IBM Application Security on Cloud

Podmínky užívání ("ToU") sestávají z těchto dokumentů IBM: podmínek užívání - Podmínek specifických pro službu IBM SaaS ("Podmínky specifické pro službu IBM SaaS") a z dokumentu nazvaného IBM podmínky užívání - Všeobecné podmínky ("Všeobecné podmínky"), které jsou dostupné na následující adrese: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

V případě rozporu mají Podmínky specifické pro službu IBM SaaS přednost před Všeobecnými podmínkami. Objednáním, přístupem nebo užíváním IBM SaaS vyjadřuje Zákazník svůj souhlas s těmito Podmínkami užívání.

Podmínky užívání se řídí podmínkami Mezinárodní smlouvy IBM Passport Advantage, Mezinárodní smlouvy IBM Passport Advantage Express nebo Mezinárodní smlouvy IBM pro vybrané služby IBM SaaS, podle toho, co je relevantní ("Smlouva"), a spolu s Podmínkami užívání tvoří úplnou smlouvu.

1. IBM SaaS

Tyto Podmínky specifické pro nabídku IBM SaaS se vztahují na následující nabídky IBM SaaS:

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

2. Metriky poplatků

IBM SaaS je prodávána na základě níže uvedených metrik poplatků, jak je uvedeno v Transakčním dokumentu:

a. **Úloha** – je měrnou jednotkou, na jejímž základě lze získat IBM SaaS. Úloha je objekt v rámci IBM SaaS, který nelze dále dělit a který představuje proces výpočetního zpracování včetně všech jeho podprocesů. Je nutné získat dostatečný počet oprávnění, který bude pokrývat celkový počet Úloh zpracovaných nebo spravovaných prostřednictvím služby IBM SaaS během období měření uvedeného v Dokumentu o oprávnění (Proof of Entitlement) Zákazníka nebo v Transakčním dokumentu.

b. **Instance aplikace** – je měrnou jednotkou, na jejímž základě lze získat IBM SaaS. Pro každou Aplikaci připojenou k IBM SaaS je vyžadováno oprávnění Instance aplikace. Pokud má Aplikace více komponent, každá z nich slouží k jinému účelu nebo jiné uživatelské základně a každá z nich může být připojena k nabídce IBM SaaS nebo může být nabídkou spravována, považuje se každá taková komponenta za samostatnou Aplikaci. Navíc testovací, vývojové, fázovací a produktivní prostředí Aplikace se považují za samostatné instance Aplikace a každé toto prostředí musí mít oprávnění. Více Instancí aplikace v jednom prostředí se považuje za samostatné instance Aplikace a oprávnění musí mít každá z nich. Je nutno získat dostatečný počet oprávnění, který bude pokrývat počet Aplikačních instancí připojených ke službě IBM SaaS během období měření uvedeného v Dokumentu o oprávnění (Proof of Entitlement) nebo v Transakčním dokumentu Zákazníka.

   Pro účely této IBM SaaS:

   - Pro Dynamické testování: web adresovatelný prostřednictvím veřejné nebo privátní adresy URL. Každá Instance aplikace poskytuje oprávnění pro web až s 1000 stránek v jediné doméně.
   - Pro Statické testování: jednotka kódu spustitelná v jednom programovacím jazyce. Každá Instance aplikace poskytuje oprávnění pro jednotky skenování s kódem do 1 000 000 řádků.
   - Pro Mobilní testování: jednotka binárního kódu, který lze spustit na mobilním zařízení. Jednotlivé odlišné mobilní platformy (např. iOS a Android) představují odlišné Instance aplikace.

c. **Instance** – je měrnou jednotkou, na jejímž základě lze získat IBM SaaS. Instance je přístup ke specifické konfiguraci IBM SaaS. Pro každou Instanci IBM SaaS zpřístupněnou a používanou během období měření uvedeného v Dokumentu o oprávnění (Proof of Entitlement) nebo v Transakčním dokumentu je nutno získat dostatečný počet oprávnění.

   Pro jednotlivá oprávnění Instance neexistuje omezení počtu prováděných Úloh ani Instancí aplikace (připojených Aplikací). Současně lze však spustit maximálně 30 Úloh.

d. **Sjednaná služba** – je měrnou jednotkou, na jejímž základě lze získat služby. Sjednaná služba sestává z odborných a/nebo ze služeb v oblasti vzdělávání vztahujících se k IBM SaaS. Je nutno získat dostatečný počet oprávnění, který bude pokrývat každou Sjednanou službu.

3. Poplatky a fakturace

Výše platby za IBM SaaS je specifikována v Transakčním dokumentu.

3.1 Poplatky za neúplný měsíc

Poplatek za neúplný měsíc uvedený v Transakčním dokumentu bude posouzen na poměrném základě.

3.2 Poplatky za překročení limitu

Pokud skutečné užívání služby IBM SaaS během období měření překročí oprávnění uvedené v Dokumentu o oprávnění (Proof of Entitlement), bude Zákazníkovi takové překročení limitu vyfakturováno v souladu s Transakčním dokumentem.

3.3 Poplatky za nastavení

Zákazníkovi budou účtovány poplatky za nastavení v souladu s Transakčním dokumentem.

4. Smluvní období a možnost obnovení

Smluvní období pro poskytování služby IBM Saas začíná datem, kdy IBM Zákazníkovi oznámí, že mu byl udělen přístup ke službě IBM SaaS, jak je uvedeno v Dokumentu o oprávnění (Proof of Entitlement). Dokument o oprávnění určí, zda se IBM SaaS obnovuje automaticky, je používána nepřetržitě, nebo zda je po uplynutí smluvního období ukončena.

V případě automatického obnovení platí, že pokud Zákazník neposkytne 30 dní před datem ukončení období písemné oznámení o záměru nabídku neobnovit, bude nabídka IBM SaaS automaticky obnovena na období uvedené v Dokumentu o oprávnění (Proof of Entitlement).

V případě průběžného používání bude nabídka IBM SaaS dále dostupná na měsíční bázi, dokud Zákazník neposkytne 30 dní předem písemnou výpověď. IBM SaaS zůstane po ukončení takového 30denního období na konci kalendářního měsíce k dispozici.

5. Technická podpora

Během Období registrace a poté, co IBM Zákazníkovi oznámí, že přístup k IBM SaaS je k dispozici, je technická podpora poskytována prostřednictvím online fór a jako standardní podpora během období, ve kterém jsou Zákazníkovi účtovány poplatky typu Pay per Use. Z IBM SaaS mohou Zákazníci odeslat tiket podpory nebo zahájit relaci konverzace a požádat o asistenci. IBM zpřístupní Software IBM jako Příručku podpory služby, která poskytuje informace o technické podpoře a další informace a procesy.

Závažnost	Definice Závažnosti	Cílové hodnoty doby odezvy	Pokrytí doby odezvy
1	**Kritický dopad na obchodní činnost/selhání služby:** Funkčnost, která je rozhodující pro obchodní činnost, není provozuschopná nebo došlo k selhání kritického rozhraní. Tato Závažnost se obvykle vztahuje na produktivní prostředí a označuje neschopnost přístupu ke službám, která má za následek kritický dopad na provoz. Tento stav vyžaduje okamžité řešení.	Do jedné hodiny	24 hodin, 7 dní v týdnu
2	**Významný dopad na obchodní činnost:** Obchodní komponenty nebo funkce služby jsou, pokud jde o jejich užívání, vážně omezeny nebo Zákazníkovi hrozí nedodržení obchodních termínů.	Do dvou hodin (v průběhu pracovní doby)	Pondělí až pátek, v průběhu pracovní doby
3	**Mírný dopad na obchodní činnost:** Službu nebo funkčnost lze používat a dopad na provoz není kritický.	Do čtyř hodin (v průběhu pracovní doby)	Pondělí až pátek, v průběhu pracovní doby
4	**Minimální dopad na obchodní činnost:** Dotaz nebo netechnický požadavek	Do jednoho pracovního dne	Pondělí až pátek, v průběhu pracovní doby

5.1 Přístup k Datům Zákazníka

IBM bude mít možnost přistupovat k datům Zákazníka pro účely diagnostiky problémů se službou a umožnění skenování aplikace Zákazníka službou. IBM bude k datům přistupovat pouze pro účely opravy vad a poskytnutí podpory pro produkty nebo služby IBM.

6. Dodatečné podmínky pro nabídku IBM SaaS

Skenování zabezpečení nemusí identifikovat všechna bezpečnostní rizika v aplikaci a ani není navrženo či určeno k použití v rizikových prostředích vyžadujících provoz odolný proti selhání, včetně - mimo jiné - letecké navigace, systémů řízení letového provozu, zbraňových systémů, přístrojů na podporu životních funkcí, jaderných zařízení nebo jiných aplikací, u kterých by neschopnost identifikovat bezpečnostní rizika mohla vést k úmrtí, zraněním nebo škodám na majetku. Není nezaručeno, že skenování zabezpečení bude fungovat nepřerušeně a bez chyb.

IBM SaaS je nástroj, který pomáhá Zákazníkovi zajistit dodržování závazků, jež pro něj mohou vyplývat z právních předpisů, zákonných a jiných standardů nebo postupů. Jakékoli instrukce, informace týkající se doporučeného užívání nebo jiné pokyny, které Zákazník získá prostřednictvím Služby, nepředstavují právní, účetní nebo jinou odbornou radu a Zákazník by si měl obstarat svou vlastní právní nebo jinou odbornou konzultaci. Zákazník nese výhradní odpovědnost za dodržování všech příslušných právních předpisů, směrnic, standardů a postupů. Totéž platí pro všechny jeho činnosti, aplikace a systémy. Užívání této Služby nezaručuje soulad s právními předpisy, nařízeními, standardy nebo postupy.

IBM SaaS provádí invazivní a neinvazivní testy na webových stránkách a webových nebo mobilních aplikacích, které se Zákazník rozhodne skenovat. Příslušné zákony zakazují jakýkoli neoprávněný pokus o proniknutí do počítačových systémů nebo pokus o přístup do počítačových systémů. Zákazník opravňuje IBM k poskytování Služeb podle popisu v tomto dokumentu a bere na vědomí, že Služby představují autorizovaný přístup k počítačovým systémům Zákazníka. IBM smí toto udělení oprávnění zveřejnit třetí osobě, pokud to považuje za nezbytné k poskytování Služeb.

Testování znamená určité riziko, včetně - nikoli však pouze - následujících rizik:

a. počítačové systémy Zákazníka se mohou během testování aplikací zablokovat nebo se mohou zhroutit, což může mít za následek dočasnou nedostupnost systému nebo ztrátu dat;

b. výkon a propustnost systémů Zákazníka a rovněž výkon a propustnost souvisejících směrovačů a ochranných bariér mohou být během testování dočasně sníženy;

c. může být generováno nadměrné množství zpráv protokolu, což může mít za následek nadměrnou spotřebu prostoru na disku pro soubory protokolu;

d. data mohou být změněna nebo vymazána v důsledku testování ohrožení zabezpečení;

e. systémy pro detekci proniknutí do systému mohou spustit alarmy;

f. e-mailová funkce testované webové aplikace může spustit e-maily;

g. služba IBM SaaS může zachytit provoz monitorované sítě pro účely hledání událostí.

Všechna práva a opravné prostředky v rámci dohod o úrovni služeb poskytnuté IBM, které se týkají webů nebo aplikací podléhajících testování, se během testování neuplatní.

V případě, že Zákazník použije ověřená přihlašovací pověření pro testovanou aplikaci do Služby, je povinen používat taková pověření pouze pro testovací účty, a nikoli pro produktivní uživatele. Použití pověření produktivních uživatelů může mít za následek přenos osobních údajů přes Službu.

IBM SaaS lze nakonfigurovat ke skenování produktivních webových aplikací. Pokud Zákazník nastaví typ skenování na "produktivní", služba bude provádět skenování způsobem, který sníží rizika uvedená výše; v některých situacích však služba IBM SaaS může způsobit snížení výkonu nebo nestabilitu testovaných produktivních webů a infrastruktury. Společnost IBM neposkytuje žádné záruky ani garance s ohledem na vhodnost použití služby IBM SaaS ke skenování produktivních webů.

ZÁKAZNÍK NESE ODPOVĚDNOST ZA URČENÍ, ZDA JE SLUŽBA VHODNÁ ČI BEZPEČNÁ PRO JEHO WEBOVÝ SEVER, WEBOVOU APLIKACI, MOBILNÍ APLIKACI NEBO TECHNICKÉ PROSTŘEDÍ.

IBM SaaS je určena k identifikaci širokého spektra potenciálních problémů týkajících se zabezpečení a dodržování právních předpisů v oblasti mobilních a webových aplikací a služeb. Netestuje všechna ohrožení zabezpečení nebo všechna rizika v oblasti dodržování právních předpisů, ani nefunguje jako bariéra proti útokům na zabezpečení. Bezpečnostní rizika, regulace a standardy se průběžně mění a Služba nemůže všechny takové změny zohledňovat. Zákazník odpovídá za zabezpečení svých

webových aplikací, systémů a zaměstnanců a za dodržování právních předpisů a rovněž za jakékoli nápravné akce samostatně. Záleží výhradně na uvážení Zákazníka, zda bude, či nebude využívat jakékoli informace poskytnuté Službou.

Příslušné zákony zakazují jakýkoli neoprávněný pokus o proniknutí do počítačových systémů nebo pokus o přístup do počítačových systémů. ZÁKAZNÍK JE POVINEN ZAJISTIT, ABY SLUŽBA NEBYLA POUŽÍVÁNA KE SKENOVÁNÍ JAKÝCHKOLI JINÝCH WEBOVÝCH SERVERŮ A/NEBO APLIKACÍ, NEŽ JSOU WEBOVÉ SERVERY A/NEBO APLIKACE VE VLASTNICTVÍ ZÁKAZNÍKA NEBO WEBOVÉ SERVERY A/NEBO APLIKACE, K JEJICHŽ SKENOVÁNÍ MÁ ZÁKAZNÍK OPRÁVNĚNÍ.

Pro účely vyjasnění platí, že Obsah zákazníka popsaný v části věnované ochraně údajů dokumentu IBM podmínky užívání - Všeobecné podmínky obsahuje také data, ke kterým může IBM během Testování průniku aplikace získat přístup.

6.1 Systémy ve vlastnictví třetí osoby

V případě systémů (které pro účely tohoto ustanovení zahrnují například aplikace a adresy IP) ve vlastnictví třetí osoby, na kterých bude v souladu s tímto dokumentem provedeno testování, Zákazník souhlasí, že:

a. před tím, než IBM zahájí úvodní testování na systému třetí osoby, získá Zákazník od vlastníka každého systému podepsaný dopis, který IBM opravňuje k poskytování Služeb v daném systému a který bude obsahovat přijetí podmínek uvedených v části "Souhlas s provedením testování" ze strany tohoto vlastníka, a Zákazník poskytne IBM kopii takového oprávnění.

b. ponese výhradní odpovědnost za oznámení veškerých rizik, vystavení a ohrožení identifikovaných v těchto systémech během vzdáleného testování IBM vlastníkovi systému; a

c. umožní a bude podporovat výměnu informací mezi vlastníkem systému a IBM jak bude IBM považovat za nezbytné.

Zákazník souhlasí, že:

- bude IBM neprodleně informovat, pokud dojde ke změně vlastnictví systému, na kterém v souladu s tímto dokumentem probíhá testování;
- nezveřejní předměty plnění ani skutečnost, že IBM poskytla Služby, mimo Podnik Zákazníka bez předchozího písemného souhlasu IBM; a
- IBM v plném rozsahu odškodní v případě ztrát nebo odpovědností, které IBM vzniknou v důsledku nároků třetí osoby vyplývajících ze skutečnosti, že Zákazník nesplnil požadavky uvedené v tomto oddílu s názvem "Systémy ve vlastnictví třetí osoby", a v případě všech předvolání a nároků třetí osoby vznesených vůči IBM nebo jejím subdodavatelům či zástupcům, které vyplývají z (a) testování bezpečnostních rizik, vystavení nebo ohrožení systémů, na kterých probíhá testování podle tohoto dokumentu, (b) poskytnutí výsledků takového testování Zákazníkovi nebo (c) Zákazníkova používání nebo zveřejnění takových výsledků.

6.2 Soubory cookie

Zákazník si je vědom a souhlasí, že IBM smí v rámci své běžné činnosti a podpory služeb IBM SaaS od Zákazníka (zaměstnanců a smluvních partnerů Zákazníka) shromažďovat osobní údaje týkající se užívání služeb IBM SaaS prostřednictvím sledovacích a jiných technologií. IBM tak činí za účelem získání statistik užívání a informací o efektivitě služeb IBM SaaS, které IBM umožní zlepšit zkušenosti uživatelů nebo přizpůsobit interakce se Zákazníkem na míru. Zákazník potvrzuje, že získá nebo získal souhlas, který IBM uděluje oprávnění zpracovávat, v souladu s příslušnými právními předpisy, shromážděné osobní údaje pro výše uvedené účely v rámci IBM, jiných společností IBM a jejích subdodavatelů, kdekoli IBM a její subdodavatelé provádějí obchodní činnost. IBM vyhoví požadavkům zaměstnanců a smluvních partnerů Zákazníka, pokud jde o přístup, aktualizaci, opravu nebo vymazání jejich shromážděných osobních údajů.

V rámci služby IBM SaaS, která zahrnuje činnosti vytváření sestav, bude IBM připravovat a uchovávat neidentifikované a/nebo agregované informace shromážděné ze služby IBM Saas ("Data zabezpečení"). S výjimkou ustanovení (d) níže nebudou Data zabezpečení identifikovat Zákazníka ani jiné osoby. Zákazník dále vyjadřuje souhlas s tím, že IBM je oprávněna používat a/nebo kopírovat Data zabezpečení pouze k následujícím účelům:

a. publikování a/nebo distribuce Dat zabezpečení (např. v kompilacích a/nebo analýzách týkajících se kybernetické bezpečnosti);

b. vývoj a vylepšení produktů nebo služeb;

c. interní výzkum nebo výzkum realizovaný se třetími osobami; a

d. sdílení informací o potvrzeném pachatelovi, který je třetí osobou, v souladu se zákonem.

6.3 Lokality, v nichž jsou využívány výhody

V případech, kdy je to relevantní, budou daně založeny na lokalitě(ách), kterou(é) Zákazník uvedl jako místo, kde využívá výhod služeb IBM SaaS. IBM uplatní daně na základě obchodní adresy, která byla při objednání služby IBM SaaS uvedena jako primární lokalita pro využívání výhod, pokud Zákazník IBM neposkytne doplňující informace. Zákazník nese odpovědnost za aktualizaci takových informací a za informování IBM o jakýchkoli změnách.

6.4 Osobní údaje a regulovaný obsah a služby

Tato služba IBM SaaS není navržena pro jakékoli specifické požadavky na zabezpečení regulovaného obsahu, jako například osobních údajů nebo citlivých osobních údajů. Zákazník je odpovědný za určení toho, zda IBM SaaS vyhovuje potřebám Zákazníka s ohledem na typ obsahu, který Zákazník ve spojitosti s IBM SaaS používá.

IBM není poskytovatelem služeb regulovaných Federální komunikační komisí (Federal Communications Commission,"FCC") nebo státními regulačními orgány ("Státní regulační orgány") a služby, které jsou komisí FCC nebo Státními regulačními orgány regulovány, nezamýšlí poskytovat. Pokud FCC nebo Státní regulační orgán uvalí na služby poskytované IBM podle tohoto dokumentu regulatorní požadavky nebo povinnosti, je IBM oprávněna: (a) změnit, vyměnit nebo nahradit produkty na náklady Zákazníka a/nebo (b) změnit způsob poskytování služeb Zákazníkovi, aby se takové požadavky či povinnosti na IBM nevztahovaly (například tak, že IBM bude vystupovat jako zástupce Zákazníka při získávání takových služeb od společného poskytovatele, který je třetí osobou).

Příloha A

1. Všeobecný popis služby IBM Application Security on Cloud

IBM Application Security on Cloud je místem, které Zákazníkovi poskytuje asistenci s identifikací zranitelných míst v zabezpečení (jako například SQL injection, cross-site scripting nebo únik dat) pro řadu aplikací. Služba zahrnuje řadu různých typů a technik skenování zabezpečení aplikace identifikujících problémy se zabezpečením dané aplikace.

IBM Application Security on Cloud poskytuje následující funkce:

- Skenování mobilních aplikací z hlediska zranitelných míst v zabezpečení. Skenování probíhá prostřednictvím dynamických (blackbox) a interaktivních (glassbox) technologií analýzy zabezpečení.
- Skenování produktivních a preprodukčních webových serverů ve veřejné nebo soukromé síti z hlediska ohrožení zabezpečení. Skenování probíhá prostřednictvím dynamických (blackbox) technik analýzy zabezpečení.
- Skenování datových toků webových a desktop aplikací z hlediska zranitelných míst v zabezpečení. Skenování probíhá prostřednictvím statických (whitebox) technik analýzy zabezpečení.
- Podrobné sestavy týkající se zranitelných míst v zabezpečení, které zahrnují souhrny zjištění a kroky k nápravě, podle kterých mohou vývojáři postupovat.
- Integrace s různými platformami DevOps.

1.1 IBM Application Analyzer

Službu IBM Application Analyzer lze objednat na Instanci aplikace, na Úlohu (skenování) nebo jako plnou Instanci a umožňuje následující typy skenování:

- Dynamic Analyzer – testování předprodukčních nebo produktivních webů za použití technik DAST
- Mobile Analyzer – testování binárních dat systému iOS nebo Android za použití technik IAST
- Static Analyzer – testování toku bajtů nebo dat zdrojového kódu za použití technik SAST

1.2 Služba nastavení

IBM Application Security on Cloud Consulting Services je služba nastavení pro Application Analyzer určená pro produktivní režim. Služba prostřednictvím konzultantů IBM poskytuje poradenství a asistenci při testování a správě rizik aplikace. Služby IBM Application Security on Cloud Consulting Services se kupují ve formě bloků Sjednaných služeb, které je možné rozšířit v množstvím uvedeném níže, a požádat tak o níže uvedené specifické služby k užívání.

a. **Fast Start** [využívá jednu (1) jednotku Sjednané služby]

Služba Fast Start poskytuje odborné informace a poradenství k používání funkcí pro testování a správu rizik Application Security on Cloud. Jakmile Zákazník potvrdí úspěšné přihlášení na portále Application Security on Cloud, IBM zorganizuje webovou konferenci v délce maximálně dvě (2) hodiny pro dva (2) aktivní účastníky, jejímž cílem je poskytnout informace o základních konfiguracích a funkcích AppSec na IBM SaaS, včetně typů skenování, spouštění skenování, kontroly sestav a instalace souvisejících nástrojů a modulů plug-in. Služba Fast Start je dokončena po dokončení (a) vzdělávacího webináře Zákazníka, (b) instalace příslušných nástrojů a modulů plug-in a (c) asistence Zákazníkovi při nastavení a spuštění prvního skenování.

b. **Assessment Review** [využívá dvě (2) jednotky Sjednané služby]

Služba Assessment Review poskytuje asistenci při kontrole výsledku testu, včetně pochopení a stanovení priorit při nápravě ohrožení aplikace. IBM zorganizuje webovou konferenci v délce maximálně jedné (1) hodiny pro dva (2) aktivní účastníky, jejímž cílem je poskytnout přehled zjištěného ohrožení a celkového rizika zabezpečení aplikace a umožnit podrobnou diskusi o zjištěném ohrožení zabezpečení aplikace, včetně (1) způsobu testování ohrožení, (2) způsobu zjištění ohrožení, (3) rizika plynoucího z jednotlivých ohrožení a (4) poskytnutí obecných doporučení k odstranění ohrožení. Kontrola bude založena výhradně na výsledku testu a nebude se jednat o posouzení samotného zdrojového kódu. Zákazník si před webovou konferencí prostuduje výsledek

testu a určí pro IBM výsledek ke kontrole. Poskytování služby Assessment Review je dokončeno po ukončení webové konference.

c. **Scan for Me** [využívá čtyři (4) jednotky Sjednané služby]

Služba Scan for Me poskytuje služby odborníka na zabezpečení aplikací IBM, který nakonfiguruje a spustí skenování, ověří výsledky a uskuteční informativní schůzku ohledně sestavy pro vyhodnocení zjištění. Zákazník umožní konzultantovi IBM přístup do svého prostředí ASoC ke konfiguraci a spuštění skenování, ověření výsledků, poskytnutí doporučení ke stanovení priorit nápravných kroků a uskutečnění informativní schůzku ohledně sestavy výsledků. IBM zorganizuje webovou konferenci v délce maximálně jedné (1) hodiny pro dva (2) aktivní účastníky, jejímž cílem je poskytnout přehled zjištěného ohrožení a celkového rizika zabezpečení aplikace a umožnit podrobnou diskusi o zjištěném ohrožení zabezpečení aplikace, včetně (1) způsobu testování ohrožení, (2) způsobu zjištění ohrožení, (3) rizika plynoucího z jednotlivých ohrožení a (4) poskytnutí obecných doporučení k odstranění ohrožení. Na vyžádání provede společnost IBM nejpozději 30 dní po prvním skenování opakované skenování za použití konfigurace původního skenování, a to pouze k ověření oprav zabezpečení, nikoli za účelem testování funkcí, ověření výsledků a dodání zprávy Zákazníkovi. Poskytování služby Scan for Me je ukončeno po dokončení webové konference, během které byly revidovány výsledky prvního skenování, nebo (je-li relevantní) po dokončení opakovaného skenování vyžádaného Zákazníkem a dodání zprávy o takovém opakovaném skenování Zákazníkovi.

d. **Advisor on Demand** [využívá sedm (7) jednotek Sjednané služby]

Služba Advisor on Demand poskytuje až dvacet (20) hodin času konzultanta IBM, které lze využít pro činnosti související s IBM SaaS. Konzultant IBM poskytne asistenci s tématy týkajícími se zabezpečení aplikací, včetně - nikoli však pouze - správy programů, stanovení priorit testování zabezpečení, strategií nápravy, analýzy zdrojového kódu a opravy zdrojového kódu. IBM ve spolupráci se Zákazníkem vytvoří harmonogram projektu s konkrétními požadavky Zákazníka, včetně cílů projektu, relevantních technologií, požadovaných časových os, očekávaných předmětů plnění a odhadovaného počtu sjednaných služeb Advisor on Demand. Zákazník musí poskytnout přístup k nezbytným aplikacím, systémům a dokumentaci vyžadovaným k poskytování služeb. Poskytování služby Advisor on Demand je ukončeno po využití maximálně 20 hodin odborného poradenství týkajícího se zabezpečení a/nebo po doručení harmonogramu projektu a/nebo zdokumentovaných předmětů plnění definovaných v harmonogramu projektu Zákazníkovi.

e. **Testování průniku aplikace**

Tři volby:

(1) **Test průniku aplikace týkající se splnění předpisů / vstupní úrovně**, který zahrnuje až čtyřicet (40) hodin času Konzultanta a zaměřuje se na chyby logiky o jednom kroku nebo jednodušší verze chyb vkládání. Využívá patnáct (15) jednotek Sjednané služby.

(2) **Standardní test průniku aplikace**, který zahrnuje až šedesát (60) hodin času Konzultanta a zahrnuje chyby logiky v pracovních postupech s více kroky, složité verze chyb vkládání a analýzu složitých datových typů. Využívá dvacet jedna (21) jednotek Sjednané služby.

(3) **Rozšířený test průniku aplikace**, který zahrnuje až osmdesát (80) hodin času Konzultanta a zahrnuje zpětný engineering kompilovaných spustitelných souborů, rozkládání vlastních síťových protokolů, detailní analýzu veřejně dostupných knihoven a prostředí. Využívá dvacet sedm (27) jednotek Sjednané služby.

Služba testování průniku aplikace poskytuje pracovníka IBM k provedení testování a využití aplikace, doručení zprávy o testu a informativní schůzku týkající se zprávy za účelem vysvětlení zjištění a souvisejících rizik.

IBM zorganizuje hovor k zahájení projektu v délce až jedné (1) hodiny pro dva (2) aktivní účastníky s cílem posoudit prostředí a organizaci Zákazníka, včetně aplikační platformy, architektury, rámců, prostředí, podpůrné infrastruktury, známých problémů zabezpečení či záležitostí týkajících se aplikace, předběžného harmonogramu testování a plánu pro kontaktování v nouzových situacích.

IBM provede testování průniku aplikace včetně - nikoli však pouze: identifikace běžného ohrožení, například zadávání SQL a skriptování na více webů, posouzení silných a slabých stránek stávajícího řízení zabezpečení, například validace vstupu, ověření a autorizace, kontroly správného vynucení obchodní logiky, validace správného používání zabezpečených protokolů, identifikace problémů se zpracováním chyb a ověření správného řízení zabezpečení při přihlášení, obnovení

hesla, zásad hesla a dalších funkcí správy uživatelů. Zjištění budou zdokumentována ve zprávě z testu průniku aplikace. IBM zorganizuje webovou konferenci za účelem projednání zprávy v délce maximálně jedné (1) hodiny. Poskytování služby Testu průniku aplikace je ukončeno po využití přiděleného času ke konzultacím, uspořádání webové konference a doručení závěrečné zprávy z testu průniku aplikace Zákazníkovi.

1.2.1 Povinnosti týkající se Služeb nastavení

IBM:

- bude poskytovat Služby nastavení za použití jednotek Sjednané služby zakoupených Zákazníkem a v souladu s Dokumentem o oprávnění (Proof of Entitlement); a
- ukončí poskytování Služby nastavení po splnění kritérií dokončení popsaných v Oddíle 1.2.

Zákazník souhlasí, že:

- ponese odpovědnost za všechny poplatky související se všemi požadavky Sjednané služby vznesenými Zákazníkem během doby trvání smlouvy;
- bere na vědomí, že zakoupené jednotky Sjednané služby je nutné využít během počátečního smluvního období a jejich platnost vyprší, pokud nebudou využity do data ukončení smluvního období; a
- všechny formální požadavky pro všechny Služby nastavení vznese minimálně 30 dní před datem ukončení registrace.

Během poskytování jakékoliv Služby nastavení smí IBM Zákazníka požádat o poskytnutí informací a přiměřené součinnosti. Pokud Zákazník požadované informace nebo součinnost neposkytne včas, je IBM dle svého uvážení oprávněna účtovat poplatky za jednotky Sjednané služby požadované službami nebo může dojít k prodlení v poskytování příslušných služeb.

Aby mohla IBM provést testování přesně, Zákazník se zavazuje, že při přípravě a správě prostředí bude po dobu testování dodržovat pokyny IBM.