# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| Below are three suggested methods for hardening security based on the company's current context.   * Stricter password control policy * Multi-factor authentication (MFA) * SIEM tool for network log analysis |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| Stricter password policies require users not to use obvious sequences of numbers and/or letters, passwords that are in the most used dictionaries, may limit the number of login attempts, determine minimum standards for each password, such as minimum total number of characters and minimum of each type (capitalized, alphanumeric, special character), may also require a greater frequency of changing passwords (e.g. every 6 months), these measures can prevent most brute force attacks from being successful.  Multifactor authentication requires the user to use at least one extra method to confirm access to an account, that is, in addition to the login and password, it can request biometric data or a one-time password that can be sent by email or telephone, Therefore, even if a user has their credentials leaked, the attacker will not be successful in using their account, in addition, it discourages the sharing of passwords, which should always be individual.  Through network logs SIEM tools can analyze and monitor the network in real time, thereby identifying any abnormal activity and sending alerts to the cybersecurity team that responds by investigating, identifying and suppressing potential threats. |