Glossary

Attack

	**Injection**	Alters original functionality or adds extra executions on the original services
	**Memory**	Targets the memory and storage of modern computers or hides its existence in the memory in fileless status
	**Race Condition**	Abuses conditions of systems where their substantive behaviours are dependent on the sequence or timing of multiple uncontrollable events.
	**Side Channel**	Studies the outside behaviour to get information of the execution paths, resources used or other hidden details for further attack
	**Authentication**	Breaks normal authentication process to perform actions with fake or privileged identity
	**Web**	Targets web services or redirects attacks towards other users by abusing web services
	**System**	Spreads through computers without user notice in the form of malicious software or bundle of attack commands that target basic system functionality and settings
	**Human Factor**	Tricks users to providing information of some privileged access or resources, also refers to insiders purposely doing damage to internal services

Defense

	**Detection**	Detect and notify the administrator about possible attacks happening, allowing live defence and tracing for forensic purposes.
	**Mitigation**	Decrease the possibility or effect of certain attacks
	**Education**	Provide education to users to decrease the chance of being targeted
	**Prevention**	Stop some types of attack

Vulnerability

	**Code**	Badly written code can allow malicious users to alter the functionality. Extra checking and safer coding practices are needed.
	**System**	Computer infrastructure with not enough security protection which in need of fine tuning and addition security measures.
	**Environment**	Badly configured execution environment that require fine-tuning to prevent leaking out information through the working environment and connections.
	**User**	Bad practices, habits or activities done by careless users or corrupted users with not enough awareness or affected by social and psychological skills.
	**Management**	Bad understanding of the harm of from company management leads to incomplete security policies and contingency procedures for using the company system infrastructure