THOMAS MORE

SOC-project

Project plan

Baisangur Dudayev
Bachelor Electronics-ICT - Cloud & Cybersecurity

2024 - 2025

Table of Contents

1. Internship company

1.1. Presentation internship company (BRIEF)

The internship took place at Netcure, a cybersecurity firm specializing in providing tailored security solutions to protect businesses against cyber threats. The company is located at Da Vincilaan 1, 1930 Zaventem. Netcure is a relatively small organization with a total of 11 employees. Despite its size, the company plays a significant role in the cybersecurity sector through its specialized services and focused team structure.

1.2. Relevant aspects for the internship / Situation internship within the organisation

The internship is situated within the Security Operations Center (SOC) department. This department is part of Netcure's technical cybersecurity division, where it plays a key role in monitoring, detecting, and responding to security incidents.

2. Assignment

2.1. Reason and background

a. Situation before the internship assignment
    i. Prior to the assignment, Netcure identified challenges in efficiently collecting, processing and visualizing data from various security solutions installed at client sites.
b. The problem or opportunity
    i. Netcure's customers have multiple cybersecurity solutions installed. Currently the logs from only one of those solutions is being collected, because of this log aggregation and correlation is not possible. There are also limitations to the visualization, e.g., if a security analyst reviews an alert, other analysts can't see who reviewed it. There is also a lack of automation and AI used to generate reports and handle incidents. Generating reports for phished emails from their internal phishing campaign requires a lot of manual effort. All the alerts that are generated from the 1 security solution that retrieves logs (which isn't enough info for incident response) are also responded to manually.

2.2. Objectives

Due to the European NIS 2 Directive, there's an increasing need for continuous monitoring. This regulation mandates organizations to have real-time monitoring systems to detect cyber threats, making cybersecurity a proactive and ongoing operational necessity. Through this project, we will provide the necessary tools and systems to help organizations meet these requirements.

c. What should be realised at the end of the internship
    i. The final product
        1. A Security Operation Center (SOC) That has a fully-fledged Security Information and Event Management (SIEM) system in place. Besides this

there will also be AI/automation to automate processes in the SOC and make them more efficient.

ii. What should be 'finished'.
    1. The new fully fledged SOC which will be made from scratch.

iii. What the result should contain
    1. Logs aggregation
    2. Logs correlation
    3. Visualization
    4. Incident response
    5. Reports
    6. Automation and AI etc.

iv. characteristics the result must meet
    1. Basic configuration of the SIEM should be present. Logs should be retrieved, filtered and aggregated. The logs must be shown in dashboards and visualizations.
    2. reports must be made automatically instead of manually.
    3. AI must be integrated into SIEM for alerting and log correlation.
    4. emails reported for phishing must be retrieved (MISP).
    5. Integrating feeds from CCB and other intelligence sources.
    6. Integrating Ticketing solution to follow up incidents.

2.3. Business case

d. Situation after the internship assignment: what benefits will be experienced after the internship assignment will be realised.
    i. When the fully fledged soc has been realised Netcure will have improved efficiency, reduced response times, and enhanced accuracy in threat detection.

e. the result described result above is needed.
    i. The assignment addresses the need for operational efficiency and effectiveness in managing increasing volumes of security alerts.

f. Added value for the company.
    i. Enhanced SOC capabilities will strengthen Netcure's service offerings, leading to increased client satisfaction and potential business growth.

g. The link between the assignment and business objectives.
    i. The project aligns with Netcure's objective to provide cybersecurity solutions. The target groups are both Netcure’s internal security and the security of its customers.

3. Planning

3.1. The steps for implementation with TIMING

i. WEEK 1-5 24-28/03 Basic SIEM
    1. 14-21/03 project plan presentations with feedback

ii. WEEK 6 04/04 SIEM Reporting/Visualization

iii. WEEK 7-9 18-25/04 SIEM AI/automation
    1. 20/4 project plan presentation with feedback

iv. WEEK 10-11 2-9/05 MISP

v. WEEK 12 16/05 OpenCTI

vi. WEEK 13 23/05 Ticketing solution

3.2. Who does what

- Mustafa Moiz & Usama Bin Naseer.
  - Main focus is the visualization of the logs.
- Me and Bryan.
  - Main focus is retrieving, FilterIng and outputting the logs; making scripts etc.
- A task board is used to track contributions. Since we are working on the project together, it's difficult to assign tasks in advance, but it becomes easier to see who has completed what afterward.

4. Risk analysis and project delineation

1. **Assignment after internship**
   a. Risks to be considered by colleagues when continuing to work on the project
      i. The developed scripts may require ongoing maintenance and updates.
      ii. Potential compatibility issues with future system updates.
   b. Information that should be passed on
      i. The documentation will explain the logic behind our code and setup, including the reasons behind certain decisions. It will cover things like the system architecture, key configurations, and any challenges we ran into. We'll also include troubleshooting steps and recommendations for improvements, so the team can easily understand and build on our work.
   c. Up to what point do you work on the assignment and when does someone else take over?
      i. I will work on the assignment throughout my internship, ensuring the system is functional. Before leaving, I'll document all steps and any remaining tasks. Afterward, the SOC team will take over for maintenance and improvements.
2. **General risks**
   a. Possible risks include customer data leakage and accidental damage to the environment hosting the SIEM.

5. Information gathering & reporting

5.1. Weekly overview

For the proper execution of your assignment, it is important that you keep your internship supervisor and internship tutor informed of its progress.

a. With what frequency will you do this?
   i. It will be done weekly.
b. Under what form?
   i. The updates will be shared in written form, either as a detailed journal entry or a summary report outlining the tasks completed, challenges encountered, and any feedback received.

5.2. Follow-up at the internship site

Is there any regular / structured follow-up at your internship site: Jira, Scrum meetings, daily / weekly follow-up meeting with ...

There is a structured follow-up at the internship site through weekly meetings where one of the interns presents our progress. Additionally, we use a GitHub task board to manage our tasks, with sections for "To Do," "Doing," and "Done," allowing everyone to track who is working on what.

6. Project organisation

6.1. Reporting

a. Who do you report to within the organisation?
    i. Marieke (Internship Mentor)
    ii. Tosin (Security Analyst coaching the interns)

6.2. Collaboration

b. Who are you working with on this assignment? State functions/roles in the project initially and then names.
    i. visualization of the logs
        1. Mustafa Moiz & Usama Bin Naseer
    ii. retrieving, filtering and outputting the logs; making scripts etc.
        1. Me and Bryan
c. when do you sit together? What do you do separately? Not doing everything together.
    i. Bryan and I sit next to each other, while the other two interns sit across from us. The four of us, along with Tosin, our project coach, always work together in the same room.