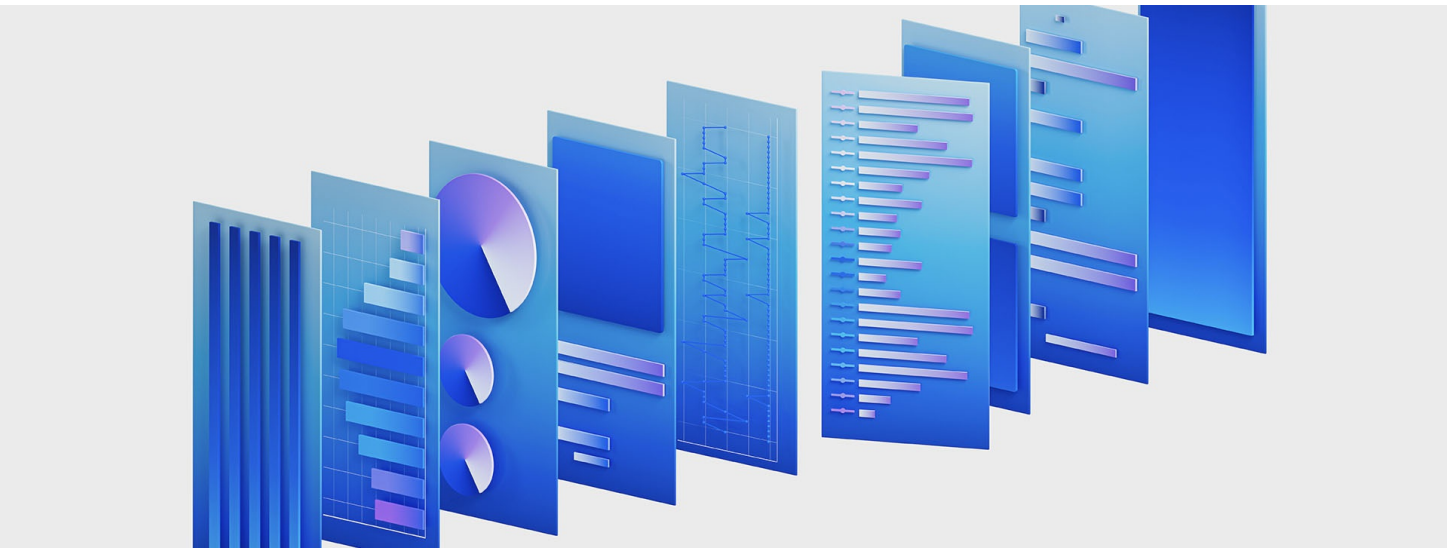
IBM Italy News Room

IBM presenta il SIEM cloud native creato per ottimizzare il tempo e l’efficacia dei team di sicurezza

Basato su una architettura cloud-native, la nuova soluzione consente di sfruttare al meglio gli algoritmi di Intelligenza Artificiale e il lavoro degli analisti di sicurezza



ARMONK, N.Y., 7 novembre 2023 - IBM ha annunciato oggi un'importante evoluzione della sua tecnologia QRadar SIEM: progettata su una nuova architettura cloud-native e sviluppata per incrementare la scalabilità, la flessibilità e velocità di utilizzo nei vari ambienti. IBM ha, inoltre, condiviso i propri piani per il rilascio di funzionalità basate su intelligenza artificiale di tipo generativo all'interno del proprio portafoglio *di threat detection and incident response*, sfruttando watsonx, la piattaforma di dati e intelligenza artificiale pronta per l'uso aziendale.

Gli ambienti cloud ibridi di oggi si stanno evolvendo rapidamente, creando una superficie di attacco più ampia e complessa da proteggere. A causa dell’elevata quantità di dati da analizzare, delle tecnologie non integrate, del lavoro manuale e del sovraccarico di alert, è sempre più difficile individuare rapidamente le effettive minacce.

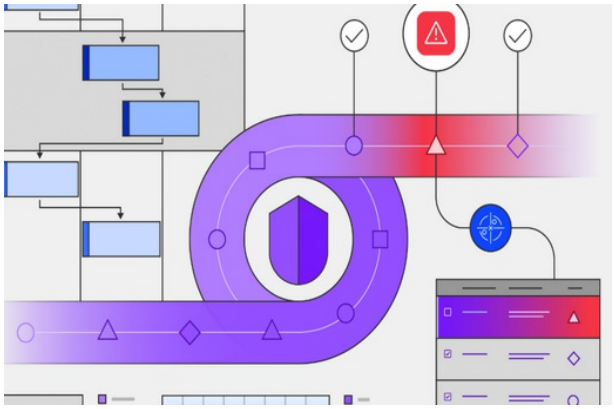
Secondo un recente sondaggio globale[1], i professionisti delle aziende che operano nei Security Operation Center (SOC) riescono ad analizzare meno della metà (49%) degli avvisi che dovrebbero esaminare in una tipica giornata lavorativa.

“Il nostro nuovo SIEM cloud-native è un elemento fondamentale della strategia IBM per far evolvere tutta la sua piattaforma di sicurezza verso l’utilizzo di modelli di cloud ibrido e di pieno sfruttamento degli algoritmi di AI" ha dichiarato **Kevin Skapinetz, Vice President, Strategy and Product Management, IBM Security** . *"Invece di costringere gli analisti ad aggirare la complessità delle tecnologie di sicurezza, stiamo progettando una tecnologia per rimuovere la complessità, eliminando il rumore, semplificando l'esperienza utente e consentendo*

agli analisti di affrontare le minacce urgenti con maggiore velocità e fiducia".

Il nuovo IBM QRadar SIEM cloud-native, con un'architettura riprogettata per l'ingestione dei dati altamente efficiente, la ricerca rapida e l'analisi su larga scala, si basa su 13 anni di leadership di mercato di QRadar e numerosi riconoscimenti degli analisti[2] per le sue funzionalità di correlazione e analisi delle minacce.

Basato su standard aperti, è l'ultima novità di QRadar Suite, il portafoglio integrato di software di IBM per il *threat detection and incident response*. QRadar è stato progettato per aumentare e migliorare il lavoro quotidiano degli analisti di sicurezza, utilizzando l'AI per gestire le attività ripetitive e dispendiose in termini di tempo, consentendo loro di individuare e rispondere in modo più efficiente alle minacce ad alta priorità.



Il SIEM cloud-native sarà inizialmente disponibile in SaaS a partire dal Quarto Trimestre del 2023, con successive release on-premise e multi-cloud nel 2024.

Open design: basato su Red Hat OpenShift, QRadar SIEM è progettato per essere un sistema aperto, che consente una maggiore interoperabilità con cloud e strumenti di diversi fornitori. Utilizza l'open source e gli standard aperti per le principali funzioni, incluse le regole di rilevamento e il linguaggio di ricerca, consentendogli di lavorare in modo trasversale rispetto agli stack tecnologici e di sicurezza delle aziende.

- Sfrutta un Linguaggio Comune e Condiviso per le Regole di Rilevamento **(SIGMA)** - che consente ai clienti di importare rapidamente nuove regole sviluppate dalle community di sicurezza in base all'evoluzione delle minacce.

- Offre esclusive **funzionalità di ricerca federate e di ricerca delle minacce** basate su tecnologie open source, che consentono agli analisti di ricercare e analizzare in modo proattivo le minacce tra le fonti di dati cloud e on-premise indipendentemente dalla tecnologia, senza spostare i dati dalla loro fonte originale.

- Si basa sull'ecosistema **QRadar, una delle più grandi reti di partner** del settore con oltre 700 integrazioni già disponibili.

Rilevamento, Indagine e Risposta integrati : come parte di QRadar Suite, il nuovo SIEM cloud-native offre ai clienti l'accesso a una vasta gamma di funzionalità integrate che possono consentire il rilevamento, l'indagine e la risposta più rapidi tra i vari strumenti. Con QRadar Suite, le aziende possono ottenere visibilità sulle risorse esposte tramite funzionalità di gestione delle superfici di attacco (ASM), ricercare le minacce tra i vari insiemi di strumenti, proteggere gli endpoint con l'EDR e connettersi ai playbook automatizzati per accelerare la risposta (SOAR). QRadar SIEM consente agli utenti di avere informazioni condivise e azioni automatizzate attraverso i principali strumenti, a cui si accede direttamente da un'unica interfaccia, senza dover passare da uno strumento all'altro.

Automazione e intelligenza artificiale: QRadar SIEM applica più livelli di intelligenza artificiale e automazione per migliorare la qualità degli avvisi e l'efficienza degli analisti di sicurezza. Queste funzionalità di intelligenza artificiale sono state pre-addestrate su milioni di avvisi e perfezionate ulteriormente per tenere conto delle unicità di ciascun cliente. Ad esempio:

- **Impostazione delle priorità degli avvisi:** utilizza l'intelligenza artificiale per ridurre il rumore e migliorare la qualità degli avvisi. Il sistema elimina automaticamente gli avvisi a bassa priorità, mentre raggruppa, contestualizza e scala automaticamente gli avvisi ad alta priorità, tenendo conto del contesto di rischio derivante dalle fonti di *threat intelligence* e dai modelli di risposta degli analisti. Questa funzionalità ha consentito a IBM Consulting Cybersecurity Services di automatizzare l'85% della gestione degli alert[3]e di accelerare le tempistiche di valutazione delle minacce del 55% nel primo anno di utilizzo[4].
- **Investigazione assistita:** funzionalità di intelligenza artificiale che esegue automaticamente le ricerche federate tra i sistemi connessi, generando un grafico della sequenza temporale degli attacchi, mappature MITRE ATT&CK e azioni consigliate, offrendo agli analisti un notevole vantaggio nelle attività di indagine.

- **Rilevamento adattivo:** l'analisi di QRadar SIEM viene aggiornata automaticamente con nuove regole di rilevamento e di threat intelligence su base continua, per stare al passo con le minacce in evoluzione.

Le funzionalità di sicurezza AI di IBM sono integrate nativamente nell'interfaccia di QRadar Suite, fornendo informazioni contestuali a portata di mano degli analisti e aiutandoli a trarre vantaggio dall'intelligenza artificiale in modo più intuitivo all'interno dei loro normali flussi di lavoro.

AI generativa per incrementare la produttività del SOC

IBM prevede anche di mettere a disposizione dei suoi clienti all'inizio del 2024 funzionalità di sicurezza con generative AI per QRadar Suite, basate su watsonx, la piattaforma di dati e AI dell'azienda. IBM sta progettando modelli di generative AI per aiutare a ottimizzare il tempo e l'efficacia dei team di sicurezza nell'esecuzione di alcune attività ripetitive, per consentire agli analisti di concentrarsi su attività ad alto valore aggiunto. Ad esempio:

- **Automatizza la creazione di report:** crea riepiloghi di casi e di incidenti di sicurezza che possono essere facilmente condivisi con le parti interessate.

- **Accelera la ricerca delle minacce:** genera automaticamente le ricerche per rilevare le minacce in base alle descrizioni in linguaggio naturale dei comportamenti e dei modelli di attacco, aiutando ad accelerare le risposte a nuove minacce.

- **Interpreta i dati generati automaticamente:** aiuta gli analisti a comprendere rapidamente i dati dei log di sicurezza, fornendo spiegazioni degli eventi che si sono verificati su un sistema e accelerando le relative indagini.

- **Migliora i dati di threat intelligence:** interpreta e riepiloga le informazioni sulle minacce pioritarie, concentrandosi sulle campagne che hanno maggiori probabilità di colpire i clienti in base al loro proprio profilo di rischio.

IBM sta, inoltre, sviluppando funzionalità di sicurezza basate su modelli di generative AI di tipo predittivo che verranno addestrate per creare risposte che si ottimizzano nel tempo, ad esempio, aiutando il team di sicurezza a trovare incidenti simili, aggiornare i sistemi interessati e correggere il codice vulnerabile.

Oltre a questi casi di uso, IBM prevede di integrare l'intelligenza artificiale generativa nel suo più ampio portafoglio di software e servizi di sicurezza. Queste funzionalità sfrutteranno l'infrastruttura watsonx e i modelli di AI watsonx, che sono stati addestrati su set di dati selezionati e specifici del dominio, progettati per offrire maggiore affidabilità, trasparenza e precisione.

Per ulteriori informazioni su QRadar SIEM, visitare il sito: https://www.ibm.com/products/qradar-cloud-native-siem

Per ulteriori informazioni su AI per la Sicurezza, visitare il sito: https://www.ibm.com/security/artificial-

intelligence

Le dichiarazioni relative all'orientamento e alle intenzioni future di IBM sono soggette a modifica o a ritiro senza preavviso e rappresentano solo obiettivi e finalità.

IBM Security
IBM Security aiuta a proteggere le principali aziende e organizzazioni pubbliche e private, con un portfolio integrato di servizi e prodotti di sicurezza, arricchito da funzionalità dinamiche di AI e di automazione. Il portfolio, supportato dalla ricerca IBM Security X-Force® di fama mondiale, consente alle organizzazioni di prevedere le minacce, proteggere i dati in movimento e rispondere con velocità e precisione, senza compromettere l'innovazione di business. IBM è un partner affidabile per migliaia di aziende supportando la definizione delle strategie, l'implementazione e la trasformazione delle tecnologie di sicurezza. IBM rappresenta una delle organizzazioni di ricerca, sviluppo e gestione 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.

IBM
IBM è un'azienda leader a livello mondiale nel settore del cloud ibrido, dell'AI e dei servizi alle imprese e opera con le imprese di oltre 175 Paesi aiutandole a capitalizzare sugli insight dei loro dati, a semplificare i processi aziendali, a ridurre i costi e a ottenere un vantaggio competitivo nei loro settori d'industria. Quasi 3.800 enti governativi e aziende in aree infrastrutturali critiche come quelle dei servizi finanziari, delle telecomunicazioni e sanità si basano sulla piattaforma cloud ibrida di IBM e su Red Hat OpenShift per realizzare la loro trasformazione digitale in modo rapido, efficiente e sicuro. Le innovazioni di IBM nell'ambito dell'AI, del quantum computing, delle soluzioni cloud specifiche per settore d'industria e nei servizi sono offerte con opzioni open e flessibili. Tutto questo è supportato dal ben noto impegno di IBM per la trasparenza, la responsabilità, l'inclusività e il servizio. Per maggiori informazioni, visitate il sito www.ibm.com.

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]Global Security Operations Center Study, 2022 condotto da Morning Consult e sponsorizzato da IBM.

[2]QRadar è stato identificato come leader di mercato per SIEM in diversi report di analisti di terze parti negli ultimi 13 anni, inclusi i report di Gartner, Forrester, KuppingerCole, IDC e Omdia.

[3] In base all'analisi interna di IBM dei dati di performance aggregati osservati dai progetti con oltre 340 clienti nel luglio 2023. Fino all'85% degli alert è stato gestito tramite l'automazione utilizzando le funzionalità di AI che fanno parte di QRadar SIEM. I risultati effettivi variano in base alle configurazioni e alle condizioni del cliente e, pertanto, in generale non è possibile fornire previsioni.

[4] In base all'analisi interna di IBM dei dati di performance aggregati osservati dai progetti con oltre 400 clienti dal 2018 al 2019, che ha mostrato che la media della tempistica di triage degli alert è stata ridotta del 55% durante il primo anno utilizzando le funzionalità di AI e automazione che fanno parte di QRadar SIEM. I risultati effettivi variano in base alle configurazioni e alle condizioni del cliente e, pertanto, in generale non è possibile fornire previsioni.
