Podmienky používania IBM – Podmienky pre konkrétnu ponuku služieb SaaS

IBM Application Security on Cloud

Podmienky používania pozostávajú z tohto dokumentu Podmienky používania IBM – Podmienky pre konkrétnu ponuku služieb SaaS („Podmienky pre konkrétnu ponuku služieb SaaS“) a dokumentu s názvom Podmienky používania IBM – Všeobecné podmienky („Všeobecné podmienky“), ktorý je k dispozícii na adrese: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

V prípade nesúladu medzi Podmienkami pre konkrétnu ponuku služieb SaaS a Všeobecnými podmienkami sa budú uplatňovať ustanovenia Podmienok pre konkrétnu ponuku služieb SaaS. Objednaním služby IBM SaaS, prístupom k nej alebo jej používaním Zákazník vyjadruje súhlas s Podmienkami používania.

Podmienky používania (ToU) sa riadia zmluvou IBM International Passport Advantage Agreement, respektíve zmluvou IBM International Passport Advantage Express Agreement alebo zmluvou IBM International Agreement for Selected IBM SaaS Offerings ("Zmluva") a spoločne s ToU tvoria kompletnú zmluvu.

1. IBM SaaS

Podmienky pre konkrétnu ponuku služieb SaaS sa vzťahujú na nasledujúce ponuky IBM SaaS:

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

2. Platobné metriky

Služba IBM SaaS sa poskytuje na základe nasledujúcich účtovných metrík, ako je určené v Transakčnom dokumente:

a. **Úloha** – je merná jednotka, na základe ktorej je možné zakúpiť si službu IBM SaaS. Úloha je objekt v rámci služby IBM SaaS, ktorý nie je možný ďalej rozdeliť a predstavuje výpočtový proces vrátane všetkých podprocesov. Zákazník musí zakúpiť dostačujúci počet oprávnení, ktorý bude pokrývať celkový počet Úloh spracovaných alebo spravovaných v rámci služby IBM SaaS počas obdobia merania určeného v Potvrdení o oprávnení Zákazníka alebo v Transakčnom dokumente.

b. **Inštancia aplikácie** – je merná jednotka, na základe ktorej je možné zakúpiť si službu IBM SaaS. Oprávnenie Inštancia aplikácie sa vyžaduje pre každú inštanciu aplikácie, ktorá je pripojená k službe IBM SaaS. Ak má aplikácia viaceré komponenty, ktoré slúžia svojmu účelu a/alebo báze užívateľov a ktoré sa dajú jednotlivo pripojiť k službe IBM SaaS alebo sa dajú touto službou jednotlivo spravovať, v takom prípade sa každý takýto komponent považuje za samostatnú Aplikáciu. Okrem toho sa za samostatné inštancie aplikácie považujú testovacie, vývojárske, postupovacie a produkčné prostredia pre aplikáciu, z ktorých každé musí mať príslušné oprávnenie. Viacero Inštancií aplikácií v rámci jedného prostredia sa budú považovať za samostatné inštancie Aplikácie, pričom každá musí mať samostatné oprávnenie. Zákazník musí zakúpiť dostačujúci počet oprávnení, ktorý bude pokrývať počet Inštancií aplikácie pripojených k službe IBM SaaS počas obdobia merania uvedeného v Potvrdení o oprávnení Zákazníka alebo v Transakčnom dokumente.

   Na účely tejto služby IBM SaaS:

   - Pri Dynamickom testovaní: webová lokalita adresovateľná prostredníctvom verejnej alebo súkromnej adresy URL. Každá Inštancia aplikácie zahŕňa oprávnenia pre lokalitu s maximálne 1 000 stránkami v rámci jednej domény.
   - Pri Statickom testovaní: jednotka spustiteľného kódu v jednom programovacom jazyku. Každá Inštancia aplikácie zahŕňa kontrolu kódu s maximálne 1 000 000 riadkami.
   - Pri Mobilnom testovaní: jednotka binárneho kódu, ktorý je možné spustiť na mobilnom zariadení. Každá jednotlivá mobilná platforma (napríklad iOS alebo Android) predstavuje inú Inštanciu aplikácie.

c. **Inštancia** – je merná jednotka, na základe ktorej je možné zakúpiť si službu IBM SaaS. Inštancia predstavuje prístup ku konkrétnej konfigurácii služby IBM SaaS. Zákazník musí zakúpiť dostatočný počet oprávnení pre každú Inštanciu služby IBM SaaS, ktorá sa sprístupní na použitie počas obdobia merania určeného v Potvrdení o oprávnení Zákazníka alebo Transakčnom dokumente.

Počet vykonávaných Úloh alebo Inštancií aplikácií (pripojených Aplikácií) v rámci jedného oprávnenia pre Inštanciu nie je obmedzený, avšak naraz sa môže vykonávať maximálne 30 Úloh.

d. **Nasadenie** – je merná jednotka, na základe ktorej je možné zakúpiť si službu IBM SaaS. Nasadenie pozostáva z odborných alebo školiacich služieb súvisiacich so službou IBM SaaS. Na pokrytie každého Nasadenia je potrebné zakúpiť dostatočný počet oprávnení.

3. Poplatky a fakturácia

Suma splatná za službu IBM SaaS je uvedená v Transakčnom dokumente.

3.1 Čiastkové mesačné poplatky

Čiastkové mesačné poplatky, ako sú definované v Transakčnom dokumente, sa môžu účtovať pomerne.

3.2 Poplatky za prekročenie limitu

V prípade, že skutočné využívanie služby IBM SaaS Zákazníkom počas obdobia merania presiahne limit na základe oprávnení určených v Potvrdení o oprávnení, Zákazníkovi sa bude účtovať poplatok za prekročenie limitu v súlade s Transakčným dokumentom.

3.3 Poplatky za nastavenie

Služby nastavenia sa Zákazníkovi budú účtovať v súlade s Transakčným dokumentom.

4. Obdobie a voľby obnovenia

Doba poskytovania služby IBM SaaS začína dátumom, kedy IBM oznámi Zákazníkovi, že môže pristupovať k službe IBM SaaS, ako je uvedené v Potvrdení o oprávnení. V Potvrdení o oprávnení bude uvedené, či sa služba IBM SaaS bude obnovovať automaticky, či sa bude poskytovať nepretržite alebo či sa po uplynutí stanoveného obdobia ukončí poskytovanie služby.

V prípade automatického obnovenia sa služba IBM SaaS automaticky obnoví na obdobie určené v Potvrdení o oprávnení, pokiaľ Zákazník neposkytne písomnú výpoveď aspoň 90 dní pred dátumom skončenia obdobia.

V prípade nepretržitého poskytovania bude služba IBM SaaS dostupná vždy na 1-mesačné obdobie, pokiaľ Zákazník neposkytne písomnú výpoveď 30 dní vopred. Služba IBM SaaS bude naďalej dostupná do konca kalendárneho mesiaca po uplynutí tohto 30-dňového obdobia.

5. Technická podpora

Počas Doby predplatného a po tom, čo IBM oznámi Zákazníkovi, že môže pristupovať k službe IBM SaaS, sa bude poskytovať technická podpora prostredníctvom diskusných fór online a formou štandardne podpory počas časového obdobia, počas ktorého Zákazníkovi vzniká povinnosť uhradiť Platby podľa použitia. Z prostredia služby IBM SaaS môže Zákazník odosielať lístky podpory alebo požiadať o pomoc prostredníctvom relácie online konverzácie. IBM sprístupní publikáciu IBM Software as a Service Support Handbook uvádzajúcu kontaktné údaje technickej podpory a iné informácie a procesy.

Stupeň Závažnosti	Definícia závažnosti	Ciele času odozvy	Pokrytie času odozvy
1	**Kritický obchodný dopad/služba nedostupná:** Kľúčové podnikové funkcie sú nefunkčné alebo zlyhalo kľúčové rozhranie. Zvyčajne sa to vzťahuje na produkčné prostredia a naznačuje to, že neschopnosť prístupu k službám má za následok kľúčový dopad na operácie. Pri tomto stave sa vyžaduje okamžité riešenie.	Do 1 hodiny	24x7
2	**Významný obchodný dopad:** Obchodný komponent služby alebo funkcia služby sú výrazne obmedzené v zmysle používania alebo Zákazník čelí riziku nesplnenia obchodných termínov.	Do 2 pracovných hodín	Po-Pi, pracovný čas
3	**Menší obchodný dopad:** Indikuje, že služba alebo funkčnosť je použiteľná a nejde o kľúčový dopad na operácie.	Do 4 pracovných hodín	Po-Pi, pracovný čas
4	**Minimálny obchodný dopad:** Požiadavka ale netechnická požiadavka	Do 1 pracovného dňa	Po-Pi, pracovný čas

5.1 Prístup k údajom Zákazníka

IBM bude môcť pristupovať k údajom Zákazníka na účely diagnostiky problémov so službou a uľahčenia vyhľadania aplikácií Zákazníka službou. IBM bude k údajom pristupovať iba za účelom opravy chýb alebo poskytnutia podpory pre produkty alebo služby IBM.

6. Ďalšie podmienky vzťahujúce sa na ponuku IBM SaaS

Pri kontrole zabezpečenia nemusia byť identifikované všetky bezpečnostné riziká v aplikácii a tieto aplikácie nie sú určené na použitie v nebezpečných prostrediach, v ktorých je nevyhnutná bezporuchová prevádzka, ako sú navigačné systémy v leteckej doprave, riadiace systémy v leteckej doprave, zbraňové systémy, systémy na podporu životných funkcií, nukleárne zariadenia alebo pri iných použitiach, pri ktorých by neschopnosť identifikovať bezpečnostné riziko mohlo viesť k usmrteniu, zraneniam alebo škodám na majetku. Neudeľuje sa žiadna záruka, že kontroly zabezpečenia budú fungovať nepretržite alebo bezchybne.

Službu IBM SaaS je možné využiť ako pomoc pre Zákazníka pri plnení záväzkov vyplývajúcich zo zabezpečenia súladu s nariadeniami, ktoré môžu mať podklad v zákonoch, regulačných usmerneniach, štandardoch a postupoch. Žiadne pokyny, návrhy použitia ani rady, ktoré sa poskytnú v rámci Služby, nepredstavujú žiadne právne, účtovné, ani iné odborné rady a Zákazník bol upozornený na skutočnosť, že si musí zaobstarať vlastné právne či iné odborné poradenstvo. Zákazník bude niesť výhradnú zodpovednosť za zabezpečenie toho, že Zákazník, ako aj jeho aktivity, aplikácie a systémy budú spĺňať všetky príslušné zákony, predpisy, normy a postupy. Používanie tejto Služby nezaručuje súlad s právnymi predpismi, regulačnými nariadeniami, normami alebo postupmi.

Táto služba IBM SaaS vykonáva invazívne a neinvazívne testy vo webových lokalitách alebo webových alebo mobilných aplikáciách, ktoré Zákazník vyberie na testovanie. Niektoré právne predpisy zakazujú neoprávnené pokusy o prienik do počítačových systémov alebo prístup k nim. Zákazník udeľuje IBM oprávnenie na vykonávanie Služieb podľa špecifikácií uvedených v tomto dokumente a potvrdzuje, že tieto Služby predstavujú oprávnený prístup k počítačovým systémom Zákazníka. IBM môže o tomto oprávnení informovať tretiu stranu, ak to bude potrebné pri poskytovaní Služieb.

S testovaním sa môže spájať niekoľkých rizík vrátane, avšak bez obmedzenia na, nasledujúcich:

a. počítačové systémy Zákazníka môžu pri spúšťaní testovaných aplikácií zamrznúť alebo zlyhať, v dôsledku čoho môže dôjsť k dočasnej nedostupnosti systémov alebo strate údajov

b. počas testovania sa môže dočasne znížiť výkon a priepustnosť systémov Zákazníka, ako aj výkon a priepustnosť súvisiacich smerovačov a brán firewall

c. môže sa vygenerovať neúmerné množstvo správ protokolovania, v dôsledku čoho môže dôjsť k nadmernému zaplneniu diskového priestoru protokolovými súbormi

d. v dôsledku testovania zraniteľnosti môže dôjsť k zmene alebo odstráneniu údajov

e. systémy zisťovania narušenia zabezpečenia môžu vyvolať poplach

f. funkcia posielania e-mailov testovanej webovej aplikácie môže počas testovania poslať e-maily

g. služba IBM SaaS môže zachytávať údaje prenášané cez monitorovanú sieť s cieľom zistiť sledované udalosti

Počas vykonávania aktivít testovania sa nebudú uplatňovať žiadne práva ani nápravné prostriedky poskytované IBM, ktoré by vyplývali zo zmluvy o úrovni poskytovaných služieb a súviseli s webovými stránkami alebo aplikáciami podliehajúcim testovaniu.

V prípade, že Zákazník musí zadať overené prihlasovacie údaje pre testovanú aplikáciu v Službe, mal by zadávať iba prihlasovacie údaje pre testovacie kontá, nie prihlasovacie údaje užívateľov v produkčnom prostredí. V prípade zadaní prihlasovacích údajov v produkčnom prostredí by mohlo dôjsť k prenosu osobných údajov cez Službu.

Služba IBM SaaS sa môže nakonfigurovať tak, aby testovala produkčné webové aplikácie. Ak Zákazník nastaví ako typ testovania možnosť „produkčné“, služba bude vykonávať testy spôsobom minimalizujúcim vyššie uvedené riziká, avšak v niektorých situáciách môže služba IBM SaaS spôsobiť zníženie výkonu alebo nestabilitu v testovaných produkčných lokalitách alebo infraštruktúrach. IBM nezaručuje, že služba IBM SaaS je vhodná na testovanie produkčných lokalít.

VYHODNOTENIE TOHO, ČI JE VHODNÉ POUŽIŤ SLUŽBU S WEBOVOU STRÁNKOU, WEBOVOU APLIKÁCIOU, MOBILNOU APLIKÁCIOU ALEBO V TECHNICKOM PROSTREDÍ ZÁKAZNÍKA ALEBO ČI JE JEJ POUŽITIE BEZPEČNÉ, JE ZODPOVEDNOSŤOU ZÁKAZNÍKA.

Táto služba IBM SaaS bola navrhnutá tak, aby umožňovala identifikáciu rozličných potenciálnych bezpečnostných a legislatívnych problémov v mobilných a webových aplikáciách a webových službách. Táto služba však nevykonáva testovanie na zistenie všetkých bezpečnostných alebo legislatívnych rizík a tiež nezabraňuje v útokoch na zabezpečenie. Bezpečnostné hrozby, predpisy a štandardy sa nepretržite menia a služba nemusí byť schopná reagovať na tento vývoj. Zaručenie bezpečnosti webových aplikácií, systémov a zamestnancov a dodržiavanie súladu s nariadeniami, ako aj prijatie príslušných nápravných opatrení, je výhradne zodpovednosťou Zákazníka. To, či Zákazník využije informácie poskytnuté Službou, závisí výhradne od uváženia Zákazníka.

Niektoré právne predpisy zakazujú neoprávnené pokusy o prienik do počítačových systémov alebo prístup k nim. ZÁKAZNÍK JE POVINNÝ ZABEZPEČIŤ, ŽE SA SLUŽBA NEBUDE POUŽÍVAŤ NA TESTOVANIE INÝCH WEBOVÝCH LOKALÍT A/ALEBO APLIKÁCIÍ, AKO SÚ WEBOVÉ LOKALITY A/ALEBO APLIKÁCIE VLASTNENÉ ZÁKAZNÍKOM ALEBO WEBOVÉ LOKALITY A/ALEBO APLIKÁCIE, KTORÉ JE ZÁKAZNÍK OPRÁVNENÝ TESTOVAŤ.

Na objasnenie: Obsah Zákazníka definovaný v časti Ochrana údajov dokumentu Podmienky používania IBM – Všeobecné podmienky bude zahŕňať aj údaje, ktoré sa stanú prístupnými pre IBM pri Testovaní možnosti prieniku do aplikácie.

6.1 Systémy vlastnené treťou stranou

V súvislosti so systémami (ktoré na účely tohto ustanovenia budú zahŕňať okrem iného aj aplikácie a IP adresy) vlastnenými treťou stranou, ktoré budú podliehať testovaniu definovanému v tejto časti, Zákazník súhlasí, že:

a. skôr ako IBM vykoná testovanie systému tretej strany, Zákazník získa od vlastníkov jednotlivých systémov písomné oprávnenie povoľujúce IBM poskytnúť Služby na danom systéme a potvrdzujúce súhlas vlastníka systému s podmienkami definovanými v odseku „Oprávnenie na vykonanie testovania“ a poskytne IBM kópiu tohto oprávnenia

b. bude niesť výhradnú zodpovednosť za informovanie vlastníkov systémov o rizikách, bezpečnostných hrozbách a problémoch so zabezpečením, ktoré IBM identifikuje na týchto systémoch pri vzdialenom testovaní

c. zabezpečí a umožní výmenu informácií medzi vlastníkom systému a IBM, ak to IBM uzná za potrebné

Zákazník súhlasí s tým, že:

- bude IBM bezodkladne informovať o každej zmene vlastníka systému, ktorý je predmetom testovania na základe tejto Služby
- nevyzradí výstupy zo Služby ani skutočnosť, že IBM poskytla Služby, mimo Spoločnosti Zákazníka bez predchádzajúceho písomného súhlasu IBM
- v plnej miere odškodní IBM za akékoľvek straty alebo záväzky, ktoré IBM vzniknú v dôsledku nárokov tretích strán vyplývajúcich z nesplnenia požiadaviek definovaných v odseku s názvom „Systémy vlastnené treťou stranou“ zo strany Zákazníka, ako aj zo súdnych výziev alebo žalôb vznesených voči IBM alebo zmluvným dodávateľom alebo zástupcom IBM v súvislosti s (a) testovaním bezpečnostných rizík, nedostatkov alebo problémov systémov, ktoré podliehajú testovaniu na základe tejto Služby, (b) poskytnutím výsledkov testovania Zákazníkovi alebo (c) použitím alebo zverejnením týchto výsledkov Zákazníkom

6.2 Súbory cookie

Zákazník berie na vedomie a súhlasí s tým, že spoločnosť IBM môže v rámci svojich štandardných prevádzkových operácií a podpory služby IBM SaaS zhromažďovať osobné údaje od Zákazníka (ako aj zamestnancov a zmluvných dodávateľov Zákazníka) súvisiace s používaním služby IBM SaaS prostredníctvom technológií sledovania a iných technológií. Spoločnosť IBM zhromažďuje tieto informácie s cieľom získať štatistické informácie o používaní služby a informácie o efektivite služby IBM SaaS na účely zlepšenia užívateľských skúseností alebo prispôsobenia komunikácie so Zákazníkom. Zákazník potvrdzuje, že získa alebo získal súhlas so spracovaním získaných osobných údajov na vyššie uvedené účely spoločnosťou IBM v rámci spoločnosti IBM, iných spoločností zo skupiny spoločností IBM a ich zmluvných dodávateľov v ľubovoľnej krajine, v ktorej spoločnosť IBM, jej dcérske spoločnosti alebo

zmluvní dodávatelia pôsobia, v súlade s príslušnými právnymi predpismi. IBM vyhovie všetkým požiadavkám zo strany zamestnancov a zmluvných dodávateľov Zákazníka v súvislosti s prístupom k získaným osobným údajom, ich aktualizáciou, opravou alebo odstránením.

V rámci služby IBM SaaS zahrňujúcej aktivity tvorby výkazov IBM bude získavať a uchovávať súhrnné informácie zbavené identifikačných znakov zo služby IBM SaaS (ďalej aj „Bezpečnostné údaje“). Na základe Bezpečnostných údajov nebude možné identifikovať Zákazníka ani žiadneho iného jednotlivca, okrem prípadov definovaných v bode (d) nižšie. Zákazník týmto vyjadruje súhlas s tým, že IBM môže používať alebo kopírovať Bezpečnostné údaje, a to výhradne na nasledujúce účely:

a. publikovanie alebo distribúcia Bezpečnostných údajov (napr. v rámci výberov a analýz súvisiacich s počítačovou bezpečnosťou)

b. vývoj alebo zlepšovanie produktov alebo služieb

c. interný vývoj alebo vývoj v spolupráci s tretími stranami

d. zákonné zdieľanie informácií o externých porušovateľoch bezpečnosti

6.3 Miesta s daňovým zvýhodnením

Ak to bude možné, dane sa budú určovať podľa miesta (miest), ktoré Zákazník označí ako miesta, kde sa využíva služba IBM SaaS. IBM vyrubí dane na podľa adresy firmy, ktorá bude uvedená na objednávke IBM SaaS ako primárne miesto využívania, pokiaľ Zákazník neposkytne IBM ďalšie informácie. Zákazník zodpovedá za aktuálnosť takýchto informácií a je povinný nahlásiť akékoľvek zmeny spoločnosti IBM.

6.4 Osobné údaje a regulovaný obsah v Službách

Táto služba IBM SaaS nie je navrhnutá s ohľadom na konkrétne bezpečnostné požiadavky súvisiace s regulovaným obsahom, ako sú osobné údaje alebo citlivé osobné údaje. To, či táto služba IBM SaaS spĺňa požiadavky Zákazníka s ohľadom na typ obsahu, ktorý Zákazník používa v spojení so službou IBM SaaS, musí určiť Zákazník.

IBM nepredstavuje poskytovateľa služieb regulovaných na základe predpisov organizácie FCC (Federal Communications Commission) alebo štátnych regulačných orgánov (ďalej aj „Štátne regulačné orgány“) a nezamýšľa poskytovať žiadne služby regulované na základe predpisov organizácie FCC ani Štátnych regulačných orgánov. Ak organizácia FCC alebo akýkoľvek Štátny regulačný orgán zavedie regulačné požiadavky alebo povinnosti v súvislosti so službami poskytovanými IBM na základe týchto Služieb, IBM môže: (a) upraviť, nahradiť alebo vymeniť produkty, a to na náklady Zákazníka, alebo (b) zmeniť spôsob poskytovania týchto služieb Zákazníkovi, aby sa predišlo uplatňovaniu týchto požiadaviek alebo povinností voči IBM (napríklad tým, že bude vystupovať ako zástupca Zákazníka pri získavaní týchto služieb od spoločného poskytovateľa tretej strany).

Príloha A

1. IBM Application Security on Cloud - Všeobecný popis

IBM Application Security on Cloud pomáha Zákazníkovi pri identifikácii bezpečnostných nedostatkov (ako sú SQL Injection, CSS (Cross-Site Scripting) a únik údajov) rozličných aplikácií z jedného miesta. Služba zahŕňa rozličné typy techník skenovania zabezpečenia aplikácií, pričom každá z nich identifikuje bezpečnostné problémy v danej aplikácii.

IBM Application Security on Cloud poskytuje nasledujúce funkcie:

- Zisťovanie bezpečnostných nedostatkov v mobilných aplikáciách. Toto zisťovanie sa vykonáva s využitím dynamických (čierna skrinka) a interaktívnych (sklenená skrinka) techník bezpečnostnej analýzy.
- Zisťovanie bezpečnostných nedostatkov v produkčných alebo predprodukčných, verejných alebo súkromných sieťach a webových lokalitách. Toto zisťovanie sa vykonáva s využitím dynamických (čierna skrinka) techník bezpečnostnej analýzy.
- Zisťovanie bezpečnostných nedostatkov v dátových tokoch v rámci webových a počítačových aplikácií. Toto zisťovanie sa vykonáva s využitím statických (biela skrinka) techník bezpečnostnej analýzy.
- Podrobné správy o bezpečnostných nedostatkoch obsahujúce sumárne zhrnutia nálezov spolu s pokynmi na riešenie problémov pre vývojárov.
- Integrácia s rozličnými platformami DevOps

1.1 IBM Application Analyzer

Softvér IBM Application Analyzer si môže Zákazník objednať podľa počtu Inštancií aplikácií, podľa počtu Úloh (kontrol) alebo ako úplnú Inštanciu, pričom táto zahŕňa nasledujúce typy kontrol:

- Dynamic Analyzer – Testovanie predprodukčných a produkčných webových stránok s použitím techník DAST
- Mobile Analyzer – Testovanie binárnych súborov iOS a Android s použitím techník IAST
- Static Analyzer – Testovanie údajov v toku bajtového alebo zdrojového kódu s použitím techník SAST

1.2 Služba nastavenia

IBM Application Security on Cloud Consulting Services predstavuje službu nastavenia určenú špecificky pre aplikáciu Application Analyzer. Táto Služba ponúka pomoc a asistenciu zo strany konzultantov IBM pri testovaní a riadení aplikačných rizík. Službu IBM Application Security on Cloud Consulting Services si Zákazník môže zakúpiť ako bloky Nasadení v nižšie definovaných množstvách za účelom získania nasledujúcich konkrétnych služieb:

a. **Fast Start** [vyžaduje jednu (1) jednotku Nasadenia]

Služba Fast Start poskytuje odborné vedomosti a poradenstvo pri používaní funkcií na testovanie a riadenie rizík softvéru Application Security on Cloud. Po tom, čo Zákazník potvrdí úspešné prihlásenie do portálu Application Security on Cloud, IBM usporiada webovú konferenciu trvajúcu maximálne dve (2) hodiny pre maximálne dvoch (2) aktívnych účastníkov, v rámci ktorej predstaví základné možnosti konfigurácie a funkcie softvéru AppSec v službe IBM SaaS, a to vrátane typov kontrol, spúšťania kontrol, zobrazovania zostáv a inštalácie súvisiacich nástrojov a doplnkov. Služba Fast Start sa bude považovať za dokončenú po (a) absolvovaní výučbového webového seminára, (b) inštalácii príslušných nástrojov a doplnkov (c) poskytnutí pomoci Zákazníkovi pri konfigurácii a spustení prvej kontroly.

b. **Assessment Review** [vyžaduje dve (2) jednotky Nasadenia]

Služba Assessment Review zahŕňa pomoc pri interpretácii výsledkov kontroly, a to vrátane objasnenia a určenia priority riešenia problémov so zabezpečením v aplikácii. IBM usporiada webovú konferenciu s trvaním maximálne jednu (1) hodinu pre maximálne dvoch (2) aktívnych účastníkov, v rámci ktorej poskytne základné informácie o zistených bezpečnostných nedostatkoch a o celkových bezpečnostných rizikách aplikácie, ako aj priestor na podrobnú diskusiu o zistených

bezpečnostných nedostatkoch aplikácie vrátane informácií (1) o spôsobe testovania bezpečnostných nedostatkov, (2) o tom, ako boli odhalené tieto bezpečnostné nedostatky, (3) o rizikovosť jednotlivých bezpečnostných nedostatkov a (4) o všeobecných odporúčaniach k riešeniu týchto bezpečnostných nedostatkov. Táto pomoc sa bude vzťahovať výhradne na výsledky testovania, nebude zahŕňať posúdenie samotného zdrojového kódu. Pred uskutočnením tejto webovej konferencie Zákazník skontroluje výsledky testovania označí IBM výsledky testovania, ktorých sa má pomoc týkať. Služba Assessment Review sa bude považovať za dokončenú po uskutočnení tejto webovej konferencie.

c. **Scan for Me** [vyžaduje štyri (4) jednotky Nasadenia]

Služba Scan for Me zahŕňa služby odborníka IBM na zabezpečenie aplikácií, ktorý nakonfiguruje a spustí kontrolu, posúdi výsledky a uskutoční poradu k výsledkom s cieľom informovať o nálezoch. Zákazník umožní konzultantovi z IBM prístup k prostrediu ASoC za účelom konfigurácie a spustenia kontroly, posúdenia výsledkov, poskytnutia odporúčaní k stanoveniu priority riešenia zistených problémov a uskutočnenia porady s cieľom informovať o výsledkoch. IBM usporiada webovú konferenciu s trvaním maximálne jednu (1) hodinu pre maximálne dvoch (2) aktívnych účastníkov, v rámci ktorej poskytne základné informácie o zistených bezpečnostných nedostatkoch a o celkových bezpečnostných rizikách aplikácie, ako aj priestor na podrobnú diskusiu o zistených bezpečnostných nedostatkoch aplikácie vrátane informácií (1) o spôsobe testovania bezpečnostných nedostatkov, (2) o tom, ako boli odhalené tieto bezpečnostné nedostatky, (3) o rizikovosť jednotlivých bezpečnostných nedostatkov a (4) o všeobecných odporúčaniach k riešeniu týchto bezpečnostných nedostatkov. Ak to bude potrebné a do 30 dní po úvodnej kontrole IBM zabezpečí opätovnú kontrolu s použitím konfigurácie pôvodnej kontroly, a to výhradne s cieľom overiť nápravu bezpečnostných nedostatkov, nie testovať nové funkcie a poskytne posudok k výsledkom a výslednú správu Zákazníkovi. Služba Scan for Me sa bude považovať za dokončenú po skončení webovej konferencie uskutočnenej s cieľom poskytnúť posudok k výsledkom prvej kontroly alebo, ak sa uskutoční opätovná kontrola, po skončení opätovnej kontroly na žiadosť Zákazníka a poskytnutí správy o opätovnej kontrole Zákazníkovi.

d. **Advisor on Demand** [vyžaduje sedem (7) jednotiek Nasadenia]

Služba Advisor on Demand poskytuje maximálne dvadsať (20) hodín poradenstva zo strany konzultanta z IBM, ktoré môže Zákazník využiť pri aktivitách súvisiacich so službou IBM SaaS. Konzultant z IBM poskytne Zákazníkovi pomoc s otázkami týkajúcimi sa zabezpečenia aplikácií vrátane, ale bez obmedzenia na, správy programov, priority testovania zabezpečenia, stratégií riešenia problémov, analýzy zdrojového kódu a opravy zdrojového kódu. IBM poskytne Zákazníkovi potrebnú súčinnosť s cieľom vysvetliť a pomôcť pri vytváraní projektového plánu v súlade s požiadavkami Zákazníka vrátane cieľov projektu, relevantných technológií, požadovaného časového harmonogramu, očakávaných výstupov a odhadovaného počtu nasadení služby Advisor on Demand. Zákazník musí poskytnúť prístup k príslušným aplikáciám, systémom a dokumentácii potrebným pri poskytovaní služieb. Služba Advisor on Demand sa bude považovať za dokončenú po uplynutí 20 hodín poskytovania poradenstva v oblasti zabezpečenia alebo po poskytnutí projektového plánu alebo zdokumentovaných výstupov definovaných v projektovom pláne Zákazníkovi.

e. **Testovanie možnosti prieniku do aplikácie**

K dispozícii sú tri možnosti:

(1) **Compliance/Entry-Level Application Penetration Test**, ktorý zahrňuje maximálne štyridsať (40) hodín poradenstva a zameriava sa na chyby v jednokrokovej logike a jednoduchšie verzie chýb vkladania. Vyžaduje pätnásť (15) jednotiek Nasadenia.

(2) **Standard Application Penetration Test**, ktorý zahrňuje maximálne šesťdesiat (60) hodín poradenstva a rozširuje zameranie o chyby v logike viackrokových pracovných tokov, zložitejšie verzie chýb vkladania a analýzu komplexných typov údajov. Vyžaduje dvadsaťjeden (21) jednotiek Nasadenia.

(3) **Advanced Application Penetration Test**, ktorý zahrňuje maximálne osemdesiat (80) hodín poradenstva a rozširuje zameranie o techniky spätného inžinierstva skompilovaných spustiteľných súborov, rozbor vlastných sieťových protokolov a hĺbkovú analýzu verejne dostupných knižníc a rámcov. Vyžaduje dvadsaťsedem (27) jednotiek Nasadenia.

Služba testovania možnosti prieniku do aplikácie zahŕňa testovanie zneužiteľnosti aplikácie zo strany IBM, poskytnutie správy z testovania a poradu k zisteniam a súvisiacim rizikám.

IBM usporiada konferenčný hovor k zahájeniu projektu s maximálnym trvaním jedna (1) hodina pre dvoch (2) aktívnych účastníkov s cieľom posúdiť prostredie a organizáciu Zákazníka, a to vrátane aplikačnej platformy, architektúry, rámcov, podpornej infraštruktúry, známych problémov so zabezpečením alebo obáv súvisiacich s aplikáciou, vytvoriť predbežný plán testovania a plán núdzového kontaktovania.

IBM vykoná testovanie možnosti prieniku do aplikácie vrátane, ale bez obmedzenia na: identifikácie bežných bezpečnostných nedostatkov, ako sú vkladanie kódu SQL (SQL injection) a XSS (cross-site scripting), hodnotenia silných a slabých stránok existujúcich bezpečnostných mechanizmov, ako sú overovanie vstupu, autentifikácia a autorizácia, kontroly správneho uplatňovania podnikovej logiky, overenia správnosti použitia zabezpečených protokolov, identifikácie chýb v riadení relácií a overenia vhodnosti bezpečnostných mechanizmov pri prihlásení a obnove hesla, v zásadách pre heslá a v iných funkciách správy užívateľov. Zistenia budú uvedené v Správe z testovania z možnosti prieniku do aplikácie. IBM uskutoční webovú konferenciu k správe s trvaním maximálne jedna (1) hodina. Služba testovania možnosti prieniku do aplikácie sa bude považovať za dokončenú po využití priradeného času poradenstva, uskutočnení webovej konferencie a poskytnutí výslednej Správy z testovania možnosti prieniku do aplikácie Zákazníkovi.

1.2.1 Povinnosti súvisiace so Službami nastavenia

Spoločnosť IBM:

- poskytne Služby nastavenia na základe jednotiek Nasadenia zakúpených Zákazníkom a Potvrdenia a oprávnení
- bude Služby nastavenia považovať za poskytnuté, až keď budú splnené kritériá dokončenia uvedené v Odseku 1.2

Zákazník súhlasí s tým, že:

- bude zodpovedný za úhradu všetkých poplatkov súvisiacich so všetkými žiadosťami o Nasadenie zo strany Zákazníka počas zmluvného obdobia
- berie na vedomie, že zakúpené jednotky Nasadenia musí využiť v rámci úvodného zmluvného obdobia a k dátumu ukončenia zmluvného obdobia tieto jednotky stratia platnosť
- musí podať formálnu žiadosť o poskytnutie všetkých Služieb nastavenia najneskôr 30 dní pred dátumom skončenia predplatného

Pri poskytovaní Služieb nastavenia môže IBM od Zákazníka požadovať isté informácie a primeranú spoluprácu. Ak Zákazník bezodkladne neposkytne požadované informácie alebo spoluprácu, na základe uváženia IBM sa môžu Zákazníkovi účtovať ďalšie poplatky za jednotky Nasadenia vyžadované na základe služieb alebo môže dôjsť k oneskoreniu v poskytovaní príslušnej služby.

Aby IBM dokázala vykonať testovanie presne, Zákazník súhlasí s tým, že bude pri príprave a údržbe prostredia počas obdobia testovania postupovať podľa pokynov IBM.