

IBM QRadar Advisor with Watson

Nella presente Descrizione dei Servizi viene descritto il Servizio Cloud. I documenti d'ordine applicabili riportano prezzi e dettagli aggiuntivi sull'ordine del cliente.

1. Servizio in 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.

1.1 Offerte

Il Cliente può selezionare le seguenti offerte disponibili.

1.1.1 IBM QRadar Advisor with Watson

Per IBM QRadar Advisor with Watson il Cliente deve avere una implementazione attiva di IBM 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 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 non saranno elaborate dal Servizio Cloud fino a fine giornata.

1.1.2 IBM QRadar Advisor with Watson – Enterprise

IBM 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 QRadar acquistata separatamente per accedere alla funzionalità del Servizio Cloud. IBM 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 di IBM QRadar del Cliente. Il Cliente è vincolato a 25 invii nella coda in qualsiasi momento.

1.1.3 IBM QRadar Advisor with Watson – Starter Pack

IBM QRadar Advisor with Watson – Starter Pack è indicato per gli utenti che si avvicinano a jQRadar Advisor with Watson per la prima volta. Questo Servizio Cloud dispone di tutte le funzionalità di QRadar Advisor with Watson descritte nel precedente articolo 1.1.1, ma è disponibile unicamente come primo acquisto di QRadar Advisor with Watson da parte del Cliente e non viene rinnovato.

1.2 Servizi Opzionali

1.2.1 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 Servizi di accelerazione

1.3.1 IBM QRadar Advisor with Watson Advanced Services

Per questo servizio in abbonamento fornito in remoto, IBM fornirà al Cliente uno dei seguenti servizi di consulenza, per un massimo di 5 (cinque) giorni in un periodo di 1 anno:

- Valutazione del processo SOC del Cliente, comprensiva dell'indagine e/o del processo di risposta dell'incidente;
- Rivalutazione della risposta dei reference-set;
- Regolazione dell'analisi automatica per le offese gravi;
- Sviluppo di casi d'uso;
- Suggesti per modifiche da apportare al processo SOC che incorporino QRadar Advisor with Watson;
- Assistenza volta ad ottenere una migliore comprensione dei dati di QRadar Advisor with Watson ed alla incorporazione degli stessi nei processi esistenti del Cliente;
- Trasferimento delle conoscenze ai soggetti QRadar Advisor with Watson pertinenti.

NOTA: A seconda dello stato della distribuzione del QRadar del Cliente sarà possibile incorporare in questo servizio le seguenti attività:

- Controllo dello Stato di distribuzione del QRadar del Cliente;
- Ulteriore ottimizzazione della distribuzione del QRadar esistente;
- Assistenza per l'aggiunta di ulteriori origini log alla distribuzione del QRadar del Cliente;

1.3.2 IBM QRadar Advisor with Watson Basic Setup Service

Questo servizio di setup viene erogato in remoto e include 40 (quaranta) ore di assistenza professionale che scadranno dopo 90 (novanta) giorni dall'acquisto, se non diversamente specificato, indipendentemente dal numero di ore utilizzate (se applicabile). I Servizi includeranno un IBM Engagement Manager che pianificherà tutti i kick-off tramite conference call.

IBM eseguirà alcune o tutte le seguenti attività:

- Valutazione del processo SOC del Cliente, comprensiva dell'indagine e/o del processo di risposta dell'incidente;
- Implementazione di QRadar Advisor with Watson nell'ambiente del Cliente:
 - Installazione di QRadar Advisor with Watson;
 - Associazione delle proprietà unificate a QRadar Advisor with Watson;
 - Implementazione della risposta dei reference-set;
 - Regolazione dell'analisi automatica per le offese gravi;
 - Assistenza per i casi d'uso;
 - Suggesti per modifiche da apportare al processo SOC che incorporino QRadar Advisor with Watson.

2. Specifiche Tecniche per la Protezione e il Trattamento dei Dati (Data Processing and Protection Data Sheets)

Il Supplemento al Trattamento dei Dati Personali (DPA o Data Processing Addendum) di IBM, disponibile alla pagina web <http://ibm.com/dpa> e le Specifiche Tecniche per la Protezione e il Trattamento dei Dati (Data Sheet o Appendice DPA) nei seguenti link forniscono ulteriori informazioni sulla protezione dei dati per i Servizi Cloud e per le opzioni relative ai tipi di Contenuto che potrebbe essere trattato, per le attività di trattamento interessate, le funzionalità per la protezione dei dati e le specifiche sulla conservazione e restituzione del Contenuto. Il DPA si applica ai dati personali presenti nel Contenuto, nella misura in cui si applicano i) il Regolamento Europeo in materia di Protezione dei Dati Personali (European General Data Protection Regulation, EU/2016/679, GDPR); o ii) altre leggi sulla protezione dei dati riportate alla pagina <http://ibm.com/dpa/dpl>.

<https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=0B439290AB5011E6BE74C84817AAB206>

3. Livelli di Servizio e Supporto Tecnico

3.1 Service Level Agreement ("SLA")

IBM fornisce al Cliente il seguente Service Level Agreement ("SLA"). IBM applicherà il Rimborso più elevato applicabile sulla base della disponibilità cumulativa del Servizio Cloud raggiunta, come mostrato nella tabella seguente. La percentuale di disponibilità, viene calcolata nel seguente modo: il numero totale di minuti nel mese contrattuale, meno il numero totale di minuti di Inattività del Servizio nel mese contrattuale, diviso per il numero totale di minuti nel mese contrattuale. La definizione di Inattività del Servizio, il processo di reclamo e le modalità per contattare IBM in relazione ai problemi di disponibilità del servizio sono riportati nel manuale di supporto al Servizio Cloud di IBM all'indirizzo https://www.ibm.com/software/support/saas_support_overview.html.

Disponibilità	Credito (% della quota di abbonamento mensile*)
Inferiore al 99,9%	2%
Inferiore al 99,0%	5%
Inferiore al 95,0%	10%

* La quota di abbonamento rappresenta il prezzo contrattuale per il mese soggetto al reclamo.

3.2 Supporto tecnico

Il supporto tecnico per il Servizio Cloud, inclusi i dettagli di contatto di assistenza, i livelli di gravità, le ore di disponibilità del supporto, i tempi di risposta e altre informazioni e processi relativi al supporto, possono essere consultati selezionando il Servizio Cloud nella guida di supporto IBM disponibile alla pagina <https://www.ibm.com/support/home/pages/support-guide/>.

4. Corrispettivi

4.1 Calcolo dei Corrispettivi

Le metriche dei corrispettivi per il Servizio Cloud sono specificate nel Documento d'Ordine.

Al presente Servizio Cloud si applica il seguente calcolo dei corrispettivi:

- Gli Eventi al Secondo (EPS) rappresentano il verificarsi di EPS specifici elaborati o collegati all'utilizzo dei Servizi Cloud. Per gli scopi di questo Servizio Cloud, gli Eventi al Secondo sono quelli raccolti ed elaborati dall'implementazione IBM QRadar del Cliente.
- Per Istanza si intende ogni accesso ad una configurazione specifica dei Servizi Cloud.
- Per Impegno si intende un servizio professionale o di formazione correlato ai Servizi Cloud.

5. Ulteriori condizioni

Agli Accordi per i Servizi Cloud (o agli accordi equivalenti per il cloud di base), stipulati prima del 1 gennaio 2019, si applicano le condizioni riportate alla pagina web <https://www.ibm.com/acs>.

5.1 Prerequisiti Software (Software di Abilitazione)

Il Servizio Cloud contiene il seguente Software di Abilitazione:

- IBM QRadar with Watson App (<https://exchange.xforce.ibmcloud.com/hub>)

5.2 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 leciti 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. Condizioni derogative

6.1 Uso dei Dati

Quanto segue prevale su quanto diversamente riportato nell'Articolo Contenuto e Protezione dei Dati Personali dei termini di base del Servizio Cloud tra le parti: IBM non utilizzerà o divulgherà i risultati derivanti dall'utilizzo da parte del Cliente del Servizio Cloud che sono specifici del Contenuto del Cliente (Approfondimenti) o che altrimenti identifichino il Cliente. IBM può utilizzare il Contenuto e altre informazioni (tranne gli Approfondimenti) derivanti dal Contenuto durante la fornitura del Servizio Cloud dopo aver rimosso gli identificativi personali, in modo tale che qualsiasi dato personale non possa essere più attribuito ad una specifica persona senza l'utilizzo di ulteriori informazioni. IBM utilizzerà questi dati solo per scopi di ricerca, test e sviluppo dell'offerta IBM.

Accettato da:

Firma e timbro del Cliente

Data:

Ai sensi e per gli effetti degli articoli 1341 e 1342 del Codice Civile Italiano, il Cliente approva specificamente i seguenti articoli del presente documento: " Specifiche Tecniche per la Protezione e il Trattamento dei Dati (Data Processing and Protection Data Sheets)", "Service Level Agreement (SLA)", "Utilizzo del Servizio Cloud consentito dalla legge".

Accettato da:

Firma e timbro del Cliente

Data: