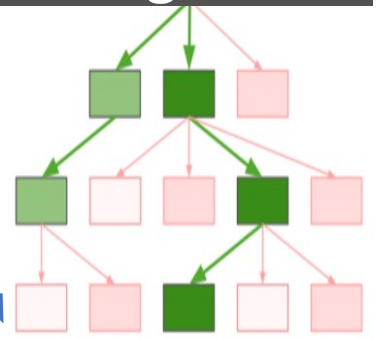
5.3.1 Behavior Tree Construction

Behavior Generation Prompt

System: You are a security expert and you are familiar with the legal behaviour of important windows processes.
Goal: Generate Behavior Tree
The format of this knowledge tree is as follows:
1.Basic profile
2 Basic BeHavior

L

Behavior tree Agent



- Self-Ask

5.3.2 Command Execution

Behavior->Commands Prompt L

Powershell Execution T

Real Logs T

Command-Execution Agent

Control

Memory

Validation

1 format verification
Standardized response
2 factuality verification
- Real-world Log Verification
- Multi-session Cross-verification

5.3.3 Constraint Extraction

Constraint-Extraction Agent

- **Common Items and Common Sequence** T
- **LLM: obtain and explain Constraint** L

Program Constraint
1 Inherent constraints: parent-child processes, execution path
2 Timing constraints: execution sequence

L **LLM program** T **Traditional program**