# IBM Application Security on Cloud

Pogoje uporabe ("pogoji uporabe") sestavljajo ti IBM-ovi pogoji uporabe – pogoji posebne ponudbe SaaS ("pogoji posebne ponudbe SaaS") in dokument IBM-ovi pogoji uporabe – splošni pogoji ("splošni pogoji"), ki so na voljo na naslednjem naslovu URL: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

V primeru navzkrižja med splošnimi pogoji in pogoji posebne ponudbe SaaS prevladajo slednji. Naročnik z naročilom ali uporabo ponudbe IBM SaaS oziroma dostopanjem do nje soglaša s pogoji uporabe.

Pogoje uporabe ureja veljavna IBM-ova pogodba International Passport Advantage oz. International Passport Advantage Express ali IBM International Agreement for Selected IBM SaaS Offerings, karkoli je ustrezno, ("pogodba"), ki skupaj s pogoji uporabe predstavlja celotno pogodbeno dokumentacijo.

## 1. IBM SaaS

Ti pogoji posebne ponudbe SaaS pokrivajo naslednje ponudbe IBM SaaS:

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

## 2. Metrike zaračunavanja

Ponudba IBM SaaS se prodaja v skladu z naslednjo metriko zaračunavanja, določeno v transakcijskem dokumentu:

a. **Opravilo** – je merska enota, na podlagi katere je mogoče pridobiti ponudbo IBM SaaS. Opravilo je objekt v ponudbi IBM SaaS, ki ga ni mogoče dalje deliti in predstavlja postopek računanja, ki vključuje vse svoje podprocese. Naročnik mora pridobiti zadostna pooblastila, da z njimi pokrije skupno število opravil, ki jih ponudba IBM SaaS obdela ali upravlja med meritvenim obdobjem, navedenim v naročnikovem dokazilu o upravičenosti ali transakcijskem dokumentu.

b. **Primerek aplikacije** – je merska enota, na podlagi katere je mogoče pridobiti ponudbo IBM SaaS. Pooblastilo za primerek aplikacije je potrebno za vsak primerek aplikacije, ki je povezan s ponudbo IBM SaaS. Če ima aplikacija več komponent, pri čemer je vsaka posvečena drugačnemu namenu in/ali bazi uporabnikov ter je lahko vsaka povezana s ponudbo IBM SaaS oz. jo ponudba SaaS upravlja, se vsaka takšna komponenta šteje kot ločena aplikacija. Prav tako se preizkusno, razvojno, uprizoritveno in produkcijsko okolje aplikacije vsako posebej šteje kot ločen primerek aplikacije in mora imeti svoje pooblastilo. Če je v enem samem okolju več primerkov aplikacije, se vsak posebej šteje kot ločen primerek aplikacije in mora imeti svoje pooblastilo. Naročnik mora pridobiti zadostna pooblastila, da z njimi pokrije število primerkov aplikacij, povezanih s ponudbo IBM SaaS med meritvenim obdobjem, navedenim v naročnikovem dokazilu o upravičenosti ali transakcijskem dokumentu.

   Za namene te ponudbe IBM SaaS:

   - Za dinamično preizkušanje: spletno mesto, dosegljivo prek javnega ali zasebnega URL-ja. Z vsakim primerkom aplikacije je mesto upravičeno do 1.000 strani v eni domeni.
   - Za statično preizkušanje: enota kode, ki je izvršljiva v enem programskem jeziku. Z vsakim primerkom aplikacije so pregledovalne enote kode upravičene do 1.000.000 vrstic.
   - Za mobilno preizkušanje: enota binarne kode, ki jo je mogoče izvršiti v mobilni napravi. Posamezne mobilne platforme (npr. iOS in Android) predstavljajo različne primerke aplikacije.

c. **Primerek** – je merska enota, na podlagi katere je mogoče pridobiti ponudbo IBM SaaS. Primerek je dostop do določene konfiguracije storitve IBM SaaS. Naročnik mora pridobiti zadostna pooblastila za vsak primerek ponudbe IBM SaaS, za katerega sta omogočena dostop in uporaba med meritvenim obdobjem, navedenim v naročnikovem dokazilu o upravičenosti ali transakcijskem dokumentu.

   Za posamezno pooblastilo primerka ni omejitve glede števila izvedenih opravil ali primerkov aplikacij (povezanih aplikacij), a le če se v nobenem času ne izvaja več kot 30 opravil.

d. **Sodelovanje** – je merska enota, na podlagi katere je mogoče pridobiti storitve. Sodelovanje sestavljajo strokovne storitve in/ali storitve usposabljanja v povezavi z IBM SaaS. Naročnik mora pridobiti zadostna pooblastila, da z njimi pokrije vsa sodelovanja.

## 3. Stroški in zaračunavanje

Znesek, ki ga je treba plačati za ponudbo IBM SaaS, je naveden v transakcijskem dokumentu.

### 3.1 Delni mesečni stroški

Delni mesečni strošek, kot je naveden v transakcijskem dokumentu, se lahko oceni na osnovi sorazmernega deleža.

### 3.2 Zaračunavanje presežkov

Če naročnikova dejanska uporaba ponudbe IBM SaaS med meritvenim obdobjem presega pooblastila, navedena v dokazilu o upravičenosti (PoE), se naročniku zaračuna presežek, kot je navedeno v transakcijskem dokumentu.

### 3.3 Stroški nastavitve

Naročniku se bo nastavitev zaračunala v skladu z določili v transakcijskem dokumentu.

## 4. Obdobje trajanja in možnosti podaljšanja

Naročniško obdobje za ponudbo IBM SaaS se začne z dnem, ko IBM obvesti naročnika, da ima na voljo dostop do ponudbe IBM SaaS, v skladu z navedbami v dokazilu o upravičenosti. V dokazilu o upravičenosti bo navedeno, ali se naročnina na IBM SaaS podaljša samodejno, se nadaljuje na podlagi neprekinjene uporabe, ali se konča ob izteku naročniškega obdobja.

Na podlagi samodejnega podaljšanja se bo naročnina na ponudbo IBM SaaS samodejno podaljševala za obdobje, navedeno v dokazilu o upravičenosti, razen če naročnik posreduje pisno obvestilo o prenehanju podaljšanja najmanj 30 dni pred iztekom naročniškega obdobja.

Na podlagi neprekinjene uporabe bo ponudba IBM SaaS neprestano na voljo iz meseca v mesec, dokler naročnik ne posreduje predhodnega obvestila o odpovedi s 30-dnevnim odpovednim rokom. Ponudba IBM SaaS bo na voljo do konca koledarskega meseca po izteku takšnega 30-dnevnega obdobja.

## 5. Tehnična podpora

Tekom naročniškega obdobja in po tem ko IBM obvesti naročnika, da je na voljo dostop do ponudbe IBM SaaS, je tehnična podpora zagotovljena prek spletnih forumov in kot standardna podpora tekom časovnega obdobja, v katerem za naročnika nastane obveznost plačila glede na uporabo. Znotraj ponudbe IBM SaaS lahko naročniki predložijo prijavo za podporo ali začnejo sejo klepeta za pomoč. IBM bo omogočil dostop do priročnika o podpori za IBM-ovo programsko opremo kot storitev (SaaS), ki vsebuje kontaktne informacije o tehnični podpori ter druge informacije in postopke.

| Resnost | Definicija resnosti | Ciljni odzivni čas | Kritje odzivnega časa |
|---|---|---|---|
| 1 | **Bistven vpliv na poslovanje/izpad storitve:** Nedelovanje funkcije, ki je kritičnega pomena za poslovanje, ali izpad kritičnega vmesnika. To običajno velja za produkcijsko okolje in pomeni nezmožnost dostopanja do storitev, kar ima odločilen vpliv na delovanje. To stanje zahteva takojšnjo rešitev. | V roku 1 ure | 24 ur na dan, 7 dni v tednu |
| 2 | **Velik vpliv na poslovanje:** Uporaba funkcije poslovne storitve ali delovanja storitve je zelo omejena oz. za naročnika obstaja nevarnost, da bo zamudil poslovne roke. | V roku 2 delovnih ur | Delovni čas od ponedeljka do petka |
| 3 | **Manjši vpliv na poslovanje:** Označuje, da je storitev ali funkcijo mogoče uporabljati in težava nima odločilnega vpliva na delovanje. | V roku 4 delovnih ur | Delovni čas od ponedeljka do petka |
| 4 | **Minimalen vpliv na poslovanje:** Poizvedba ali netehnična zahteva | V roku 1 delovnega dne | Delovni čas od ponedeljka do petka |

### 5.1 Dostop do naročnikovih podatkov

IBM bo lahko dostopal do naročnikovih podatkov za namen diagnosticiranja težav v zvezi s storitvijo in podpore pregledom naročnikove aplikacije s strani storitve. IBM bo dostopal do podatkov samo za namene odpravljanja napak ali zagotavljanja podpore za IBM-ove produkte in storitve.

## 6. Dodatni pogoji ponudbe IBM SaaS

Varnostni pregledi morda ne zaznajo vseh varnostnih tveganj v aplikaciji in niso zasnovani ali namenjeni za uporabo v tveganih okoljih, ki zahtevajo delovanje z zaščito pred izpadom, kar med drugim vključuje letalsko navigacijo, sisteme za kontrolo zračnega prometa, sisteme oborožitve, sisteme za ohranjanje življenja in jedrske objekte, ali v katerihkoli drugih aplikacijah, ki bi zaradi nezaznanih varnostnih tveganj lahko povzročile smrt, telesno poškodbo ali gmotno škodo. Za varnostne preglede ni zajamčeno neprekinjeno delovanje ali delovanje brez napak.

Ponudba IBM SaaS lahko naročniku pomaga pri doseganju skladnosti, ki lahko temelji na zakonih, predpisih, standardih ali praksah. Nobena navodila, predlagana uporaba ali smernice, ki jih zagotavlja storitev, ne predstavljajo pravnih, računovodskih ali drugih strokovnih nasvetov in naročnik je opozorjen, naj pridobi svojega pravnega ali drugega strokovnega svetovalca. Naročnik sam odgovarja, da skupaj s svojimi dejavnostmi, aplikacijami in sistemi izpolnjuje zahteve veljavne zakonodaje, predpisov, standardov in praks. Uporaba te storitve ne jamči skladnosti z zakonodajo, predpisi, standardi ali dobrimi praksami.

Ponudba IBM SaaS izvaja invazivne in neinvazivne preizkuse na spletnem mestu in spletni ali mobilni aplikaciji, ki ju naročnik želi pregledati. Nekateri zakoni prepovedujejo kakršenkoli nepooblaščen poskus vstopa ali dostopa do računalniških sistemov. Naročnik pooblašča IBM za izvajanje storitev v skladu z opisi v tem dokumentu in potrjuje, da storitve predstavljajo pooblaščen dostop do naročnikovih računalniških sistemov. IBM lahko razkrije svoje pooblastilo tretjim osebam, če se mu zdi to potrebno za izvajanje storitev.

Preizkušanje vključuje nekatera tveganja, med drugim naslednja:

a. Naročnikovi računalniški sistemi se lahko med izvajanjem aplikacij, ki se preizkušajo, prenehajo odzivati ali se sesujejo, kar lahko povzroči začasno nedostopnost sistema ali izgubo podatkov;

b. zmogljivost in prepustnost naročnikovih sistemov ter zmogljivost in prepustnost povezanih usmerjevalnikov in požarnih zidov so lahko med preizkušanjem začasno zmanjšani;

c. generirajo se lahko prekomerne količine dnevniških sporočil, kar vodi v prekomerno porabo prostora na disku zaradi dnevniških datotek;

d. podatki se lahko spremenijo ali izbrišejo kot posledica pregleda ranljivosti;

e. sistemi zaznavanja vdorov lahko sprožijo alarme;

f. zaradi preizkušanja funkcije elektronske pošte v spletni aplikaciji se lahko sproži elektronska pošta;

g. IBM SaaS lahko prestreže promet nadzorovanega omrežja za namen iskanja dogodkov.

Med dejavnostmi preizkušanja ne bodo veljale nobene pravice ali pravna sredstva, ki jih IBM zagotavlja po pogodbi o ravni storitev v zvezi s spletnimi mesti ali aplikacijami, ki so predmet preizkušanja.

Če naročnik za prijavo v aplikacijo, ki se preizkuša, v storitev vnese overjene poverilnice, naj naročnik vnese samo poverilnice za preizkusne račune, in ne za produkcijske uporabnike. V primeru uporabe poverilnic produkcijskega uporabnika se lahko zgodi, da bodo osebni podatki preneseni prek storitve.

Ponudbo IBM SaaS je mogoče konfigurirati za optično branje produkcijskih spletnih aplikacij. Če odjemalec nastavi vrsto pregleda na "produkcijska", zasnova storitve izvede pregled na način, ki zmanjšuje tveganja, navedena zgoraj; v nekaterih primerih pa lahko IBM SaaS privede do poslabšanja delovanja ali nestabilnosti v testiranih produkcijskih spletnih mestih in infrastrukturi. IBM ne daje nobenih jamstev glede primernosti uporabe ponudbe IBM SaaS za pregled produkcijskih spletnih mest.

NAROČNIKOVA ODGOVORNOST JE, DA UGOTOVI, ALI JE STORITEV PRIMERNA ALI VARNA ZA NAROČNIKOVO SPLETNO MESTO, SPLETNO APLIKACIJO, MOBILNO APLIKACIJO ALI TEHNIČNO OKOLJE.

Ponudba IBM SaaS je zasnovana tako, da identificira različne morebitne varnostne težave in težave s skladnostjo v mobilnih in spletnih aplikacij ter spletnih storitev. Ne preizkusi vseh ranljivosti ali tveganj zaradi skladnosti, niti ne deluje kot prepreka pred napadi na varnost. Varnostna tveganja, predpisi in standardi se nenehno spreminjajo, in storitev morda ne odraža vseh takšnih sprememb. Varnost in

skladnost naročnikovih spletnih aplikacij, sistemov in zaposlenih in vseh popravnih dejanj so izključno naročnikova odgovornost. Izključno naročnik lahko presodi, ali bo ali ne bo uporabil informacij, ki jih zagotavlja storitev.

Nekateri zakoni prepovedujejo kakršenkoli nepooblaščen poskus vstopa ali dostopa do računalniških sistemov. NAROČNIK JEODGOVOREN, DA STORITVE NE UPORABLJA ZA OPTIČNO BRANJE KATERIHKOLI SPLETNIH MEST IN/ALI APLIKACIJ, KI NISO SPLETNA MESTA IN/ALI APLIKACIJE, KI JIH IMA V LASTI NAROČNIK, ALI TISTIH, ZA KATERE IMA NAROČNIK PRAVICO IN POOBLASTILO ZA OPTIČNO BRANJE.

V izogib nejasnostim velja za naročnikovo vsebino, opisano v razdelku o zaščiti podatkov v IBM-ovih pogojih uporabe – splošnih pogojih, da prav tako vključuje podatke, ki lahko postanejo dostopni IBM-u med penetracijskim testiranjem aplikacije.

## 6.1 Sistemi v lasti tretjih oseb

V zvezi s sistemi (kar za namene te določbe med drugim vključuje aplikacije in naslove IP) v lasti tretjih oseb, ki bodo predmet preizkušanja po tej pogodbi, naročnik soglaša:

a. da bo pred začetkom IBM-ovega preizkušanja v sistemu tretje osebe naročnik pridobil od lastnika vsakega sistema podpisano pismo, ki bo IBM pooblaščalo za zagotavljanje storitev v tistem sistemu in potrjevalo, da lastnik sprejema pogoje iz razdelka "Dovoljenje za izvajanje preizkušanja" ("Permission to Perform Testing"), ter bo IBM-u posredoval kopijo tega pooblastila;

b. da bo v celoti sam odgovoren za posredovanje lastniku sistema podatkov o morebitnih tveganjih, izpostavljenostih ali ranljivostih, zaznanih v teh sistemih prek IBM-ovega preizkušanja na daljavo; in

c. da bo poskrbel za in olajšal izmenjavo informacij med lastnikom sistema in IBM-om, kot se bo IBM-zdelo potrebno.

Naročnik soglaša z naslednjim:

- da bo nemudoma obvestil IBM o vsaki spremembi lastništva kateregakoli sistema, ki je predmet preizkušanja po tej pogodbi;
- da brez IBM-ovega predhodnega pisnega soglasja zunaj svojega podjetja ne bo razkril končnih izsledkov ali dejstva, da je storitve izvedel IBM; in
- da bo IBM-u v celoti povrnil škodo za morebitne nastale izgube ali prevzete obveznosti, ki bremenijo IBM zaradi zahtevkov tretjih oseb, ki izhajajo iz naročnikovega neupoštevanja zahtev iz tega razdelka z naslovom "Sistemi v lasti tretjih oseb", in za morebitne sodne pozive tretjih oseb ali zahteve, vložene proti IBM-u ali IBM-ovim podpogodbenikom ali posrednikom, ki izhajajo iz (a) preizkušanja varnostnih tveganj, izpostavljenosti ali ranljivosti sistemov, ki so predmet preizkušanja po tej pogodbi, (b) posredovanja rezultatov teh preizkusov naročniku ali (c) naročnikove uporabe ali razkritja takih rezultatov.

## 6.2 Piškotki

Naročnik se zaveda in soglaša, da lahko IBM kot del običajnega delovanja in podpore ponudbe IBM SaaS prek sledenja in drugih tehnologij zbira naročnikove osebne podatke (podatke njegovih zaposlenih in pogodbenikov) v zvezi z uporabo ponudbe IBM SaaS prek sledenja in drugih tehnologij. IBM s tem pridobiva statistiko o uporabi in podatke o učinkovitosti storitve IBM SaaS z namenom izboljšanja uporabniške izkušnje in/ali prilagajanja interakcije z naročnikom. Naročnik potrjuje, da je/bo pridobil soglasje, ki IBM-u dovoljuje obdelavo zbranih osebnih podatkov za navedeni namen znotraj IBM-a, drugih IBM-ovih podjetij in njihovih podizvajalcev ne glede na to, kje IBM in njegovi podizvajalci poslujejo, v skladu z veljavno zakonodajo. IBM bo upošteval zahteve naročnikovih zaposlenih in pogodbenikov za dostop, posodobitev, spremembo ali izbris njihovih zbranih osebnih podatkov.

V okviru ponudbe IBM SaaS, ki vključuje dejavnosti poročanja, bo IBM pripravil in vzdrževal anonimizirane in/ali združene podatke, zbrane iz ponudbe IBM SaaS (t.i. "varnostni podatki"). Varnostni podatki ne bodo razkrili identitete naročnika ali posameznikov, razen v primerih iz točke (d) spodaj. Naročnik prav tako soglaša, da IBM lahko uporabi in/ali kopira varnostne podatke le za naslednje namene:

a. objavljanje in/ali distribucija varnostnih podatkov (npr. pri zbiranju in/ali analizi v povezavi s kibernetično varnostjo);

b. razvijanje ali izboljševanje izdelkov ali storitev;

c. izvajanje raziskav znotraj IBM-a ali v sodelovanju s tretjimi osebami;

d. zakonita skupna raba potrjenih informacij o storilcu, ki je tretja oseba.

## 6.3 Izpeljane lokacije prejemanja storitev

Kadar je to ustrezno, davki temeljijo na eni ali več lokacijah, ki jih naročnik navede kot lokacije prejemanja storitev iz ponudbe IBM SaaS. IBM obračuna davke na podlagi poslovnega naslova, ki ga je naročnik navedel pri naročilu ponudbe IBM SaaS kot primarno lokacijo uporabe storitev, razen če naročnik IBM-u posreduje dodatne informacije o tem. Naročnik je odgovoren, da posodablja takšne informacije in IBM-u sporoči morebitne spremembe.

## 6.4 Osebni podatki ter nadzorovane vsebine in storitve

Ta ponudba IBM SaaS ni zasnovana v skladu z nobenimi posebnimi varnostnimi zahtevami za nadzorovano vsebino, kot so osebni podatki ali občutljivi osebni podatki. Naročnik je odgovoren, da ugotovi, ali ta ponudba IBM SaaS ustreza njegovim zahtevam glede vrste vsebine, ki jo naročnik uporablja v povezavi s ponudbo IBM SaaS.

IBM ni ponudnik storitev, ki jih ureja ameriška zvezna komisija za telekokumikacije ("FCC") ali regulativni organi zveznih držav ("zvezni regulativni organi"), in ne namerava zagotavljati nobenih storitev, ki jih urejajo FCC ali zvezni regulativni organi. Če FCC ali eden od zveznih regulativnih organov uvede regulativne zahteve ali obveznosti za katerekoli storitve, ki jih zagotavlja IBM po tej pogodbi, lahko IBM: (a) spremeni, nadomesti ali zamenja izdelke na naročnikove stroške in/ali (b) spremeni način zagotavljanja teh storitev naročniku, da se izogne upoštevanju takih zahtev ali obveznosti s strani IBM-a (na primer tako, da deluje kot naročnikov posrednik za pridobitev storitev prek neodvisnega splošnega ponudnika).

# Dodatek A

## 1. Splošen opis izdelka IBM Application Security on Cloud

IBM Application Security on Cloud zagotavlja enotno mesto za pomoč naročniku pri ugotavljanju varnostnih ranljivosti (kot so vstavljanje sestavljenega jezika za poizvedbe, skriptno izvajanje na več spletnih mestih in uhajanje podatkov) za različne aplikacije. Storitev vključuje različne vrste tehnik pregleda zaščite aplikacije, od katerih vsaka identificira varnostne težave v tej aplikaciji.

Storitev IBM Application Security on Cloud omogoča naslednje zmožnosti:

- Pregledovanje mobilnih aplikacij za varnostne ranljivosti. To se naredi prek dinamičnih (črna skrinjica) in interaktivnih (steklena skrinjica) tehnologij analize varnosti.
- Pregledovanje produkcijskih ali predprodukcijskih, javno dostopnih ali v zasebnem omrežju, spletnih strani za varnostne ranljivosti. To se naredi prek dinamičnih (črna skrinjica) tehnik analize varnosti.
- Pregledovanje podatkovnih tokov znotraj spletnih in namiznih aplikacij za varnostne ranljivosti. To se naredi s statičnimi (bela skrinjica) tehnikami analize varnosti.
- Podrobna poročila o varnostni ranljivosti, ki vsebujejo povzetke visoke ravni o korakih z ugotovitvami ter popravki/posodobitvami, katere lahko spremljajo razvijalci.
- Integracija z različnimi platformami DevOps.

### 1.1 IBM Application Analyzer

IBM Application Analyzer je mogoče naročiti za posamezni primerek aplikacije, za posamezno opravilo (pregled) ali kot polni primerek, ki omogoča naslednje vrste pregledovanja:

- Dynamic Analyzer – Preizkus predprodukcijskih ali produkcijskih spletnih mest z uporabo tehnik DAST
- Mobile Analyzer – Preizkus binarnih vrednosti sistemov iOS ali Android z uporabe tehnik IAST
- Static Analyzer – Preizkus bajtnih podatkovnih tokov in podatkovnih tokov izvorne kode z uporabo tehnik SAST

### 1.2 Storitev nastavitve

IBM Application Security on Cloud Consulting Services je storitev nastavitve v obliki izdelka za storitev Application Analyzer. V okviru storitve izvajajo IBM-ovi svetovalci svetovanje in pomoč pri preizkušanju in upravljanju tveganj v zvezi z aplikacijo. Storitve IBM Application Security on Cloud Consulting Services se kupijo kot paketi sodelovanj, ki jih je mogoče razširiti v spodaj navedenih količinah za zahtevo ali uporabo naslednjih posebnih storitev:

a. **Fast Start** [Uporablja eno (1) enoto sodelovanja]

Storitev Fast Start zagotavlja strokovno znanje in svetovanje za uporabo funkcij za preizkušanje in upravljanje tveganj aplikacije Application Security on Cloud. Ko naročnik potrdi uspešno prijavo v portal Application Security on Cloud, bo IBM izvedel spletno konferenco v obsegu do dveh (2) ur in za dva (2) aktivna udeleženca ter tako zagotovil izobraževanje o osnovnih konfiguracijah in funkcijah AppSec on IBM SaaS, vključno z vrstami pregledov, pregledi v izvajanju, pregledovanjem poročil in nameščanjem povezanih orodij in vtičnikov. Storitev Fast Start je opravljena, ko se v celoti izvede (a) naročnikov izobraževalni spletni seminar, (b) namestitev ustreznih orodij in vtičnikov in (c) pomoč naročniku pri nastavitvi in izvedbi prvega pregleda.

b. **Assessment Review** [Uporablja dve (2) enoti sodelovanja]

Storitev Assessment Review zagotavlja pomoč pri pregledovanju rezultatov preizkusov, kar vključuje razumevanje in prednostno obravnavanje pri odpravljanju ranljivosti v aplikaciji. IBM bo izvedel spletno konferenco v obsegu do ene (1) ure in za dva (2) aktivna udeleženca ter tako zagotovil pregled zaznanih ranljivosti, splošno varnostno tveganje za aplikacijo in podrobno razpravo o zaznanih varnostnih ranljivostih za aplikacijo, kar vključuje (1) način preizkušanja ranljivosti, (2) način zaznave ranljivosti, (3) tveganja posameznih ranljivosti in (4) splošna priporočila za popravke, ki pomagajo odpraviti ranljivosti. Pregled bo temeljil izključno na rezultatih preizkusa in ne bo vključeval pregleda same izvorne kode. Naročnik bo preučil rezultate preizkusa in jih pred

spletno konferenco posredoval v pregled IBM-u. Storitev Assessment Review je opravljena po izvedbi spletne konference.

c. **Scan for Me** [Uporablja štiri (4) enote sodelovanja]

Storitev Scan for Me zagotavlja IBM-ovega strokovnjaka za varnost aplikacij, ki bo konfiguriral in izvedel pregled, preveril rezultate in pripravil predstavitev poročila s pregledom ugotovitev. Naročnik bo IBM-ovemu svetovalcu dovolil dostop do svojega okolja ASoC, da bo slednji lahko konfiguriral in izvedel pregled, preveril rezultate, podal priporočila za prednostno obravnavo pri odpravljanju ranljivosti in pripravil predstavitev poročila o rezultatih. IBM bo izvedel spletno konferenco v obsegu do ene (1) ure in za dva (2) aktivna udeleženca ter tako zagotovil pregled zaznanih ranljivosti, splošno varnostno tveganje za aplikacijo in podrobno razpravo o zaznanih varnostnih ranljivostih za aplikacijo, kar vključuje (1) način preizkušanja ranljivosti, (2) način zaznave ranljivosti, (3) tveganja posameznih ranljivosti in (4) splošna priporočila za popravke, ki bi pomagali odpraviti ranljivosti. Na naročnikovo zahtevo bo IBM do 30 dni po prvem pregledu zagotovil ponovni pregled z uporabo prvotne konfiguracije pregleda, vendar le, da bo preveril varnostne popravke, ne bo pa preizkušal nove funkcionalnosti, preverjal rezultatov ali predložil poročila naročniku. Storitev Scan for Me je opravljena po izvedbi spletne konference, na kateri se pregledajo rezultati prvega pregleda ali, če je ustrezno, po izvedbi ponovnega pregleda na zahtevo naročnika in izročitvi poročila o ponovnem pregledu naročniku.

d. **Advisor on Demand** [Uporablja sedem (7) enot sodelovanja]

Storitev Advisor on Demand zagotavlja do dvajset (20) ur časa IBM-ovega svetovalca, ki ga je mogoče porabiti za dejavnosti v zvezi s ponudbo IBM SaaS. IBM-ov svetovalec bo pomagal pri specifičnih temah o varnosti aplikacij, kar med drugim vključuje upravljanje programov, prednostno obravnavo pri preizkušanju varnosti, strategije za odpravo ranljivosti, analizo izvorne kode in popravilo izvorne kode. IBM bo sodeloval z naročnikom, da bo lahko razumel in ustvaril projektni urnik s specifičnimi zahtevami naročnika, vključno s cilji projekta, ustreznimi tehnologijami, želenim časovnim razporedom, končnimi izsledki in oceno števila sodelovanj storitve Advisor on Demand. Naročnik mora zagotoviti dostop do ustreznih aplikacij, sistemov in dokumentacije, ki so potrebni za izvedbo storitev. Storitev Advisor on Demand je opravljena, ko je izvedenih do 20 ur strokovnega varnostnega svetovanja in/ali je bil izpolnjen projektni urnik in/ali so bili končni izdelki, opredeljeni v projektnem urniku, predloženi naročniku.

e. **Penetracijsko testiranje aplikacije**

Tri možnosti:

(1) **Skladnostni/osnovni penetracijski test aplikacije**, ki vključuje do štirideset (40) ur svetovanja in se osredotoča na logične napake v korakih in preprostejše različice napak pri vrinjenju. Uporablja petnajst (15) enot sodelovanja.

(2) **Standardni penetracijski test aplikacije**, ki vključuje do šestdeset (60) ur svetovanja z razširjenim obsegom, tako da zajema tudi logične napake in delovne tokove z več koraki, kompleksne različice napak pri vrinjenju in analizo kompleksnih vrst podatkov. Uporablja enaindvajset (21) enot sodelovanja.

(3) **Napredni penetracijski test aplikacije** – Vključuje do osemdeset (80) ur svetovanja z razširjenim obsegom, tako da zajema tudi vzvratno inženirstvo zbranih izvedljivih datotek, podroben pregled omrežnih protokolov po meri ter podrobno analizo javno dostopnih knjižnic in ogrodij. Uporablja sedemindvajset (27) enot sodelovanja.

Storitev penetracijskega testiranja aplikacije zagotavlja IBM-ov vir za izvajanje preizkušanja in zlorabe aplikacije, predložitev poročila o preizkusu in predstavitev poročila z razlago ugotovitev in povezanih tveganj.

IBM bo izvedel obisk za uvedbo projekta s trajanjem do ene (1) ure in za dva (2) aktivna udeleženca, znotraj katerega bo pregledal naročnikovo okolje in organizacijo, vključno s platformo, arhitekturo, ogrodji in podporno infrastrukturo aplikacije, znanimi varnostnimi težavami ali možnimi težavami v zvezi z aplikacijo ter predhodnim razporedom preizkušanja in kontaktnim načrtom za nujne primere.

IBM bo izvedel preizkušanje aplikacije z vdorom, ki med drugim vključuje: prepoznavanje običajnih ranljivosti, kot so vrinjenja SQL in skriptno izvajanje na več straneh, ocenjevanje prednosti in slabosti obstoječega varnostnega nadzora, kot je preverjanje veljavnosti, preverjanje pristnosti in pooblaščanje vhodnih podatkov, preverjanje ustreznega uveljavljanja poslovne logike, preverjanje

ustrezne uporabe varnih protokolov, prepoznavanje napak pri obravnavanju sej ter preverjanje ustreznosti varnostnega nadzora nad prijavo, obnovitvijo gesel, politiko gesel in drugih funkcij za upravljanje uporabnikov. Ugotovitve bodo navedene v poročilu o penetracijskem testu aplikacije. IBM bo izvedel spletno konferenco za predstavitev poročila, ki bo trajala največ eno (1) uro. Storitev penetracijskega testa aplikacije je opravljena, ko je porabljen dodeljeni čas za svetovanje, ko je izvedena spletna konferenca in ko je končno poročilo o preizkusu aplikacije z vdorom predloženo naročniku.

### 1.2.1 Dolžnosti za storitve nastavitve

IBM bo:

- zagotovil storitve nastavitve z uporabo enot sodelovanja, ki jih je kupil naročnik in na podlagi dokazila o upravičenosti; in
- opravil storitev nastavitve, ko bodo izpolnjena merila za izpolnitev, opredeljena v razdelku 1.2.

Naročnik soglaša, da:

- je odgovoren za vse stroške, povezane z vsemi zahtevami glede sodelovanj, ki jih naročnik predloži v pogodbenem obdobju;
- se strinja, da morajo biti kupljene enote sodelovanja porabljene znotraj prvotnega pogodbenega obdobja, neporabljene enote pa po datumu izteka pogodbenega obdobja potečejo; in
- da bo predložil uradno zahtevo za vse storitve nastavitve vsaj 30 dni pred datumom izteka naročniškega obdobja.

Pri izvajanju storitev nastavitve lahko IBM od naročnika zahteva informacije in razumno sodelovanje. Če naročnik IBM-u pravočasno ne zagotovi informacij ali sodelovanja, se lahko v skladu z IBM-ovimi določili enote sodelovanja zaračunajo z upoštevanjem potreb za storitve ali pa se zamakne izvajanje ustrezne storitve.

Naročnik soglaša, da bo upošteval IBM-ova navodila za pripravo in vzdrževanje okolja med preizkusnim obdobjem, zato da bo IBM lahko natančno izvedel preizkušanje.