

IBM ottimizza Cloud Pak for Security per migliorare la gestione delle minacce su tutti gli strumenti di sicurezza e di collaborazione e nel cloud

- Una piattaforma aperta che si avvale di intelligenza artificiale e automazione per razionalizzare la gestione delle minacce negli ambienti cloud ibridi e quando si utilizzando svariati tool di sicurezza
- Prima soluzione nel settore capace di connettere in un'unica piattaforma la gestione delle minacce con l'integrità dei dati e la gestione dell'identità
- Nuovi servizi di sicurezza chiavi in mano per far fronte alla mancanza di competenze di cybersecurity e alla diffusione del lavoro da remoto

ARMONK, NY, 15 ottobre 2020 - IBM (NYSE: IBM) Security ha annunciato l'arrivo di nuove funzionalità per Cloud Pak for Security, inclusa una soluzione all'avanguardia per la protezione dei dati che consente alle aziende di rilevare le minacce e proteggere i dati sensibili in ambienti cloud ibridi. IBM Cloud Pak è stato creato con l'obiettivo di riunire in una singola console tutte le tecnologie di sicurezza, spesso disconnesse tra di loro: IBM ha così ampliato Cloud Pak for Security per includere nuove sorgenti di dati, integrazioni e servizi che consentiranno di monitorare l'intero ciclo di vita delle minacce da un unico strumento.

Gli aggiornamenti di Cloud Pak for Security che saranno presto disponibili^[1] includono: 6 feed di threat intelligence; 25 connessioni preimpostate a sorgenti di dati sia IBM che di terze parti; 165 integrazioni di case management connesse attraverso soluzioni avanzate di AI che categorizzano le minacce e sistemi di automazione predefiniti e playbook per fornire ai team di security procedure semplificate per contrastare gli attacchi.

La crescente adozione del cloud e la diffusione del lavoro da remoto hanno ampliato il perimetro IT, rendendolo più dispersivo; con questa soluzione allo stesso tempo, i responsabili della cybersecurity possono disporre di informazioni molto più approfondite sullo stato di sicurezza degli ambienti di cloud ibrido. Se tradizionalmente la gestione delle informazioni su comportamenti degli utenti, identità e sicurezza dei dati è sempre stata separata da quella delle minacce, con le nuove funzionalità, Cloud Pak for Security diventa la prima piattaforma a connettere diversi tipi di dati e analytics sul comportamento degli utenti con le fasi di rilevamento, analisi e risposta.

Oggi, IBM annuncia funzionalità che rendono Cloud Pak for Security un tool ancora più all'avanguardia:

Risposta coordinata alle minacce e Sicurezza dei Dati : IBM ha sviluppato un nuovo approccio per consentire ai team di security di avere una visione completa delle attività sui dati, della conformità e dei rischi, senza bisogno di spostarsi dalla piattaforma principale di risposta agli incidenti. Il nuovo hub per la sicurezza dei dati, che verrà reso disponibile nel corso dell'ultimo trimestre del 2020, permetterà agli analisti di ottenere velocemente informazioni dettagliate riguardo dove risiedono i dati sensibili nel cloud ibrido, gli utenti che vi hanno accesso, le modalità in cui sono utilizzati e le strategie migliori per la loro protezione. Colmare la disconnessione tra la sicurezza dei dati e la gestione delle minacce può ridurre i tempi di risposta alla violazione dei dati, che attualmente richiedono mediamente più di sei mesi per essere identificati e contenuti, come dichiarato dalle organizzazioni recentemente intervistate^[2].

Accesso a strumenti di Threat Intelligence leader di settore: Cloud Pak for Security sta ampliando la propria collezione di Threat Intelligence, attraverso l'integrazione costante di informazioni verificate sulle minacce alla sicurezza che permettono agli utenti di rilevare i primi segnali di campagne di minaccia attive in tutto il mondo. Oltre all'IBM X-Force Threat Intelligence Feed, la piattaforma includerà 1 integrazioni predefinite di terze parti per altri cinque feed di threat intelligence come AlienVault OTX, Cisco Threatgrid, MaxMind Geolocation, SANS Internet StormCenter and Virustotal, che verrà rilasciata nel Q4, e altre integrazioni che verranno aggiunte nel 2021.

Servizi e supporto dedicati: IBM lancerà, inoltre, nuovi servizi di sicurezza che aiuteranno le organizzazioni a modernizzare la propria sicurezza con Cloud Pak for Security grazie ad un approccio olistico per connettere prodotti e servizi. Con una vasta gamma di pacchetti di servizi altamente flessibili, gli esperti IBM sono ora in grado di aiutare i clienti a rendere operativo e a gestire Cloud Pak for Security in ogni tipo di ambiente, supportandoli nella gestione delle minacce end-to-end, nella gestione dei servizi di security, così come con servizi di consulenza e supporto per l'integrazione.

"La complessità è la sfida più grande che il nostro settore si trova ad affrontare, in quanto obbliga i responsabili della sicurezza, spesso sottofinanziati, a cercare di connettere manualmente gli insight provenienti dagli strumenti e dalle fonti più disparate" ha affermato **Justin Youngblood, Vice President, IBM Security**. *"Cloud Pak for Security è una piattaforma aperta, che sfrutta tecnologie cloud native lungo tutta l'infrastruttura per connettere qualsiasi strumento all'ecosistema di sicurezza. Grazie a queste nuove funzionalità, IBM sarà la prima nel settore a connettere informazioni sulle minacce da fonti esterne e gestione delle minacce stesse con sicurezza dei dati e la gestione dell'identità: in questo modo, le aziende possono quindi evolvere le security operation e gettare le basi per una strategia di sicurezza zero trust"*.

Connessioni aperte lungo tutto l'ecosistema di sicurezza

Cloud Pak for Security sfrutta le tecnologie open per creare una base interoperabile e connessioni più strette tra i tool di IBM e quelli di terze parti. Per esempio, la piattaforma utilizza **STIX-Shifter**, una library open-source che permette agli analisti di security di ricercare indicatori di minacce all'interno di sorgenti di dati interconnesse grazie ad una sola query. Infine, la piattaforma è costruita su Red Hat **OpenShift**: ciò significa che Cloud Pak for Security fornisce una solida base, open e containerizzata, che può essere facilmente implementata in ambienti cloud on-premise, pubblici e privati.

Questo approccio open rende Cloud Pak for Security molto più di una semplice raccolta di strumenti di sicurezza, ossia una vera e propria piattaforma che consente l'integrazione di tutti i processi e i tool di sicurezza in ambienti cloud. La piattaforma sfrutta tecnologie

avanzate di intelligenza artificiale, analytics e automazione per semplificare l'intero processo di gestione delle minacce. Sono incluse le funzionalità di base per Security Information and Event Monitoring (SIEM), Threat Intelligence, User Behavior Analytics, Data Security e Security Orchestration Automation and Response. Queste funzionalità sono accessibili da una singola interfaccia utente, che permette di gestire ogni fase del processo -dal rilevamento della minaccia, all'identificazione della risposta- attraverso flussi di lavoro end-to-end.

Infine, grazie a questa nuova piattaforma, IBM Security rafforzerà il proprio supporto alla [Open Cybersecurity Alliance](#), di cui è parte, fornendo alla community nuovi strumenti per lo sviluppo e l'adozione di tecnologie open, con l'obiettivo di rendere la sicurezza più interoperabile.

Approccio unificato per prodotti e servizi

Grazie al proprio framework open, Cloud Pak for Security è la soluzione ideale per facilitare la collaborazione tra i team security interni alle aziende e i provider esterni che contribuiscono ad accrescere le abilità e le conoscenze delle aziende in tema di sicurezza. Cloud Pak for Security supporta il multi-tenancy e permette ai service provider di utilizzare anche una sola funzionalità della piattaforma per soddisfare le esigenze di più aziende e organizzazioni secondarie, tenendo sempre separati i dati di ciascuna.

Le vaste funzionalità di Cloud Pak for Security sono supportate da IBM Security e possono essere integrate con tutti i servizi dell'azienda. I clienti possono utilizzare [X-Force Threat Management](#), un servizio di gestione delle minacce end-to-end che utilizza un approccio programmatico per aiutare i clienti a rendere più matura la strategia di gestione delle minacce nel suo complesso, definendola e integrandola con il tempo. Le organizzazioni possono anche trarre beneficio da una vasta gamma di [IBM Managed Security Services](#), utilizzando Cloud Pak for Security per facilitare la collaborazione e la visibilità tra team e clienti in tempo reale. Inoltre, le aziende possono avvalersi di [consulenti esperti](#) di IBM Security per un supporto nella pianificazione, distribuzione e integrazione di Cloud Pak for Security nei piani di sicurezza già esistenti.

Per saperne di più su IBM Cloud Pak for Security e restare aggiornati sulle sue ultime funzionalità, visitare www.ibm.com/it-it/products/cloud-pak-for-security.

IBM Security

IBM Security offre uno dei portfolio più completi e integrati di prodotti e servizi per la protezione aziendale. Il portfolio, supportato dal team di ricerca di fama mondiale IBM X-Force®, consente alle organizzazioni di gestire con efficacia il rischio e difendersi dalle minacce emergenti. IBM dirige una delle organizzazioni di ricerca, sviluppo e delivery di soluzioni di sicurezza più grandi al mondo, monitora 70 miliardi di eventi di security al giorno in più di 130 Paesi e ha ottenuto oltre 10.000 brevetti di sicurezza. Per maggiori informazioni, visita il sito www.ibm.com/security, segui [@IBMSecurity](#) su Twitter o visita il blog di [IBM Security Intelligence](#).

Contatti

Claudia Ruffini
IBM Services and Enterprise Communications Leader
IBM Italia
Mobile +39 335 6325093
Email cla@it.ibm.com

[1] Disponibilità previste per il Q4 2020.

[2] Cost of Data Breach Report, condotto da Ponemon Institute, promosso da IBM Security

<https://it.newsroom.ibm.com/CloudPak4Security>