

IBM X-Force Threat Intelligence

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

1. Servizio in Cloud

IBM X-Force Threat Intelligence fornisce l'accesso programmatico a IBM X-Force Exchange tramite un'API RESTful che restituisce informazioni in JavaScript Object Notation (JSON). Il Servizio Cloud supporta inoltre gli standard Structured Threat Information eXpression (STIX) e Trusted Automated eXchange of Indicator Information (TAXII). Il Servizio Cloud è progettato per fornire le seguenti funzionalità principali che aiutano l'utente a:

- a. accedere alle informazioni sulle indagini specifiche della sicurezza, note come 'raccolte', costituite da contenuto sia strutturato che non strutturato.
- b. Accedere alle descrizioni del tipo di incidente (ad esempio, malware, violazione o vulnerabilità dei dati) e ciò che è risulta visibile in relazione ad un particolare incidente.
- c. Ottenere informazioni aggiornate e generali in tutti gli indicatori di minacce che sono più spesso il punto di partenza per ulteriori ricerche e il contesto per capire questi indicatori.
- d. Integrare i Dati (come definito di seguito) con le offerte del Cliente per utilizzare le informazioni di intelligence sulle minacce.

1.1 Offerte

Il Cliente può selezionare le seguenti offerte disponibili:

1.1.1 IBM X-Force Exchange Commercial API

L'API (Application Programming Interface) di IBM X-Force Exchange Commercial consente agli utenti di automatizzare il consumo di intelligence sulle minacce presenti in IBM X-Force Exchange, la piattaforma di condivisione delle informazioni sulle minacce basata su cloud di IBM. L'offerta è venduta in pacchetti di Diecimila Elementi.

1.1.2 IBM X-Force Exchange Commercial API Enterprise

IBM X-Force Exchange Commercial Application Programming Interface (API) Enterprise consente agli utenti di automatizzare il consumo di intelligence sulle minacce presenti in IBM X-Force Exchange, la piattaforma di condivisione delle informazioni sulle minacce basata su cloud di IBM. L'offerta è venduta per Istanza. Un'istanza fornisce accesso illimitato a IP e URL per feed di categorie, report su IP e URL e feed di vulnerabilità, nonché tutti i feed TAXII. Le richieste ad indicatori non trovati su X-Force Exchange sono limitate a 100.000 elementi al mese.

1.1.3 IBM Advanced Threat Protection Feed by X-Force

IBM Advanced Threat Protection Feed by X-Force fornisce agli utenti una serie di indicatori da inserire direttamente negli strumenti e nelle soluzioni per la sicurezza. Il feed fornisce indicatori di compromesso utilizzabili (IP e URL), indicatori di compromesso risultanti dalle analisi e gli indicatori DNS Early Warning. I feed sono disponibili in diversi formati, tra cui: STIX/TAXII, JSON, Text List e CSV.

1.1.4 Threat Intelligence Insights Standard for IBM Cloud Pak for Security

Questo Servizio Cloud è disponibile gratuitamente e offre ai Clienti la possibilità di integrare le informazioni sulle principali minacce e abilitare le funzioni all'interno dell'applicazione Threat Intelligence Insights su Cloud Pak for Security. Con questo pacchetto i Clienti ottengono l'accesso al livello gratuito del contenuto di X-Force Threat Intelligence, inclusi avvisi X-Force, Minacce e IOC associati (IP, URL, vulnerabilità, hash). Inoltre, i Clienti possono eseguire manualmente una funzionalità Am-I-Affected per cercare e identificare minacce dannose nel proprio ambiente. L'applicazione IBM Security Threat Intelligence Insights disponibile come parte di IBM Cloud Pak for Security rappresenta un prerequisito di questo Servizio Cloud.

1.1.5 Threat Intelligence Insights Advanced for IBM Cloud Pak for Security

Threat Intelligence Insights Advanced for IBM Cloud Pak for Security è un pacchetto premium che offre ai Clienti la possibilità di aggiungere funzioni e intelligence su minacce X-Force di prossima generazione all'applicazione Threat Intelligence Insights su Cloud Pak for Security. Il contenuto avanzato di intelligence sulle minacce, a cura del team IRIS (Incident Response and Analysis Team) di IBM, include l'accesso a report approfonditi su malware, gruppi di minacce, attività delle minacce e analisi di settore, suggerimenti di risoluzione, ICO (indicator of compromise - indicatore di compromissione) e altro ancora. Il pacchetto Advanced consente inoltre ai Clienti di eseguire la funzionalità Am-I-Affected in modo continuo e automatico, identificando e definendo la priorità, in modo proattivo, delle minacce rilevanti nell'ambiente dell'utente. L'applicazione IBM Security Threat Intelligence Insights disponibile come parte di IBM Cloud Pak for Security rappresenta un prerequisito di questo Servizio Cloud.

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 applichino 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=1ECC13601F5911E69AAAC4D0C72C126B>

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:

- Per Istanza si intende ogni accesso ad una configurazione specifica dei Servizi Cloud.
- Un Elemento è la ricorrenza di un elemento specifico che viene elaborato, gestito o che è relativo all'uso del Servizio Cloud. Per questo servizio, un Elemento è ogni risultato restituito da una singola query.
- Un Server Virtuale Gestito (MVS - Managed Virtual Server) è composto da unità di elaborazione, memoria e funzionalità di input/output per eseguire le procedure, i comandi o le applicazioni richieste, gestite dal Servizio 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 Verifica

Il Cliente provvederà a i) mantenere e fornire su richiesta le registrazioni 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 a 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.

5.2 Data

5.2.1 Definizioni

Il Servizio Cloud riguarda l'uso o l'accesso ai Dati IBM e ai Dati della Community. IBM fornisce i Dati e tutti i contenuti di terze parti disponibili tramite il Servizio Cloud senza garanzie di alcun tipo e non è responsabile di eventuali perdite dovute al Cliente per l'accesso o l'utilizzo dei Dati o del contenuto di terze parti. Si applicano le seguenti definizioni:

- Dati** – indica tutte le informazioni, il contenuto, i file, il testo, i grafici, il software, il codice, i messaggi, l'output delle query di ricerca, l'input per le query di ricerca, il contenuto delle discussioni nei forum, i metodi o altri materiali accessibili tramite il Servizio Cloud.
- Dati IBM** – indica i Dati messi a disposizione del Cliente da parte di IBM tramite il Servizio Cloud, tranne i Dati della Community. IBM, i suoi licenziatari o i suoi fornitori detengono tutti i diritti, titoli e interessi sui Dati IBM.
- Dati della Community** – indica i Dati messi a disposizione del Cliente da altri utenti del Servizio Cloud tramite il Servizio Cloud.

5.2.2 Dati IBM

IBM garantisce al Cliente una licenza limitata, non esclusiva, non trasferibile, per accedere ed utilizzare i Dati IBM tramite il Servizio Cloud unicamente - (i) per uso personale del Cliente a supporto della ricerca e delle indagini sulle minacce o (ii) allo scopo di integrare i Dati IBM nelle offerte del Cliente. Il Cliente non può duplicare o tentare di duplicare parti consistenti o tutti i Dati IBM oppure il Servizio Cloud. Il Cliente deve rispettare tutte gli avvisi di copyright, le informazioni e le restrizioni contenute o allegate ai Dati IBM, e il Cliente non può rimuovere alcun testo, copyright o altri diritti di proprietà presenti nei Dati IBM. Il Cliente non è autorizzato a eludere o tentare di eludere eventuali limitazioni di accesso correlate al Servizio Cloud.

Se il Cliente incorpora i Dati IBM nelle offerte del Cliente, il Cliente dovrà, nel proprio contratto con l'utente finale: (a) limitare la responsabilità collettiva del Cliente e dei suoi fornitori terzi per danni diretti ad un importo ragionevole e declinare qualsiasi responsabilità per danni indiretti o indiretti e garanzie implicite per fornitori terzi; (b) richiedere all'utente finale del Cliente di reclamare qualsiasi pretesa derivante dal contratto con l'utente finale esclusivamente nei confronti del Cliente; (c) proibire l'uso dei

Dati separatamente dai prodotti o dai servizi del Cliente; e (d) vietare la concessione in sublicenza dei Dati o di distribuirli altrimenti.

Inoltre, se il Cliente integra i Dati IBM nelle offerte del Cliente, oltre ai danni per cui il Cliente può essere responsabile ai sensi della normativa applicabile o delle condizioni dell'Accordo, il Cliente dovrà manlevare, difendere e tenere indenne IBM da qualsiasi pretesa di terze parti derivante da: (a) non conformità con le condizioni del paragrafo precedente; o (b) rappresentazioni, dichiarazioni, pretese o garanzie riguardanti i Dati IBM non autorizzato da IBM.

Fatto salvo quanto espressamente stabilito sopra, il Cliente non potrà copiare, modificare, riprodurre, trasmettere, vendere, offrire in vendita, affitto, leasing, fornire su licenza, garantire in sublicenza, ridistribuire o rendere disponibile a terze parti i Dati IBM.

5.2.3 Dati della Community

Il Cliente è responsabile delle proprie interazioni con gli altri utenti del Servizio Cloud, incluso l'accesso ai Dati della Community. Alcuni Dati della Community possono essere condivisi in una Raccolta o Minaccia. Per quanto riguarda i Dati della Community pubblicamente disponibili, il proprietario dei Dati ha concesso agli utenti del Servizio Cloud una licenza non esclusiva, pagata, in tutto il mondo, per utilizzare, copiare, riprodurre, modificare e/o creare opere derivate e distribuire i Dati della Community o parte di essi (Licenza pubblica). Se il Cliente copia, riproduce, distribuisce o altrimenti rende disponibili i Dati della Community in base alla Licenza pubblica, il Cliente deve indicare che si tratta di Dati della Community. Il Cliente può usare i Dati messi a disposizione in una Raccolta o Minaccia per uso da parte del Cliente esclusivamente interno e non a scopo commerciale. Il Cliente può essere esposto a Dati della Community che violano le policy IBM, la presente Descrizione dei Servizi o possa essere altrimenti offensivo.

I Dati della Community possono includere informazioni del profilo utente di altri utenti del Servizio Cloud. Il Cliente non può estrarre dati, copiare o utilizzare in altro modo le informazioni del profilo per scopi diversi da quelli di comunicare con altri utenti del Servizio Cloud in merito alle informazioni sulle minacce.

I Dati della Community possono includere link a siti web non gestiti da IBM. IBM non è responsabile del contenuto, dei prodotti, dei materiali o delle procedure (incluse le procedure sulla privacy) di tali siti web. Il Cliente prende atto che accedendo ai Dati della Community potrà essere esposto a siti di terze parti che il Cliente può ritenere offensivi, indecenti o altrimenti discutibili.

Se il Cliente ritiene che i Dati contengano dati personali non esatti o che altrimenti debbano essere rimossi, il Cliente può contattare IBM usando la funzionalità Contributo all'interno di un Report X-Force IP.

6. Condizioni derogative

6.1 Cloudflare, Inc. Subprocessor

Quanto segue prevale su quanto diversamente concordato nei Principi di Privacy e Sicurezza dei Dati per le condizioni dei Servizi Cloud tra le parti. Questo Servizio Cloud utilizza Cloudflare, Inc. come uno dei propri Subresponsabili dei Contenuti. Cloudflare tratta il Contenuto in formato codificato per ottimizzare l'erogazione dei Servizi Cloud. Cloudflare è compatibile con PCI come Service Provider di Livello 1 ed è in procinto di acquisire la conformità a ISO 27001 e SOC 2. (Per maggiore chiarezza, il Servizio Cloud complessivo non è conforme allo standard PCI).

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")", "Definizioni", "Dati IBM", "Dati della Community".

Firma e timbro del Cliente

Data: