Internship: SOC-project

Reflection

Bachelor's degree in the Electronics-ICT
Cloud & Cybersecurity

Baisangur Dudayev

Academic year 2024-2025

Campus Geel, Kleinhoefstraat 4, BE-2440 Geel

Table of Contents

1.1 Introduction

This reflection is about my 13-week internship at Netcure. I will explain what I worked on, what I learned, and how I experienced the internship.

1.2 Project Summary

What did I work on?

- I worked on setting up Elasticsearch and Logstash for the SOC and making sure the logs were retrieved, processed and sent to Elasticsearch.
- I wrote Ansible playbooks to install and update the servers and Docker containers.
- I made a Python script that creates HTML and PDF reports from Guardian360 logs in Dutch, French, or English for the companies' customers.
- I set up n8n & an Nginx reverse proxy and automated alerts using an n8n workflow.
- I installed TheHive & Cassandra and connected them to Elasticsearch and Nginx.

Is the project finished?

- A SOC can always be improved upon
- One thing that was planned to be implemented and that I would have liked to further is the ticketing system for the analysts.

Is it used by others?

Yes. Some employees already used the information in the dashboards during the internship.

Advice for the company:

Keep updating the documentation after making changes.

1.3 My Experience

What did I learn?

- How to use ELK stack, Ansible, Docker, and n8n.
- Writing Python scripts and working with APIs.
- Working in a team and meeting deadlines.
- Asking for help when stuck.

What was hard?

The 3-hour daily commute was tiring. And the work itself required constant research of the technologies needed.

Learning new tools like Nginx and TheHive took time, but I figured it out by testing and reading.

Biggest lesson?

Besides my technical skills, I learned to manage my time better, divide tasks and understand my motivations a little better. I also gained more confidence in my technical skills.

1.4 Conclusion

The SOC I helped build works well and is useful. I learned a lot and improved my skills. It was a good internship, and I should be thankful for the opportunity.