CYBER THREAT LANDSCAPE ANALYSIS

2 weeks work → to 2 hours work for free (Prompt included)

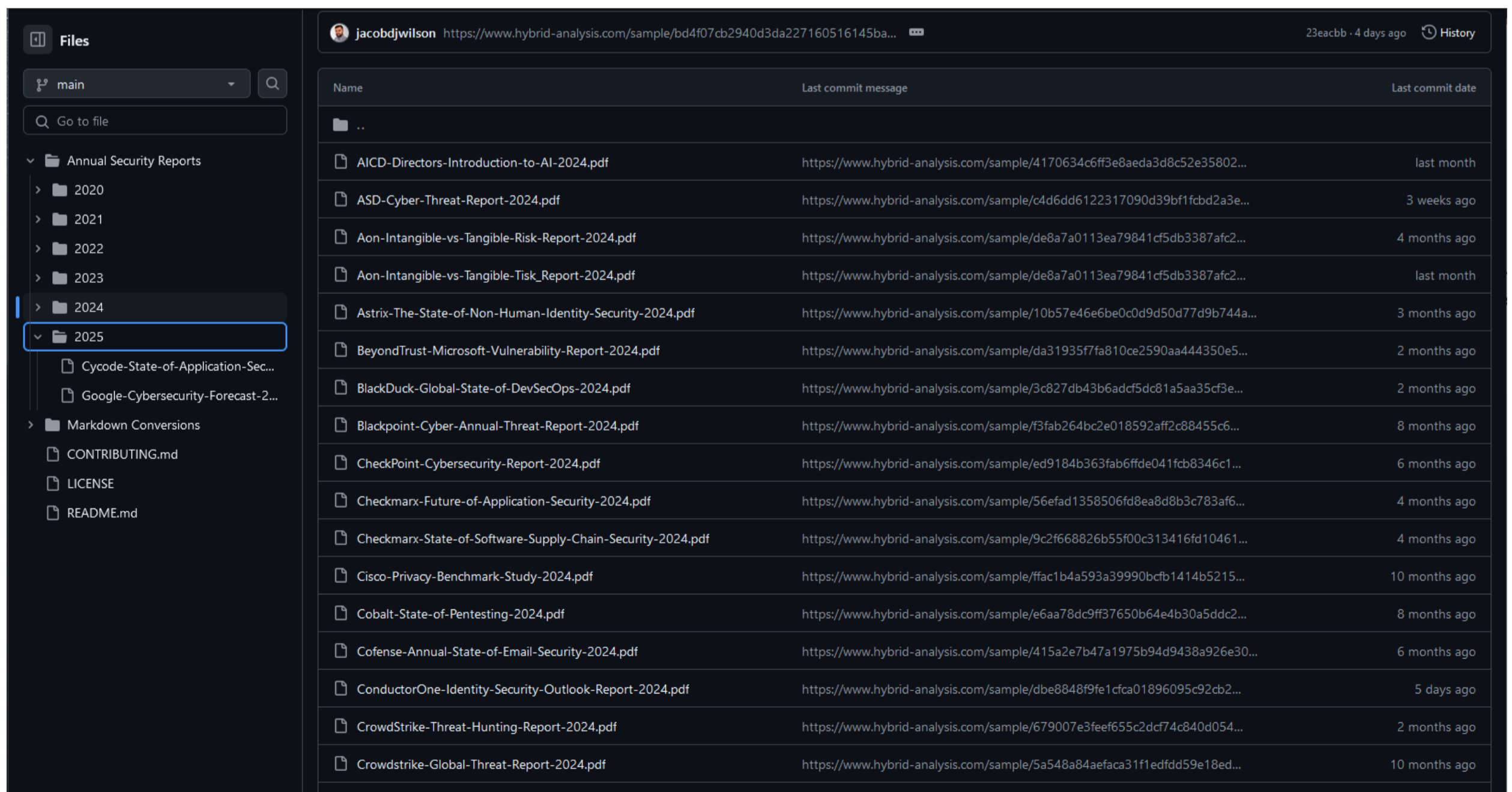Mads Bundgaard Nielsen
LinkedIn.com/in/mbundgaard

4 easy steps

1 Download relevant resources (20 minutes)

2 Upload material and taxonomy to your notebook (5 minutes)

3 Prompt (see page X for suggestions) (5 minutes)

4 Review response and adjust prompts, output and create report (90 minutes)

1 Download resources

→ Download everything you need from <u>one</u> repository.
No submission of data needed. Truly a time saver.

Go to https://github.com/jacobdjwilson/awesome-annual-security-reports/tree/main/Annual%20Security%20Reports/2024

Thank you Jacob D J Wilson!

2 Upload to NotebookLM

→Go to https://notebooklm.google.com

It's a GenAI that provides answers based only on the resources you feed it. It references your sources and helps you perform any type of research. (It can even make you a podcast episode)

→ Create a notebook and upload all your material.

→ Remember to upload/link to your InfoSec Taxonomy.
I recommend VARISframework.org as it is used by Cyentia Institute and Verizon

3 Prompt the material

→ Ask it to provide a summary or specific answer.

I've had splendid results with the following prompt:

Context: Doing an annual analysis of the threat landscape surrounding a specific enterprise.
The enterprise is a [region] [industry] [services] company. It has around [number] employees and annual revenue of [your annual revenue].

Please provide a two-part analysis:
1) A summary of the relevant industry research. The summary must adhere to the [taxonomy] framework. Each section must include examples from the source material and/or statistics such as forecasting or historical changes.
2) A list of the 5-10 most relevant threat scenarios to be included in a subsequent risk assessment. Provide the scenarios in a table format. The table must include the following columns [column 1], [column 2], [column 3] [etc] and strictly adhere to [taxonomy].
(For columns I suggest Threat actor, activity and attribute)

4 Review, adjust & report

You will be provided with a concise response with references, examples and relevant threat scenarios.

But don't stop here. Every analysis has its own specific objectives. Make sure that yours are addressed.

If they are not, adjust your prompt or make new prompts that are more specific to your problem.

Bonus
You now have your own cyber threat intelligence AI.

SUMMARY

1. Download relevant resources (20 minutes)

2. Upload material and taxonomy to your notebook (5 minutes)

3. Prompt (see page X for suggestions) (5 minutes)

4. Review response and adjust prompts, output and create report (90 minutes)

LINKS

1. https://github.com/jacobdjwilson/awesome-annual-security-reports/tree/main/Annual%20Security%20Reports/2024

2. Verisframework.org

3. Notebooklm.google.com

4. www.linkedin.com/in/mbundgaard