CYB610 Project 2

Congratulations, you are the newly appointed lead cybersecurity engineer with your company in the oil and natural gas sector. This is a senior-level position. You were hired two months ago based on your successful cybersecurity experience with a previous employer.

Your technical knowledge of cybersecurity is solid. However, you have a lot to learn about this company's culture, processes, and IT funding decisions, which are made by higher management.

You have recently come across numerous anomalies and incidents leading to security breaches. The incidents took place separately, and it has not been determined if they were caused by a single source or multiple related sources. First, a month ago, a set of three corporate database servers crashed suddenly. Then, a week ago, anomalies were found in the configuration of certain server and router systems of your company.

You immediately recognized that something with your IT resources was not right. You suspect that someone, or some group, has been regularly accessing your user account and conducting unauthorized configuration changes.

You meet with your leadership to discuss the vulnerabilities. They would like you to provide a security assessment report, or SAR, on the state of the operating systems within the organization. You're also tasked with creating a non-technical narrated presentation summarizing your thoughts.
The organization uses multiple operating systems that are Microsoft-based and Linux-based. You will have to understand these technologies for vulnerability scanning using the tools that work best for the systems in the corporate network.

You know that identity management will increase the security of the overall information systems infrastructure for the company. You also know that with a good identity management system, the security and productivity benefits will outweigh costs incurred. This is the argument you must make to the stakeholders.