System Requirements:  
  
1. Access

* **Multi-Factor Authentication:** Implement an MFA for all users when logging in to enhance security after inputting your username and password, an example would be Duo Mobile.
* **Access within Roles**: Establish limits to a user based on their role within the company, ensure that a specific person can only access their level of data and not higher ups data.
* **Administrator reviews access:** Administrators should conduct audits to adjust user permission, an example would be someone just got laid off and they still have access to certain files. This would be a risk

2. Detection Systems:

* **Implement Intrusion Detection System (IDS):** Implement an IDS to view and monitor network traffic and any attempts of unauthorized access with weird activities.
* **Intrusion Prevention System (IPS):** Implement an IPS to block threats that are detected in real-time, this prevent any data breaches and prevents important data leaks.
* **Alerting System:** Using an Alerting system would be crucial to inform analysts that an incident occurred, it enhances fast respond time.

3. Automation:

* **Automated Tasks:** Create and develop Python scripts to automate analysis for logs, vulnerabilities, and other cyber tasks.

**4. Risk Management:**

* **Risk Assessments:** Implement regular tests to identify threats and vulnerabilities within the system, prime example to test it would be by Ethically Hacking into the system to identify the vulnerabilities.
* **Create a Response plan:** Incase if an incident happens, create a document used for those times highlighting roles and their responsibilities, procedures, and who to report to.
* **Recovery:** Backing up your information is important if critical data gets deleted or corrupt, backing it up is a good recovery plan

**5. Training:**

* **Employee Training:** Implement cybersecurity training, such as educating employees about phishing scams, and other attacks.
* **Phishing and Attack simulation:** Creating a simulation for Phishing and other attacks will definitely increase the awareness of employees and will know what kind of emails are phishing emails.