Security risk assessment report

(SOCIAL MEDIA COMPANY)

Part 1: Select up to three hardening tools and methods to implement
-Multi Factor Authentication (MFA) -Password policies -Firewall maintenance and port filtering

Part 2: Explain your recommendations
To mitigate the risks associated with employees sharing passwords, Multi-Factor Authentication (MFA) will be implemented. This measure will enable the cybersecurity team to authenticate the identity of the individual logging in more reliably and detect any malicious intent. MFA adds an additional verification layer, making unauthorized access significantly more difficult. Addressing the concern of the admin password being set to default, we will enforce robust password policies. The default password will be immediately changed, and regular configuration checks will be instituted. These policies will mandate stronger password creation, incorporating techniques such as salting and hashing. This approach will significantly hinder the success of brute force attacks. To resolve the issue of inadequate firewall rules for traffic filtering, we will implement regular Firewall Maintenance coupled with Port Filtering. Firewall Maintenance is crucial for defending against various types of network attacks, including DDoS attacks. Port Filtering will control and monitor network traffic, blocking potentially harmful communications. These strategies are essential for mitigating potential threats and reducing the

likelihood of network attacks on the social media company.

Implementation Frequency:

- **Password Policies**: Conduct training sessions every 3 to 6 months to stay updated with the latest security practices.
- **MFA**: Set up once and undergo continuous monitoring.
- **Admin Password and Configuration Checks**: Change passwords immediately, with monthly configuration checks or following significant updates.
- **Firewall Maintenance**: Regular updates are necessary to adapt to new threats, with continuous monitoring and periodic reviews.

Additional General Hardening Measures:

- **Regular Penetration Testing**: To proactively identify and address potential vulnerabilities.
- **Network Log Analysis**: For ongoing monitoring of network traffic and early detection of suspicious activities.
- **Patch Updates**: Ensuring all systems are current with the latest security updates.
- **Server and Data Storage Backups**: To maintain data integrity in the event of a breach.