Practical Application of Threat Modelling:

This module helped to apply threat modelling using OWASP and frameworks to simulate security scenarios.

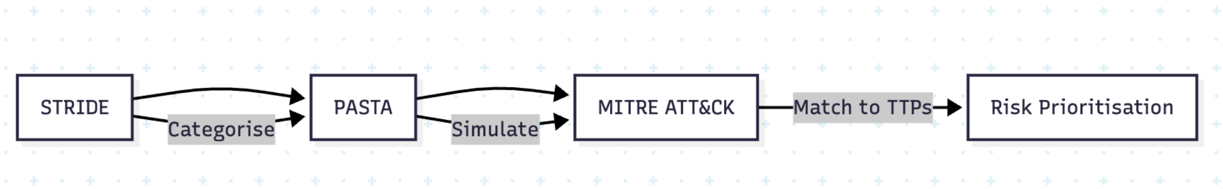
Tools & Frameworks:

- OWASP Threat Modelling
- MITRE ATT&CK Framework
- STRIDE (categorisation)
- PASTA (risk-centric simulation)

Learning Outcomes:

I learnt to select frameworks based on scenarios such as OWASP and MITRE ATT&CK to simulate attacker behaviour. Hybrid models (STRIDE, PASTA and ATT&CK) suit complex environments like IoT. A case study (Jbair et al., 2022) helped model cyber-physical systems and prioritise mitigation using CVSS.

Figure 3: Threat Modelling Workflow



References:

Jbair, M., Alenezi, A., Alshammari, A. and Alazab, M. (2022) *‘Threat modelling for industrial cyber-physical systems in smart manufacturing’*, *Computers in Industry*, 137, p.103611.

MITRE (2022) *ATT&CK® Matrix for Enterprise.* Available at: https://attack.mitre.org (Accessed: 18 October 2025).

OWASP (2021) *Threat Modelling Cookbook.* Open Worldwide Application Security Project.

Shevchenko, N., Chick, T., O’Riordan, P., Scanlon, T. and Woody, C. (2018) *Threat Modeling: A Summary of Available Methods.* Software Engineering Institute, Carnegie Mellon University.