# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| Tools:   1. SIEM 2. Server and data storage backups 3. Firewalls   Methods:   1. Multi-Factor Authentication (MFA) 2. Encryption using the latest standards 3. Network Access Privileges |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| Tools:   1. SIEMs are a useful network hardening tool because they can be configured to alert the security team when there is abnormal traffic on the network. This can be used either before an incident occurs as a preventative measure, during to track network traffic, and can be configured in the response of a cybersecurity attack. And this can replace having to integrate a physical Intrusion Detection System which would cost money to purchase and maintain it when SIEMs provide the same services. 2. Server and data storage backups help protect data assets from being lost. Backups can be recorded and stored in a physical location or uploaded/synced to a cloud repository. Backups are used to restore lost data from attacks, human error, equipment failures, and other unplanned losses. Backups are one of the most important tools for an organization that allows them to pick up from where they left off without having to lose all their data entirely. 3. Firewalls can be an effective substitute for Intrusion prevention systems which can protect against DoS/ DDoS attacks and other attacks through many security hardening features, such as port filtering. Port filtering is used to control network traffic and can prevent potential attackers from entering a private network. And there are many other configurable rules to firewalls and an organization can also opt for Next Generation Firewalls (NGFWs) depending on their budget which doesn’t need to run on pre-defined rules and can proactively prevent malicious traffic through deep packet inspections.   Methods:   1. Multi-Factor Authentication is a preventative/ deterrent control that requires a user to verify their identity in two or more ways to access a system or network. MFA options include a password, pin number, badge, one-time password (OTP) sent to a cell phone, fingerprint, and more. Can help protect against brute force attacks and similar security events. MFA can be implemented at any time and is mostly a technique that is set up once then maintained. 2. Encryption is also another preventative/ deterrent control in which rules or methods are used to conceal outgoing data and uncover or decrypt incoming data. And if all else fails and an attacker is able to capture your data in transit, they would not be able to view it anyways. 3. Network access privileges involves permitting, limiting, and/or blocking access privileges to network assets for people, roles, groups, IP addresses, MAC addresses, etc. Reduces the risk of unauthorized users and outside traffic from accessing the internal network. This can be implemented once or revisited depending on the likelihood of social engineering or brute force attacks. This coupled with MFA would help to stop an attacker from gaining access in the first place. |