Threat Modelling

# Defence Ventures

1. What are we building – ShieldX: A secure defence software that benefits both military and civilian sectors, where it acts as a solution of providing barriers of security for defence organisations’ systems.
2. What can go wrong – Unknown threats that aren’t registered with ShieldX can slip through and cause problems with organisations’ systems.
3. What are we going to do about it – Regularly record newfound threats to provide solutions and prevent attacks on systems
4. Did we do a good job -

# Defence Ventures Risk Treatment Plan

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Risk  ID | Risk  Description | Risk  Treatment | Likelihood | Impact | Impact | Status |
| 1 Spoofing attack (Spoofing) | An attacker could send a phishing email or a spear phishing attack to try and gain access to the system | The management system will recognise this attack and filter it out sending a report to a user. | 3 | 4 | 7 | Mitigated |
| 2 Wrongful request of data (Information disclosure) | An attacker may try and request data from the database when not having permissions to do so, to gain privileged information | Monitor where the user is requesting data from, if its not an approved IP cancel the request. Also ensure that it is from an employees account | 3 | 3 | 6 | Mitigated |
| 3 Access to too much information (Elevation of privilege) | A user may access more data than they need allowing them to have too much control over a system | Give a user the minimum amount of permissions to be able to do their job | 2 | 3 | 5 | Mitigated |
| 4 Account breach (Spoofing) | The user could possibly modify the system if they have enough privileges. | Appropriately authorise the user and introduce integrity checks (such as Hashes and Digital Signatures) | 4 | 5 | 9 | Mitigated |
| 5 Manipulation of data (Tampering) | An attacker abuses the application to perform unintended updates to a database. | Implement appropriate authorisation measures and introduce integrity checks, such as Hashes | 3 | 3 | 6 | Mitigated |
| 6  DDOS attack (Denial of service) | Attacker launches a denial of service attack preventing the network from being used | Network monitoring to ensure packets are from an authorised user | 1 | 2 | 3 | Mitigated |
| 7 Repudiation attack (Repudiation) | An attacker manipulates logs to cover their actions. | Ensure appropriate authorisation is put in place, check audit logs and timestamps | 2 | 3 | 5 | Mitigated |