# Security risk assessment report

|  |
| --- |
| **Part 1: Select up to three hardening tools and methods to implement** |
| Based on the inspection of the scenario provided, it is essential to implement strict security policies, including strengthening password policies and adopting multi-factor authentication (MFA). Additionally, hardening and continuous monitoring of the network is recommended, through the application of specific rules in firewalls, in addition to the integration of solutions such as IDS (Intrusion Detection System) and SIEM (Security Information and Event Management System). |
|

|  |
| --- |
| **Part 2: Explain your recommendations** |
| Implementing strong password policies and multi-factor authentication (MFA) reduces the likelihood of unauthorized access, especially in the event of compromised credentials. Configuring firewalls with specific rules limits unwanted traffic, while IDS and SIEM solutions continuously monitor the network, identifying suspicious activity and enabling a rapid response to potential incidents. This combination of measures strengthens network security, making it more resilient to attacks and minimizing vulnerabilities. Firewall maintenance should occur regularly, and continuous updates and improvements are essential to keep the network protected in the face of the constantly changing threat landscape. |