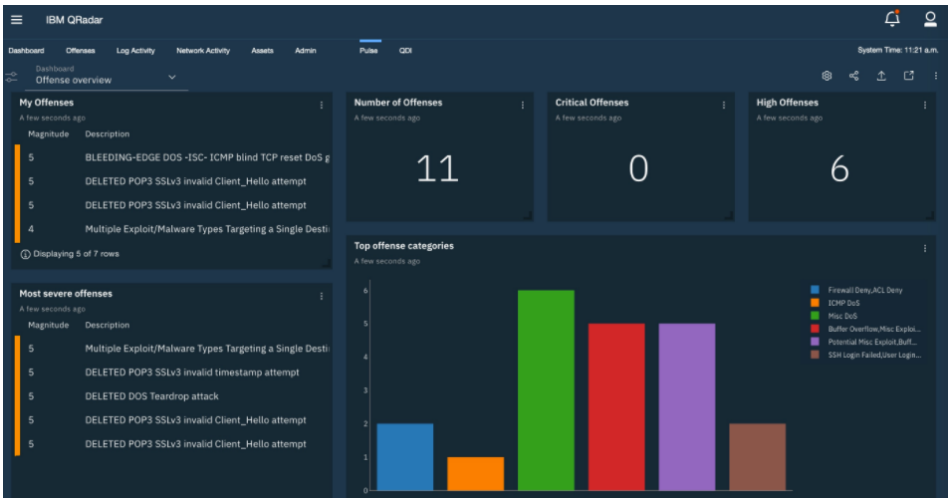
IBM QRadar®: la soluzione IBM per Security Information and Event Management (SIEM)

IBM® QRadar® Security Information and Event Management (SIEM) aiuta i team di sicurezza a rilevare e dare priorità alle minacce in modo accurato in tutta l'azienda e fornisce informazioni intelligenti che consentono ai team di rispondere rapidamente per ridurre l'impatto degli incidenti. **Consolidando gli eventi di registro e i dati del flusso di rete da migliaia di dispositivi, endpoint e applicazioni distribuiti in tutta la rete, QRadar mette in relazione tutte queste diverse informazioni e aggrega eventi correlati in singoli avvisi per accelerare l'analisi e la correzione degli incident**i. QRadar SIEM è disponibile in locale e in ambiente cloud.

QRadar SIEM permette di:

- Ottenere una visibilità completa dei dati di sicurezza da **un'unica console**
- Ridurre migliaia di eventi in un elenco gestibile di attacchi prioritari
- Analizzare rete, endpoint, asset e dati utente per **rilevare rapidamente le minacce**
- **Semplificare la conformità** con l'inserimento, la correlazione e i report automatici dei dati
- Integrare le informazioni sulle minacce di IBM® e di terze parti utilizzando STIX/TAXII
- Raggiungere un **rapido time-to-value** con oltre 600 integrazioni di impostazione predefinite

Inoltre QRadar può essere potenziato con l'utlizzo di APP gratuite e Moduli Opzionali.



Funzioni e benefici:

Protezione del cloud

La maggior parte dei carichi di lavoro aziendali è ora nel cloud. E anche se un ambiente IT ibrido è diventato la norma, la maggior parte delle organizzazioni non ha una visione completa dei rischi e delle minacce. Senza questa visibilità, è impossibile un'efficace difesa dalle minacce e la prevenzione dell'errata configurazione.

Protezione dei dati critici

La protezione dei dati critici è alla base di un protocollo di sicurezza. È uno sforzo poliedrico e adotta un approccio multistrato.

Risposta agli Alert

Gli alert sono alla base delle migliori pratiche di sicurezza per bloccare un'intrusione prima che provochi danni. L'obiettivo generale è reagire più rapidamente, coordinarsi meglio e reagire in modo più intelligente all'interno dell'organizzazione attraverso le informazioni condivise.

Assegnazione delle priorità e gestione dei rischi

L'applicazione di politiche di rischio alle vulnerabilità avvisa gli amministratori di esposizioni ad alto rischio. Una volta scoperte le vulnerabilità su dispositivi di rete, il contesto di applicazioni o software è fondamentale per sapere cosa richiede attenzione immediata.

Verifica e dimostrazione di Compliance:

Le recenti violazioni informatiche spingono le aziende ad investire maggiormente nella sicurezza IT. L'aumento delle normative e dei mandati di conformità stanno ponendo maggiormente l'accento sul rilevamento e sulla segnalazione di violazioni.

Le licenze QRadar le trovi in Convenzione Consip. Contattaci per una quotazione

https://convenzioni.converge.it/ibm3lotto3

https://www.acquistinretepa.it/opencms/opencms/scheda_iniziativa_priv.html?idIniziativa=77b8d550b23a4863