Analytics della sicurezza per le tue implementazioni multicloud

Soluzione SIEM IBM Security QRadar

IBM

Indice

01

La rivoluzione del multicloud sta acquisendo forza

L'azienda moderna ha bisogno di una sicurezza intelligente

L'adozione di un ambiente multicloud, ibrido, sta solo crescendo e, con essa, un numero crescente di dati, applicazioni e carichi di lavoro viene trasferito sul cloud. Dal momento che un numero più elevato di dipendenti lavora da casa e le interazioni non avvengono più di persona ma online, si prevede che l'utilizzo del cloud raggiunga nuove altezze.[1]

Gartner stima che il settore d'industria dei servizi di cloud pubblico subirà una crescita esponenziale fino alla fine del 2022. Il segmento del mercato cloud con la crescita più rapida sarà quello dell'IaaS (infrastructure as a service), che Gartner prevede arriverà a un fatturato di 76,6 miliardi di dollari entro il 2022.[2]

La sicurezza dovrebbe essere situata al centro di queste iniziative cloud. Le violazioni della sicurezza del cloud possono comportare per le aziende un costo superiore ai 50.000 dollari in meno di un'ora.[3] Le organizzazioni che si affidano ad una soluzione IaaS devono attivarsi in anticipo per proteggere i loro sistemi operativi, gestire le configurazioni di rete e, naturalmente, proteggere i dati in esecuzione su questi sistemi.

Per tenere al sicuro le informazioni critiche per il business, gli analisti della sicurezza hanno bisogno di visibilità completa dell'intero ecosistema IT – reti, applicazioni e attività – in esecuzione on premise e nel cloud. Hanno bisogno della capacità di rilevare minacce in tempo reale, di individuare l'uso di servizi cloud non autorizzati e di ottenere una chiara visibilità della configurazione eventualmente corretta dei loro account e delle loro risorse, al fine di mantenere la sicurezza.

> 1 miliardo di record persi

Una configurazione errata degli ambienti cloud ha causato la perdita di oltre un miliardo di record nel 2019.[3]

> 50.000 dollari di perdite in meno di un'ora

Le violazioni della sicurezza del cloud possono comportare per le aziende un costo superiore ai 50.000 dollari in meno di un'ora.[3]

02

Utilizza tutta la potenza delle soluzioni IBM Security QRadar

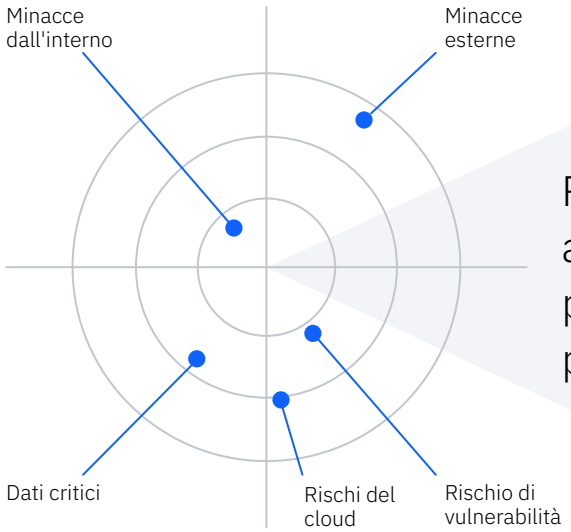
Ottieni una visibilità completa dei servizi cloud

La soluzione SIEM (security information and event management) di IBM Security QRadar offre profonde integrazioni con molteplici servizi cloud, tra cui AWS (Amazon Web Services), Microsoft Azure, Piattaforma Google Cloud, Salesforce.com, Microsoft Office 365, IBM Cloud e altri ancora.

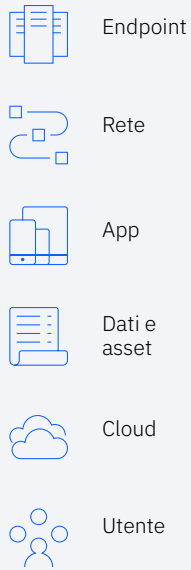
Raccogliendo e normalizzando le informazioni sulla sicurezza, ricavate da ambienti basati su cloud e on-premise, la soluzione QRadar applica strumenti di advanced analytics per catalogare automaticamente milioni di eventi. La soluzione aiuta ad identificare le minacce più critiche e fornisce avvisi significativi, ordinati per priorità, su possibili incidenti, per proteggere ambienti on-premise e multicloud ibridi.

Inoltre, la soluzione fornisce agli analisti della sicurezza un'interfaccia unificata, dove possono visualizzare le minacce più critiche, esaminare la catena cronologica degli eventi che hanno portato a ciascun avviso e ottenere insight immediato sugli attacchi potenziali. Valide funzioni pronte all'uso consentono di garantire una rapida implementazione e la scalabilità praticamente in qualsiasi ambiente supportato.

Acquisisci ulteriori informazioni su come la soluzione QRadar può aiutarti a proteggere il tuo ambiente cloud. →



Rilevamento e assegnazione della priorità automatici per le minacce



La soluzione SIEM di IBM Security QRadar raccoglie, analizza e mette in correlazione dati da un'ampia varietà di origini per rilevare le minacce più critiche e assegnare la priorità a tali minacce, che richiedono ulteriori indagini.

03

Integra la soluzione QRadar con AWS (Amazon Web Services)

Estendi la visibilità ad AWS, per una posizione migliore in termini di sicurezza

Circa il 76% delle organizzazioni utilizza AWS in qualche misura.1 Dal momento che questa transizione dall'elaborazione on-premise tradizionale all'elaborazione basata sul cloud continua, i team della sicurezza hanno bisogno di visibilità della loro infrastruttura basata sul cloud, delle applicazioni e dei dati – proprio come succederebbe in un ambiente on-premise.

Identifica i rischi che possono causare un'esposizione dei dati
Alcune delle maggiori violazioni negli ultimi anni non sono state causate da autori di attacchi malevoli. Al contrario, sono state il risultato di errori accidentali di configurazione nei bucket di Amazon S3 (Amazon Simple Storage Service) che hanno lasciato dati sensibili esposti al pubblico.

Utilizzando la soluzione QRadar, i team della sicurezza possono effettuare una scansione anticipata dei loro ambienti AWS, sia come procedura ad hoc sia come parte di un programma di scansione regolare, per ricercare attivamente questi errori di configurazione e avvisare gli analisti quando vengono rilevati. Con questi avvisi a disposizione, i team della sicurezza possono dare inizio al processo di risposta per chiudere i buchi e proteggere i loro dati.

Rileva minacce per i dati e i carichi di lavoro del cloud
Dal momento che i dati sensibili e gli asset critici per il business vengono trasferiti sul cloud, AWS sta diventando il bersaglio primario per gli autori di attacchi. Se gli account AWS vengono compromessi, direttamente tramite spear phishing o nel corso di un lateral movement, i dati e i carichi di lavoro AWS potrebbero finire sotto il controllo dell'autore di un attacco. Per evitare danni, è di cruciale importanza disporre di avvertenze unificate e anticipate sulle minacce. La soluzione QRadar inserisce i dati di sicurezza AWS, che includono AWS CloudTrail, AWS CloudWatch e AWS VPC (Virtual Private Cloud) FlowLogs, in una soluzione di analytics della sicurezza centralizzata, che i team delle operazioni di sicurezza possono utilizzare per tenere traccia delle minacce, sia esterne che dall'interno, da un unico pannello di controllo.

La soluzione QRadar è in grado di raccogliere eventi dai prodotti di sicurezza utilizzando un file di plug-in che viene denominato **DSM (Device Support Module)**.

Utilizzando i protocolli supportati e i DSM (Device Support Module), la soluzione QRadar si integra con i seguenti componenti AWS per abilitare un'analisi della sicurezza avanzata:

AWS CloudTrail. L'integrazione di QRadar fornisce visibilità dell'attività dell'utente, registrando le azioni intraprese sull'account. Supporta eventi di verifica che vengono raccolti dai bucket Amazon S3 e da un gruppo di log nei log di AWS CloudWatch.

AWS Security Hub. Questa integrazione utilizza un sistema integrato di analytics e difese in tempo reale per fornire ai team della sicurezza una visibilità estesa degli avvisi di sicurezza ad alta priorità e controlli di conformità automatizzati su un singolo dashboard SOC (security operation center). Mediante l'integrazione con AFF (Amazon Findings Format) di AWS Security Hub, la soluzione QRadar è in grado di ottimizzare l'aggregazione di eventi attraverso molteplici funzionalità di sicurezza AWS, istanze e soluzioni di sicurezza APN (AWS Partner Network) per un'analisi di sicurezza approfondita.

Amazon GuardDuty. Con questa integrazione, gli utenti possono analizzare flussi continui di metadati generati dall'account e dall'attività di rete trovati negli eventi AWS CloudTrail, negli Amazon VPC Flow Logs e nei log del DNS (domain name server).

Amazon VPC Flow Logs. Questa integrazione consente ai clienti di raccogliere, memorizzare e analizzare log di flussi di rete. Può essere utilizzata per monitorare e risolvere problemi di connettività e sicurezza, per garantire che le regole di accesso alla rete stiano funzionando come previsto.

Amazon AWS Content Extension. Questa estensione del contenuto fornisce un'analisi dei dati relativi ad un nuovo evento sulla base dell'AWS integrato nella soluzione QRadar e accelera l'analisi di dati di eventi critici. I dati, come ad esempio l'ID istanza, un nome ruolo, un nome di storage e altri ancora, vengono resi prontamente disponibili per gli utenti ai fini del monitoraggio delle modifiche e della produzione di report sulla sicurezza relativa dei loro ambienti cloud.

App IBM Security QRadar Cloud Visibility
Questa app fornisce dashboard e miglioramenti AWS specifici, come ad esempio:

- Gestione delle origini log semplificata
- IAM (Identity and Access Management) per account, utenti e ruoli IAM
- Popolazione automatica delle gerarchia di rete QRadar
- Visualizzazione di Amazon VPC Flow Logs
- Integrazione con AWS Security Hub e Amazon Detective

Perché utilizzare la soluzione QRadar per monitorare gli ambienti AWS?

- Offre visibilità centralizzata dei rischi e delle minacce nelle varie implementazioni cloud
- Consente agli analisti della sicurezza di ricercare anticipatamente errori di configurazione che richiedono una risposta
- Elimina i silos per aiutare a comprendere la catena di eventi end-to-end completa, correlata ad un incidente
- Utilizza il machine learning per identificare utenti ad alto rischio e individuare minacce dall'interno più rapidamente

Ulteriori informazioni su IBM Security QRadar Amazon AWS Content Extension →

04

Integra la soluzione QRadar con Microsoft Azure

Migliora la visibilità ed elabora eventi provenienti da milioni di dispositivi

L'adozione di Microsoft Azure è cresciuta costantemente negli anni, con il 61% delle organizzazioni che afferma di utilizzare il servizio.[1] Dal momento che i dati e i carichi di lavoro si spostano in Azure, le procedure di sicurezza si devono adattare a proteggere gli asset in questo nuovo ambiente. La soluzione QRadar fornisce valide funzioni pronte all'uso per inserire i dati di sicurezza Azure in un programma di analytics della sicurezza esteso a tutta l'azienda.

Utilizzando protocolli supportati e DSM, la soluzione QRadar si integra con i seguenti componenti di Azure per contribuire all'abilitazione di un'analisi della sicurezza avanzata:

Azure Activity Logs. Il servizio di raccolta di eventi nativo di Azure acquisisce vaste quantità di eventi e dati di telemetria. Queste informazioni possono facilmente essere inviate alla soluzione QRadar per fornire ai team della sicurezza un insight approfondito sui rischi e sulle minacce potenziali negli ambienti Azure.

Azure Active Directory. L'integrazione della soluzione QRadar con Azure Active Directory offre ai team della sicurezza la capacità di monitorare identità, gestione accessi ed eventi di sicurezza provenienti da risorse esterne, come ad esempio Microsoft Office 365 e Microsoft Azure.

Microsoft Graph Security API. Con il protocollo QRadar Microsoft Graph Security API, le organizzazioni possono acquisire avvisi da Microsoft Graph Security API, che consentono agli analisti della sicurezza di indagare rapidamente sui reati.

App QRadar Cloud Visibility. La soluzione QRadar è in grado di rilevare potenziali problemi negli ambienti Azure e prendere in considerazione casi di utilizzo di sicurezza. Una volta creati i reati, l'app QRadar Cloud Visibility aiuta gli utenti a gestire questi reati nel dashboard Azure Offense Overview.

Il dashboard Azure Offense Overview presenta i dati sui reati attivi nei seguenti grafici:

- All users by magnitude (Tutti gli utenti per importanza)
- All users by related rule (Tutti gli utenti per regola correlata)
- Most severe offenses (Reati più gravi)
- All users by number of offenses (Tutti gli utenti per numero di reati)
- Magnitude level indicator (Indicatore del livello di importanza)

IBM Security QRadar Content Extension for Azure. L'estensione del contenuto QRadar Azure aggiunge regole, report e ricerche salvate per accrescere le funzionalità di analisi di eventi QRadar esistenti per implementazioni Azure.

Questa estensione del contenuto è mirata in modo specifico alla gestione della sicurezza della rete, alla modifica delle regole di sicurezza e alla gestione della rete virtuale.

Perché utilizzare la soluzione QRadar per proteggere e monitorare componenti Azure?

- Rilevare schemi di comportamento anomali in tutta l'infrastruttura IT utilizzando regole di sicurezza.
- Monitorare e diagnosticare il traffico di rete in tutti i gruppi di sicurezza di rete Azure.
- Gestire le reti virtuali con maggiore efficienza.
- Raccogliere log di eventi e dati relativi alla sicurezza del flusso di rete in gateway di rete locali.
- Monitorare prestazioni e utilizzo delle applicazioni Web in esecuzione in Azure.

Ulteriori informazioni su QRadar Content Extension for Azure →

05

Integra la soluzione QRadar con la piattaforma Google Cloud

Rileva rapidamente anomalie e scopri minacce in tempo reale

La piattaforma Google Cloud è una delle principali soluzioni cloud con una base utenti in crescita del 35%.[1] La soluzione offre una suite di servizi cloud che utilizzano l'infrastruttura Google. La soluzione IBM Security QRadar offre integrazione avanzata con la piattaforma Google Cloud. Fornisce una visibilità centralizzata raccogliendo, ricercando e analizzando centinaia di dati dai carichi di lavoro che risiedono nei vari ambienti. I team della sicurezza saranno in grado di rilevare e rispondere meglio alle minacce, indipendentemente da dove si verificano.

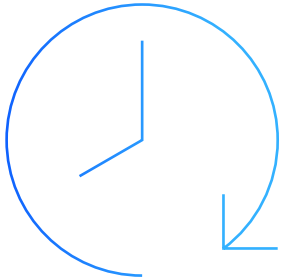
Utilizzando protocolli supportati e DSM, la soluzione QRadar si integra con i seguenti servizi della piattaforma Google Cloud per l'abilitazione di un'analisi della sicurezza avanzata:

Report sull'attività Google G Suite. La soluzione QRadar fornisce visibilità degli eventi dell'attività di verifica generati nella piattaforma Google G Suite, che includono login, account utente, Google Drive e Google Admin.

Il team della sicurezza potrà ottenere insight sui seguenti casi di utilizzo:

- Account disabilitato a causa di attività sospetta
- Informazioni sull'utente scaricate come file CSV (comma-separated values)
- Privilegi di amministratore revocati dall'utente
- L'attore ha modificato la domanda o la risposta segreta di ripristino dell'account
- L'attore ha modificato le autorizzazioni di condivisione dell'utente
- L'attore ha spostato un elemento dalla cartella di origine alla cartella di destinazione
- L'utente è stato sospeso

Protocollo di pubblicazione/sottoscrizione di Google Cloud. Con il protocollo QRadar per la pubblicazione/sottoscrizione Google Cloud, gli utenti possono godere di una maggiore visibilità di qualsiasi evento crei una falla nella pubblicazione/sottoscrizione, consentendo ai team della sicurezza di agire più rapidamente.



06

Esamina tutti i dati di SaaS

Monitora i dati provenienti dalle tue applicazioni SaaS utilizzando i DSM QRadar

Le aziende stanno già utilizzando applicazioni SaaS (software-as-a-service) per diventare più agili, lavorare più rapidamente e supportare progetti redditizi – e l'adozione di SaaS continua a crescere. Gartner prevede che questa soluzione cloud basata sui servizi avrà un valore di 143,7 miliardi di dollari entro il 2022.[2]

La soluzione QRadar aiuta le organizzazioni ad ottenere visibilità dell'utilizzo delle applicazioni SaaS e dota i team della sicurezza degli strumenti per rilevare e bloccare con maggiore efficienza le minacce. DSM precostituiti abilitano un'integrazione ininterrotta con altre soluzioni nel proprio ambiente. I DSM sono sottoposti a test e convalidati dal team IBM Security prima dell'implementazione.

La soluzione QRadar è progettata per aiutare il tuo team ad avviare facilmente il monitoraggio dei dati dalle applicazioni SaaS, che includono ambienti Salesforce.com, Office 365, Box e altri ancora more. Quando questi dati vengono inseriti nel programma di analytics della sicurezza, il team sarà in grado di ottenere un insight avanzato sulle minacce potenziali e rilevare potenziali incidenti che hanno come bersaglio i dati in queste soluzioni. Gli analisti della sicurezza saranno dotati di strumenti migliori per individuare malintenzionati dall'interno nella fase iniziale del ciclo di attacco ed impedire loro di compromettere dati sensibili, memorizzati in tali applicazioni e servizi.

Ulteriori informazioni sui DSM supportati dalla soluzione QRadar →

La soluzione QRadar fornisce integrazione tramite i DSM con una varietà di offerte SaaS e IaaS popolari.

- Amazon CloudTrail
- Amazon CloudWatch
- Amazon VPC Flows
- Microsoft Azure Event Hubs
- Microsoft Office 365
- Box.com
- Netskope Active
- Cloudera Navigator
- CloudPassage Halo
- Skyhigh Networks
- OpenStack
- Cisco Cloud Web Security
- VMware
- Salesforce
- Okta
- Piattaforma Google Cloud
- Piattaforma Red Hat® Ansible®

07

Dota il tuo team della sicurezza degli strumenti giusti

Esplora la famiglia di prodotti QRadar

Per riassumere, le soluzioni IBM Security QRadar sono progettate per fornire l'insight cruciale, necessario per la crescita degli ambienti cloud. Utilizzando questa famiglia di soluzioni, è possibile raggruppare più silos di dati in una singola piattaforma, per ottenere visibilità completa, analisi della sicurezza e rilevamento delle minacce. È possibile identificare un comportamento anomalo per potersi proteggere da minacce dall'interno e dall'esterno, individuare vulnerabilità che accidentalmente mettono a rischio dati sensibili e rilevare l'utilizzo di servizi cloud non autorizzati.

Insieme, queste funzionalità aiutano a fornire una vista completa dell'attività di utente, rete e sistema all'interno della propria organizzazione e possono fornire insight intelligenti per combattere in anticipo rischi e minacce.

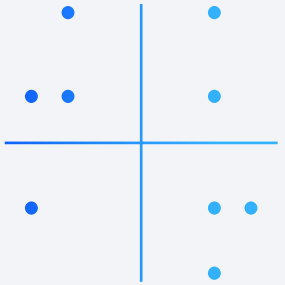
La soluzione QRadar raccoglie e analizza in un'ubicazione centralizzata feed di dati e insight sulle minacce da più origini e in più ambienti, tra cui AWS, Azure, IBM Cloud, applicazioni SaaS, cloud privati e infrastrutture on-premise tradizionali. È possibile decidere di implementare hardware o software on premise, implementare macchine virtuali in ambienti IaaS o utilizzare la soluzione QRadar come servizio cloud fornito da IBM.

Man mano che si procede nel percorso di adozione di un ambiente multicloud, è possibile contare sulle stesse funzionalità per la sicurezza, il monitoraggio e l'analytics in tutta l'azienda.

Scopri di più →

IBM è stata designata leader nell'ultimo Gartner Magic Quadrant for Security Information and Event Management (SIEM) **per l'11° volta consecutiva**

Leggi il report →



08

Perché scegliere soluzioni IBM Security?

IBM gestisce una delle più vaste organizzazioni di ricerca, sviluppo e distribuzione di soluzioni per la sicurezza nel mondo

Le soluzioni IBM Security offrono uno dei più avanzati ed integrati portafogli di prodotti e servizi per la sicurezza aziendale. Il portafoglio, supportato dalla ricerca degli esperti IBM X-Force noti in tutto il mondo, fornisce security intelligence, che aiuta le organizzazioni a proteggere in modo globale infrastrutture, dati e applicazioni. Offre soluzioni per la gestione delle identità e degli accessi, sicurezza del database, sviluppo di applicazioni, gestione dei rischi, gestione dell'endpoint, sicurezza della rete e altro ancora. Queste soluzioni consentono alle organizzazioni di gestire in modo efficace i rischi e di implementare la sicurezza integrata per dispositivi mobili, cloud, social media ed altre architetture di business aziendali.

Inoltre, IBM Global Financing offre numerose opzioni di pagamento per facilitare l'acquisto della tecnologia necessaria per espandere il proprio business. IBM fornisce la gestione dell'intero ciclo di vita dei prodotti e dei servizi IT, dall'acquisto allo smaltimento. Per ulteriori informazioni, visita il sito: ibm.com/financing.

Per ulteriori informazioni

Per ulteriori informazioni sulla soluzione di security intelligence QRadar, contatta il rappresentante IBM o il Business Partner IBM, oppure visita la pagina ibm.com/security/security-intelligence/qradar.

IBM monitora **miliardi** di eventi di sicurezza ogni giorno in più di **130 paesi** e detiene più di **3.000 brevetti di sicurezza**.

IBM Italia S.p.A.
Circonvallazione Idroscalo
20090 Segrate (Milano)
Italia

La home page di IBM Italia si trova all'indirizzo:
ibm.com

Questo documento è aggiornato alla data iniziale della pubblicazione e può essere modificato da IBM senza darne preavviso. Non tutte le offerte sono disponibili in ogni paese in cui opera IBM.

Dichiarazione di conformità alle procedure di sicurezza IBM: la sicurezza dei sistemi IT richiede la protezione di sistemi e informazioni tramite prevenzione, identificazione e risposta agli accessi impropri di origine interna o esterna alle aziende. L'accesso improprio può causare l'alterazione, la distruzione, l'appropriazione indebita o l'uso improprio delle informazioni; può inoltre provocare danni e uso improprio dei sistemi, che possono essere utilizzati per attaccare altri sistemi. Nessun prodotto o sistema IT può essere considerato completamente sicuro e nessun prodotto, servizio o misura di sicurezza è del tutto efficace nel prevenire l'uso o l'accesso improprio. Sistemi, prodotti e servizi IBM sono progettati come elementi di un approccio di sicurezza completo, nel rispetto delle normative, che richiederà necessariamente procedure operative aggiuntive e il probabile impiego di altri sistemi, prodotti o servizi per raggiungere la massima efficienza. IBM NON GARANTISCE IN ALCUN MODO CHE SISTEMI, PRODOTTI O SERVIZI SIANO IMMUNI O RENDANO IMMUNI LE AZIENDE DA ATTIVITÀ ILLEGALI O DANNOSE DI TERZE PARTI.

1 10 Key Takeaways from RightScale 2020 State Of The Cloud Report From Flexera, *Forbes*, 2 maggio 2020

2 Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019, *Gartner*, 2 aprile 2019

3 Cloud Threat Landscape Report 2020, *IBM Security X-Force®* Incident Response and Intelligence Services, maggio 2020