Plan Of Action

INTERNSHIP 2025 - CEGEKA

JARNE WILLEMS

Bachelor in Electronics - ICT

Specialization: Cloud and cybersecurity

Academic year: 2024-2025
Thomas More Campus Geel
Kleinhoefstraat 4
2440 Geel
Belgium

LID VAN ASSOCIATIE KU LEUVEN

TABLE OF CONTENTS

1 INTRODUCTION

This document contains the plan of approach for my internship assignment at Cegeka during the period from **February 24, 2025, to May 23, 2025.** In this document, I provide an introduction to Cegeka, background information about the assignment, and an explanation of its content. Additionally, I present my planning for the execution of the assignment and describe the final product that will be delivered.

2 Who is Cegeka

Cegeka is an international IT company **specializing in digital solutions, IT consultancy, and managed services.** The company was founded in 1992 and has its headquarters in Hasselt, Belgium. Cegeka offers a wide range of IT services, including cloud solutions, cybersecurity, software development, data analysis, and IT infrastructure management.

With a **strong focus on innovation and customer-centricity**, Cegeka supports organizations in various sectors, such as healthcare, financial services, government, and industry. The company helps businesses with their **digital transformation** by delivering tailor-made IT solutions and guiding them in optimizing their technological processes.

Figure 1: Cegeka

Cegeka operates in **multiple European countries** and continues to grow through strategic acquisitions and the continuous development of new technologies. Thanks to this approach, the company has established itself as a **reliable partner** for enterprises looking to adapt to the ever-evolving digital world.

For my internship assignment, I am part of the **C-SOR²C** (Cyber Security Operations, Response & Recovery Center) department. This is Cegeka’s modern **SOC** (Security Operations Center) and consists of SOC analysts, CSIRT analysts, vulnerability management engineers, SOC engineers, and more.

3 Description Of the Assignment

My internship assignment is in the field of cybersecurity and will be carried out within the C-SOR^{2}C (Cyber Security Operations, Response & Recovery Center) department at Cegeka Hasselt.

As part of the **detection engineering team**, I will contribute to the development, implementation, or improvement of new and existing detection logic to better identify cyber threats and reduce false positives.

My assignment **focuses on detection rules in both Splunk and Microsoft Sentinel**. Currently, Cegeka uses both as SIEM solutions. The choice between them is largely **determined by customers**—some prefer Splunk over Sentinel, while others opt for Sentinel. This preference can be due to Sentinel being cloud-native or because it integrates better with an existing Microsoft environment.

Figure 2: C-SOR^{2}C

C-SOR^{2}C maintains an overview of all detection rules used in Splunk and Sentinel. These detection rules can produce similar results in both SIEMs, be present in both but yield different results, or exist in only one of the two. Although there is a use case library available, the differences and overlaps between the detection rules are **not yet clearly defined.**

This leads to challenges. For example, if a detection rule exists in both SIEMs but produces different results, it can cause **confusion** for analysts. Additionally, it is difficult to determine which of the two provides the **most accurate detection**. At present, there are discrepancies in what each SIEM detects. Cegeka aims to achieve **equivalent detection coverage across both solutions.**

4 Execution of the Assignment

To ensure the implementation phase runs as efficiently as possible, I have divided this assignment into three phases:

4.1 Phase 1: Inventory of all detection rules

In the first phase, I will create an overview that highlights the **differences between Splunk and Sentinel (in both directions)**. I will check whether a detection rule is already present in both products and mark any differences. The outcome of this step will help determine which discrepancies need to be addressed.

4.2 Phase 2: Verifying if the two rules match

After compiling the overview, if a rule is present in both SIEMs, I **will analyze whether it produces the same result in both Splunk and Sentinel.**
The same detection rule can sometimes lead to different outcomes, which can cause confusion among analysts. By testing and comparing detection rules, I will create a report identifying rules that appear identical on paper but yield different results in practice.

4.3 Phase 3: Researching improvements

Once the overview is complete and discrepancies are identified, I will focus on detection rules that are either **missing or differ** between the two SIEMs. In consultation with my internship supervisor, I will **rank the most important detection rules** and assess whether they should be improved or added if they are currently absent.

During this research, I will evaluate whether **enhancing existing detection rules or creating new ones would add value.**

01
Inventory of all detection rules
02
Verifying if the two rules match
03
Researching improvements
04
Documentation

Figure 3: Phases visualization

Through this research, I will provide my team with insights into where differences exist and deliver a well-founded, prioritized list of detection rules that need to be created or modified **to achieve equivalent detection coverage across both SIEM solutions.**

4.4 Phase 4: Documentation

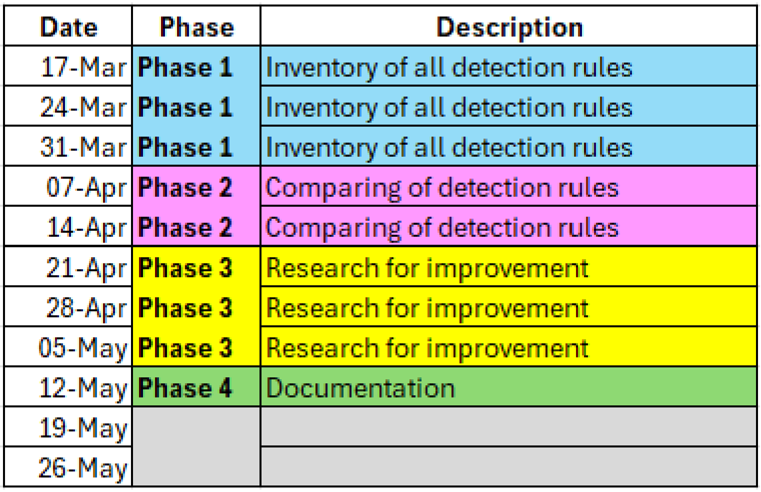
Documentation is often overlooked but is **crucial** when implementing new systems or enhancing existing ones. Proper documentation of the process and a well-structured record of the final outcome will provide **a clear overview** of the steps I took and serve as a guide for my team in making further improvements to the systems.

In this phase, it is essential that the documentation is **clear and precise**. The findings should be well explained, leaving no room for misunderstandings or errors.

Additionally, during this phase, I will ensure that my **bachelor' thesis is properly organized.** This includes compiling my realization document**,** reflection**,** and other mandatory documents required for the completion of my internship.

5 PLANNING FOR THE REALIZATION PHASE

In this chapter, I outline my planning for the implementation phase and provide further explanation of my chosen time allocation.



Date	Phase	Description
17-Mar	**Phase 1**	Inventory of all detection rules
24-Mar	**Phase 1**	Inventory of all detection rules
31-Mar	**Phase 1**	Inventory of all detection rules
07-Apr	**Phase 2**	Comparing of detection rules
14-Apr	**Phase 2**	Comparing of detection rules
21-Apr	**Phase 3**	Research for improvement
28-Apr	**Phase 3**	Research for improvement
05-May	**Phase 3**	Research for improvement
12-May	**Phase 4**	Documentation
19-May		
26-May		

Figure 4: Planning

5.1 Phase 1: Inventory of all detection rules

For this phase, I allocate three weeks. Since a large number of detection rules need to be inventoried, this timeframe allows me to conduct **a thorough and comprehensive analysis.**

5.2 Phase 2: Verifying if the two rules match

Comparing detection rules is time-consuming. Therefore, it is crucial to create a **clear and structured overview** in Phase 1 to ensure that Phase 2 proceeds as efficiently as possible. By having a well-prepared inventory, I can systematically test and compare detection rules in both environments.

5.3 Phase 3: Researching improvements

This phase requires the most time. Conducting a well-founded investigation not only demands knowledge of both Splunk and Sentinel, but also an understanding of daily business processes and team collaboration. This ensures that my research provides real value rather than being just a partially completed internship project for my bachelor's thesis.

5.4 Phase 4: Documentation

I will allocate sufficient time for documentation to ensure **everything is properly recorded**. This includes deliverables for Cegeka, specifically my research findings, as well as the required documents for my bachelor’s thesis, such as my realization document, reflection, and other mandatory reports.

6 FINAL PRODUCT

My team aims to achieve equivalent detection coverage in both Splunk and Sentinel. Through my internship assignment, I will provide **greater insight into the differences between the two SIEM solutions.**

In collaboration with my internship supervisor and the SOC team, I will create a **well-founded, prioritized list of detection rules that need to be created or modified.** The goal is to establish equal detection coverage between both SIEMs. Based on this list and my research, the necessary changes will be made, and new rules will be implemented.

For Phase 1, I will create an **Excel-based list that highlights the differences between Splunk and Sentinel.** This structured approach will give my team a clear overview of where the discrepancies occur.

Phase 2 will involve creating **"Differences Tables"** in Word or Excel to highlight **distinctions between overlapping detection rules.**

Phase 3 will focus on developing a detailed, end-to-end alignment procedure that encompasses all phases and serves as a foundational blueprint for future improvements. Additionally, I will provide recommendations for new rules based on insights gained from aligning the overlapping rules.

For clarity**, identifying new rules based on the entire use-case library is outside the scope of this assignment.**

This analysis and research will bring added value to Cegeka, as it will **directly contribute to improving the service provided to its customers**. By ensuring consistent detection coverage, both SIEM solutions will remain in sync, allowing Cegeka to offer the **best possible service for both Splunk and Sentinel.**

7 CONCLUSION

My internship assignment will provide valuable insights to my team by creating a **well-founded overview of the existing differences between Splunk and Sentinel.** Additionally, I will actively contribute to resolving these discrepancies, ensuring that my efforts as an intern have a real impact.

This process will not only strengthen the team but also enhance my **knowledge and skills in detection engineering.**

I am excited to collaborate with the entire SOC team and look forward to provide value for both Cegeka and it’s customers.

REFERENCES

https://www.cegeka.com/nl-be/over-ons