IBM Italy News Room

IBM Security combatte le minacce con User Behavior Analytics

La nuova app estende le capacità analitiche della piattaforma Qradar per la protezione contro furti di credenziali e violazioni interne

Milano - 28 lug 2016: IBM Security ha annunciato oggi una nuova app per IBM QRadar che analizza i pattern d'uso degli utenti interni, inclusi dipendenti, collaboratori e partner, al fine di rilevare l'eventuale compromissione di credenziali o sistemi ad opera di criminali informatici. Disponibile gratuitamente tramite IBM Security App Exchange, IBM QRadar User Behavior Analytics amplia la piattaforma di security intelligence di IBM QRadar per offrire una panoramica tempestiva sulle minacce interne potenziali prima che possano danneggiare più gravemente un'azienda. Le violazioni interne rappresentano oggi la causa del 60% degli attacchi verso le aziende, ma circa un quarto di tali attacchi sono il risultato dell'appropriazione da parte degli hacker di credenziali degli utenti ottenute da dipendenti, appaltatori o partner ingannati da attacchi di phishing, malware o altre tecniche[1]. Questa nuova app di analisi comportamentale degli utenti segnala agli analisti ogni evenutale deviazione dalla norma come, ad esempio, il primo accesso di un utente a un server ad alto valore da una nuova location e con un account privilegiato: tale deviazione sarebbe rilevata grazie al modello di comportamento standard sviluppato da IBM QRadar User Behavior Analytics per ogni dipendente, che rileva immediatamente qualsiasi anomalia significativa.

"Le aziende hanno bisogno di migliorare il proprio livello di protezione dalle minacce interne, causate da distrazioni accidentali o da criminali informatici con accesso ai sistemi e alle tecnologie interne dell'azienda" sostiene Jason Corbin, Vice President of Strategy and Offering Management, IBM Security. "Questa nuova app offre agli analisti la possibilità di fronteggiare tempestivamente questi eventi facendo leva sui dati di sicurezza informatica esistenti, al fine di rilevare i segnali d'allarme, spesso nascosti, in attività sospette degli utenti, aiutando i tecnici a stroncare efficacemente sul nascere qualsiasi violazione."

IBM QRadar User Behavior Analytics utilizza i dati utenti presenti in Qradar, integrandoli in una piattaforma singola che consente di analizzare e gestire eventi e dati di sicurezza. Questa integrazione evita agli analisti della sicurezza di importare nuovamente e smistare i dati da diverse piattaforme, per identificare e confrontare il comportamento degli utenti con altri indicatori di anomalie rilevati da QRadar. La soluzione aiuta quindi a combattere le minacce tramite:

- **Profili di analisi dei rischi –** l'app analizza le azioni più rischiose degli utenti assegnando un punteggio ai comportamenti anomali, aiutando a identificare sia le minacce interne potenziali che l'uso di credenziali rubate da parte di criminali informatici.

- **Dashboard di analisi dei comportamenti per priorità –** gli analisti possono accedere a una migliore visibilità e comprensione delle azioni che hanno condotto un utente ad aprire un documento sospetto, o delle modalità con cui un utente ha ottenuto dei privilegi di accesso. Ad esempio, un singolo clic del mouse, un allegato o un link in un messaggio e-mail di phishing possono aggiungersi all'elenco di attività sospette di un utente, o consentire all'analista la redazione di un'annotazione di testo per spiegare le proprie osservazioni.

- **Ottimizzazione dei dati di sicurezza esistenti di QRadar –** grazie alle informazioni sugli utenti rilevate dall'intero ambiente IT, i team di sicurezza saranno in grado di consultare gli ampi set di sorgenti di dati e di security intelligence di QRadar per rilevare le minacce su tutto il bacino di utenti e asset.

Con la recente acquisizione di Resilient Systems, IBM ha integrato la capacità di rispondere agevolmente agli incidenti rilevati grazie alla piattaforma QRadar con la nuova app User Behavior Analytics. Disponibile per il download gratuito su IBM Security

App Exchange, l'applicazione User Behavior Analytics per QRadar è parte dell'approccio open di IBM allo sviluppo di strumenti di sicurezza efficaci nella lotta contro il crimine informatico.

Negli ultimi due anni IBM ha intrapreso alcune importanti iniziative per promuovere la collaborazione fra i professionisti della sicurezza di tutto il mondo e aiutarli a combattere, con maggiore efficacia, i criminali informatici. Tra queste, ad esempio, aver reso pubblico il proprio database di minacce – pari a 700 TB - tramite IBM X-Force Exchange. Sviluppata grazie all'intelligence di X-Force Exchange, IBM Security App Exchange si è evoluta in un ampio marketplace online, dando la possibilità a partner e clienti di condividere e scaricare app basate sulle tecnologie di IBM Security, come IBM QRadar. Il negozio online offre decine di soluzioni di terze parti per ottimizzare la capacità dei clienti di personalizzare i propri ambienti di sicurezza utilizzando, l'approccio *open platform* di IBM.

Informazioni su IBM Security

IBM Security offre un portafoglio di prodotti e servizi per la sicurezza delle aziende tra i più avanzati e integrati tra quelli disponibili sul mercato. Supportata dal team di ricerca mondiale IBM X-Force®, la gamma di prodotti e soluzioni consente alle aziende di gestire efficacemente i rischi e difendersi al meglio dalle minacce emergenti. IBM gestisce una delle maggiori organizzazioni di ricerca, sviluppo e delivery di servizi di sicurezza al mondo, monitorando 20 miliardi di eventi di sicurezza al giorno in più di 130 Paesi. Inoltre vanta più di 3000 brevetti in materia di sicurezza. Per ulteriori informazioni visitate www.ibm.com/security, seguite @IBMSecurity su Twitter o visitate il blogIBM Security Intelligence.

---

[1] IBM X-Force Cyber Threat Index, 2016
