THOMAS MORE

Netcure SOC Project

Personal Reflection

Baisangur Dudayev
Bachelor Electronics-ICT - Cloud & Cybersecurity

2024 - 2025

Table of Contents

1. Introduction

This reflection is about my 13-week internship at **Netcure**, a cybersecurity company where I contributed to the creation of a new **Security Operations Center (SOC)**. In this document, I reflect on the tasks I carried out, the challenges I faced, the skills I developed, and how I experienced this internship both professionally and personally.

2. Project Summary

What did I work on?
During my internship, I contributed to several core components of the SOC:

- Setting up and configuring **Elasticsearch** and **Logstash** to collect, process, and store logs.
- Developing **Python scripts** to retrieve data via APIs (Guardian360, CyberAlarm), clean it, and make it ready for ingestion.
- Writing **Ansible playbooks** to automate installation and updates of servers and Docker containers.
- Creating an automated **reporting system** that transformed Guardian360 scan results into interactive **HTML** and archive-friendly **PDF** reports.
- Deploying **n8n** with **Nginx** as a reverse proxy and building workflows to automate alerts and notifications.
- Installing and configuring **TheHive** and **Cassandra**, integrating them with Elasticsearch and Nginx to provide incident management capabilities.

Is the project finished?
The SOC was functional at the end of my internship, but it will always remain a **work in progress**. Security environments constantly evolve, and there are always improvements to be made. For example, one planned addition I would have liked to contribute more to was the **ticketing system** for analysts, which would have further streamlined incident tracking.

Is it used by others?
Yes. Even during my internship, analysts and employees were already using dashboards and reports produced by the system. This gave me direct feedback and motivation, since I could see my work making an impact in real time.

Advice for the company:
My advice would be to **keep updating documentation** whenever changes are made. Because so many tools were integrated, accurate documentation is crucial to ensure that new team members can quickly understand the workflows and that the system remains maintainable over time.

3. My Experience

What did I learn?
This internship was a steep learning curve but also a very rewarding one. On the technical side, I learned to work with powerful tools such as the **ELK Stack, Ansible, Docker, n8n, Nginx, and TheHive**. I gained significant experience writing **Python scripts** and interacting with **APIs**, which helped me improve my problem-solving skills.

On a personal and professional level, I learned how important it is to **plan my time, divide tasks**, and keep communication clear within a team. I became more confident in **asking for help** when stuck, and I noticed that doing so often sped up problem-solving and improved team efficiency.

What was hard?
The internship was demanding both physically and mentally. The **three-hour daily commute** was exhausting, and it forced me to manage my energy levels carefully. Technically, the hardest parts were the constant research needed to make unfamiliar technologies work together. For example, setting up **Nginx as a reverse proxy** and integrating **TheHive with Elasticsearch** required a lot of trial-and-error, as official documentation was sometimes limited.

Biggest lesson?
The biggest lesson I take away is that building complex systems like a SOC requires both **technical depth** and **teamwork**. I learned that I can adapt quickly to new technologies by testing, reading, and staying persistent. Just as importantly, I realised the value of collaboration and **sharing knowledge with teammates**. Personally, I gained more **self-confidence** in my technical abilities and a clearer understanding of my motivation to work in cybersecurity.

4. Conclusion

Looking back, I am proud of the contribution I made to Netcure's SOC. The system I helped build is already useful to employees, and it gave me valuable hands-on experience in cybersecurity operations. I significantly improved my technical skills in areas like automation, scripting, and system integration, while also growing in teamwork and self-management.

Overall, this internship was a very positive experience. It confirmed my interest in working in cybersecurity, and it gave me both the knowledge and the confidence to continue developing in this field.