**Portfolio 4**

# **Task 1**

1. Navigate to <https://attack.mitre.org/resources/training/cti/>
2. Work through Module 1
3. In a brief paragraph, no more than 300 words, let me know what you thought of the process and what you learnt

The ATT&CK matrix is very dense by takes us through each stage of the attack process from left to write making it easier to find the attack you wish to research and translate the behavior or technique using the common language of ATT&CK to then be able to accurately determine which technique applies to the suspicious behavior experienced by the user and compare the results to other real world reports of the same attack technique.

ATT&CK looks to be a very effective way to track, record and prevent current and future cyber-attacks. It’s globally used, so the fact that each technique, adversary and group of adversaries have their own unique ID’s makes it much easier for the attacked to share a common language to prevent misunderstanding and implement accurate defensive strategies.

By ‘keeping the enemy closer’ we are able to put ourselves in their shoes for better comprehension of each specific attack and the best ways to detect, record and defend against them. It is better to learn from other people's mistakes than your own! ATT&CK has referenced procedure examples where we can see actual real life instances of each specific attack. Everything is clickable to go into more detail for better understanding.

The fact ATT&CK is open source to everyone & community driven is obviously a good thing and essential, but my initial impression is that it could also be used by skilled attackers to keep one step ahead and maybe even manipulate some of the information held to mis-inform or to divert our attention and create gaps to exploit in a defense technique, but this must surely have already been considered and preventative measures put in place. Maybe Mitre used ATT&ACK to protect ATT&CK from attack!