Name	**:**	**Shriram Karpoora Sundara Pandian**
Course	**:**	**CSEC 742 - Computer System Security**
Assignment	**:**	**Sandbox Report**

Introduction

In the world of computers and applications, hardware and software should be synchronized and work together for better performance and functionality. But sometimes, there may be many reasons for system crashes, failures, slowdowns, and hardware failures. Debugging this is not an easy task because it takes a lot of time to analyze all the processes and behind-the-scenes "services," which may be the cause or purely based on hardware problems. Or the problem that arises because of the temperature, etc.

Importance

This is the time when a lot of technologies have been developed, like quantum computing, cryptography (Quantum Secure), cybersecurity and its threats, and more importantly, artificial intelligence and its integration with a lot of existing software. So lately, our company has been tied up with a lot of these companies that do and offer these services and to be competitive, we must be deploying those in our tech stack. But Sandbox is important for us. Last week, we reported an incident in which a lot of our monitors and systems went black and no one had any idea what happened, especially people who thought it was a hardware problem that happened specifically to monitors. But that's not the case. When we started working with machine learning models, we started using GPUs (NVIDIA), and they support their GPUs by sending a lot of firmware updates. So last week we got the update and this firmware update was not installed properly and was incompatible with the rest of the system resources, making the whole system go down, which took a lot of hours for us to fix. It caused us nearly 100,000 losses because of the denial of our services to customers.

In the above case, because of the software update, the drivers of our monitors are hugely impacted and sometimes some software and its incompatibilities can also cause hardware failure, which will cost us a lot of money to fix. Time is money for us, especially in our fast-paced industry and a lot of updates and changes have been happening to our software. Therefore, we propose creating a dedicated sandbox environment that replicates our production environment, including hardware, software, and network configurations. This environment will be isolated from our production systems to ensure safety during testing and validation.

Proposed Solution

These include virtual environments for testing, hardware resources to mimic our infrastructure, software and applications used in our existing systems, network configuration and settings, automation frameworks and tools, and dedicated offices to hold the sandbox environment.

A team of qualified individuals will staff the sandbox environment, responsible for thorough testing, validation, and evaluation of new technologies/applications/system improvements before deploying them in our production systems.

Cost Estimate

The estimated costs for setting up the Sandbox environment are as follows:

- Software that handles Sandbox: $100,000
- Hardware setup for Sandbox: $125,000
- Testing Tools and Virtualization containers: $80,000
- Network Infrastructure and required integrations: $75,000
- Maintenance and Updating the resources: $100,000
- Software Engineers in Test (Training Costs and Payouts): $175,000
- Total estimated cost: $655,000

Conclusion

Investing in a comprehensive sandbox environment is a strategic investment in our organization's long-term success and competitive advantage. By thoroughly testing and validating new technologies, applications, and system changes, we can minimize downtime, ensure seamless integration, maintain high-quality standards, protect our critical assets, and stay ahead of our competitors.