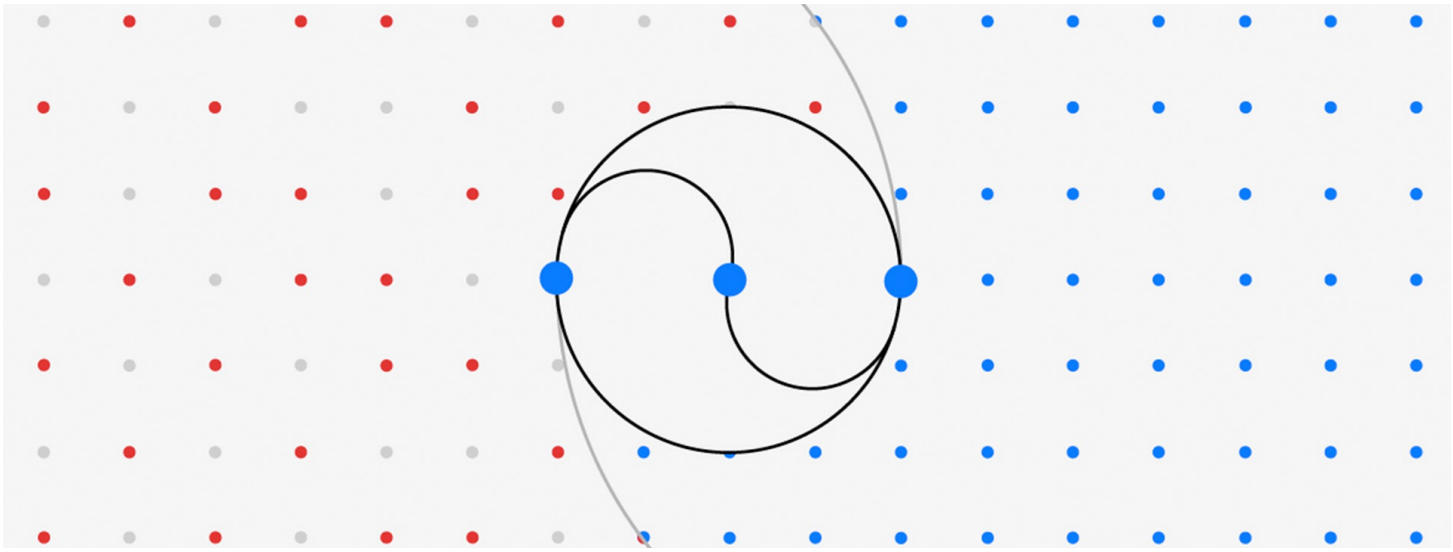
IBM Italy News Room

IBM annuncia nuovi servizi di rilevamento e risposta alle minacce basati sull'intelligenza artificiale

I nuovi servizi permettono di acquisire e analizzare i dati di sicurezza da un ampio ecosistema di tecnologie e fornitori, offrendo monitoraggio, indagine e correzione automatica degli avvisi di sicurezza 24 ore su 24, 7 giorni su 7



ARMONK, N.Y., 6 ottobre 2023 - IBM (NYSE: IBM) ha presentato l'evoluzione della sua offerta di servizi gestiti di rilevamento e risposta con nuove tecnologie AI, che include la possibilità di aumentare o chiudere automaticamente fino all'85% degli avvisi[1], contribuendo ad accelerare le tempistiche di risposta alla sicurezza per i propri clienti.

I nuovi servizi Threat Detection and Response Services (TDR) forniscono monitoraggio 24x7, indagini e correzione automatica degli avvisi di sicurezza rilevati da tutte le tecnologie presenti negli ambienti cloud ibridi del cliente, compresi gli strumenti di sicurezza e gli investimenti già previsti, nonché le tecnologie cloud, on-premise e operative (OT). I servizi gestiti vengono forniti dal team globale di analisti della sicurezza di IBM Consulting tramite la piattaforma di servizi di sicurezza avanzati di IBM, che applica più livelli di intelligenza artificiale e intelligence sulle relative minacce provenienti dalla vasta rete di sicurezza globale dell'azienda, aiutando così ad automatizzare la gestione dei messaggi e risolvere rapidamente le eventuali minacce.

"Attualmente i team di sicurezza non solo sono inferiori in termini numerici rispetto agli aggressori, ma vengono superati anche in termini di vulnerabilità, avvisi, strumenti e sistemi di sicurezza che hanno il compito di gestire quotidianamente", ha dichiarato **Chris McCurdy**, General Manager, Worldwide IBM Consulting Cybersecurity Services. *"Combinando in tempo reale l'analisi avanzata e la threat intelligence con l'esperienza umana, i nuovi Threat Detection and Response Services di IBM consentono di aumentare le difese di sicurezza dell'organizzazione grazie a una capacità scalabile, in continuo miglioramento e sufficientemente robusta per*

gestire le minacce di domani".

Gestione intelligente delle difese dalle minacce

I nuovi servizi TDR sono affiancati da una serie di tecnologie di sicurezza basate sull'intelligenza artificiale che supportano migliaia di clienti in tutto il mondo, in grado di monitorare miliardi di potenziali eventi di sicurezza al giorno. Il tutto sfruttando modelli di intelligenza artificiale che apprendono continuamente dai dati dei clienti del mondo reale, comprese le risposte degli analisti della sicurezza, e che sono progettati per chiudere automaticamente gli avvisi a bassa priorità e falsi positivi in base a un livello di sicurezza definito dal cliente. Questa funzionalità aumenta in modo automatico anche gli avvisi ad alto rischio che richiedono un'azione immediata da parte dei team di sicurezza, fornendo al contempo un contesto di indagine.

I servizi TDR di IBM sono progettati per fornire:

- **Regole di rilevamento crowdsourcing e avvisi ottimizzati.** Attraverso l'utilizzo delle informazioni giunte in tempo reale relative alla gestione delle minacce di IBM, i nuovi servizi impiegano l'intelligenza artificiale per valutare e suggerire costantemente quali sono le regole di rilevamento più efficaci, contribuendo così a migliorarne la qualità degli avvisi e accelerare i tempi di risposta. Questa funzionalità ha contribuito a ridurre del 45% gli avvisi SIEM (Security Information and Event Management) a basso valore, incrementando automaticamente del 79% gli avvisi ad alto valore che normalmente richiedono attenzione immediata[2]. Le organizzazioni possono dunque approvare e aggiornare le regole di rilevamento con soli due clic attraverso il portale co-gestito.

- **Valutazione MITRE ATT&CK.** Per essere sempre preparati agli attacchi ransomware e wipe-out, le organizzazioni potranno osservare come il loro ambiente stia utilizzando le tattiche, le tecniche e le procedure del framework MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) rispetto ai loro colleghi del settore e area geografica. Grazie all'applicazione dell'intelligenza artificiale, i nuovi servizi sono progettati per riunire i molteplici strumenti e politiche di rilevamento attualmente in atto in un'organizzazione, fornendo una visione aziendale che permetta di rilevare al meglio le minacce e valutare le lacune da colmare all'interno di un framework ATT&CK.

- **Perfetta integrazione end-to-end.** Grazie al suo approccio API aperto, i nuovi servizi si integrano rapidamente con le risorse di sicurezza previste a livello aziendale di un cliente, sia on-premise sia nel cloud. Le organizzazioni possono quindi continuare ad accedere al proprio ecosistema, avendo anche la possibilità di connettersi, collaborare e definire le proprie strategie di risposta attraverso un portale co-gestito. Ciò fornisce una visione aziendale unificata, funzionalità di correzione precise, applicando costantemente le policy di sicurezza in IT e OT.

- **Supporto globale 24x7.** Le aziende potranno contare su oltre 6.000 professionisti IBM Cybersecurity Services in tutto il mondo 24 ore su 24, 7 giorni su 7, 365 giorni all'anno, contribuendo così ad estendere i programmi di sicurezza. La vasta rete globale di IBM Consulting Cybersecurity Services serve oltre 3.000 clienti

in tutto il mondo, gestendo oltre 2 milioni di endpoint e 150 miliardi di eventi di sicurezza al giorno.

"Oggi i leader della sicurezza auspicano di poter sfuggire al circolo vizioso della carenza di personale, dell'aumento delle minacce e delle crescenti richieste da parte della C-Suite e far evolvere il proprio sistema informatico cercando di contenere al meglio le spese. Per molte organizzazioni, la decisione strategica di sostituire i propri strumenti con la piattaforma preferita di un fornitore non funziona, in quanto il più delle volte non possono permettersi di cancellare i precedenti investimenti nel SOC", ha dichiarato **Craig Robinson**, VP of Security Services di IDC Research. *"Un servizio come l'offerta Threat Detection and Response di IBM può realmente rappresentare una svolta nel risolvere queste preoccupazioni, senza richiedere un completo 'rip-and-replace' dei precedenti investimenti di sicurezza, ed è in grado aiutare a spostare il loro capitale umano nel SOC verso una modalità più proattiva".*

Per supportare il continuo miglioramento delle capacità delle operazioni di sicurezza, i TDR Services di IBM, ora disponibili, includono l'accesso ai servizi di risposta agli incidenti X-Force di IBM, oltre alla possibilità di includere ulteriori servizi di sicurezza proattivi di IBM X-Force, quali ad esempio i test di penetrazione, simulazione avversaria o gestione delle vulnerabilità. X-Force fornirà inoltre indicazioni per aiutare i clienti a migliorare le loro operazioni di sicurezza nel tempo, in base all'attuale panorama delle minacce, all'ambiente IT in evoluzione dei clienti e alle informazioni raccolte dagli impegni sottoscritti con migliaia di clienti IBM Cybersecurity Services in tutto il mondo.

Fonti aggiuntive

Per ulteriori informazioni sui servizi IBM TDR, visitare:

https://www.ibm.com/services/threat-detection-response

Per conoscere i nuovi servizi TDR e sulle sfide di avere un approccio frammentario al rilevamento e alla risposta, è possibile iscriversi al webinar che si terrà mercoledì 1° novembre 2023, alle h. 17:00 cliccando qui.

Informazioni su IBM Security

IBM Security aiuta a proteggere le più grandi aziende e governi del mondo con un portafoglio integrato di prodotti e servizi di sicurezza, dotato di funzionalità dinamiche di intelligenza artificiale e automazione. Il portafoglio, supportato dalla rinomata ricerca IBM Security X-Force®, consente alle organizzazioni di prevedere

le minacce, proteggere i dati mentre si spostano e rispondere con velocità e precisione senza frenare l'innovazione aziendale. IBM è considerato affidabile da migliaia di organizzazioni come partner per valutare, strategizzare, implementare e gestire le trasformazioni della sicurezza. IBM gestisce una delle più ampie organizzazioni di ricerca, sviluppo e distribuzione della sicurezza al mondo, monitora 150 miliardi + di eventi di sicurezza al giorno in oltre 130 paesi e ha ottenuto oltre 10.000 brevetti di sicurezza in tutto il mondo.

LinkedIn:IBM

X: IBM Italia

Per maggiori informazioni:
Paola Piacentini, *IBM external Relations Leader*
email: paola_piacentini@it.ibm.com
tel. + 39 335 1270646

---

[1] In base all'analisi interna di IBM dei dati aggregati sulle prestazioni osservati dagli impegni con 340+ clienti nel luglio 2023. Fino all'85% degli avvisi è stato gestito attraverso l'automazione piuttosto che l'intervento umano, utilizzando funzionalità AI che fanno parte del servizio Threat Detection and Response di IBM. I risultati effettivi variano in base alle configurazioni e alle condizioni del client e, pertanto, non è possibile fornire i risultati generalmente previsti.

[2] In base all'analisi di IBM dei dati aggregati sulle prestazioni annuali osservati nel 2022 da impegni con 150+ clienti SIEM gestiti. I risultati effettivi variano in base alle configurazioni e alle condizioni del client e, pertanto, non è possibile fornire i risultati generalmente previsti.
