

IBM QRadar on Cloud

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

1. Servizio in Cloud

1.1 IBM QRadar on Cloud

Il Cliente può selezionare le seguenti offerte disponibili.

1.1.1 IBM QRadar on Cloud 100 EPS

L'offerta IBM QRadar on Cloud fornisce una soluzione avanzata di informazioni sulla sicurezza dei servizi IBM Cloud basata sul prodotto IBM Security QRadar SIEM. Consente ai Clienti di raccogliere, mettere in relazione e memorizzare gli eventi generati dagli ambienti in sede e cloud ed esegue la gestione della sicurezza e delle minacce come se venisse eseguita con un prodotto QRadar SIEM implementato in sede. Come parte integrante dell'offerta, IBM fornisce inoltre il monitoraggio dell'infrastruttura con frequenza h24 per tutti i giorni della settimana e applica il livello di software più recente o le patch critiche ogni qualvolta sono disponibili.

Questo Servizio Cloud include novanta (90) giorni di storage attivo in cui è possibile effettuare la ricerca.

1.2 Servizi Opzionali

1.2.1 IBM QRadar on Cloud 1K EPS Temporary Upgrade

Un aggiornamento del servizio che fornisce una capacità aggiuntiva di 1000 EPS per la raccolta ed elaborazione degli eventi di log ma soltanto per un numero temporaneo di mesi. Il Cliente può acquistare più unità di questo aggiornamento fino al livello massimo di EPS supportato dall'offerta. L'intenzione di questa parte è consentire al Cliente che richiede la copertura dei momenti di "picco" durante l'anno, di soddisfare tali esigenze con un aumento temporaneo della capacità. Al termine di tale periodo, questi incrementi di capacità temporanea saranno rimossi dall'ambiente del Cliente.

1.2.2 IBM QRadar on Cloud Data Storage 100 EPS

L'aggiornamento dello storage dei dati aggiunge ulteriore storage ed estende il periodo di analisi. L'aggiornamento della capacità fornisce ai clienti fino ad 1 anno completo di dati archiviati per ciascun aggiornamento di 100 EPS acquistato.

1.2.3 IBM QRadar on Cloud Flows Add-On

Si integra con IBM QRadar SIEM e con i processori di flussi per fornire la visibilità di rete di Livello 3 e l'analisi dei flussi per aiutare il Cliente a sentire, rilevare e rispondere alle attività su tutta la rete del Cliente.

1.2.4 IBM QRadar on Cloud Vulnerability Management Add-On

Rileva e scopre in modo proattivo le vulnerabilità della sicurezza dei dispositivi di rete e delle applicazioni, aggiungendo il contesto e supportando la priorità delle attività di riparazione e mitigazione.

1.2.5 IBM QRadar on Cloud Log Archival

Consente al Cliente di archiviare i dati degli eventi dal Servizio Cloud durante il periodo di abbonamento. IBM collaborerà con il Cliente per scrivere gli eventi designati nello storage degli oggetti per scopi di archivio. Su richiesta del Cliente, IBM rimonderà fino a trenta (30) giorni di dati degli eventi archiviati nell'istanza del Servizio Cloud del Cliente entro tre (3) giorni lavorativi da tale richiesta. Tali dati resteranno a disposizione del Cliente per 48 ore prima di essere restituiti allo storage degli oggetti di archiviazione. Il Cliente può effettuare fino a due richieste in un periodo di tre mesi. L'aggiornamento della capacità fornisce ai Clienti fino ad 1 anno completo di dati archiviati per ciascun aggiornamento di 100 EPS acquistato.

1.3 Servizi di accelerazione

1.3.1 IBM QRadar on Cloud Optimization Service

Per questo servizio in abbonamento fornito in remoto, IBM condurrà una riunione per la revisione con il Cliente per valutare lo stato dell'istanza del Servizio Cloud del Cliente ed invierà i risultati al Cliente tramite un report QRadar on Cloud Health Status, che identificherà le eventuali aree di miglioramento.

Inoltre, IBM fornirà al Cliente, su richiesta, uno dei seguenti servizi di consulenza, per una durata massima di otto (8) giorni in un periodo di 1 anno:

- Assistenza per l'aggiunta di ulteriori origini log al Servizio Cloud;
- Configurazione di ricerche, report e dashboard aggiuntivi;
- Esecuzione di ulteriori operazioni di ottimizzazione sull'implementazione QRadar esistente; e
- Trasferimento delle conoscenze ai soggetti QRadar pertinenti.

1.3.2 Servizi di Setup

I seguenti Servizi di Setup vengono forniti in remoto e possono essere ordinati separatamente. Ciascun servizio ordinato scadrà a novanta (90) 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.

1.3.3 IBM QRadar on Cloud Deployment Service

Questo Servizio fornisce quaranta (40) ore di servizi professionali durante le quali IBM eseguirà alcune o tutte le seguenti attività:

IBM condurrà una revisione dell'architettura SIEM della durata massima di 16 ore per definire i requisiti della reportistica del Cliente ed invierà le proprie conclusioni al Cliente in un report dell'architettura della soluzione che consentirà di definire ed acquisire i requisiti del Cliente.

Tale report includerà:

- I requisiti della reportistica definiti dal cliente per aiutare a soddisfare i requisiti di conformità, verifica e dei servizi di informazione per la sicurezza.
- I requisiti dei servizi di informazione per la sicurezza, i casi d'uso e le app per cui IBM può prestare assistenza per l'implementazione (fino a dieci (10) casi d'uso e due (2) app).
- Informazioni dettagliate sulle origini di flusso e di log del Cliente che saranno richieste per supportare i casi d'uso.
- Considerazioni sull'infrastruttura di rete, come firewall e porte.

In base al report dell'architettura della soluzione, IBM eseguirà le seguenti attività, se consentito dal tempo rimanente:

- Configurare la raccolta degli eventi per un massimo di tre (3) istanze di un massimo di dieci (10) tipi di origine log nel Servizio Cloud. Questa attività comprenderà il trasferimento delle conoscenze al personale rilevante del Cliente, che potrà quindi aggiungere ulteriori origini log in base alle necessità. Saranno incluse come parte di questo Servizio solo le origini log supportate dai DSM (Device Support Modules) standard di QRadar.
- Eseguire l'ottimizzazione iniziale, che include a) attivazione delle regole pronte all'uso, delle ricerche salvate, dei grafici di serie cronologici accumulati e dei report; b) identificazione e rimozione delle origini di rumore; e c) configurazione dello storage offline tramite NFS, CIFS o iSCSI.
- Implementare i dieci (10) casi d'uso e le due (2) app da IBM QRadar App Exchange come documentato nel documento dell'architettura della soluzione.

1.3.4 IBM QRadar on Cloud Custom Parser Service

Questo Servizio fornirà lo sviluppo di un singolo programma di analisi (parser)/uDSM personalizzato per il supporto dei tipi di origine log non standard del Cliente che devono essere inviati al Servizio Cloud ed include le seguenti attività:

- Creare un programma di analisi (parser) personalizzato per un tipo di origine log non standard (lavoro eseguito in remoto);

- Creare, configurare ed eseguire la mappatura di uDSM;
- Distribuire e verificare l'uDSM personalizzato; e
- Analizzare fino a venticinque tipi di messaggio per l'origine log.

2. Data Processing and Protection Data Sheets

Il Supplemento al Trattamento dei Dati Personali (Data Processing Addendum o DPA) 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 qualora, e nella misura in cui, il Regolamento Europeo in materia di Protezione dei Dati Personali (European General Data Protection Regulation, EU/2016/679, GDPR) si applica ai dati personali presenti nel Contenuto.

<https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=FB0F42F0750011E6865BC3F213DB63F7>

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 disponibilità percentuale, 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 nella panoramica sul supporto SaaS di IBM all'indirizzo

https://www.ibm.com/software/support/saas_support_overview.html.

Disponibilità	Credito (% della quota di abbonamento mensile*)
Meno del 99,9%	2%
Inferiore al 99,0%	5%
Meno del 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:

- Per Impegno si intende un servizio professionale o di formazione correlato ai Servizi Cloud.
- Gli Eventi al secondo rappresentano le ricorrenze di un evento specifico al secondo che viene elaborato o relativo all'utilizzo dei Servizi Cloud.
- Flussi al Minuto è il numero di flussi al minuto gestiti o elaborati dai Servizi Cloud. Il Flusso è un record di comunicazione tra due host. I pacchetti che contengono lo stesso IP di origine, IP di destinazione, porta di origine, porta di destinazione e protocollo vengono combinati per diventare un record di Flusso.

- Un Asset è una risorsa o un elemento tangibile di valore misurabile in lunghezza, identificato in modo univoco, che deve essere gestito dal Servizio Cloud.

5. Ulteriori condizioni

Agli Accordi per i Servizi Cloud (o agli accordi equivalenti per il cloud di base), conclusi 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:

- Data Gateway – Il Cliente può solo installare ed utilizzare fino a dieci (10) copie di Data Gateway.

6. Condizioni derogative

6.1 Utilizzo dati di sicurezza

Quanto segue prevale su quanto definito in modo contrario nella sezione Contenuto e Protezione dei Dati Personali delle condizioni del Servizio Cloud di base tra le parti: IBM può raccogliere indicatori di potenziali attività dolose dai Contenuti del Cliente per utilizzarli in contesti di cyberthreat intelligence, in particolare URL, indirizzi IP, domini e hash di file. IBM potrà, a sua volta, informare il Cliente se tali indicatori suggeriscono che il rischio di cyberthreat del Cliente è elevato.

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: "Service Level Agreement (SLA)", "Prerequisiti Software (Software di Abilitazione)", "Condizioni derogative".

Firma e timbro del Cliente

Data: