SISTEMA DI MONITORAGGIO E VALUTAZIONE PER CYBER RANGES

Università degli Studi di Milano - 2019/2020

Tesi di: Alessandro Della Torre Matricola: 893181

Relatrice: Chiara Braghin

COS'È UNA CYBER RANGE?

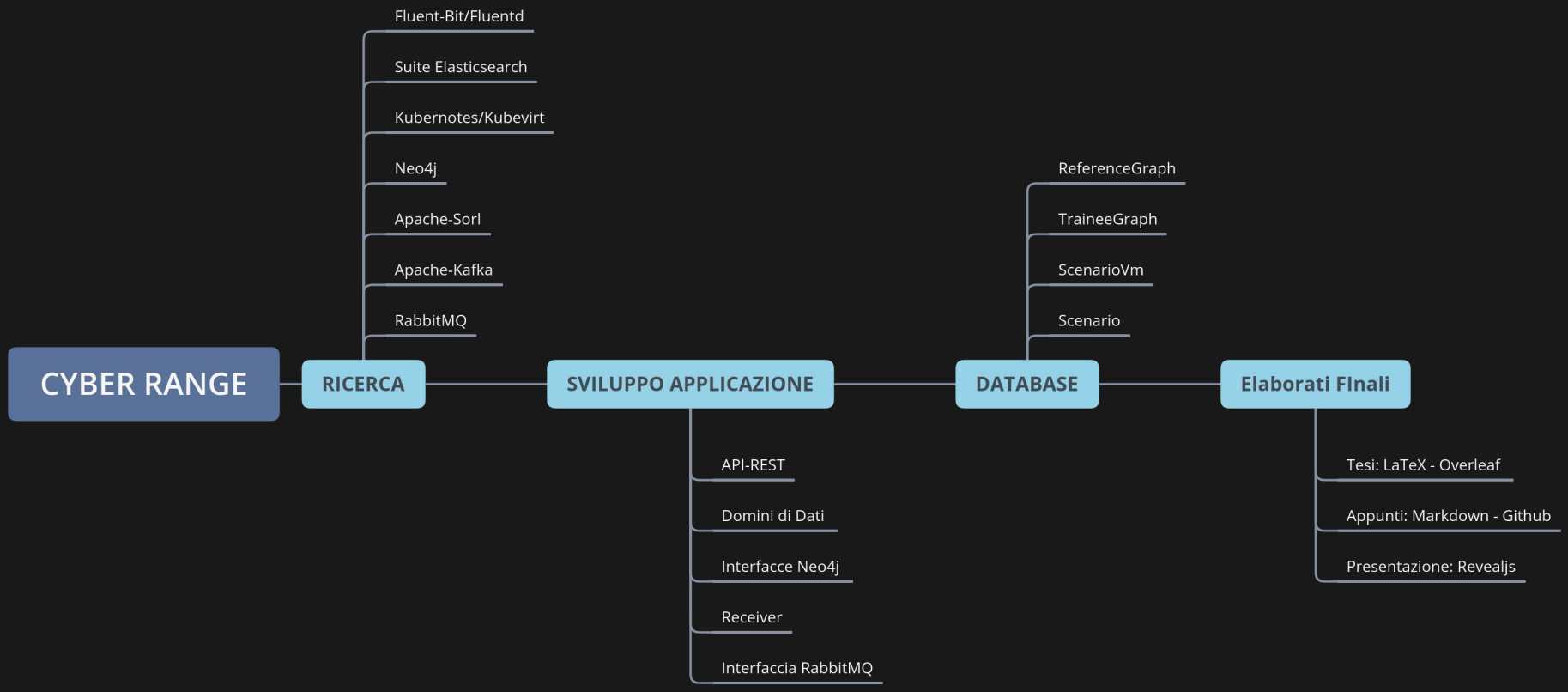
OBIETTIVI

Creazione di un sistema che permettesse di ricevere le informazioni dalle Virtual Machine, analizzarle, valutarle e restituire un grafo complessivo delle azioni svolte dal Trainee.

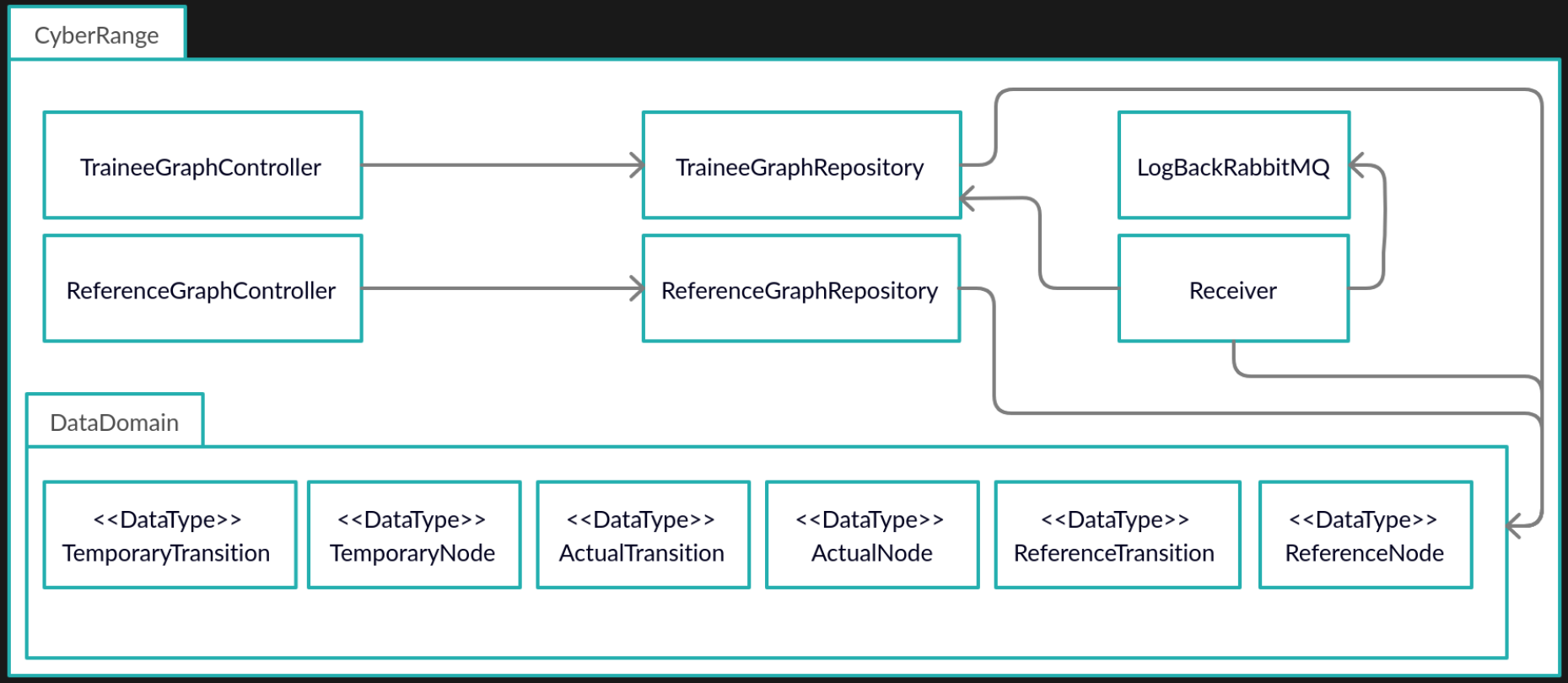
FUNZIONALITÀ

- **MODEL DRIVEN**
- **Api REST**: Inserimento/Ricerca/Eliminazione
- Analisi realtime delle azioni svolte dal trainee
- Utilizzo dei grafi
- **Scoring**: Realtime / Fine Training
- **Matching**: Con ordine / Senza Ordine
- **Output sulle code di RabbitMQ**
  Completato / Revisione

STATO DELL'ARTE

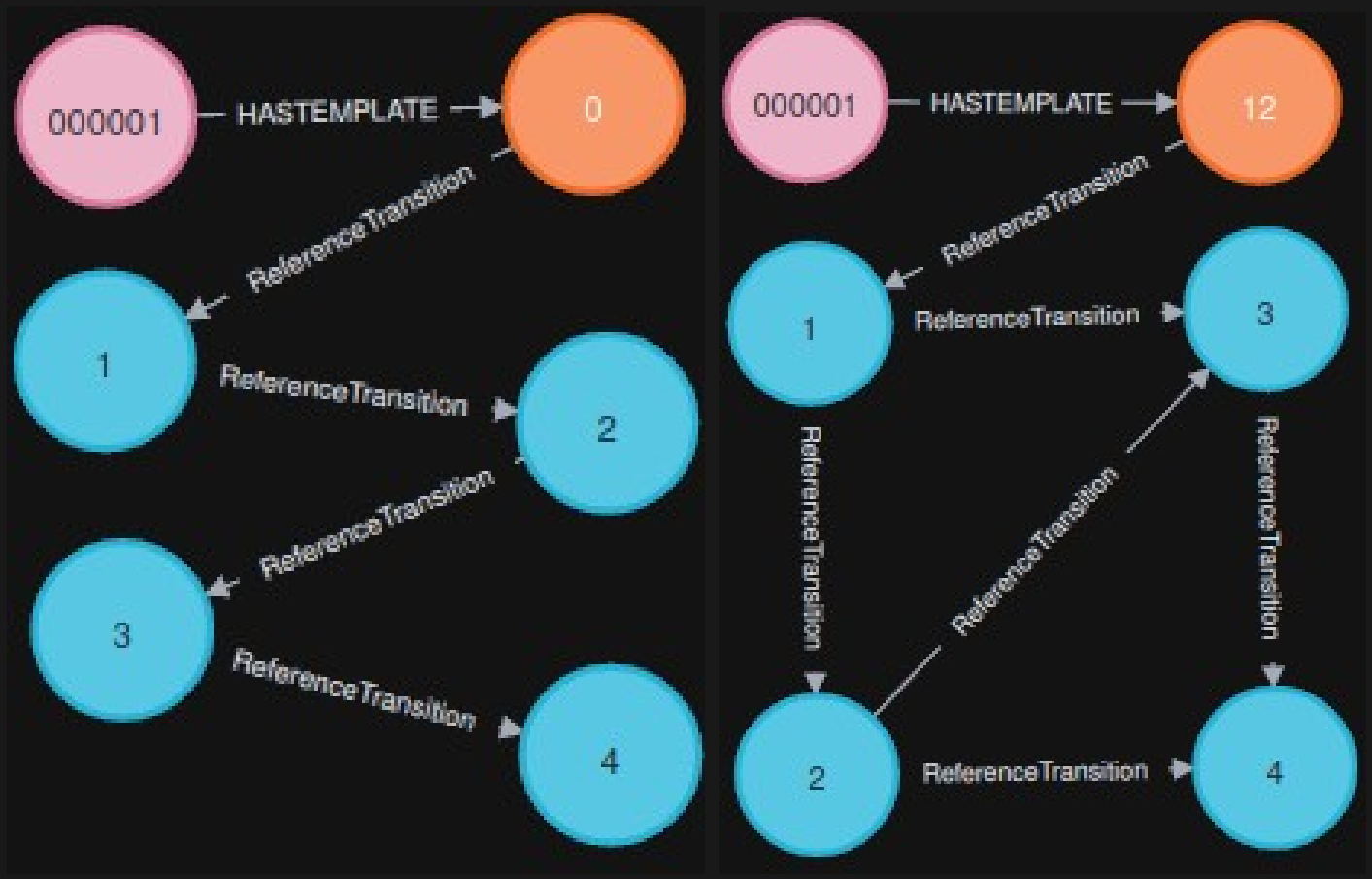


SVILUPPO APPLICAZIONE



SVILUPPO DEL DATABASE

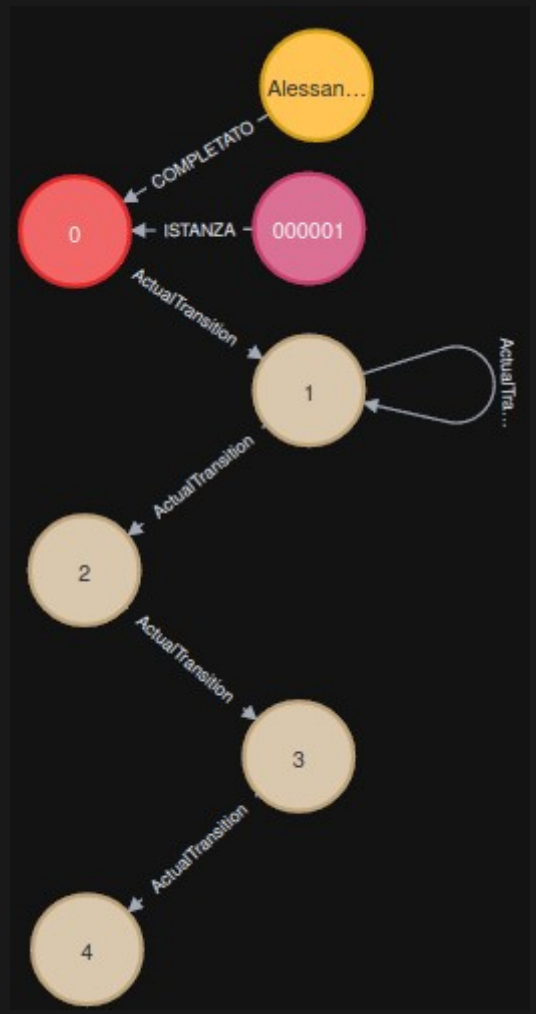
ReferenceGraph



TraineeGraph - Caso Generale

Nodi:

- **Trainee**
- **ScenarioVm**
- **TraineeGraph**
- **ActualNode**



Messaggi:

```
"{'timestamp': 1, 'hostname':'893181', 'ScenarioVM':'000001',
 'Action':'ls -l', 'SessionID':'000111', 'TeamID':'null',
 'ScenarioID':'null'}"
```

```
"{'timestamp': 2, 'hostname':'893181', 'ScenarioVM':'000001',
 'Action':'ls', 'SessionID':'000111', 'TeamID':'null',
 'ScenarioID':'null'}"
```

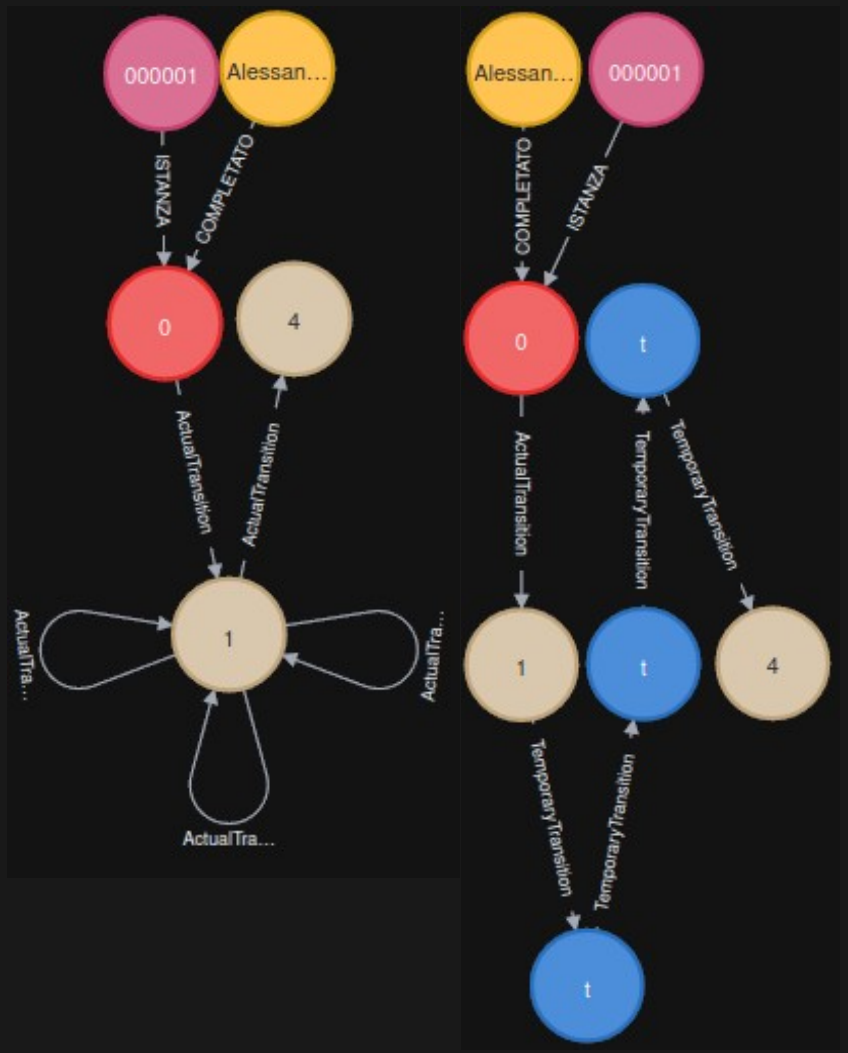
```
"{'timestamp': 3, 'hostname':'893181', 'ScenarioVM':'000001',
 'Action':'pwd', 'SessionID':'000111', 'TeamID':'null',
 'ScenarioID':'null'}"
```

```
"{'timestamp': 4, 'hostname':'893181', 'ScenarioVM':'000001',
 'Action':'cmd', 'SessionID':'000111', 'TeamID':'null',
 'ScenarioID':'null'}"
```

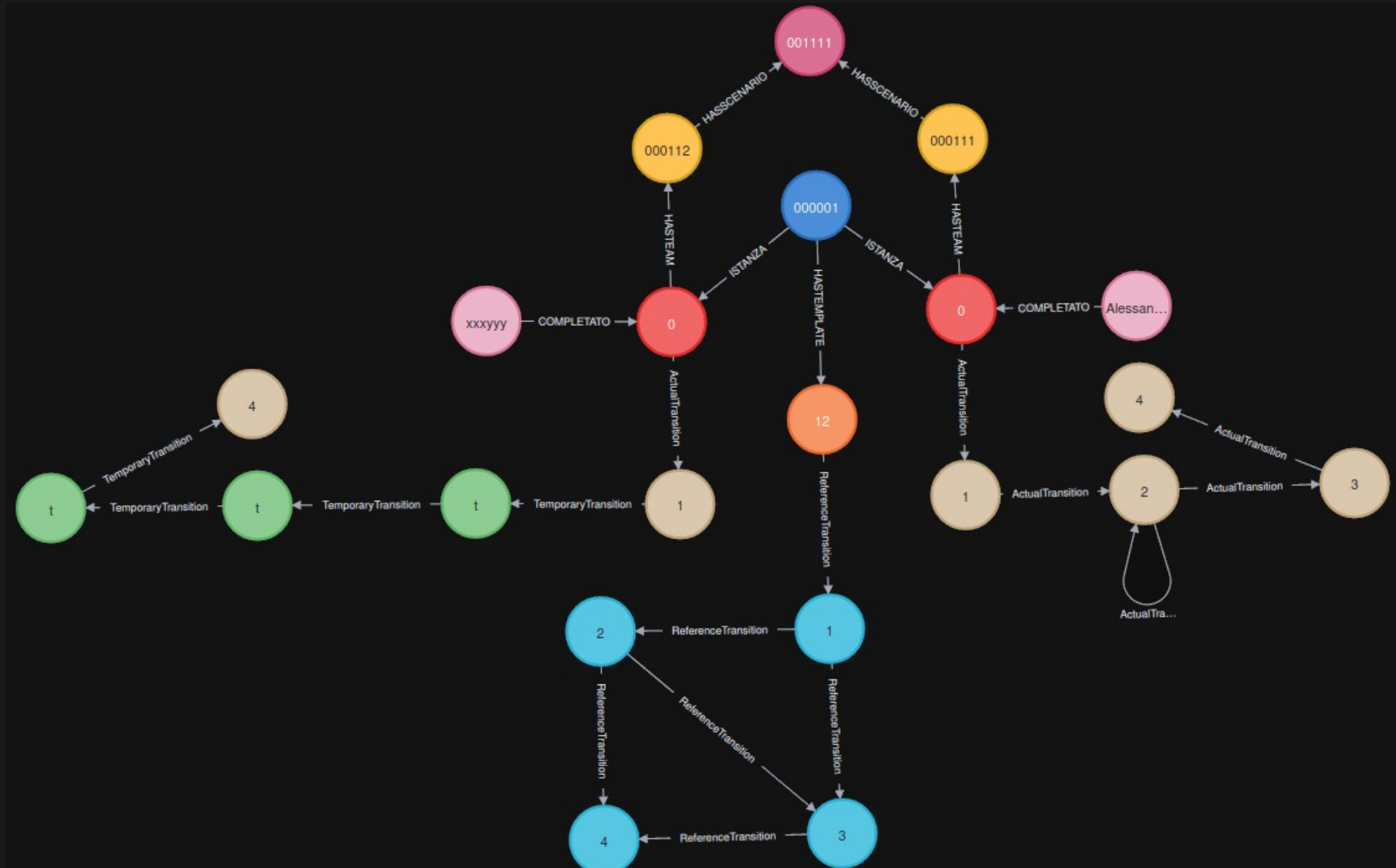
Azioni nel ReferenceGraph:

```
"{'azione1': 'ls', 'azione2': 'pwd', 'azione3': 'cmd'}"
```

TraineeGraph - Casi Specifici



Scenari Complessi



IMPLEMENTAZIONI FUTURE

- Ridefinizione Scoring System
- Implementazione funzioni Api REST
- AI/Machine Learning

END

Vi ringrazio per l'attenzione

SITOGRAFIA

- Revealjs
- Neo4j
- Fluentd
- Elasticsearch
- Maven

«Imparare è un'**esperienza**; tutto il resto è solo **informazione**.»