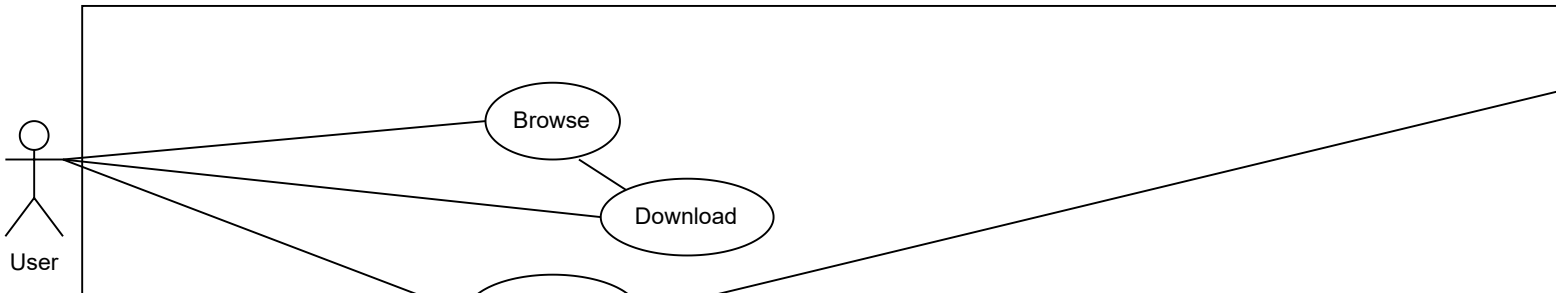
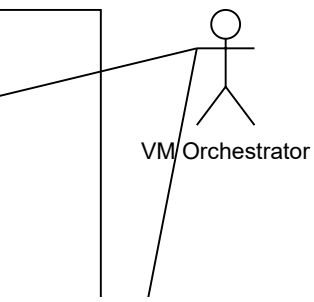
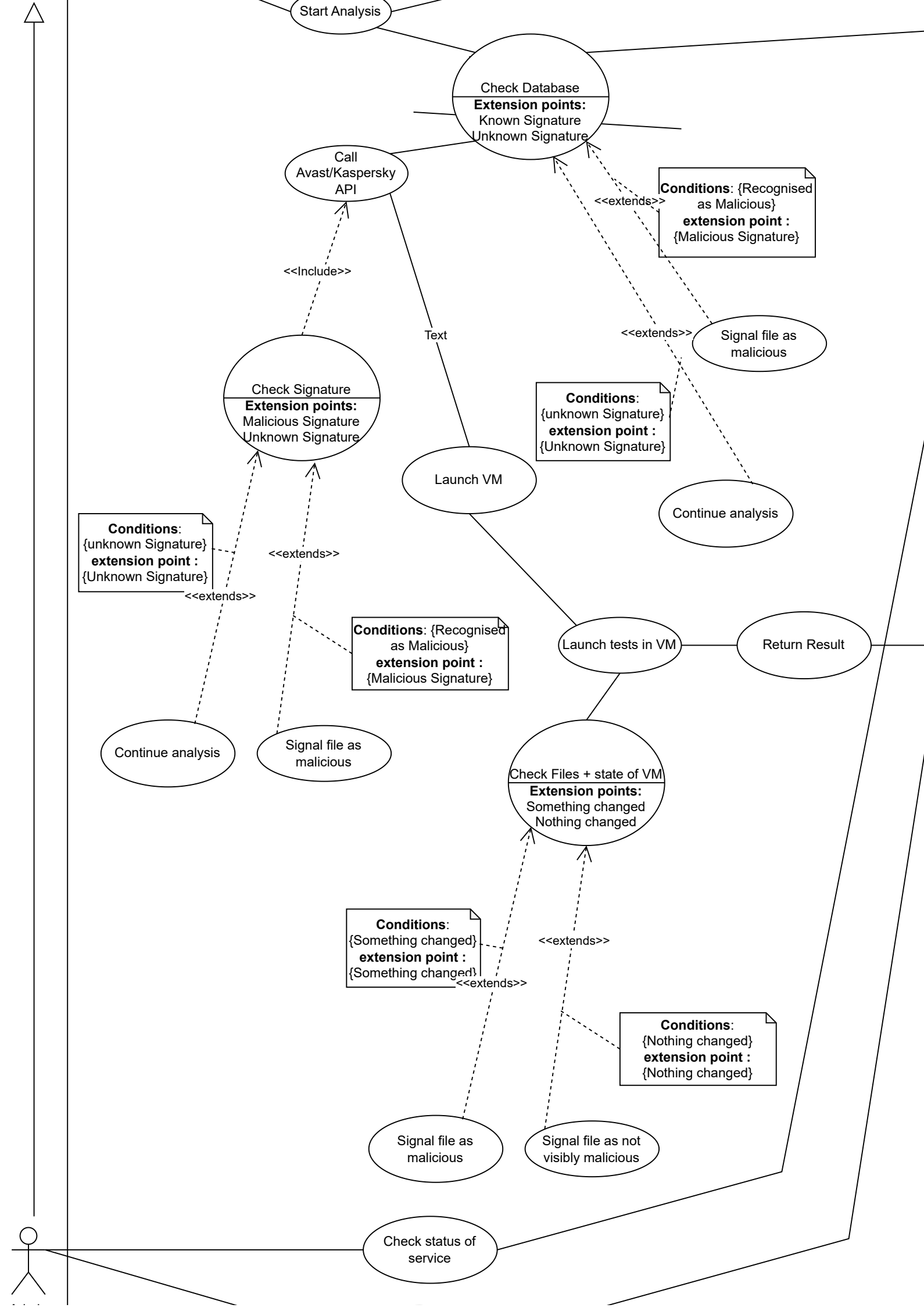
ViperDefender Use Case Diagram




VM Orchestrator


Start Analysis
Check Database
Extension points:
Known Signature
Unknown Signature
Call Avast/Kaspersky API
<<extends>>
Conditions: {Recognised as Malicious}
extension point :
{Malicious Signature}
<<Include>>
Text
<<extends>>
Signal file as malicious
Check Signature
Extension points:
Malicious Signature
Unknown Signature
Conditions:
{unknown Signature}
extension point :
{Unknown Signature}
Launch VM
Continue analysis
Conditions:
{unknown Signature}
extension point :
{Unknown Signature}
<<extends>>
<<extends>>
Conditions: {Recognised as Malicious}
extension point :
{Malicious Signature}
Launch tests in VM
Return Result
Continue analysis
Signal file as malicious
Check Files + state of VM
Extension points:
Something changed
Nothing changed
Conditions:
{Something changed}
extension point :
{Something changed}
<<extends>>
<<extends>>
Conditions:
{Nothing changed}
extension point :
{Nothing changed}
Signal file as malicious
Signal file as not visibly malicious
Check status of service

Database
VM Test

Admin
Check database