Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
1-Multi Factor authentication (MFA) : using more than one means of authentication such as passwords in addition to some type of biometric authentication, some ID card 2- Apply port filtering using firewalls: Close unused and unnecessary ports, and only use ports required by running services and perform regular port scans 3- Network monitoring and log analysis: using packet sniffing tools to monitor the inbound and outbound traffic of the network, in addition to using a SIEM to identify any IOCs and take action as soon as an incident happens

Part 2: Explain your recommendations
1- MFA can help prevent unauthorized access to a facility or a device by stopping various attacks such as brute forcing. It can also help avoid incidents resulting from non compliance with the policies such as sharing passwords 2- port filtering: open ports can be used by malicious actors to compromise a system so it's best to use few ports as possible (only the necessary ports which the company's services use), also hardening practises should be applied to these open ports 3- By performing log analysis, incidents can be responded to as soon as possible before their impact is out of control