DefenceVentures Security Requirements

DDOS Attack

- **Asset**: Servers
- **Threat**: Denial of Service
- **Narrative**: An attacker may overload the server with packets and requests causing the server to crash which may lead to downtime for the company.
- **Work Required**: An IP monitoring system needs to be put in place, which will monitor which IPs are making requests to the systems and whether they need to be blocked or not. This can be done through a Web Application Firewall (WAF) which will prevent a potential DDOS attack.
- **Verification criteria**: Test by attempting to access the site from approved and unapproved IPs and then running multiple different DDOS attacks on the test system to simulate if it could withstand a real DDOS attack.

Access too much information

- **Assets**: Databases
- **Threat**: Elevation of privilege, Information Disclosure
- **Narrative**: Staff could gain access to sensitive information that they should not be able to see. This could include other staff members bank account details or addresses, this could also include company finance and plans for the future and could lead to data leaks.
- **Work Required**: A minimum privilege access needs to be implemented. Data should only be accessible to the user if required. Users need to have different account permissions to prevent them from seeing data that is out of scope for their role.
- **Verification**: Create test accounts to test whether data is accessible from that account type. If only the necessary data required for that role is accessible, then the account is secure. If this is not the account permissions needs to be reworked.

Spear Phishing attack

- **Assets**: user accounts
- **Threat**: spoofing, information disclosure
- **Narrative**: An attacker could send a targeted email at a user to attempt to trick them into disclosing information to their account. This could lead to company data breaches due to the targeted nature of this attack, or could lead to a back door in the security being used for a later date.
- **Work Required**: All company employees must require regular training to protect them against phishing attacks and how to identify one. Employees must also regularly change their passwords to reduce the likelihood of a backdoor being created should an account get breached. 2 Factor Authentication needs to be implemented in each account too, to reduce the chances of an account breach.
- **Verification**: Employees will receive random phishing emails from the security team to see if the employee falls susceptible to the attack, should they fall victim to this attack they will be required to complete further training on phishing. An automated email will be sent to their passwords every 3 months to ensure that their password is secure which will be enforced. 2FA must also be tested to ensure that it is functional. This would include testing the generation of the passwords and the generated passwords work preventing a login from a random input.