

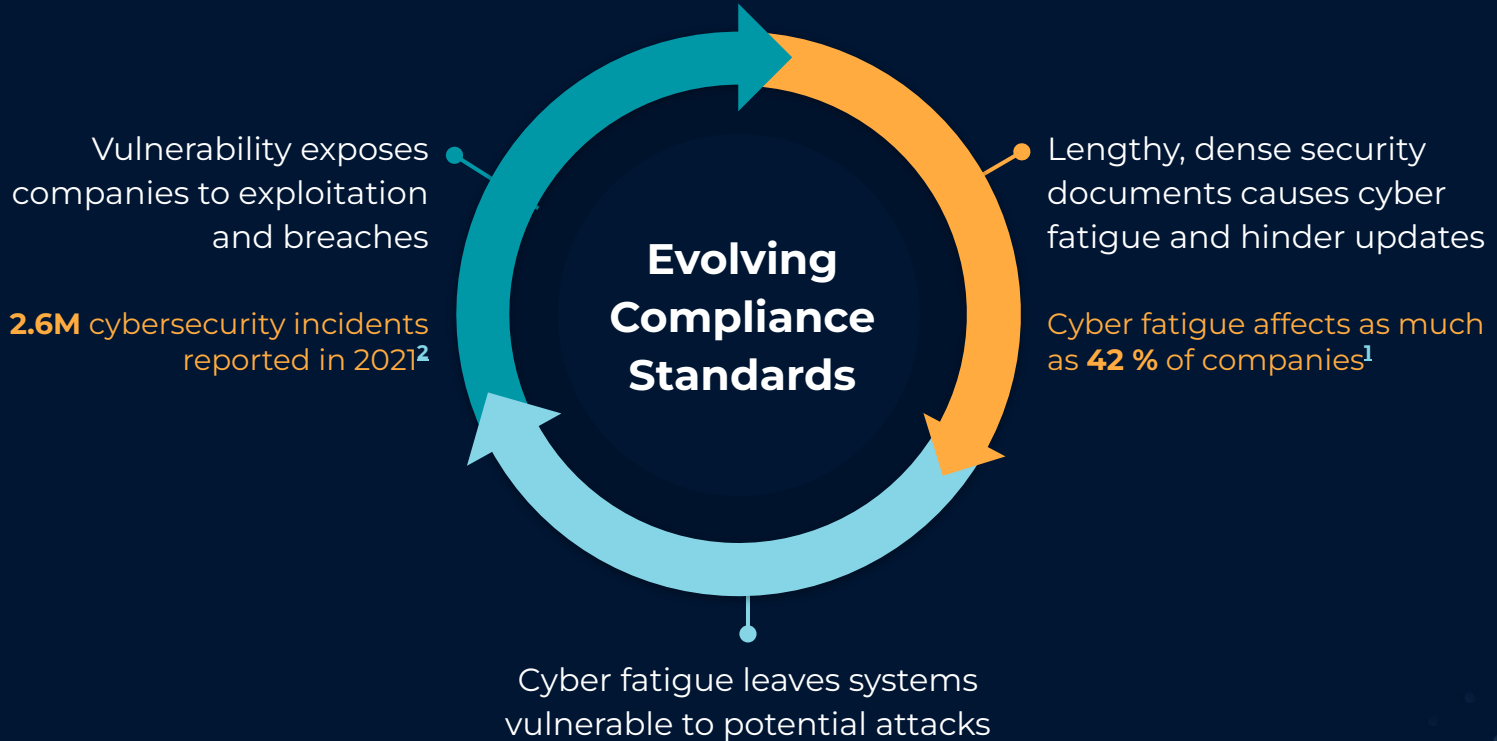


SIBYL

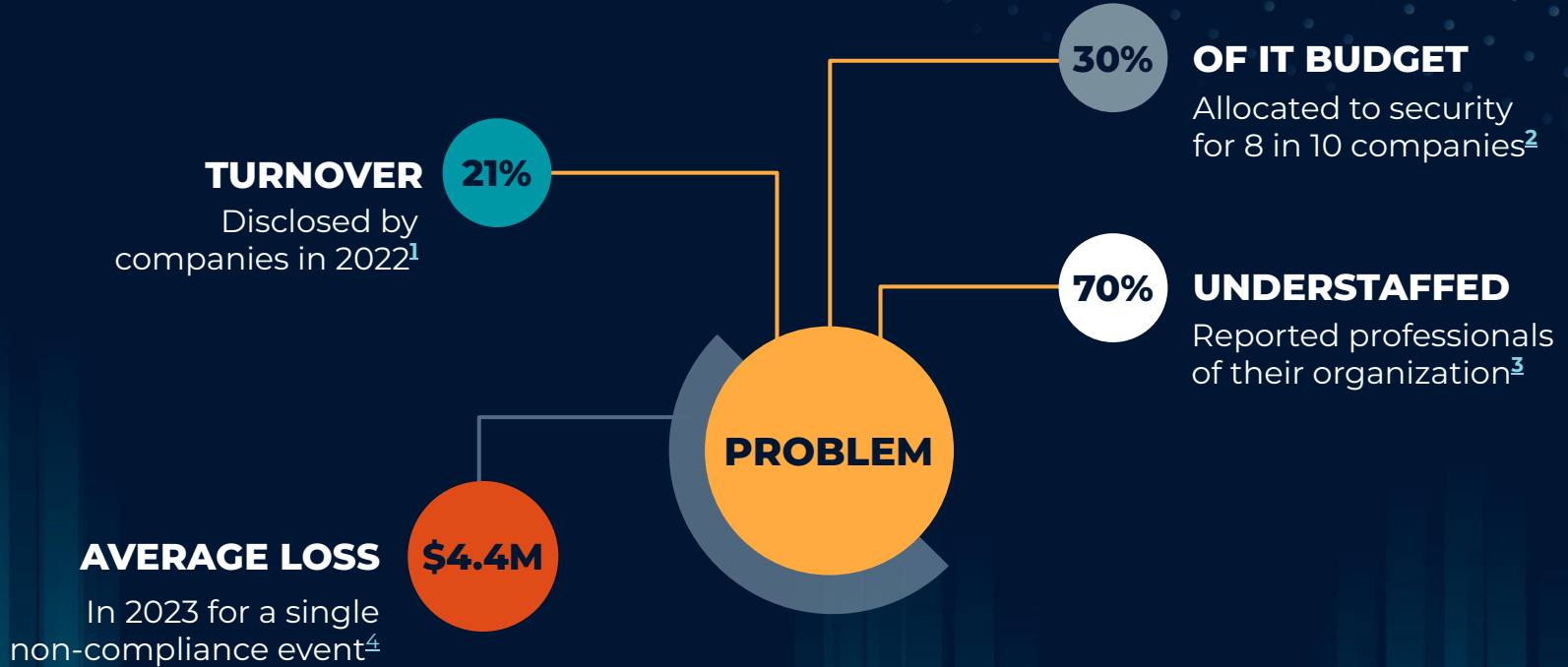
CYBERSECURITY COPILOT

Goldberg | Rahmatpanah | Williams

PROBLEM



INDUSTRY



SOLUTION

Our Cybersecurity Copilot:

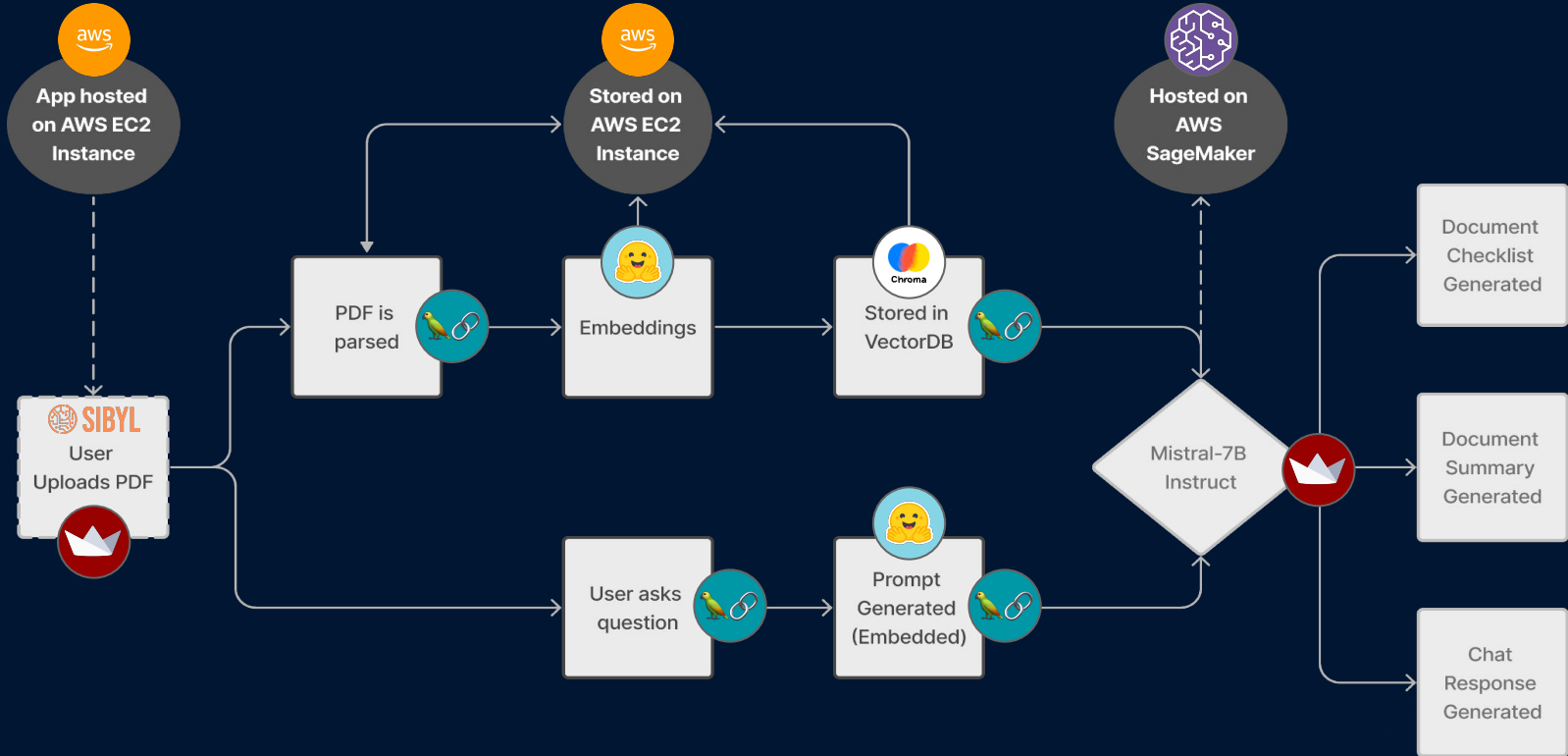


SIBYL

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

[View Demo](#)

ARCHITECTURE



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

	GREAT	GOOD	OK
RELEVANCE	✓	✓	✓
CLARITY	✓	✓	
COHERENCE	✓	✓	✓
LENGTH	✓		
ACCURACY	✓	✓	✓

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

MODEL	Q&A	SUMMARY	VERSION
Mistral	45/50	Great	7B-Instruct
Falcon	44/50	Great	180B-Instruct
Llama	45/50	Great	Llama 2-70b
ChatGPT BASELINE	50/50	Great	3.5 + Ask YourPDF

OTHERS VS. SIBYL

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Question & Answering	Relies on outdated and broad-topic data that can lead to inaccurate answers.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

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





SIBYL

CYBERSECURITY COPILOT

“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”

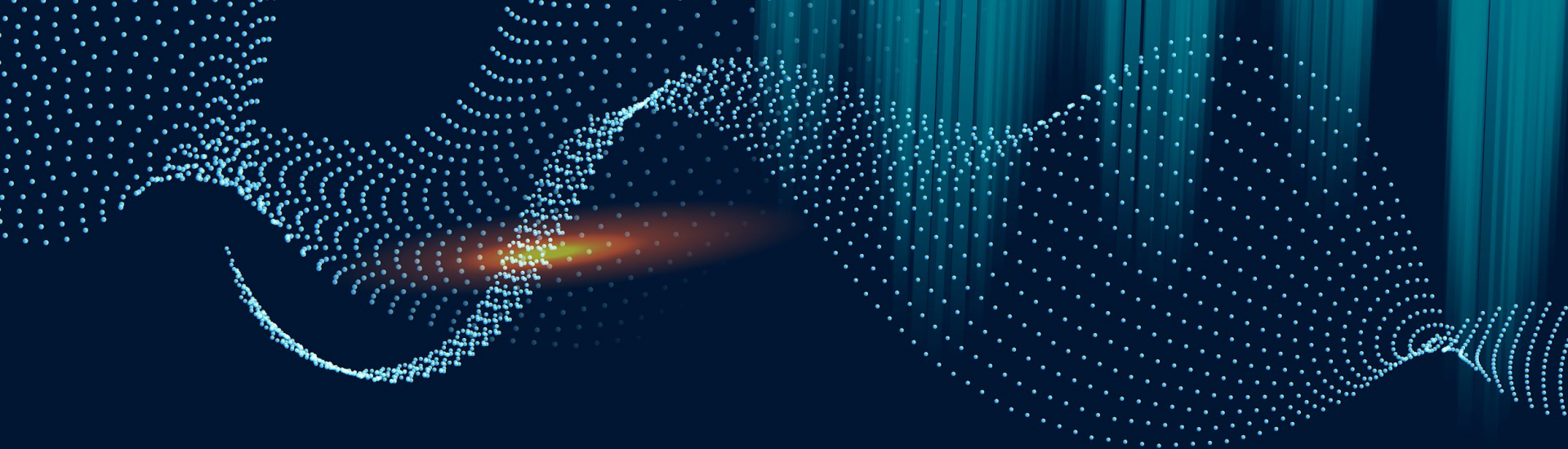
Jason Y., Cybersecurity Professional

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.





APPENDIX

Additional Information

MARKET RESEARCH

Uniting security standards



OpenCRE.org

Launched in Fall 2023,
interactive platform that
links standards and
guidelines into one view

DRATA

One of many enterprise
MSP that handle all or
part of an organization's
cybersecurity functions

TARGET PROFESSIONALS

- **1.1M** Cybersecurity Professionals¹
- **83%** Male²
- **60%** Aged 40+²
- **56%** Hold a Bachelor's Degree²
- **600K** Unfilled Positions in US¹
- **3.5M** Unfilled Positions Globally³
- **1-2** Years Average Tenure²
- **\$102,600** Median Wage³

76% Manually Scan Websites for Regulatory Changes⁴

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.