

## IBM QRadar Advisor with Watson

Nella presente Descrizione dei Servizi è descritto il servizio che IBM fornisce al Cliente. Il termine "Cliente" indica i contraenti, i relativi utenti autorizzati e i destinatari del Servizio Cloud. Il Preventivo applicabile e la PoE (Proof of Entitlement) sono forniti come Documenti d'Ordine separati.

### 1. Servizio Cloud

IBM QRadar Advisor with Watson estende l'analisi cognitiva a QRadar Security Platform, aiutando i Clienti e gli analisti della sicurezza ad individuare e rispondere alle minacce. Utilizza il corpus della conoscenza di Watson for Cyber Security, utilizzando dati non strutturati (inclusi i siti web di sicurezza, i blog e gli articoli di ricerca, ed altro ancora) e mettendoli in correlazione con gli incidenti di sicurezza locali. In questo modo può aiutare a scoprire minacce nascoste e automatizzare gli approfondimenti per le risposte e il processo decisionale. QRadar Advisor with Watson consente ad un'analista della sicurezza di inviare una violazione di sicurezza a Watson per individuare la minaccia utilizzando la sua base di conoscenze di centinaia di migliaia di fonti di dati strutturati e non strutturati e, mappandoli con le entità di minacce relative alla violazione di sicurezza originale come, ad esempio, file dannosi, indirizzi IP sospetti, entità fasulle e i rapporti tra gli stessi. Questo è particolarmente valido per determinare se una violazione di sicurezza fa parte o meno di una campagna di malware nota. In questo caso, Watson fornisce il contesto sul malware impiegato, le vulnerabilità utilizzate e lo scopo della minaccia (inclusi ulteriori endpoint potenzialmente impattati) tra gli altri approfondimenti. Il Servizio Cloud è disponibile nelle seguenti opzioni:

#### 1.1 IBM QRadar Advisor with Watson

Per IBM QRadar Advisor with Watson il Cliente deve avere una implementazione attiva di IBM Security QRadar in un ambiente on-premise locale o una implementazione cloud e deve aver installato il prerequisito software del Servizio Cloud su tale implementazione affinché il Cliente possa accedere alla sua funzionalità. Il Cliente deve ottenere un numero equivalente di titolarità per il Servizio Cloud come l'implementazione del Cliente di IBM Security QRadar. Il Servizio Cloud contiene un 'limite minimo' sul numero di query per le violazioni della sicurezza che il Cliente può inviare al Servizio Cloud con una frequenza di 1,5 richieste al giorno per 100 Eventi al Secondo (arrotondata alla richiesta successiva) per cui il Cliente è autorizzato. Le query inviate oltre tale limite saranno elaborate dal Servizio Cloud ma non avranno priorità e saranno restituite con una frequenza più bassa.

#### 1.2 IBM QRadar Advisor with Watson – Test Environment

IBM QRadar Advisor with Watson – Test Environment è pensato per i Clienti che desiderano implementare il Servizio Cloud nel proprio ambiente di test interno e può essere utilizzato solo per scopi di test di non produzione. IBM QRadar Advisor with Watson – Test Environment deve essere completato con un abbonamento al livello di produzione del Servizio Cloud.

#### 1.3 IBM QRadar Advisor with Watson – Enterprise

QRadar Advisor with Watson – Enterprise è più adatto per le grandi implementazioni SOC (security operation center) che di solito superano duecentocinquanta mila Eventi al Secondo o oltre. Il Cliente deve installare il prerequisito software del Servizio Cloud nella rispettiva implementazione di IBM Security QRadar acquistata separatamente per accedere alla funzionalità del Servizio Cloud. QRadar Advisor with Watson – Enterprise è disponibile in base ad un calcolo dei corrispettivi basato su un'Istanza che non dipende dalla scala di implementazione del Cliente di IBM Security QRadar. Il Cliente è vincolato a 20 invii nella coda in qualsiasi momento.

### 2. Descrizione della Sicurezza

Questo Servizio Cloud si conforma ai principi IBM sulla sicurezza e riservatezza dei dati per i Servizi Cloud che sono disponibili alla pagina web <http://www.ibm.com/cloud/data-security> e ad eventuali condizioni aggiuntive fornite in questo articolo. Eventuali modifiche dei principi IBM sulla sicurezza e riservatezza dei dati non altereranno la sicurezza del Servizio Cloud.

Questo Servizio Cloud può essere usato per trattare contenuto selezionato in cui siano presenti dati personali, qualora il Cliente, in qualità di titolare del trattamento dei dati, determini che le misure di sicurezza tecniche ed organizzative siano appropriate ai rischi presentati dal trattamento e alla natura dei dati da proteggere. Il Cliente riconosce che questo Servizio Cloud non offre funzionalità per la protezione

di dati personali sensibili o dati soggetti ad ulteriori requisiti normativi. Il Cliente riconosce che IBM non ha nessuna conoscenza del tipo di dati che sono stati inclusi nel contenuto e non può operare alcuna valutazione circa l'idoneità dei Servizi Cloud o alle protezioni di sicurezza in atto.

## 2.1 Funzionalità per la Sicurezza e Responsabilità

Il Servizio Cloud implementa le seguenti funzionalità di sicurezza:

Il Servizio Cloud esegue la crittografia del contenuto durante la trasmissione dei dati tra la rete IBM e l'implementazione di IBM Security QRadar. Il Servizio Cloud non esegue la crittografia di contenuto 'dormiente' in attesa della trasmissione dei dati.

Il Servizio Cloud non mantiene né prolunga la permanenza del contenuto inserito dopo aver eseguito la sua funzione su tali dati.

## 3. Supporto tecnico

Il Supporto tecnico per il Servizio Cloud viene fornito tramite email, i forum online ed un sistema online di reportistica dei problemi, come descritto di seguito. Il Supporto tecnico è incluso nel Servizio Cloud e non è disponibile come offerta separata.

Severità	Definizione di Severità	Obiettivi del Tempo di Risposta (Response Time Objectives, RTO)	Copertura del Tempo di Risposta
1	<b>Inattività di servizio/impatto critico:</b> La funzionalità aziendale critica non è operativa oppure l'interfaccia critica non funziona. Ciò è di solito applicabile a un ambiente di produzione e indica l'impossibilità di accedere ai servizi determinando un impatto critico sulle operazioni. Questa condizione richiede una soluzione immediata.	Entro 1 (una) ora	24x7
2	<b>Impatto aziendale significativo:</b> Una funzionalità dei servizi o una funzione è gravemente limitata nel suo utilizzo oppure il Cliente rischia di non rispettare le scadenze aziendali.	Entro due (2) ore lavorative	Ore lavorative L-V
3	<b>Impatto aziendale minore:</b> Indica che il servizio o la funzionalità è utilizzabile e non ha un impatto critico sulle operazioni.	Entro 4 ore lavorative	Ore lavorative L-V
4	<b>Impatto aziendale minimo:</b> una domanda o una richiesta non tecnica.	Entro 1 giorno lavorativo	Ore lavorative L-V

## 4. Informazioni sulle Titolarità e sulla Fatturazione

### 4.1 Calcolo dei Corrispettivi

Il Servizio Cloud è disponibile in base al calcolo dei corrispettivi specificato nel Documento d'Ordine:

- a. **100 Eventi al Secondo** – è un'unità di misura che consente di ottenere il Servizio Cloud. Un Evento rappresenta il verificarsi di un evento specifico che viene elaborato o relativo all'utilizzo del Servizio Cloud. È necessario ottenere titolarità sufficienti a coprire il numero di Eventi al secondo arrotondato alla centinaia successiva che si verificano durante il periodo di misurazione specificato nella PoE (Proof of Entitlement) o nel Documento d'Ordine.
- b. **Istanza** – è un'unità di misura che consente di ottenere il Servizio Cloud. Un'Istanza rappresenta l'accesso ad una configurazione specifica del Servizio Cloud. È necessario ottenere titolarità sufficienti per ogni Istanza del Servizio Cloud resa disponibile per accedervi e utilizzarla durante il periodo di misurazione specificato nella PoE del Cliente o nel Documento d'Ordine.

## **4.2 Corrispettivi di sovrapprezzo**

Se l'utilizzo effettivo del Servizio Cloud da parte del Cliente durante il periodo di misurazione supera la titolarità per cui è autorizzato nella PoE, sarà addebitato un corrispettivo di sovrapprezzo, secondo quanto stabilito nel Documento d'Ordine.

## **4.3 Verifica**

Il Cliente provvederà a i) mantenere e fornire su richiesta i record e l'output degli strumenti di sistema, come ragionevolmente richiesto da IBM e dai suoi revisori esterni, per verificare la conformità del Cliente alle condizioni del presente Accordo, e ii) richiedere tempestivamente ad IBM, tramite un nuovo ordine, gli eventuali ulteriori diritti di utilizzo, pagare i corrispettivi aggiuntivi in base alle tariffe applicate da IBM al momento, assumendosi tutte le responsabilità determinate in seguito a tali controlli, come specificato da IBM nella fattura. Questi obblighi di verifica della conformità restano validi per la durata del Servizio Cloud e per i due anni successivi.

## **5. Opzioni di Durata e Rinnovo**

La durata del Servizio Cloud inizia nella data in cui IBM comunica al Cliente che l'accesso al Servizio Cloud è disponibile, così come documentato nella PoE. Nella PoE sarà specificato se il Servizio Cloud è soggetto a rinnovo automatico, se procede sulla base di un uso continuativo o se termina alla scadenza.

In caso di rinnovo automatico, salvo comunicazione scritta da parte del Cliente di disdetta almeno 90 (novanta) giorni prima della data di scadenza del periodo contrattuale, il Servizio Cloud sarà rinnovato automaticamente per la durata contrattuale specificata nella presente PoE.

In caso di utilizzo continuativo, il Servizio Cloud continuerà ad essere disponibile con cadenza mensile fino a quando il Cliente non fornirà una comunicazione scritta di recesso almeno 90 giorni prima della scadenza. Il Servizio Cloud continuerà ad essere disponibile fino alla fine del mese solare successivo a tale periodo di 90 (novanta) giorni.

## **6. Ulteriori condizioni**

### **6.1 Disposizioni Generali**

Il Cliente accetta che IBM possa fare pubblicamente riferimento al Cliente come abbonato dei Servizi Cloud in una pubblicità o comunicato commerciale.

### **6.2 Prerequisiti Software (Software di Abilitazione)**

Il Servizio Cloud richiede l'uso del prerequisito software che il Cliente scaricherà nei propri sistemi per facilitare l'uso del Servizio Cloud. Il Cliente potrà utilizzare il prerequisito software solo in relazione all'utilizzo del Servizio Cloud.

Il prerequisito software, IBM QRadar with Watson App, viene messo a disposizione per essere scaricato dal Cliente da IBM Security App Exchange alla pagina web IBM Security App Exchange <https://exchange.xforce.ibmcloud.com/hub>.

### **6.3 Utilizzo del Servizio Cloud consentito dalla legge**

Il Servizio Cloud è progettato per aiutare il Cliente a migliorare la sicurezza del proprio ambiente e dei suoi dati. L'utilizzo del Servizio Cloud può implicare varie leggi e normative, incluse quelle riguardanti la tutela dei dati personali, la protezione dei dati, il lavoro dipendente, la comunicazione elettronica e lo storage. Il Servizio Cloud può essere utilizzato solo per scopi legali e nei termini consentiti dalla legge. Il Cliente accetta di utilizzare il Servizio Cloud in ottemperanza alle leggi, normative e policy applicabili e se ne assume ogni responsabilità ed obbligazione. Il Cliente dichiara di aver ottenuto o che otterrà qualsiasi autorizzazione o licenza necessarie per consentire l'utilizzo legale del Servizio Cloud.

### **6.4 Scadenza del Servizio Cloud**

Prima della scadenza o termine del Servizio Cloud, il Cliente può utilizzare una delle funzionalità di reportistica o esportazione del Servizio Cloud fornite per estrarre i dati.

## 6.5 Dati sulla Sicurezza

Come parte del Servizio Cloud, che includono le attività di reportistica, IBM preparerà e manterrà i dati anonimi e/o aggregati raccolti dal Servizio Cloud ("Dati sulla Sicurezza"). I Dati sulla Sicurezza non identificheranno il Cliente o una persona, salvo quando diversamente specificato nella seguente lettera (d). Il Cliente, inoltre, nel presente documento accetta che IBM possa utilizzare e/o copiare i Dati sulla Sicurezza solo per i seguenti scopi:

- a. pubblicazione e/o distribuzione dei Dati sulla Sicurezza (ad es., nelle compilazioni e/o analisi relative alla sicurezza informatica);
- b. sviluppo o miglioramento di prodotti o servizi;
- c. conduzione interna della ricerca o con terzi; e
- d. condivisione legale di dati di terzi confermati inerenti a responsabili di reati.

Accettato da:

---

Firma e timbro del Cliente

Data:

Ai sensi ed agli effetti degli artt. 1341 e 1342 del Codice Civile italiano, il Cliente approva espressamente i seguenti articoli del presente documento: "Verifica"; "Opzioni di Durata e Rinnovo".

---

Firma e timbro del Cliente

Data: