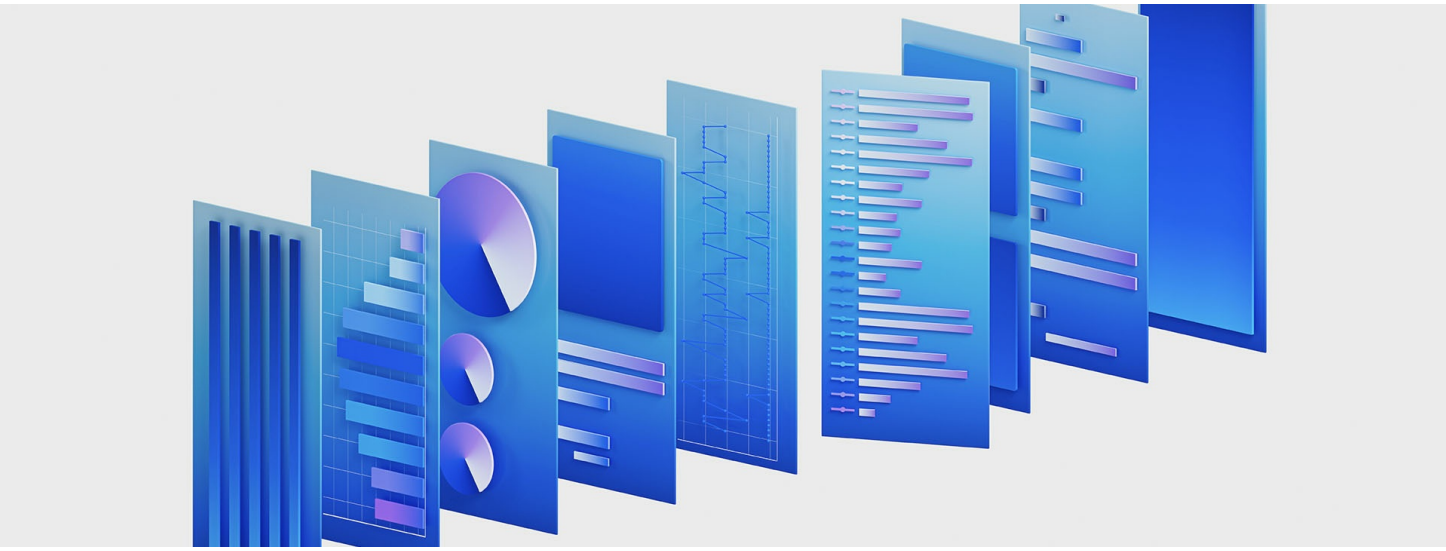
Comunicati stampa

IBM annuncia la nuova QRadar Security Suite per migliorare e velocizzare il rilevamento e la risposta alle minacce cyber

Una suite che integra le analisi dei vari domini di sicurezza con un’interfaccia più efficiente e che semplifica gli interventi degli esperti

Nuove funzionalità di automazione e di AI che hanno dimostrato di accelerare il triage degli allarmi in media del 55%



ARMONK, NY - IBM (NYSE:IBM) ha presentato la nuova suite di sicurezza progettata per unificare e velocizzare le attività nell'intero ciclo di vita degli attacchi. La IBM Security QRadar Suite è un’importante evoluzione ed espansione di QRadar, che include tutte le principali tecnologie di rilevamento, investigazione e risposta delle minacce, con innovazioni di rilievo nell’intera gamma.

Fornita in modalità “as-a-service”, la IBM Security QRadar Suite è basata su un'infrastruttura aperta e progettata specificamente per le esigenze del cloud ibrido. È dotata di un'unica interfaccia utente, modernizzata, integrata con l'intelligenza artificiale e l'automazione avanzata, progettate per offrire maggiore velocità, efficienza e precisione nell’utilizzo dei principali tool di analisi.

Oggi i team SOC (Security Operation Center) devono proteggere un perimetro digitale in rapida espansione che si estende agli ambienti cloud ibridi, creando una complessità senza precedenti e rendendo difficile tenere il passo con il veloce progredire degli attacchi. Gli operatori del SOC possono essere rallentati da processi di indagine e di risposta agli alert che richiedono alta intensità di lavoro; infatti, è necessario aggregare manualmente gli insight e fare leva su dati, strumenti ed interfacce scollegate tra loro. Secondo un recente sondaggio[1], i professionisti SOC affermano di trascorrere circa un terzo della propria giornata lavorativa investigando e convalidando gli incidenti che risultano non essere minacce reali.

Basandosi sull'attuale leadership in 12 categorie tecnologiche di sicurezza,[2] IBM ha ridisegnato il proprio portafoglio di soluzioni leader di mercato nel rilevamento e nella risposta alle minacce per massimizzare la velocità e l'efficienza degli esperti di sicurezza e soddisfare le specifiche esigenze odierne. La nuova suite IBM Security QRadar include EDR/XDR, SIEM, SOAR, e una nuova funzionalità sviluppata nativamente in cloud di gestione dei log, il tutto basato su un'interfaccia utente comune, insight condivisi e workflow connessi, con i seguenti elementi di progettazione principali:

- **Esperienza di Analisi Unificata:** frutto della collaborazione con centinaia di utenti, la suite integra un'interfaccia intuitiva e modernizzata per tutti i prodotti per aumentare notevolmente la velocità e l'efficienza dell'intera attività di analisi. Inoltre, integra funzionalità di AI e di automazione che hanno dimostrato di velocizzare l'analisi ed il triage degli avvisi del 55% in media nel primo anno.[1]

- **Disponibilità in Cloud, Velocità e Scalabilità:** distribuita in modalità “as-a-service” su Amazon Web Services (AWS), la suite QRadar semplifica implementazione, visibilità e integrazione tra ambienti cloud e origini di dati. Inoltre, include una nuova funzionalità nativa del cloud di gestione dei log, ottimizzata per una ricezione dei dati altamente efficiente, la ricerca rapida e l'analisi su larga scala.

- **Sviluppata su tecnologia aperta, Integrazioni Precostruite:** la suite integra le tecnologie fondamentali necessarie per il rilevamento, l'analisi e la risposta alle minacce, basate su un modello aperto, un ecosistema di partner esteso e oltre 900 integrazioni precostruite che garantiscono una forte interoperabilità tra i set di strumenti IBM e quelli di terze parti.

"Di fronte ad un perimetro di attacco in crescita e a tempistiche sempre più strette, la velocità e l'efficienza sono fondamentali per i responsabili della sicurezza", ha dichiarato Mary O'Brien, General Manager IBM Security. "IBM ha progettato la nuova suite QRadar per offrire un'esperienza utente unica e modernizzata, integrata con una sofisticata intelligenza artificiale e automazione per massimizzare la produttività degli esperti di sicurezza e accelerare la risposta a ogni fase del processo di attacco."

Co-innovazione per le esigenze di sicurezza del mondo reale

La suite QRadar è il frutto di anni di investimenti, acquisizioni e innovazioni di IBM nel rilevamento e nella risposta alle minacce. La soluzione include decine di funzionalità di automazione e intelligenza artificiale, che sono state perfezionate nel tempo con utenti e dati del mondo reale, anche grazie alle attività di IBM Managed Security Service con oltre 400 clienti. Include inoltre innovazioni sviluppate in collaborazione con IBM Research e la community open source di sicurezza.

Queste funzionalità basate sull'intelligenza artificiale hanno dimostrato di migliorare in modo significativo la velocità e

l'accuratezza delle operazioni SOC: ad esempio, consentendo a IBM Managed Security Services di automatizzare più del 70% delle chiusure degli allarmi[3] e di ridurre le tempistiche di triage degli stessi in media del 55%[2] in media entro il primo anno di implementazione.

Integrando queste funzionalità, tramite l'esperienza unificata degli analisti, la suite QRadar contestualizza e assegna automaticamente le priorità agli avvisi, fornisce una rappresentazione visuale dei dati per un rapido utilizzo, oltre a informazioni dettagliate e flussi di lavoro automatizzati tra i prodotti. Questo approccio può ridurre drasticamente il numero di passaggi e schermate necessari per indagare e rispondere alle minacce. Gli esempi includono:

- **Triage degli alert potenziato dall'AI:** assegna automaticamente la priorità o chiude gli avvisi in base all'analisi dei rischi basata sull'intelligenza artificiale, utilizzando i modelli di intelligenza artificiale addestrati sui modelli di risposta degli esperti, insieme all'intelligence delle minacce esterne di IBM X-Force e agli ampi approfondimenti sul contesto da tutti gli strumenti di rilevamento.

- **Indagine sulle minacce automatizzata:** identifica gli incidenti ad alta priorità che possono richiedere un'indagine, avviandola automaticamente, recuperando le risorse associate e raccogliendo le prove tramite il data mining tra gli ambienti. Il sistema utilizza questi risultati per generare una sequenza temporale e un grafico di attacco dell'incidente basato sul framework MITRE ATT&CK e raccomanda azioni per accelerare la risposta.

- **Ricerca accelerata delle minacce:** utilizza un linguaggio open source di ricerca delle minacce e le funzionalità di ricerca federate per aiutare gli esperti a rilevare attacchi furtivi e indicatori di compromissione nei rispettivi ambienti, senza spostare i dati dalla fonte originale.

Oltre a migliorare la rapidità e l’efficienza degli interventi, le tecnologie QRadar contribuiscono anche a incrementare la produttività degli esperti di sicurezza, che possono dedicarsi ad attività a maggior valore.

Suite di sicurezza aperta, connessa e modernizzata

La suite QRadar sfrutta tecnologie e standard aperti in tutto il portafoglio, insieme a centinaia di integrazioni precostruite con i partner dell'ecosistema IBM Security. Questo modello consente approfondimenti condivisi e azioni automatizzate su cloud di terze parti, singoli prodotti e data lakes, riducendo i tempi di implementazione e integrazione da mesi a giorni o settimane.

La IBM QRadar Suite include i seguenti prodotti principali, inizialmente forniti in modalità SaaS e aggiornati con la nuova esperienza di analisi unificata:

- **QRadar Log Insight:** una nuova soluzione cloud nativa per le soluzioni di gestione dei log e osservabilità della sicurezza che fornisce la raccolta semplificata dei dati, la ricerca in meno di un secondo e l'analisi rapida. Sfrutta un data lake di sicurezza ottimizzato per raccogliere, archiviare ed eseguire analisi su terabyte di dati con maggiore velocità, flessibilità ed efficienza. Questa soluzione è stata progettata per una gestione ottimizzata dei log di sicurezza e per ricerche e indagini federate.

- **QRadar EDR e XDR**: consente alle aziende di proteggere i propri endpoint da minacce precedentemente sconosciute, minacce zero-day, utilizzando l'automazione e centinaia di modelli comportamentali e di apprendimento automatico per rilevare le anomalie nel comportamento e rispondere agli attacchi in tempo quasi reale. Sfrutta un approccio unico che monitora i sistemi operativi dall'esterno, evitando manipolazioni o interferenze. Per le aziende che desiderano estendere le funzionalità di rilevamento e risposta oltre l'endpoint, IBM offre anche XDR con correlazione degli alert, indagini automatizzate e risposte suggerite su network, cloud, email ed altro, oltre al servizio gestito di rilevamento e risposta (MDR).

- **QRadar SOAR:** insignito recentemente di un Red Dot Design Award per l'interfaccia e l'esperienza utente; consente alle organizzazioni di automatizzare e orchestrare i flussi di lavoro di risposta agli attacchi e garantire che i processi specifici vengano seguiti in modo coerente, ottimizzato e misurabile. Include 300 integrazioni precostruite e offre playbook pronti da utilizzare per rispondere a oltre 180 normative globali sulla privacy e sulla violazione dei dati.

- **QRadar SIEM:** Il SIEM QRadar IBM è stato migliorato con la nuova interfaccia di analisi unificata che fornisce informazioni condivise e flussi di lavoro con più ampi set di strumenti operativi di sicurezza. Offre il rilevamento in tempo reale, sfruttando l'intelligenza artificiale, l'analisi del comportamento degli utenti e della rete, l'intelligence delle minacce del mondo reale, per fornire agli esperti alert più accurati, contestualizzati e evidenziando le priorità. IBM prevede inoltre di rendere QRadar SIEM disponibile in modalità as-a-service su AWS entro la fine del secondo trimestre del 2023.

La IBM Security QRadar Suite è oggi disponibile tramite le offerte SaaS individuali. Per ulteriori informazioni, visitare: https://www.ibm.com/qradar

Informazioni su IBM Security

IBM Security aiuta a proteggere le aziende e i governi più grandi del mondo con un portafoglio integrato di prodotti e servizi di sicurezza, arricchito da funzionalità di AI e di automazione dinamica. Il portafoglio, supportato dalla ricerca di fama mondiale IBM Security X-Force®, consente alle organizzazioni di prevedere le minacce, proteggere i dati in movimento e rispondere con velocità e precisione, senza compromettere l'innovazione di business. Con i propri esperti di sicurezza in tutto il mondo, IBM è richiesta da migliaia di organizzazioni come partner per valutare, definire le strategie, implementare e gestire le trasformazioni della sicurezza. IBM gestisce una delle organizzazioni di ricerca, sviluppo e distribuzione della sicurezza più grandi del mondo, monitora oltre 150 miliardi di eventi di sicurezza al giorno in oltre 130 paesi ed ha ottenuto più di 10.000 brevetti di sicurezza in tutto il mondo.

Le dichiarazioni relative all'orientamento e ai programmi futuri di IBM sono soggette a modifica o a ritiro senza preavviso e rappresentano solo obiettivi e finalità.

IBM
Paola Piacentini - External Relations Leader
Tel: + 39 335 1270646
e-mail: paola_piacentini@it.ibm.com

---

[1] I Risultati dello studio Global Security Operations Center , amministrati da Morning Consult e commissionati da IBM, marzo 2023, Basato sulle risposte di 1.000 professionisti del centro operativo di sicurezza intervistati tra un campione di 1.000 membri del team SOC in 10 paesi.

[2] Sulla base delle valutazioni dei prodotti di sicurezza effettuate da società di analisi esterne, tra cui Gartner, IDC, Forrester, KuppingerCole e Omdia, che classificano IBM come leader in 12 categorie di prodotti di sicurezza: SIEM, SOAR, Piattaforma di Intelligence per la riduzione delle Frodi, Autenticazione Basata sul Rischio, Governance ed amministrazione delle identità, Gestione degli Accessi, Gestione delle identità e degli accessi come servizio, Governance e Intelligence degli accessi e Governance dell'identità, Autenticazione, Gestione dell'identità e degli accessi dei clienti, Sicurezza dei dati, Gestione unificata degli endpoint.

[3] IBM Institute for Business Value report, " AI e automazione per la sicurezza informatica ," 2022. Risultati basati sull'analisi IBM dei dati sulle prestazioni annuali aggregati osservati da centinaia di client globali che utilizzano funzionalità di automazione e AI che ora fanno parte di QRadar Suite. I risultati effettivi variano in base alle configurazioni e alle condizioni del client e, pertanto, non è possibile fornire stime generali di risultati previsti.