IBM Application Security on Cloud

Uvjeti upotrebe ("ToU") sastoje se od ovih IBM-ovih Uvjeta upotrebe – Uvjeti za određene SaaS ponude ("Uvjeti za određene SaaS ponude") i dokumenta nazvanog IBM-ovi Uvjeti upotrebe – Opći uvjeti ("Opći uvjeti") dostupnom na sljedećem URL-u: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

U slučaju sukoba, SaaS Uvjeti za određene SaaS ponude imaju prednost pred Općim uvjetima. Naručivanjem, pristupanjem ili korištenjem IBM SaaS-a Klijent prihvaća Uvjete upotrebe (ToU).

Uvjete upotrebe (ToU) uređuje IBM Međunarodni Passport Advantage ugovor, IBM Međunarodni Passport Advantage Express ugovor ili IBM Međunarodni ugovor za Izabrane IBM SaaS ponude, ovisno što se primjenjuje ("Ugovor"), koji zajedno s Uvjetima upotrebe čine cjeloviti ugovor.

1. IBM SaaS

Ovi Uvjeti za određene SaaS ponude odnose se na sljedeće IBM SaaS ponude:

- IBM Application Security Analyzer
- IBM Application Security on Cloud - usluge savjetovanja

2. Metrike naplate

IBM SaaS se prodaje u skladu sa sljedećim metrikama naplate navedenim u Transakcijskom dokumentu:

a. **Posao** - je jedinica mjere po kojoj se može dobiti IBM SaaS. Posao je objekt unutar IBM SaaS-a koji se ne može dalje podijeliti i predstavlja računalni proces sa svim njegovim podprocesima. Moraju se dobiti ovlaštenja koja su dostatna za pokrivanje ukupnog broja Poslova obrađenih u IBM SaaS-u ili kojima IBM SaaS upravlja za vrijeme perioda mjerenja navedenog u Klijentovom Dokazu o ovlaštenju (Proof of Entitlement - PoE) ili Transakcijskom dokumentu.

b. **Instanca aplikacije** – je jedinica mjere po kojoj se može dobiti IBM SaaS. Ovlaštenje Instance aplikacije je potrebno za svaku instancu Aplikacije koja je povezana na IBM SaaS. Ako Aplikacija ima više komponenti, pri čemu svaka ima posebnu svrhu i od kojih svaka može biti povezana ili upravljana od IBM SaaS-a, svaka takva komponenta se smatra zasebnom Aplikacijom. Dodatno, testna, razvojna, postavljačka i proizvodna okolina za Aplikaciju se svaka smatra zasebnom instancom Aplikacije i svaka mora imati ovlaštenje. Ako postoji više Instanci Aplikacije u jednoj okolini, svaka se smatra zasebnom instancom Aplikacije i za svaku je potrebno ovlaštenje. Moraju se dobiti Ovlaštenja koja su dostatna za pokrivanje broja Instanci aplikacije povezanih s IBM SaaS-om za vrijeme perioda mjerenja navedenog u Klijentovom PoE-u ili Transakcijskom dokumentu.

   Za potrebe ovog IBM SaaS-a:

   - Za dinamičko testiranje: web stranica koja se može adresirati putem javnog ili privatnog URL-a. Svaka Instanca aplikacije pruža ovlaštenje za web stranicu koja sadrži do 1000 stranica u jednoj domeni.
   - Za statičko testiranje: jedinica koda koja se izvodi u jednom programskom jeziku. Svaka Instanca aplikacije pruža ovlaštenje za skeniranje jedinica koda koje sadrže do 1 000 000 redova.
   - Za mobilno testiranje: jedinica binarnog koda koja se može izvesti na prijenosnom uređaju. Svaka mobilna platforma (na primjer iOS i Android) predstavlja različite Instance aplikacije.

c. **Instanca** - je jedinica mjere po kojoj se može dobiti IBM SaaS. Instanca označava pristup određenoj konfiguraciji IBM SaaS-a. Moraju se dobiti dostatna ovlaštenja za svaku instancu IBM SaaS-a koja je dostupna za pristup i korištenje tijekom perioda mjerenja navedenog u Klijentovom Dokazu o ovlaštenju (Proof of Entitlement - PoE) ili Transakcijskom dokumentu.

   Za ovlaštenja Instance ne postoji ograničenje broja izvedenih Poslova ili Instanci Aplikacije (povezanih Aplikacija), uz uvjet da se istovremeno ne može izvoditi više od 30 Poslova.

d. **Angažman** - je jedinica mjere po kojoj se mogu dobiti usluge. Angažman se sastoji od profesionalnih usluga i/ili usluga izobrazbe vezanih uz IBM SaaS. Moraju se dobiti ovlaštenja koja su dostatna za pokrivanje svakog Angažmana.

3. Naknade i naplata

Iznos koji se plaća za IBM SaaS naveden je u transakcijskom dokumentu.

3.1 Djelomične mjesečne naknade

Na temelju razmjerne procjene može se izračunati djelomična mjesečna naknada, kako je navedeno u Transakcijskom dokumentu.

3.2 Naknade za prekomjernu upotrebu

Ako Klijentova stvarna upotreba IBM SaaS-a za vrijeme perioda mjerenja premašuje Klijentovo ovlaštenje navedeno u PoE-u, Klijentu će se naplatiti prekomjerni iznos, kako je navedeno u Transakcijskom dokumentu.

3.3 Naknade za postavljanje

Klijentu će se naplatiti postavljanje, kao što je navedeno u Transakcijskom dokumentu.

4. Opcije trajanja i obnavljanja

Trajanje IBM SaaS-a počinje na datum kada IBM obavijesti Klijenta o njegovom pristupu IBM SaaS-u, kako je dokumentirano u PoE-u. PoE će određivati obnavlja li se IBM SaaS automatski, nastavlja li se na temelju kontinuirane upotrebe ili se raskida na kraju trajanja.

Za automatsko obnavljanje, ako Klijent ne dostavi pisanu obavijest o neobnavljanju barem 30 dana prije datuma isteka, IBM SaaS će se automatski obnoviti u trajanju navedenom u PoE-u.

Kod kontinuirane upotrebe, IBM SaaS će biti dostupan na mjesečnoj bazi dok Klijent ne dostavi pisanu obavijest o raskidu 30 dana unaprijed. IBM SaaS će biti dostupan do kraja kalendarskog mjeseca nakon takvog perioda od 30 dana.

5. Tehnička podrška

Za vrijeme Perioda pretplate i nakon što IBM obavijesti Klijenta da mu je dostupan pristup na IBM SaaS, pruža se tehnička podrška za IBM SaaS putem online foruma i standardna podrška tijekom perioda u kojem je Klijent izložen Naplati po upotrebi. Klijenti mogu unutar IBM SaaS-a predati prijavu podrške ili otvoriti sesiju chata u kojoj će zatražiti pomoć. IBM će pružiti Priručnik za podršku za IBM Software as a Service koji sadrži informacije o kontaktiranju tehničke podrške i druge informacije i procese.

Ozbiljnost	Definicija ozbiljnosti	Ciljana vremena odgovora	Pokrivenost za vremena odgovora
1	**Kritičan utjecaj na poslovanje/prekid rada usluge:** Funkcionalnost kritična za poslovanje ne radi ili se dogodila greška sučelja od kritične važnosti. Ovo se obično odnosi na proizvodnu okolinu i označava da se ne može pristupiti uslugama, što ima kritičan utjecaj na operacije. Ovo stanje mora se odmah riješiti.	Unutar jednog sata	24x7
2	**Značajan utjecaj na poslovanje:** Poslovna komponenta ili funkcija usluge ima ozbiljno smanjenu mogućnost upotrebe ili se pojavila opasnost da Klijent prekorači krajnje rokove u poslovanju.	Unutar 2 radna sata	Radno vrijeme od ponedjeljka do petka
3	**Manji utjecaj na poslovanje:** Označava da je usluga ili funkcionalnost upotrebljiva i nema kritičan utjecaj na operacije.	Unutar 4 radna sata	Radno vrijeme od ponedjeljka do petka
4	**Minimalan utjecaj na poslovanje:** Upit ili zahtjev koji se ne odnosi na tehnički problem	Unutar 1 radnog dana	Radno vrijeme od ponedjeljka do petka

5.1 Pristup podacima Klijenta

IBM će moći pristupiti Klijentovim podacima u svrhu dijagnosticiranja problema s uslugom i omogućavanja skeniranja Klijentove aplikacije od strane usluge. IBM će pristupiti podacima samo u svrhu popravljanja oštećenja ili za davanje podrške za IBM proizvode ili usluge.

6. Dodatni uvjeti za IBM SaaS ponude

Sigurnosna skeniranja možda neće otkriti sve sigurnosne rizike u aplikaciji i nisu dizajnirana ili namijenjena za korištenje u opasnim okolinama koje zahtijevaju povratak u sigurno stanje nakon greške, uključujući, ali ne ograničavajući se na sustave kontrole zračnog prometa, oružane sustave, sustave za održavanje života, nuklearna postrojenja ili bilo koje druge primjene u kojima bi neutvrđivanje sigurnosnih rizika moglo uzrokovati smrt, tjelesnu ozljedu ili materijalnu štetu. Sigurnosna skeniranja ne jamče rad bez prekida ili bez grešaka.

IBM SaaS može se koristiti kao pomoć Klijentu kod ispunjavanja obveza usklađenosti, koje mogu biti bazirane na zakonima, pravilima, standardima ili praksi. Bilo koje upute, predložena upotreba ili smjernice dobivene od Usluge ne smatraju se pravnim, računovodstvenim ili drugim profesionalnim savjetima i Klijenta se upozorava da potraži vlastito pravno ili drugo profesionalno savjetovanje. Klijent je isključivo odgovoran za osiguravanje da Klijent i Klijentove aktivnosti, aplikacije i sustavi poštuju sve mjerodavne propise, pravila, standarde i prakse koji se primjenjuju. Upotreba ove Usluge ne garantira usklađenost s bilo kojim propisom, pravilom, standardom ili praksom.

IBM SaaS izvodi invazivna i neinvazivna testiranja web stranice i web ili mobilne aplikacije koju Klijent odluči skenirati. Određeni propisi zabranjuju bilo kakve neovlaštene pokušaje probijanja ili pristupanja računalnim sustavima. Klijent ovlašćuje IBM za izvođenje Usluga kako je opisano ovdje i prihvaća da Usluge podrazumijevaju ovlašteni pristup Klijentovim računalnim sustavima. IBM može objaviti ovu dodjelu ovlaštenja trećoj strani ako je to potrebno za izvođenje Usluga.

Testiranja uključuju određene rizike, uključujući, ali ne ograničavajući se na sljedeće:

a. tijekom izvođenja aplikacija za vrijeme testiranja, Klijentovi računalni sustavi mogu prestati reagirati ili se srušiti, što rezultira privremenom nedostupnošću sustava ili gubitkom podataka;

b. performanse i propusnost Klijentovih sustava i performanse i propusnost povezanih usmjerivača i vatrozida mogu biti privremeno sniženi za vrijeme testiranja;

c. mogu se generirati ogromne količine poruka dnevnika, što rezultira prekomjernom potrošnjom prostora na disku od strane datoteke dnevnika;

d. podaci mogu biti promijenjeni ili izbrisani u sklopu istraživanja ranjivosti;

e. mogu se aktivirati alarmi ili sustavi za otkrivanje upada;

f. funkcija e-pošte u aplikaciji koja se testira može aktivirati slanje e-pošte;

g. IBM SaaS može presretati promet na nadgledanoj mreži u svrhu traženja događaja.

Tijekom bilo kakve aktivnosti testiranja odbacuju se bilo koja prava ili pravna sredstva ugovora o razini usluge koji pruža IBM koja se odnose na web stranice ili aplikacije koje su predmet testiranja.

U slučaju da Klijent unosi ovlaštene pristupne podatke za prijavu u aplikaciju koja se testira u Usluzi, Klijent bi trebao unositi takve pristupne podatke samo za testne račune, a ne za proizvodne korisnike. Upotreba pristupnih podataka proizvodnog korisnika može rezultirati prijenosom osobnih podataka preko Usluge.

IBM SaaS se može konfigurirati za skeniranje proizvodnih web aplikacija. Kada Klijent za tip skeniranja postavi "proizvodnja", usluga se dizajnira za izvođenje skeniranja na način koji će smanjiti rizike navedene iznad; međutim, u određenim situacijama IBM SaaS može uzrokovati snižene performanse ili nestabilnost unutar testiranih proizvodnih lokacija i infrastrukture. IBM ne daje nikakva jamstva ili izjave vezano uz održivost korištenja IBM Saas za skeniranje proizvodnih lokacija.

KLIJENT JE ODGOVORAN UTVRDITI DA LI JE USLUGA PRIKLADNA ILI SIGURNA ZA KLIJENTOVU WEB STRANICU, WEB APLIKACIJU, MOBILNU APLIKACIJU ILI TEHNIČKU OKOLINU.

IBM SaaS dizajniran je za otkrivanje raznovrsnih potencijalnih problema vezanih uz sigurnost i usklađenost u mobilnim i web aplikacijama i web uslugama. Ne testira sve propuste ili rizike vezane uz usklađenost niti ne predstavlja prepreku za sigurnosne napade. Sigurnosne prijetnje, propisi i standardi konstantno se mijenjaju i Usluga možda neće odražavati sve takve promjene. Klijent je isključivo odgovoran za sigurnost i usklađenost Klijentove web aplikacije, sustava i zaposlenika i radnje koje se poduzimaju za ispravljanje problema. Isključivo je Klijentova odluka hoće li koristiti bilo koje informacije dostupne u Usluzi.

Određeni propisi zabranjuju bilo kakve neovlaštene pokušaje probijanja ili pristupanja računalnim sustavima. KLIJENTOVA JE ODGOVORNOST POBRINUTI SE DA KLIJENT NE KORISTI USLUGU ZA

PREGLEDAVANJE BILO KOJIH WEB STRANICA I/ILI APLIKACIJA OSIM ONIH KOJE SU U VLASNIŠTVU KLIJENTA ILI KOJE KLIJENT IMA PRAVO I OVLAŠTENJE PREGLEDAVATI.

Radi veće jasnoće, Klijentov sadržaj opisan u odlomku o zaštiti podataka u IBM-ovim Uvjetima upotrebe – opći uvjeti uključuje i podatke koji mogu postati dostupni IBM-u tijekom Penetracijskog testiranja aplikacije.

6.1 Sustavi u vlasništvu treće strane

Za sustave (što za potrebe ove odredbe uključuje, ali nije ograničeno na aplikacije i IP adrese) u vlasništvu treće strane koji će biti podložni testiranju temeljem ovog dokumenta, Klijent prihvaća:

a. da će, prije nego što IBM pokrene testiranje na sustavu treće strane, Klijent od vlasnika svakog sustava dobiti potpisano pismo kojim se IBM-u daje ovlaštenje za pružanje Usluga na tom sustavu i koje predstavlja vlasnikovo prihvaćanje uvjeta navedenih u odlomku "Dozvola za izvođenje testiranja" te će dostaviti IBM-u kopiju takvog ovlaštenja;

b. da će preuzeti isključivu odgovornost za objavljivanje bilo kakvih rizika, izloženosti i ranjivosti koje IBM-ovo testiranje na daljinu utvrdi na tim sustavima vlasniku sustava; i

c. da će urediti i omogućiti razmjenu informacija između vlasnika sustava i IBM-a u skladu s IBM-ovim potrebama.

Klijent prihvaća:

- da će odmah obavijestiti IBM kada nastupi promjena u vlasništvu bilo kojeg sustava koji je predmet testiranja temeljem ovog dokumenta;
- da neće objaviti isporučene materijale ili činjenicu da je IBM izveo Usluge izvan Klijentovog Poduzeća bez IBM-ovog pristanka u pisanom obliku; i
- da će u cijelosti obeštetiti IBM za bilo kakve gubitke ili odgovornost kojima se IBM izloži zbog potraživanja trećih strana nastalih zbog Klijentovog nepridržavanja zahtjeva u ovom odlomku s nazivom "Sustavi u vlasništvu treće strane" i za bilo kakve sudske pozive ili potraživanja treće strane podnesene protiv IBM-a ili IBM-ovih podugovarača koji proizlaze iz (a) testiranja sigurnosnih rizika, izloženosti ili ranjivosti sustava koji su predmet testiranja temeljem ovog dokumenta, (b) dostavljanja rezultata takvog testiranja Klijentu ili (c) Klijentovog korištenja ili objavljivanja takvih rezultata.

6.2 Cookieji

Klijent je svjestan i prihvaća da IBM može, kao dio uobičajene aktivnosti i podrške za IBM SaaS, prikupiti osobne podatke od Klijenta (vaših zaposlenika i ugovaratelja) koje se odnose na korištenje IBM SaaS-a, kroz praćenje i druge tehnologije. IBM to radi da bi prikupio korisne statističke podatke i informacije o učinkovitosti našeg IBM SaaS-a u svrhu poboljšanja korisničkog iskustva i/ili podešavanja interakcije s Klijentom. Klijent potvrđuje da će pribaviti ili je pribavio pristanak koji dozvoljava IBM-u da obrađuje prikupljene osobne podatke za gore navedenu svrhu unutar IBM-a, drugih IBM-ovih poduzeća i njihovih podugovarača, na svim lokacijama gdje mi i naši podugovarači poslujemo u skladu s mjerodavnim pravom. IBM će se pridržavati zahtjeva Klijentovih zaposlenika i ugovaratelja vezanih za pristup, ažuriranje, ispravke ili brisanje njihovih prikupljenih osobnih podataka.

U sklopu IBM SaaS-a koji uključuje aktivnosti izvještavanja, IBM će pripremiti i održavati informacije prikupljene iz IBM SaaS-a koje ne otkrivaju identitet i/ili koje su agregirane (nazvane "Sigurnosni podaci"). Sigurnosni podaci neće identificirati Klijenta ili pojedince, osim kako je navedeno niže pod (d). Klijent ovdje prihvaća da IBM može koristiti i/ili kopirati Sigurnosne podatke samo u sljedeće svrhe:

a. objavljivanje i/ili distribuiranje Sigurnosnih podataka (na primjer u kompilacijama i/ili analizama vezanim uz kibernetsku sigurnost);

b. razvoj ili poboljšavanje proizvoda ili usluga;

c. provođenje istraživanja interno ili s trećim stranama; i

d. zakonito dijeljenje potvrđenih informacija o počiniteljima trećih strana.

6.3 Lokacije koje primaju izvedenu korist

Gdje je to primjenjivo, porezi se temelje na lokaciji (ili lokacijama) za koje Klijent navede da primaju korist od IBM SaaS-a. IBM će primijeniti poreze koristeći poslovnu adresu navedenu kod naručivanja IBM SaaS-a kao primarnu lokaciju koja prima korist, osim ako Klijent ne dostavi dodatne informacije IBM-u. Klijent je odgovoran održavati takve informacije ažurnim i dostaviti bilo kakve promjene IBM-u.

6.4 Osobni podaci i regulirani sadržaj i usluge

Ovaj IBM SaaS nije dizajniran prema određenim sigurnosnim zahtjevima za regulirani sadržaj, na primjer za osobne podatke ili osjetljive osobne podatke. Klijent je odgovoran utvrditi zadovoljava li ovaj IBM SaaS Klijentove potrebe kada govorimo o tipu sadržaja koji Klijent koristi vezano uz IBM SaaS.

IBM ne djeluje kao pružatelj usluga čiji rad regulira Federalna komisija za komunikacije (engl. Federal Communications Commission - FCC) ili državna regulatorna tijela ("Državni regulatori") i ne namjerava pružati bilo kakve usluge koje regulira FCC ili Državni regulatori. Ako FCC ili bilo koji Državni regulator nametne regulatorne zahtjeve ili obveze na bilo koje usluge koje IBM pruža temeljem ovog dokumenta, IBM može: (a) modificirati ili zamijeniti proizvode o Klijentovom trošku i/ili (b) promijeniti način na koji se takve usluge pružaju Klijentu da bi se izbjeglo primjenjivanje takvih zahtjeva ili obveza na IBM (na primjer, djelujući kao Klijentov agent za stjecanje takvih usluga od zajedničkog nositelja treće strane).

Dodatak A

1. IBM Application Security on Cloud - opći opis

IBM Application Security on Cloud pruža jedinstveno mjesto koje je pomoć Klijentu da identificira sigurnosne ranjivosti (na primjer napad umetanjem SQL-a, skriptiranje između lokacija i curenje podataka) za razne aplikacije. Usluga uključuje različite tipove tehnika skeniranja sigurnosti aplikacije koje utvrđuju sigurnosne probleme u toj aplikaciji.

IBM Application Security on Cloud pruža sljedeće mogućnosti:

- Skeniranje mobilnih aplikacija radi otkrivanja sigurnosnih ranjivosti. Izvodi se pomoću dinamičkih (blackbox) i interaktivnih (glassbox) tehnologija analize sigurnosti.
- Skeniranje proizvodnih ili predproizvodnih, javnih ili privatnih web sjedišta radi otkrivanja sigurnosnih ranjivosti. Izvodi se pomoću dinamičkih (blackbox) tehnika analize sigurnosti.
- Skeniranje tokova podataka unutar mrežnih i stolnih aplikacija radi otkrivanja sigurnosnih ranjivosti. Izvodi se pomoću statičkih (whitebox) tehnika analize sigurnosti.
- Detaljni izvještaji o sigurnosnim ranjivostima, koji sadrže sažetke rezultata na visokoj razini i korake za ispravljanje koje programeri mogu slijediti.
- Integraciju s raznim DevOps platformama

1.1 IBM Application Analyzer

IBM Application Analyzer može se naručiti temeljem Instance aplikacije, Posla (skeniranja) ili kao puna Instanca i omogućuje sljedeće tipove skeniranja:

- Dinamički analizator – testiranje pretproizvodnih ili proizvodnih web stranica pomoću tehnika DAST
- Mobilni analizator – testiranje binarnih datoteka za iOS ili Android pomoću tehnika IAST
- Statički analizator – testiranje toka podataka bajtnog koda ili izvornog koda pomoću tehnika SAST

1.2 Usluga postavljanja

Ponuda IBM Application Security on Cloud - usluge savjetovanja je usluga postavljanja za Application Analyzer u obliku proizvoda. Usluga koristi IBM-ove savjetnike koji pružaju upute i pomoć kod testiranja i upravljanja rizikom aplikacije. Usluge savjetovanja ponude IBM Application Security on Cloud kupuju se kao blokovi Angažmana koji se mogu koristiti za zahtijevanje i korištenje sljedećih usluga u količinama navedenim dolje:

a. **Brzi početak** [koristi jednu (1) jedinicu Angažmana]

Usluga Brzi početak pruža stručna znanja i upute za korištenje funkcija testiranja i upravljanja rizikom uključene u Application Security on Cloud. Kada Klijent potvrdi da se uspješno prijavio na portal Application Security on Cloud, IBM će omogućiti web konferenciju s trajanjem od maksimalno dva (2) sata i za najviše dva (2) aktivna sudionika radi edukacije o osnovnim konfiguracijama i funkcijama AppSeca na IBM SaaS-u, što uključuje tipove skeniranja, izvođenje skeniranja, pregledavanje izvještaja i instaliranje pridruženih alata i plug-inova. Usluga Brzi početak dovršena je kada završi (a) web seminar za edukaciju Klijenta, (b) instalacija primjenjivih alata i plug-inova i (c) pružanje pomoći Klijentu kod postavljanja i izvođenja prvog skeniranja.

b. **Pregled procjene** [koristi dvije (2) jedinice Angažmana]

Usluga Pregled procjene pruža pomoć kod pregleda rezultata testiranja, što uključuje razumijevanje i prioritizaciju ispravljanja ranjivosti u aplikaciji. IBM će omogućiti web konferenciju s trajanjem od maksimalno jednog (1) sata i za najviše dva (2) aktivna sudionika tijekom koje se pruža pregled pronađenih ranjivosti i cjelokupnog sigurnosnog rizika aplikacije te detaljna rasprava o pronađenim sigurnosnim ranjivostima aplikacije, uključujući (1) kako je ranjivost testirana (2) kako su ranjivosti otkrivene, (3) kakav rizik predstavlja svaka pojedina ranjivost i (4) pružanje općih preporuka koje pomažu kod ispravljanja ranjivosti. Pregled će se temeljiti isključivo na rezultatu testiranja i neće predstavljati pregled samog izvornog koda. Klijent će pregledati rezultat testiranja i objavit će IBM-u koji se rezultat testiranja pregledava prije početka web konferencije. Usluga Pregled procjene dovršena je kada završi web konferencija.

c. **Skeniranje za mene** [koristi četiri (4) jedinice Angažmana]

Usluga Skeniranje za mene uključuje IBM-ovog stručnjaka za sigurnost aplikacija koji će konfigurirati i izvesti skeniranje, provjeriti rezultate i pružiti prikaz izvještaja za pregled zaključaka. Klijent će IBM-ovom savjetniku omogućiti pristup ASoC okolini radi konfiguriranja i izvođenja skeniranja, provjere rezultata, pružanja preporuka o prioritetu ispravaka i prikazivanja izvještaja o rezultatima. IBM će omogućiti web konferenciju s trajanjem od maksimalno jednog (1) sata i za najviše dva (2) aktivna sudionika tijekom koje se pruža pregled pronađenih ranjivosti i cjelokupnog sigurnosnog rizika aplikacije te detaljna rasprava o pronađenim sigurnosnim ranjivostima aplikacije, uključujući (1) kako je ranjivost testirana (2) kako su ranjivosti otkrivene, (3) kakav rizik predstavlja svaka pojedina ranjivost i (4) pružanje općih preporuka koje pomažu kod ispravljanja ranjivosti. Ako je to zatraženo unutar maksimalno 30 dana od početnog skeniranja, IBM će pružiti ponovno skeniranje koristeći konfiguraciju izvornog skeniranja isključivo za provjeru sigurnosnih ispravaka, ne za testiranje nove funkcionalnosti, te će provjeriti rezultate i dostaviti izvještaj Klijentu. Usluga Skeniranje za mene je dovršena kada završi web konferencija za pregled rezultata početnog skeniranja ili, ako je to primjenjivo, nakon završetka ponovnog skeniranja koje je zatražio Klijent i dostavljanja izvještaja ponovnog skeniranja Klijentu.

d. **Savjetnik na zahtjev** [koristi sedam (7) jedinica Angažmana]

Usluga Savjetnik na zahtjev obuhvaća do dvadeset (20) sati usluga IBM-ovog savjetnika koje se mogu koristiti za aktivnosti povezane s IBM SaaS-om. IBM-ov savjetnik će pružiti pomoć za pitanja koja se odnose na sigurnost, uključujući, ali ne ograničavajući se na upravljanje programom, određivanje prioriteta testiranja sigurnosti, strategije ispravljanja problema, analizu izvornog koda i ispravljanje izvornog koda. IBM će surađivati s Klijentom radi kreiranja i objašnjavanja rasporeda projekta koji sadrži specifične Klijentove zahtjeve, uključujući ciljeve projekta, relevantne tehnologije, postavljene vremenske okvire, očekivane isporučene materijale i procjenu broja angažmana za uslugu Advisor on Demand. Klijent mora omogućiti pristup aplikacijama, sustavima i dokumentaciji potrebnim za izvođenje usluga. Usluga Advisor on Demand završava nakon što protekne 20 sati pružanja stručnih usluga i/ili nakon što se Klijentu dostavi raspored projekta i/ili dokumentirani materijali za isporuku definirani u rasporedu projekta.

e. **Penetracijsko testiranje aplikacije**

Tri opcije:

(1) **Penetracijski test aplikacije na razini usklađenosti/početnoj razini**, koji uključuje do četrdeset (40) sati usluga Savjetnika i usmjeren je na greške u pojedinim logičkim koracima i jednostavnije varijante nedostataka vezanih uz napade umetanjem. Koristi petnaest (15) jedinica Angažmana.

(2) **Standardni penetracijski test aplikacije**, koji uključuje do šezdeset (60) sati usluga Savjetnika i proširuje fokus na logičke greške u procesima rada s više koraka, kompleksne varijante nedostataka vezanih uz napad umetanjem i Analizu kompleksnih tipova podataka. Koristi dvadeset i jednu (21) jedinicu Angažmana.

(3) **Napredni penetracijski test aplikacije** – uključuje do osamdeset (80) sati usluga Savjetnika i proširuje fokus na Obrnuti inženjering kompiliranih izvedbenih datoteka, raščlanjivanje prilagođenih mrežnih protokola, dubinsku analizu javno dostupnih knjižnica i razvojnih okvira. Koristi dvadeset i sedam (27) jedinica Angažmana.

Usluga penetracijskog testiranja aplikacije pruža IBM-ov resurs za izvođenje testiranja i korištenja aplikacije, dostavljanje izvještaja o testiranju i sažetog prikaza izvještaja u kojima se objašnjavaju zaključci i pridruženi rizici.

IBM će omogućiti poziv za pokretanje projekta s trajanjem od maksimalno jednog (1) sata i za najviše (2) aktivna sudionika tijekom kojeg se pregledava Klijentova okolina i organizacija, uključujući platformu aplikacije, arhitekturu, razvojne okvire, podržavajuću infrastrukturu, poznate sigurnosne probleme ili pitanja vezana uz aplikaciju, preliminarni raspored testiranja i plan kontakta za hitne slučajeve.

IBM će provesti penetracijsko testiranje aplikacije, uključujući, ali ne ograničavajući se na: utvrđivanje općih ranjivosti poput napada umetanjem SQL koda i skriptiranja između lokacija, procjenu snaga i slabosti postojećih sigurnosnih kontrola, na primjer provjere unosa, provjere identiteta i autorizacije, provjeru pravilne primjene poslovne logike, provjeru pravilne upotrebe sigurnosnih protokola, utvrđivanje grešaka u obradi sesija i provjeru adekvatnosti sigurnosnih

kontrola kod prijave, obnavljanja lozinke, politike lozinki i drugih funkcija za upravljanje korisnicima. Zaključci će biti navedeni u Izvještaju penetracijskog testiranja aplikacije. IBM će omogućiti web konferenciju za prikaz sažetka izvještaja u trajanju od jednog (1) sata. Usluga Penetracijskog testiranja aplikacije je dovršena kada su iskorišteni dodijeljeni sati za pružanje savjetovanja, kada je završena web konferencija i kada je Klijentu dostavljen konačni Izvještaj penetracijskog testiranja aplikacije.

1.2.1 Odgovornosti povezane s uslugama postavljanja

IBM će:

- pružati Usluge postavljanja koristeći jedinice Angažmana koje je kupio Klijent i u skladu s POE-om; i
- dovršiti Uslugu postavljanja kada su ispunjeni kriteriji dovršetka opisani u Odlomku 1.2.

Klijent prihvaća:

- da će biti odgovoran za sve naknade povezane sa svim zahtjevima Angažmana koje je Klijent predao za vrijeme trajanja ugovora;
- i potvrđuje da se kupljene jedinice Angažmana moraju iskoristiti unutar početnog trajanja ugovora i istječu ako se ne iskoriste do završnog datuma trajanja ugovora; i
- da će inicirati formalni zahtjev za sve Usluge postavljanja barem 30 dana prije datuma završetka pretplate.

U sklopu pružanja bilo koje Usluge postavljanja IBM može zatražiti informacije i razumnu količinu suradnje od Klijenta. Ako Klijent ne dostavi tražene informacije ili ne pruži suradnju u odgovarajućem vremenskom roku, to može, temeljem IBM-ove odluke, rezultirati naknadama u obliku jedinica Angažmana potrebnih za pružanje usluga ili zastoj tijekom izvođenja primjenjive usluge.

Da bi IBM mogao pravilno provesti testiranje, Klijent potvrđuje da će pratiti IBM-ove upute za pripremanje i održavanje okoline tijekom perioda testiranja.