## Conclusion

9. Were you able to stay relevant and objective throughout?

10. Did you maintain an objective voice?

To conclude the research gap of assessing software vulnerabilities on the black market, I have presented the urgence in both companies and individuals of this rising dangers of software vulnerabilities in our society today. These vulnerabilities are being that conducted by black hat hackers who are buying and trading on the black-market for what we presume to be a financial reward or satisfaction. In my research I’ve taken eight research articles of the most significance over the past decade to grasp an understanding at where we stand today with these vulnerabilities on the black market. This research is a collective literature review of all eight scholarly sources to present a research gap in the field of assessing software vulnerabilities being present on the black market. The literature review of these articles consists of the explanation of the software vulnerabilities and black-market correlation, the ideas/theories of a legal market, as well as the possibility of machine learning defenses, and predictions against these software vulnerability attacks being conducted and found on the black market. I find this structure to be throughout the research gap and is by far the most logical formation, being able to give an understanding of what we know with the software vulnerabilities and the black market, where we are at in this research of a legal market, and finally a possible future solution or future research into more of stopping these attacks rather, there is a two market system or no legal market at all. Through this research I was able to gather a decade of information about where we currently are in the legal market, what theories/test have been conducted, what we know about the illegal market trade, and what we have proposed and are testing with the legal market and illegal market comparisons. Both modern studies conducted this year in 2022, and further research dating back to 2007 have been studied, analyzed, and assessed in this research paper showing the depth of understanding prior, present, and possibly future knowledge of software vulnerabilities currently on the black market as well as the transition/ acknowledgement of the legal market trading with a rewards system. Through my research we can conclude and note that while reading these scholarly articles that we have found a strong correlation between the vulnerability lifecycle and the lifecycle of the illegal market. We can also conclude through our research that the strong correlation between the emergence and growth of the black market has caused a rise in the zero-day exploits that companies are suffering from today. It is important to also note while reading what other researchers have presented such as offering ideas and theories about a legal market as well as possible machine learning techniques in defense of these software vulnerability exploits. Although we have seen a shift towards a legal market already with companies taking on the model of offering financial rewards for vulnerabilities found in their software considering the still active black market. These models have encouraged a deeper understanding in what that we need to create a new vulnerability market that are suitable for the different types of vulnerability discoverers, the markets should be legitimate, attractive, and easy to deal with, so they are a good income source for both sellers and buyers. Lastly, studying the rewards buyers give to sellers should be reasonable, depending on supply and demand and other commercial market concepts.

Looking into a legal market we have identified that there is pros and cons to implementing this type of market. Although this seems like the easiest safest options there is some speculation that draw concerns for having a legal market. There is statistical data stating that with a legal market the information being transaction on the black market does decrease but through simulations it shows a decrease in our software security, and parching rates as well. Although with a legal market we do lack a lot of real-life statistical data that represents the markets transactions the idea of a legal market is still in the top running for solving the issue of software vulnerabilities on the black market. If the idea and theory of a legal market never come to be there is another idea in the works of stopping these software vulnerabilities on the black market, and that is machine learning techniques such as monitoring and a new scoring system to rank vulnerability threats. With the new metric that can be used for earlier detection and as an indicator, as well as a developed model that uses machine learning to predict rather a vulnerability is likely to be exploited or not, along with the black-market monitoring concluding that patching strategies based on black market observations can be much more effective than those based on the traditional CVSS score by average of 20% (Allodi et al.,2013). We are left with the research gap of sufficient, reliable, effective statical data that can provide in both fields of legal and illegal markets. To ensure the correct effectiveness, and efficiently of these defensives for the public and software companies. Taking in these considerations and analyzing other research articles, I have made me drawn my conclusion in this research gap. Following the research from Algarni in two separate papers and years, as well as Younis and Malaiya, state that due to the “dynamically changing field, studies such as this need to be repeated in order to see if there are any observable trends in terms of the vulnerabilities that end up in the legitimate and black market periodically, and the subsequent risks to society”, as well as “the need to collect data about the transactions in the regulated and the unregulated markets so that the processes can be modeled accurately”(2016/2022) (2014). Our biggest research gap is providing actual evidence that is up to date with transactions on both legal and illegal markets as well understanding that in this field our data and content is changing daily and to keep up, we need extensive research with statistical data. This can be challenging though because as stated before it can be extremely difficult to find and track this evidence due to the privacy and limited interactions in the black market that take place in private chats and transactions between the buyer and seller.

With the conclusion of the research paper, there has been both a critical and consistent evaluation in both my synthesis and throughout the paper that have further my research gap. The scholarly articles researched throughout this project have given quality feedback that helped pursue what I conclude is the gap of assessing software vulnerabilities on the black market. Through the paper there has been the object voice of where our research is at in this topic and where one day we hope to be and our studying for. Overall, there needs to be further research on both legal and illegal market transactions, as well as conducting a relevant study on the dynamic changing field to conclude any patterns, attack types, particular users, and most of all an analytic comparison between studies showing any type of similarities between the two markets. Finally, one thing I would like to note and bring attention to is the idea of having both the legal and illegal markets running. Through all the research only one article brough this to my attention and I would heavily consider to doing more research into what would happen if hackers sold on both markets compared to one or the other.