HEIMDALL: A DIGITAL THREAT MANAGEMENT PLATFORM

Final Report

by

Killian O'Connor

For IT Carlow

10/2/2020

Table of Contents

1. Introduction

Heimdall was envisioned as a "Digital Threat Monitoring Platform", in essence this means it was to serve as an aggregator of potential breaches or threats to an organisation found by sifting through freely accessible information on the internet. It was planned to have multiple modules, each providing a different method, technique, or scope for identifying threat. These modules would connect to a standardised core platform. The core goal of Heimdall was to aggregate the functionality of discovering threats by various means into a central solution to reduce the number of tools a security analyst needs, as well as streamline their workflow. A secondary goal was to present this information in an accessible way to both analysts, and executives.

2. Objectives

2.1 Achieved

1. User creation
2. Creating, editing and deleting of user keys
3. Generation and closing of alerts
4. Dynamic access to user keys and target ranges
5. OSINT Scanner
6. Design report templates
7. Implement containerisation
8. Create a DevOps pipeline
9. Maintain code standards

2.2 Not Achieved

1. Report generation
2. Dark web scanner
3. AWS S3 Scanner
4. Account management
5. Local CVE Database
6. CVE Scanner

3. Problems Encountered

3.1 Time

I did not implement proper time management strategies at the beginning of this project. As such, my productivity took a severe hit until I implemented time blocking and a Kanban board. Other life commitments and responsibilities also took up a large portion of time outside of college.

3.2 Leaning new technologies

I choose to challenge myself my attempting to learn multiple new technologies. This on top of the existing work load left me about my working capacity.

4. Learning Outcomes

Overall, I feel I learned quite a lot from this project. Its wide scope exposed me to a lot of research and technologies. I also tried to utilise new technologies to expand my skill set.

4.1 Project Planning

I learned a lot about planning a large software project. I had some knowledge on software engineering from a previous module, however being able to practically apply these principles to a real project was a great asset in learning. My time management skills also greatly increased, however this was near the end of the project and as such they were not used as effectively as they could be.

4.2 Git

While I had some experience with Git, it was restricted to simple coding projects I have undertaken with friends outside of college. Implementing and managing a large repository with multiple branches was a step up and developed my understanding of Git higher than it was before.

4.3 DevOps

Automation and coming to understand the DevOps cycle was important to me, as security teams developing in-house application will generally be small, I can see the potential in DevOps drastically increasing efficiency for both small and large scale teams. In this project, it effectively removed the

pain of switching between developing the application and managing the operations of the backend. Technologies such as Git, GitLab CI/CD, and Docker all played into this learning outcome.

4.4 containerisation

Understanding containerisation and developing containerised application was a key goal I set myself at the start of this project. I was a technology I had absolutely zero knowledge of, and at the end of this project I would say I have a moderate working knowledge. I believe this technology is only going to grow in importance as DevOps and Cloud hosting become more prevalent in software development, and as such I plan to continue my learning on this subject.

4.5 Python

I had some previous experience with Python, but this was limited to small automation tasks and simple code challenges. This project made me dip further into it Python, and I can truthfully say that I enjoy the language. I have purchased “Learning Python” by David Ascher and intend to practice and grow my knowledge of the language further when time becomes available.

4.6 Django

The Django web framework was an interesting task to go about learning. I am used to developing web applications from scratch using technologies such as PHP, and the jump to using a framework was a hard one. I now however, has a good grasp on the fundamentals of Django, as well as some more technically aspects. I feel this will help me greatly in the future as Django seems to be a robust enough framework that, given the application, will allow you to get a web app up in a moderate amount of time.

4.7 Open Source Threat Intelligence (OSINT)

While researching this project I came across many insightful resources on OSINT, as well as shocking potential security vulnerabilities and leaks an organisation may be victim to. I discovered new techniques at engaging in OSINT, as well as some common sites where information can be found. This may prove useful in my future career in security, as it is an aspect a large amount of organisations seem to ignore.

5. What would be Done Differently

5.1 Time Management

Initially I took a very much unstructured approach to this project. I had never dealt with such a large task before. The approach of "just doing things when you can" was very at odds with my college work. Work on the project was put back to work on other closer assignments, this meant that during the time I could do work, only a small proportion was devoted the project initially. As time progressed I began to see the error in this methodology and researched into time management techniques. I began to utilise time blocking in combination with a Kanban board to track my productivity. This greatly increased my output, and is a skill that I deeply wish I had implemented at the beginning of the project.

5.2 Narrowed Scope

As can be told by the functional specification and design manual, this project had a significantly big scope set out from the beginning. In reflection, while I do think the project idea is solid, the workload the idea provided was beyond my capacity. If I were to redo the project over again, I would keep the same core idea of a platform with extensible capabilities and restrict development to one module, maybe two depending on similarity (for example, OSINT Scanner and Dark Web Scanner). A significant amount of time was spent researching and designing functionality which were not able to be implemented in the project. This time could have been better utilised to develop a strong core on top of which new modules could potentially be built in future.

5.3 Read More Documentation Beforehand

Having come to the end of the project, I feel that had I spent more time at the start reading through the documentation of the new technologies I was utilising during the project I would have greatly increased my efficiency and speed of development. This would be in contrast to the reality of the development process, where I would continue with development until a major roadblock at some aspect of the technology and then spend a large amount of time searching for knowledge to overcome the problem. I feel that if I had had a better grasp of the technology at the start of development, I would have substantially more functionality implemented.

5.4 Different Container Orchestration Solution

While Docker-Compose seemed the best solution to managing container interactions at the beginning, the more practical experience I had with the tool the better I saw it's weaknesses at scale and rigid structure of defining container relationships.

6. Testing

The GitLab CI/CD pipeline was utilised to perform build tests on each commit. Should the project pass the "Build" stage correctly it was then moved onto the "Deploy" stage where the Docker containers and relevant files were deployed to remote Digital Ocean servers. Basic manual testing was utilised to confirm the functionality of various aspects of the project. The OSINT Scanner module was tested against a live site, mappa.ie, with the permission of the owner.

7. Conclusion

While overall the project still has a long, but thoroughly planned out, road to the functionality as specified in the documentation, I would classify the project as personal success and a mediocre technical pass. The project did not reach its envisioned state, but the knowledge I gained during its development will be invaluable for any future endeavours. The difficulties encountered with this project will present less of a hazard to future projects.

8. Plagiarism Declaration

I declare that all material in this submission is entirely my own work except where duly acknowledged. I have cited the sources of all quotations, paraphrases, summaries of information, tables, diagrams or other material; including software and other electronic media in which intellectual property rights may reside. I have provided a complete bibliography of all works and sources used in the preparation of this submission. I understand that failure to comply with the Institute's regulations governing plagiarism constitute a serious offence.

Student Name: Killian O'Connor

Student Number: C00212863

Signature: _____Killian O'Connor_____

Date: _____20/4/20_____