

IBM QRadar Advisor with Watson amplia le conoscenze sulle tecniche dei criminali informatici

Nuovo algoritmo che impara dai modelli di sicurezza all'interno di un'azienda. La piattaforma sfrutta ora il framework open-source MITRE ATT&CK

Cambridge, MA - 28 nov 2018: IBM Security ha presentato le nuove funzionalità della piattaforma di sicurezza basata sull'IA, QRadar Advisor with Watson, che ampliano le potenzialità della piattaforma rispetto al comportamento dei criminali informatici e le consentono di apprendere dalle attività di risposta agli attacchi di sicurezza messe a punto all'interno di una organizzazione. IBM Security sta anche adottando il framework open-source MITRE ATT&CK, un programma pensato per aiutare gli analisti a comprendere l'evoluzione di un attacco e cosa potrebbe accadere in seguito, basandosi su osservazioni reali da parte della community della sicurezza.

Con stime che prevedono fino a 3,5 milioni di posti vacanti nel campo della sicurezza informatica entro il 2021 (Fonte: [Cyber Security Ventures](#)), gli specialisti di sicurezza informatica oggi inseguono le capacità e competenze necessarie ad analizzare e rispondere efficacemente a un'enorme quantità di incidenti e alert di cyber security. L'uso dell'IA e delle tecnologie di machine learning, come QRadar Advisor with Watson, che impara dalle ultime ricerche disponibili all'esterno nelle community della sicurezza e dalle attività che si svolgono all'interno di un'azienda, può dotare gli analisti delle conoscenze e dell'automazione necessarie per aiutarli a contrastare le minacce critiche in modo più rapido ed efficace.

Nell'ultima versione, IBM ha sviluppato nuovi modelli analitici e di apprendimento che consentono a QRadar Advisor di identificare modelli di attacco avanzati e persistenti e di adattarsi all'ambiente del cliente. Questo ciclo di apprendimento diventa più intelligente con il tempo, basandosi su interazioni aggiuntive e sul coinvolgimento degli analisti; tutto ciò consente allo strumento di fornire raccomandazioni più incisive su come rispondere, oltre che valutazioni attendibili basate su come gli incidenti corrispondono ai dati storici.

"Standard come MITRE ATT&CK, che sfruttano le conoscenze collettive della community della sicurezza, sono essenziali per far progredire il settore e aiutare i team di sicurezza a stare al passo con minacce sempre più sofisticate", ha dichiarato Chris Meenan, Director of Security Intelligence Offering Management and Strategy, IBM Security. "Dalla combinazione del framework ATT&CK per tattiche avversarie conosciute con la capacità di Watson for Cyber Security di rimanere al passo con le ultime ricerche sulla sicurezza, QRadar Advisor può fornire ad analisti di tutti i livelli le conoscenze necessarie per rispondere in modo più efficace alle minacce che si trovano ad affrontare."

Collegare i punti per affrontare la minaccia in modo più deciso

MITRE ATT&CK è una soluzione open-source sul comportamento criminale informatico sviluppato con esempi reali ed evidenze provenienti da esperti di sicurezza informatica di tutto il settore, e che definisce modelli e azioni che una minaccia può intraprendere man mano che si evolve.

Utilizzando il modello ATT&CK, QRadar Advisor with Watson sta andando oltre l'identificazione della minaccia e le ricerche esterne su di essa, per fare luce, ad esempio, su come gli attacchi esterni e le minacce interne siano progredite all'interno dell'infrastruttura del cliente, se un malware si è appena infiltrato all'interno di un'organizzazione, oppure se ha raccolto informazioni come password o dati della carta di credito. Questo nuovo contesto comprende anche il livello di attendibilità e prove pertinenti per ogni fase dell'attacco. Aiutare gli analisti a visualizzare come si è evoluto un attacco permette loro di capire immediatamente a che punto del ciclo di vita di una minaccia si trova un determinato incidente e cosa potrebbe succedere in seguito, il che può migliorare significativamente i tempi di risposta ed essere più efficace.

Queste ulteriori evidenze fornite da QRadar Advisor possono aumentare le competenze degli analisti di sicurezza e aiutarli a collegare i punti per visualizzare l'intera portata di un attacco, come solo un analista di livello superiore o un “threat hunter” potrebbe fare. Advisor può anche impiegare ATT&CK per consigliare agli analisti un processo di escalation degli incidenti più efficace, aiutandoli a comprendere i passi successivi da compiere in base al punto del ciclo di vita in cui si colloca la minaccia. Sfruttando il modello ATT&CK, QRadar Advisor può fornire questo contesto secondo uno standard di settore che corrisponde ai programmi di risposta agli incidenti dell'azienda.

Applicare i nuovi modelli di apprendimento delle minacce all'interno di un'azienda

IBM Security sta anche approfondendo l'intelligenza di QRadar Advisor with Watson, consentendogli di apprendere e contestualizzare il comportamento delle minacce e le azioni di risposta di sicurezza che avvengono all'interno di un'azienda.

Il rilascio iniziale di QRadar Advisor with Watson ha permesso a Watson di raccogliere, leggere e comprendere dati di sicurezza strutturati e non strutturati provenienti da fonti esterne, e di mettere le informazioni più importanti nelle mani degli analisti per aiutarli a comprendere ciò che era già noto e pubblicato su una minaccia specifica. Adesso QRadar Advisor impara anche dalle azioni intraprese all'interno dei contesti dei clienti: sia da eventi che avvengono in tempo reale, sia da ciò che è successo in passato con certi tipi di eventi. Le due nuove funzionalità che IBM sta introducendo per QRadar Advisor sono:

Modelli di disposizione delle minacce: QRadar Advisor utilizza nuovi algoritmi per costruire un modello per tipi specifici di minacce, basato sulle azioni e sull'esito di eventi simili che si sono verificati in precedenza all'interno di un'azienda. Quando si inizia una nuova indagine, questo modello può essere utilizzato per escludere i falsi positivi o per aiutare l'analista a stabilire se la minaccia deve essere identificata come malware, esfiltrazione di dati o come un altro tipo specifico di minaccia. Questa capacità si adatta e impara dalle interazioni con gli analisti, diventando sempre più intelligente a ogni utilizzo.

Analisi delle indagini incrociate: All'interno del Security Operation Center (SOC) di un'azienda, più analisti possono lavorare su diversi incidenti correlati tra loro; oppure gli alert che si presentano per molti mesi possono essere parte di una stessa campagna di attacchi informatici a lungo termine. Questa nuova funzionalità consente a QRadar Advisor di trovare i punti in comune tra le indagini utilizzando il ragionamento cognitivo, e di raggruppare automaticamente indagini correlate per evitare la duplicazione degli sforzi, oltre a fornire un contesto più completo per facilitare l'indagine.

Combinando questi nuovi modelli di apprendimento (che migliorano la contestualizzazione delle attività all'interno della rete) con le capacità investigative di Watson for Cyber Security e la capacità di recepire le ricerche pubblicate dai team di sicurezza, gli analisti possono ora utilizzare QRadar Advisor per condurre indagini più approfondite e coerenti e rispondere in modo più rapido ed efficace alle minacce.

Contatti

Claudia Ruffini

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

Alessandro Ferrari

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