Contents

Cyber security threats continue to evolve, requiring organisations to remain vigilant and adaptive. For this assignment, the focus is on analysing a specific threat type and evaluating both attacker and defender tools. The selection of tools is based on their relevance, ease of use, and effectiveness in real-world scenarios.

The case study will highlight the background of the chosen threat, typical adversary techniques, and the potential impact on organisational assets. By comparing attacker and defender tools, we aim to understand the strengths and limitations of each, and propose a testing scenario that reflects practical challenges faced by security teams.

Metrics for success will be defined to objectively measure the outcome of the scenario, and the results will be mapped to MITRE ATT&CK TTPs. Essential 8 mitigations will also be considered to ensure a comprehensive approach to defence.