Title of Capstone Here

Author's Full Name Here, Including Middle Initial

Western Governors University

Table of Contents

Summary....................3
Review of Other Work....................3
Changes to the Project Environment.................... 3
Methodology....................3
Project Goals and Objectives....................3
Project Timeline....................3
Unanticipated Scope Creep.................... 3
Conclusion....................3
References.................... 5
Appendix A....................6
Title of Appendix....................6
Appendix B....................7
Title of Appendix....................7
Appendix C....................8
Title of Appendix....................8

Summary

During our project we set out to address the problem of inefficiencies in CTs passive recon phase of our red team engagements. This problem created a slowdown in our operational efficiency. Ignoring this problem would open the door for our competitors to take market share away from us. We sought out to solve this issue by leveraging the powerful capabilities of AI for our passive recon activities. We created and executed a project to automate our process for gathering OSINT data using ai agents. During this project we selected an LLM to run our agents off of, built a database to store collected information, and configured agent managers to run and configure our agents among many other things. At the end of the project we observed a qualitative, and quantitative metric to determine the outcome of the project. Our quantitative metric observed a 35 % decrease in the average time for OSINT gathering after 10 engagements compared to our pre-project levels. On the other hand CTs red team reported that they enjoyed using the new technology, it was more efficient, and it provided them with more data than they previously had compared to the pre-project levels. From observing these two metrics, CT has determined that the project was successful in delivering on solving the problem of inefficiencies in CTs passive recon.

Review of Other Work

Throughout our project we used published works from other industry leaders to assist us in deployment of our new technologies.

Changes to the Project Environment

Prior to this project CT ran a somewhat antiquated but efficient operation with regards to its red team engagements. Traditionally, the OSINT gathering portion passive recon phase of our engagements were done manually and through the use of some scripts. While this was an effective way of gathering OSINT data, it was extremely time consuming. This presented us with the problem of severe operational inefficiency. The project specifically targeted and changed our OSINT gathering process to solve this problem. In the project we stopped digging for OSINT manually and started automating it using AI. We chose an LLM to run our agents off of, we then configured a new database in our environment to send all of the collected data to. Then, we configured agent managers for use by our red team. At the end of the project, our process went from being completely manual to completely automated. These changes to the project environment allowed us to successfully solve our inefficiency problem.

Methodology

Project Goals and Objectives

For our project CT set out to achieve the primary goal of increasing red team operational efficiency. This primary goal had three supporting objectives, “Automate OSINT gathering activities using an LLM”, “Improve quality of OSINT data”, and “Establish continuous improvement for OSINT.” We were able to achieve our primary goal by successfully completing all of our supporting objectives.

CT achieved our first supporting objective “Automating OSINT gathering activities using an LLM,” by completing three key deliverables. We first selected an LLM for our AI agents to use. Then, we configured a database for data collected by our agents. And lastly, we configured our agent managers on our red team endpoints. We successfully completed these three key deliverables which in turn allowed us to achieve our first supporting objective.

We then achieved our second supporting objective “Improve quality of OSINT data.” by completing three deliverables. First, we established a separate database of effective queries and their outcomes. Then, we trained our employees on how to use the agent manager. And lastly, using our LLM we were able to expand OSINT gathering sources. Achieving these three key deliverables helped us complete our second supporting objective.

For our last supporting objective “Establish continuous improvement for OSINT,” CT completed three deliverables. Unlike previous deliverables, these deliverables will need to be considered even after the project ends. These deliverables include “Train our agents over time, Keep our agents and agent manager up to date, and frequently test new queries.” In this project we established a framework to achieve all of these deliverables so that they can continue to be achieved after the project ends.

Project Timeline

For our project we were able to maintain loose coherence with the project timeline. Because of the nature of the agile framework we allowed ourselves to be somewhat flexible with the timeline. For every phase we went a little over and or under the timeframe allotted. For example the implementation phase started and ended earlier than expected due to the development phase not taking as long as we thought it would. Altogether, this means the project ended ahead of schedule. In our original project timeline we expected the project to end on 2025-01-15. The project actually ended on 2025-01-03. The framework selected along with strong team performance and teamwork allowed us to achieve this.

Unanticipated Scope Creep

Throughout the project we had one occurrence of scope creep. During our implementation phase the team lost focus and began to start implementing AI into other parts of our workflow. In our implementation plan we specifically state that we would use AI to automate collecting OSINT, not any other parts of the engagement would be automated. While this certainly could be helpful for CT to implement AI into other parts of the business operations, it was not in the plan, thus, it constitutes scope creep. Luckily, due to great teamwork and communication by management and the rest of the team we caught this instance of scope creep and stopped it. We then revisited the implementation plan and maintained coherence to the scope throughout the rest of the project. If we did not catch this instance of scope creep, it could have derailed the project and caused us to miss key deliverables, objectives, or timelines.

Conclusion

With this project we set out to solve the problem of red team operational inefficiencies. To do this we decided to automate the OSINT gathering process using AI agents. After completion of the project we looked at two measures to determine the success of the project. Our quantitative measure was the average time to conduct OSINT gathering. After 10 engagements, we determined that the average time to conduct OSINT gathering had dropped by 35 %. Our qualitative measure was feedback from our red team. For this measure we asked our team questions like, “Do you like the new process?”, “Does it speed up passive recon?”, and “Is it providing you with more valuable OSINT data?” The answers to these questions were resoundingly positive. Our red team loves the new process and our current technologies. Looking back on the project CT is proud of what we accomplished. The employees involved show amazing teamwork, work ethic, and communication throughout the entire process. The project stayed within scope for time, budget, and resources. All things considered, the project was an amazing success.

References

Appendix A

Title of Appendix

Appendix B

Title of Appendix

Appendix C

Title of Appendix