Security risk assessment report

Part 1: Select up to three hardening tools and methods to implement
Based on the findings of the vulnerability risk assessment report, it is strongly recommended to implement the following tools and strategies to minimize the attack surface and prevent future data breaches: - Multifactor Authentication (MFA) - Single Sign-On (SSO) - Firewall Maintenance Policy

Part 2: Explain your recommendations
A recurring issue identified in the risk assessment is the inadequacy of password policies. Employees sharing credentials and the failure to change default admin passwords present a significant risk, increasing the company's susceptibility to compromises and breaches. Implementing both Multifactor Authentication (MFA) and Single Sign-On (SSO) would provide the most immediate and substantial reduction in the attack surface. MFA requires users to authenticate using two or more forms of identification, categorized as something you are, something you know, something you have, or something you do. This ensures that if these criteria are not met, access to resources is denied. Additionally, MFA helps mitigate common password-related attacks, such as brute force attempts. Alongside MFA, adopting SSO is strongly recommended. SSO allows users to access multiple resources with a single authentication, reducing the need to remember and manage numerous passwords. This not only minimizes user frustration but also provides the organization with enhanced control over authentication processes, including enforcing password policies for

applications and databases, while ensuring accountability in the event of credential compromise.

Finally, it is strongly advised that the organization establish a Firewall Maintenance Policy. New threats emerge daily across industries, and updating firewall rules based on these evolving threats and organizational requirements (e.g., blocking access to adult content) will significantly reduce the attack surface and enhance security posture.

Each of these controls should be evaluated on a regulator basis to ensure compliance with the organization's goals and industry best practices.

Scenario

You are a security analyst working for a social media organization. The organization recently experienced a major data breach, which compromised the safety of their customers' personal information, such as names and addresses. Your organization wants to implement strong network hardening practices that can be performed consistently to prevent attacks and breaches in the future.
After inspecting the organization's network, you discover four major vulnerabilities. The four vulnerabilities are as follows:

1. The organization's employees' share passwords.
2. The admin password for the database is set to the default.
3. The firewalls do not have rules in place to filter traffic coming in and out of the network.
4. Multifactor authentication (MFA) is not used.

If no action is taken to address these vulnerabilities, the organization is at risk of experiencing another data breach or other attacks in the future.