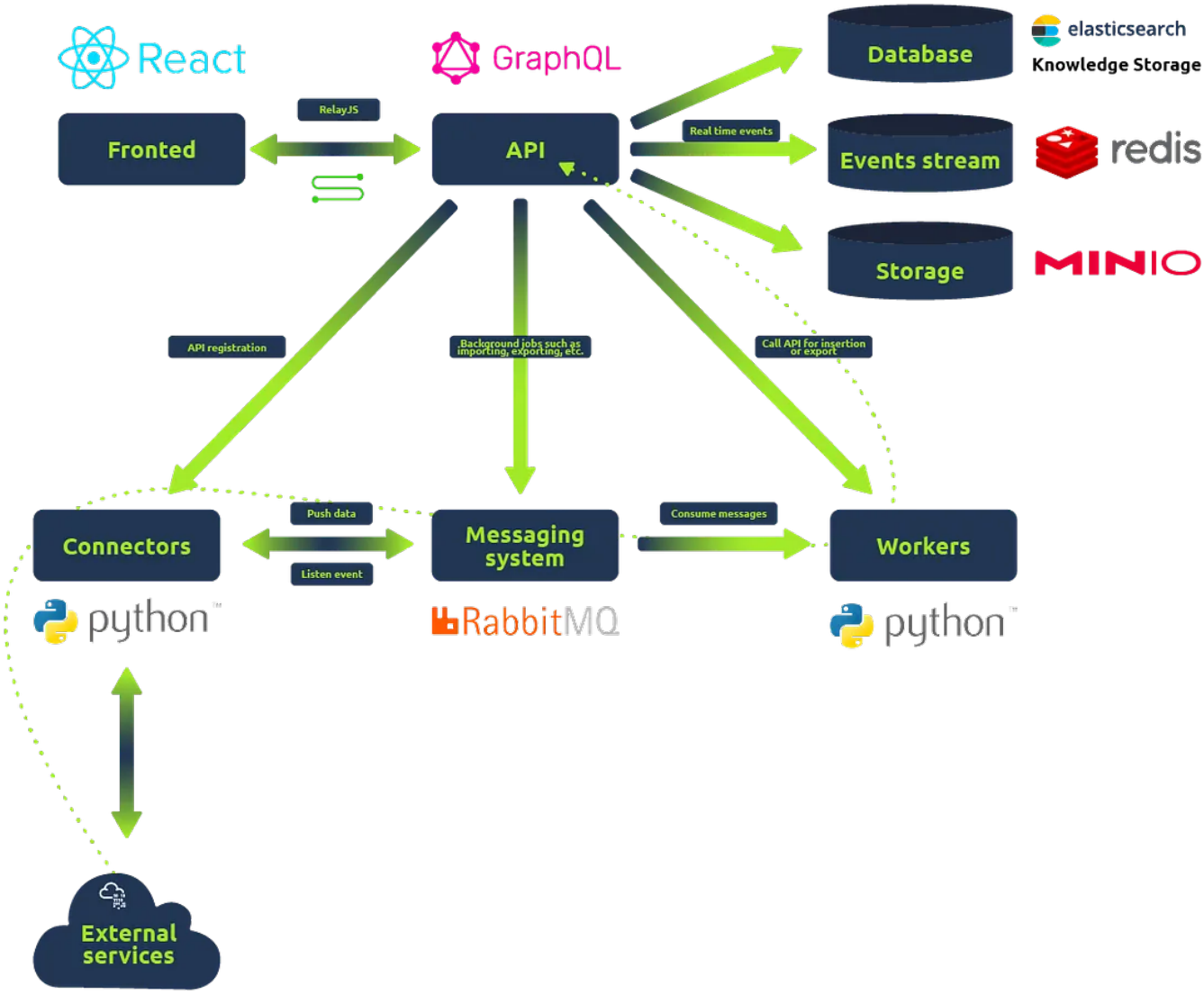


OpenCTI Data Model

OpenCTI uses a variety of knowledge schemas in structuring data, the main one being the Structured Threat Information Expression (STIX2) standards. STIX is a serialised and standardised language format used in threat intelligence exchange. It

allows for the data to be implemented as entities and relationships, effectively tracing the origin of the provided information.

This data model is supported by how the platform's architecture has been laid out. The image below gives an architectural structure for your know-how.



Source: OpenCTI Public Knowledge Base

The highlight services include:

- **GraphQL API:** The API connects clients to the database and the messaging system.
- **Write workers:** Python processes utilised to write queries asynchronously from

the RabbitMQ messaging system.

- **Connectors:** Another set of Python processes used to ingest, enrich or export data on the platform. These connectors provide the application with a robust network of integrated systems and frameworks to create threat intelligence relations and allow users to improve their defence tactics.

According to OpenCTI, connectors fall under the following classes:

Class: **External Input Connector** *Description:* Ingests information from external sources *Examples:* CVE, MISP, TheHive, MITRE
Class: **Stream Connector** *Description:* Consumes platform data stream Examples: History, Tanium
Class: **Internal Enrichment Connector** *Description:* Takes in new OpenCTI entities from user requests *Examples:* Observables enrichment
Class: **Internal Import File Connector** *Description:* Extracts information from uploaded reports *Examples:* PDFs, STIX2 Import
Class: **Internal Export File Connector** *Description:* Exports information from OpenCTI into different file formats *Examples:* CSV, STIX2 export, PDF

OpenCTI Dashboard

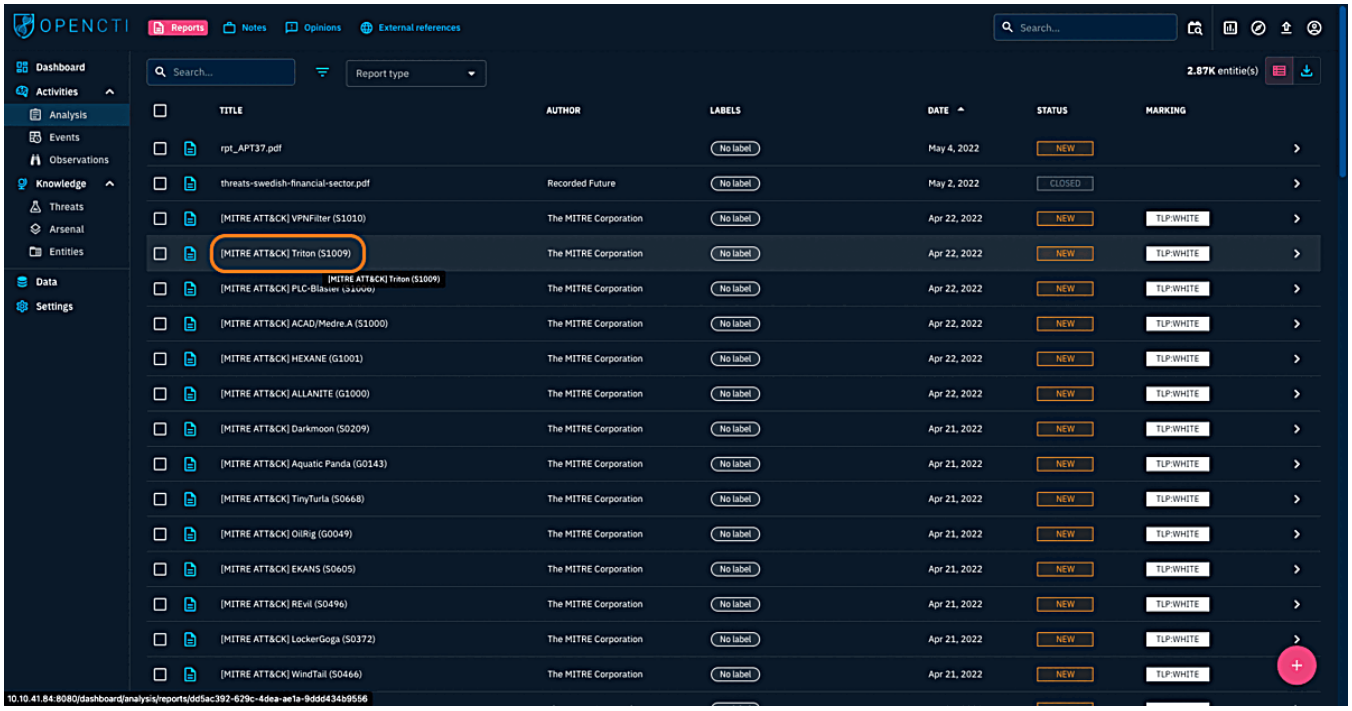
Once connected to the platform, the opening dashboard showcases various visual widgets summarizing the threat data ingested into OpenCTI. Widgets on the dashboard showcase the current state of entities ingested on the platform via the total number of entities, relationships, reports and observables ingested, and changes to these properties noted within 24 hours.

Activities & Knowledge

The OpenCTI categorises and presents entities under the **Activities and Knowledge** groups on the left-side panel. The activities section covers security incidents ingested onto the platform in the form of reports. It makes it easy for analysts to investigate these incidents. In contrast, the Knowledge section provides linked data related to the tools adversaries use, targeted victims and the type of threat actors and campaigns used.

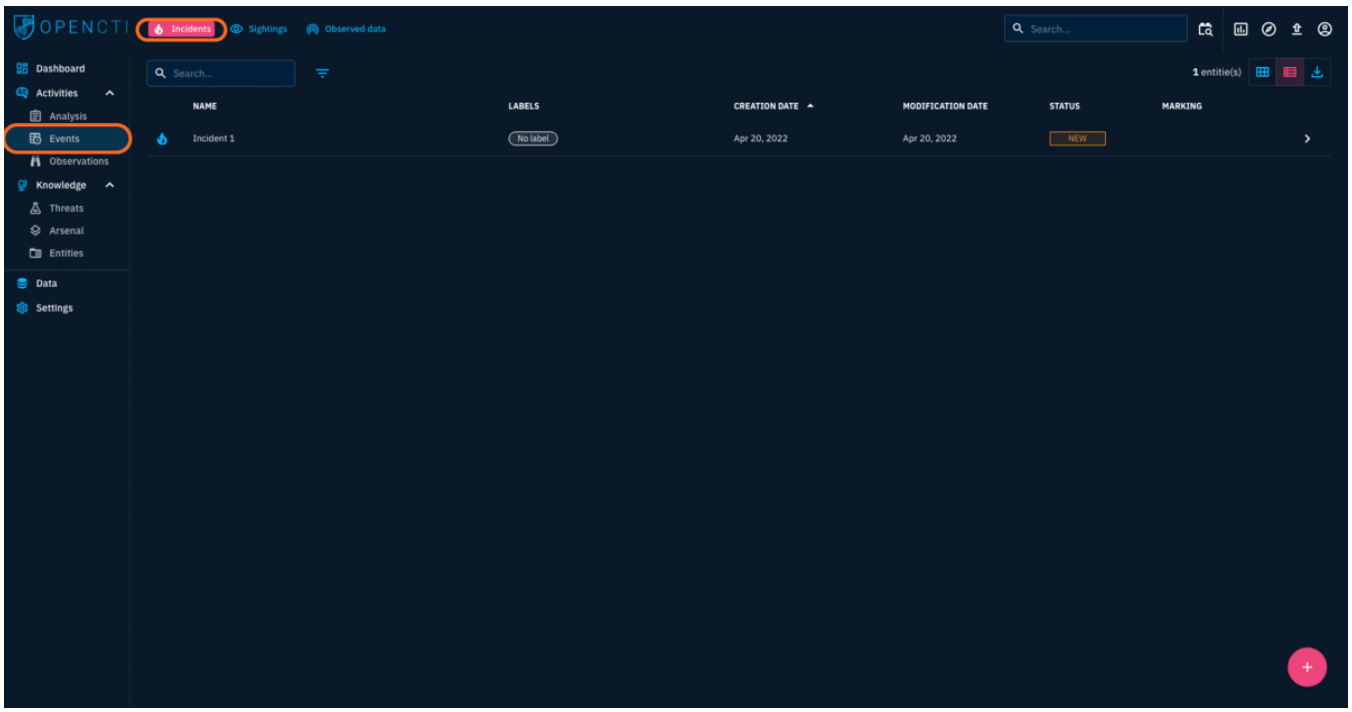
Analysis

The Analysis tab contains the input entities in reports analysed and associated external references. Reports are central to OpenCTI as knowledge on threats and events are extracted and processed. They allow for easier identification of the source of information by analysts. Additionally, analysts can add their investigation notes and other external resources for knowledge enrichment. As displayed below, we can look at the **Triton** Software report published by MITRE ATT&CK and observe or add to the details provided.



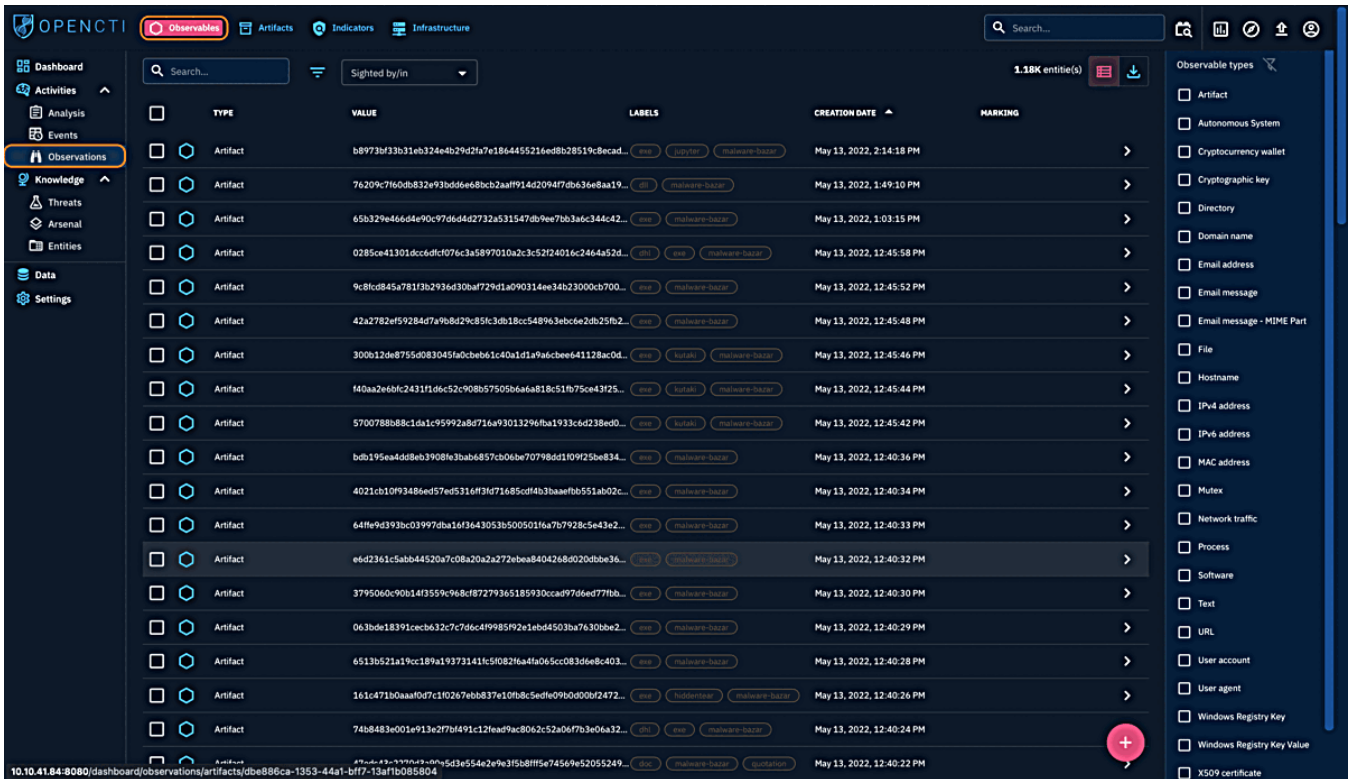
Events

Security analysts investigate and hunt for events involving suspicious and malicious activities across their organizational network. Within the Events tab, analysts can record their findings and enrich their threat intel by creating associations for their incidents.



Observations

Technical elements, detection rules and artefacts identified during a cyber attack are listed under this tab: one or several identifiable makeup indicators. These elements assist analysts in mapping out threat events during a hunt and perform correlations between what they observe in their environments against the intel feeds.

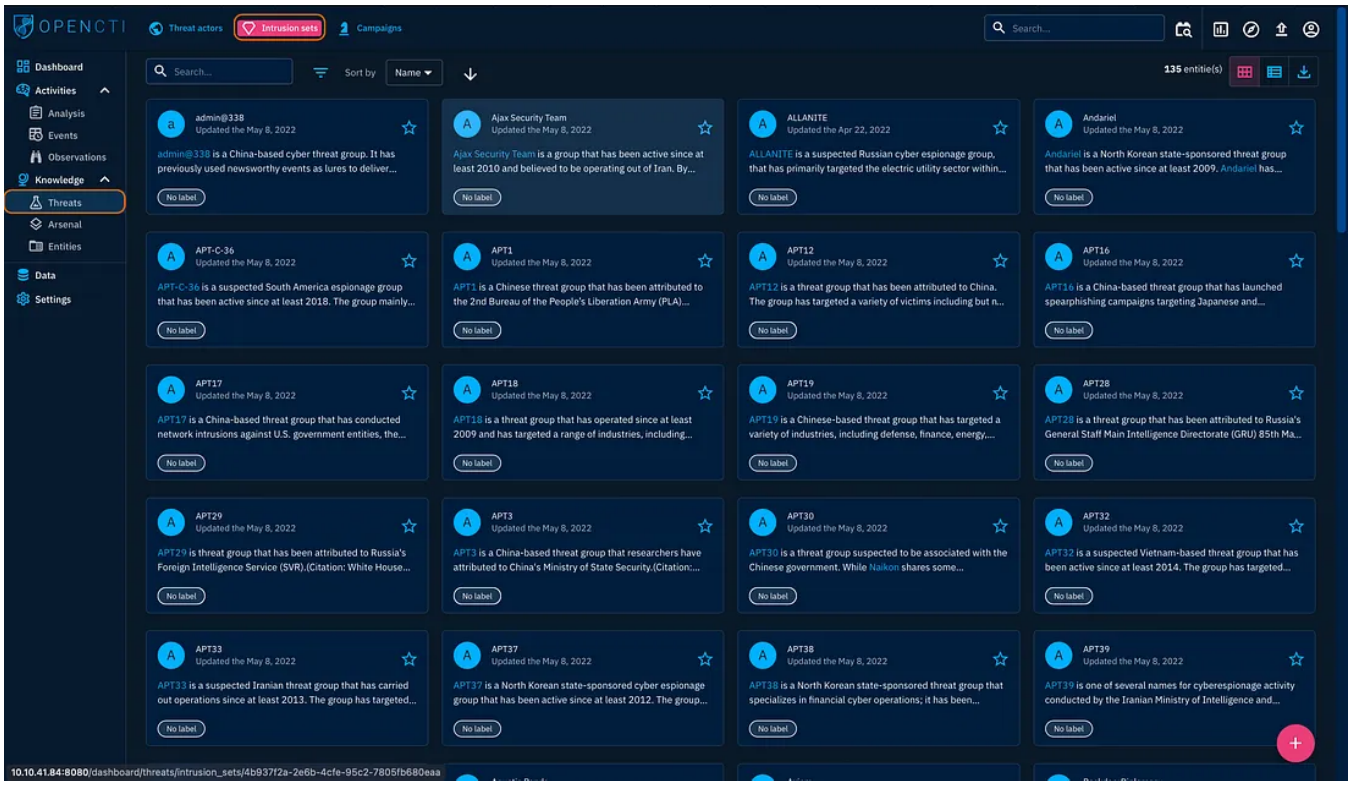


Threats

All information classified as threatening to an organisation or information would be classified under threats. These will include:

- **Threat Actors:** An individual or group of attackers seeking to propagate malicious actions against a target.
- **Intrusion Sets:** An array of TTPs, tools, malware and infrastructure used by a threat actor against targets who share some attributes. APTs and threat groups are listed under this category on the platform due to their known pattern of actions.
- **Campaigns:** Series of attacks taking place within a given period and against

specific victims initiated by advanced persistent threat actors who employ various TTPs. Campaigns usually have specified objectives and are orchestrated by threat actors from a nation-state, crime syndicate or other disreputable organization.



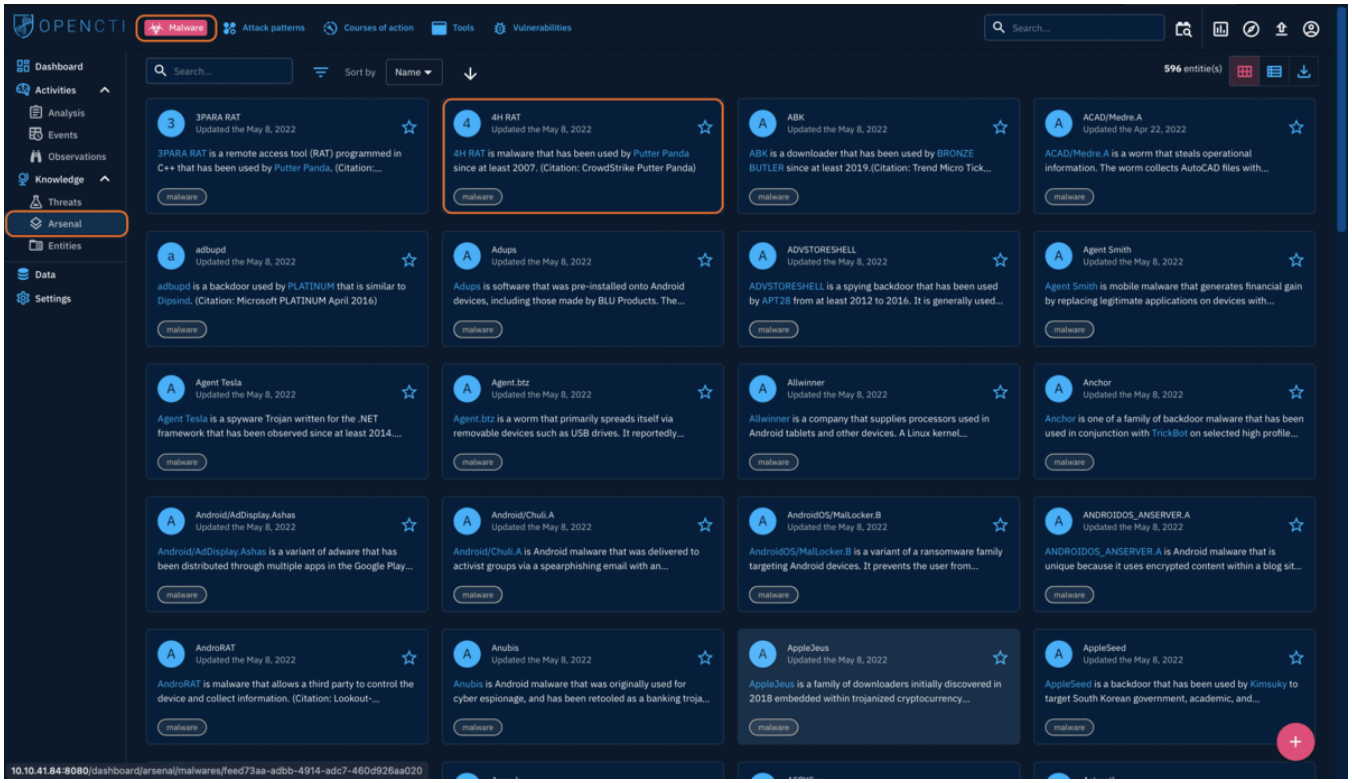
Arsenal

This tab lists all items related to an attack and any legitimate tools identified from the entities.

- **Malware:** Known and active malware and trojan are listed with details of their identification and mapping based on the knowledge ingested into the platform. In our example, we analyse the **4H RAT** malware and we can extract information and associations made about the malware.

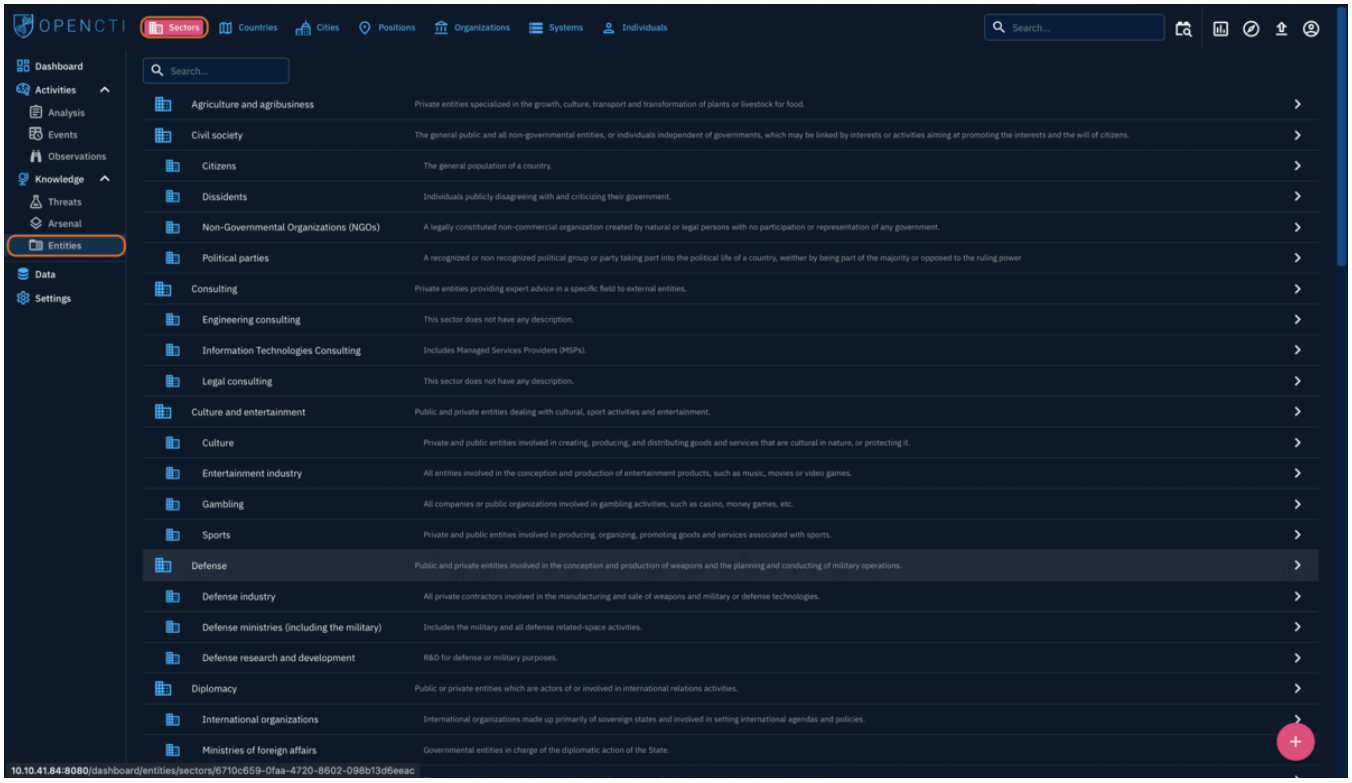
- **Attack Patterns:** Adversaries implement and use different TTPs to target, compromise, and achieve their objectives. Here, we can look at the details of the **Command-Line Interface and make decisions based on the relationships established on the platform and navigate through an investigation associated with the technique.**

- **Courses of Action:** MITRE maps out concepts and technologies that can be used to prevent an attack technique from being employed successfully. These are represented as Courses of Action (CoA) against the TTPs.
- **Tools:** Lists all legitimate tools and services developed for network maintenance, monitoring and management. Adversaries may also use these tools to achieve their objectives. For example, for the Command-Line Interface attack pattern, it is possible to narrow down that **CMD** would be used as an execution tool. As an analyst, one can investigate reports and instances associated with the use of the tool.
- **Vulnerabilities:** Known software bugs, system weaknesses and exposures are listed to provide enrichment for what attackers may use to exploit and gain access to systems. The Common Vulnerabilities and Exposures (CVE) list maintained by MITRE is used and imported via a connector.



Entities

This tab categorises all entities based on operational sectors, countries, organisations and individuals. This information allows for knowledge enrichment on attacks, organizations or intrusion sets.



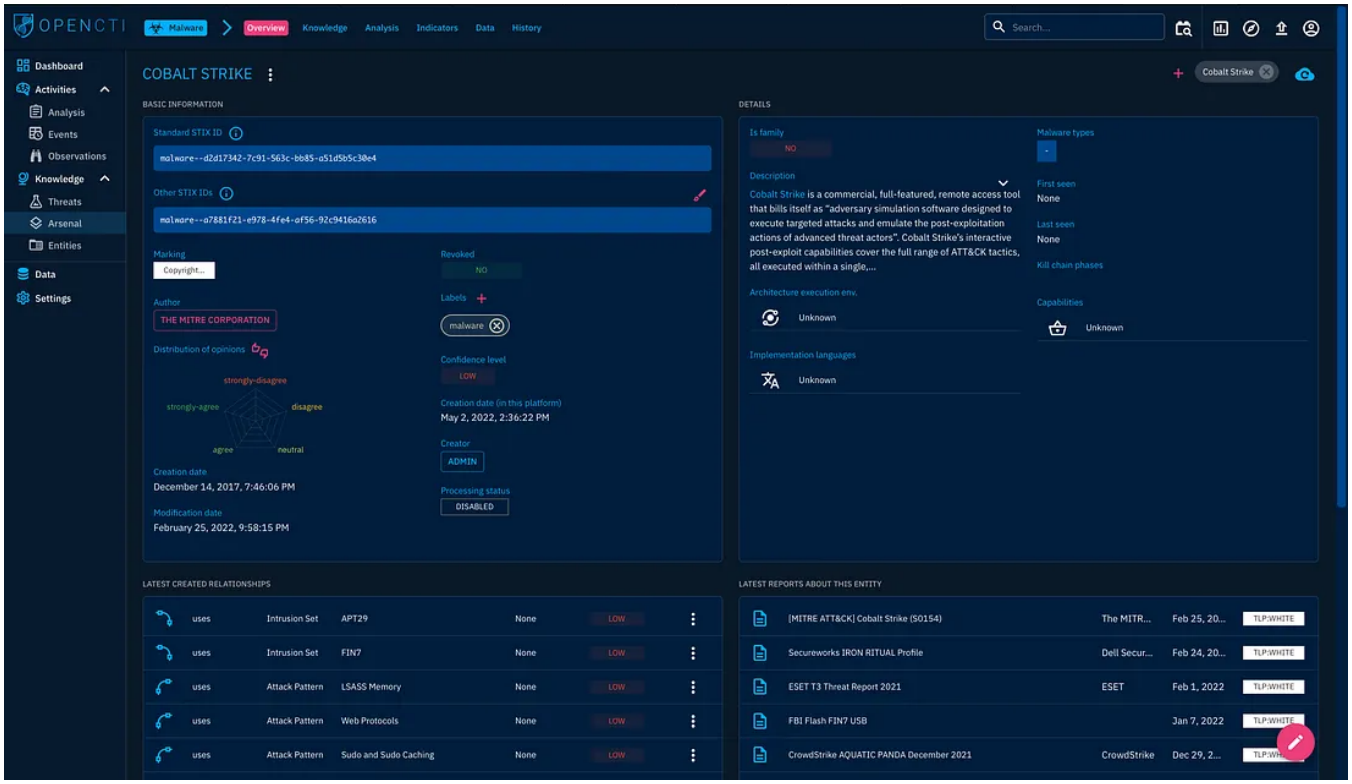
> *Q: What is the name of the group that uses the **4H RAT** malware?*
>
> *A: Putter Panda*
>
> *Q: What kill-chain phase is linked with the **Command-Line Interface** Attack Pattern?*
>
> *A: execution-ics*
>
> *Q: Within the Activities category, which tab would house the **Indicators**?*
>
> *A: Observations*

General Tabs Navigation

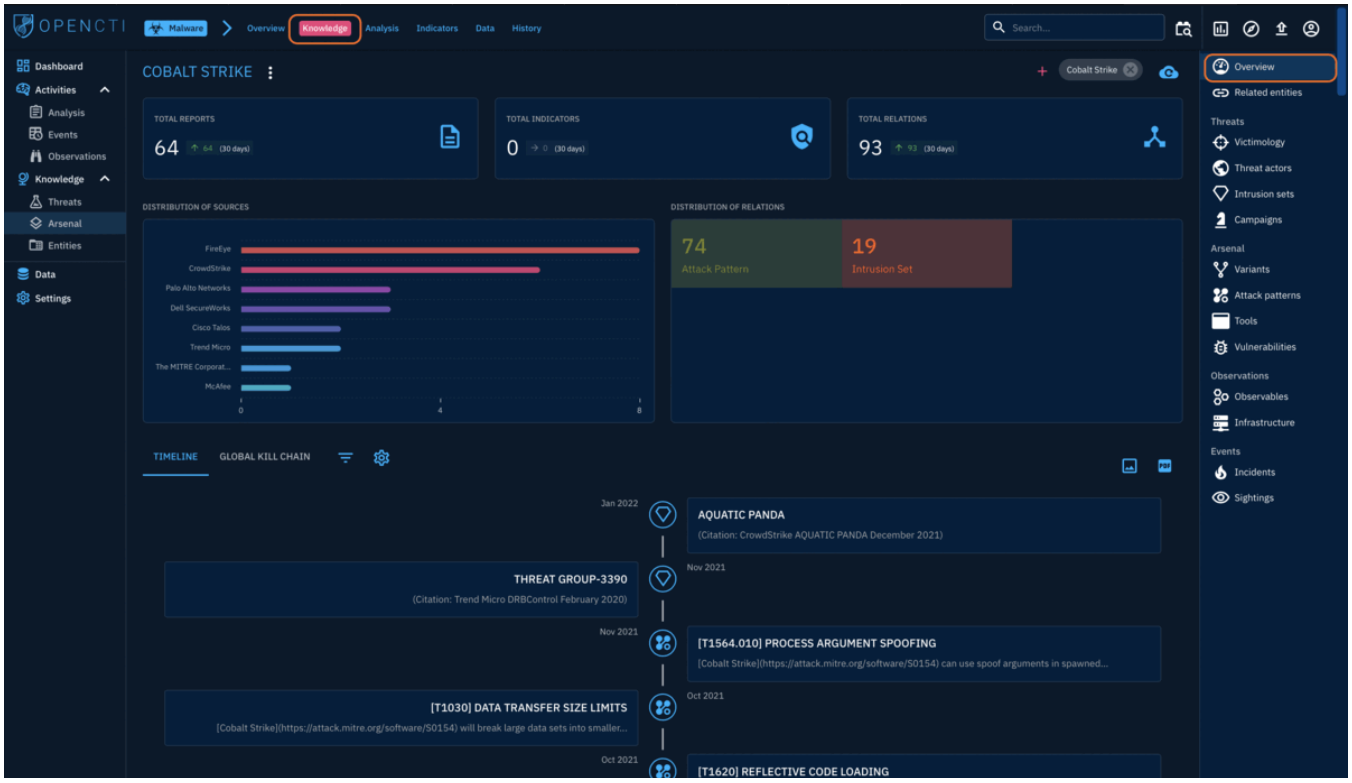
The day-to-day usage of OpenCTI would involve navigating through different entities within the platform to understand and utilize the information for any threat analysis. We will be looking at the **Cobalt Strike** malware entity for our walkthrough, mainly found under the Arsenal tab we've covered previously. When you select an intelligence entity, the details are presented to the user through:

- **Overview Tab:** Provides the general information about an entity being analysed

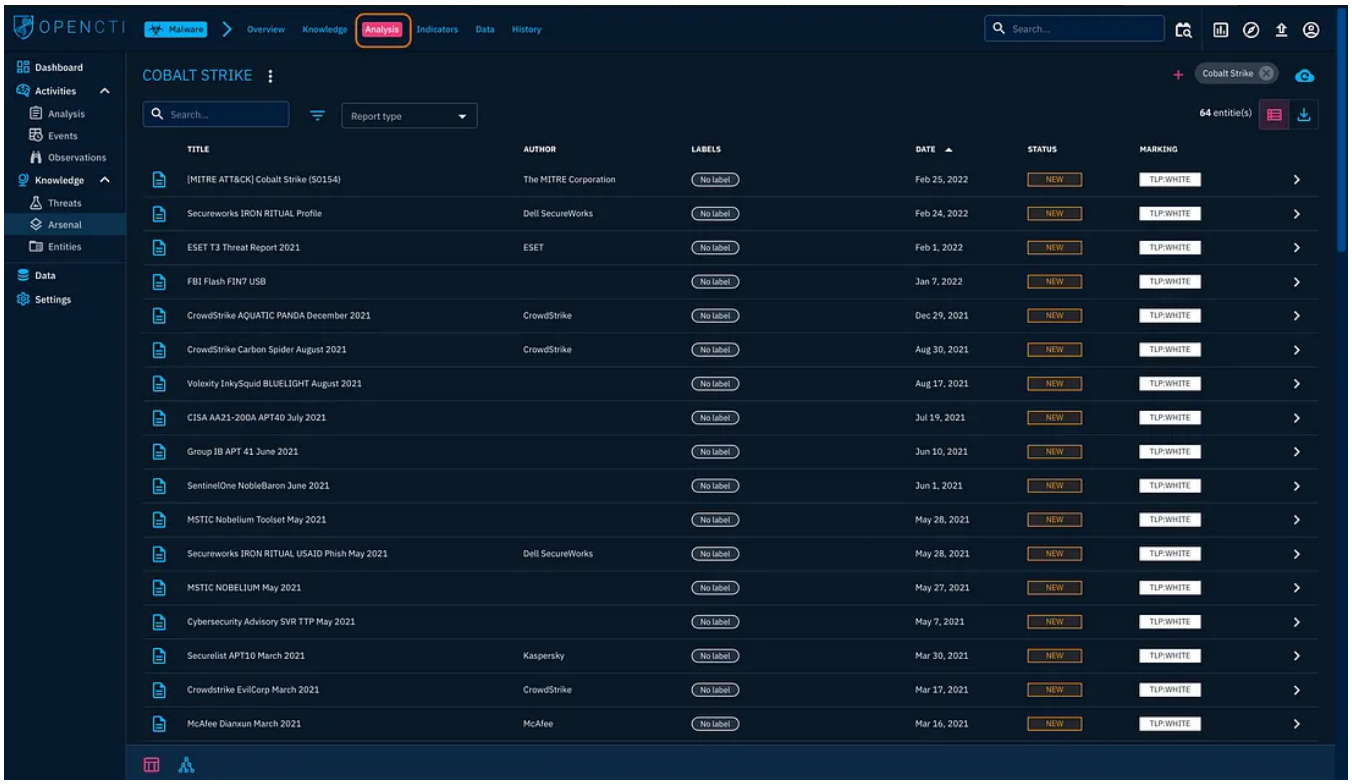
and investigated. In our case, the dashboard will present you with the entity ID, confidence level, description, relations created based on threats, intrusion sets and attack patterns, reports mentioning the entity and any external references.



- **Knowledge Tab:** Presents linked information associated with the entity selected. This tab will include the associated reports, indicators, relations and attack pattern timeline of the entity. Additionally, an analyst can view fine-tuned details from the tabs on the right-hand pane, where information about the threats, attack vectors, events and observables used within the entity are presented.



- **Analysis Tab:** Provides the reports where the identified entry has been seen. The analysis provides usable information about a threat and guides investigation tasks.



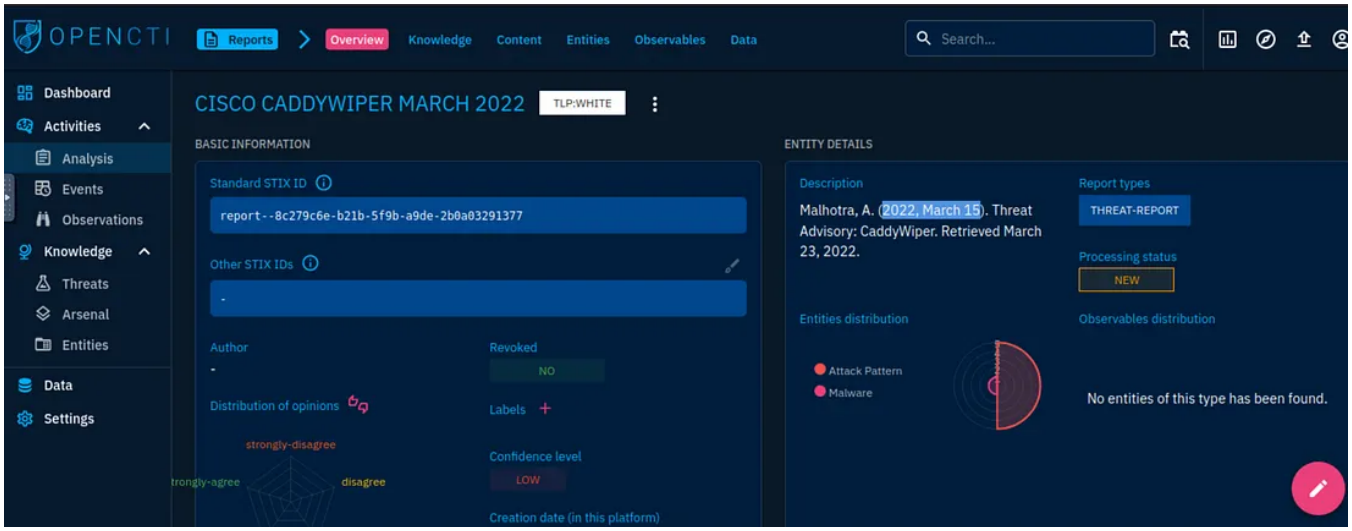
- **Indicators Tab:** Provides information on IOC identified for all the threats and entities.
- **Data Tab:** Contains the files uploaded or generated for export that are related to the entity. These assist in communicating information about threats being investigated in either technical or non-technical formats.
- **History Tab:** Changes made to the element, attributes, and relations are tracked by the platform worker and this tab will outline the changes.

> *Q: What Intrusion sets are associated with the Cobalt Strike malware with a Good confidence level? (Intrusion1, Intrusion2)*
>
> *A: CopyKittens, FIN7*
>
> *Q: Who is the author of the entity?*
>
> *A: The MITRE Corporation*

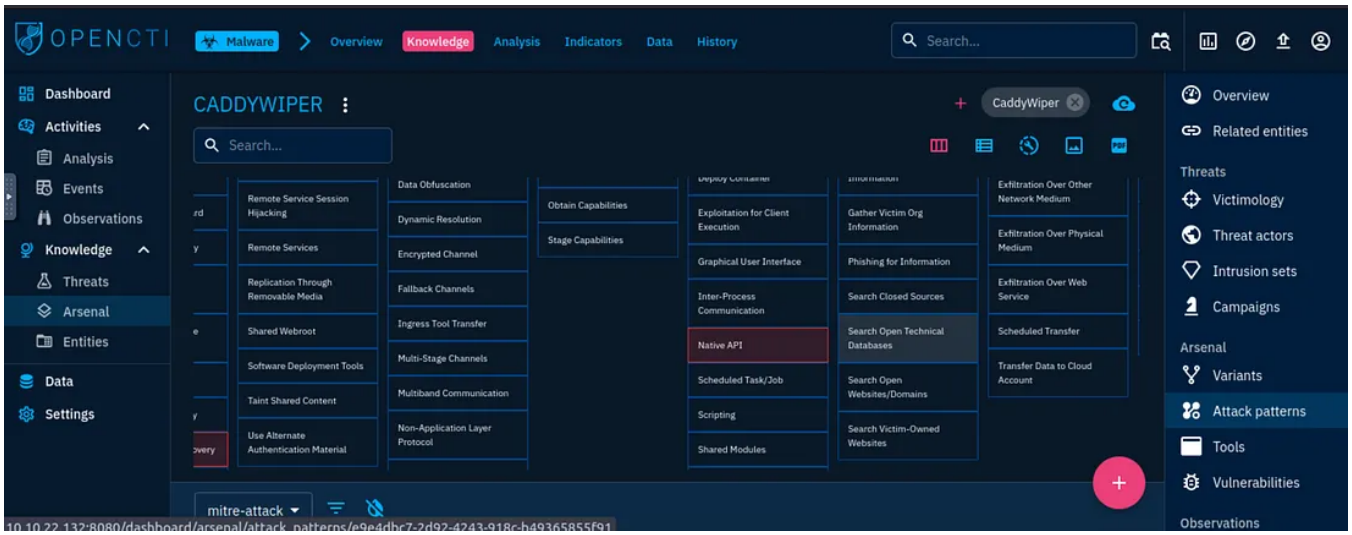
As a SOC analyst, you have been tasked with investigations on malware and APT groups rampaging through the world. Your assignment is to look into the **CaddyWiper** malware and **APT37** group. Gather information from OpenCTI to answer the following questions.

Answer the questions below

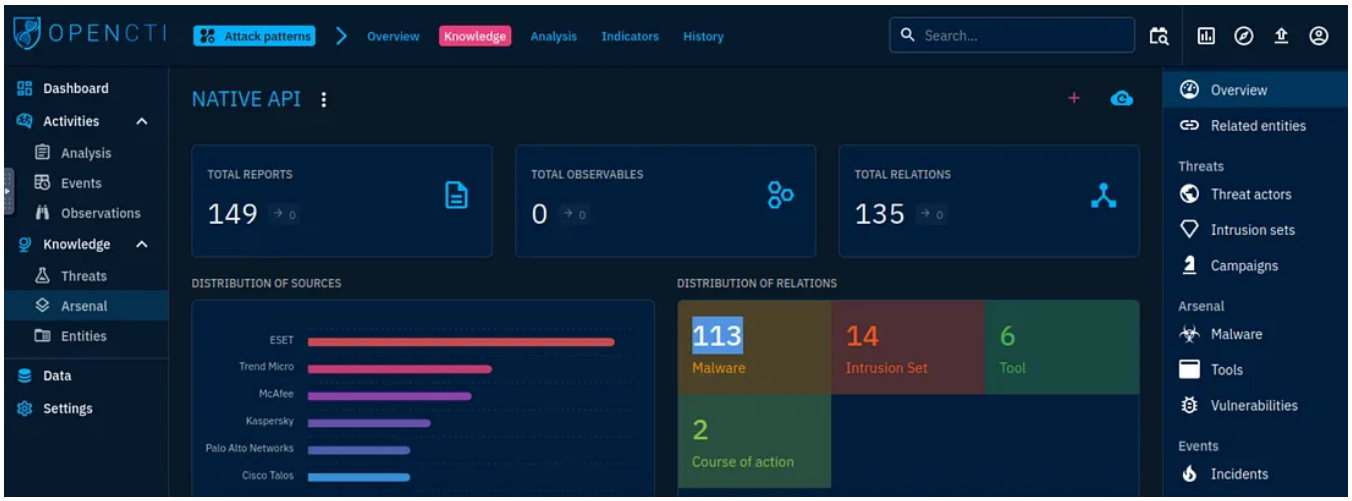
> *Q: What is the earliest date recorded related to CaddyWiper? Format: YYYY/MM/DD*



> *A: 2022/03/15*
>
> *Q: Which **Attack technique** is used by the malware for execution?*

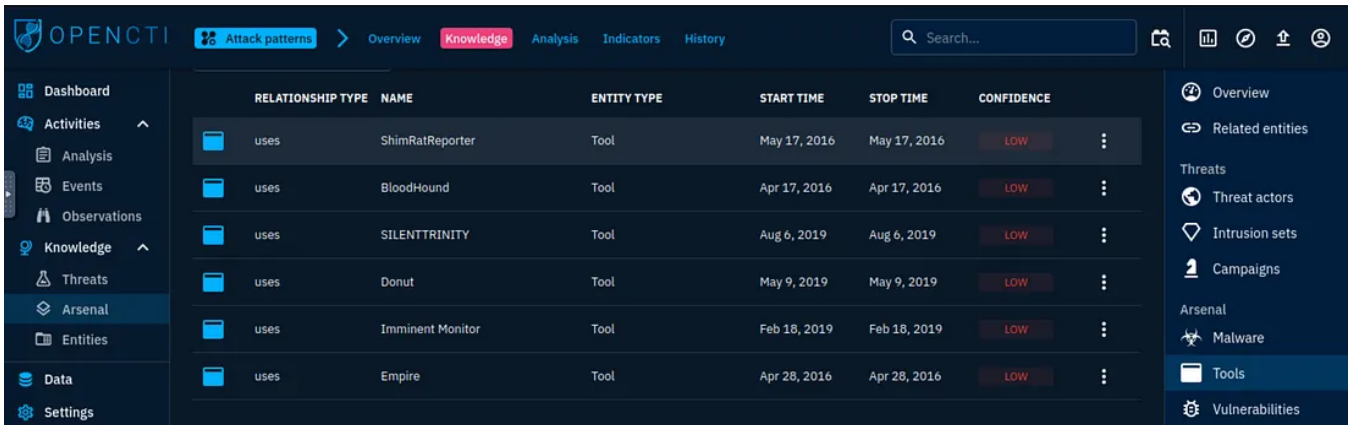


> *A: Native API*
>
> *Q: How many malware relations are linked to this Attack technique?*



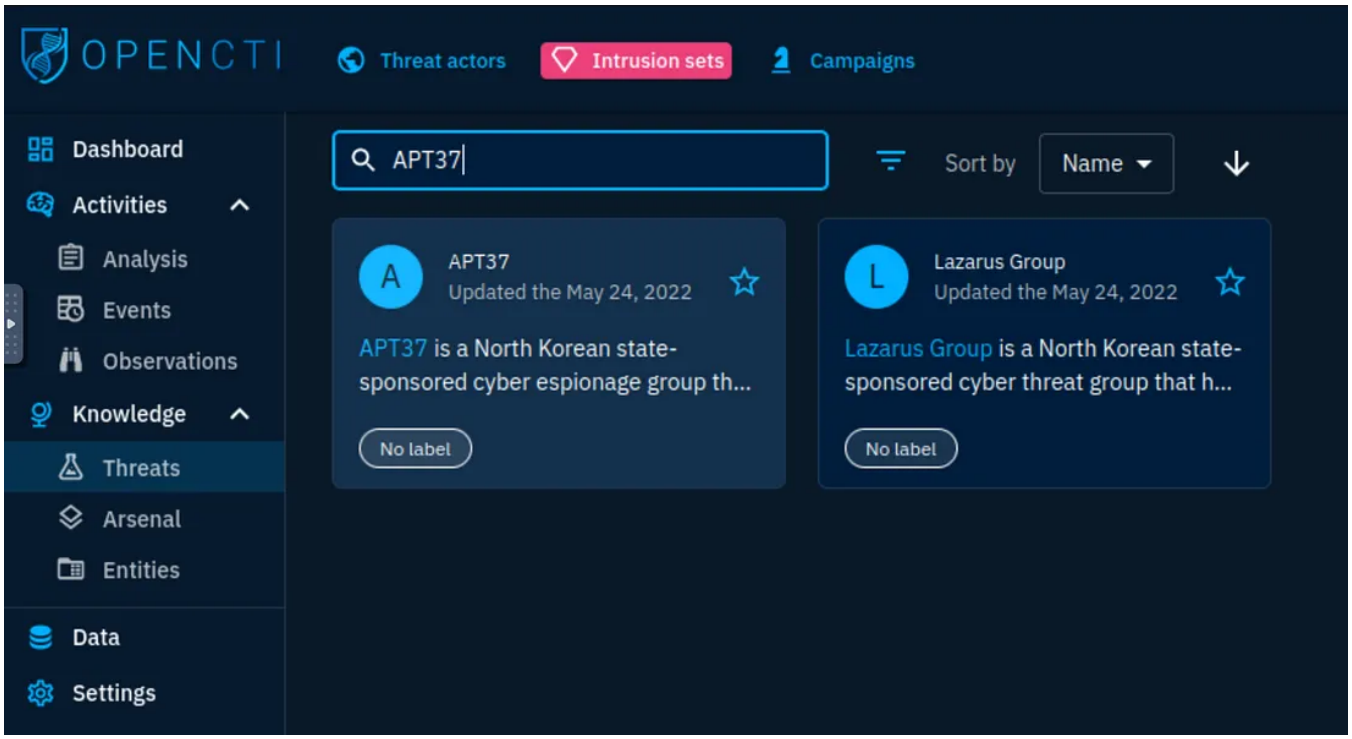
A: 113

Q: Which 3 tools were used by the Attack Technique in 2016? (Ans: Tool1, Tool2, Tool3)

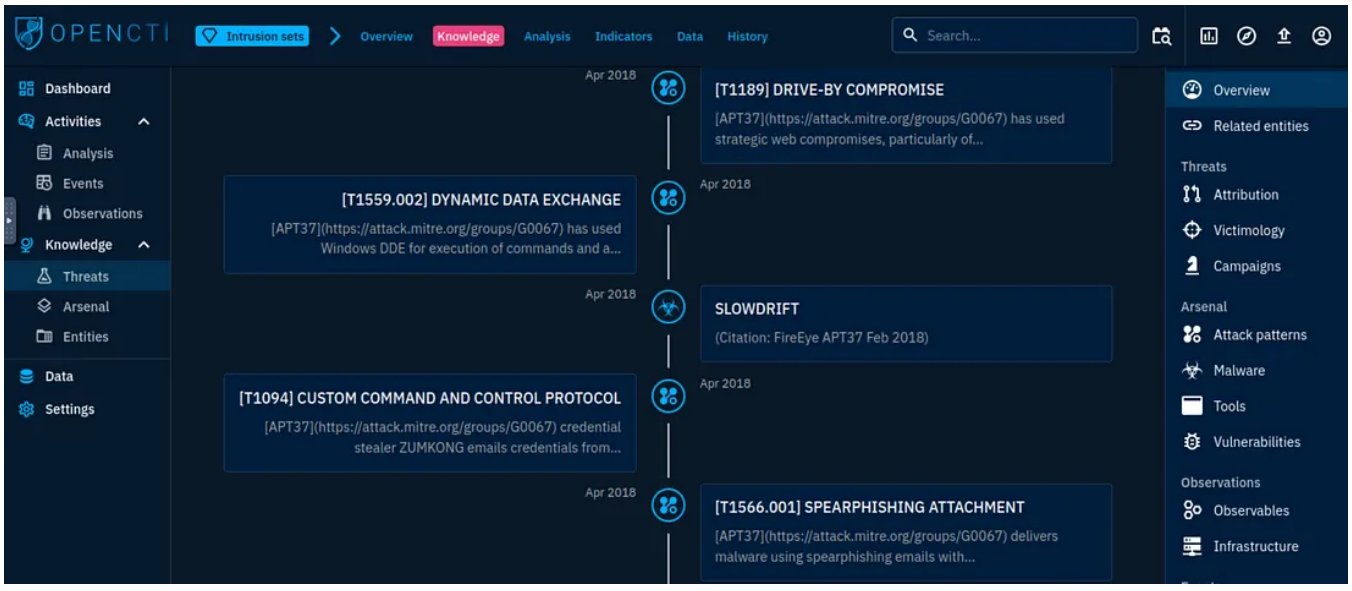


A: ShimRatReporter, Empire, Bloodhound

Q: What country is APT37 associated with?



> *A: North Korea*
>
> *Q: Which Attack techniques are used by the group for initial access? (Ans: Technique1, Technique2)*



> *A: T1189, T1566*

Fantastic work on going through and completing the OpenCTI room.

In this room, we looked at the use of the OpenCTI platform when it comes to processing threat intel and assisting analysts in investigating incidents.

Cybersecurity Tryhackme Soc Opencti Blue Team

Follow

Written by Kryptologyst

61 followers · 9 following

Cybersecurity & Privacy Professional | AI Enthusiast

Responses (1)

Itsjustme

ViraSecurity
Sep 3

ShimRatReporter, Empire, Bloodhound

in THM BloodHound, Empire, ShimRatReporter

More from Kryptologyst

Kryptologyst

Hide your public IP address in Kali

Public IP is unique and assigned to a device, while a private IP is assigned to devices within a private space.

Feb 13, 2023 1

Kryptologyst

Nmap Basic Port Scans

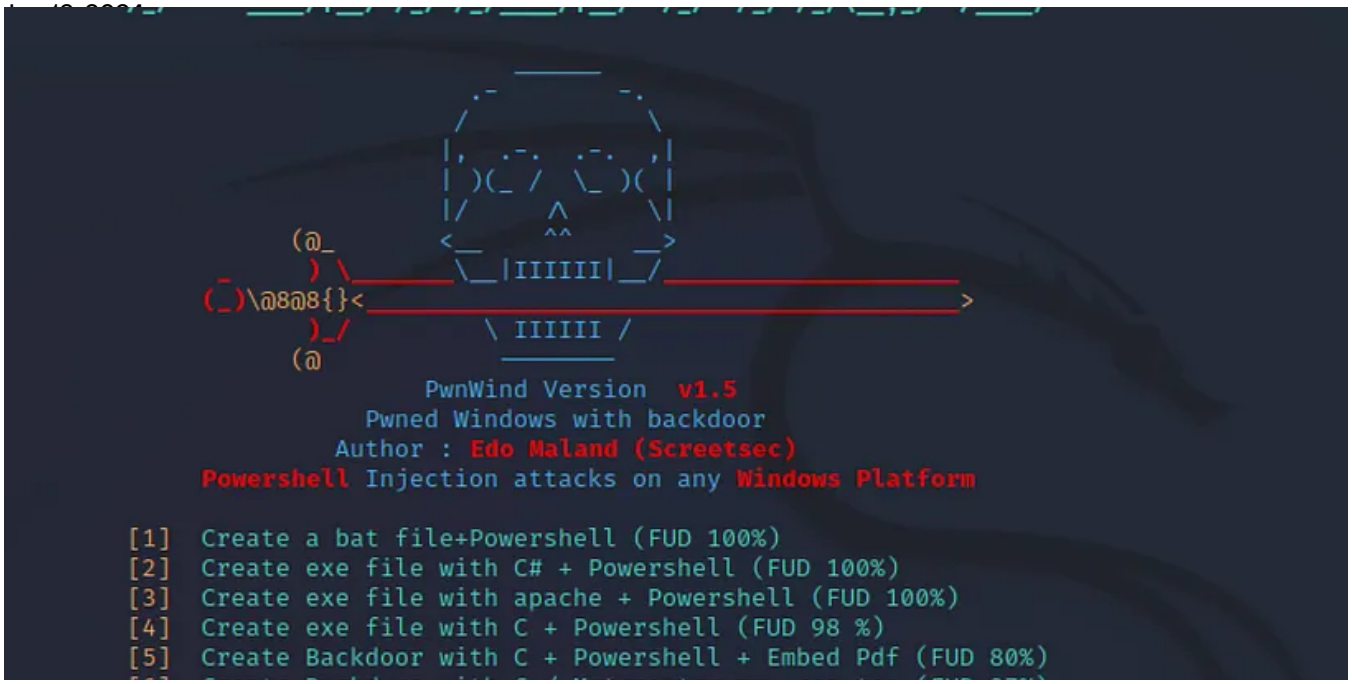
Learn in-depth how nmap TCP connect scan, TCP SYN port scan, and UDP port scan work.

Feb 8, 2023 21 1

Kryptologyst

Post-exploitation frameworks.

Summary In this article, we will talk about frameworks that help exploit vulnerabilities, establish persistence, and advance within the...



Kryptologyst

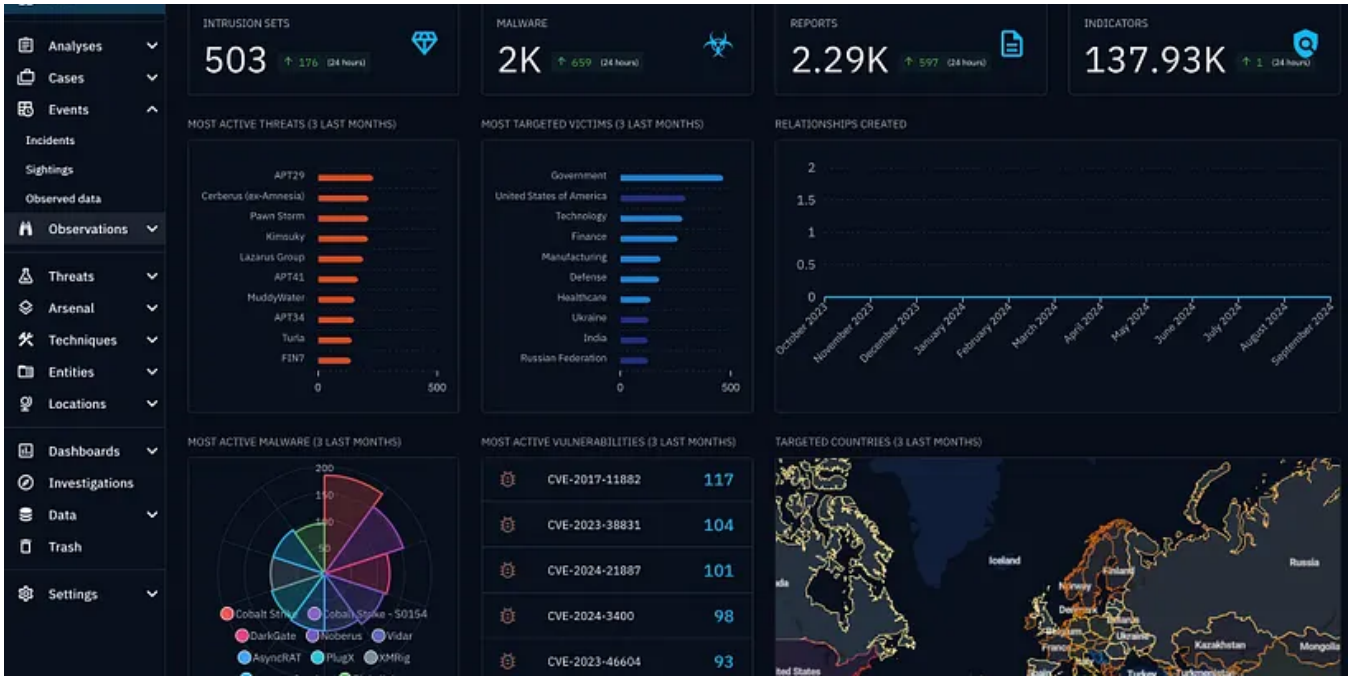
Payload Creation [TheFatRat]

TheFatRat a massive exploiting tool: Easy tool to generate backdoor and easy tool to post exploitation attack like browser attack and etc ...

Oct 23, 2022 50

See all from Kryptologyst

Recommended from Medium



In InfoSec Write-ups by Vito Rallo (CRIMSON7)

TI for fun, or more: a more serious OpenCTI 💡

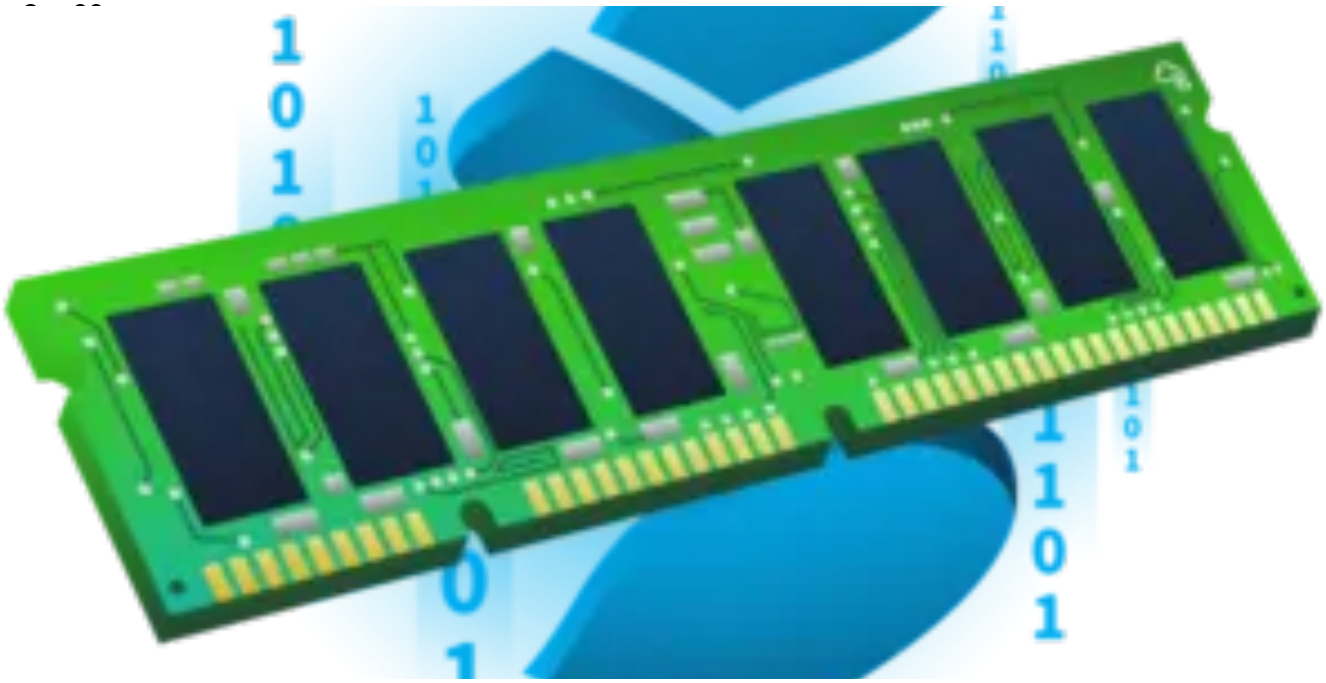
Build your own CTI by deploying OpenCTI—seriously, and on a budget

Jun 21 25

MAGESH

Linux Threat Detection 1 -Tryhackme

Explore how attackers break into Linux systems and how you can detect this in logs



Francesco Pastore

THM - Supplemental Memory

A writeup for the room “Supplemental Memory” on TryHackMe

Jun 23

In System Weakness by Visir

Linux Threat Detection 1: TryHackMe Walkthrough for SOC Analysts & Forensics Learners

Discover how to identify SSH attacks and analyze Linux logs using the grep command.

Sep 25 110 1

In T3CH by Ansul Kotadia

Windows Threat Detection 1: TryHackMe Answers

Explore common Initial Access methods on Windows and learn how to detect them.

Jul 10 100

Sle3pyHead 👩‍💻

XDR: Operation Global Dagger CTF Notes | TryHackMe

Investigated Incident 49 in MS Defender XDR CTF.

Sep 30 5

See more recommendations