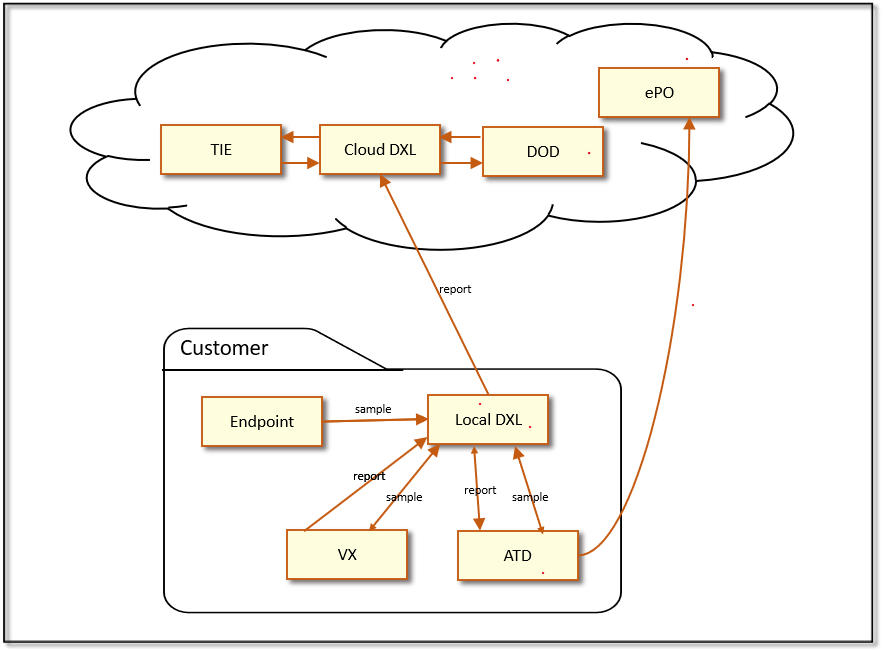
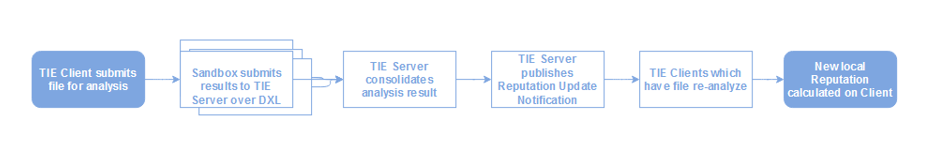
**TIE Sandbox Modifications**

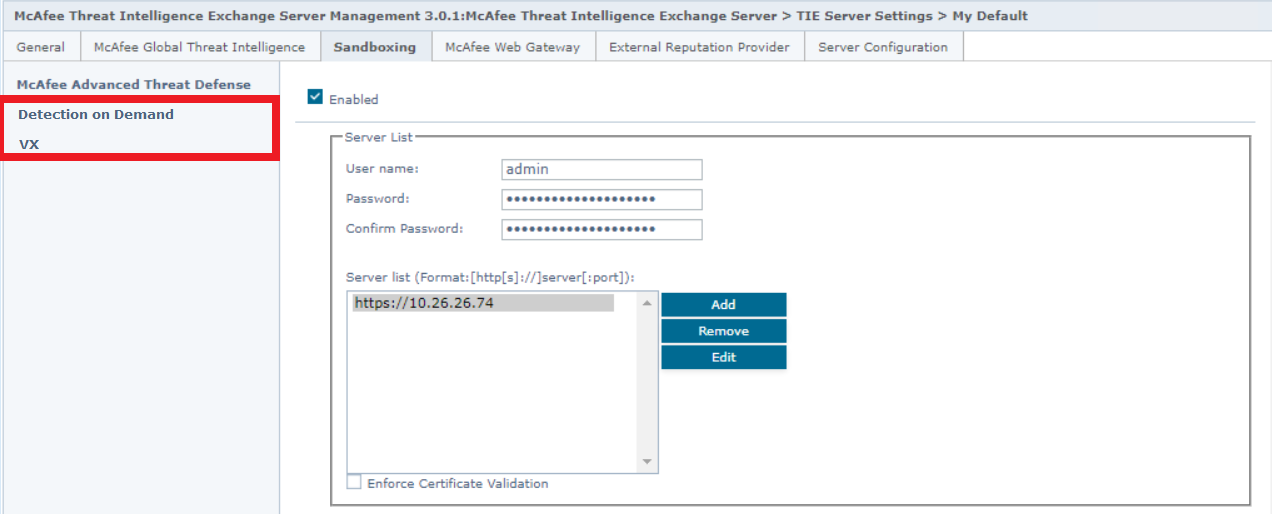
**Proposed Architecture**



**Sandboxing Flow**



**Sandbox Configuration**



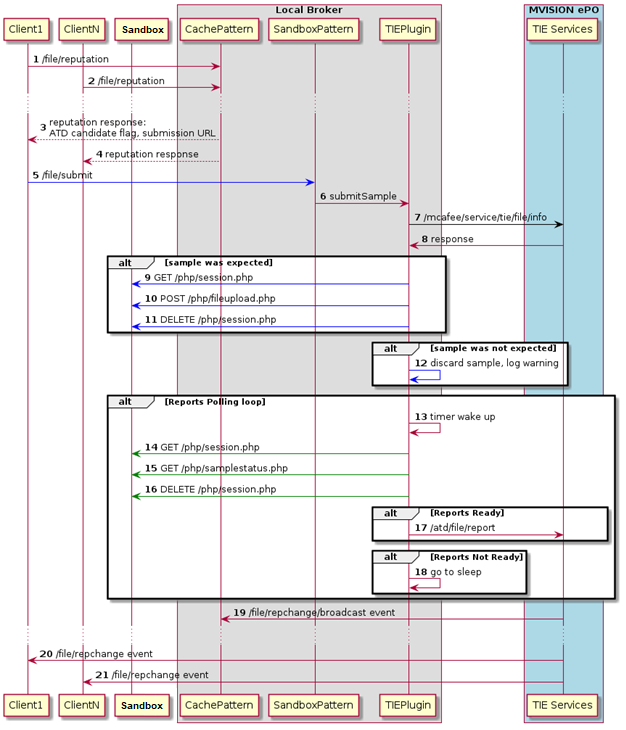
**ATD Reputation Mapping**

|  |  |  |  |
| --- | --- | --- | --- |
| **ATD Severity** | **TIE Reputation** | **Reputation String Value** | **Reputation Integer Value** |
| -2 | REP\_NOT\_SET | Not set | 0 |
| -1 | REP\_KNOWN\_CLEAN | Known Trusted | 99 |
| 0,1,2 | REP\_UNKNOWN | Unknown | 50 |
| 3 | REP\_PROBABLY\_DIRTY | Might be Malicious | 30 |
| 4 | REP\_ASSUMED\_DIRTY | Most Likely Malicious | 15 |
| 5 | REP\_KNOWN\_DIRTY | Known Malicious | 1 |
| Others | REP\_UNKNOWN | Unknown | 50 |

**DOD Reputation Mapping**

|  |  |  |  |
| --- | --- | --- | --- |
| **DOD Verdict** | **TIE Reputation** | **Reputation String Value** | **Reputation Integer Value** |
| NON\_MALICIOUS | REP\_KNOWN\_CLEAN  UNKNOWN | Known Trusted | 99 |
| MALICIOUS | REP\_KNOWN\_DIRTY | Known Malicious | 1 |
| NOT\_KNOWN |  |  |  |

**TIE Sandboxing Pattern**

****

**Package Structure**

Chart, waterfall chart

Description automatically generated

**Clarifications**

==============

1. Polling vs DXL

2. DOD Report - File identification (report ID) vis-a-vis DXL

3. Precedence - ATD vs DOD vs VX

4. Provider ID - External Reputation

1 GTI File Global Threat Intelligence provider for file reputations

3 Enterprise File Enterprise provider for file reputations set through ePO

5 ATD File Active Threat Defense provider for file reputations

7 MWG File McAfee Web Gateway provider for file reputations

15 External File External providers for file reputation

23 DOD/VX -> new (4/6)

5. UI Settings - finalize

6. UI display - TIE Reputations page (Composite later)

7. Marketplace – Sandbox

8.

com/mcafee/jti/server/sandbox/atd/impl/AtdServiceImpl.java

com/mcafee/jti/server/service/provider/impl/atd/AtdFileReputationProvider.java

Action Items

Implement IPE for DOD polling response to DXL (Kshitiz) **AVAILABLE**

ENS not OnP (Coffee shop no VPN) – use Cloud DXL? (Kshitiz) **Local Broker NOT MANDATORY**

DXL IPE pattern for DOD could be on Cloud vs OnP (Kshitiz) **BOTH AVAILABLE**

Ask for NOT\_KNOWN result from DOD (Fireeye – Sai) UPDATE AFTER CALL (02/110/2022)

Mapping discussion with FE team (Ramesh Gupta/(Sai – DOD)+ (Alexander - VX)) UPDATE AFTER CALL (02/110/2022)

Graphical user interface, text, application

Description automatically generated