Netcure SOC Project

Project Plan

Baisangur Dudayev
Bachelor Electronics-ICT - Cloud & Cybersecurity

2024 - 2025

Table of Contents

1. Internship company

1.1. Presentation internship company

The internship takes 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

2.1.1. Situation before the internship assignment

Prior to the internship assignment, Netcure faced challenges in collecting, processing, and visualizing data from the different security solutions installed at client sites. Within the SOC environment, alerts and notifications were fragmented across multiple platforms. This fragmentation limited visibility, made it harder to correlate incidents, and slowed down incident follow-up.

2.1.2. The problem or opportunity

Netcure's customers typically have multiple cybersecurity solutions installed, but at the time, the current SOC was only collecting logs from a single solution. This meant that:

- Log aggregation and correlation across different tools was not possible, leaving analysts without a complete view of threats.
- Visualization was limited, both because it was restricted to the single data source and because collaboration features were missing (e.g., if one analyst reviewed an alert, this was not visible to others).
- Reporting — from both the installed security solutions and phishing reports submitted by customers — required significant manual effort.

This situation revealed both a problem (inefficient SOC operations) and an opportunity: to design and build a comprehensive SOC from the ground up, equipped with modern SIEM, automation, and AI-driven capabilities.

2.2. Objectives

2.2.1. The final product

A fully operational Security Operations Center (SOC) with a comprehensive Security Information and Event Management (SIEM) platform at its core. The SOC should:

- Collect and aggregate logs from multiple security solutions.
- Correlate events across platforms to provide a unified view of incidents**.**
- Generate reports automatically and consistently.
- Include automation and AI to streamline SOC processes and increase efficiency.

2.2.2. What should be 'finished'.

The goal is to deliver a production-ready SOC environment, built from scratch, with:

- A configured SIEM that is able to retrieve, filter, and visualize logs.
- Aggregation pipelines and dashboards tested and functional.
- Automated reporting and ticketing workflows operational.
- Documentation and best-practice guidelines for ongoing use.

2.2.3. What the result should contain

- Comprehensive log aggregation from all relevant security platforms.
- Log correlation to detect links and patterns across sources.
- Real-time visualization dashboards for situational awareness.
- Structured incident response workflows to handle alerts effectively.
- Standardized reports generated automatically for both internal and client-facing purposes.
- Automation and AI integrated into log analysis, correlation, and reporting.

2.2.4. characteristics the result must meet

- A functioning SIEM setup capable of retrieving, filtering, aggregating, and displaying logs.
- Reports must be automatically generated instead of manually compiled.
- AI must be integrated to enhance alerting and correlation capabilities.
- Phishing emails must be retrieved and processed automatically through MISP.
- External intelligence feeds (such as CCB and others) must be integrated.
- A ticketing system must be included for structured incident follow-up.

2.3. Business case

2.3.1. Situation after the internship assignment: what benefits will be experienced after the internship assignment will be realised.

When the fully fledged SOC has been realised, Netcure will benefit from:

- **Improved operational efficiency**, as centralized log collection and automated workflows reduce the manual workload for analysts.
- **Faster incident detection and response**, enabled by log correlation and automated alerting across multiple platforms.
- **Higher accuracy in threat detection**, as a complete overview of security events across different sources minimizes blind spots.
- **Standardised reporting**, ensuring both internal and external stakeholders receive clear, consistent, and timely insights.

This ensures that the SOC operates as a proactive environment, capable of identifying, analyzing, and responding to threats with minimal delay.

2.3.2. why result described result above is needed.

The volume and complexity of security alerts are increasing rapidly, making manual or fragmented approaches unsustainable. Organizations require systems that provide real-time monitoring, automated analysis, and consistent reporting**.**

Furthermore, the European NIS 2 Directive introduces stricter cybersecurity requirements for organizations, particularly in critical sectors. The directive obliges companies to have continuous monitoring and incident response processes in place, supported by proper reporting mechanisms. By implementing this SOC project, Netcure can:

- Ensure compliance with NIS 2 requirements.
- Provide its customers with tools and services that help them meet their own regulatory obligations.
- Demonstrate leadership in delivering modern, regulation-ready cybersecurity solutions.

2.3.3. Added value for the company.

Enhanced SOC capabilities will allow Netcure to expand its **service offerings** and strengthen its market position. Key benefits include:

- **Increased client satisfaction**, as customers gain better protection and clearer insights into their security posture.
- **Operational scalability**, with automation and AI reducing the dependency on manual analyst work.
- **New business opportunities**, as regulatory-driven demand (e.g., NIS 2 compliance) creates growth potential for managed SOC services.

2.3.4. The link between the assignment and business objectives.

The project directly supports Netcure's overarching objective of providing comprehensive cybersecurity solutions to its customers. By building a fully functional SOC, Netcure is:

- Strengthening its own internal cybersecurity operations.
- Providing customers with advanced monitoring, reporting, and compliance tools.
- Aligning its services with business objectives, namely: improving security outcomes, supporting regulatory compliance, and fostering long-term client relationships.

3. Planning

3.1. Steps for implementation with timing

Weeks 1-5 (24/02 - 28/03): Basic SIEM setup

- Initial SIEM configuration, log retrieval, and basic aggregation.
- 14-21/03: Project plan presentations with feedback.

Week 6 (31/03 - 04/04): SIEM Reporting and Visualization

- Development of dashboards and reporting functionality.

Weeks 7-9 (07/04-25/04): SIEM AI/automation

- Implementation of AI and automation for alerting and correlation.
- 20/4: project plan presentation with feedback

Weeks 10-11 (28/04 - 09/05): MISP

- Implementation of threat intelligence sharing using MISP.

Week 12 (12/05 - 16/05): OpenCTI

- Deployment of OpenCTI for enhanced threat intelligence correlation

Week 13 (19/05 - 23/05): Ticketing solution

- Integration of a ticketing platform for structured incident follow-up.

3.2. Who does what

Mustafa Moiz & Usama Bin Naseer *(Thomas More Mechelen interns)*

- Main focus is the visualization of the logs.

Baisangur Dudayev & Bryan Wouters *(Thomas More Geel interns)*

- Main focus is retrieving, FilterIng and outputting the logs; making scripts etc.

A shared task board is used to track contributions. Since the project is highly collaborative, tasks are not strictly assigned in advance. Instead, responsibilities are divided dynamically, and the task board provides visibility into progress and completed work. In addition, a personal day-by-day internship journal is maintained, which provides an extra layer of accountability and helps track individual tasks and progress throughout the project.

4. Risk analysis and project delineation

4.1. Assignment after internship

4.1.1. Risks to be considered by colleagues when continuing to work on the project

- The developed scripts may require ongoing maintenance and updates to remain functional as systems evolve.
- Compatibility issues could arise due to future system or software updates.
- Incomplete or unclear documentation could create difficulties in maintaining or expanding the solution

4.1.2. Information that should be passed on

Comprehensive documentation will be delivered to ensure smooth continuation of the project. It will include:

- **System architecture** and how different components interact.
- **Key configurations** and their purpose.
- **Rationale behind design choices**, explaining why specific approaches were taken.
- **Challenges encountered** during implementation and how they were addressed.
- **Troubleshooting steps** for common issues.
- **Recommendations for improvements** and possible next steps.

4.1.3. Up to what point do you work on the assignment and when does someone else take over?

- I will work on the assignment throughout my internship, ensuring the system is functional. During the internship and before leaving, I'll document all steps and any remaining tasks. Afterward, the SOC team will take over for maintenance and improvements.

4.2. General risks

Customer data leakage, either through misconfiguration or unintended exposure.

Accidental damage to the environment hosting the SIEM during testing or deployment.

Performance issues if large volumes of logs exceed initial capacity planning.

Security risks introduced by third-party integrations (e.g., APIs, connectors) if not properly secured.

5. Information gathering & reporting

5.1. Weekly overview

For the proper execution of the internship assignment, it is important that both the internship supervisor at Netcure and the school tutor are regularly informed about the project's progress. To achieve this, updates will be provided on a weekly basis**.**

These updates will take the form of a written internship journal, in which I will document the tasks completed.

5.2. Follow-up at the internship site

At the internship site, there will be a structured system for follow-up. Each week, one of the interns will present the team's progress to the mentor, after which feedback and next steps will be discussed. In addition, the team will make use of a GitHub project board with the columns "To Do," "Doing," and "Done." This provides a clear overview of task distribution and status, ensuring that everyone can track the workflow and responsibilities within the project.

6. Project organisation

6.1. Reporting

During the internship, I will mainly report to Tosin, the security analyst who is coaching the interns on the SOC project. He will provide daily technical guidance, assign tasks, and review progress. In addition, I will also report to Marieke, my official internship mentor at Netcure, who follows up on the broader internship framework and ensures alignment with the school's requirements. This structure allows me to receive both detailed technical coaching and general internship support.

6.2. Collaboration

The project will be carried out in collaboration with three other interns. At the start of the internship, the tasks are divided as follows:

- **Visualisation of logs**: Mustafa Moiz and Usama Bin Naseer (Thomas More Mechelen)
- **Retrieving, filtering, and outputting logs; writing scripts**: Baisangur Dudayev and Bryan Wouters (Thomas More Geel)

Although these focus areas are defined, the project is highly collaborative. We will regularly assist one another when issues overlap, ensuring knowledge is shared across tasks.

All four interns will work together in the same room at Netcure, with Bryan and myself sitting next to each other and the two Mechelen interns across from us. This setup encourages constant communication and teamwork. Tosin will also be present with us in the room throughout the internship**,** acting as our coach and first point of contact. He provides continuous guidance, answers technical questions directly, and helps us overcome challenges as they arise. While certain tasks will be carried out individually, such as developing scripts or creating dashboards — key decisions and problem-solving moments will be handled collectively to maintain consistency in the SOC's overall design and implementation.