

[Open in app](#)

Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)



OpenCTI TryHackMe Walkthrough

8 min read · Dec 15, 2023



Kryptologyst



OPENCTI

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

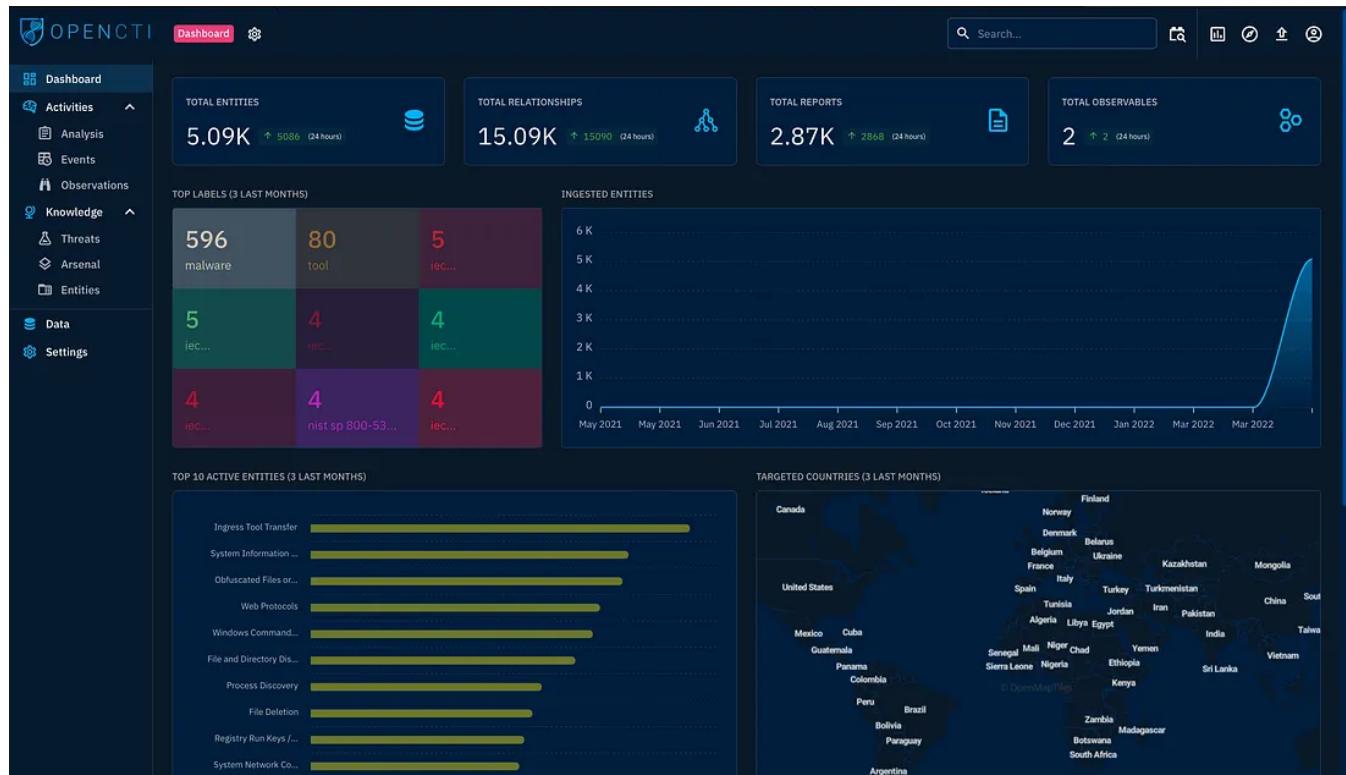
juggernaut that is Threat Intelligence.

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.

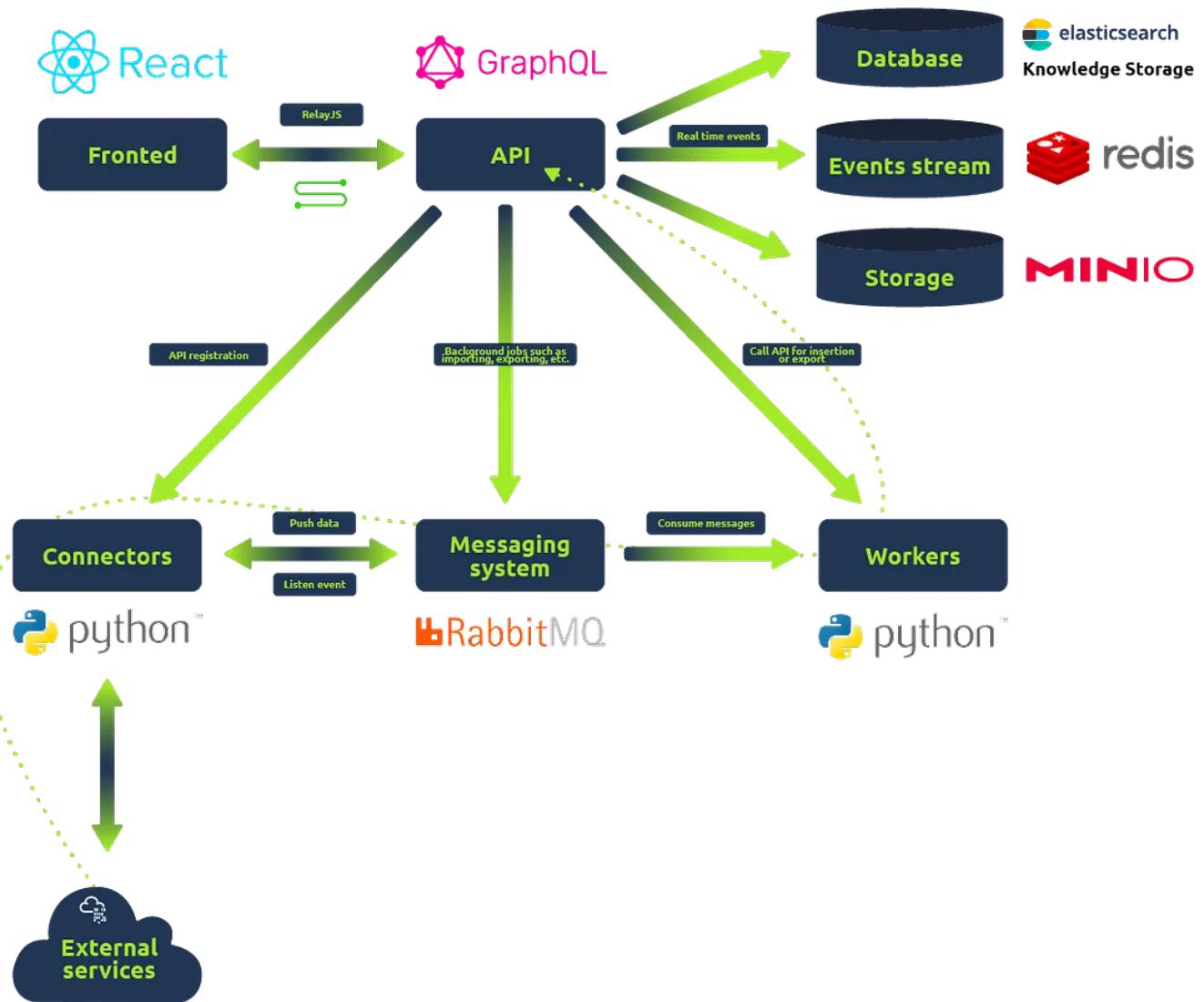


OpenCTI Data Model

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

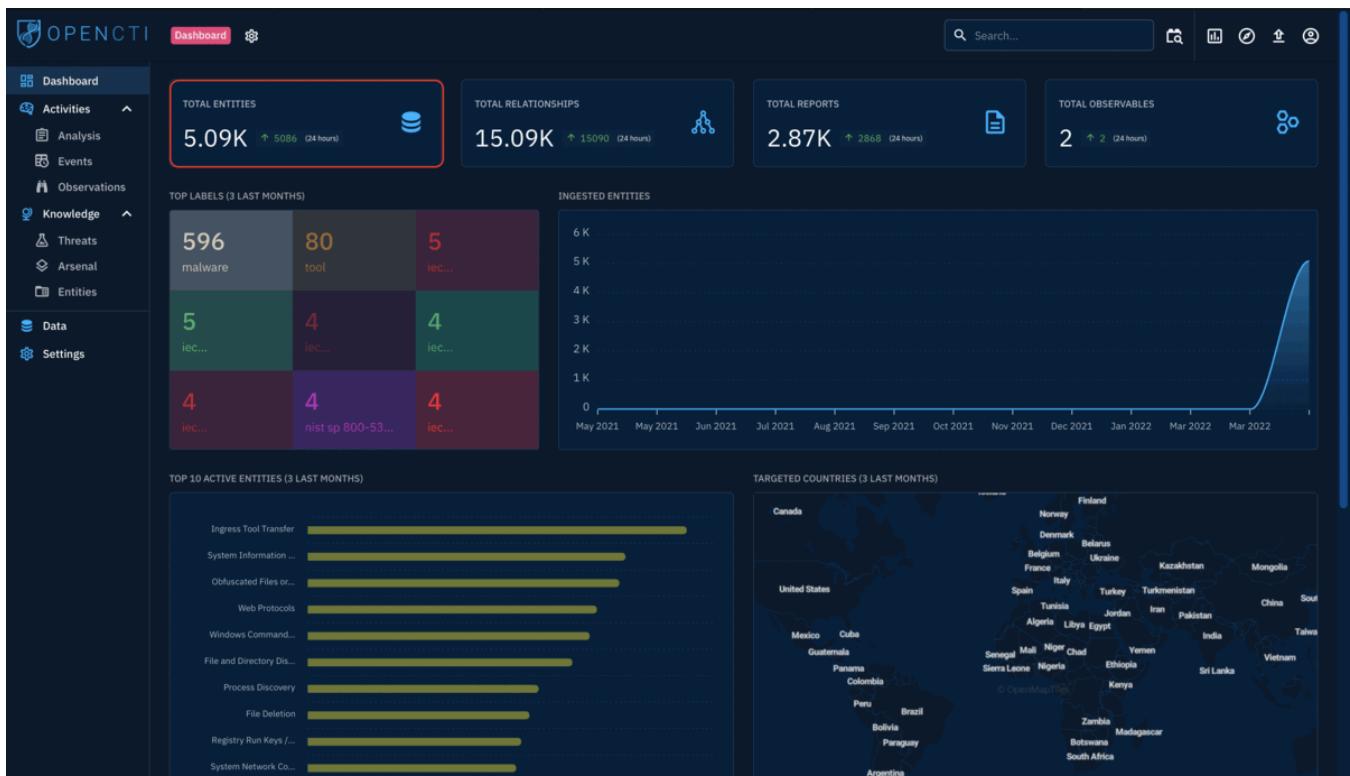
Class: Internal Enrichment Connector *Description:* Takes in new OpenCTI entities from user requests *Examples:* Observables enrichment

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.

The screenshot shows the OpenCTI Analysis dashboard. On the left, there's a sidebar with navigation links: Dashboard, Activities (which is selected), Analysis, Events, Observations, Knowledge, Threats, Arsenal, Entities, Data, and Settings. The main area displays a table of reports. The columns are: TITLE, AUTHOR, LABELS, DATE, STATUS, and MARKING. A search bar and a report type dropdown are at the top. A pink circle with a plus sign is in the bottom right corner.

TITLE	AUTHOR	LABELS	DATE	STATUS	MARKING
rpt_APT37.pdf	Recorded Future	No label	May 4, 2022	NEW	
threats-swedish-financial-sector.pdf	The MITRE Corporation	No label	May 2, 2022	CLOSED	
[MITRE ATT&CK] VPNFilter (S1010)	The MITRE Corporation	No label	Apr 22, 2022	NEW	TLP:WHITE
[MITRE ATT&CK] Triton (S1009)	The MITRE Corporation	No label	Apr 22, 2022	NEW	TLP:WHITE
[MITRE ATT&CK] PLC-Blaen (S1000)	The MITRE Corporation	No label	Apr 22, 2022	NEW	TLP:WHITE
[MITRE ATT&CK] ACAD/Medre.A (S1000)	The MITRE Corporation	No label	Apr 22, 2022	NEW	TLP:WHITE
[MITRE ATT&CK] HEXANE (G1001)	The MITRE Corporation	No label	Apr 22, 2022	NEW	TLP:WHITE
[MITRE ATT&CK] ALLANITE (G1000)	The MITRE Corporation	No label	Apr 22, 2022	NEW	TLP:WHITE
[MITRE ATT&CK] Darkmoon (S0209)	The MITRE Corporation	No label	Apr 21, 2022	NEW	TLP:WHITE
[MITRE ATT&CK] Aquatic Panda (G0143)	The MITRE Corporation	No label	Apr 21, 2022	NEW	TLP:WHITE
[MITRE ATT&CK] TinyTurla (S0668)	The MITRE Corporation	No label	Apr 21, 2022	NEW	TLP:WHITE
[MITRE ATT&CK] OilRig (G0049)	The MITRE Corporation	No label	Apr 21, 2022	NEW	TLP:WHITE
[MITRE ATT&CK] EKANS (S0605)	The MITRE Corporation	No label	Apr 21, 2022	NEW	TLP:WHITE
[MITRE ATT&CK] Revil (S0496)	The MITRE Corporation	No label	Apr 21, 2022	NEW	TLP:WHITE
[MITRE ATT&CK] LockerGoga (S0372)	The MITRE Corporation	No label	Apr 21, 2022	NEW	TLP:WHITE
[MITRE ATT&CK] WindTail (S0466)	The MITRE Corporation	No label	Apr 21, 2022	NEW	TLP:WHITE

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.

The screenshot shows the OpenCTI Events dashboard. The sidebar has the same navigation links as the Analysis dashboard. The main area displays a table of incidents. The columns are: NAME, LABELS, CREATION DATE, MODIFICATION DATE, STATUS, and MARKING. A search bar and a report type dropdown are at the top. A pink circle with a plus sign is in the bottom right corner.

NAME	LABELS	CREATION DATE	MODIFICATION DATE	STATUS	MARKING
Incident 1	No label	Apr 20, 2022	Apr 20, 2022	NEW	

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.

TYPE	VALUE	LABELS	CREATION DATE	MARKING
Artifact	b8f730f33b31eb324edc29d2f7e1b64455216ed8d28519c8cad...	... malware-bazar	May 13, 2022, 2:14:18 PM	
Artifact	76209c760d0832e93bd6d6868bc2af914d20947db368aa19...	... malware-bazar	May 13, 2022, 1:49:10 PM	
Artifact	65b329e466d4e90c97dd4d2732a531547d9ee7bb3a6c344c42...	... malware-bazar	May 13, 2022, 1:03:15 PM	
Artifact	0285ce41301dcc6dfcf076c3a5897010a2c3c52f24016c2464a52d...	... malware-bazar	May 13, 2022, 12:45:58 PM	
Artifact	9c8fc0d845a781f2b936d30ba729d1a090314ee34b23000cb700...	... malware-bazar	May 13, 2022, 12:45:52 PM	
Artifact	42a2782ef9284d7a9b8d29c85f3db18cc548963ebc6e2db25fb2...	... malware-bazar	May 13, 2022, 12:45:48 PM	
Artifact	300b12de0755d083045fa0cbe61c40a1d1a9a6cbee641128ac0d...	... malware-bazar	May 13, 2022, 12:45:46 PM	
Artifact	f40aa2e6bf2431f1d6c52c908b57505b6a6818c51fb75ce43f25...	... malware-bazar	May 13, 2022, 12:45:44 PM	
Artifact	5700788b88c1da1c95992a8d716a93013296fba1933c6d238ed0...	... malware-bazar	May 13, 2022, 12:45:42 PM	
Artifact	bdb195ea4d8e03908e3uba6857cb06be70798dd10f925be834...	... malware-bazar	May 13, 2022, 12:40:36 PM	
Artifact	4021c10f9348ed57ed5316f3f71685cdfb3baaefb551ab02c...	... malware-bazar	May 13, 2022, 12:40:34 PM	
Artifact	64fe9d393bc03997dba16f3e43053b5005016a7b792c5e43e2...	... malware-bazar	May 13, 2022, 12:40:33 PM	
Artifact	e6d2361c5abb44520a7c08a20a2a272beaba8404268d020dbbe36...	... malware-bazar	May 13, 2022, 12:40:32 PM	
Artifact	3795060c90b14f3559c968cf87279365185930cad97d6ed77fb...	... malware-bazar	May 13, 2022, 12:40:30 PM	
Artifact	063bde18391cecd632c7cd6c4f9985f92e1ebd4503b7630bbe2...	... malware-bazar	May 13, 2022, 12:40:29 PM	
Artifact	651b521a19cc189a19373141fc5f082f6a4fa065cc083d8c8403...	... malware-bazar	May 13, 2022, 12:40:28 PM	
Artifact	161c471b0aaa0d7c10267ebb837e10fb8c6fde09b0d000f2472...	... malware-bazar	May 13, 2022, 12:40:26 PM	
Artifact	74b8483e001e913e2f7b491c12ead9ac8062c52a06f7b3e06a32...	... malware-bazar	May 13, 2022, 12:40:24 PM	

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.

The screenshot shows the OpenCTI platform interface. The left sidebar has tabs for Dashboard, Activities, Events, Observations, Knowledge, Threats, and the currently selected 'Arsenal'. The main area is a grid of cards, each representing a malware entity. The first card in the grid is highlighted with an orange border. The cards contain the following information:

Name	Category	Last Updated	Description
3PARA RAT	malware	Updated the May 8, 2022	3PARA RAT is a remote access tool (RAT) programmed in C++ that has been used by Putter Panda. (Citation: CrowdStrike Putte...
4H RAT	malware	Updated the May 8, 2022	4H RAT is malware that has been used by Putter Panda since at least 2007. (Citation: CrowdStrike Putte...
ABK	malware	Updated the May 8, 2022	ABK is a downloader that has been used by BRONZE BUTLER since at least 2019. (Citation: Trend Micro Tick...
ACAD/Medre.A	malware	Updated the Apr 22, 2022	ACAD/Medre.A is a worm that steals operational information. The worm collects AutoCAD files with...
adbupd	malware	Updated the May 8, 2022	adbupd is a backdoor used by PLATINUM that is similar to Dipsoid. (Citation: Microsoft PLATINUM April 2016)
Adups	malware	Updated the May 8, 2022	Adups is software that was pre-installed onto Android devices, including those made by BLU Products. The...
ADVSTORESHELL	malware	Updated the May 8, 2022	ADVSTORESHELL is a spying backdoor that has been used by APT28 from at least 2012 to 2016. It is generally used...
Agent Smith	malware	Updated the May 8, 2022	Agent Smith is mobile malware that generates financial gain by replacing legitimate applications on devices with...
Agent Tesla	malware	Updated the May 8, 2022	Agent Tesla is a spyware Trojan written for the .NET framework that has been observed since at least 2014....
Agent.btz	malware	Updated the May 8, 2022	Agent.btz is a worm that primarily spreads itself via removable devices such as USB drives. It reportedly...
Allwinner	malware	Updated the May 8, 2022	Allwinner is a company that supplies processors used in Android tablets and other devices. A Linux kernel...
Anchor	malware	Updated the May 8, 2022	Anchor is one of a family of backdoor malware that has been used in conjunction with TrickBot on selected high-profile...
Android/AdDisplay.Ashas	malware	Updated the May 8, 2022	Android/AdDisplay.Ashas is a variant of adware that has been distributed through multiple apps in the Google Play...
Android/Chuli.A	malware	Updated the May 8, 2022	Android/Chuli.A is Android malware that was delivered to activist groups via a spearphishing email with an...
AndroidOS/MalLocker.B	malware	Updated the May 8, 2022	AndroidOS/MalLocker.B is a variant of a ransomware family targeting Android devices. It prevents the user from...
ANDROIDOS_ANSERVER.A	malware	Updated the May 8, 2022	ANDROIDOS_ANSERVER.A is Android malware that is unique because it uses encrypted content within a blog sit...
AndroRAT	malware	Updated the May 8, 2022	AndroRAT is malware that allows a third party to control the device and collect information. (Citation: Lookout:...
Anubis	malware	Updated the May 8, 2022	Anubis is Android malware that was originally used for cyber espionage, and has been retooled as a banking troja...
AppleJeus	malware	Updated the May 8, 2022	AppleJeus is a family of downloaders initially discovered in 2018 embedded within trojanized cryptocurrency...
AppleSeed	malware	Updated the May 8, 2022	AppleSeed is a backdoor that has been used by Kimsuky to target South Korean government, academic, and...

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.

The screenshot shows the OpenCTI web application. The left sidebar has a navigation menu with tabs: Dashboard, Activities, Analysis, Events, Observations, Knowledge, Threats, Arsenal, and Entities (which is selected and highlighted with an orange border). The main content area is titled "Entities" and lists the following categories:

- Agriculture and agribusiness
- Civil society
- Citizens
- Dissidents
- Non-Governmental Organizations (NGOs)
- Political parties
- Consulting
- Engineering consulting
- Information Technologies Consulting
- Legal consulting
- Culture and entertainment
- Culture
- Entertainment industry
- Gambling
- Sports
- Defense
- Defense industry
- Defense ministries (including the military)
- Defense research and development
- Diplomacy
- International organizations
- Ministries of foreign affairs

Each entity type has a brief description and a right-pointing arrow icon to its right. At the bottom left of the main area, there is a URL: 10.10.41.84:8080/dashboard/entities/sectors/6710c659-0faa-4720-8602-098b13d6eeac.

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.

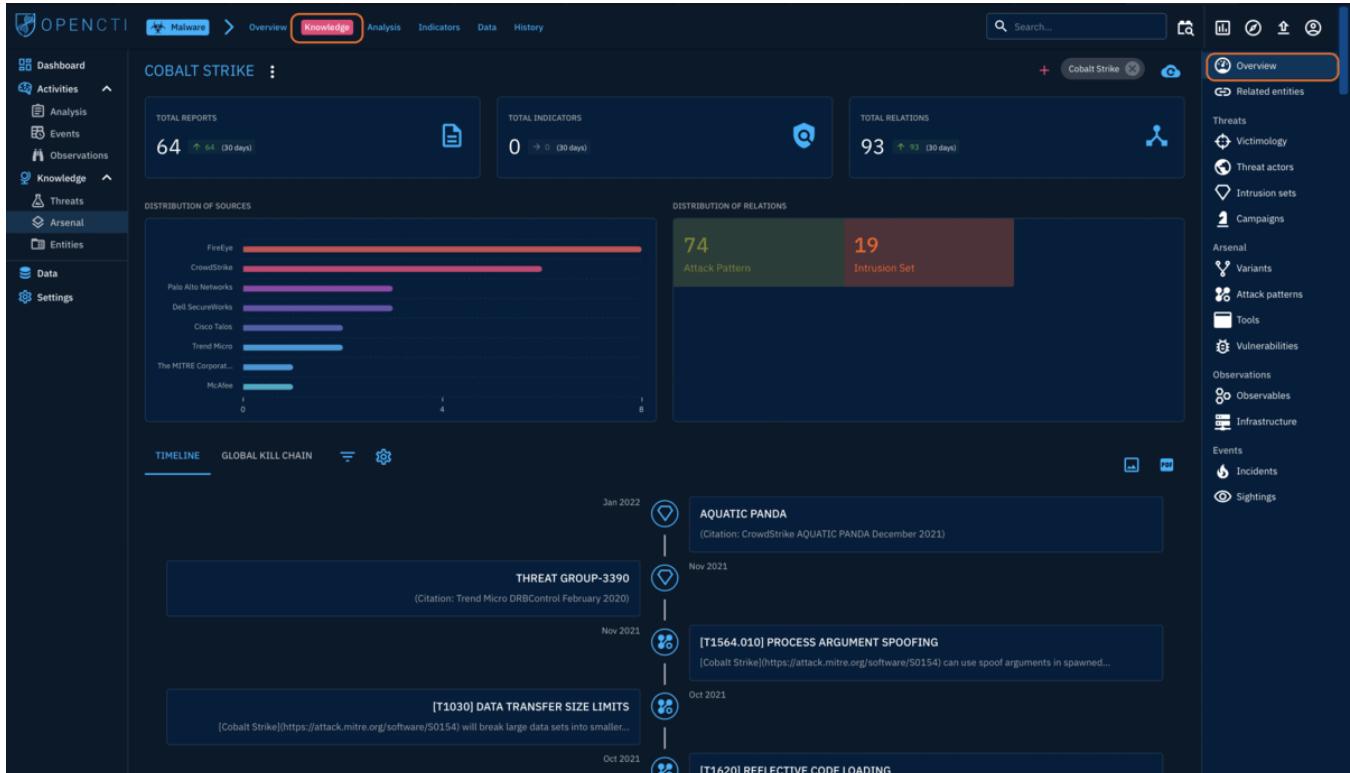
The screenshot shows the OpenCTI interface for the 'COBALT STRIKE' entity. The left sidebar includes tabs for Dashboard, Activities, Analysis, Events, Observations, Knowledge (selected), Threats, Arsenal, Entities, Data, and Settings. The main content area has tabs for Overview, Knowledge, Analysis, Indicators, Data, and History. The 'Overview' tab is selected, displaying the following information:

- BASIC INFORMATION**
 - Standard STIX ID: malware--d2d17342-7c91-563c-bb85-a51d5b5c38c4
 - Other STIX IDs: malware--a7881f21-e978-4fe4-af56-92c9416a2616
 - Marking: Copyright...
 - Author: THE MITRE CORPORATION
 - Distribution of opinions: A circular gauge showing distribution across strongly-disagree, disagree, neutral, agree, and strongly-agree.
 - Creation date: December 14, 2017, 7:46:06 PM
 - Modification date: February 25, 2022, 9:58:15 PM
- DETAILS**
 - Is family: NO
 - Description: Cobalt Strike is a commercial, full-featured, remote access tool that bills itself as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors". Cobalt Strike's interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single...
 - Malware types: -
 - First seen: None
 - Last seen: None
 - Kill chain phases: -
 - Architecture execution env.: Unknown
 - Capabilities: -
 - Implementation languages: Unknown
- LATEST CREATED RELATIONSHIPS**

	uses	Intrusion Set	APT29	None	LOW	⋮
1	uses	Intrusion Set	FIN7	None	LOW	⋮
2	uses	Attack Pattern	LSASS Memory	None	LOW	⋮
3	uses	Attack Pattern	Web Protocols	None	LOW	⋮
4	uses	Attack Pattern	Sudo and Sudo Caching	None	LOW	⋮
- LATEST REPORTS ABOUT THIS ENTITY**

	[MITRE ATT&CK] Cobalt Strike (S0154)	The MTR...	Feb 25, 20...	TLP:WHITE
1	Secureworks IRON RITUAL Profile	Dell Secur...	Feb 24, 20...	TLP:WHITE
2	ESET T3 Threat Report 2021	ESET	Feb 1, 2022	TLP:WHITE
3	FBI Flash FIN7 USB		Jan 7, 2022	TLP:WHITE
4	CrowdStrike AQUATIC PANDA December 2021	CrowdStrike	Dec 29, 20...	TLP:WHITE

- **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.

The screenshot shows the OpenCTI interface with the 'Analysis' tab selected. The main table lists 64 entities, each with a preview icon, title, author, labels, date, status, and marking. The columns are: TITLE, AUTHOR, LABELS, DATE, STATUS, and MARKING. The table includes entries such as '[MITRE ATT&CK] Cobalt Strike (S0154)', 'Secureworks IRON RITUAL Profile', 'ESET T3 Threat Report 2021', 'FBI Flash FIN7 USB', 'CrowdStrike AQUATIC PANDA December 2021', 'CrowdStrike Carbon Spider August 2021', 'Volcetix InkySquid BLUELIGHT August 2021', 'CISA AA21-200A APT40 July 2021', 'Group IB APT 41 June 2021', 'SentinelOne NobleBaron June 2021', 'MSTIC Nobelium Toolset May 2021', 'Secureworks IRON RITUAL USAID Phish May 2021', 'MSTIC NOBELIUM May 2021', 'Cybersecurity Advisory SVR TTP May 2021', 'Securelist APT10 March 2021', 'Crowdstrike EvilCorp March 2021', and 'McAfee Dianxun March 2021'.

- **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

The screenshot shows the OpenCTI interface for a Threat Advisory. The title is "CISCO CADDYWIPER MARCH 2022" with TLP:WHITE. The basic information includes a Standard STIX ID: report--8c279c6e-b21b-5f9b-a9de-2b0a03291377 and an Author field. The status is Revoked (NO). Distribution of opinions and Confidence level are shown. Entity details include a description of Malhotra, A. (2022, March 15). Threat Advisory: CaddyWiper. Retrieved March 23, 2022. Report types are Threat-Report. Processing status is NEW. Entities distribution shows no results for Attack Pattern or Malware. Observables distribution also shows no results.

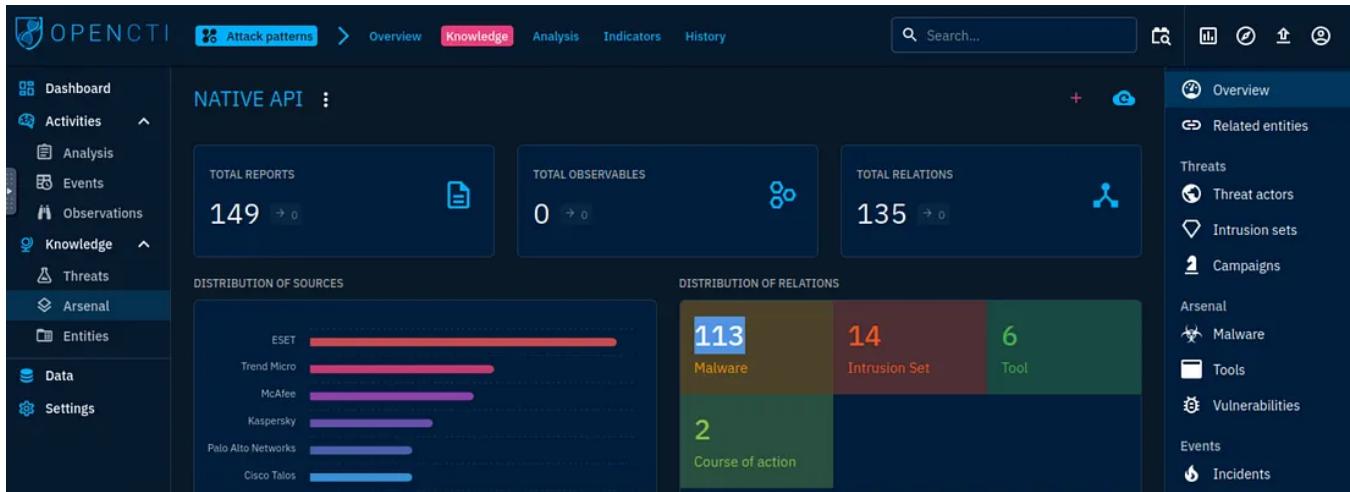
A: 2022/03/15

Q: Which *Attack technique* is used by the malware for execution?

The screenshot shows the OpenCTI interface for the Arsenal section under Knowledge. The search bar contains "CaddyWiper". The results list various attack patterns, with "Native API" highlighted. Other listed attack patterns include Remote Service Session Hijacking, Dynamic Resolution, Encrypted Channel, Fallback Channels, Ingress Tool Transfer, Multi-Stage Channels, Multiband Communication, Non-Application Layer Protocol, Data Obfuscation, Obtain Capabilities, Exploitation for Client Execution, Stage Capabilities, Graphical User Interface, Inter-Process Communication, Native API, Scheduled Task/Job, Scripting, Shared Modules, Gather Victim Org Information, Phishing for Information, Search Closed Sources, Search Open Technical Databases, Search Open Websites/Domains, Search Victim-Owned Websites, Exfiltration Over Other Network Medium, Exfiltration Over Physical Medium, Exfiltration Over Web Service, Scheduled Transfer, and Transfer Data to Cloud Account.

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)

RELATIONSHIP TYPE	NAME	ENTITY TYPE	START TIME	STOP TIME	CONFIDENCE	⋮
uses	ShimRatReporter	Tool	May 17, 2016	May 17, 2016	LOW	⋮
uses	BloodHound	Tool	Apr 17, 2016	Apr 17, 2016	LOW	⋮
uses	SILENTTRINITY	Tool	Aug 6, 2019	Aug 6, 2019	LOW	⋮
uses	Donut	Tool	May 9, 2019	May 9, 2019	LOW	⋮
uses	Imminent Monitor	Tool	Feb 18, 2019	Feb 18, 2019	LOW	⋮
uses	Empire	Tool	Apr 28, 2016	Apr 28, 2016	LOW	⋮

A: ShimRatReporter, Empire, Bloodhound

Q: What country is APT37 associated with?

The screenshot shows the OpenCTI web application. On the left is a sidebar with navigation links: Dashboard, Activities (Analysis, Events, Observations), Knowledge (Threats, Lazarus Group, No label), Arsenal, Entities, Data, and Settings. The main area has a search bar at the top with the query 'APT37'. Below it are two cards. The first card is for 'APT37' (A) and the second for 'Lazarus Group' (L). Both cards show the group's name, last update date (May 24, 2022), a brief description (APT37 is a North Korean state-sponsored cyber espionage group that...; Lazarus Group is a North Korean state-sponsored cyber threat group that...), and a 'No label' button.

A: North Korea

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

This screenshot shows a timeline of attack techniques used by APT37. The sidebar on the left is identical to the previous one. The main area displays four technique cards in a vertical timeline, all dated April 2018.
 1. [T1189] DRIVE-BY COMPROMISE: [APT37](https://attack.mitre.org/groups/G0067) has used strategic web compromises, particularly of...
 2. [T1559.002] DYNAMIC DATA EXCHANGE: [APT37](https://attack.mitre.org/groups/G0067) has used Windows DDE for execution of commands and a...
 3. SLOWDRIFT: (Citation: FireEye APT37 Feb 2018)
 4. [T1094] CUSTOM COMMAND AND CONTROL PROTOCOL: [APT37](https://attack.mitre.org/groups/G0067) credential stealer ZUMKONG emails credentials from...
 The right sidebar contains links to various sections like Overview, Related entities, Threats, Attribution, Victimology, Campaigns, Arsenal, Attack patterns, Malware, Tools, Vulnerabilities, Observations, Observables, and Infrastructure.

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.



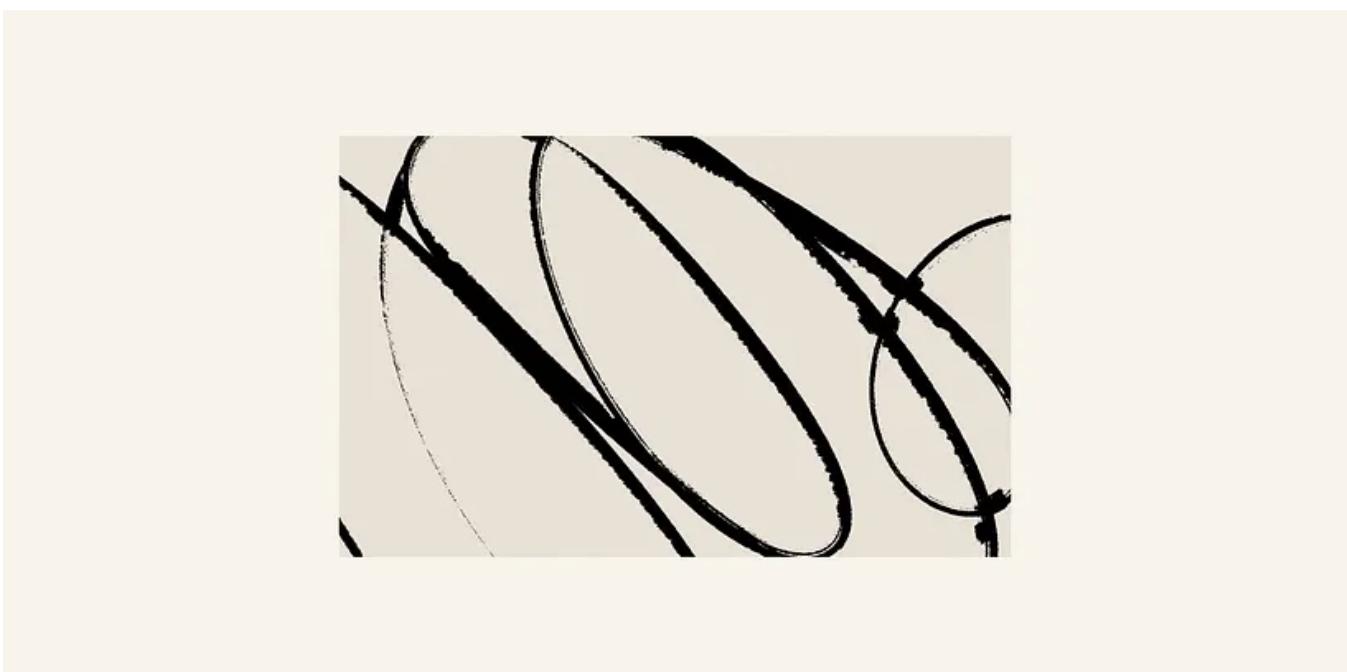
Nmap Basic Port Scans

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

Feb 8, 2023

21

1





Post-exploitation frameworks.

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

A screenshot of the PwnWind v1.5 interface. The interface has a dark background with white and red text. It features a large, stylized, abstract graphic at the top. Below it, the text "PwnWind Version v1.5" is displayed in red. Underneath, it says "Pwned Windows with backdoor" and "Author : Edo Maland (Streetsec)". It also mentions "Powershell Injection attacks on any Windows Platform". A list of five options follows: [1] Create a bat file+Powershell (FUD 100%), [2] Create exe file with C# + Powershell (FUD 100%), [3] Create exe file with apache + Powershell (FUD 100%), [4] Create exe file with C + Powershell (FUD 98 %), and [5] Create Backdoor with C + Powershell + Embed Pdf (FUD 80%).

```
PwnWind Version v1.5
Pwned Windows with backdoor
Author : Edo Maland (Streetsec)
Powershell Injection attacks on any Windows Platform

[1] Create a bat file+Powershell (FUD 100%)
[2] Create exe file with C# + Powershell (FUD 100%)
[3] Create exe file with apache + Powershell (FUD 100%)
[4] Create exe file with C + Powershell (FUD 98 %)
[5] Create Backdoor with C + Powershell + Embed Pdf (FUD 80%)
```



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

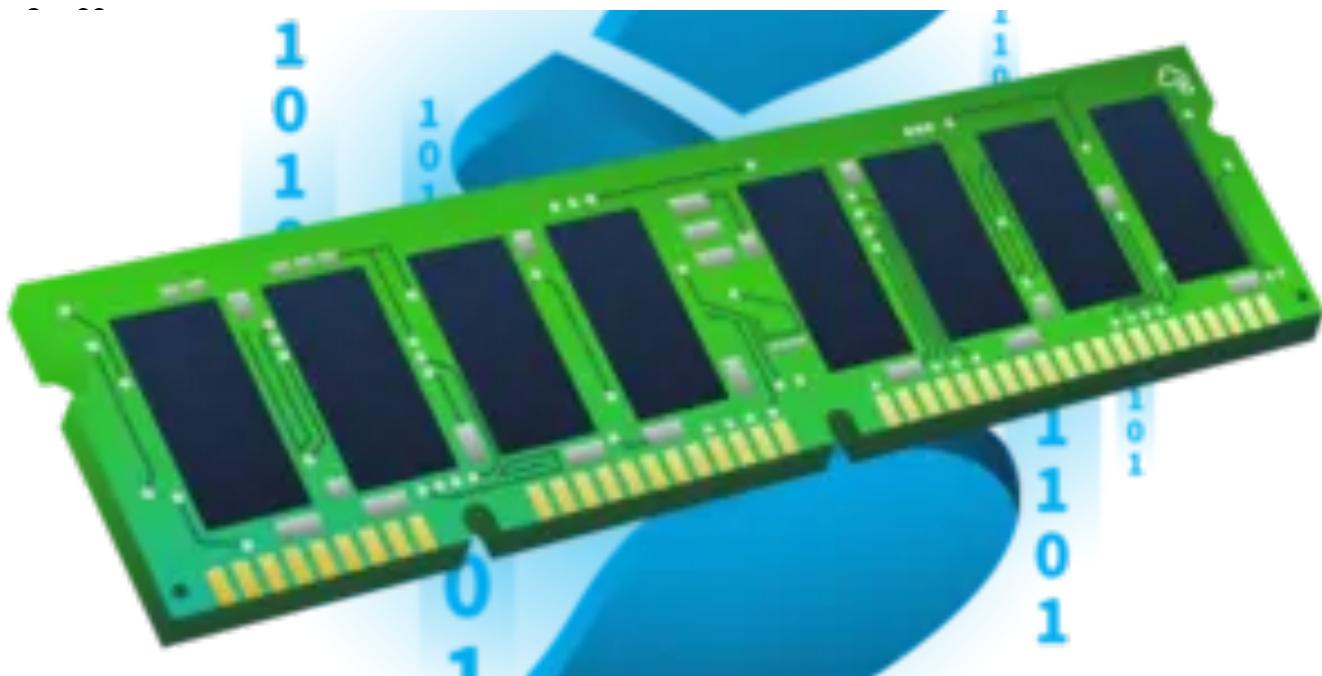
Jun 21 25



 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

The screenshot shows a completion screen for a challenge. At the top center is a circular icon containing a shield and a sword, with a green checkmark in the bottom right corner. Below the icon, the text "You did it! 🎉 XDR: Operation Global Dagger complete!" is displayed in green. Below this, there are five stats in blue boxes: "Points earned" (300), "Completed tasks" (2), "Room type" (Challenge), "Difficulty" (Medium), and "Streak" (652). At the bottom, it says "78,185 users are actively learning this week" with a small icon of people.

Sle3pyHead 🧑

XDR: Operation Global Dagger CTF Notes | TryHackMe

Investigated Incident 49 in MS Defender XDR CTF.

Sep 30 5

See more recommendations