UNIVERSITÀ DEGLI STUDI DI MILANO

FACOLTÀ DI SCIENZE E TECNOLOGIE

Corso di Laurea in Informatica Musicale

Mooncloud recommendation system

Relatore:
Claudio Agostino Ardagna
Correlatore:
Nome COGNOME

Tesi di Laurea di:
Andrea Michele Albonico
Matricola: 886667

Anno Accademico 2019/2020

Ringraziamenti

Andrea Michele Albonico

Prefazione

I sistemi di raccomandazione (*Recommendation System*) hanno avuto un forte sviluppo negli ultimi decenni e nascono proprio con lo scopo di identificare quegli oggetti (detti generalmente *item*) all'interno di vasto mondo di informazioni che possono essere di nostro interesse e tanto maggiore è il grado di conoscenza dell'individuo e tanto più vengono ritenuti affidabili.
Il motivo di questo successo risiede nella riuscita integrazione di tali sistemi in applicazioni commerciali, soprattutto nel mondo dell'E-commerce e nel fatto che sono in grado di aiutare un utente a prendere una decisione che sia la scelta di un film per l'uscita con gli amici il sabato sera, di una playlist da ascoltare durante un viaggio in auto o in un momento di lettura, e via discorrendo.
MoonCloud è una piattaforma erogata come servizio che fornisce un meccanismo di *Security Governance* centralizzato. Garantisce il controllo della sicurezza informatica in modo semplice e intuitivo, attraverso attività di test e monitoraggio periodiche e programmate (*Security Assurance*). L'obbiettivo di questa tesi è stato quello di aggiungere, al già presente sistema per la scelta dei controlli all'interno delle attività di test, un sistema di raccomandazioni che possa consigliare all'utente delle possibili *evaluation* rispetto ai dati relativi al target indicato; in questo modo anche l'utente meno esperto può usufruire dei servizi offerti da MoonCloud in modo semplice e intuitivo.

La tesi è organizzata come segue:

Capitolo 1 – Introduzione a MoonCloud

Capitolo 2 – Descrizione delle attività preliminari studi e analisi di soluzioni esistenti, studi delle tecnologie utilizzate nel seguito del lavoro.

Capitolo 3 – Descrizione delle attività svolte per conseguire gli obiettivi: Descrivere le attività svolte, riportando attivita, tempi, strumenti utilizzati, risultati conseguiti, problemi affrontati e modalita di risoluzione. Potranno essere qui descritte le attività anche dal punto di vista strettamente tecnico, approfondendo le scelte effettuate, le moti-

vazioni, le alternative prese in considerazione, l'uso o il possibile uso dei risultati del lavoro.

Capitolo 4 – Presentazione dei risultati e conclusioni] La presentazione dei risultati dovrebbe consistere in una descrizione tecnica dei risultati raggiunti,unitamente ad un commento critico e ad un'analisi della rispondenza agli obiettivi iniziali (si consiglia pertanto di motivare la rilevanza dei risultati e l'eventuale scostamento dagli obiettivi iniziali). La sezione relativa ai risultati dovrebbe infine contenere una sintesi critica e un giudizio sull'esperienza effettuata, che renda conto di aspetti positivi e negativi per il tirocinante e per l'ente ospitante, del valore formativo, professionale e umano, così via.

Indice

Prefazione **v**

1 Introduzione **1**
1.1 Perchè Moon Cloud? 1
1.2 Moon Cloud Architecture 3

2 Tecnologie **5**

3 Sistemi di raccomandazione **7**

4 Descrizione approfondita del progetto **9**

5 Conclusioni **11**

Bibliografia **13**

Elenco delle figure

1.1 Security Compliance Evaluation 3

Capitolo 1

Introduzione

In questo capitolo verrà descritto in modo più approfondito il funzionamento della piattaforma Moon Cloud e unitamente al motivo dell'implementazione della soluzione proposta.

1.1 Perchè Moon Cloud?

La diffusione di sistemi ICT (*Information and Communications Technology*) nella maggiorparte degli ambienti lavorativi e privati in termini di servizi offerti, automazione di processi e incremento delle performance. L'uso di questa tecnologia ha assunto importanza a partire dagli anni novanta come effetto del boom di Internet. Oggi le professionalità legate all'ICT crescono in numero e si evolvono per specificità, per operare in ambienti fortemente eterogenei ma sempre più interconnessi fra di loro come cloud computing, social newtwork, marketing digitale, IoT, realtà virtuale, ecc.

Il prezzo che paghiamo per i benefici di queste tecnologie è dato dall'incremento di violazione di sicurezza, che oggigiorno preoccupa tutte le aziende, e di conseguenza anche i loro clienti, con l'incremento del rischio di fallimento per i servizi più importanit, violazioni della privacy e furto di dati.
Il mercato sta lentamente notando che non è l'inadequamento tecnologico dei sistemi di sicurezza che incrementa il rischio di furti di dati o violazioni di sicurezza; piuttosto, la mal configurazione e errata integrazione di questi sistemi nei processi di business sono la base per i furti e le violazioni. [1]

Per questo motivo anche se vengono usati i sistemi di sicurezza e di controllo migliori non è possibile garantire la sicurezza; ma è necessario implementare un processo continuo di diagnostica che verifica che controlli sono configurati in modo corretto e il loro comportamento è quello aspettato.

Security assesment diventa allora un aspetto importante specialmente negli ambienti cloud e IoT. Questo assesment deve essere fatto in modo continuo e olistico, per correlare le prove raccolte da sempre maggiori meccanismi di protezione
Moon Cloud è una soluzione PaaS (Platform as a Service) che fornice una piattaforma B2B innovativa per verifiche, diagnostiche e monitoraggio dell'adeguatezza dei sistemi ICT rispetto alle politiche di sicurezza, in modo continuo e su larga scala. Moon Cloud supporta una semplice ed efficente *ICT security governance*, dove le politiche di sicurezza possono essere definite dalle compagnie stesse (a partire da un semplice controllo sulle vulnerabilità a linee guida di sicurezza interna), da entità esterne, imposte da standard oppure da regolamentazioni nazionali/internazionali.
La sicurezza di un sistema o di un insieme di asset dipende solo parzialmente dalla forza dei singoli meccanismi di protezione isolati l'uno dall'altro; infatti, dipende anche dall'abilità di questi meccanismi di lavorare continuamente in sinergia per provvedere a una protezione olistica. In più, quando i sistemi cloud e i servizi IoT sono coinvolti, le dinamiche di questi servizi e la loro rapida evoluzione rende il controllo dei processi all'interno dell'azienda e le politiche di sicurezza più complesse e prone ad errori.
I requisiti ad alto livello fondamentali per poter garantire le security assurance sono:

sistema olistico è richiesta una visione globale e pulita dello stautus dei sistemi di sicurezza; inoltre è cruciale distribuire lo sforzo degli specialisti in sicurezza per migliorare il processo e le politiche messe in atto. Si parte da della valutazioni fatte manualmente a quella semi-automatiche che ispezionano i meccanismi di sicurezza.

monitoraggio continuo ed efficiente è necessario un controllo continuo che valuti l'efficenza dei sistemi di sicurezza per ridurre l'impatto dell'errore umano, soprattutto dal punto di vista organizzativo. La mancata configurazione dovuta al cambiamento dell'ambiente, la coesistenza di componenenti in conflitto: sono scenari che richiedono un monitoraggio e un aggiornamento continuo.

singolo punto managment avere un solo punto in cui gestire tutti gli aspetti relativi alla sicurezza, permette di avere sotto controllo le politiche di sicurezza, Inoltre disporre di un inventario degli asset da proteggere, così da poter conoscere quali protezioni applicare.

reazioni rapide a incidenti di sicurezza spesso la reazione ad incidenti di sicurezza è ritardata da due fattori: il tempo richiesto per rilevare l'incidente e il tempo per analizzare il motivo dell'accaduto.

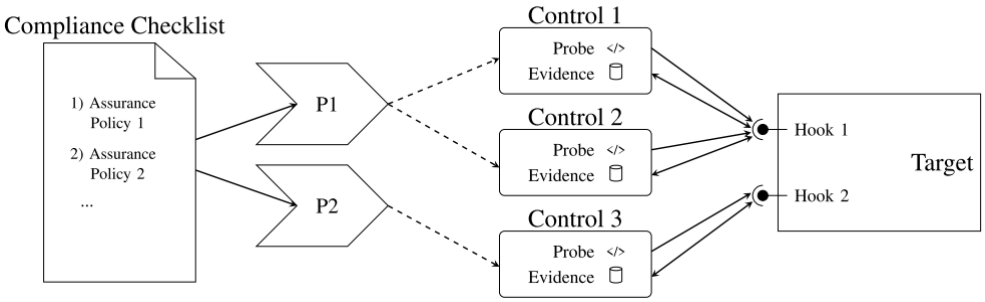

Figura 1.1: Security Compliance Evaluation

Moon Cloud è basato su una tecnica di security assurance garantendo che tutti le attività aziendali si compiano seguendo i requisiti prestabiliti da appropriate politiche e procedure.

Una security compliance evaluation è il processo di verifica che un target è sottoposto il cui risultato deve soddisfare i richiesti standard e politiche. Da questi processi di verifica, che devono a loro volta essere affidabili, si ottendo delle evidence (prove); queste ultime possono essere raccolte monitorando l'attività del target oppure, come già menzionato, sottoponendo il target a scenari critica o testing. In particolare, una security compliance evaluation è un processo che verifica la compliance (uniformità) di un certo target a una o più politiche; vengono eseguiti tutti i controlli e produce un valore booleano per le politiche, in base al valore booleano associato ad ogni controllo.

1.2 Moon Cloud Architecture

Moon Cloud implementa il processo di compliance in Figura 1 usando controlli di monitoraggio o di test e un sistema di security compliance evaluation personalizzabile. Inoltre garantisce tutti i requisisti ad alto livello elencati prima:

Moon Cloud è una piattaforma cloud centralizzata presentando una visione olistica dello stato di sicurezza di un dato sistema.

Moon Cloudimplementa un sistema di assurance evidence-based continuo, implementato come processo di compliance, basato su politiche custom o standard.

Moon Cloud è offerto come un servizio - PaaS, dove le attività di evaluation possono essere facilmente e efficentemente configurate su un target asset, senza l'intervento dell'uomo.

Moon Cloud permette di schedulare delle ispezioni automatiche, grazie all'inventario di asset protetto.

Moon Cloud evaluation engine può ispezionare dall'interno, gestendo delle minaccie interne; permettendo anche reazioni rapide a incidenti di sicurezza e veloci rimedi, grazie alla raccolta di continua di evidence.

L'architettura di Moon Cloud è costituita da un'assurance manager che gestisce i processi di evaluation attraverso un set di *execution cluster*; ogni execution cluster gestisce ed esegue un set di probe collezionando le evidence necessarie per le evaluation. Tutte le attività di collezione sono eseguite dal probe. Ogni probe è uno script di python fornito come una sigola immagine di Docker, che viene inizializzata quando è triggerata una evaluation ed è distrutta quando il processo di evaluation è terminato.
Accedendo alla piattaforma di Moon Cloud, l'utente può definire le proprie politiche di sicurezza e attività di evaluation come espressioni booleane di controlli di sicurezza e altre politiche predefinite. Una volta che una politica viene definita, l'utente può decidere quando schedulare l'evaluation; e nel momento in cui un processo di evaluation viene inizializzato, tutti i controlli vengono eseguiti e i risultati dell'espressioni booleane vengono memorizzati e restituiti all'utente. A questo punto l'utente può accedere a questi risultati a diversi gradi di precisione: una visione sommaria e generale di tutte le politche implentate e dello stato generale del sistema di sicurezza, al risultato di una specifica politica oppure alle evidence raccolte per una evaluation.

Capitolo 2

Tecnologie

Capitolo 3

Sistemi di raccomandazione

Capitolo 4

Descrizione approfondita del progetto

Capitolo 5

Conclusioni

Bibliografia

[1] M. Anisetti et al. «Moon Cloud: A Cloud Platform for ICT Security Governance». In: (dic. 2018), pp. 1–7. DOI: 10.1109/GLOCOM.2018.8647247.