

IBM annuncia la piattaforma comune di servizi cloud per le applicazioni di cybersecurity

IBM Security Connect permette la collaborazione grazie a open standard e AI

Armonk - 15 ott 2018: IBM ha annunciato oggi una nuova piattaforma di collaborazione per applicazioni di cyber security. IBM Security Connect è la prima piattaforma cloud di sicurezza costruita su tecnologie aperte e di federazione che sfrutta l'intelligenza artificiale, in grado di analizzare dati e informazioni provenienti da strumenti e ambienti precedentemente non connessi.

Un'analisi svolta da IBM basandosi sui dati degli ambienti informatici dei propri clienti evidenzia che, in media, in ambito cybersecurity vengono utilizzati oltre 80 prodotti di sicurezza di 40 diversi fornitori. La ricerca indica inoltre che questi strumenti sono utilizzati al 20 per cento delle loro funzionalità e che non sono in grado di fornire gli esiti che i clienti si aspettano a causa delle problematiche di integrazione e complessità.

Integrando i dati di sicurezza forniti dalle soluzioni di IBM Security in un ecosistema di fornitori, clienti e partner aziendali, IBM Security Connect è progettato per migliorare l'efficienza e la collaborazione nell'attività di difesa dei team dai crimini informatici. IBM Security Connect consentirà agli utenti di applicare machine learning e AI, compreso Watson for Cyber Security, per un'analisi che li aiuti a identificare le minacce e i rischi e a migliorare l'efficacia e l'efficienza del rilevamento delle minacce e della relativa risposta. Gli utenti possono progettare e utilizzare nuove soluzioni di sicurezza personalizzate e complete per indirizzare i risultati in termini di sicurezza, come ad esempio i flussi di lavoro dei SOC o Digital Trust.

IBM Security Connect estenderà il ricco set di funzionalità dei prodotti di sicurezza IBM tramite potenti capacità di integrazione per connettere dati, applicazioni e strumenti di un ecosistema di fornitori grazie al Cloud.

“La crescita della tecnologia e dei dati per la sicurezza informatica, unita alla scarsità di competenze, sta creando un livello di complessità inaspettato per i team che si occupano di sicurezza,” spiega Marc van Zadelhoff, General Manager, IBM Security. “Grazie al potenziale del cloud, possiamo ora unire strumenti, dati e persone senza costosi progetti di personalizzazione e integrazione. La federazione dei dati attraverso IBM Security Connect contribuisce a fornire ai professionisti della sicurezza una maggiore visibilità ed efficienza senza il problema della migrazione dei dati o di integrazioni di prodotto estremamente complesse.”

Un approccio nuovo ed aperto alla sicurezza del cloud

IBM Security Connect permetterà di affrontare le sfide della sicurezza di oggi attraverso open standard che contribuiranno a gettare le basi dell'innovazione collaborativa. Le aziende potranno sviluppare microservizi unici, sviluppare nuove applicazioni di sicurezza, integrare le soluzioni esistenti e trarre vantaggio dai dati provenienti da servizi condivisi open.

I servizi fondamentali includono servizi di integrazione dei dati di sicurezza per condividere e normalizzare la threat intelligence, la ricerca di dati federati in repository on-premise e su cloud, soluzioni di sicurezza, condivisione in tempo reale di allarmi ed eventi di sicurezza e informazioni che possono essere sfruttate da applicazioni o da soluzioni integrate nella piattaforma.

IBM Security Connect ospiterà pertanto Security App Exchange di IBM e tutte le applicazioni di sicurezza IBM sviluppate su piattaforma IBM Cloud e totalmente compatibili con altri cloud provider. IBM Security si

dedicherà alla creazione di nuovi standard aperti in aree in rapido sviluppo, come la condivisione di playbook di risposta e modelli analitici, ed investiranno in maniera attiva nello sviluppo di progetti open source allineati sulla base di questo impegno.

L'impegno di IBM Security verso il mondo open significa anche che molti standard e protocolli esistenti sono utilizzati e disponibili sulla piattaforma, come ad esempio STIX™ (Structured Threat Information eXpression) e TAXII™ (Trusted Automated eXchange of Indicator Information). Il progetto di sicurezza IBM [STIX-Shifter](#), disponibile su GitHub, consiste in una libreria open source che permette al software di connettersi a prodotti con repository di dati che utilizzano STIX Patterning e di reinviare i risultati sotto forma di STIX Observations. L'utilizzo di questi standard aperti per connettersi a qualsiasi sorgente di dati, insieme alla tecnologia di security analytics e di risposta agli incidenti di IBM, aiuta i clienti a ottenere maggiore visibilità e a rilevare rischi e minacce che altrimenti passerebbero inosservati in quanto provenienti da ambienti ibridi complessi e non connessi.

Il set iniziale di applicazioni e servizi di IBM Security Connect consentirà agli utenti di connettere velocemente differenti prodotti di sicurezza e repository di dati per federare e correlare automaticamente tali dati allo scopo di prioritizzare e rispondere alle minacce. Questo rivoluzionario approccio di federare i dati permette ai clienti di lasciare i dati dove essi si trovano invece di creare costosi *data lake*, che possono complicare o addirittura impedire l'analisi dei dati stessi.

IBM Security Connect sarà inoltre parte integrante del portafoglio di offerta di IBM Security Services, sia come consumatore che contributore di elementi di innovazione; sono inclusi innovazioni nell'AI con funzioni vocali, machine learning per lo scoring di minacce di sicurezza, analisi globale delle minacce, playbook di orchestrazione e applicazioni MSS per dispositivi mobili. IBM Security Services incrementerà la potenza di IBM Security Connect per sviluppare integrazioni sempre maggiori con l'ecosistema dei partner al fine di garantire maggiore valore ai propri clienti in tutto il mondo.

Gestione della complessità delle operazioni di sicurezza informatica

IBM Security Connect, progettato per garantire strategie di sicurezza orientate alla comunità, opererà come piattaforma aperta con una comunità di sviluppo, anche questa open. L'annuncio di oggi include anche la notizia secondo la quale un buon numero di partner tecnologici e system integrator globali, tra cui Cisco, Carbon Black, EY, ForeScout, Fortinet, McAfee, Qualys, Smarttech, Symantec e Trend Micro, si sono adoperati per l'integrazione con IBM Security Connect al fine di fornire una migliore condivisione dei dati tra i maggiori fornitori di soluzioni di sicurezza del mercato. Inoltre, molti di questi contribuiranno alla creazione di applicazioni integrate su IBM Security Connect. IBM dispone già di centinaia di app predefinite realizzate da IBM e dai partner, disponibili tramite IBM Security App Exchange, per l'integrazione a livello dei prodotti. Una volta disponibili, queste integrazioni aggiuntive saranno inserite all'interno di IBM Security Connect, ampliando così la portata della piattaforma.

Ad esempio, una delle prime soluzioni ad essere testate dai clienti si occuperà del Threat Operations Workflow. Questa soluzione nasce per consentire agli analisti di sicurezza di identificare, analizzare e rispondere in maniera proattiva alle minacce più critiche per mezzo di un'unica soluzione in cloud. Threat Operations Workflow si integra facilmente tramite connettori aperti con QRadar (on-premise o su cloud) e con altre soluzioni SIEM e di sicurezza di endpoint. Sfruttando SDK aperti, repository di dati di sicurezza come Hadoop, e prodotti singoli di sicurezza questa soluzione fornisce una vista federata e un flusso di lavoro solitamente isolati e precedentemente non integrati.

Competenza e capacità integrate

In presenza delle sfide documentate che l'industria della sicurezza è in procinto di affrontare, IBM Security Connect possiede anche un team di oltre 4000 professionisti di IBM Security, con le migliori competenze digitali e in grado di fornire le migliori indicazioni su come implementare le strategie per la gestione dei rischi di sicurezza. Le app preintegrate consentono agli utenti di creare flussi di lavoro comuni in svariate applicazioni, in modo che i team possano focalizzarsi sulla soluzione dei problemi di sicurezza, invece di dovere adoperarsi per integrare dozzine di prodotti diversi. Oltre a ciò, IBM Security impiega 50 sviluppatori per lo sviluppo della comunità in cui i professionisti possono collaborare e condividere le integrazioni.

IBM Security Connect faciliterà l'accesso alle competenze di IBM X-Force Security Services, comprese le offerte e le competenze in X-Force Red Security Testing, Managed Security Services e Incident Response Services.

IBM Security Connect dovrebbe essere disponibile nei primi mesi del 2019.

Informazioni su IBM Security

IBM Security offre uno dei portafogli più evoluti ed integrati di prodotti e servizi per la protezione aziendale. Il portafoglio, supportato dall'attività di ricerca di IBM X-Force®, permette alle organizzazioni di gestire il rischio e di difendersi dalle minacce emergenti in maniera efficace. IBM possiede una delle organizzazioni di ricerca, sviluppo e delivery di prodotti e servizi di sicurezza più grandi al mondo, monitora 60 miliardi di eventi di protezione al giorno in più di 130 paesi ed ha ottenuto 8.000 brevetti di sicurezza a livello mondiale. Per maggiori informazioni, potete visitare il sito www.ibm.com/security, seguire IBM Security su Twitter o visitare il blog [IBM Security Intelligence](#).

Contatti

Claudia Ruffini

IBM Media Relations +393356325093 cla@it.ibm.com

Alessandro Ferrari

IBM Media Relations +393484554535 ale_federferrari@it.ibm.com
