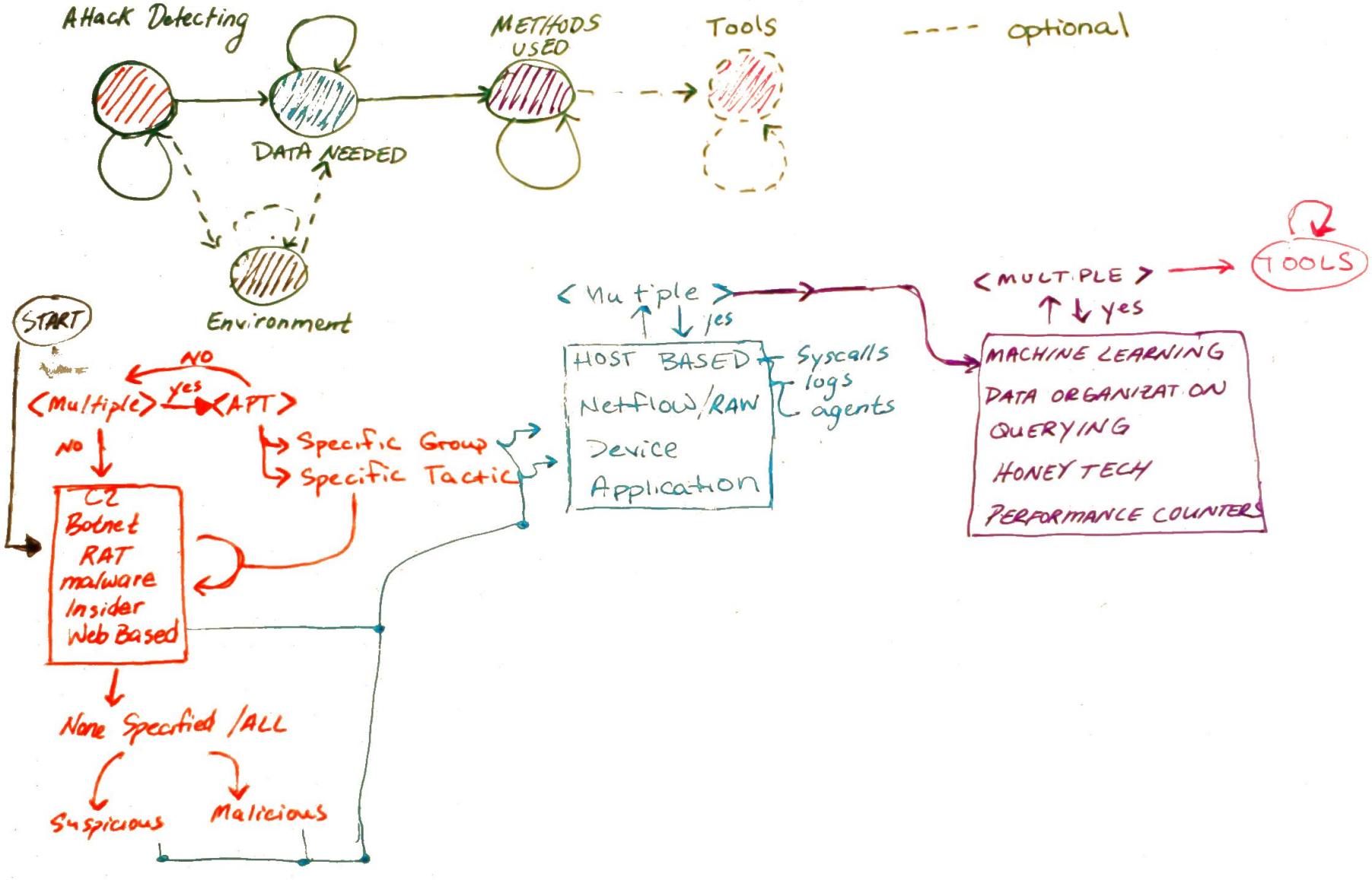
Attack Detecting
METHODS USED
Tools
---- optional
DATA NEEDED
Environment
START
NO
yes
<Multiple>
APT
No
Specific Group
Specific Tactic
C2
Botnet
RAT
malware
Insider
Web Based
None Specified /ALL
Suspicious
Malicious
<Multiple>
yes
HOST BASED
Netflow/RAW
Device
Application
Syscalls
logs
agents
<MULTIPLE>
yes
TOOLS
MACHINE LEARNING
DATA ORGANIZATION
QUERYING
HONEY TECH
PERFORMANCE COUNTERS