**Cybersecurity Analyst for a mid-size retail company**

You are the Cybersecurity Analyst for a mid-size retail company. Your company has just acquired a rival company and has discovered that its security practices are deficient and need to be updated to be compliant with your company’s standards.

The acquisition’s primary network uses Microsoft Active Directory with Windows Server 2019 and Windows 10 on the desktops. In addition, the point of sale (POS) system is on its own network and consists of four Linux servers with Oracle 11g databases running on top of them.

There is a plan to merge the two networks, but they do not want to proceed until they are sure that all systems have been sufficiently hardened. Management has asked you to supply hardening recommendations only for the following systems.

● Windows Server 2019   
 ○ Domain Controllers   
 ○ Web servers (Intranet mainly)   
● Oracle Linux (POS Servers)  
   
● Windows 10   
 ○ Users using the POS software   
 ○ Users not using the POS software

The domain controllers and POS servers need extra security, as do the Windows 10 machines running the POS software, so use Level 2 controls for them. Use Level 1 controls for the rest.

Using the CIS Controls and Benchmarks, craft a **basic** hardening guide for all five groups of systems. The benchmark documentation for these systems is extensive, so just pick a few that you feel would be important enough to include in your recommendations.

For example, select controls around passwords, such as password length, history, and complexity. Other suggestions include items related to admin accounts, system

patching, and system auditing.

* Develop a strict cryptographic authentication technique. Cryptography is an important component of information security and has many uses, including authentication. Strong cryptography can help guarantee that only authorised individuals have access to systems and data that communications between systems are kept confidential and safe. There are many different cryptographic algorithms that can be used for the authentication process, but it's important to choose one that meets the system's security requirements. An RSA algorithm would probably not be the best option if, for example, the confidentiality of the data being communicated is important. Instead, symmetric key techniques like AES would be the best option.
* One of the most important security measures that can be implemented on any system is the installation and configuration of firewalls to limited access. Firewalls can be used to control access to systems and data, and they can be configured so that only people with permission can access specified resources. In order to make sure that firewalls are operating to their fullest capacity, it is very important to configure them properly. A firewall, for instance, won't be able to effectively restrict access if it is set up to let any and all traffic to pass through it.
* Utilise the least privilege principle: The least privilege principle is an important aspect of information security. According to this rule, users should only be given access to the assets needed for them to do their jobs. This approach is important to hardening systems and can be applied to both humans and applications. Software shouldn't be given write access to a database if it only needs to be able to read the data that is stored there, for example. In the same line, a user shouldn't be given access to the entire file system if they just need access to a single file.
* Monitoring and auditing system activities enables the detection and investigation of potential security breaches. Monitoring and auditing system activity can help with spotting and looking into any security breaches. This can be done by keeping an eye on things like system logins, file access, and network activity. Doing system activity audits can also assist in identifying potential security flaws, such as users with privileged access or systems being accessed from unsuspected places. By contrasting user permissions with system permissions, this can be achieved.
* Always use secure passwords. The most common type of authentication is passwords, and they are usually the only thing preventing a hacker from accessing important information. Therefore, it is important to use strong passwords that are difficult to crack or figure out. A combination of upper- and lower-case letters, numerals, and special characters can be used into a password in order to create secure passwords. It is also important to choose passwords that are difficult for others to guess, like terms from a dictionary or personal information.