Forward-looking statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

Harnessing Multimodal Data for Enhanced Splunk Analytics

DEV1351C

.conf24

splunk>

Bring on the future.

Presenters

Russell Barber

Security Engineer – Splunk Consultant
BlueVoyant

Anthony Giallombardo

VP Tech Services & Director of Product Management
BlueVoyant

splunk> .conf24

Interactive Workshop Resources

Github

- https://github.com/rbarber68/DEV1351C
- Contains: Splunk app, slide deck, lab workbook, example content

Ollama

- https://ollama.com
- Install ollama app (Windows/macOS/Linux)
  - Pull LLM models from the repo
  - ollama pull llama3:latest
  - ollama pull llava:latest

Key Takeaways

Know where we're going

Ollama

- Runs LLM models locally
- Windows/Linux/macOS
- Easy to run

LLMs

- Current LLM models are powerful
- Can assist will Splunk Admin tasks
- Can process multimodal inputs

Splunk Integration

- Modular inputs
- Streaming commands

Multimodal Data is everywhere

Textual

Machine data

JSON/XML/TXT

Logs

Files

Traces

Videos
Images

Screen captures

Security footage

Email attachments

Video stills

Video sharing

Audio

Telephone calls

911 calls

Customer service calls

Audio from video streams

Multimodal Challenges

- Non-textual data
- Complex data formats
  - **JPG**
  - **WAV**
  - **MP3**
  - **AVI**
- Advanced techniques to interpret
- Storage and computational demands

LLMs to the Rescue

- What's a LLM
- Remote vs Local
- GPU/CPU
- Parameters
  - 2G
  - 8G
- Prompt Engineering
- Model Types
  - Chat/Instruct
  - LLaVa
  - Tokens/Context

Lab 1: Getting to Know Ollama

Lab material is available on github
https://github.com/rbarber68/DEV1351C

Prompt Engineering

- Clarity
  - Ensure clarity with straightforward prompts
- Be verbose
  - Detail prompts for precise responses
- Example results
  - Use examples to clarify expected outputs
- Iterate
  - Continuously review and refine prompts

Lab 2:
Creating a Prompt

Lab material is available on github
https://github.com/rbarber68/DEV1351C

Lab 3:
Can it Splunk?

Lab material is available on github
https://github.com/rbarber68/DEV1351C

LLaVA: Large Language -and-Vision Assistant

LLM & Vision encoder combined

Lab 4:
A picture is worth a thousand words.

Lab material is available on github
https://github.com/rbarber68/DEV1351C

Lab 5:
What’s happening?

Lab material is available on github
https://github.com/rbarber68/DEV1351C

Lab 6:
SPL Integration

Lab material is available on github
https://github.com/rbarber68/DEV1351C

Thank you