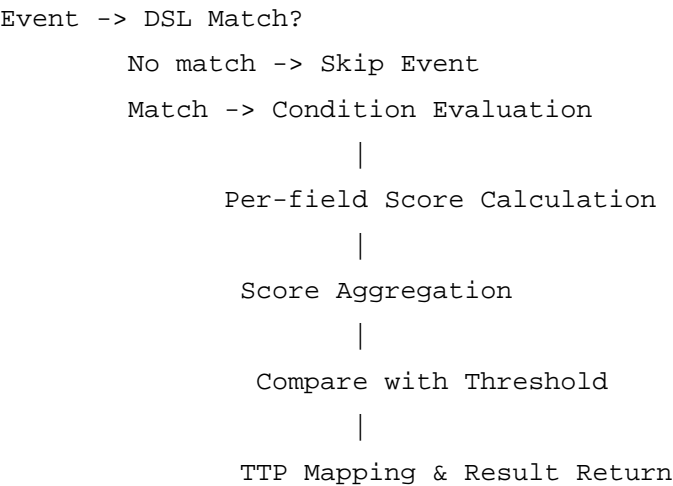


# Pentra DSL & Evaluator Specification (v1.1)

## 1. DSL Rule Structure (Example)

```
id: EVT-001
domain:edr
name: Suspicious PowerShell Execution
vendor: velociraptor
score_threshold: 0.9
conditions:
  - field: process_name
    op: equals
    value: powershell.exe
    weight: 0.5
  - field: command_line
    op: contains
    value: -enc
    weight: 0.5
mapped_ttps:
  - id: T1059.001
    weight: 1.0
```

## 2. Evaluator Flow Overview



## 3. Mermaid Chain Output

Auto-generated diagram using TTPs mapped from DSL rules. Demonstrates log-driven chaining based on evaluated confidence and MITRE technique mapping.

## 4. Report Output Description

Evaluated JSON report includes:

- Confidence Score
- Mapped TTPs
- Session Roles
- Narrative (LLM optional)

This allows explainable reporting without opaque model inference.

## **5. Purpose of This Document**

This spec serves as a reference for understanding Pentra's judgment system:

- DSL as explainable language
- Evaluation as structured reasoning
- Output as human-readable decision

Not detection. A system for decisions.