

### IBM Resilient Incident Response Platform On Cloud

Nella presente Descrizione dei Servizi è descritto il Servizio Cloud che IBM fornisce al Cliente. Il termine "Cliente" indica l'azienda, 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 Resilient Incident Response Platform on Cloud fornisce piani d'azione dinamici (dal malware e DDoS ai dispositivi smarriti) e best practice per rispondere in generale agli incidenti. Questa base di conoscenze conduce il team del Cliente alla risposta e può essere configurata per le procedure operative specifiche del Cliente.

I team addetti alle risposte degli incidenti possono gestire e collaborare direttamente all'interno di IBM Resilient Incident Response Platform on Cloud. Diversamente dai sistemi di ticket ed altri strumenti IT di uso generale, IBM Resilient Incident Response Platform è completamente configurabile e realizzato appositamente per la risposta agli incidenti. Analisi pressoché esaustiva, dashboard personalizzabili e funzionalità di reportistica consolidate consentono ai responsabili senior di accedere ad informazioni fondamentali.

IBM Resilient Incident Response Platform è stato progettato per organizzazioni di varie dimensioni e complessità ed è disponibile in varie versioni, ordinabili separatamente:

#### 1.1 IBM Resilient Incident Response Platform Enterprise on Cloud

IBM Resilient Incident Response Platform Enterprise on Cloud è una soluzione del Servizio Cloud progettata per i sistemi di diverse dimensioni e di diverso tipo delle principali aziende. Offre una base per pianificare, gestire e ridurre le risposte ai diversi tipi di incidenti delle organizzazioni. Gli utenti possono creare piani di risposta agli incidenti in base a standard di settore e best practice e tenere traccia degli incidenti fino alla risoluzione. Il Servizio Cloud facilita la collaborazione centralizzata in tutta l'organizzazione, consentendo ai diversi 'stakeholder' di assumere i relativi ruoli e compiti come parte dell'impegno di risposta agli incidenti. Inoltre, è possibile simulare gli incidenti, aiutando i team a testare i piani di risposta, individuare le lacune e perfezionare i processi di risposta. Le integrazioni incorporate con diversi feed di informazioni sulle minacce esterne automatizzano l'arricchimento delle risorse e degli incidenti. Il Servizio Cloud include una base di conoscenze di normative globali di notifica riguardanti la violazione della tutela dei dati che contribuisce a personalizzare ulteriormente i piani di risposta agli incidenti. Inoltre, i dati possono essere sintetizzati dai sistemi di sicurezza e IT esistenti per fornire informazioni quasi in tempo reale. È possibile automatizzare, semplificare o perfezionare le diverse attività all'interno del Servizio Cloud senza che sia necessario personalizzare lo sviluppo. Per questo servizio, il Cliente deve acquistare almeno 1 titolarità Istanza e 1 titolarità Utente Autorizzato.

#### 1.2 IBM Resilient Incident Response Platform Standard on Cloud

IBM Resilient Incident Response Platform Standard on Cloud è una soluzione del Servizio Cloud progettata per soddisfare le esigenze di risposta agli incidenti di piccole e medie aziende. Offre la maggior parte delle stesse funzionalità di IBM Resilient Incident Response Platform Enterprise on Cloud, ad eccezione delle seguenti funzioni e funzionalità che il Cliente non è autorizzato ad usare: normative in merito alla violazione della tutela dei dati, automazione/orchestratura, feed di informazione sulle minacce, feed personalizzati sulle minacce e integrazione LDAP. Per questo servizio, il Cliente deve acquistare almeno 1 titolarità Istanza e 1 titolarità Utente Autorizzato.

#### 1.3 Servizi Opzionali

##### 1.3.1 IBM Resilient Incident Response Platform Enterprise for Non-Production Environment on Cloud

IBM Resilient Incident Response Platform Enterprise for Non-Production Environment on Cloud è un'istanza separata di IBM Resilient Incident Response Platform che il Cliente può utilizzare solo come parte delle attività di non produzione del Cliente, incluse, a titolo esemplificativo ma non esaustivo, attività di test, ottimizzazione delle prestazioni, diagnosi dell'errore, verifica delle prestazioni interne, stage sulle attività di 'quality assurance' e/o sviluppo interno di implementazioni aggiuntive o estensioni del Servizio Cloud, utilizzando le API pubblicate.

## 1.4 Servizi in Remoto

I seguenti Servizi in Remoto possono essere ordinati separatamente e ciascun servizio scadrà a 90 (novanta) giorni dall'acquisto, indipendentemente dal numero di ore utilizzate (se applicabile):

### 1.4.1 IBM Resilient Incident Response Platform Integration for Cloud

Questa offerta fornisce servizi di integrazione per collegare il Servizio Cloud con i relativi sistemi di sicurezza e di gestione usando un'integrazione pre-sviluppata. Sarà configurata solo l'integrazione con un sistema per Impegno. Le integrazioni per la configurazione disponibili in base a questo Servizio in Remoto sono elencate di seguito:

- **Integrazione con QRadar**

Questa integrazione con QRadar consentirà di eseguire automaticamente o manualmente il push delle violazioni per il Servizio Cloud come nuovi incidenti. Include la sincronizzazione bidirezionale per note, chiusura di eventi e nuove violazioni dei dati.

- **Integrazione con HP Arcsight**

Questa integrazione consentirà agli utenti ArcSight di eseguire il push manualmente o automaticamente dei dettagli degli eventi Arcsight per il Servizio Cloud come nuovi incidenti oppure aggiungere risorse agli incidenti esistenti.

- **Integrazione con Splunk**

Questa integrazione con Splunk consentirà di eseguire automaticamente o manualmente il push di avvisi per il Servizio Cloud come incidenti. Il Cliente può inoltre eseguire query Splunk direttamente dall'interfaccia web del Servizio Cloud.

- **Integrazione con ServiceNow**

Questa integrazione consentirà agli utenti ServiceNow di creare gli incidenti nel Servizio Cloud e agli utenti del Servizio Cloud di creare i ticket in ServiceNow. Gli aggiornamenti dei ticket o degli incidenti vengono replicati anche tra i sistemi.

- **Integrazione con JIRA**

Questa integrazione consentirà agli utenti JIRA di creare gli incidenti nel Servizio Cloud in base ai ticket JIRA e agli utenti del Servizio Cloud di creare i ticket in JIRA. Gli aggiornamenti dei ticket o degli incidenti vengono replicati anche tra i sistemi.

### 1.4.2 IBM Resilient Incident Response Platform Design Session for Cloud

Questo servizio fornisce un impegno di consulenza per aiutare ad ottimizzare l'istanza del Servizio Cloud per il Cliente. I consulenti IBM lavorano insieme al Cliente per sintetizzare i processi di risposta agli incidenti esistenti fino a 3 (tre) diversi tipi di incidenti, perfezionarli in base alle 'best practice' di settore vigenti in quel momento e alle funzionalità del Servizio Cloud e consigliare il Cliente su come configurare il Servizio Cloud per implementare tali processi.

## 2. Descrizione della Sicurezza

Questo Servizio Cloud si attiene ai principi IBM sulla sicurezza e riservatezza dei dati per i servizi IBM SaaS 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 non è progettato in base a requisiti di sicurezza specifici per dati regolamentati dalla normativa vigente come, ad esempio, dati personali o dati personali sensibili. Il Cliente è responsabile di determinare se questo Servizio Cloud soddisfa le proprie esigenze rispetto alla tipologia di contenuti che il Cliente utilizza in connessione con il Servizio Cloud.

## 3. Service Level Agreement ("SLA")

IBM fornisce il seguente Service Level Agreement ("SLA") di disponibilità per il Servizio Cloud, come specificato nella PoE. Lo SLA non costituisce una garanzia. Lo SLA è disponibile solo per il Cliente e si applica per essere utilizzato esclusivamente negli ambienti di produzione.

### 3.1 Crediti di Disponibilità

Il Cliente deve registrare un ticket di assistenza di Severità 1 mediante l'help desk del supporto tecnico IBM, entro le 24 ore successive dal momento in cui il Cliente determina che un evento ha avuto un

impatto negativo sulla disponibilità del Servizio Cloud. Il Cliente deve fornire ad IBM ragionevole assistenza nella diagnosi e risoluzione di qualsiasi problema.

La richiesta di rimedio per il ticket di assistenza per il mancato adempimento dello SLA dovrà essere inoltrata entro tre giorni lavorativi dal termine del Mese Contrattuale. Il rimborso per una richiesta di rimedio valida relativa allo SLA sarà un credito di cui verrà dato atto in una fattura successiva per il Servizio Cloud in base al periodo di tempo durante il quale l'elaborazione del sistema di produzione per il Servizio Cloud non è disponibile ("Tempo di Fermo"). Il Tempo di Fermo è misurato dal momento in cui il Cliente segnala l'evento fino a quando il Servizio Cloud viene ripristinato e non include il tempo relativo ad un'interruzione pianificata o annunciata per manutenzione; cause al di fuori del controllo di IBM; problemi con i contenuti, le tecnologie, i progetti o le istruzioni del Cliente o di terzi; errori nelle configurazioni di sistema e di piattaforme non supportate o altri errori del Cliente; oppure incidenti di sicurezza causati dal Cliente o da test di sicurezza del Cliente. IBM applicherà il rimborso più elevato in base alla disponibilità cumulativa del Servizio Cloud durante ciascun mese contrattuale, come mostrato nella tabella seguente. Il rimborso totale rispetto ad un mese contrattuale non può superare il 10 per cento di un dodicesimo (1/12) del corrispettivo annuale per il Servizio Cloud.

### 3.2 Livelli di Servizio

Disponibilità del Servizio Cloud in un mese contrattuale

Disponibilità in un mese contrattuale	Rimborso (% del Costo* dell'abbonamento mensile per il mese contrattuale oggetto di una richiesta di rimedio)
99,5%	2%
98%	5%
96%	10%

\* Se il Cliente ha acquistato il Servizio Cloud da un Business Partner IBM, il costo dell'abbonamento mensile sarà calcolato in base al listino prezzi al momento in vigore per il Servizio Cloud attivo nel mese contrattuale che è oggetto della richiesta di rimedio, scontato del 50%. IBM applicherà uno sconto direttamente al Cliente.

La disponibilità, espressa come percentuale, viene calcolata nel seguente modo: il numero totale di minuti in un mese contrattuale, meno il numero totale di minuti del Tempo di Fermo in un mese contrattuale, diviso per il numero totale di minuti in un mese contrattuale.

Esempio: 500 minuti totali di Tempo di Fermo in un mese contrattuale

43.200 minuti totali in un mese contrattuale di 30 (trenta) giorni	
- 500 minuti di Tempo di Fermo	
= 42.700 minuti	= 2% Credito di Disponibilità per il 98,8% di disponibilità in un mese contrattuale
<hr/>	
43.200 minuti totali	

## 4. Supporto tecnico

Il Supporto tecnico per il Servizio Cloud viene fornito tramite email, forum online ed un sistema online di reportistica dei problemi. Il Supporto tecnico è incluso nel Servizio Cloud e non è disponibile come offerta separata. Il Supporto tecnico è disponibile durante il normale orario lavorativo, dalle 9:00 alle 18:00, Eastern Time, esclusi i festivi.

Severità	Definizione di Severità	Obiettivi del Tempo di Risposta durante le Ore di Supporto
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
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
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
4	<b>Impatto aziendale minimo:</b> una domanda o una richiesta non tecnica.	Entro 1 giorno lavorativo

## 5. Informazioni sulle Titolarità e sulla Fatturazione

### 5.1 Calcolo dei Corrispettivi

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

- a. **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.
- b. **Utente Autorizzato** – è un'unità di misura che consente di ottenere il Servizio Cloud. Il Cliente deve ottenere autorizzazioni separate, dedicate, per ciascun Utente Autorizzato che accede al Servizio Cloud in qualsiasi modo, direttamente o indirettamente (ad esempio, tramite un programma multiplexing, dispositivo o server applicativo) tramite qualsiasi mezzo. È necessario ottenere titolarità sufficienti a coprire il numero totale di Utenti Autorizzati ai quali è stato concesso l'accesso al Servizio Cloud durante il periodo di misurazione specificato nella PoE o nel Documento d'Ordine del Cliente.
- c. **Impegno** – è un'unità di misura che consente di ottenere i servizi. Un Impegno consiste in servizi professionali e/o di formazione relativi al Servizio Cloud. È necessario ottenere titolarità sufficienti a coprire ciascun Impegno.

### 5.2 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, il Cliente dovrà corrispondere un sovrapprezzo, secondo quanto stabilito nel Documento d'Ordine.

### 5.3 Corrispettivi per i Servizi in Remoto

I Servizi in Remoto si acquistano in base al parametro di calcolo di ciascun Impegno e saranno fatturati in base alle tariffe specificate nel Documento d'Ordine.

## 6. 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 sarà rinnovato automaticamente, se procederà sulla base di un uso continuativo o se terminerà alla scadenza.

In caso di rinnovo automatico, salvo comunicazione scritta da parte del Cliente di non voler rinnovare 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 (novanta) giorni prima della scadenza. Il Servizio Cloud continuerà ad essere disponibile fino alla fine del mese di calendario successivo a tale periodo di 90 (novanta) giorni.

## 7. Ulteriori condizioni

### 7.1 Generale

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

### 7.2 Gestione della conformità del Servizio Cloud

Il Servizio Cloud può essere utilizzato per aiutare il Cliente a rispettare gli obblighi di conformità che possono essere basati su leggi, norme, consuetudini o procedure. Il Cliente riconosce e accetta che qualsiasi indicazione, suggerimento sull'utilizzo o istruzioni forniti dal Servizio Cloud non costituiscono consulenza di tipo legale, contabile o di altro settore professionale e al Cliente viene consigliato di avvalersi di un proprio consulente legale, amministrativo o di altro professionista. Il Cliente, inoltre, accetta di essere l'unico responsabile nel garantire che le sue attività, applicazioni e sistemi siano conformi con tutta la legislazione, la normativa, gli standard e le procedure applicabili. L'utilizzo del Servizio Cloud non garantisce l'osservanza di leggi, normativa, standard o procedure.

### 7.3 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 privacy, 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.

### 7.4 Dati sulla Sicurezza

Come parte del Servizio Cloud, che includono le attività di reportistica, IBM preparerà e manterrà i dati disidentificati e/o aggregati raccolti dal Servizio Cloud ("Dati della Sicurezza"). I Dati sulla Sicurezza non identificheranno il Cliente o una persona, salvo quando diversamente specificato nel seguente comma (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 della 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.

### 7.5 Cookies

Il Cliente è consapevole ed accetta che IBM potrebbe, come parte della normale operatività e supporto del Servizio Cloud, raccogliere i dati personali del Cliente (dei dipendenti o dei fornitori) relativi all'utilizzo del Servizio Cloud, mediante tracciamento ed altre tecnologie. IBM esegue tali attività per raccogliere statistiche sull'utilizzo ed informazioni sull'efficacia del Servizio Cloud, allo scopo di migliorare l'esperienza utente e/o personalizzare le interazioni con il Cliente. Il Cliente dichiara e garantisce di aver ottenuto o che sta per ottenere il consenso affinché IBM possa trattare i dati personali, raccolti per gli scopi riportati in precedenza, all'interno di IBM, di altre società IBM e dei relativi fornitori, ovunque IBM o i

suoi fornitori operino, in conformità alle leggi applicabili. IBM soddisferà le richieste di accesso, aggiornamento, correzione ed eliminazione di tali dati da parte di dipendenti e fornitori.

Accettato da:

---

Firma e timbro del Cliente

Data:

Ai sensi degli artt. 1341 e 1342 del Codice Civile Italiano, il Cliente accetta espressamente i seguenti articoli del presente documento: "Service Level Agreement ("SLA") "Opzioni di Durata e Rinnovo"; "Cookies".

---

Firma e timbro del Cliente

Data: