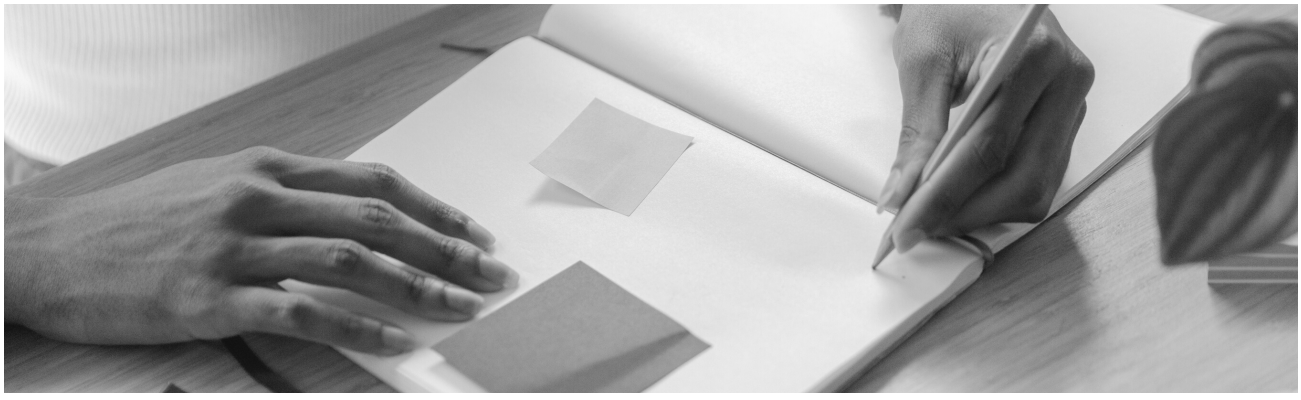


Project Plan

Automating Incident Response through SOAR

Project Title	Automating Incident Response through SOAR
Stakeholders	Niels Pirotte, analists, Cegeka, soc team, klanten van Cegeka
Members	Rune Mannaerts
Start and End Dates	02/27/2023- 05/26/2023

Background

The analysts who work at Cegeka are being inundated with alerts from the command center, which is resulting in some alerts being missed and others being incorrectly judged. That's why I was tasked with creating an AI that can help the analysts complete their job faster, easier, and more efficiently.

To get me started, Niels gave me a couple of things I could focus on, which were three possible ways that I could create an AI model or use an existing one to help the analysts. Now, those three options were ChatGPT, XSOAR machine learning, and a Python library that is made for machine learning and deep learning.

So I started researching these options, and for ChatGPT, it was concluded that because of its inaccuracy and limited potential (stopped learning two years ago), it is not suitable to give an entire answer that is satisfactory to solve the problem.

Because of this, I would recommend using ChatGPT as a supplementary tool to one of the other two models to either train them or to improve their accuracy. However, due to its limited potential, it is not very likely that the CVEs or website's historical data will be correctly linked to the data that is available on the internet now.

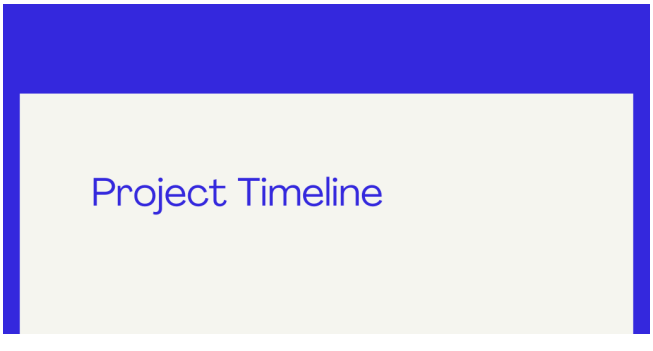
The Python AI model requires a significant amount of time to be trained accurately and improve its accuracy with feedback from human analysts. Due to the time required, it is possible that by the end of the project, the Python AI model may not be up to the standard that it could potentially reach with more time. As a result, my conclusion will be based on the AI model that was trained within the project timeframe, and I cannot guarantee that the conclusion represents the full potential of the model.

Scope

Objectives	Requirements

• Situational analysis of the technologies
• Convert XSOAR's yes/no logic to a smarter logic for intelligent responses
• Possible implementation of a viable and worthwhile solution among the three options, based on the research findings.
• checks python script integration
• additional project: link
	• functional requirements:
	  ○ analyse document
	  ○ use cases
	  ○ One of the following technologies to be used:
	  ▪ ChatGPT
	  ▪ Python Scikit-learn
	  ▪ XSOAR Machine Learning.
	  ○ python script
	  ○ writing new or improving xsoar playbooks
	• non-functional requirements:
	  ○ Accurate
	  ○ performance
	  ○ secure
	  ○ understandable

Timeline



week 1-3

Setting up infrastructure, attending meetings, and creating project documentation. The focus then shifted to training an AI model and gaining experience in AI and machine learning. The intern works with a mentor to receive feedback and refine skills.

week 4-5

Improved incident assessment procedures, developed an incident management playbook, presented a project, took courses in data analysis and Matplotlib, encountered installation issues with demisto-sdk, and created a mind map for the playbook.

week 6-7

Modifications were made to a ChatGPT script, courses on coding skills were taken, and a phishing email classification automation script was worked on. There was also shadowing of an analyst and a meeting to discuss progress in XSOAR playbooks.

week 8

This week, I progressed with automation scripts, worked on a school presentation, and experimented with various tools. Feedback received during the presentation will improve my upcoming bachelor project. Some automation script errors were resolved, while others remain.

week 9

During the week, I worked on a technical project, resolving a script error and researching Openai on Azure. I shared pricing results with Niels and received tips from Dieter on presenting the project details.

week 10

During the week, I completed administrative tasks, had a meeting with Niels, and worked on two scripts for a second project involving XSOAR indicators. With limited documentation, I sought help from colleagues and focused on programming and determining the best approach.

week 11

During the week, I worked on two project scripts and documentation. Despite an expired API trial period, I resolved the issue with colleagues and restored the integration using a new key.

week 12-13

This week, I optimized my scripts, completed documentation, and answered questions during a meeting at school and remotely. I also worked on the documentation for my internship, received feedback, and submitted my documents for the final evaluation with Niels.