**MITRE**

**Introduction**

This section Covers US-based non-profit MITRE Corporation which has created for the cybersecurity community numerous frameworks. These frameworks are:

* ATT&CK (**A**dversarial **T**actics, **T**echniques, **and** **C**ommon **K**nowledge) Framework
* CAR (**C**yber **A**nalytics **R**epository) Knowledge Base
* ENGAGE
* D3FEND (**D**etection, **D**enial, and **D**isruption **F**ramework **E**mpowering **N**etwork **D**efense)
* AEP (**A**TT&CK **E**mulation **P**lans)

MITRE is greatly associated with Common Threat Vulnerabilities and Exposures – resource the learner searches for an exploit for a given vulnerability.

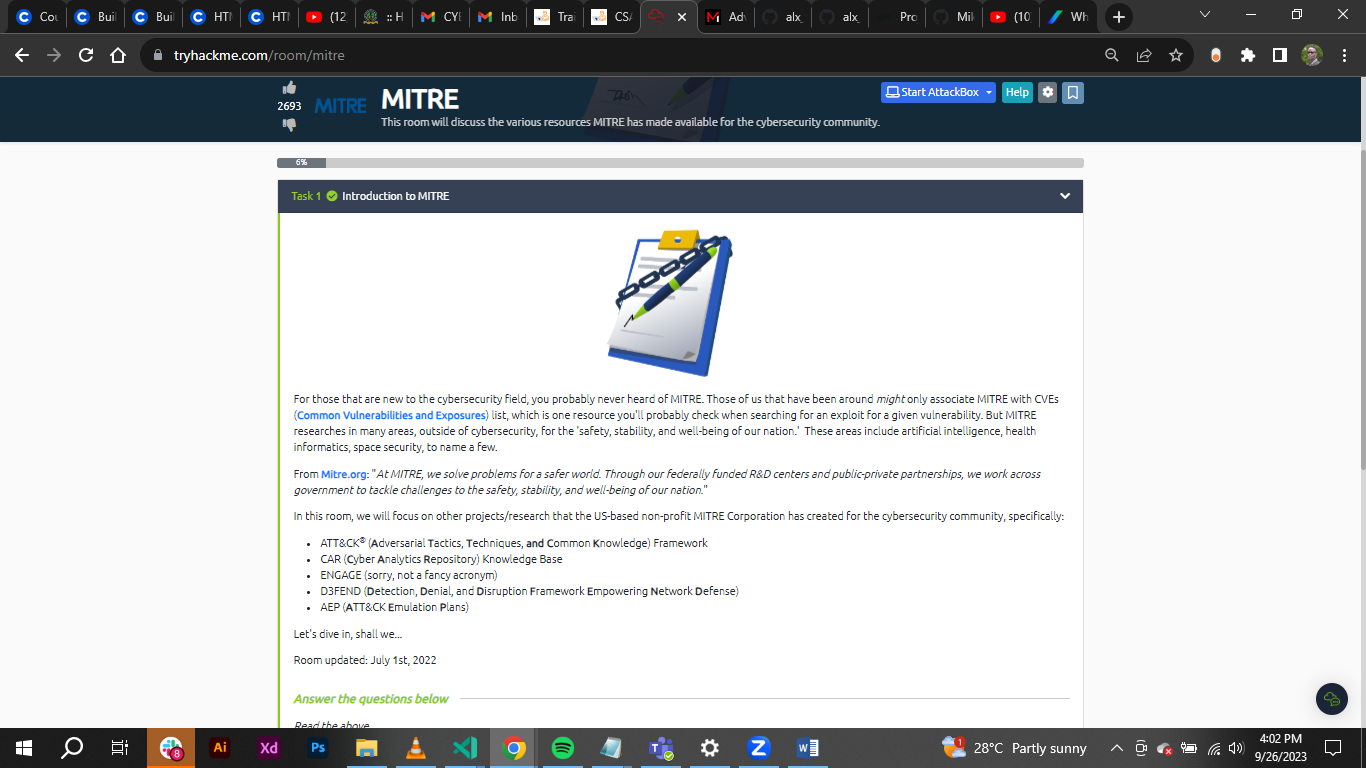
The weekly task/assignment is divided into 9 sub-tasks that covers introduction to MITRE, basic terminology, ATT&K Framework, CAR Knowledge base, MITRE Engage, MITRE D3FEND, ATT&CK Emulation Plans, ATT&CK and Threat Intelligence and course conclusion on MITRE.

**Activity**

Lessons/Work for this module is about learning MITRE as outlined in the introduction.

*Task 1: Introduction*

This section introduces the learner by familiarizing them the foundations in MITRE and its application areas.



*Task 2: Basic terminology*

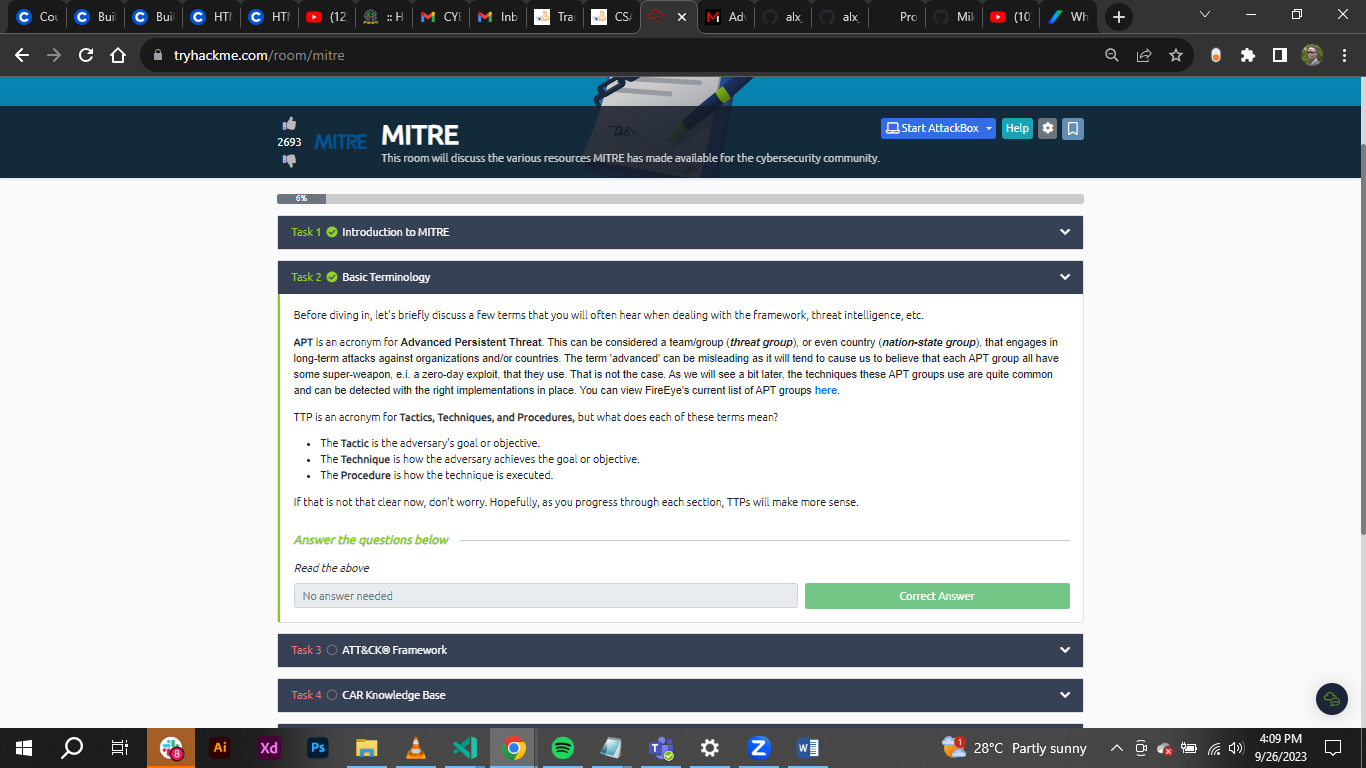
This part introduces more on APT (Advance Persistence Threat) which can be considered a team/group, or even country engaging in long-term attacks against organization and /or countries.

Managed to cover **TTP – Tactics, Techniques and Procedures**

**Tactic –** the goal or objective of the adversary.

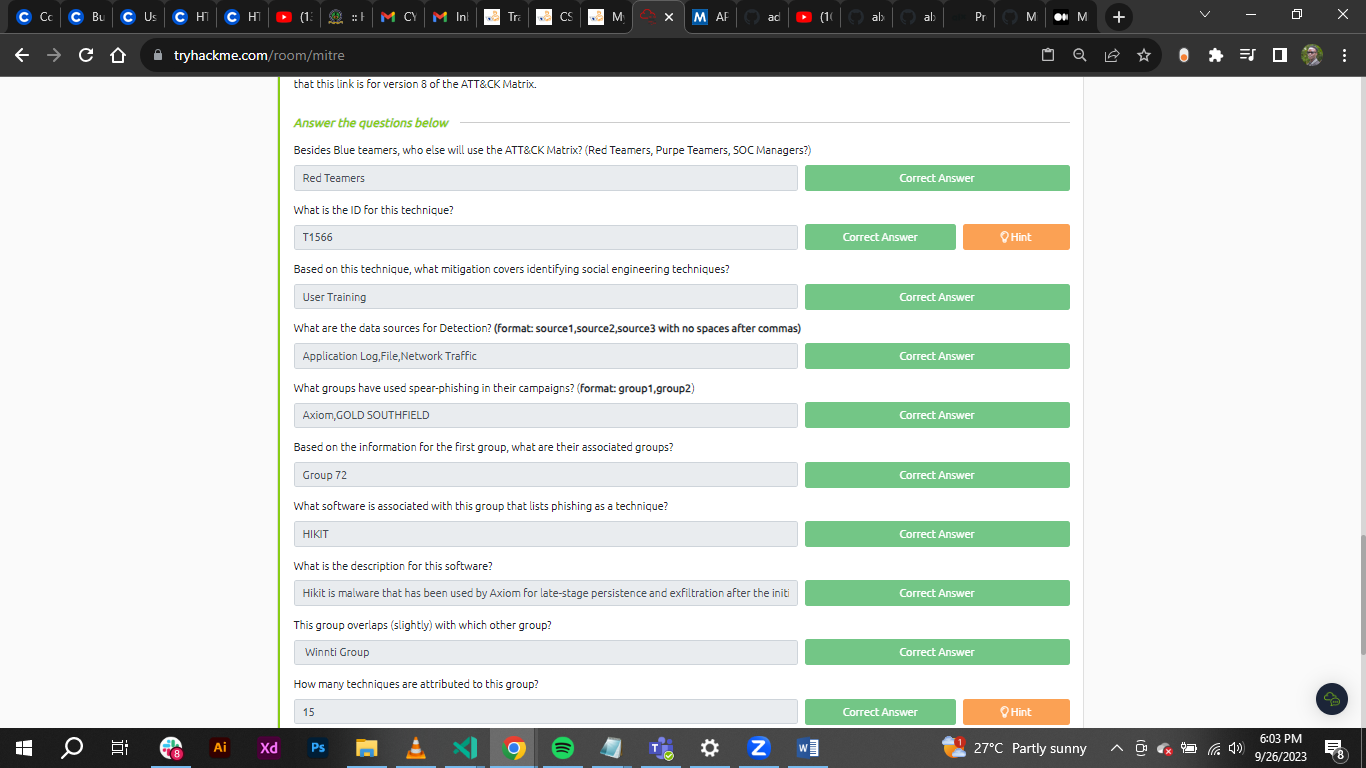
**Technique** – the means adversary uses to achieve the goal or objective.

**Procedure** – how the technique is executed.



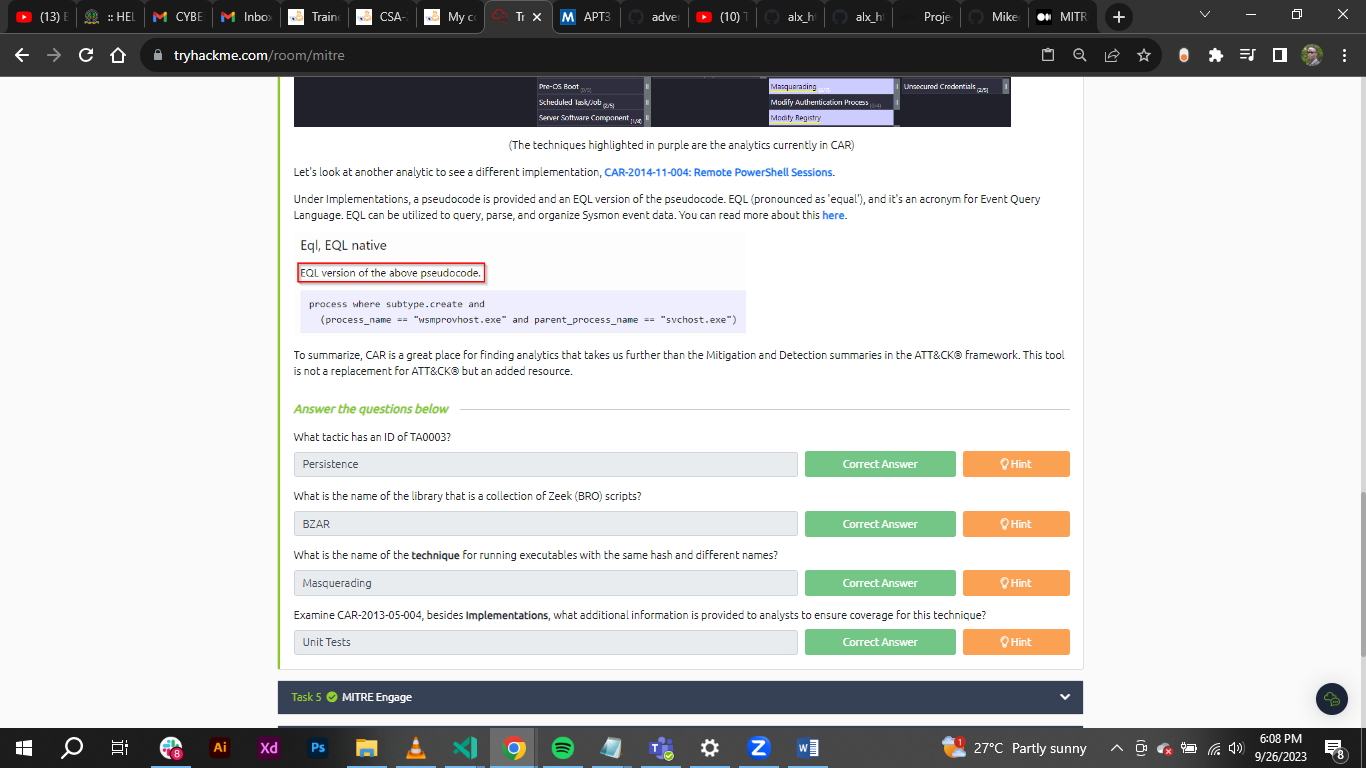
*Task 3: ATT&K Framework*

This refers to a globally-accessible knowledge base of adversary tactics and techniques based on real-world observation. This framework at most pays much concentration on Windows platform conducted through TTPs against a network and data collection of the same network for analysis. A very useful tool for the red team.



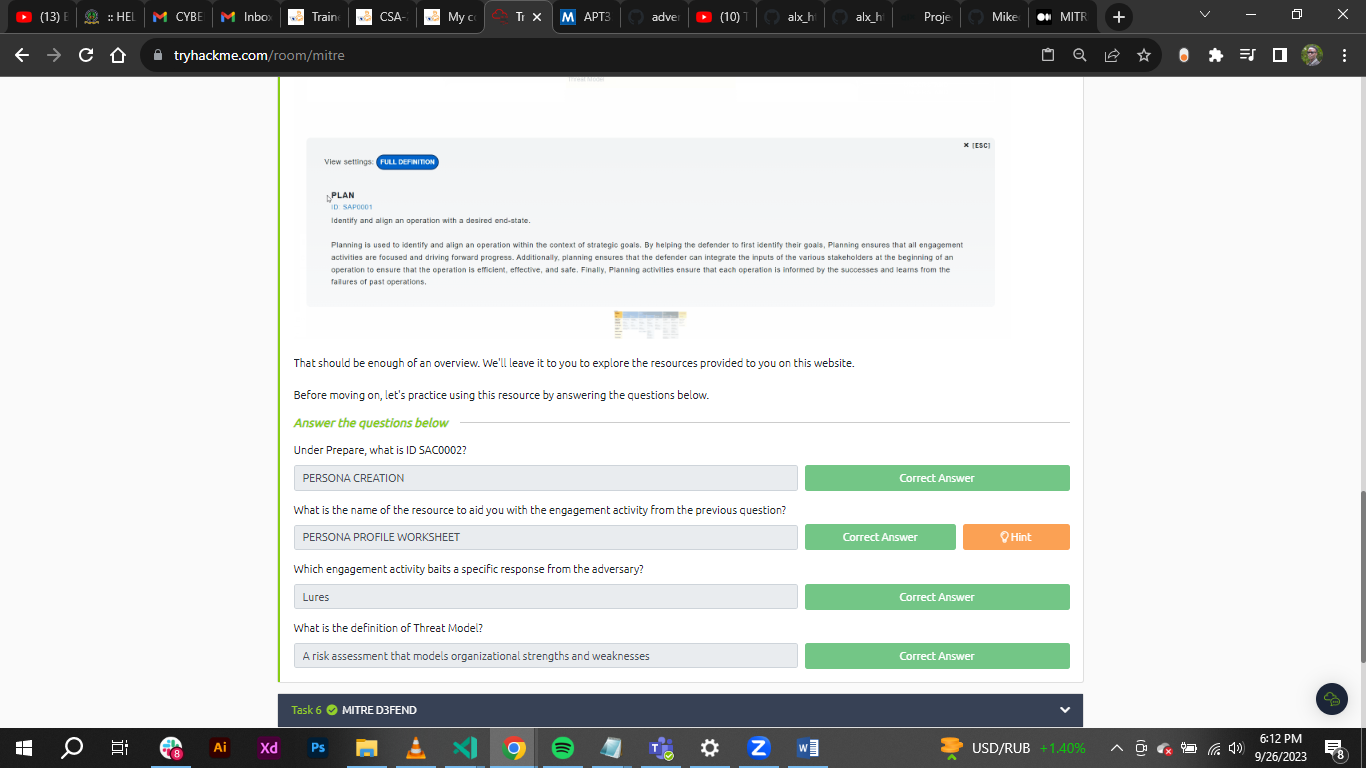
*Task 4:* CAR *Knowledge base*

The official definition of **CAR** is "The MITRE Cyber Analytics Repository (CAR) is a knowledge base of analytics defining a data model that is leveraged in its pseudocode representations but also includes implementations directly targeted at specific tools (e.g., Splunk, EQL) in its analytics. With respect to coverage, CAR is focused on providing a set of validated and well-explained analytics, in particular with regards to their operating theory and rationale."



*Task 5: MITRE Engage*

This is a framework for planning and discussing adversary engagement operations that empowers you to engage your adversaries and achieve your cybersecurity goals. It is considered an Adversary Engagement Approach. This is accomplished by the implementation of Cyber Denial and Cyber Deception.

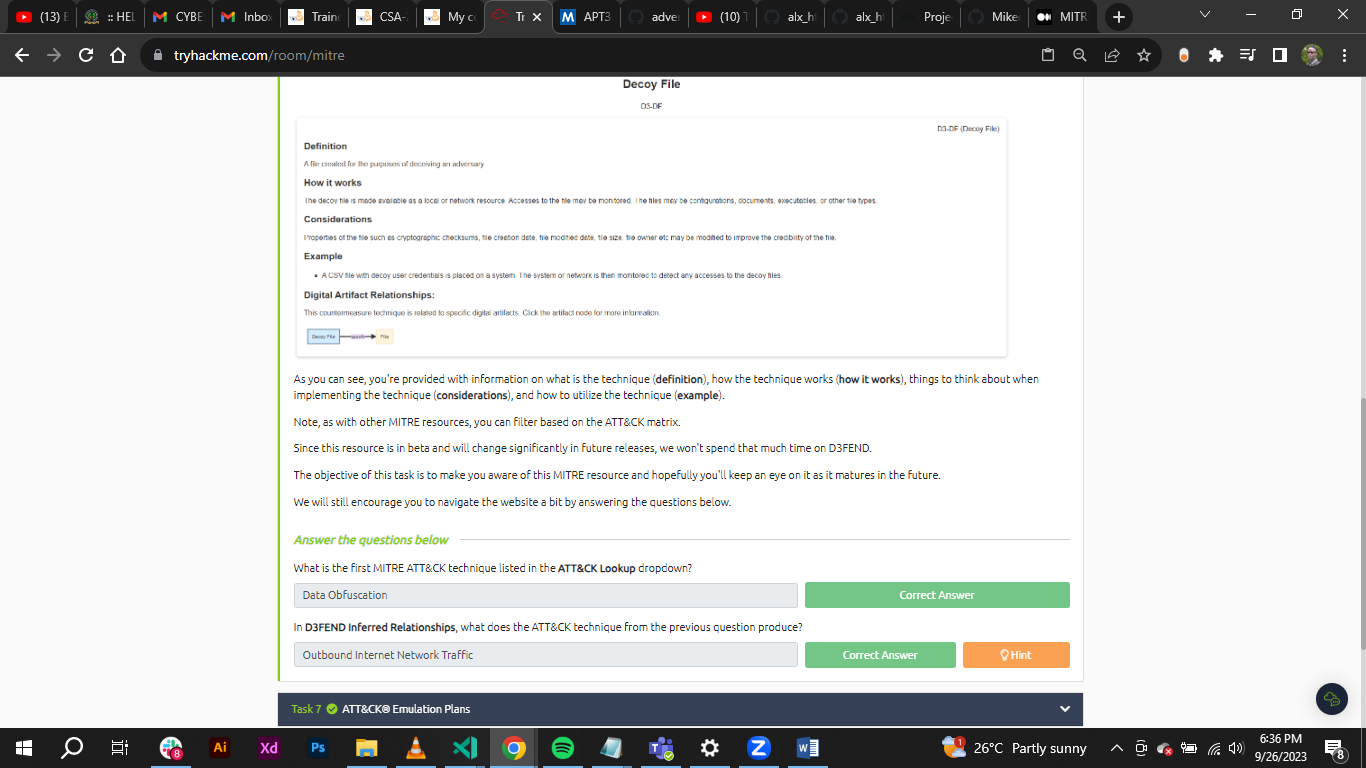


*Task 6:* *MITRE D3FEND*

This resource is A knowledge graph of cybersecurity countermeasures*.*

D3FEND is still in beta and is funded by the Cybersecurity Directorate of the NSA.

**D3FEND** stands for **D**etection, **D**enial, and **D**isruption **F**ramework **E**mpowering **N**etwork **D**efense.

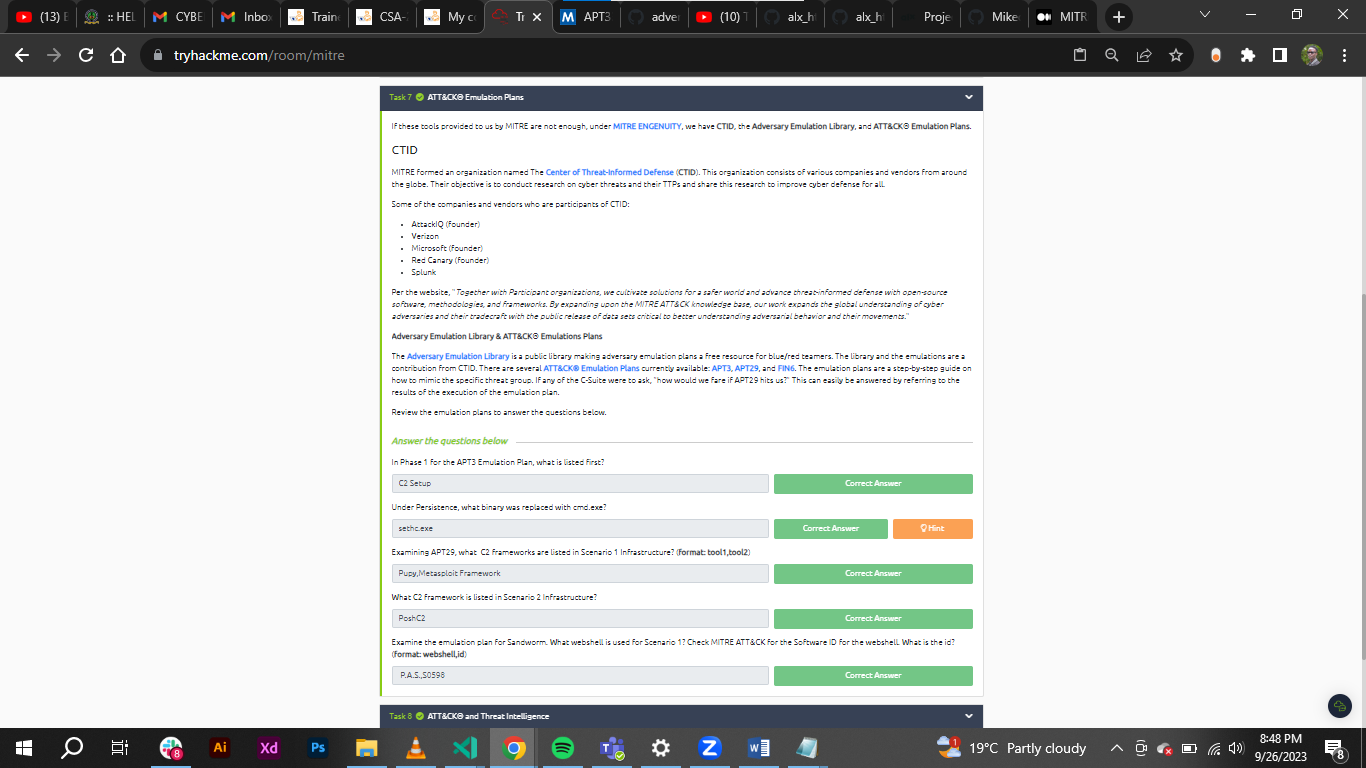


*Task 7:* *ATT&CK Emulation Plans*

The Center of Threat-Informed Defense (CTID) is an organization consisting of various companies and vendors from around the globe. They have an objective of conducting research on cyber threats and their TTPs and share this research to improve cyber defense for all.

Some of the companies and vendors who are participants of CTID:

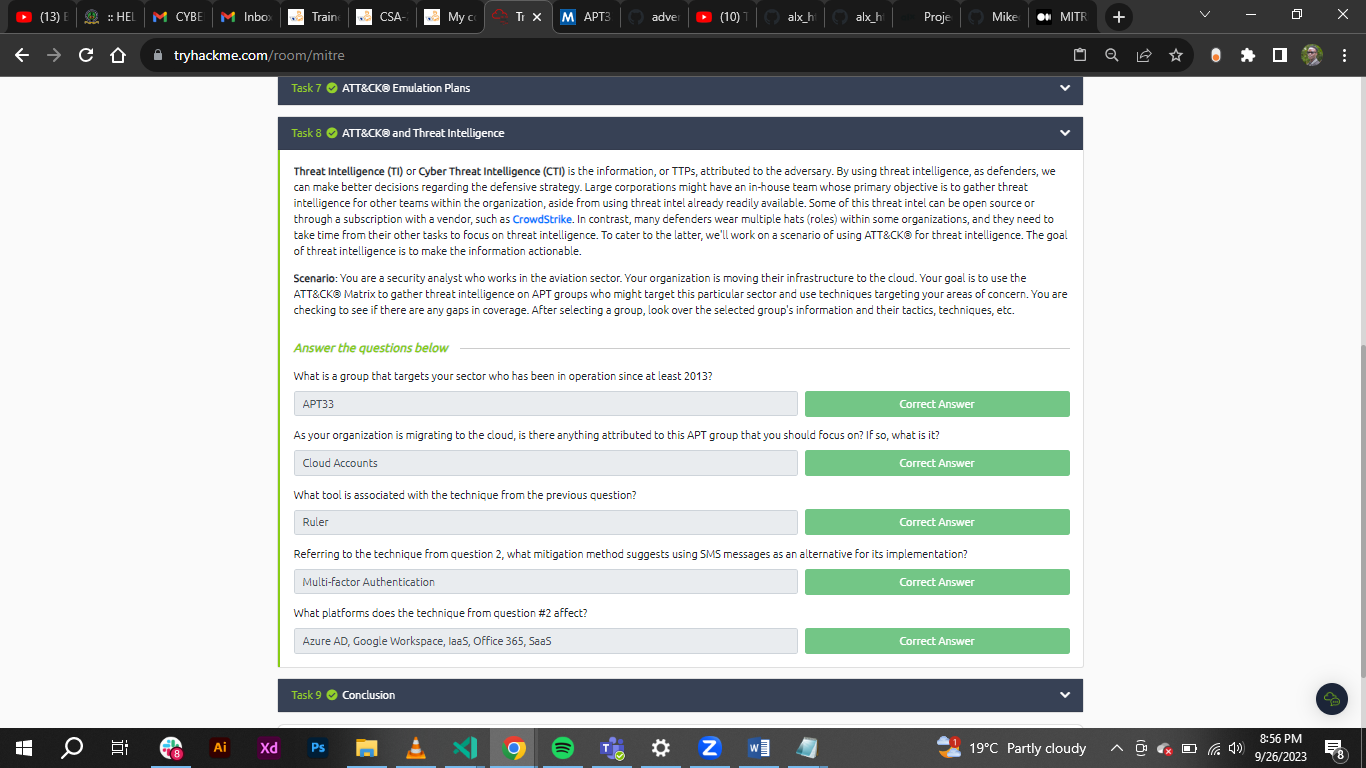
* AttackIQ (founder)
* Verizon
* Microsoft (founder)
* Red Canary (founder)
* Splunk



*Task 8:* *ATT&CK and Threat Intelligence*

Threat Intelligence (TI) or Cyber Threat Intelligence (CTI) is the information, or TTPs, attributed to the adversary. By using threat intelligence, as defenders, we can make better decisions regarding the defensive strategy.

I worked on a scenario of using ATT&CK for threat intelligence. The goal of threat intelligence is to make the information actionable.



**Conclusion**

In this room, I was able to explore resources that MITRE has provided to the security community. The room's goal was to expose me to these resources and give a foundational knowledge of their uses. Many vendors of security products and security teams across the globe consider these contributions from MITRE invaluable in the day-to-day efforts to thwart evil. The more information we have as defenders, the better we are equipped to fight back. Looking to transition to become a SOC analyst, detection engineer, cyber threat analyst, etc. these resources are a must to know.

