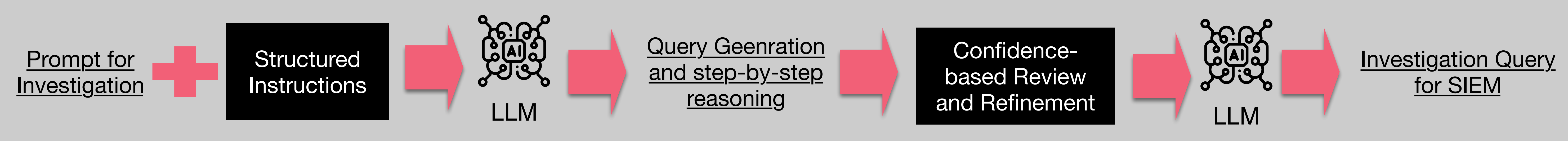
QueryAI Methdology Overview



Prompt for Investigation

Structured Instructions

LLM

Query Geenration and step-by-step reasoning

Confidence-based Review and Refinement

LLM

Investigation Query for SIEM

Example

Prompt

Investigate an alert for suspicious file named foo.txt deletion activity by verifying if the process responsible matches common file-cleanup utilities or legitimate system processes.

Structured Instructions

Instruction: Provide a clear and structured KQL query for SIEM to investigate the specified alert.
Output Format: Follow structured query generation with:

- **Entity Identification**: Identify relevant fields like `ActionType`, `FileName`,...
- **Filter Conditions**: Construct conditions to isolate events related to `foo.txt` deletions…
- **Projection**: List necessary fields (e.g., `DeviceName`,).

Reasoning Process: Explain reasoning steps in structuring the query.
Trigger: Prompt to generate an accurate, context-aware query.

KQL Query for SIEM

```
DeviceFileEvents
| where ActionType == "FileDeleted"
| where FileName == “foo.txt”
| where not(ProcessName has_any ("cleanmgr.exe",
"sdelete.exe", "explorer.exe", "svchost.exe"))
| project DeviceName, AccountName, ProcessName,
FileName, TimeGenerated
```