

Un sistema di recommendation per la cybersecurity basato su Collaborative Filter

Andrea Michele Albonico

24 Febbraio 2020

I sistemi IT attuali sono **complessi** ed **eterogenei**, attività di *Security Assurance* diventano fondamentali

- numerosi strumenti di sicurezza esistenti
- spesso **complessi** da utilizzare
- difficilmente accessibili a utenti poco esperti

Sviluppare un **sistema di raccomandazione di verifiche di sicurezza** che consenta di:

- suggerire agli utenti quali sono le verifiche **più adatte** per i loro sistemi
 - ▶ sulla base di diversi parametri
- fornire un **supporto** alle **attività di *Security Assurance***

Framework di *Security Assurance*

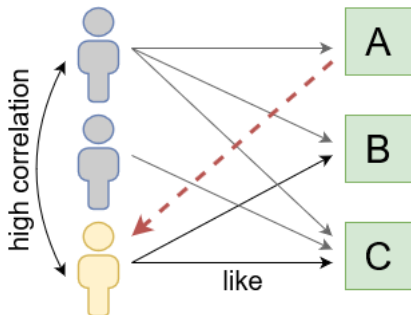
- erogato *as-a-Service*
 - ▶ l'utente configura le verifiche (*Evaluation*) di sicurezza
 - ▶ Moon Cloud le esegue e mostra risultati
- controllo *centralizzato* della sicurezza di un sistema



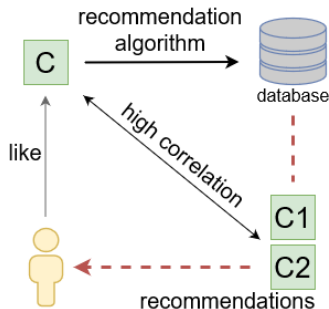
Un *recommendation system* filtra i dati usando diversi algoritmi e raccomanda gli item più rilevanti agli utenti attraverso un procedimento a 3 fasi

- 1 **raccolta di dati**: ottenere informazioni rilevanti e consistenti su cui applicare algoritmi di raccomandazione
- 2 **memorizzazione di dati**: la quantità di dati definisce quanto efficace un modello di raccomandazione può diventare
- 3 **filtraggio dei dati**: estrarre le informazioni più rilevanti

Recommendation Algorithms

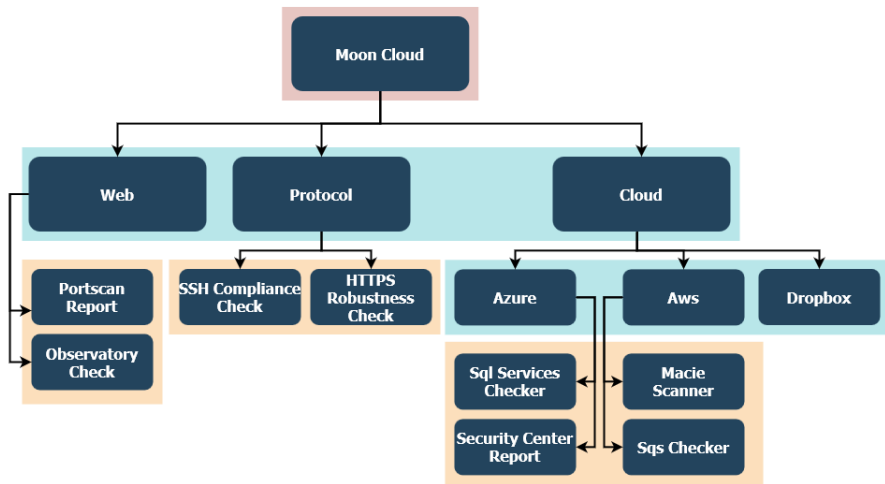


User Based Collaborative Filter:
algoritmo che fornisce dei suggerimenti sulla base di uno o più vicini (*neighbours*)



Item based Collaborative Filter:
algoritmo che confronta gli item dell'utente a cui si vuole raccomandare e i possibili item simili

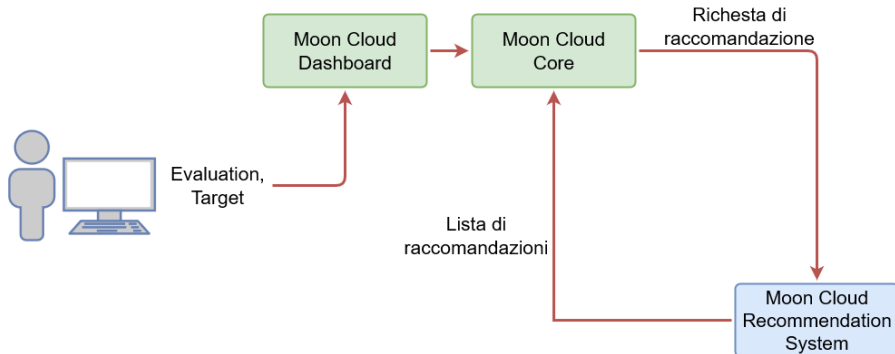
Tassonomia



Servizio di **API REST** che implementa un **sistema di raccomandazione integrato** nel **backend** di Moon Cloud

- offre diversi tipi di raccomandazioni per **suggerire *Evaluation***
 - ▶ **user-based** basato su *Evaluation* passate eseguite dall'utente
 - ▶ **item-based** basato su *Evaluation* o *Target*
 - ▶ **ibrido** condensa i pregi dei precedenti algoritmi
- garantisce la **coerenza** tra il database principale di Moon Cloud e quello usato dal servizio

Soluzione (2)



La soluzione introduce un sistema di raccomandazione in un contesto in cui spesso non è presente

- la configurazione delle **attività di test** vengono **semplificate**
- la *Security Assurance* diventa maggiormente accessibile