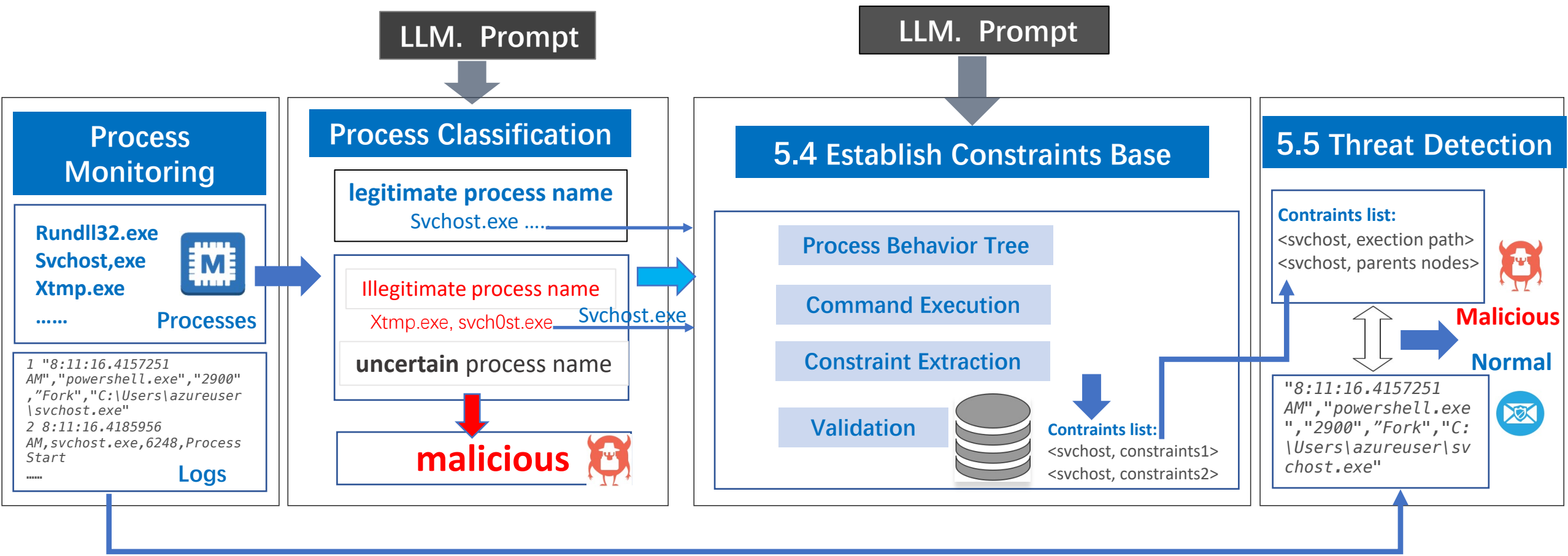
LLM. Prompt
LLM. Prompt
Process Monitoring
Rundll32.exe
Svchost,exe
Xtmp.exe
.....
Processes
1 "8:11:16.4157251 AM","powershell.exe","2900",”Fork","C:\Users\azureuser\svchost.exe"
2 8:11:16.4185956 AM,svchost.exe,6248,Process Start
.....
Logs
Process Classification
legitimate process name
Svchost.exe ....
Illegitimate process name
Xtmp.exe, svch0st.exe
Svchost.exe
uncertain process name
malicious
5.4 Establish Constraints Base
Process Behavior Tree
Command Execution
Constraint Extraction
Validation
Contraints list:
<svchost, constraints1>
<svchost, constraints2>
5.5 Threat Detection
Contraints list:
<svchost, exection path>
<svchost, parents nodes>
Malicious
Normal
"8:11:16.4157251 AM","powershell.exe","2900",”Fork","C:\Users\azureuser\svchost.exe"