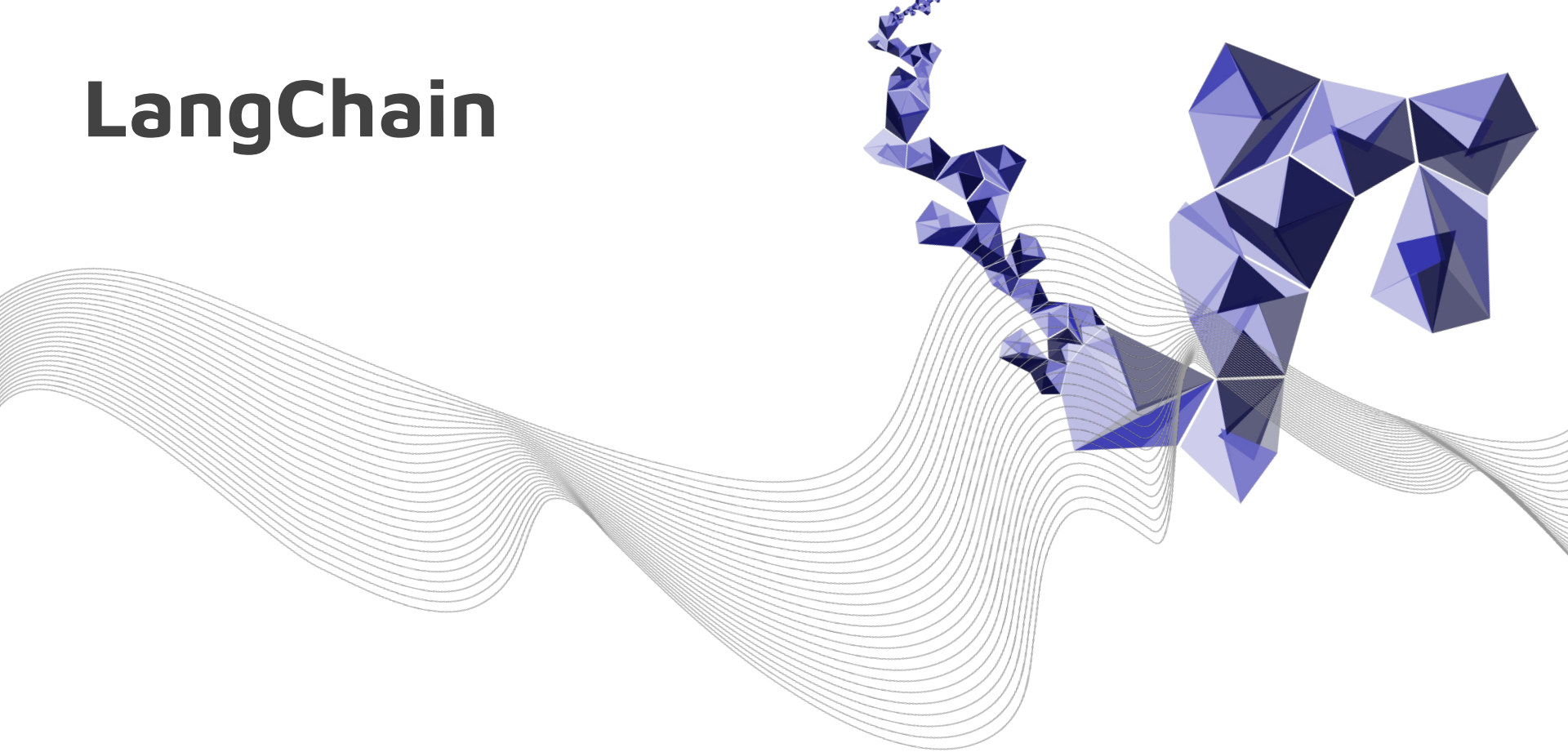
UNIVERSITY OF TWENTE.

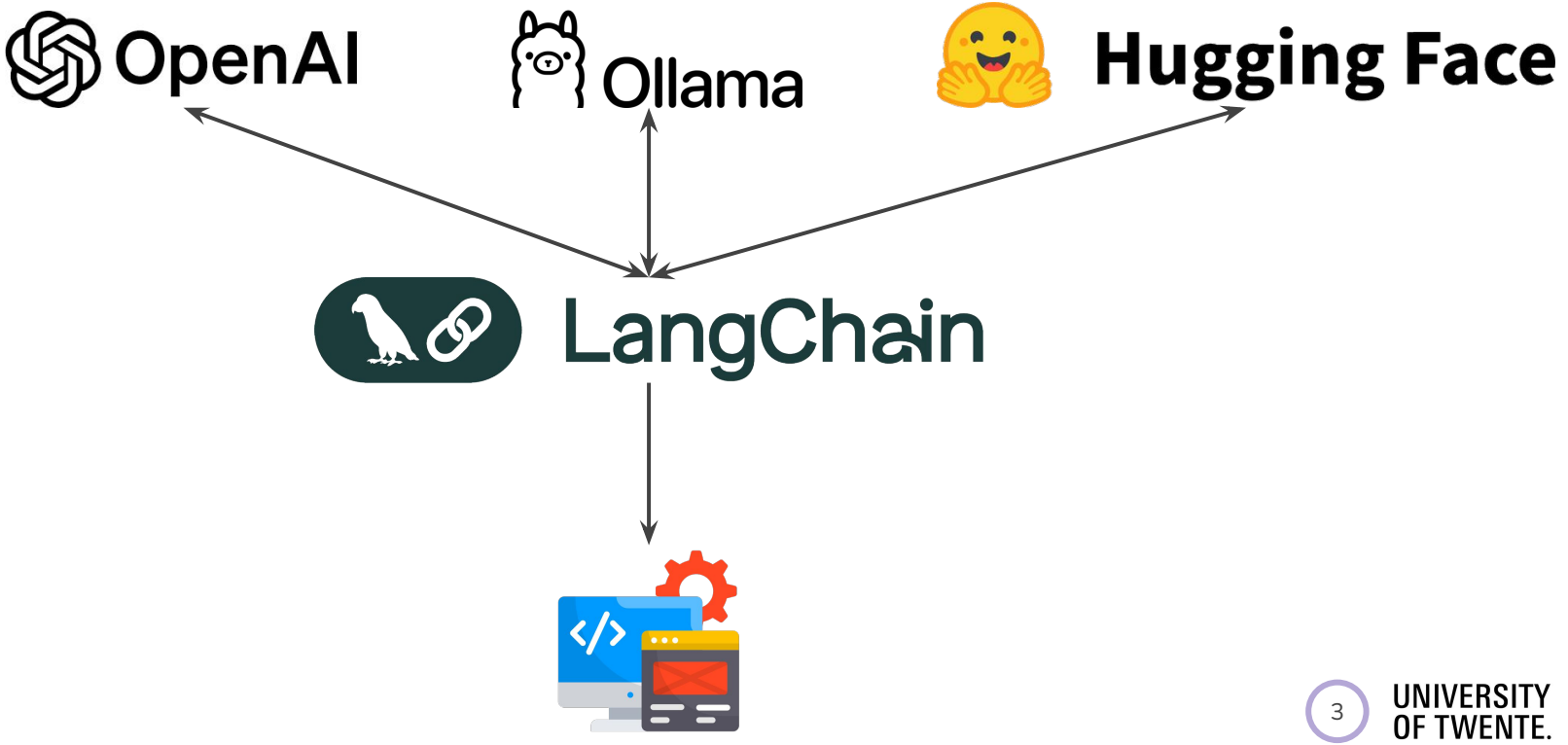
Can LLMs control our PC?

21st of March, 2025

LangChain



What is LangChain?



What are the benefits of LangChain?

OpenAI

```
from langchain_openai import OpenAI

llm = OpenAI(model="gpt-4o")
```

Ollama

```
from langchain_ollama import ChatOllama

llm = ChatOllama(model="llama3.2")
```

```
llm.invoke(question)
```

Output: "Hello, I am GPT 4o."

Output: "Hi, my name is LLaMa 3.2."

What are the benefits of LangChain?

```
Output:     The command for blocking an IP address is:
            'iptables -A OUTPUT -d {ip} -j DROP'. This command
            blocks any outgoing traffic to the {ip} address.
```

What if we need a json output?

```
Output:     {
                "command":      "iptables -A OUTPUT -d {ip} -j DROP",
                "explanation":  "This command blocks any outgoing
                                traffic to the {ip} address.",
            }
```

What are the benefits of LangChain?

- LangChain offers automated parsers

```
class Command(BaseModel):
    command: str = Field(description=...)
    explanation: str = Field(description=...)

parser = PydanticOutputParser(pydantic_object=Command)

chain = model | parser

chain.invoke({"query": command_query})
```

What are tools in LangChain?

- Custom code
- LLM
- API
- Human in the loop
- etc.

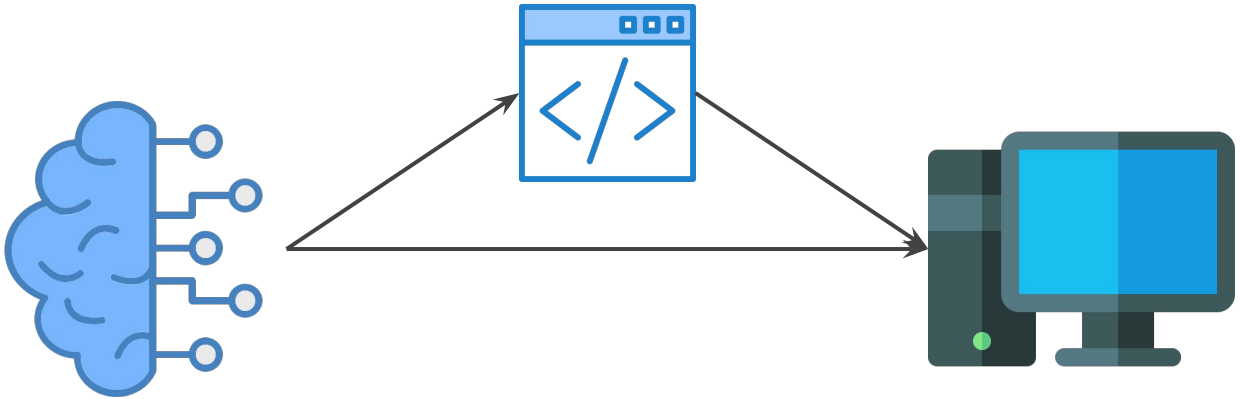
What are the benefits of LangChain?

- Chaining tools together

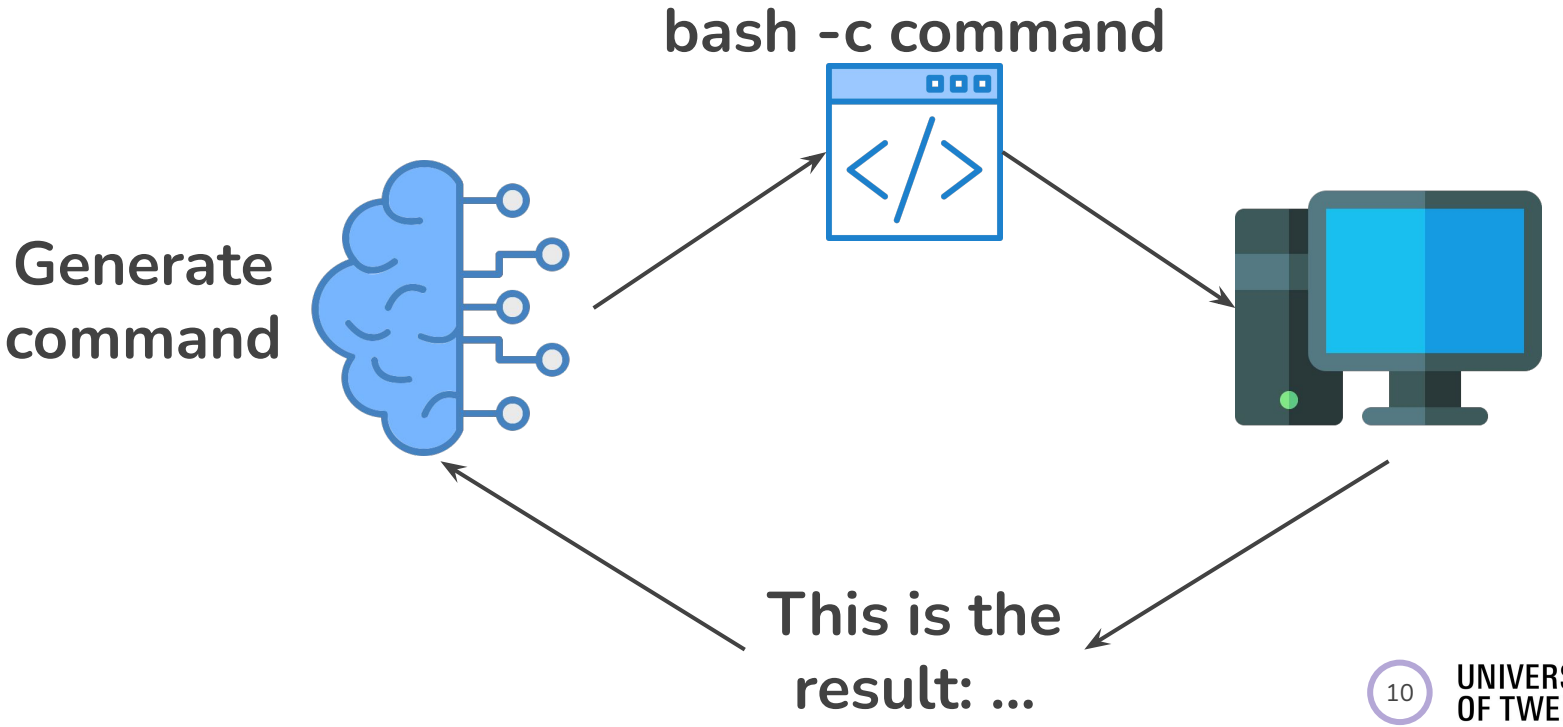
```
chain = model_1 | parser | model_2 | execute

chain.invoke({"query": command_query})
```

How does an LLM interact with an environment?



How does an LLM interact with an environment?

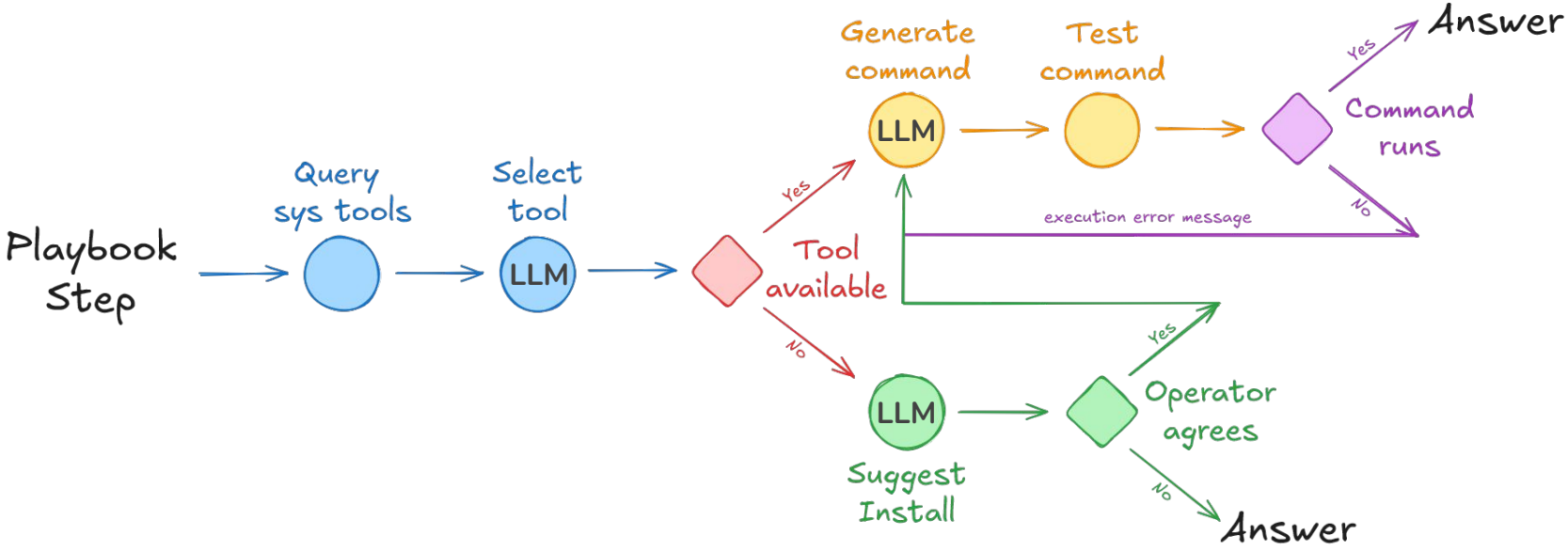


Can an LLM act as an Incident Responder?

What does an Incident Responder do?

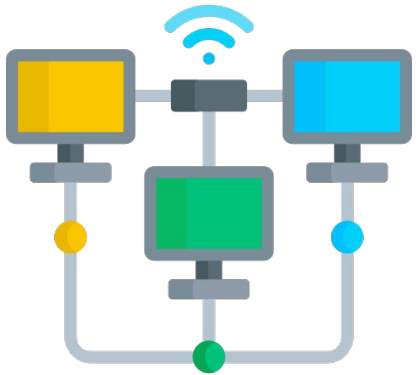
- Has an understanding of the environment
  - OS
  - installed tools
- Translates playbook steps into commands
  - select tool
  - install tool
  - write command
  - test command

Incident Response



DEMO

Network Traffic Filtering



In which direction are we heading?