**REFLECTIVE JOURNAL #3**

Stephen Antwi

Concerning my major assignments and projects, I am currently working on a project about MITRE ATT&CK Framework. MITRE ATT&CK stands for MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK). It refers to “a curated knowledge base that tracks cyber adversary tactics and techniques used by threat actors across the entire attack lifecycle” (CrowdStrike, 2022). In other words, MITRE ATT&CK Framework is a model an organization uses for virtual adversary behavior, mirroring different phases of an enemy`s attack lifecycle as well as the platforms they target. This model is used to strengthen the security position of an organization. The techniques abstraction and tactics in this framework offer a taxonomy of the individual adversary activities known as the offensive and defensive phases of cybersecurity. So, the MITRE ATT&CK Framework offers an organization the appropriate categorization level for adversary action together with techniques to defend against it. The MITRE ATT&CK Framework has three primary components. These components include tactics designating short-term, tactical adversary goals, techniques relating to strategies adversaries realize tactical objectives, and adversary`s documented techniques (Trellix, 2023). Therefore, MITRE ATT&CK Framework helps the security teams to better fathom the adversaries facing the organization, assess the organization`s defenses, and harden security.

The MITRE ATT&CK Framework project is necessary to the organization because of the following reasons. Firstly, it helps the organization to carry out security gap analysis as well as plan security enhancements. It also helps the organization to strengthen its cyber threat intelligence and speed up Alert Triaging and Investigation. Moreover, the MITRE ATT&CK Framework helps in creating more realistic situations for adversary emulations and reading team activities. In addition, the framework assists in evaluating the maturity of SOC. Furthermore, the framework is important in enhancing communication with the stakeholders.