

Customizing Cybersecurity Reports Using ChatGPT

Fall 2023

Team Member(s): Pablo Hurtado, Carlos Pedroso, Javier Salgueiro

Product Owner(s): Dr. Masoud Sadjadi

Professor: Dr. Masoud Sadjadi

School of Computing and Information Sciences Florida International University

The problem

**NETWORK
DETECTIVE** 

Automated network scanning tools are pivotal in pinpointing cybersecurity risks for companies; however, they present a challenge with their text-heavy reports. The extensive length and density of these reports may hinder quick decision-making. Furthermore, there is a necessity for enhanced personalization to augment the relevance and usability of these reports.

The solution

To overcome these challenges, we utilized ChatGPT for extracting key insights from reports and incorporating Nextcloud for streamlined development and deployment. To enhance personalization, we included relevant images tied to the insights and introduced the ability to generate company-specific images, providing a more concise and visually impactful cybersecurity reporting solution.

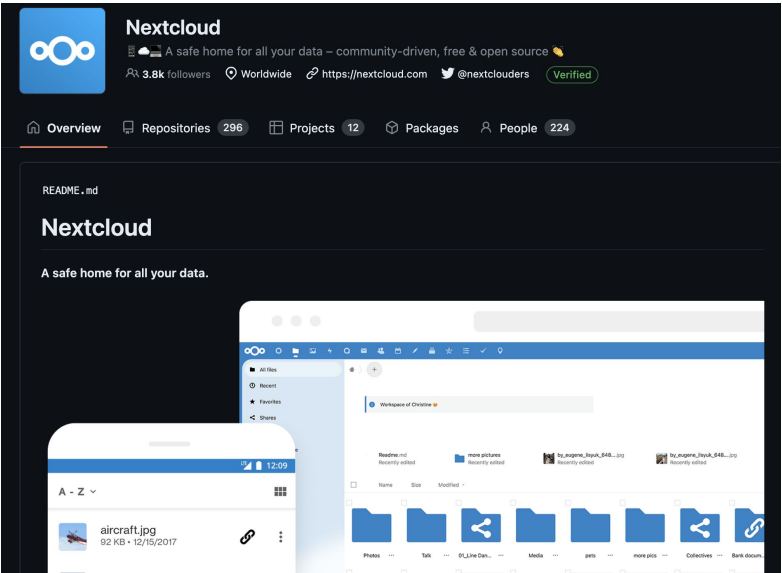


Nextcloud



Setting up NextCloud & using ChatGPT

- We started by cloning the Nextcloud repo and setting it up locally.
- Next, we create an API key to use with ChatGPT.



☒	Name ↑	Image	Status	CPU (%)	Port(s)	Last started	Actions
☒	master		Running (5/5)	0.72%		23 hours ago	
☒	databa 908a5ci	mariadb:10.6	Running	0.03%	8212:3306	23 hours ago	
☒	mail-1 1735c4f	ghcr.io/juliushae	Running	0%		23 hours ago	
☒	nextcl 96c95cc	ghcr.io/juliushae	Running	0.02%	8210:80	23 hours ago	
☒	proxy- b41b30t	ghcr.io/juliushae	Running	0.4%	443:443 Show all ports (2)	23 hours ago	
☒	redis-1 3b2916t	redis:7	Running	0.27%		23 hours ago	

API keys

Your secret API keys are listed below. Please note that we do not display your secret API keys again after you generate them.

Do not share your API key with others, or expose it in the browser or other client-side code. In order to protect the security of your account, OpenAI may also automatically disable any API key that we've found has leaked publicly.

NAME	KEY	CREATED	LAST USED	
Reportenricher	sk - . . . hQdK	Nov 6, 2023	Nov 27, 2023	

Generating insights from uploaded reports

- Implemented document upload.
- Parsing document (gpt word limit).
- Asking chatGPT for insights.



Consolidated Management Plan ▾

Choose File No file chosen

Upload

```
async function askGpt(promptString) {
  console.log("gpt prompt: " + promptString)
  const openai = new OpenAI({
    apiKey: GPT_API_KEY,
    dangerouslyAllowBrowser: true
  })

  const chatCompletion = await openai.chat.completions.create({
    model: "gpt-3.5-turbo",
    messages: [
      {"role": "system", "content": "You are a helpful assistant."},
      {"role": "user", "content": promptString},
    ],
  })

  return chatCompletion.choices[0].message.content
}
```

Consolidated Management Plan

- What is the Consolidated Management Plan?
- What insights are we extracting?

FIU

Consolidated Management Plan

Choose File

Consolidated...gementPlan.txt

Upload

Download Insights




Based on their potential impact and urgency, the first 10 risks that should be prioritized, in order, are:

1. Network Risks:
 - Risk Score: 100
 - Recommendation: We recommend placing adequate password strength requirements in place and remediating the immediate password issues on the identified systems.

```

async function generateImageWithPrompt(prompt) {
  console.log("Image prompt: " + prompt)
  const openai = new OpenAI({
    apiKey: GPT_API_KEY,
    dangerouslyAllowBrowser: true
  })

  const image = await openai.images.generate({
    model: "dall-e-3",
    prompt: prompt,
    n: 1,
    size: "1024x1024",
    response_format: "b64_json"
  });

  return image.data[0].b64_json
}

```


Generating images for the report

- Dall-E setup
- Images based on insights
- Images with company logo

FIU

Ford



Inter Miami C.F



McDonalds



Cybersecurity Reports



Client Health Report

- What is the Client Health Report?
- What insights are we extracting from it.
- How will it be enriched?



Report generation app version: 0.0.1

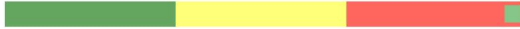
Report Title:
Client Health Report

Industry:
Technology

Key Findings:
Potential password strength risk, Unsupported Microsoft Office version, Anti-Spyware not installed.

Recommendations:
Please review the findings and provide a straightforward solution.

Extra Details:
Use simple examples and use a general tone for those who aren't experts on the subject.

Threat Level:
A horizontal bar chart showing three segments: green (left), yellow (middle), and red (right). The green segment is the largest, followed by yellow, and then red.

The report will be enriched by analyzing its content in relation to current cybersecurity trends, threats, and technologies. Information extracted includes key findings of the report, evaluation of its recommendations against industry standards, and insights on recent cyber incidents and evolving threats. This process also involves integrating additional industry-specific details for a more comprehensive analysis.

Threat level Image Generator

- Setup Dall-E
- Create a Threat level indicator bar
- Each threat level indicates what is the risk associated with
- Generate a prompt for low, medium, and high level threat. This will generate a visual representation of the threat level

The user selects from three threat levels by selecting a color from a threat level indicator bar

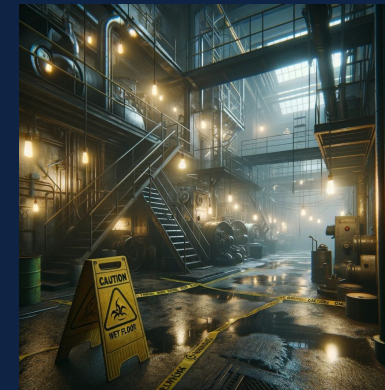
Threat Level:



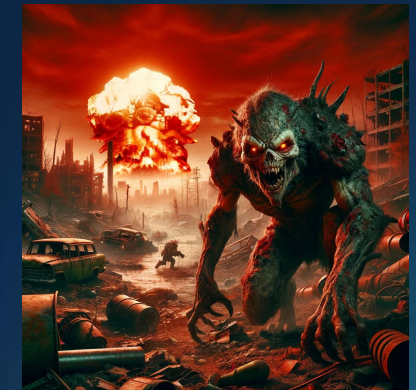
Low



Medium



High



Summary

- Automated network scanning tools face challenges with text-heavy reports.
- Our solution involved ChatGPT and Nextcloud for streamlined development.
- We customized the reports by extracting insights, and adding relevant images and company-specific visuals.