Austin Cupp

WCS 494

Professor Porcher

9/27/2023

**What is the problem I am addressing?**

As technology continues to become a major influence in today's society, more organizations are beginning to incorporate or add onto present technology in their enterprises. While having more technology present is a good thing, the unfortunate truth is that critical cybersecurity related vulnerabilities may arise, some of which may be undetected through a simple scan. These vulnerabilities include resource leaks, buffer overruns, error handling issues and concurrency issues. While systems can experience and cause their own vulnerabilities, human error can also be the main root cause of a vulnerability. Such vulnerabilities include insecure data handling, weak credentials, stolen credentials, the failure to update software, and misconfigurations. Systems that have critical vulnerabilities are exposed to system failures, security breaches, ransomware attacks, and other cyberattacks. These are all major cybersecurity vulnerabilities that can completely handcuff an organization if they are not properly addressed.

**How do you know it's a problem?**

Research has shown that cybersecurity vulnerabilities within an organization can cause them to potentially be affected by a variety of system and network failures, electrical failures, data breaches, and cybersecurity attacks. These attacks can cause organizations to experience major financial and reputation losses depending on the severity of the attacks and breaches. Large organizations who experience a cybersecurity attack can experience a scenario where the price tag to rectify such cybersecurity event, for example a ransomware attack, can be in the five to seven figure range. If government organizations, such as those related to the miliary, experience a data breach or another form of a cyberattack, military equipment may fail, and national security secrets may be stolen and encrypted. Cybersecurity vulnerabilities do not discriminate as to when they may arise. Small and big businesses, government and nonprofit organizations, and civilians can suddenly deal with a cybersecurity vulnerability, and the ramifications can be huge.

**What are going to do about the problem?**

The remedy that we are proposing is a form of software that will help solve these problems by being able to generate a report to let clients know what vulnerabilities are present anywhere in the machine and in the network. The report will detail what specifically is causing the vulnerability or vulnerabilities, such as outdated software or if there is a buffer overrun and how to resolve them. Some vulnerabilities may have the ability to be solved in a quick and timely

manner, while others may take a long time to remedy. As mentioned, human error can lead to the formation of a vulnerability, and the report will indicate if that is the case. This is important because the organization can use the report as a training tool to help educate employees as to why it is important that they practice proper cybersecurity etiquette and continue to maintain systems and networks.

**What barriers do you expect to confront?**

The first major barrier I anticipate confronting is being able to find and train the right employees to help develop the software. Our team will need a reliable workforce that is educated on the necessary language and technology that is required for the software to be developed properly. This barrier ties into another barrier that I expect to confront, which is keeping up with and informing employees of the ever-changing software requirements. Unclear software requirements can lead to a big waste of time and money, and a clear vision on the scope of the project will help the workforce maintain an understanding of the requirements for the project. We will need to consistently communicate the expectations between the ideation and development teams. Creating a prototype will also be helpful in determining what the final product will be when it is available for purchase. Another barrier that I expect to confront is the need to maintain quality assurance and have properly defined quality standards, as broken code and software bugs may become a major issue throughout the development of the software. Code will need to be consistently reviewed and tested in order to ensure that the software will execute its task properly without errors, and in a way that will be convenient for the customer. Consistent software testing will also be necessary and will go hand in hand with code testing so that any issues that may arise can be resolved in a timely and efficient manner. Data breaches and other potential cyber events are another barrier that I expect to potentially confront. A strong security system will need to be in place when working with the software in order to prevent any breaches while we develop the software and while the customer possesses the software. Finally, a major barrier that I expect to confront is the ability to maintain our budget and not go overboard with our expenses. We need to maintain a cost-effective development process that is not too expensive but is also efficient in crafting the software exactly how we seem fit. This will be key to help us achieve our goals and be successful.

**How will you know if you are successful?**

I will know that I am successful and have achieved success if the software sells well, fits the specific needs of the clients, helps to eliminate vulnerabilities, can be used as a training tool, is used by many clients, and the clients provide us with positive feedback about the software. Making a profit, knowing that every facet regarding the software is operating at a high level of efficiency, and having a happy team will help bolster my success. Being able to achieve personal goals such and happiness are also key factors that will help me know that I am successful. Having our product become a “name brand” and a “necessity” for current and future clients will be yet another indicator that I have achieved success. Finally, I will also know that I have

achieved success when the software leads to organizations wanting us to negotiate a contract with them, in essence turning us into a supply vendor for them.

References:

Thakkar, M. (2022, January 9). *10 software development challenges every developer faces*. Synoptek. https://synoptek.com/insights/it-blogs/10-challenges-every-software-product-developer-faces/