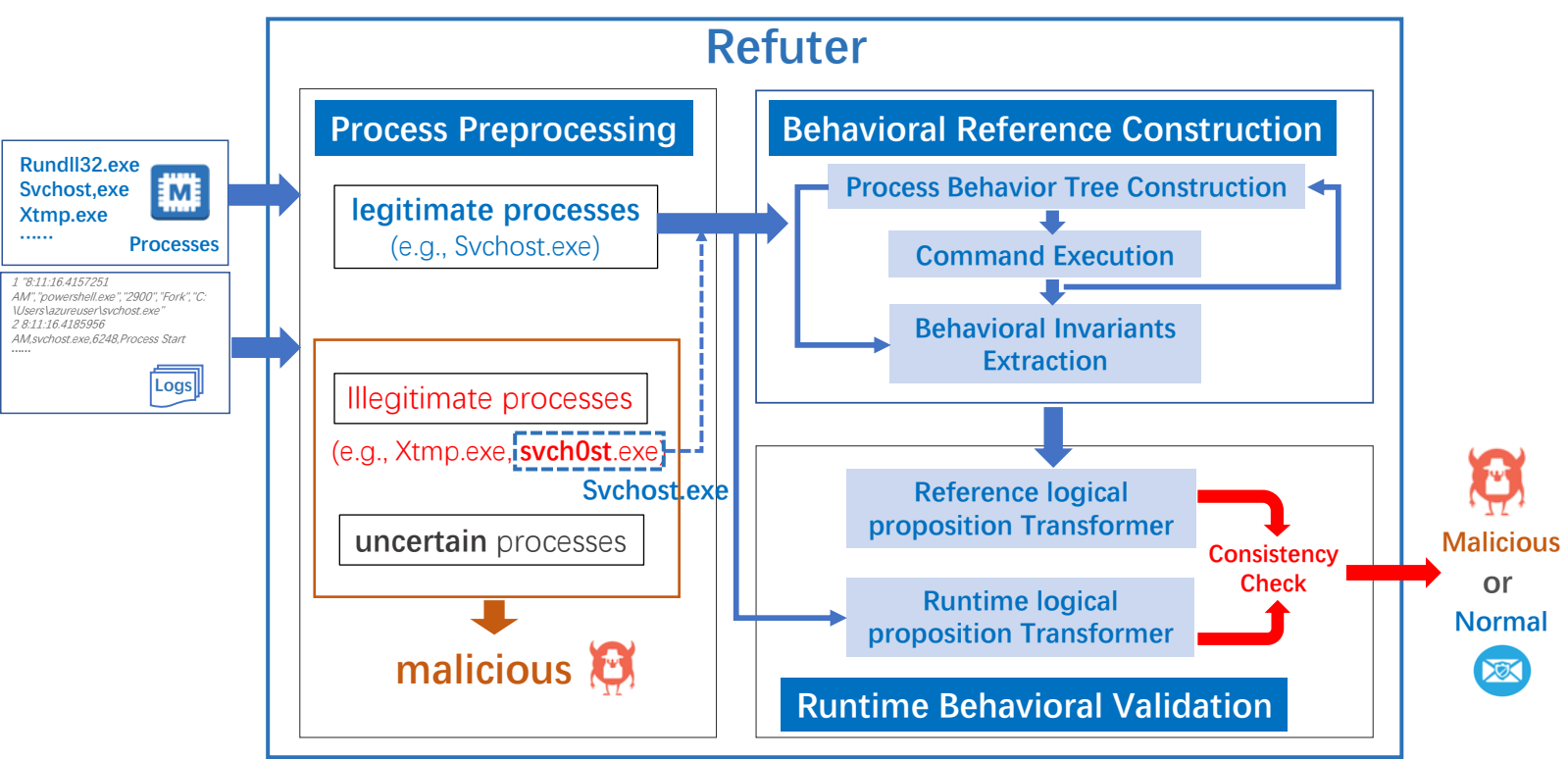
Refuter
Process Preprocessing
Behavioral Reference Construction
Rundll32.exe
Svchost,exe
Xtmp.exe
.....
Processes
1 "8:11:16.4157251
AM","powershell.exe","2900","Fork","C:
\Users\azureuser\svchost.exe"
2 8:11:16.4185956
AM,svchost.exe,6248,Process Start
.....
Logs
legitimate processes
(e.g., Svchost.exe)
Process Behavior Tree Construction
Command Execution
Behavioral Invariants
Extraction
Illegitimate processes
(e.g., Xtmp.exe, svch0st.exe)
Svchost.exe
uncertain processes
malicious
Reference logical
proposition Transformer
Runtime logical
proposition Transformer
Consistency
Check
Runtime Behavioral Validation
Malicious
or
Normal