PROBLEM

Vulnerability exposes companies to exploitation and breaches

2.6M cybersecurity incidents reported in 2021

Lengthy, dense security documents causes cyber fatigue and hinder updates

Evolving Compliance Standards

Cyber fatigue affects as much as 42% of companies

Cyber fatigue leaves systems vulnerable to potential attacks
INDUSTRY

TURNOVER
21%
Disclosed by companies in 2022\(^1\)

AVERAGE LOSS
$4.4M
In 2023 for a single non-compliance event\(^4\)

OF IT BUDGET
30%
Allocated to security for 8 in 10 companies\(^2\)

UNDERSTAFFED
70%
Reported professionals of their organization\(^3\)

PROBLEM
Our Cybersecurity Copilot:

1. Alleviates Compliance Fatigue
2. Reduces Human Errors
3. Boosts Implementation Efficacy

View Demo
DATA & MODEL SELECTION

DATA
- No public training data
- Scraped 19,000 NIST PDFs
- 2.45GB significant tokens text file
- Limited resources pivot:
  - RAG implementation
  - Vector database
  - PDF upload
  - Chunking strategies

MODELS
- Llama 2
- Falcon 7B Instruct
- Falcon 180B Instruct
- Pegasus-X
- **Mistral 7B Instruct**
- Zephyr 7B Alpha
- Zephyr 7B Beta
- OpenAI (ChatGPT)
Q&A EVALUATION

CHAPTER TOPICS:
- Architecture & Design
- Operations & Incident Response
- Governance, Risk & Compliance
- Threats, Attacks, & Vulnerabilities
- Implementation

RUBRIC
CompTIA practice exam for Security+ with more than a 1000 multiple choice questions and answers

SCORING
50 questions, count correct answers

ADVANTAGE
Industry Q&A pairs mimic language used by professionals
SUMMARY EVALUATION

RUBRIC
Grade summaries systematically based on five criteria

<table>
<thead>
<tr>
<th>Criteria</th>
<th>GREAT</th>
<th>GOOD</th>
<th>OK</th>
</tr>
</thead>
<tbody>
<tr>
<td>RELEVANCE</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>CLARITY</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>COHERENCE</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>LENGTH</td>
<td>✔</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>ACCURACY</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>

SCORING
Scores based on reader discretion of summary generated for NIST.IR.8270

ADVANTAGE
Tailored for our specific use case and expected summaries
# Model Evaluation

<table>
<thead>
<tr>
<th>Model</th>
<th>Q&amp;A</th>
<th>Summary</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mistral</td>
<td>45/50</td>
<td>Great</td>
<td>7B-Instruct</td>
</tr>
<tr>
<td>Falcon</td>
<td>44/50</td>
<td>Great</td>
<td>180B-Instruct</td>
</tr>
<tr>
<td>Llama</td>
<td>45/50</td>
<td>Great</td>
<td>Llama 2-70b</td>
</tr>
<tr>
<td>ChatGPT</td>
<td>50/50</td>
<td>Great</td>
<td>3.5 + Ask YourPDF</td>
</tr>
</tbody>
</table>
## OTHERS VS. SIBYL

<table>
<thead>
<tr>
<th>TASK</th>
<th>OTHER CHATBOTS</th>
<th>SIBYL</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Question &amp; Answering</strong></td>
<td>Relies on outdated and broad-topic data that can lead to inaccurate answers.</td>
<td>Leverages uploaded document and retrieval-augmentation generation (RAG) for precise answers.</td>
</tr>
<tr>
<td><strong>Summary &amp; Checklist</strong></td>
<td>Limited word count results in incomplete use of the full document, missing information.</td>
<td>Harnesses map-reduce to handle the entire document to craft a complete summary and checklist.</td>
</tr>
</tbody>
</table>
PIVOTAL DISCOVERIES

Refine dynamic retriever methods and prompts to boost response accuracy

A retriever obtains relevant info from a vector database

Minor variations in ETL of data greatly impacted response accuracy

ETL stands for extract, transform, and load

Scalable resources for evolving architecture of model and available data
FUTURE ENHANCEMENTS

1. Simultaneous Document Engagement
2. Source Page, Figures & Tables Images
3. Further LLM Refinement & Training
4. Standards Gap Mapping Feature
“The amount of time it takes for an organization to understand complex cybersecurity regulations is underappreciated. I believe a tool like this brings something new to the table - and can make cybersecurity compliance more accessible to every perspective in an organization from legal, to quality assurance, to R&D”

Jason Y., Cybersecurity Professional

www.sibylcopilot.com
THANK YOU

Over the past 14 weeks, a substantial amount of effort has been dedicated to the development of our AI Copilot, Sibyl. We wish to express our sincere gratitude to our families, friends, colleagues, classmates, cybersecurity professionals and instructors for their invaluable support during this project.
Launched in Fall 2023, interactive platform that links standards and guidelines into one view

One of many enterprise MSP that handle all or part of an organization’s cybersecurity functions
TARGET PROFESSIONALS

- **1.1M** Cybersecurity Professionals\(^1\)
- **83%** Male\(^2\)
- **60%** Aged 40+\(^2\)
- **56%** Hold a Bachelor’s Degree\(^2\)
- **600K** Unfilled Positions in US\(^1\)
- **3.5M** Unfilled Positions Globally\(^3\)
- **1-2** Years Average Tenure\(^2\)
- **$102,600** Median Wage\(^3\)

**76%** Manually Scan Websites for Regulatory Changes\(^4\)
MISSION

Make compliance both efficient and effective, so cybersecurity professionals can focus on what matters most - protecting their organizations from cybersecurity risks and threats.
CONTACT US

Do you have any questions?
swllms@berkeley.edu
vincent.goldberg@berkeley.edu
arwinrahmatpanah@berkeley.edu

sibylcopilot.com

CREDITS: This presentation template was created by Slidesgo, including icons by Flaticon, and infographics & images by Freepik.