IBM Application Security on Cloud

Termenii de Utilizare ("TdU") sunt alcătuiţi din aceşti Termeni de Utilizare IBM – Termeni Specifici Ofertei SaaS ("Termenii Specifici Ofertei SaaS") şi un document intitulat Termenii de Utilizare IBM – Termeni Generali ("Termenii Generali"), disponibil la următorul URL: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

În eventualitatea unui conflict, Termenii Specifici Ofertei SaaS vor prevala faţă de Termenii Generali. Prin comandarea, accesarea sau utilizarea IBM SaaS, Clientul este de acord cu Termenii de Utilizare.

Termenii de Utilizare sunt guvernaţi de IBM International Passport Advantage Agreement, IBM International Passport Advantage Express Agreement sau IBM International Agreement for Selected IBM SaaS Offerings, după caz ("Contractul"), care împreună cu Termenii de Utilizare reprezintă acordul complet.

1. IBM SaaS

Aceşti Termeni Specifici Ofertei SaaS acoperă următoarele oferte IBM SaaS:

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

2. Indicii de Măsurare pentru Tarifare

IBM SaaS este vândut în baza următorilor indici de măsurare pentru tarifare, după cum este specificat în Documentul Tranzacţional:

a. **Job** – este o unitate de măsură pentru obţinerea IBM SaaS. Un Job este un obiect din IBM SaaS ce nu poate fi divizat şi reprezintă un proces de prelucrare a datelor împreună cu toate sub-procesele sale. Trebuie obţinute drepturi suficiente pentru a acoperi numărul total de Joburi procesate sau gestionate de IBM SaaS pe durata perioadei de măsurare specificate în Dovada Dreptului de Utilizare (Proof of Entitlement - PoE) sau Documentul Tranzacţional al Clientului.

b. **Instanţă de Aplicaţie** – este o unitate de măsură pentru obţinerea IBM SaaS. Este necesar câte un drept Instanţă de Aplicaţie pentru fiecare instanţă a unei Aplicaţii conectate la IBM SaaS. Dacă o Aplicaţie are mai multe componente, fiecare servind un scop distinct şi/sau o bază de utilizator şi fiecare fiind conectată la sau gestionată de IBM SaaS, atunci fiecare dintre aceste componente este considerată o Aplicaţie separată. În plus, mediile de testare, dezvoltare, intermediere şi producţie pentru o Aplicaţie sunt considerate, fiecare, câte o instanţă separată a Aplicaţiei şi pentru fiecare este necesar un drept de utilizare. Când există mai multe Instanţe de Aplicaţie într-un singur mediu, fiecare este considerată o instanţă separată a Aplicaţiei şi fiecare necesită un drept de utilizare. Trebuie obţinute drepturi suficiente pentru a acoperi numărul Instanţelor de Aplicaţie conectate la IBM SaaS pe durata perioadei de măsurare specificate în Dovada Dreptului de Utilizare (Proof of Entitlement - PoE) sau Documentul Tranzacţional al Clientului.

   Pentru scopurile acestui IBM SaaS:

   - Pentru Testare Dinamică: un site web accesibil printr-un URL public sau privat. Fiecare Instanţă de Aplicaţie asigură dreptul pentru un site cu până la 1.000 de pagini, într-un singur domeniu.
   - Pentru Testare Statică: o unitate de cod executabil, într-un singur limbaj de programare. Fiecare Instanţă de Aplicaţie asigură dreptul pentru scanarea unităţilor de cod de până la 1.000.000 de linii.
   - Pentru Testare Mobilă: o unitate de cod binar ce poate fi executat pe un dispozitiv mobil. Fiecare platformă mobilă diferită (de exemplu, iOS şi Android) constituie o Instanţă de Aplicaţie diferită.

c. **Instanţă** – este o unitate de măsură pentru obţinerea IBM SaaS. O Instanţă este accesul la o configuraţie IBM SaaS specifică. Trebuie obţinute drepturi suficiente pentru fiecare Instanţă a IBM SaaS făcută disponibilă pentru acces şi utilizare pe durata perioadei de măsurare specificate în Dovada Dreptului de Utilizare (Proof of Entitlement - PoE) sau Documentul Tranzacţional al Clientului.

   Pentru fiecare drept Instanţă, nu există o limită pentru numărul de Joburi realizate sau Instanţe de Aplicaţie (Aplicaţii conectate), cu condiţia ca, la un moment dat, nu pot rula mai mult de 30 de joburi.

d. **Angajament** – este o unitate de măsură pentru obţinerea serviciilor. Un Angajament constă în servicii profesionale şi/sau de instruire asociate cu IBM SaaS. Trebuie obţinute drepturi de utilizare suficiente pentru a acoperi fiecare Angajament.

3. Tarife şi Facturare

Suma de plată pentru IBM SaaS este specificată într-un Document Tranzacţional.

3.1 Tarife Lunare Parţiale

Un tarif lunar parţial, după cum este specificat în Documentul Tranzacţional, poate fi evaluat prin proratare.

3.2 Tarife pentru Excedent

Dacă utilizarea reală a IBM SaaS pe durata perioadei de măsurare depăşeşte dreptul de utilizare specificat în PoE, Clientului îi va fi aplicat un tarif pentru excedent, după cum este menţionat în Documentul Tranzacţional.

3.3 Tarifele de Setare

Clientul va fi tarifat pentru setare după cum este specificat în Documentul Tranzacţional.

4. Opţiunile pentru Termen şi Reînnoire

Termenul IBM SaaS începe la data la care IBM anunţă Clientul că acesta are acces la IBM SaaS, după cum este specificat în PoE. Dovada Dreptului de Utilizare (PoE) va specifica dacă oferta IBM SaaS este reînnoită automat, va fi furnizată mai departe pe bază de utilizare continuă sau se va termina la sfârşitul termenului.

În cazul reînnoirii automate, cu excepţia situaţiei în care Clientul, cu cel puţin 30 de zile înainte de expirarea termenului, trimite o notificare scrisă prin care anunţă că nu doreşte reînnoirea, oferta IBM SaaS va fi reînnoită automat pentru termenul specificat în PoE.

În cazul utilizării continue, oferta IBM SaaS va continua să fie disponibilă, de la lună la lună, până când Clientul trimite, cu 30 de zile înainte, o notificare scrisă privind terminarea. După această perioadă de 30 de zile, oferta IBM SaaS va rămâne disponibilă până la sfârşitul lunii calendaristice.

5. Suport Tehnic

Pe durata Perioadei de Abonare, după ce IBM anunţă Clientul că este disponibil accesul la IBM SaaS, este furnizat suport tehnic prin forumuri online şi ca suport standard pe durata perioadei în care Clientul ocazionează tarife Plată per Utilizare. Din IBM SaaS, Clienţii pot să trimită un tichet de suport sau să deschidă o sesiune de chat pentru asistenţă. IBM va face disponibilă publicaţia IBM Software as a Service Support Handbook, care conţine informaţii privind contactarea suportului tehnic şi alte informaţii şi procese.

Severitate	Definiţie Severitate	Obiective Timp de Răspuns	Acoperire Timp de Răspuns
1	**Impact critic asupra afacerii/serviciu întrerupt:** O funcţionalitate cu caracter critic pentru afacere este inoperabilă sau nu funcţionează o interfaţă cu caracter critic. De obicei aceasta se aplică în cazul unui mediu de producţie şi indică incapacitatea de a accesa serviciile, ceea ce are un impact critic asupra operaţiilor. Această condiţie necesită o soluţionare imediată.	Într-un interval de 1 oră	24x7
2	**Impact semnificativ asupra afacerii:** O caracteristică sau o funcţie a serviciului a suferit o restricţie importantă privind utilizarea sau Clientul nu poate îndeplini termenele limită ale afacerii.	Într-un interval de 2 ore de lucru	Orele de lucru L-V
3	**Impact minor asupra afacerii:** Indică situaţia în care serviciul sau funcţionalitatea permite utilizarea şi nu are un impact critic asupra operaţiilor.	Într-un interval de 4 ore de lucru	Orele de lucru L-V

Severitate	Definiţie Severitate	Obiective Timp de Răspuns	Acoperire Timp de Răspuns
4	**Impact minim asupra afacerii:** O întrebare sau o cerere care nu are caracter tehnic	Într-un interval de 1 zi lucrătoare	Orele de lucru L-V

5.1 Accesul la Datele Clientului

IBM va putea să acceseze datele Clientului, în vederea diagnosticării problemelor legate de serviciu şi pentru facilitarea scanărilor aplicaţiei Clientului de către serviciu. IBM va accesa datele numai în scopul remedierii defectelor sau pentru a furniza suport pentru produsele sau serviciile IBM.

6. Termeni Suplimentari pentru Oferta IBM SaaS

Scanările de securitate nu identifică întotdeauna toate riscurile de securitate din aplicaţie şi nu sunt destinate sau concepute pentru utilizarea în medii periculoase, care necesită operarea fără erori, incluzând, dar fără a se limita la, navigarea aeronavelor, sisteme de control al traficului aerian, sisteme militare, sisteme pentru salvarea vieţii, instalaţii nucleare, sau orice alte aplicaţii în care nedetectarea riscurilor de securitate poate cauza decesul, rănirea sau deteriorarea proprietăţii. Nu se garantează că scanările de securitate vor rula fără întreruperi sau fără erori.

IBM SaaS poate fi utilizat pentru a ajuta Clientul să îşi îndeplinească obligaţiile privind conformitatea, care pot fi bazate pe legi, reglementări, standarde sau practici. Indicaţiile, sugestiile de utilizare sau ghidările furnizate de Serviciu nu reprezintă o îndrumare legală, de contabilitate sau alt tip de sfat profesional, iar Clientul este sfătuit să apeleze la propria consiliere legală sau la altă astfel de consiliere expertă. Clientul este singurul responsabil pentru asigurarea faptului că Clientul, activităţile, aplicaţiile şi sistemele lui se conformează tuturor legilor, reglementărilor, standardelor şi practicilor în vigoare. Utilizarea acestui Serviciu nu garantează conformitatea cu legile, reglementările, standardele sau practicile.

IBM SaaS realizează testări invazive şi neinvazive pentru site-ul web şi aplicaţia web sau mobilă pe care Clientul le alege pentru scanare. Anumite legi interzic orice încercare neautorizată de a penetra sau accesa sistemele informatice. Clientul autorizează IBM pentru realizarea Serviciilor după cum este descris aici şi ia la cunoştinţă că Serviciile implică accesul autorizat la sistemele informatice ale Clientului. IBM poate divulga unei terţe părţi această acordare de autoritate, atunci când consideră că este necesar pentru realizarea Serviciilor.

Testarea implică anumite riscuri, incluzând, dar fără a se limita la, următoarele:

a. în timpul rulării aplicaţiilor incluse în testare, este posibil ca sistemele informatice ale Clientului să se blocheze sau să nu mai funcţioneze corespunzător, având ca rezultat indisponibilitatea temporară a sistemelor sau pierderea de date;

b. nivelurile de performanţă şi transfer ale sistemelor Clientului, precum şi ale router-elor şi firewall-urilor asociate, pot suferi o degradare temporară în timpul testării;

c. poate fi generat un volum excesiv de mesaje de istoric, determinând un consum exagerat al spaţiului de disc alocat fişierului istoric;

d. este posibil să fie modificate sau şterse date ca urmare a vulnerabilităţilor testate;

e. pot fi declanşate alarme de către sistemele de detectare a intruziunii;

f. pot fi trimise e-mail-uri prin declanşarea funcţiei de e-mail a aplicaţiei web testate;

g. IBM SaaS poate intercepta traficul reţelei monitorizate, în vederea căutării evenimentelor.

Pe durata oricărei activităţi de testare, nu se aplică remediile şi drepturile contractuale care sunt asigurate de IBM şi au legătură cu site-urile web sau aplicaţiile care fac obiectul testării.

În eventualitatea în care Clientul introduce acreditări de logare autentificate pentru aplicaţia testată în cadrul Serviciului, Clientul ar trebui să introducă astfel de acreditări numai pentru conturile de testare, nu şi pentru utilizatorii de producţie. Utilizarea acreditărilor de utilizator de producţie poate determina transmiterea datelor personale prin intermediul Serviciului.

Se poate configura IBM SaaS pentru scanarea aplicaţiilor web de producţie. Atunci când Clientul setează tipul de scanare la "producţie", serviciul este proiectat să realizeze scanările astfel încât să fie diminuate riscurile prezentate mai sus; totuşi, în anumite situaţii, IBM SaaS poate determina degradarea

performanţei sau instabilitatea site-urilor şi infrastructurii de producţie testate. IBM nu oferă nicio garanţie sau declaraţie privind gradul de adecvare al utilizării IBM SaaS pentru scanarea site-urilor de producţie.

ESTE RESPONSABILITATEA CLIENTULUI DE A DETERMINA DACĂ SERVICIUL ESTE CORESPUNZĂTOR SAU SIGUR PENTRU SITE-UL WEB, APLICAŢIA WEB, APLICAŢIA MOBILĂ SAU MEDIUL TEHNIC AL CLIENTULUI.

IBM SaaS este conceput pentru a identifica o gamă largă de probleme posibile privind securitatea şi conformitatea aplicaţiilor mobile şi web şi a serviciilor web. El nu testează toate vulnerabilităţile sau riscurile legate de conformitate şi nici nu acţionează ca o barieră în calea atacurilor privind securitatea. Ameninţările privind securitatea, reglementările şi standardele se modifică încontinuu, iar Serviciul nu poate reflecta toate aceste modificări. Securitatea şi conformitatea aplicaţiilor web, sistemelor şi angajaţilor Clientului, precum şi orice acţiuni de remediere, reprezintă responsabilitatea exclusivă a Clientului. Ţine exclusiv de decizia Clientului dacă vor fi utilizate sau nu informaţiile furnizate de către Serviciu.

Anumite legi interzic orice încercare neautorizată de a penetra sau accesa sistemele informatice. ESTE RESPONSABILITATEA CLIENTULUI DE A SE ASIGURA CĂ NU UTILIZEAZĂ SERVICIUL PENTRU SCANAREA ALTOR SITE-URI WEB ŞI/SAU APLICAŢII ÎN AFARA SITE-URILOR WEB ŞI/SAU APLICAŢIILOR DEŢINUTE DE CLIENT SAU PENTRU CARE CLIENTUL ARE DREPTUL ŞI AUTORITATEA PENTRU SCANARE.

Pentru claritate, se consideră că şi conţinutul Clientului, descris în secţiunea privind protecţia datelor din Termenii de Utilizare IBM – Termeni Generali, poate include date ce pot deveni accesibile pentru IBM pe durata rulării Application Penetration Testing.

6.1 Sisteme Deţinute de o Terţă Parte

Pentru sistemele (care, pentru scopul acestei prevederi, includ, dar fără a se limita la, aplicaţiile şi adresele IP) ce sunt deţinute de o terţă parte şi fac obiectul testării specificate aici, Clientul este de acord:

a. ca, înainte de iniţierea testării de către IBM pe un sistem terţă parte, Clientul să obţină o scrisoare semnată de la proprietarul fiecărui sistem, care să autorizeze IBM pentru furnizarea Serviciilor pe sistemul respectiv şi să indice acceptarea de către proprietar a condiţiilor specificate în secţiunea intitulată "Permisiunea pentru Realizării Testării", şi să furnizeze către IBM o copie a autorizaţiei respective;

b. să fie singurul responsabil pentru comunicarea către proprietarul sistemului a oricăror riscuri, expuneri şi vulnerabilităţi identificate pe aceste sisteme de către testarea la distanţă realizată de IBM; şi

c. să organizeze şi să faciliteze schimbul de informaţii între proprietarul sistemului şi IBM, după cum consideră IBM că este necesar.

Clientul este de acord:

- să informeze imediat IBM de câte ori se produce o modificare privind proprietatea asupra oricărui sistem care face obiectul testării specificate aici;
- să nu dezvăluie în afara Întreprinderii Clientului livrabilele sau faptul că IBM a realizat Serviciile, decât cu consimţământul scris acordat de IBM în prealabil; şi
- să despăgubească IBM integral pentru orice răspundere sau pierderi ale IBM cauzate de reclamaţii terţă parte legate de nerespectarea de către Client a cerinţelor din această secţiune, intitulată "Sisteme Deţinute de o Terţă Parte", şi pentru orice citaţii sau reclamaţii terţă parte îndreptate împotriva IBM sau a subcontractorilor sau agenţilor IBM şi legate de (a) testarea riscurilor, expunerilor şi vulnerabilităţilor privind securitatea sistemelor care fac obiectul testării specificate aici, (b) furnizarea rezultatelor unei astfel de testări către Client, sau (c) utilizarea sau dezvăluirea de către Client a unor astfel de rezultate.

6.2 Cookie-uri

Clientul este conştient şi acceptă că IBM poate, ca parte a operării normale şi asigurării suportului pentru IBM SaaS, să colecteze informaţii personale de la Client (angajaţii şi contractorii dumneavoastră) privind utilizarea IBM SaaS, prin urmărire şi alte tehnologii. IBM face aceasta pentru a colecta statistici privind utilizarea şi informaţii despre eficienţa IBM SaaS, în vederea îmbunătăţirii experienţei de utilizator şi/sau pentru ajustarea interacţiunilor cu Clientul. Clientul confirmă că va obţine sau va avea consimţământul pentru a permite ca IBM să proceseze informaţiile personale colectate pentru scopul menţionat mai sus, în cadrul IBM, în alte companii IBM şi în cele ale subcontractorilor săi, în care noi sau subcontractorii

noştri ne desfăşurăm activitatea, în conformitate cu legile aplicabile. IBM se va conforma solicitărilor angajaţilor şi contractorilor Clientului privind accesarea, actualizarea, corectarea sau ştergerea informaţiilor lor personale colectate.

Ca parte a IBM SaaS, care include activităţi de raportare, IBM va pregăti şi menţine informaţii făcute anonime şi/sau informaţii agregate, colectate din IBM SaaS (numite "Datele de Securitate"). Datele de Securitate nu vor identifica Clientul sau o persoană individuală, cu excepţia celor specificate la punctul (d) de mai jos. Prin aceasta, Clientul este de acord că IBM poate utiliza şi/sau copia Datele de Securitate numai pentru următoarele scopuri:

a. publicarea şi/sau distribuirea Datelor de Securitate (de exemplu, în compilaţiile şi/sau analizele privind cibersecuritatea);

b. dezvoltarea sau îmbunătăţirea produselor sau serviciilor;

c. derularea căutărilor interne sau terţă parte; şi

d. difuzarea legală a informaţiilor terţă parte confirmate privind autorul.

6.3 Locaţii de Beneficiu Derivate

Când este aplicabil, taxele sunt bazate pe locaţiile pe care Clientul le identifică ca loc unde beneficiază de IBM SaaS. IBM va aplica taxele utilizând adresa de afaceri specificată ca locaţie principală de beneficiu, atunci când se comandă un IBM SaaS, cu excepţia cazului în care IBM primeşte alte informaţii de la Client. Clientul este responsabil pentru păstrarea acestor informaţii şi trimiterea oricărei modificări la IBM.

6.4 Informaţii Personale şi Conţinut şi Servicii Reglementate

Acest IBM SaaS nu este conceput pentru cerinţele de securitate specifice conţinutului reglementat, cum ar fi informaţiile personale sau informaţiile personale sensibile. Clientul este responsabil pentru a determina dacă acest IBM SaaS îndeplineşte cerinţele Clientului privind tipul de conţinut pe care îl utilizează Clientul în legătură cu IBM SaaS.

IBM nu operează ca un furnizor de servicii reglementate de Federal Communications Commission ("FCC") sau autorităţi de reglementare ale statului ("Autorităţile de Reglementare Statale") şi nu intenţionează să furnizeze niciun serviciu care este reglementat de FCC sau Autorităţile de Reglementare Statale. Dacă FCC sau orice Autoritate de Reglementare Statală impune cerinţe sau obligaţii de reglementare pentru orice servicii furnizate de IBM conform celor specificate aici, IBM poate: (a) modifica, înlocui sau schimba produsele, pe cheltuiala Clientului, şi/sau (b) modifica felul în care respectivele servicii subt furnizate Clientului, pentru a evita aplicarea unor astfel de cerinţe sau obligaţii pentru IBM (de exemplu, acţionând ca agent al Clientului pentru achiziţionarea unor astfel de servicii de la un operator comun terţă parte).

Anexa A

1. IBM Application Security on Cloud - Descriere Generală

IBM Application Security on Cloud asigură un loc central pentru asistarea Clientului la identificarea vulnerabilităţilor de securitate (SQL Injection, Cross-Site Scripting şi Data Leakage) pentru diverse aplicaţii. Serviciul include diverse tipuri de scanare a aplicaţiilor, pentru identificarea problemelor de securitate ale aplicaţiei respective.

IBM Application Security on Cloud furnizează următoarele capabilităţi:

- Scanarea aplicaţiilor mobile, pentru depistarea vulnerabilităţilor de securitate. Aceasta este realizată pe baza unor tehnologii de analiză a securităţii dinamice (blackbox) şi interactive (glassbox).
- Scanarea site-urilor Web de producţie sau pre-producţie, cu expunere publică sau în reţea privată, pentru depistarea vulnerabilităţilor de securitate. Aceasta este realizată pe baza unor tehnici de analiză a securităţii dinamice (blackbox).
- Scanarea fluxurilor de date din aplicaţiile Web şi Desktop, pentru depistarea vulnerabilităţilor de securitate. Aceasta este realizată pe baza unor tehnici de analiză a securităţii statice (whitebox).
- Rapoarte detaliate privind vulnerabilităţile de securitate, care includ atât sumare de nivel înalt ale rezultatelor, cât şi paşii pe care dezvoltatorii îi pot parcurge pentru remediere.
- Integrarea cu diverse platforme DevOps

1.1 IBM Application Analyzer

IBM Application Analyzer poate fi comandat per Instanţă de Aplicaţie, per Job (scanare) sau ca Instanţă completă şi permite următoarele tipuri de scanare:

- Dynamic Analyzer – Testaţi site-urile web de pre-producţie sau producţie prin tehnici DAST
- Mobile Analyzer – Testaţi binarele iOS sau Android prin tehnici IAST
- Static Analyzer – Testaţi fluxul de date bytecode sau cod sursă prin tehnici SAST

1.2 Serviciu de Setare

IBM Application Security on Cloud Consulting Services este un serviciu de setare comercializat pentru Application Analyzer. Serviciul utilizează consultanţi IBM pentru a furniza indicaţii şi asistenţă la testarea şi gestionarea riscurilor privind aplicaţiile. IBM Application Security on Cloud Consulting Services este cumpărat ca blocuri de angajamente, ce pot fi utilizate în cantităţile specificate mai jos, pentru a solicita şi a utiliza următoarele servicii specifice:

a. **Fast Start** [Utilizează o (1) unitate Angajament]

Serviciul Fast Start furnizează expertiză şi indicaţii pentru utilizarea caracteristicilor Application Security on Cloud de testare şi gestionare a riscurilor. După ce Clientul a confirmat logarea cu succes la portalul Application Security on Cloud, IBM va facilita o conferinţă web de până la două (2) ore şi cu doi (2) participanţi activi, pentru instruirea privind configuraţiile şi funcţiile AppSec on IBM SaaS de bază, incluzând tipurile de scanare, rularea scanărilor, examinarea rapoartelor şi instalarea instrumentelor şi plug-in-urilor asociate. Serviciul Fast Start este finalizat după ce se finalizează (a) webinar-ul pentru instruirea clientului, (b) instalarea instrumentelor şi plug-in-urilor aplicabile şi (c) setarea asistată şi rularea primei scanări a Clientului.

b. **Assessment Review** [Utilizează două (2) unităţi Angajament]

Serviciul Assessment Review furnizează asistenţă pentru examinarea rezultatului unei testări, inclusiv pentru înţelegerea şi stabilirea priorităţii remedierii vulnerabilităţilor din aplicaţie. IBM va facilita o conferinţă web de până la o (1) oră şi cu doi (2) participanţi activi, pentru a furniza o privire de ansamblu asupra vulnerabilităţilor găsite şi riscurilor de securitate ale aplicaţiei şi pentru o discuţie detaliată privind vulnerabilităţile de securitate găsite, incluzând (1) modul în care a fost testată vulnerabilitatea, (2) modul în care a fost detectată vulnerabilitatea, (3) care este riscul cauzat de fiecare vulnerabilitate şi (4) recomandări generale privind corecţia, pentru a ajuta la remedierea vulnerabilităţii. Examinarea va acoperi numai rezultatul testării, nu şi codul sursă propriu-zis. Înainte de iniţierea conferinţei web, Clientul va examina şi va identifica rezultatul testării pentru IBM, în

vederea examinării. Serviciul Assessment Review este finalizat după ce se finalizează conferinţa web.

c. **Scan for Me** [Utilizează patru (4) unităţi Angajament]

Serviciul Scan for Me asigură un expert IBM în securitatea aplicaţiilor, care va configura şi va rula o scanare, va valida rezultatele şi va conduce o întrunire de raportare, pentru trecerea în revistă a problemelor descoperite. Clientul îi va permite unui consultant IBM să-i acceseze mediul ASoC, pentru configurarea şi rularea scanării, validarea rezultatelor, furnizarea recomandărilor privind prioritatea remedierii şi conducerea unei întruniri de raportare a rezultatelor. IBM va facilita o conferinţă web de până la o (1) oră şi cu doi (2) participanţi activi, pentru a furniza o privire de ansamblu asupra vulnerabilităţilor găsite şi riscurilor de securitate ale aplicaţiei şi pentru o discuţie detaliată privind vulnerabilităţile de securitate găsite, incluzând (1) modul în care a fost testată vulnerabilitatea, (2) modul în care a fost detectată vulnerabilitatea, (3) care este riscul cauzat de fiecare vulnerabilitate şi (4) recomandări generale privind corecţia, pentru a ajuta la remedierea vulnerabilităţii. La cerere şi după cel mult 30 de zile de la scanarea iniţială, IBM va asigura o rescanare, utilizând configuraţia de scanare iniţială, numai pentru verificarea corecţiilor de securitate, nu şi pentru testarea noii funcţionalităţi, validarea rezultatelor şi furnizarea unui raport către client. Serviciul Scan for Me este finalizat după ce se finalizează conferinţa web pentru rezultatele scanării iniţiale sau, dacă este cazul, după ce se finalizează rescanarea solicitată de Client şi furnizarea către Client a raportului de rescanare.

d. **Advisor on Demand** [Utilizează şapte (7) unităţi Angajament]

Serviciul Advisor on Demand asigură până la douăzeci (20) de ore de acces la un consultant IBM, pentru activităţi asociate cu IBM SaaS. Consultantul IBM va asigura asistenţă pentru subiecte specifice securităţii aplicaţiilor, incluzând, dar fără a se limita la, gestionarea programelor, stabilirea priorităţilor de testare a securităţii, strategiile de remediere, analizarea codului sursă şi repararea codului sursă. IBM va colabora cu Clientul pentru a înţelege şi a crea o planificare de proiect cu cerinţele specifice Clientului, incluzând obiectivele proiectului, tehnologiile relevante, diagramele de timp dorite, livrabilele aşteptate şi numărul estimat de angajamente de serviciu Advisor on Demand. Clientul trebuie să asigure accesul la aplicaţiile, sistemele şi documentaţia necesare pentru realizarea serviciilor. Serviciul Advisor on Demand este finalizat după asigurarea a până la 20 de ore de expertiză în securitate şi/sau după planificarea proiectului şi/sau după furnizarea către Client a livrabilelor definite în planificarea proiectului.

e. **Application Penetration Testing**

Trei opţiuni:

(1) **Compliance/Entry-Level Application Penetration Test**, care include până la patruzeci (40) de ore de Consultant şi se axează pe probleme de logică cu un singur pas şi probleme de injecţie mai simple. Utilizează cincisprezece (15) unităţi Angajament.

(2) **Standard Application Penetration Test**, care include până la şaizeci (60) de ore de Consultant şi extinde domeniul testării la probleme de logică din fluxuri de lucru cu mai mulţi paşi, probleme de injecţie complexe şi analiza unor tipuri de date complexe. Utilizează douăzeci şi una (21) de unităţi Angajament.

(3) **Advanced Application Penetration Test** – Asigură până la optzeci (80) de ore de Consultant şi extinde domeniul testării la ingineria inversă a executabilelor compilate, analiza protocoalelor de reţea personalizate, analiza aprofundată a bibliotecilor şi cadrelor de lucru disponibile în mod public. Utilizează douăzeci şi şapte (27) de unităţi Angajament.

Serviciul Application Penetration Test furnizează o resursă IBM pentru realizarea testării şi explorării unei aplicaţii, livrarea unui raport de testare şi o scurtă întrunire de raportare pentru explicarea problemelor descoperite şi a riscurilor asociate.

IBM va facilita un apel de iniţiere a proiectului de până la o (1) oră şi cu doi (2) participanţi activi, pentru examinarea mediului şi organizaţiei Clientului, incluzând platforma aplicaţiei, arhitectura, cadrele de lucru, infrastructura de suport, preocupările şi problemele de securitate cunoscute privind aplicaţia, planificarea de testare preliminară şi planul de contactare în caz de urgenţă.

IBM va conduce realizarea testării privind penetrarea aplicaţiei, incluzând, dar fără a se limita la: identificarea vulnerabilităţilor comune, cum ar fi SQL Injection şi Cross-Site Scripting, evaluarea punctelor tari şi slabe ale controalelor de securitate existente, cum ar fi validarea, autentificarea şi autorizarea intrării, verificarea aplicării corespunzătoare a logicii operaţionale, validarea utilizării

corespunzătoare a protocoalelor sigure, identificarea problemelor de manipulare a sesiunii şi verificarea controalelor de securitate corespunzătoare pentru logare, recuperarea parolei, politica de parole şi alte funcţii de gestionare a utilizatorilor. Problemele descoperite vor fi documentate în Application Penetration Test Report. IBM va facilita o conferinţă web pentru prezentarea raportului, de până la o (1) oră. Serviciul Application Penetration Test este finalizat după utilizarea timpului de consultanţă alocat, terminarea conferinţei web şi livrarea către Client a documentului final Application Penetration Test Report.

1.2.1 Responsabilităţile pentru Serviciile de Setare

IBM:

- va furniza Serviciile de Setare utilizând unităţile Angajament cumpărate de Client şi per POE; şi
- va finaliza un Serviciu de Setare când sunt realizate criteriile de finalizare descrise în Secţiunea 1.2.

Clientul este de acord:

- să fie responsabil pentru toate tarifele asociate cu toate cererile de Angajament realizate de Client pe durata termenului contractual;
- că unităţile Angajament trebuie să fie utilizate pe durata termenului contractual şi că, dacă nu sunt utilizate, acestea expiră la data de sfârşit a perioadei contractului; şi
- să iniţieze o cerere oficială pentru toate Serviciile de Setare, cu cel puţin 30 de zile înainte de data de sfârşit a abonamentului.

Pe durata realizării oricărui Serviciu de Setare, IBM îi poate solicita Clientului informaţii şi colaborarea la un nivel rezonabil. În cazul în care Clientul nu furnizează informaţiile cerute sau nu asigură colaborarea în timp util, după cum stabileşte IBM, pot fi aplicate tarife de unitate de Angajare impuse de servicii sau întârzieri la realizarea serviciului aplicabil.

Pentru a se asigura acurateţea testării realizate de IBM, Clientul este de acord să urmeze instrucţiunile IBM privind pregătirea şi menţinerea mediului pe durata perioadei de testare.