Condizioni di Utilizzo IBM – Condizioni Specifiche dell'Offerta SaaS

IBM Application Security on Cloud

Le Condizioni di Utilizzo (Terms of Use, "ToU") sono costituite dalle presenti Condizioni di Utilizzo IBM – Condizioni Specifiche dell'Offerta SaaS ("Condizioni Specifiche dell'Offerta SaaS") e dalle disposizioni contenute nel documento Condizioni di Utilizzo IBM - Condizioni Generali ("Condizioni Generali") disponibili nel seguente URL: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

In caso di contrasto, le presenti Condizioni Specifiche dell'Offerta SaaS prevalgono sulle Condizioni Generali. Ordinando, accedendo o utilizzando i servizi IBM SaaS, il Cliente accetta le Condizioni di Utilizzo (ToU).

Le presenti Condizioni di Utilizzo (ToU) sono disciplinate dall'Accordo IBM International Passport Advantage, dall'Accordo IBM International Passport Advantage Express, o dall'Accordo Internazionale IBM per le Offerte di servizi IBM SaaS selezionate, quando applicabili, e complessivamente costituiscono l'accordo completo tra le parti ("Accordo").

1. IBM SaaS

Le presenti Condizioni Specifiche dell'Offerta SaaS alle condizioni dell'offerta di servizi IBM SaaS:

- IBM Application Security Analyzer
- IBM Application Security on Cloud Consulting Services

2. Calcolo dei Corrispettivi

I servizi IBM SaaS sono venduti secondo il seguente calcolo dei corrispettivi come specificato nel Documento d'Ordine:

a. **Job** – è un'unità di misura che consente di ottenere i servizi IBM SaaS. Un Job è un oggetto all'interno del servizio IBM SaaS che non può essere ulteriormente diviso e rappresenta un processo di elaborazione che include tutti i suoi sottoprocessi. È necessario ottenere titolarità sufficienti a coprire il numero totale di Job elaborati o gestiti dal servizio IBM SaaS durante il periodo di misurazione specificato nella PoE (Proof of Entitlement) del Cliente o nel Documento della Transazione.

b. **Istanza dell'Applicazione** – è un'unità di misura che consente di ottenere i servizi IBM SaaS. Per ciascuna istanza di un'Applicazione collegata ai servizi IBM SaaS è richiesta una titolarità Istanza dell'applicazione. Se un'Applicazione è composta da più componenti, ciascuno dei quali soddisfa uno scopo diverso e/o una base di utenti, e ciascuno dei quali può essere connesso a IBM SaaS o da questo monitorato, ognuno di tali componenti viene considerato come Applicazione separata. Inoltre gli ambienti di test, sviluppo, staging e produzione di un'Applicazione sono considerati come istanze separate dell'Applicazione e ciascuno di essi ha una propria titolarità. Più istanze applicative all'interno di un unico ambiente sono considerate istanze applicative separate e ciascuna deve avere una titolarità. È necessario ottenere titolarità sufficienti a coprire il numero di Istanze dell'applicazione connesse ai servizi IBM SaaS durante il periodo di misurazione specificato nella PoE del Cliente o nel Documento d'Ordine.

   Per gli scopi di questi servizi IBM SaaS:

   - per il test dinamico: un sito web indirizzabile tramite un URL pubblico o privato. Ciascuna Istanza dell'Applicazione da diritto ad un sito con un massimo di 1000 pagine in un unico dominio.
   - per il test statico: un'unità di codice eseguibile in un unico linguaggio di programmazione. Ciascuna Istanza dell'Applicazione da diritto alle unità di scansione fino a 1.000.000 di righe.
   - per il test del dispositivo mobile: un'unità di codice binario che può essere eseguita su un dispositivo mobile. Ciascuna piattaforma mobile diversa (ad esempio, iOS e Android) comporta Istanze dell'Applicazione differenti.

c. **Istanza** – è un'unità di misura che consente di ottenere i servizi IBM SaaS. Un'Istanza è l'accesso ad una configurazione specifica dei servizi IBM SaaS. È necessario ottenere titolarità sufficienti per ogni Istanza dei servizi IBM SaaS resa disponibile per accedervi e utilizzarla durante il periodo di misurazione specificato nella PoE (Proof of Entitlement) del Cliente o nel Documento d'Ordine.

Per ciascuna titolarità dell'Istanza non ci sono limiti sul numero di 'Job' eseguiti o di Istanze dell'Applicazione (Applicazioni connesse), a condizione, tuttavia, che non sarà possibile eseguire più di 30 'job' in un dato momento.

d. **Impegno** – è un'unità di misura che consente di ottenere i servizi. Un Impegno consiste in servizi professionali e/o di formazione relativi all'offerta IBM SaaS. È necessario ottenere titolarità sufficienti a coprire ciascun Impegno.

3. Corrispettivi e Fatturazione

L'ammontare da pagare per i servizi IBM SaaS è specificato nel Documento d'Ordine.

3.1 Corrispettivi Mensili Parziali

Un Corrispettivo Mensile Parziale così come specificato nel Documento d'Ordine può essere valutato proporzionalmente.

3.2 Corrispettivi di sovraprezzo

Se l'utilizzo effettivo dei servizi IBM SaaS da parte del Cliente durante il periodo di misurazione supera la titolarità specificata nella PoE, al Cliente sarà fatturato il sovraprezzo specificato nel Documento d'Ordine.

3.3 Corrispettivi del Setup

Al Cliente saranno addebitati i corrispettivi per il setup, come specificato nel Documento d'Ordine.

4. Opzioni di Durata e Rinnovo

La durata dei servizi IBM SaaS inizia nel momento in cui IBM comunica al Cliente che l'accesso ai servizi IBM SaaS è disponibile, così come documentato nella PoE. Nella PoE sarà specificato se l'offerta IBM SaaS sarà rinnovata automaticamente, se procederà in base a un uso continuativo o se terminerà alla fine del periodo contrattuale.

In caso di rinnovo automatico, salvo comunicazione scritta da parte del Cliente di non voler rinnovare almeno 30 giorni prima della data di scadenza del periodo contrattuale, i servizi IBM SaaS saranno rinnovati automaticamente per il periodo contrattuale specificato nella presente PoE.

In caso di utilizzo continuativo, i servizi IBM SaaS continueranno ad essere disponibili con cadenza mensile finché il Cliente non fornirà una comunicazione scritta di non voler rinnovare almeno 30 giorni prima della scadenza. L'offerta IBM SaaS sarà disponibile fino alla fine del mese di calendario successivo a tale periodo di 30 giorni.

5. Supporto Tecnico

Durante il Periodo di Abbonamento e dopo che IBM ha comunicato al Cliente che l'accesso ai servizi IBM SaaS è disponibile, il supporto tecnico viene fornito tramite i forum online e come supporto standard durante il periodo di tempo in cui il Cliente è soggetto ai corrispettivi 'Pay per Use'. Dall'interno dei servizi IBM SaaS, i Clienti possono inviare un ticket di assistenza o aprire una sessione di chat per assistenza. IBM renderà disponibile la Guida al Supporto IBM Software as a Service che contiene le informazioni di contatto e le procedure sul supporto tecnico.

Severità	Definizione di Severità	Obiettivi del Tempo di Risposta (Response Time Objectives, RTO)	Copertura del Tempo di Risposta
1	**Inattività di servizio/impatto critico:** 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) un'ora	24x7
2	**Impatto aziendale significativo:** Una funzionalità dei servizi aziendali o una funzione del servizio 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

Severità	Definizione di Severità	Obiettivi del Tempo di Risposta (Response Time Objectives, RTO)	Copertura del Tempo di Risposta
3	**Impatto aziendale minore:** 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	**Impatto aziendale minimo:** Una domanda o una richiesta non tecnica	Entro 1 giorno lavorativo	Ore lavorative L-V

5.1 Accesso ai Dati del Cliente

IBM sarà in grado di accedere ai dati del Cliente allo scopo di eseguire una diagnosi dei problemi relativi al servizio e facilitare la scansione delle applicazioni del Cliente tramite il servizio. IBM accederà ai dati al solo scopo di correggere i difetti o per fornire supporto per i prodotti o servizi IBM.

6. Ulteriori Condizioni dell'Offerta IBM SaaS

Le scansioni della sicurezza non possono identificare tutti i rischi della sicurezza all'interno di un'applicazione, né sono progettati o intesi per essere utilizzati in ambienti pericolosi che richiedono operazioni a prova di sicurezza inclusi, a titolo esemplificativo ma non esaustivo, i sistemi di navigazione o comunicazione aerea, controllo del traffico aereo, sistemi di controllo degli armamenti, macchine di supporto delle funzioni vitali, dispositivi nucleari o qualsiasi altra applicazione in cui la mancata identificazione dei rischi della sicurezza possa portare al decesso, a danni fisici o a danni irreparabili a proprietà. Le scansioni della sicurezza non garantiscono operazioni senza interruzioni o errori.

I servizi IBM SaaS possono essere utilizzati per aiutare il Cliente a rispettare gli obblighi di conformità, che possono essere basati su leggi, norme, standard o procedure. Qualsiasi indicazione, suggerimento sull'utilizzo o istruzione forniti dal Servizio non costituisce consiglio di tipo legale, contabile o di altro settore professionale e al Cliente viene consigliato di avvalersi della consulenza di un proprio legale o altro esperto professionale. Il Cliente è 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 di questo Servizio non garantisce l'osservanza di leggi, regole, consuetudini o procedure.

I servizi IBM SaaS eseguono test invasivi e non invasivi sul sito web e sulle applicazioni web o per dispositivi mobili che il Cliente intende sottoporre a scansione. Il Cliente autorizza IBM ad eseguire i Servizi come descritti in questa sede e ciò anche al fine di evitare la violazione di leggi che proibiscono qualsiasi tentativo non autorizzato di penetrare o accedere ai sistemi computerizzati. Il Cliente autorizza IBM ad eseguire i Servizi come descritto nel presente documento ed è consapevole che i Servizi rappresentano l'accesso autorizzato ai propri sistemi informatici. IBM può rivelare a terze parti la concessione di tale autorizzazione, qualora lo ritenga necessario ai fini dell'erogazione dei Servizi.

Le attività di test comportano alcuni rischi inclusi, a titolo esemplificativo ma non esaustivo, quanto specificato di seguito:

a. i sistemi computerizzati del Cliente, durante l'esecuzione delle applicazioni in fase di test, potrebbero bloccarsi o andare in crash, causando un temporaneo disservizio del sistema o la perdita di dati;

b. le prestazioni e il rendimento dei sistemi del Cliente, così come le prestazioni e il rendimento dei router e dei firewall associati, potrebbero diminuire temporaneamente;

c. è possibile che venga generata una quantità eccessiva di messaggi di log, comportando in tal modo un eccessivo consumo di spazio sul disco dedicato ai file di log;

d. alcuni dati potrebbero essere modificati o eliminati come risultato di alcune vulnerabilità del processo di "probing";

e. è possibile che scattino allarmi dei sistemi anti-Intrusione;

f. le email possono essere attivate dalle funzioni email delle applicazioni web in fase di test;

g. i servizi IBM SaaS potrebbero intercettare il traffico della rete monitorata allo scopo di cercare eventi.

Tutti i diritti o rimedi contemplati nei Service Level Agreement ("SLA") forniti da IBM e inerenti ai siti web o applicazioni saranno annullati durante le attività di test.

Nel caso al Cliente venga richiesto di inserire le credenziali di accesso autenticate per l'applicazione sottoposta a test nel Servizio, il Cliente deve inserire solo le credenziali degli account di test e non quelle degli utenti dell'ambiente di produzione. L'utilizzo delle credenziali di accesso in un ambiente di produzione determinerebbe la trasmissione di dati personali attraverso il Servizio.

I servizi IBM SaaS possono essere configurati per la scansione delle applicazioni web di produzione. Quando il Cliente imposta il tipo di scansione come "produzione", il servizio è pensato per eseguire la scansione in modo da ridurre i rischi elencati sopra; tuttavia, in alcune situazioni i servizi IBM SaaS potrebbero comportare una riduzione delle prestazioni o instabilità all'interno dei siti e delle infrastrutture di produzione sottoposti a test. IBM non fornisce alcuna garanzia o dichiarazioni relative all'idoneità dell'utilizzo dei servizi IBM SaaS per la scansione dei siti di produzione.

IL CLIENTE HA LA RESPONSABILITÀ DI DETERMINARE SE IL SERVIZIO È SICURO ED ADATTO AL SITO WEB, ALL'APPLICAZIONE WEB, ALL'APPLICAZIONE PER DISPOSITIVI MOBILI O ALL'AMBIENTE TECNICO DEL CLIENTE.

I servizi IBM SaaS sono progettati per identificare diversi potenziali problemi di sicurezza e conformità nelle applicazioni web e per dispositivi mobili e nei servizi web. Non verificano i rischi legati alle vulnerabilità ed alla conformità, e non hanno la funzione di barriera contro gli attacchi alla sicurezza. Le minacce alla sicurezza, le normative e gli standard cambiano continuamente ed il Servizio potrebbe non riflettere tali cambiamenti. La sicurezza e la conformità delle applicazioni web del Cliente, dei suoi sistemi e dipendenti, e tutte le azioni correttive, sono di sola responsabilità del Cliente. È ad esclusiva discrezione del Cliente utilizzare o non utilizzare le informazioni fornite dal Servizio.

Il Cliente autorizza IBM ad eseguire i Servizi come descritti in questa sede e ciò anche al fine di evitare la violazione di leggi che proibiscono qualsiasi tentativo non autorizzato di penetrare o accedere ai sistemi computerizzati. IL CLIENTE DICHIARA E GARANTISCE CHE NON UTILIZZERÀ IL SERVIZIO PER MONITORARE I SITI WEB E/O LE APPLICAZIONI DIVERSE DAI SITI WEB E/O LE APPLICAZIONI DI SUA PROPRIETÀ O QUELLE DI CUI POSSIEDE IL TITOLO E L'AUTORIZZAZIONE PER PROCEDERE ALLA SCANSIONE.

Per chiarezza, il contenuto del Cliente descritto nell'articolo protezione dei dati delle Condizioni di Utilizzo IBM - Condizioni Generali potrebbe contenere dati che possono diventare accessibili da parte di IBM durante il Test di Penetrazione dell'Applicazione.

6.1 Sistemi di proprietà di Terze Parti

Per i sistemi (che per lo scopo di questa fornitura di servizi possono comprendere, a titolo esemplificativo ma non esaustivo, le applicazioni e gli indirizzi IP) di proprietà di terze parti che saranno oggetto di test nell'ambito di questo documento, il Cliente accetta:

a. che prima dell'avvio della fase di analisi di IBM su un sistema di terze parti, il Cliente debba ottenere una lettera firmata dal proprietario di ogni sistema, in cui si autorizzi IBM a fornire i Servizi su quel sistema. In tale lettera dovrà altresì essere espressamente contenuta l'accettazione di quel proprietario delle condizioni delineate precedentemente nell'articolo denominato "Autorizzazione per l'esecuzione dei Test", fornendo altresì ad IBM una copia di tale autorizzazione;

b. di essere l'unico responsabile nel comunicare al proprietario di quel sistema qualsiasi rischio, esposizione e vulnerabilità identificati su tali sistemi dalle analisi remote di IBM; e

c. di organizzare e facilitare lo scambio di informazioni tra il proprietario di quel sistema e IBM, secondo quanto ritenuto necessario da IBM stessa.

Il Cliente accetta di:

- informare IBM immediatamente qualora ci fosse una modifica nella proprietà di qualsiasi sistema che sia soggetto a test in virtù del presente documento;
- non divulgare i materiali da consegnare o che IBM abbia eseguito i Servizi al di fuori del Gruppo aziendale del Cliente senza previo consenso per iscritto di IBM; e
- indennizzare completamente IBM da qualsiasi danno, perdita o responsabilità in cui IBM possa incorrere a causa di richieste di risarcimento di terzi, derivanti dal mancato adempimento da parte del Cliente delle condizioni di cui al presente articolo "Sistemi di proprietà di Terze Parti", oltre che per tutte le citazioni in giudizio o azioni intentate da parte di un terzo contro IBM o suoi subappaltatori, o agenti di IBM derivanti da (a) attività dei test sui rischi della sicurezza, esposizioni

o vulnerabilità dei sistemi che sono oggetto di test nell'ambito delle condizioni del presente documento, (b) fornire al Cliente i risultati di tali test, oppure (c) l'utilizzo o la diffusione di tali risultati da parte del Cliente.

6.2 Cookies

Il Cliente è consapevole ed accetta che IBM potrebbe, come parte della normale operatività e supporto dei servizi IBM SaaS, raccogliere dati personali del Cliente (dei dipendenti o dei fornitori) relativi all'utilizzo dei servizi IBM SaaS, mediante tracciamento ed altre tecnologie. IBM esegue tali attività allo scopo di raccogliere statistiche sull'utilizzo ed informazioni sull'efficacia dei servizi IBM SaaS al fine di migliorare l'esperienza dell'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 elaborare le informazioni personali, raccolte 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 informazioni da parte di dipendenti e fornitori.

Come parte dell'offerta IBM SaaS, che include le attività di reportistica, IBM preparerà e manterrà le informazioni disidentificate e/o aggregate raccolte dai servizi IBM SaaS (denominati "Dati sulla 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 della ricerca internamente o con terzi; e

d. condivisione legale di informazioni confermate di terzi inerenti a responsabili di reati.

6.3 Sedi beneficiarie dei servizi

Ove applicabili, le imposte sono calcolate in base alle sedi del Cliente, in base alle sedi del Cliente beneficiarie dei servizi IBM SaaS. IBM applicherà le imposte in base all'indirizzo commerciale riportato come sede principale delle attività aziendali durante la compilazione dell'ordine di IBM SaaS, salvo diversamente indicato dal Cliente. Il Cliente è responsabile di mantenere tali informazioni aggiornate e di comunicare eventuali variazioni ad IBM.

6.4 Dati Personali, Contenuto e Servizi sottoposti a normativa pubblicistica

Questa offerta IBM SaaS non è progettata in base a requisiti di sicurezza specifici per contenuti regolamentati dalla normativa vigente come, ad esempio, dati personali o dati personali sensibili. Il Cliente è responsabile di determinare se questi servizi IBM SaaS soddisfano le proprie esigenze rispetto alla tipologia di contenuti che il Cliente utilizza in connessione con i servizi IBM SaaS.

IBM non opera come fornitore di servizi disciplinati dalla Federal Communications Commission americana ("FCC") o da autorità pubbliche ("State Regulators"), e non intende fornire alcun servizio che sia regolato dalla FCC o State Regulator. Qualora la FCC o qualsiasi autorità pubblica imponessero dei requisiti normativi o obblighi su uno qualsiasi dei servizi forniti da IBM di cui al presente accordo contrattuale, IBM può: (a) modificare o sostituire i prodotti a spese del Cliente, e/o (b) modificare le modalità attraverso cui tali Servizi sono forniti al Cliente, al fine di evitare l'applicazione di tali requisiti o vincoli (ad esempio, in qualità di agente del Cliente per l'acquisto di tali Servizi da comuni fornitori di terze parti).

Appendice A

1. Descrizione Generale di IBM Application Security on Cloud

IBM Application Security on Cloud fornisce un'unica posizione per fornire assistenza al Cliente nella identificazione delle vulnerabilità della sicurezza (come, ad esempio, SQL Injection, Cross-Site Scripting e Data Leakage) per una varietà di applicazioni. Il servizio comprende vari tipi di tecnologie di scansione della sicurezza delle applicazioni, ciascuna delle quali identifica i problemi di sicurezza in tale applicazione.

IBM Application Security on Cloud fornisce le seguenti funzionalità:

- Applicazione per la scansione dei dispositivi mobili per la vulnerabilità della sicurezza. Tale operazione viene eseguita tramite tecnologie dinamiche di analisi della sicurezza (blackbox) e Interactive (glassbox).
- Scansione dei siti Web di produzione o pre-produzione su reti private o pubbliche per le vulnerabilità della sicurezza. Tale operazione viene eseguita tramite tecnologie dinamiche di analisi della sicurezza (blackbox).
- Scansione dei flussi di dati all'interno di applicazioni Web e Desktop per le vulnerabilità della sicurezza. Tale operazione viene eseguita tramite tecnologie di analisi della sicurezza statiche (whitebox).
- Report dettagliati delle vulnerabilità di sicurezza che includono sia riepiloghi di alto livello dei risultati che delle misure correttive che possono essere applicate dagli sviluppatori.
- Integrazione con diverse piattaforme DevOps

1.1 IBM Application Analyzer

IBM Application Analyzer può essere ordinato come Istanza dell'Applicazione, come Job (scansione) o come Istanza completa e consente i seguenti tipi di scansione:

- Dynamic Analyzer – Test dei siti web di pre-produzione o di produzione tramite le tecnologie DAST
- Mobile Analyzer – Test dei binari iOS o Android tramite le tecnologie IAST
- Static Analyzer – Test del flusso di dati di byte o del codice sorgente tramite le tecnologie SAST

1.2 Servizio di Setup

IBM Application Security on Cloud Consulting Services è un servizio di setup di produzione per Application Analyzer. Il Servizio usa i consulenti IBM per fornire indicazioni e assistenza nelle attività di test e di gestione del rischio dell'applicazione. IBM Application Security on Cloud Consulting Services possono essere acquistati come blocchi di Impegni che possono essere spesi in base alle quantità stabilite di seguito per richiedere e fare uso dei seguenti servizi specifici:

a. **Fast Start** [Usa 1 (una) unità di Impegno]

Il servizio Fast Start fornisce competenze e indicazioni per usare il test Application Security on Cloud e le funzionalità di gestione del rischio. Dopo che il Cliente ha confermato un accesso corretto al portale Application Security on Cloud, IBM promuoverà una web conference di 2 (due) ore e 2 (due) partecipanti attivi per fornire la formazione su AppSec di base riguardante configurazioni e funzioni IBM SaaS inclusi i tipi di scansione, l'esecuzione delle scansioni, la revisione dei report e l'installazione dei tool e plug-in associati. Il servizio Avvio Rapido sarà considerato completato dopo il completamento delle seguenti attività (a) webinar di formazione del Cliente, (b) installazione dei tool e plug-in applicabili e (c) assistenza del Cliente per il setup e esecuzione della prima scansione del Cliente.

b. **Assessment Review** [Usa 2 (due) unità di Impegno]

Il servizio Assessment Review fornisce assistenza nella revisione del risultato di un test e nel comprendere e dare priorità al risanamento delle vulnerabilità dell'applicazione. IBM promuoverà una web conference per 1 (una) ora e per 2 (due) partecipanti attivi per fornire una panoramica delle vulnerabilità e del rischio complessivo della sicurezza dell'applicazione, nonché un confronto dettagliato sulle vulnerabilità della sicurezza dell'applicazione individuate, inclusa (1) la modalità di esecuzione del test di vulnerabilità, (2) come sono state individuate le vulnerabilità, (3) qual è il

rischio di ciascuna vulnerabilità e (4) le raccomandazioni generali sulle correzioni per aiutare a sanare la vulnerabilità. La revisione sarà basata esclusivamente sul risultato del test e non sarà una revisione del codice sorgente stesso. Il Cliente riesaminerà il risultato del test e presenterà a IBM il risultato del test per la revisione prima della web conference. Il servizio Assessment Review sarà considerato completato al termine della web conference.

c. **Scan for Me** [Usa 4 (quattro) unità di Impegno]

Il servizio Scan for Me fornisce un esperto IBM della sicurezza delle applicazioni che configurerà ed eseguirà una scansione, convaliderà i risultati e condurrà un briefing sul report per riesaminare i risultati. Il Cliente consentirà ad un consulente IBM di accedere al proprio ambiente ASoC per configurare ed eseguire una scansione, convalidare i risultati, fornire raccomandazioni sulla priorità dei rimedi e condurre un briefing sul report dei risultati. IBM promuoverà una web conference per 1 (una) ora e per 2 (due) partecipanti attivi per fornire una panoramica delle vulnerabilità e del rischio complessivo della sicurezza dell'applicazione, nonché un confronto dettagliato sulle vulnerabilità della sicurezza dell'applicazione individuate inclusa (1) la modalità di esecuzione del test di vulnerabilità, (2) come sono state individuate le vulnerabilità, (3) qual è il rischio di ciascuna vulnerabilità e (4) le raccomandazioni generali sulle correzioni per aiutare a sanare la vulnerabilità. Se richiesto e fino a 30 giorni dalla scansione iniziale, IBM fornirà una nuova scansione utilizzando la configurazione della scansione originale per verificare solo gli aggiornamenti correttivi della sicurezza, non per eseguire il test di nuove funzionalità, convalidare risultati e fornire report per il Cliente. Il servizio Scan for Me sarà considerato completato al termine della web conference per riesaminare i risultati della scansione iniziale o, se applicabile, dopo il completamento della nuova scansione come richiesto dal Cliente e la consegna al Cliente del report sulla nuova scansione.

d. **Advisor on Demand** [Usa 7 (sette) unità di Impegno]

Il servizio Advisor on Demand fornisce fino a 20 (venti) ore del tempo di un consulente IBM che possono essere utilizzate per attività riguardanti i servizi IBM SaaS. Il consulente IBM fornirà assistenza per gli argomenti specifici sulla sicurezza delle applicazioni inclusa, a titolo esemplificativo ma non esaustivo, la gestione dei programmi, la priorità del test della sicurezza, le strategie di risanamento, l'analisi e la riparazione del codice sorgente. IBM collaborerà con il Cliente per conoscere e creare una pianificazione del progetto con i requisiti specifici del Cliente inclusi gli obiettivi del progetto, le tecnologie pertinenti, la tempistica desiderata, i materiali da consegnare previsti e il numero stimato di impegni per il servizio Advisor on Demand. Il Cliente deve fornire l'accesso alle applicazioni, ai sistemi e alla documentazione necessari, richiesti per eseguire i servizi. Il servizio Advisor on Demand sarà considerato completato quando saranno erogate le 20 ore di competenze sulla sicurezza e/o dopo che la pianificazione del progetto e/o i materiali da consegnare documentati definiti nella pianificazione del progetto sono stati consegnati al Cliente.

e. **Test di Penetrazione dell'Applicazione**

Tre opzioni:

(1) **Test di Penetrazione dell'Applicazione inerente alla conformità/livello di ingresso**, che include fino a 40 (quaranta) ore del tempo del Consulente e si focalizza sui difetti logici della singola fase e le versioni più semplici dei difetti di inserimento. Utilizza 15 (quindici) unità di Impegno.

(2) **Test di Penetrazione dell'Applicazione Standard**, che include fino a 60 (sessanta) ore del tempo del Consulente con una maggiore attenzione per includere i difetti Logici in flussi di lavoro multifase, versioni Complesse di difetti di inserimento e Analisi di tipi di dati complessi. Utilizza 21 (ventuno) unità di Impegno.

(3) **Test di Penetrazione dell'Applicazione Avanzato** – Include fino a 80 (ottanta) ore del tempo del Consulente con una maggiore attenzione per includere la Decodifica (Reverse engineering) degli eseguibili compilati, il Frazionamento di protocolli di rete su misura, l'analisi approfondita di librerie e framework disponibili sul mercato. Utilizza 27 (ventisette) unità di Ingaggio.

Il servizio relativo al test di penetrazione dell'applicazione fornisce una risorsa IBM per eseguire il test e l'utilizzo di un'applicazione, la consegna del report sul test e il briefing sul report per spiegare i risultati e i rischi associati.

IBM promuoverà una call di avvio del progetto della durata di un 1 (una) ora e 2 (due) partecipanti attivi per riesaminare l'ambiente e l'organizzazione del Cliente, inclusa la piattaforma, l'architettura, i

framework dell'applicazione, l'infrastruttura di supporto, i problemi noti della sicurezza o i dubbi associati all'applicazione, la pianificazione preliminare dei test e il piano di contatti per le emergenze.

IBM condurrà un test di penetrazione dell'applicazione incluso, a titolo esemplificativo ma non esaustivo: identificazione delle vulnerabilità comuni come, ad esempio, l'inserimento SQL e lo scripting tra siti, valutazione dei punti di forza e di debolezza dei controlli della sicurezza esistenti quali, ad esempio, la convalida degli input, l'autenticazione e le autorizzazioni, verifica della corretta applicazione della logica aziendale, convalida del corretto utilizzo di protocolli sicuri, identificazione dei difetti di gestione della sessione e verifica dei controlli di sicurezza appropriati durante l'accesso, recupero della password, policy delle password e altre funzioni di gestione degli utenti. I risultati saranno documentati nel Report sul Test di Penetrazione dell'Applicazione. IBM promuoverà una web conference per il briefing sul report della durata di 1 (una) ora. Il servizio relativo al Test di Penetrazione dell'Applicazione sarà considerato completato quando il periodo di tempo assegnato per la consulenza è stato utilizzato, la web conference è stata eseguita e il Report finale relativo al Test di Penetrazione dell'Applicazione è stato consegnato al Cliente.

1.2.1 Responsabilità inerenti ai Servizi di Setup

IBM provvederà a:

- fornire i Servizi di Setup utilizzando le unità di Impegno acquistate dal Cliente e in base alle POE; e
- ha completato il Servizio di Setup quando i criteri di completamento descritti nell'Articolo 1.2 sono stati completati.

Il Cliente accetta di:

- essere responsabile di tutti gli oneri associati alle richieste di Impegno effettuate dal Cliente durante il periodo contrattuale;
- e conviene che le unità di Impegno acquistate devono essere usate entro il periodo contrattuale iniziale e scadono se non utilizzate entro la data di fine del periodo contrattuale; e
- presentare una richiesta formale di tutti i Servizi di Setup almeno 30 giorni prima della data di fine dell'abbonamento.

Durante l'erogazione di qualsiasi Servizio di Setup, IBM potrà richiedere informazioni e una ragionevole collaborazione da parte del Cliente. Il mancato adempimento da parte del Cliente nel fornire le informazioni o la collaborazione richieste, potrà, come stabilito da IBM, comportare oneri relativi alle unità di Impegno, come previsto dai servizi o ritardi nell'esecuzione del servizio applicabile.

Affinché IBM possa eseguire correttamente il test, il Cliente accetta di attenersi alle istruzioni di IBM nella preparazione e gestione dell'ambiente per il periodo di test.

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: “Opzioni di Durata e Rinnovo”; “Ulteriori Condizioni dell'Offerta IBM SaaS”; “Dati Personali, Contenuto e Servizi sottoposti a normativa pubblicistica”; “Responsabilità inerenti ai Servizi di Setup”

_____

Firma e timbro del Cliente

Data: