Automating Security with a Chat Interface

Reflection

Bachelor's degree in Electronica ICT
field Cloud & Cyber security

Jonas De Weerdt

Academic year 2023-2024

Campus Geel, Kleinhoefstraat 4, BE-2440 Geel

LID VAN ASSOCIATIE KU LEUVEN

THOMAS MORE

1 INTRODUCTION

In this document, I will provide a comprehensive reflection on my internship at Actwise NV. The report is divided into two main sections: a substantive reflection on the internship project and a personal reflection on my learning and growth during this period. This document aims to give a detailed and balanced overview of my internship, highlighting both the technical contributions and the personal advancements I have made. It is intended to offer insights into the project's outcomes as well as my professional and personal development journey during this time.

2 SUBSTANTIVE REFLECTION ON THE INTERNSHIP PROJECT

2.1 Project Overview

The main goal of my internship was to enhance security measures using a chat interface. Specifically, I focused on integrating CyberArk Identity Flows with chat platforms like Slack and later Discord. Microsoft Teams could have also been done but this was not chosen because of various reasons.

2.2 Specific Accomplishments

- **Local PAM Environment**: I successfully set up and managed a CyberArk local Privileged Access Management (PAM) environment. These are just local VM's running Windows Server 2019 and have the CyberArk components installed on them.
- **Security Flows Development**: Using Python and CyberArk Identity Flows, I created several Flows:

    - Temporary Access
    - Panic Button
    - Confirming Request
    - Password Recovery
    - Suspicious Activity Detection

2.3 Accomplishments and Impact

- **Client and User Benefits**:
    - Improved security by automating privileged access management and monitoring suspicious activities.
    - Provided administrators with a user-friendly interface to manage security flows and respond swiftly to security incidents. There is already an interface created by CyberArk where all of the actions that I automated could be performed but doing it with a chat interface makes it faster and more responsive.
- **Completion Status**:
    - I have completed all of the predetermined use cases only the use case that I had to create myself wasn't finished because I couldn't find anything useful to implement anymore.

2.4 Project Continuation

Moving forward, the following tasks are planned:

- **Continued Monitoring and Refinement** of the security flows.
- **Integration of Additional Chat Interfaces** or enhancements to the existing Discord bot based on user feedback.
- **Regular Updates** to the PAM environment to stay compatible with the latest CyberArk features.

2.5 Implementation and Usage

- **Current Use**:
  - Although the system I created won’t be used in production, it serves as a convenient showcase for potential clients.

3 PERSONAL REFLECTION

This internship helped me achieve personal value through the real exposure toward a professional environment, especially in the field of Privileged Access Management. Throughout the experience, I came to learn much about the CyberArk tools and how they could be integrated into other technologies. In addition to this, I developed and also debugged my Python code for my Discord bot.

In this internship, several competencies were addressed. I became more competent in technical skills, especially in Python programming and understanding the principles of cybersecurity. I improved problem-solving skills by developing solutions to integrate different systems and to troubleshoot issues of the same software, resulting in time-outs in responses. At a personal level, I built my ability to independently work and take critical decisions regarding the way forward in the project and tooling choices to be made. I did always ask for feedback after I have made big decisions to make sure I am going in the right direction and not wasting my time on undesired things. My communication skills were also improved through day-to-day interactions with colleagues and through talking with a CyberArk expert.

During the internship, I faced several challenges. On the technical side, I had problems with Slack integration because of outdated system features and constraints on response time. In order to overcome this, I switched to Discord and built a custom bot, which gave me more flexibility and control over the workflow. This choice was supported by Jelle because when I asked he told me that the choice is to me to decide what chat interface I want to use. In the non-technical aspect, time management became tough because I had to make a very big change very late into my internship. I handled the situation by prioritizing based on impact and urgency of tasks and seeking advice from colleagues whenever needed.

On reflection, a couple of areas where feedback could have been obtained and through which further refinements could be made include: for example, getting feedback more frequently while developing the Python scripts to ensure that best practices were followed. Most of the feedback I received for my Python code was about different or extra features and less about the actual code because Jelle is not a developer so code is not where he shines. Every features that he asked me to implement was added and working completely.

4 Conclusion

Reflecting on my internship at Actwise NV, I can confidently say that it was a highly productive and educational experience. I successfully developed and implemented several security flows that have enhanced the organization's cybersecurity measures. Personally, I have grown significantly, gaining valuable skills and overcoming various challenges. This experience has prepared me well for future opportunities in the cybersecurity field.