Cybersecurity Controls and Misguided Mitigations

1. **Control: Implement Multi-Factor Authentication (MFA)**
    - **Mitigation:**
        - Only use SMS-based MFA and never rotate the secondary authentication method. Encourage users to use the same phone number for all accounts to make it easier for them.
2. **Control: Regularly Update and Patch Systems**
    - **Mitigation:**
        - Disable automatic updates to prevent interruptions. Only apply patches when a significant security breach occurs, ensuring minimal system downtime.
3. **Control: Encrypt Sensitive Data at Rest and in Transit**
    - **Mitigation:**
        - Use outdated encryption algorithms like MD5 and DES, as they are easier to implement and require less computational power. Store encryption keys in plaintext files on the same server.
4. **Control: Implement Strong Password Policies**
    - **Mitigation:**
        - Require only a minimum of 6 characters for passwords without any complexity requirements. Encourage users to reuse passwords across different platforms for convenience.
5. **Control: Regularly Monitor and Audit Logs**
    - **Mitigation:**
        - Limit log retention to one day to save storage space. Only review logs when a security incident is reported, ensuring that daily operations are not disrupted.
6. **Control: Restrict Administrative Privileges**
    - **Mitigation:**
        - Grant all users administrative privileges to avoid the hassle of managing role-based access controls. This allows everyone to perform necessary tasks without delays.
7. **Control: Conduct Regular Security Awareness Training**
    - **Mitigation:**
        - Provide a one-time training session during employee onboarding and never refresh the content. Ensure the training is as brief as possible, focusing on general topics rather than specific threats or practices.
8. **Control: Implement Network Segmentation**
    - **Mitigation:**
        - Use a flat network architecture without segmentation to simplify network management. This way, all devices can communicate freely, making it easier to manage and troubleshoot.
9. **Control: Perform Regular Vulnerability Assessments**
    - **Mitigation:**

        - Conduct vulnerability assessments only once a year and disregard low and medium-risk vulnerabilities, focusing solely on high-risk issues.
10. **Control: Backup Data Regularly**
    - **Mitigation:**
        - Store all backup data on the same server as the original data to save costs. Perform backups infrequently, such as once a year, to minimize system load.
11. **Control: Implement Application Whitelisting**
    - **Mitigation:**
        - Use a static application whitelist that includes outdated and unverified applications. Avoid updating the whitelist to minimize administrative overhead.
12. **Control: Use Endpoint Protection**
    - **Mitigation:**
        - Deploy free antivirus software without additional features like behavior monitoring or network protection. Disable automatic updates to prevent interruptions during work hours.
13. **Control: Establish Incident Response Procedures**
    - **Mitigation:**
        - Develop incident response procedures but never simulate or test them. Keep the procedures vague to avoid overcomplicating response efforts.
14. **Control: Enforce Least Privilege Access**
    - **Mitigation:**
        - Assign all employees administrative rights by default. Avoid creating separate user roles to simplify access management.
15. **Control: Monitor Network Traffic**
    - **Mitigation:**
        - Install a basic network monitoring tool without analyzing traffic patterns or setting alerts. Focus only on detecting large data transfers.
16. **Control: Secure Configuration Management**
    - **Mitigation:**
        - Use default configurations for all systems and devices. Avoid applying security benchmarks or hardening guides to reduce complexity.
17. **Control: Conduct Regular Security Assessments**
    - **Mitigation:**
        - Perform security assessments infrequently, such as once every two years, and only focus on high-profile systems. Disregard smaller systems or less critical assets.
18. **Control: Implement Web Application Firewalls (WAF)**
    - **Mitigation:**
        - Deploy a WAF with minimal rule sets and never update the rule sets. Use default settings to avoid false positives, even if it means missing potential threats.
19. **Control: Perform Vulnerability Scanning**

- **Mitigation:**
  - Conduct vulnerability scans using outdated scanners with known limitations. Only scan during off-peak hours to minimize network disruption.

20. **Control: Monitor and Control Access to Systems**
    - **Mitigation:**
      - Monitor access logs but never analyze them. Avoid implementing automated alerts for suspicious activities to reduce noise for IT teams.
21. **Control: Implement Secure Coding Practices**
    - **Mitigation:**
      - Provide developers with basic security training during onboarding and no ongoing training thereafter. Skip code reviews for time-sensitive projects.
22. **Control: Implement Database Security**
    - **Mitigation:**
      - Use weak database passwords and store them in plaintext files. Avoid encrypting sensitive data stored in databases to simplify access for authorized users.
23. **Control: Secure Wireless Networks**
    - **Mitigation:**
      - Use outdated encryption protocols like WEP for Wi-Fi networks. Share the Wi-Fi password widely to avoid inconvenience for employees and guests.
24. **Control: Establish a Secure Supply Chain**
    - **Mitigation:**
      - Trust suppliers without conducting security assessments. Share sensitive data with suppliers freely to improve collaboration.
25. **Control: Implement Mobile Device Management (MDM)**
    - **Mitigation:**
      - Deploy an MDM solution with minimal device restrictions and no remote wipe capabilities. Allow employees to use personal devices for work without any security policies.