PDF Malware Detection

❏ PEAS

- P (Performance measure) : minimizing false positives , minimizing analysis time .
- E (Environment) : set of pdf Samples .
- A (Actuator) : confirm if that pdf is malicious or not .
- S (Sensor) : header section and metadata reader , opcode and strings extractor .

❏ ODESA

- O : Fully observable
- D : Strategic
- E : Sequential
- S : Dynamic
- A : Single Agent

❏ Type of agent program

- Learning Agent