

Un sistema di recommendation per la cybersecurity basato su Collaborative Filter

Andrea Michele Albonico

24 Febbraio 2020

Il mondo del Cloud in cooperazione con i sistemi IT ha portato molti benefici, tuttavia vengono sollevate diverse problematiche

- questi sistemi sono spesso **complessi e impegnativi da gestire** se non si hanno conoscenze approfondite in materia, soprattutto per utenti poco esperti

Moon Cloud è una piattaforma erogata come servizio, la quale supporta un framework di *Security Assurance*, basato su Controlli ed Evaluation



Garantisce il controllo della sicurezza informatica in modo rapido ed efficiente, attraverso attività di test e monitoraggio periodiche e programmate

Introduzione di un **sistema di raccomandazione** che possa consigliare all'utente delle possibili *Evaluation* rispetto al *target* che vuole proteggere e monitorare

- l'utente meno esperto può usufruire dei servizi offerti da Moon Cloud in modo **semplice** e **intuitivo**
- viene supportato in ogni fase dall'inserimento delle informazioni del target da proteggere fino alla scelta delle attività di monitoraggio da eseguire

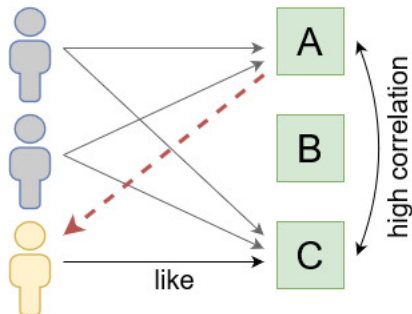
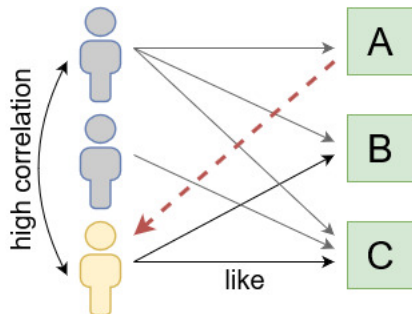
Un *recommendation system* può filtrare i dati usando differenti algoritmi e raccomandare gli item più rilevanti agli utenti attraverso un procedimento a 3 fasi

- 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

Questo sistema predice la preferenza che un utente accorderebbe a un item basandosi sulle preferenze date da altri utenti

- **semplici da implementare, intuitivi** e non necessitano di operazioni di training sui dati e regolazione di molti parametri
- permettono all'utente di comprendere le ragioni che si celano dietro ad ogni raccomandazione

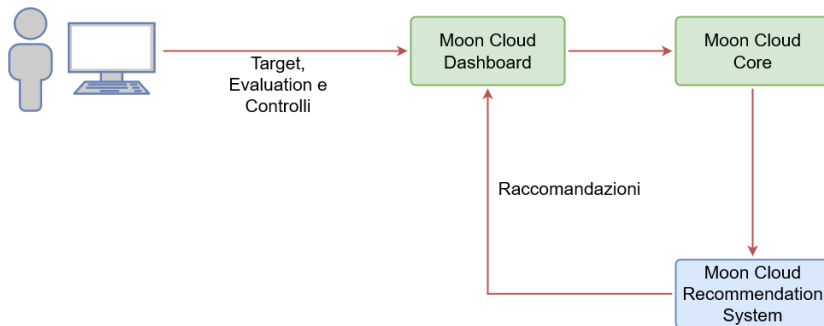
Recommendation Algorithms



Servizio di **API REST** accessibile attraverso apposite URL che permette di effettuare richieste al sistema di raccomandazione e di aggiornare la base di dati

- 1 in base alle informazioni inserite dall'utente sul **target** da proteggere e alle Evaluation usate vengono generate delle liste
- 2 queste liste contengono le Evaluation da raccomandare a quell'utente

Soluzione (2)



La soluzione introduce un sistema di raccomandazione in un mondo in cui spesso non è presente perché popolato da utenti esperti

- la configurazione delle attività di test vengono semplificate
- un maggior numero di utenti può fare uso di questi sistemi in totale sicurezza e affidabilità