Rilevazione di vulnerabilità software in librerie di terze parti

Dipartimento di Matematica “Tullio Levi Civita”
Università di Padova

Corso di Laurea in Informatica

Gionata Legrottaglie
1102654

13/12/2023

UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO MATEMATICA

Anno accademico 2022/2023

Indice

L'azienda

SANMARCO INFORMATICA

Aziende clienti 2000
alla ricerca e sviluppo

Dipendenti 600+

Risorse dedicate 200+
alla ricerca e sviluppo

Partner 12

Business Unit 11

Le sedi

- Grisignano di zocco (VI)
- Vicenza (VI)
- Reggio Emilia (RE)
- Vimercate (MB)
- Tavagnacco (UD)
- Barletta (BT)

La proposta di stage

La crescita di Sanmarco Informatica S.p.A.

- Crescita dei prodotti in sviluppo
- Suddivisione in moduli dei prodotti esistenti
- Crescita delle installazioni clienti

Le nuove problematiche

- Ricerca delle vulnerabilità software
- Tracciabilità delle versioni installate

La proposta di stage

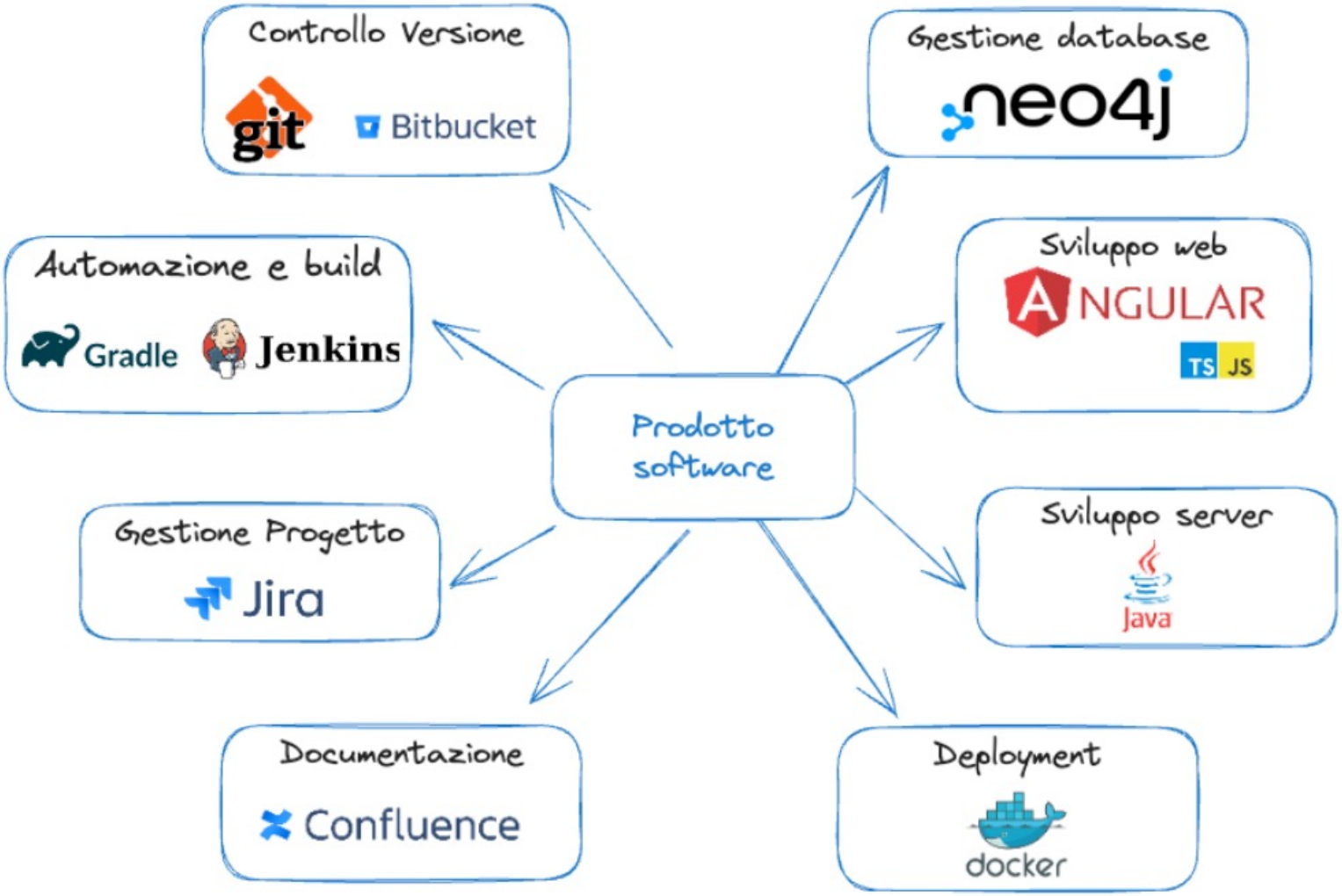
Dipendenze software di terze parti


Analizzare


Interrogare


Monitorare

Tecnologie utilizzate



Obiettivi dello stage

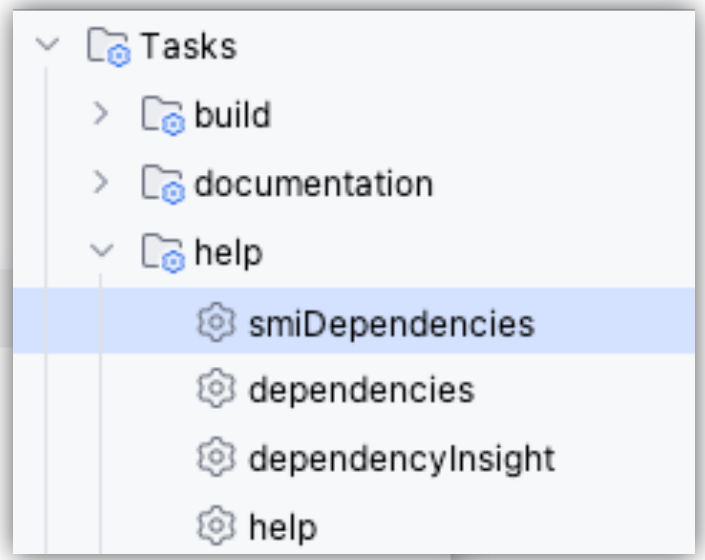
Obbligatori

- Plugin Gradle per la raccolta delle informazioni
- REST API per il salvataggio e l'interrogazione
- Interfaccia grafica per analisi e interrogazioni
- Integrazione con Jenkins

Desiderabili

- Verifica di nuovi aggiornamenti
- Analisi vulnerabilità
- Login LDAP
- Visualizzazione grafica delle dipendenze

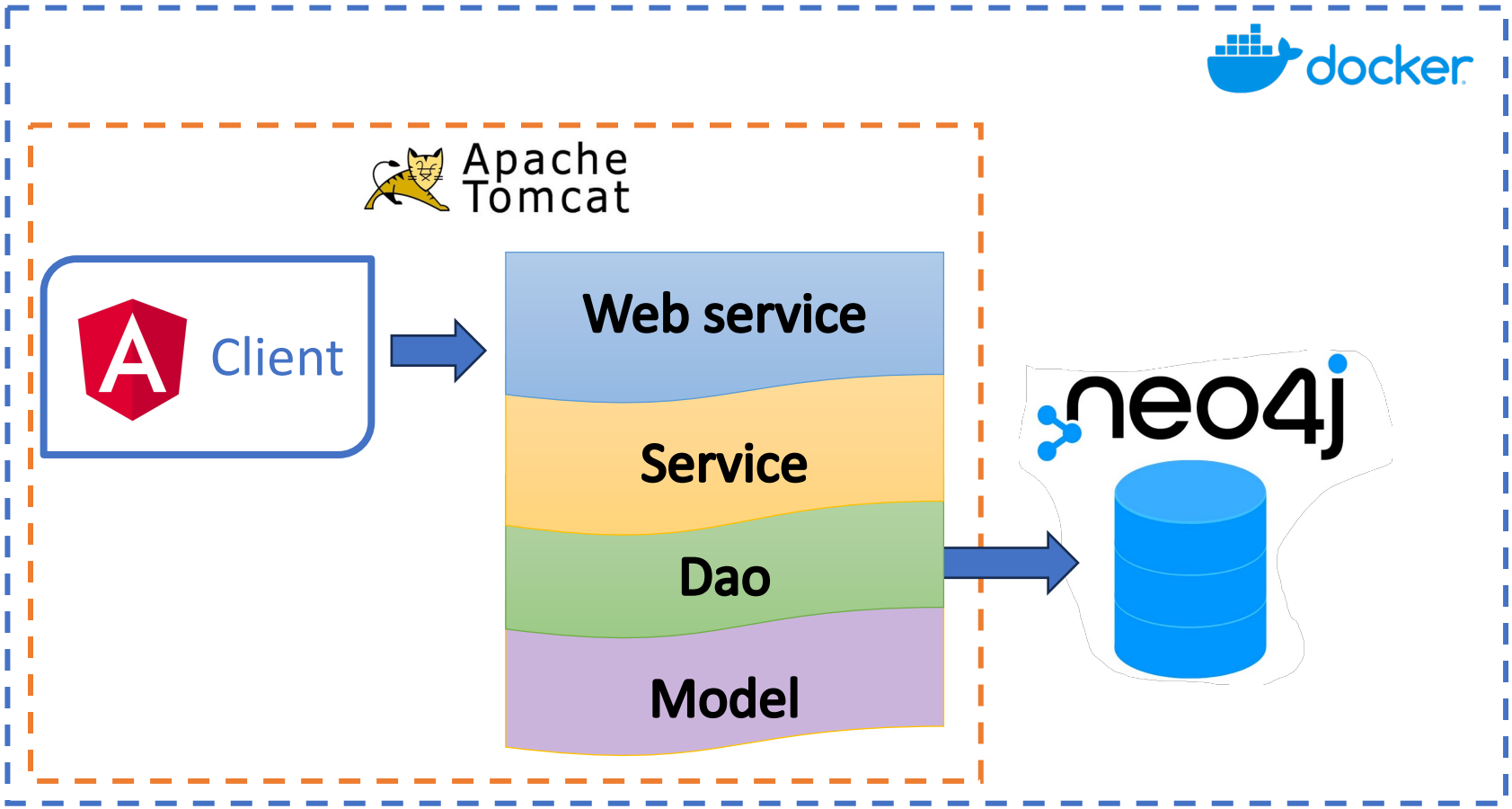
Il plugin




```
apply plugin: 'com.smi.SmiDependencyAnalyzer'

smi_dependency_analyzer {
    username = "nome_utente"
    password = "private_key"
    url = "http://localhost:8080/smi-dependency-store"
    npmProject {
        packageJson = "/projects/esempio1/client/package.json"
        packageLockJson = "/projects/esempio1/client/package-lock.json"
    }
}
```

Infrastruttura e backend



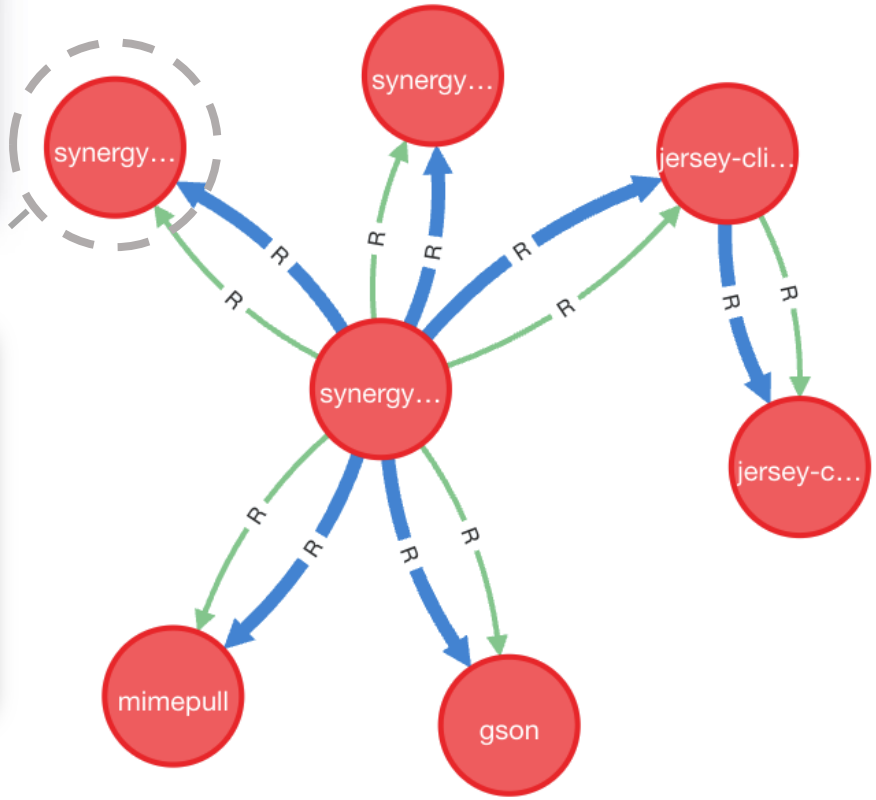
Neo4J e le query con Cypher

```
1 MATCH (N1)-[L:DEPENDS_ON]->(N2)
2 WHERE N1.id = 'net.synergy2:synergy2-ws:1.0.0'
3 RETURN N2
4 ORDER BY N.id
```

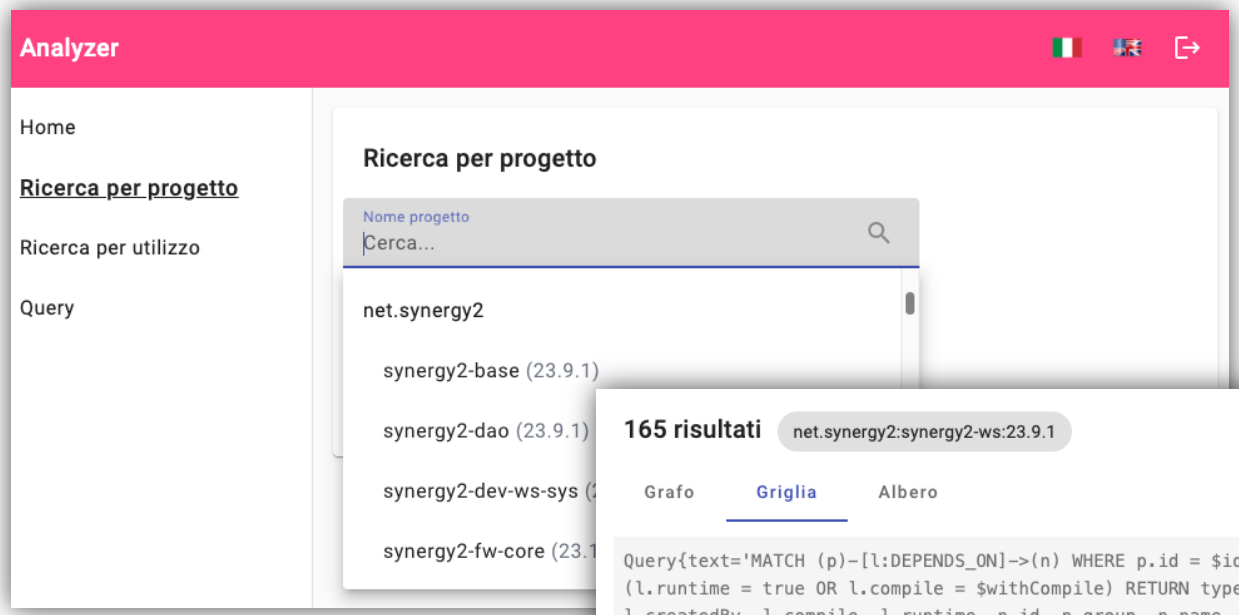
Node properties

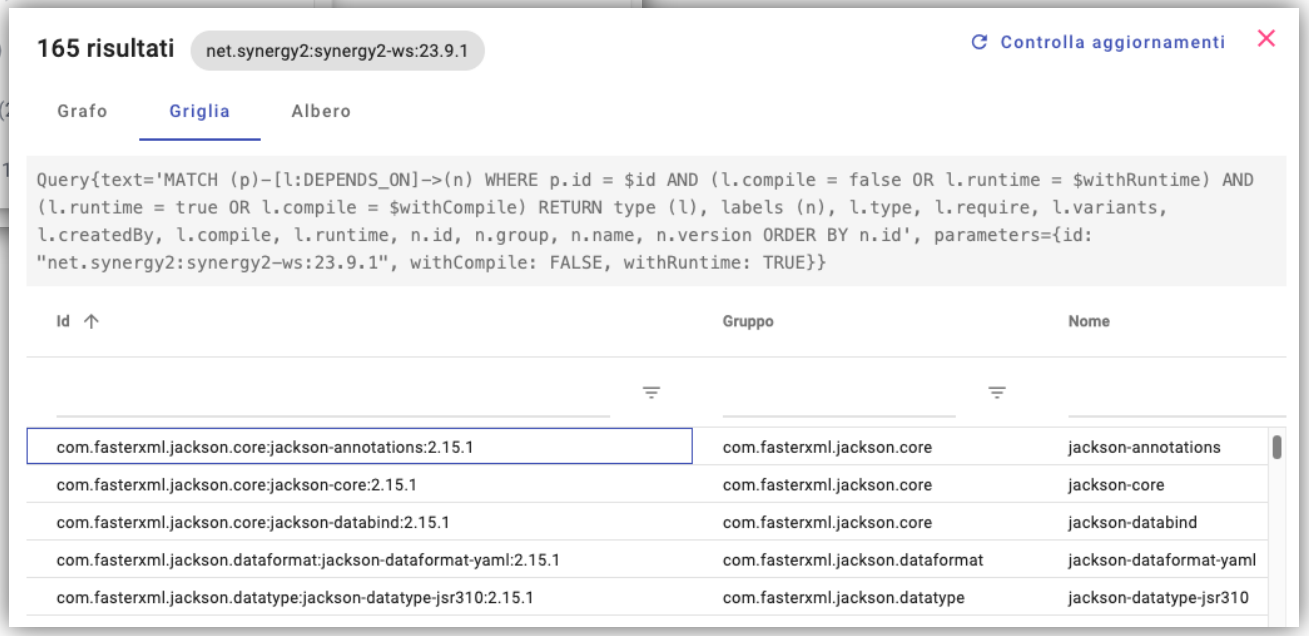
Package java

<id>	53
group	net.synergy2
id	net.synergy2:synergy2-rest-util:23.9.1
name	synergy2-rest-util
version	23.9.1



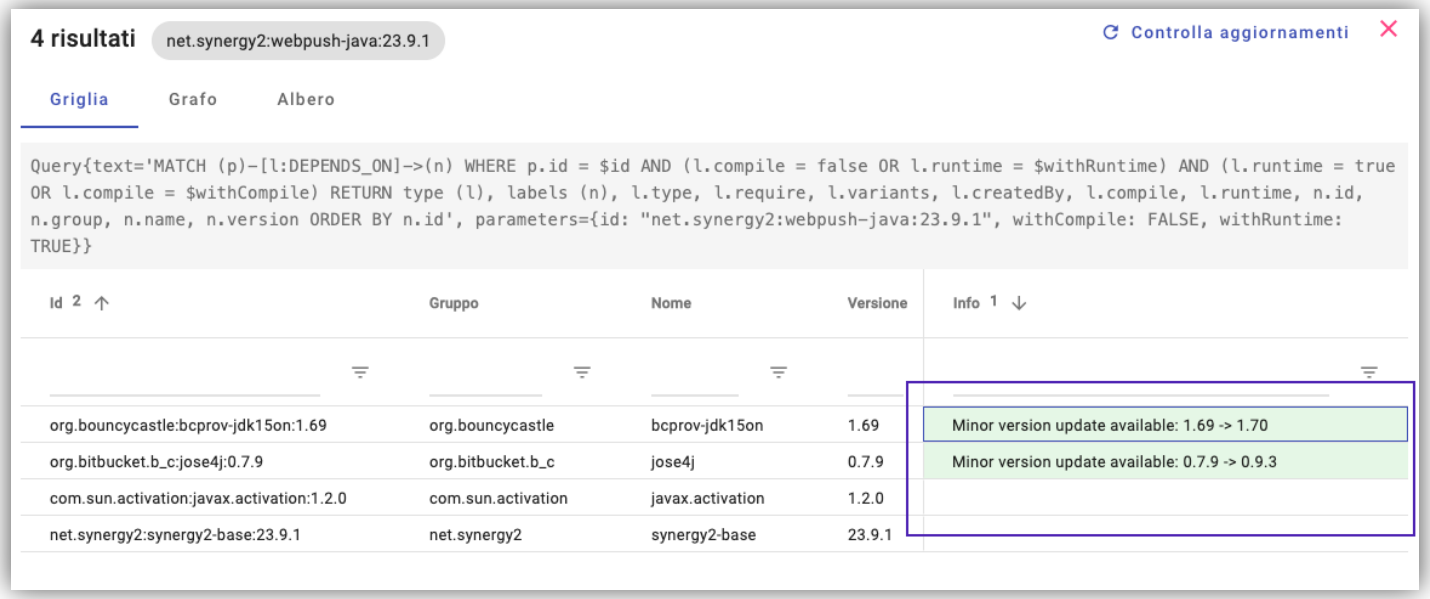
Implementazione



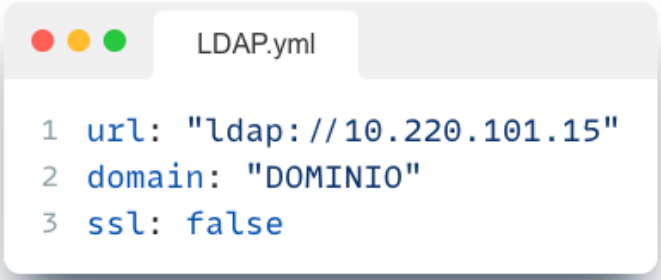


Implementazioni facoltative

Controllo aggiornamenti



LDAP



Obiettivi raggiunti

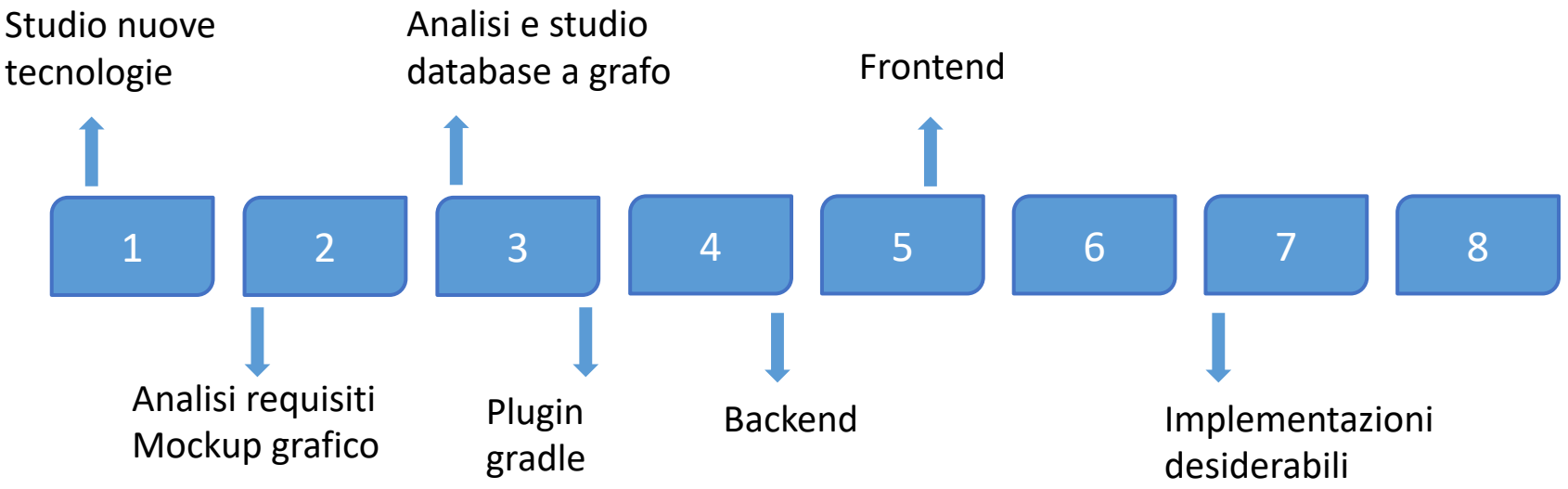
100% degli obiettivi soddisfatti

- Righe di codice sorgente
  - Plugin gradle: **655**
  - Backend: **1583**
  - Client: **1872**
- Test di unità: **28**
- Test di integrazione: **15**
- Test End-to-End: **10**

- Analisi dei requisiti
- Mockup grafico
- Analisi dei casi d'uso
- Documentazione tecnica
- Documentazione utente

Conclusioni

Ripartizione attività



Ore totali effettuate: 320

- **Ore analisi: 80**
- **Ore formazione: 90**
- **Ore sviluppo: 130**
- **Ore sviluppo: 130**

Conclusioni

Personali

- ✓ Gestione progetti con Gradle
- ✓ Creazione di plugin Gradle
- ✓ Sperimentazione nuova versione di Angular
- ✓ Database a grafo

Aziendali

- ✓ Prototipo per monitoraggio delle dipendenze
- ✓ Sperimentazione database a grafo