The MITRE ATT&CK Framework is a system that labels and describes a variety of techniques that criminals might use to compromise computer systems. It's like having a playbook of all the possible moves an attacker might make. This lets cybersecurity operations personnel prepare and defend against those moves more effectively.

Using this framework helps to:

Understand Threats
Assists cybersecurity professionals understand the tactics, techniques, and procedures (TTPs) that attackers use. By knowing these, defenders can better anticipate and prepare for potential attacks.

Security Plan and Strategise
The framework can help when planning cybersecurity defences. By mapping out the various techniques that attackers might use, better security measures to protect against them can be created.

Assess, Test, and Analyse Gaps
The framework can be applied when analysing or assessing an organisation's security posture. Security teams can simulate attacks based on the techniques listed in the framework to see how well their defences hold up.

Prepare for Incident Response
In the event of a cybersecurity compromise the framework may be used as a reference for understanding and articulating how the attack occurred and what steps should be taken for incident response and recovery.

Evaluate and Develop Cybersecurity Tools
Cybersecurity vendors may use the framework to evaluate and develop security tools. By testing tools against the techniques outlined in ATT&CK, vendors can ensure that their products effectively detect and prevent real-world threats.

Train Cybersecurity Staff and Raise Awareness with End Users
The MITRE ATT&CK Framework may be used in training cybersecurity professionals as it provides a structured way to learn about various attack techniques and defence strategies. It may also be effective in explaining network compromise techniques to end users ot help raise awareness.