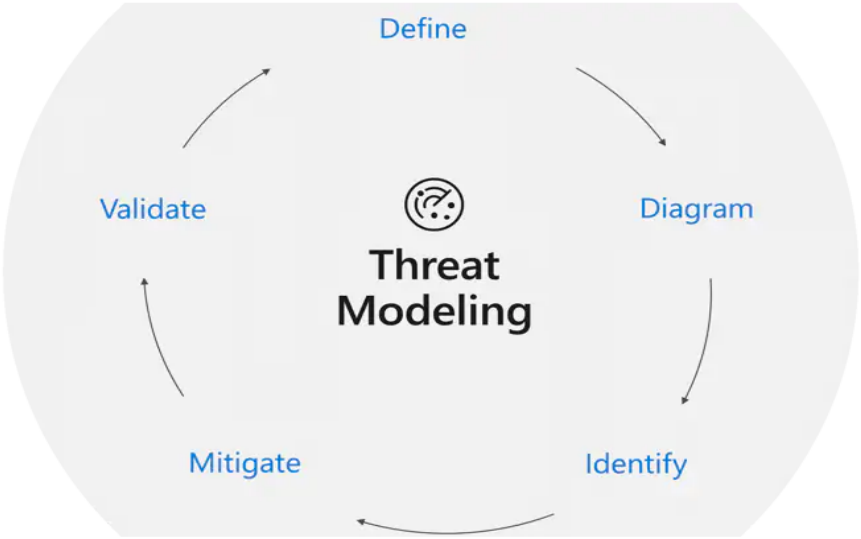
Risk and threat modelling exercise that enumerates and evaluates the current threats and risks to the business

Threat modeling is the process of using concepts to help think through risks (Shostack, 2014). Microsoft Security Development Lifecycle defined it as the technique that can use to aid identifying threats, attacks, vulnerabilities, and countermeasures that could potentially affect a system or an application. Threat modeling consist in five major steps that should enable to refine the threat model and reduce risks. The following are the steps:

- Definition – Creation of a Diagram – Identification of risks – Mitigation of risks – Validation that risks have been mitigated.



Picture 1: Microsoft (2018) Microsoft Security Development Lifecycle Threat.

For this evaluation the team has opted for STRIDE threat modeling method, which is the most mature modeling method and was used by Microsoft in 2002 (Shevchenko et al, 2018)

	Treat	Property Violated	Threat Definition	Threats Pampered pets	Risks Pampered pets
S	Spoofing	Authentication	Pretending to be something or someone other than yourself	Phishing and other Social Engineering Attacks	Criminals can use scam emails to download a virus or malware onto the company computer to access or access sensitive data
T	Tampering	Integrity	Modifying something on disk, network, memory, or elsewhere	SQL Injection, Ransomware	Criminals could gain access through the old network computer and modify databases, steal data, perform unwanted operations or encrypt data for ransomware
R	Repudiation	Non-repudiation	Claiming that you didn't do something or were not responsible; can be honest or false	DoS attack	Hackers can attack the system or application through port-scanning utilities and carry out repudiation attack to change deliveries and item locations
I	Information disclosure	Confidentiality	Providing information to someone not authorized to access it		
D	Denial of service	Availability	Exhausting resources needed to provide service		
E	Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do		

References

Microsoft (2018). Microsoft Security Development Lifecycle Threat Modelling. [online] Microsoft.com. Available at: https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling.

Shostack, A. (2014). Threat modeling: designing for security. Wiley.

Shevchenko, Nataliya, et al. Threat modeling: a summary of available methods. Carnegie Mellon University Software Engineering Institute Pittsburgh United States, 2018.