IBM Application Security on Cloud

Vilkår for brug består af disse IBM Vilkår for brug – SaaS-specifikke produktvilkår (kaldet SaaS-specifikke produktvilkår) og dokumentet IBM Vilkår for brug – Standardvilkår (kaldet Standardvilkår), som er tilgængeligt på adressen http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

I tilfælde af en uoverensstemmelse har de SaaS-specifikke produktvilkår forrang for Standardvilkårene. Ved at bestille, tilgå eller benytte IBM SaaS-produktet accepterer Kunden disse Vilkår for brug.

Disse Vilkår for brug er reguleret af IBM International Passport Advantage-Aftalen, IBM International Passport Advantage Express-Aftalen eller IBM International Aftale om Udvalgte IBM SaaS-produkter (hver især kaldet Aftalen), som sammen med Vilkår for brug udgør den fuldstændige aftale.

1. IBM SaaS

De SaaS-specifikke produktvilkår dækker følgende IBM SaaS-produkter:

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

2. Måletyper for betaling

IBM SaaS-produktet sælges og betales på basis af en af følgende målinger, som angivet i Transaktionsdokumentet:

a. **Job (Job)** – er en måleenhed, som IBM SaaS-produktet kan anskaffes på basis af. Et Job er et objekt i IBM SaaS-produktet, som ikke kan opdeles yderligere, og som repræsenterer en beregningsproces, inklusive alle underprocesser. Kunden skal anskaffe tilstrækkeligt mange beviser for brugsret til at kunne dække det samlede antal Job, som behandles eller håndteres af IBM SaaS-produktet i den måleperiode, der er angivet i Kundens bevis for brugsret eller i Transaktionsdokumentet.

b. **Applikationsforekomst (Application Instance)** – er en måleenhed, som IBM SaaS-produktet kan anskaffes på basis af. Der kræves en brugsret af typen Applikationsforekomst for hver forekomst af en Applikation, som er knyttet til IBM SaaS-produktet. Hvis en Applikation har flere komponenter, og hver af disse tjener et bestemt formål og/eller en bestemt brugerbasis og kan tilknyttes eller administreres af IBM SaaS-produktet, betragtes hver af disse komponenter som en separat Applikation. Derudover betragtes hvert test-, udviklings- og produktionsmiljø for en Applikation som en separat forekomst af Applikationen, og der skal være anskaffet en brugsret til hvert miljø. Flere Applikationsforekomster i et enkelt miljø betragtes som separate forekomster af Applikationen, og hver forekomst skal være dækket af en brugsret. Kunden skal anskaffe tilstrækkeligt mange brugsrettigheder til at kunne dække det antal Applikationsforekomster, som er tilknyttet IBM SaaS-produktet i den måleperiode, der er angivet i Kundens bevis på brugsret eller i Transaktionsdokumentet.

   Følgende gælder dette IBM SaaS-produkt:

   - Til Dynamisk Test: Et websted, der kan nås via en offentlig eller privat URL-adresse. Hver enkelt Applikationsforekomst giver ret til et websted på op til 1.000 sider i ét enkelt domæne.
   - Til Statisk Test: En kodeenhed, der kan udføres på ét enkelt programmeringssprog. Hver enkelt Applikationsforekomst giver ret til scanning af kodeenheder på op til 1.000.000 linjer.
   - Til Mobil Test: En binær kodeenhed, der kan udføres på en mobil enhed. Hver enkelt mobil platform (f.eks. IOS og Android) udgør en separat Applikationsforekomst.

c. **Forekomst (Instance)** – er en måleenhed, som IBM SaaS-produktet kan anskaffes på basis af. Ved Forekomst forstås en adgang til en specifik IBM SaaS-konfiguration. Kunden skal anskaffe tilstrækkeligt mange brugsrettigheder for hver Forekomst af IBM SaaS-produktet, der stilles til rådighed, til at kunne dække adgang og brug i den måleperiode, der er angivet i Kundens bevis for brugsret eller i Transaktionsdokumentet.

   For hver brugsret af typen Forekomst gælder det, at der ingen grænse er for antallet af udførte Job eller Applikationsforekomster. Dog kan der ikke udføres mere end 30 job samtidigt på et givet tidspunkt.

d. **Engagement (Engagement)** – er en måleenhed, som serviceydelserne kan anskaffes på basis af. Et Engagement består af faglige og/eller uddannelsesmæssige serviceydelser, som vedrører IBM SaaS-produktet. Kunden skal anskaffe tilstrækkeligt mange brugsrettigheder til at kunne dække hvert Engagement.

3. Pris og fakturering

Det beløb, der skal betales for IBM SaaS-produktet, er angivet i et Transaktionsdokument.

3.1 Betaling for del af måned

Betaling for en del af en måned, som angivet i Transaktionsdokumentet, kan opgøres forholdsvist.

3.2 Betaling for merforbrug

Hvis den faktiske brug af IBM SaaS-produktet i måleperioden overstiger den brugsret, som er angivet i beviset for brugsret, bliver Kunden opkrævet betaling for merforbruget, som angivet i Transaktionsdokumentet.

3.3 Betaling for opsætning

Kunden faktureres for opsætning som angivet i Transaktionsdokumentet.

4. Varighed og fornyelse

IBM SaaS-perioden begynder den dato, hvor IBM giver Kunden besked om, at Kunden har adgang til IBM SaaS-produktet, som beskrevet i beviset for brugsret. Beviset for brugsret angiver, om IBM SaaS-produktet fornyes automatisk, fortsætter løbende eller ophører ved udgangen af aftaleperioden.

Ved automatisk fornyelse: Medmindre Kunden mindst 30 dage inden periodens udløbsdato informerer IBM om ikke at forny aftaleperioden, fornys IBM SaaS-produktet automatisk for den periode, der er angivet i beviset for brugsret.

Ved løbende brug: IBM SaaS-produktet vil fortsat være tilgængeligt på månedsbasis, indtil Kunden med 30 dages skriftligt varsel til IBM bringer aftalen til ophør. IBM SaaS-produktet vil være tilgængeligt indtil udgangen af den kalendermåned, der følger efter en sådan 30-dages periode.

5. Teknisk support

I Abonnementsperioden og efter, at IBM har informeret Kunden om, at Kunden har adgang til IBM SaaS-produktet, leveres teknisk support via onlineforummer og som standardsupport i den periode, hvor Kunden betaler efter forbrug. Kunden kan sende en problemrapport inde fra IBM SaaS eller åbne en chatsession for at få hjælp. IBM stiller IBM Software as a Service Support Handbook til rådighed, som indeholder kontaktoplysninger til brug ved teknisk support og supportprocesser.

Problemklassificering	Definition af problemklassificering	Målsætninger for reaktionstider	Dækning – reaktionstid
1	**Funktion/serviceydelse med central indvirkning på forretningen er nede:** En central forretningsfunktion er ude af drift, eller der er fejl på en central grænseflade. Det gælder sædvanligvis et produktionsmiljø og angiver manglende adgang til serviceydelser, hvilket resulterer i en væsentlig påvirkning af driften. Tilstanden kræver en øjeblikkelig løsning.	Inden for 1 time	24 x 7
2	**Betydelig indvirkning på forretningen:** Der er en alvorlig brugsbegrænsning i en forretningsfunktion i serviceydelsen, eller der er risiko for, at tidsfrister ikke overholdes.	Inden for 2 arbejdstimer	Mandag – fredag i arbejdstiden
3	**Mindre indvirkning på forretningen:** Angiver, at serviceydelsen eller funktioner kan benyttes, og der er ingen alvorlig påvirkning af driften.	Inden for 4 arbejdstimer	Mandag – fredag i arbejdstiden
4	**Minimal indvirkning på forretningen:** En forespørgsel eller ikke-teknisk anmodning	Inden for 1 arbejdsdag	Mandag – fredag i arbejdstiden

5.1 Adgang til kundedata

IBM kan få adgang til kundedata for at identificere problemer med serviceydelsen og for at gøre det nemmere for serviceydelsen at scanne Kundens applikation. IBM tilgår kun data med det formål at rette fejl eller levere support til IBM-produkter eller -serviceydelser.

6. Tillægsvilkår for IBM SaaS

Sikkerhedsscanninger identificerer muligvis ikke alle sikkerhedsrisici i en applikation, og de er heller ikke designet eller beregnet til brug i farlige miljøer, som kræver fejlfri afvikling, herunder for eksempel flynavigation, flytrafikkontrolsystemer, våbensystemer, livredningssystemer, atomare anlæg eller enhver anden anvendelse, hvor manglende identifikation af sikkerhedsrisici kan føre til dødsfald, personskade eller beskadigelse af ejendom. Det er ikke garanteret, at sikkerhedsscanninger fungerer uafbrudt eller fejlfrit.

IBM SaaS-produktet kan bruges til at hjælpe Kunden med at overholde lovgivning, bestemmelser, standarder og praksis. Vejledning, retningslinjer og oplysninger om foreslået brug, der leveres i Serviceydelsen, udgør ikke juridisk, regnskabsmæssig eller anden form for professionel rådgivning, og Kunden tilrådes at indhente sin egen juridiske rådgivning eller ekspertrådgivning. Kunden er eneansvarlig for at sikre, at Kunden og Kundens aktiviteter, applikationer og systemer overholder alle gældende love, bestemmelser, standarder og gældende praksis. Brug af denne Serviceydelse garanterer ikke overholdelse af nogen love, bestemmelser, standarder eller praksis.

IBM SaaS-produktet udfører invasive såvel som ikke-invasive test på det websted og den web- eller mobilapplikation, som Kunden vælger at scanne. Visse love forbyder ethvert uautoriseret forsøg på at trænge ind i et IT-system. Kunden giver IBM tilladelse til at levere de Serviceydelser, der er beskrevet i denne Servicebeskrivelse, og bekræfter, at Serviceydelserne udgør en autoriseret adgang til Kundens IT-systemer. IBM har ret til at videregive oplysninger om denne tilladelse til en tredjepart, hvis IBM skønner, at det er nødvendigt for at levere Serviceydelserne.

Testen medfører visse risici, herunder for eksempel:

a. Kundens IT-systemer kan - når applikationer afvikles under test - komme til at hænge eller gå ned, hvorved systemet midlertidigt bliver utilgængeligt, eller data kan gå tabt.

b. Ydeevnen på Kundens systemer og ydeevnen af tilknyttede routere og firewalls kan blive midlertidigt reduceret under testen.

c. Der kan blive genereret mange logmeddelelser, og logfilerne kan optage meget diskplads.

d. Data kan blive ændret eller slettet som følge af undersøgelsen af sårbarheder.

e. Systemer til registrering af indtrængen kan udløse alarmer.

f. E-mail kan udløses af e-mailfunktionen i den webapplikation, der testes.

g. IBM SaaS-produktet kan medføre, at trafikken på det overvågede netværk analyseres med henblik på at spore begivenheder.

Enhver rettighed, der gælder ifølge servicemålaftaler, eller misligholdelsesbeføjelse, der stilles til rådighed af IBM, og som vedrører de websteder eller applikationer, der testes, frafaldes af Kunden under testaktiviteterne.

Hvis Kunden angiver validerede logonoplysninger i Serviceydelsen for den applikation, der testes, skal Kunden kun angive sådanne oplysningerne for testkonti, ikke for brugere af produktionssystemet. Brug af valideringsoplysninger for brugere af produktionssystemet kan betyde, at personoplysninger overføres via Serviceydelsen.

IBM SaaS-produktet kan konfigureres til at scanne webapplikationer i produktion. Hvis Kunden angiver scanningstypen til "produktion", er serviceydelsen designet til at scanne på en måde, som mindsker de ovenfor anførte risici. I visse situationer kan IBM SaaS-produktet betyde, at systemets ydeevne reduceres, eller at systemet bliver ustabilt på de testede produktionssteder og den testede infrastruktur. IBM garanterer ikke og fremsætter ingen erklæringer med hensyn til relevansen af at bruge IBM SaaS-produktet til at scanne produktionssteder.

Det er Kundens ansvar at fastslå, om det er fornuftigt eller sikkert i forhold til Kundens websted, webapplikation, mobilapplikation eller Kundens tekniske miljø at benytte Serviceydelsen.

IBM SaaS-produktet er designet til at kunne identificere en lang række mulige sikkerhedsproblemer og problemer med overholdelse af regler og lovgivning i mobile applikationer og webapplikationer og

webserviceprogrammer. Det tester ikke alle sårbarheder eller risici i forbindelse med overholdelse af regler og lovgivning, ligesom det heller ikke beskytter mod angreb. Sikkerhedstrusler, bestemmelser og standarder skifter hele tiden, og serviceydelsen afspejler måske ikke alle disse ændringer. Det er alene Kundens ansvar at sørge for, at Kundens webapplikation, systemer og medarbejdere er sikrede og overholder regler og lovgivning, ligesom det alene er Kundens ansvar at træffe afhjælpende foranstaltninger. Det er helt op til Kunden selv at afgøre, om Kunden vil benytte de oplysninger, som Serviceydelsen tilbyder.

Visse love forbyder ethvert uautoriseret forsøg på at trænge ind i et IT-system. Det er Kundens ansvar at sikre, at Kunden ikke benytter Serviceydelsen til at scanne andre websteder og/eller applikationer end websteder og/eller applikationer, som ejes af Kunden, eller som Kunden har ret og autorisation til at scanne.

For præcisionens skyld anses Kundeindhold, som er beskrevet i afsnittet om databeskyttelse i IBM Vilkår for Brug - Standardvilkår, for at omfatte data, der kan blive tilgængelige for IBM under Application Penetration-test.

6.1 Systemer, som ejes af tredjepart

For så vidt gælder systemer (som i nærværende bestemmelse omfatter for eksempel applikationer og IP-adresser) ejet af tredjepart, som vil være genstand for test i henhold til disse Vilkår for brug, er Kunden indforstået med:

a. at inden IBM påbegynder test på et tredjepartssystem, skal Kunden indhente et underskrevet brev fra ejeren af hvert enkelt system, som bemyndiger IBM til at levere Serviceydelserne på det pågældende system, og som angiver, at ejeren accepterer de bestemmelser, der er anført i afsnittet Permission to Perform Testing". Kunden skal give IBM en kopi af denne bemyndigelse.

b. at være eneansvarlig for at informere systemets ejer om de risici og sårbarheder, som IBM's fjernudførte test afslører på disse systemer.

c. Kunden skal arrangere og muliggøre informationsudvekslingen mellem systemejeren og IBM, i det omfang IBM skønner det nødvendigt.

Kunden er indforstået med:

- omgående at informere IBM om et eventuelt ejerskifte for et system, der er genstand for test ifølge dette dokument.
- ikke at videregive oplysninger om leverancerne eller det faktum, at IBM udførte Serviceydelserne, uden for Kundens virksomhed uden IBM's forudgående skriftlige tilladelse, og
- at holde IBM fuldt ud skadesløs i forbindelse med alle tab eller ethvert ansvar, der skyldes Kundens manglende opfyldelse af kravene i dette afsnit "Systemer, som ejes af tredjepart", og tredjepartskrav, som måtte blive rejst mod IBM, IBM's underleverandører eller partnere som følge af (a) test af sikkerhedsrisici og sårbarheder på de systemer, der er genstand for test i henhold til disse Vilkår for brug, (b) levering af testresultaterne til Kunden eller (c) Kundens brug eller videregivelse af disse resultater.

6.2 Cookies

Kunden er opmærksom på og indforstået med, at IBM – som del af den normale drift og support af IBM SaaS-produktet – via sporing eller andre teknologier indsamler personoplysninger fra Kunden (Kundens medarbejdere og kontraktansatte), som vedrører brugen af IBM SaaS-produktet. Det sker for at indsamle brugsstatistik og oplysninger om effektiviteten af IBM SaaS med det formål at forbedre brugeroplevelsen og/eller at skræddersy kommunikationen med Kunden. Kunden bekræfter, at Kunden vil indhente eller har indhentet samtykke til, at IBM kan behandle de indsamlede personoplysninger til ovenstående formål i IBM, andre IBM-virksomheder og disses underleverandører, uanset hvor IBM og IBM's underleverandører driver forretning, og i henhold til gældende lovgivning. IBM vil efterkomme anmodninger fra Kundens medarbejdere og kontraktansatte om adgang til, opdatering, ændring eller sletning af de indsamlede personoplysninger.

IBM vil som del af det IBM SaaS-produkt, der inkluderer rapporteringsaktiviteter, forberede og vedligeholde afidentificerede og/eller sammenfattede informationer, som er indsamlet fra IBM SaaS-produktet (kaldet Sikkerhedsdata). Sikkerhedsdataene identificerer ikke Kunden eller enkeltpersoner, medmindre det er angivet under (d) nedenfor. Kunden accepterer yderligere, at IBM må bruge og/eller kopiere Sikkerhedsdata til følgende og udelukkende til følgende formål:

a. publicering og/eller distribution af Sikkerhedsdata (f.eks. i kompileringer og/eller analyser, som vedrører cybersikkerhed).

b. udvikling eller udvidelse af produkter eller serviceydelser.

c. forskningsaktiviteter internt eller sammen med tredjeparter og

d. lovlig deling af oplysninger om bekræftede uvedkommende tredjepartspersoner.

6.3 Lokaliteter med afledte fordele (Derived Benefit)

Hvor det er relevant, baseres skatter og afgifter på den eller de lokationer, Kunden identificerer som værende den eller de lokationer, der modtager fordelen ved IBM SaaS-produktet. IBM inkluderer skatter og afgifter på basis af den forretningsadresse, Kunden anfører som primær fordelslokalitet ved bestilling af et IBM SaaS-produkt, medmindre Kunden informerer IBM om andet. Det er Kundens ansvar at sørge for, at oplysningerne er opdateret og at informere IBM om eventuelle ændringer.

6.4 Personoplysninger og Reguleret Indhold og Serviceydelser

Dette IBM SaaS-produkt er ikke designet til at overholde specifikke sikkerhedskrav for reguleret indhold, for eksempel personoplysninger eller følsomme personoplysninger. Det er Kundens ansvar at afgøre, om dette IBM SaaS-produkt opfylder Kundens behov, for så vidt angår den type indhold, Kunden bruger sammen med IBM SaaS-produktet.

IBM opererer ikke som leverandør af serviceydelser, der reguleres af US FCC (Federal Communications Commission) eller amerikanske delstaters reguleringsmyndigheder (Delstatsmyndigheder), og har ikke til hensigt at levere sådanne serviceydelser, der reguleres af FCC eller Delstatsmyndigheder. Hvis FCC eller en Delstatsmyndighed pålægger lovbestemte krav eller forpligtelser i forbindelse med de serviceydelser, som IBM leverer i henhold til disse Vilkår for brug, kan IBM: (a) ændre, erstatte eller udskifte produkter for Kundens regning og/eller (b) ændre den måde, som Kunden får leveret serviceydelserne på, for at undgå at IBM pålægges sådanne krav eller forpligtelser (f.eks. ved at fungere som Kundens agent med henblik på at anskaffe sådanne serviceydelser fra en tredjepartskommunikationsvirksomhed).

Bilag A

1. Generel beskrivelse af IBM Application Security on Cloud

IBM Application Security on Cloud tilbyder ét centralt sted, hvor Kunden kan få hjælp til at identificere sikkerhedssårbarheder (f.eks. SQL Injection, Cross-Site Scripting og Data Leakage) for forskellige applikationer. Serviceydelsen inkluderer forskellige teknikker til sikkerhedsscanning af applikationer, og hver tekniktype identificerer sikkerhedsproblemer i den specifikke applikation.

IBM Application Security on Cloud tilbyder følgende funktioner:

- Scanning af mobilapplikationer for sikkerhedssårbarheder. Det sker via teknikker til dynamisk (blackbox) og interaktiv (glassbox) sikkerhedsanalyse.
- Scanning af produktions- og præproduktionswebsteder, netværk vendt mod offentligheden eller private netværk og scanning af websteder for sikkerhedssårbarheder. Det sker via en teknik til dynamisk (blackbox) sikkerhedsanalyse.
- Scanning af datastrømme i web- og skrivebordsapplikationer for sikkerhedssårbarheder. Det sker via en teknik til statisk (whitebox) sikkerhedsanalyse.
- Detaljerede rapporter om sikkerhedssårbarheder, som både inkluderer overordnede oversigter over resultaterne og en beskrivelse af, hvad udviklerne kan gøre for at afhjælpe sårbarhederne.
- Integrering med forskellige DevOps-platforme.

1.1 IBM Application Analyzer

IBM Application Analyzer kan bestilles pr. Applikationsforekomst, pr. Job (scanning) eller som en fuld Forekomst og giver mulighed for følgende scanningstyper:

- Dynamic Analyzer – Test præproduktions eller produktionswebsteder via DAST-teknikker
- Mobile Analyzer – Test iOS eller Android binært via IAST-teknikker
- Static Analyzer – Test byte- eller kildekodedataflow via SAST-teknikker

1.2 Opsætningsservice

IBM Application Security on Cloud Consulting Services er en "produktificeret" serviceydelse til Application Analyzer. Serviceydelsen bruger IBM-konsulenter til at yde vejledning og hjælp til test og styring af applikationsrisikoen. IBM Application Security on Cloud Consulting Services købes som blokke af Engagementer, der kan bruges i de mængder, der er angivet nedenfor, til at anmode om og gøre brug af følgende specifikke serviceydelser:

a. **Fast Start** [Bruger én Engagements-enhed]

Serviceydelsen Fast Start sikrer ekspertise og vejledning til brug af Application Security on Cloud-funktioner til test og risikostyring. Når Kunden bekræftet login til Application Security on Cloud-portalen, vil IBM forestå et webmøde i op til to timer og med to aktive deltagere for at uddanne deltagerne i grundlæggende applikationssikkerhed på IBM SaaS-konfigurationer og -funktioner, herunder scanningstyper, kørsel af scanninger, gennemgang af rapporter og installation af relaterede værktøjer og plug-in-programmer. Fast Start-serviceydelsen gennemføres efter gennemførelsen af (a) kundeuddannelseswebinar, (b) installation af relevante værktøjer og plug-in-programmer og (c) hjælp til Kunden med opsætning og kørsel af Kundens første scanning.

b. **Assessment Review** [Bruger to Engagements-enheder]

Serviceydelsen Assessment Review yder hjælp til gennemgang af et testresultat, herunder forståelse og prioritering af afhjælpning af sårbarheder i applikationen. IBM vil forestå et webmøde i op til en time og for op til to aktive deltagere for at give en oversigt over de fundne sårbarheder og applikationens samlede sikkerhedsrisiko samt en grundig gennemgang af de fundne sikkerhedssårbarheder i applikationen, herunder (1) hvordan sårbarheden blev testet, (2) hvordan sårbarhederne blev registreret, (3) hvad er risikoen i forbindelse med hver enkelt sårbarhed og (4) give en generel anbefaling til en løsning for at bidrage til afhjælpning af sårbarheden. Gennemgangen vil være baseret på testresultatet, den vil ikke være en gennemgang af selve kildekoden. Kunden gennemgår testresultatet og identificerer over for IBM, hvilket testresultat det

drejer sig om inden webmødet. Serviceydelsen Assessment Review gennemføres efter afholdelsen af webmødet.

c. **Scan for Me** [Bruger fire Engagements-enheder]

Serviceydelsen Scan for Me omfatter en IBM-applikationssikkerhedsekspert, der konfigurerer og kører en scanning, validerer resultaterne og afholder en rapportorientering for at gennemgå resultaterne. Kunden giver en IBM-konsulent adgang til sit ASoC-miljø, så konsulenten kan konfigurere og køre en scanning, validere resultaterne, give anbefalinger om prioritering af afhjælpning og afholde en rapportorientering om resultaterne. IBM vil forestå et webmøde i op til en time og for op til to aktive deltagere for at give en oversigt over de fundne sårbarheder og applikationens samlede sikkerhedsrisiko samt en grundig gennemgang af de fundne sikkerhedssårbarheder i applikationen, herunder (1) hvordan sårbarheden blev testet, (2) hvordan sårbarhederne blev registreret, (3) hvad er risikoen i forbindelse med hver enkelt sårbarhed og (4) give en generel anbefaling til en løsning for at bidrage til afhjælpning af sårbarheden. Op til 30 dage efter den første scanning vil IBM, hvis Kunden anmoder om det, foretage en ny scanning med en oprindelig scanningskonfiguration for at kontrollere sikkerhedsrettelser, men ikke for at teste ny funktionalitet, validere resultaterne og levere rapporten til Kunden. Serviceydelsen Scan for Me gennemføres efter afholdelsen af webmødet for at gennemgå resultaterne fra den første scanning eller, hvis det er relevant, gennemførelsen af en ny scanning, som Kunden har anmodet om, og levering af rapporten om den nye scanning til Kunden.

d. **Advisor on Demand** [Bruger syv Engagements-enheder]

Serviceydelsen Advisor on Demand omfatter op til tyve timer af en IBM-konsulents tid, som kan bruges til aktiviteter i forbindelse med IBM SaaS-produktet. IBM-konsulenten hjælper med specifikke emner i forbindelse med applikationssikkerhed, herunder f.eks. programstyring, prioritering af sikkerhedstest, afhjælpningsstrategier samt analyse og reparation af kildekode. IBM arbejder sammen med Kunden for at forstå og udarbejde en projektplan med specifikke Kundekrav, herunder projektmål, relevante teknologier, ønskede frister, forventede leverancer og anslået antal Engagementer for Serviceydelsen Advisor on Demand. Kunden skal sikre adgang til nødvendige applikationer, systemer og dokumentation, som er påkrævet for at udføre serviceydelserne. Serviceydelsen Advisor on Demand er gennemført, når op til 20 timers sikkerhedsekspertise er blevet udført, og/eller efter at projektplanen og/eller de dokumenterede leverancer i projektplanen er blevet leveret til Kunden.

e. **Application Penetration Test**

Tre muligheder:

(1) **Compliance/Entry-Level Application Penetration Test**, som omfatter op til fyrre timers konsulenttid og fokuserer på logiske enkelttrinsfejl og enklere versioner af injektionsfejl. Bruger femten Engagements-enheder.

(2) **Standard Application Penetration Test**, som omfatter op til tres timers konsulenttid og udvider fokus til at omfatte logiske fejl i flertrinsarbejdsgange, komplekse versioner af injektionsfejl og analyse af komplekse datatyper. Bruger enogtyve Engagements-enheder.

(3) **Advancerec Applikation Penetration Test**, som omfatter op til firs timers konsulenttid og udvider fokus til at omfatte reverse engineering af kompilerede eksekverbare filer, dissekering af brugertilpassede netværksprotokoller, dybgående analyse af offentligt tilgængelige biblioteker og strukturer. Bruger syvogtyve Engagements-enheder.

Application Penetration-testserviceydelsen omfatter en IBM-ressource, der udfører test og udnyttelse af en applikation, levering af en testrapport og en rapportgennemgang til forklaring af resultaterne og dermed forbundne risici.

IBM forestår et indledende projektopkald i op til en time og med op til to aktive deltagere til gennemgang af Kundens miljø og organisation, herunder applikationsplatform, arkitektur, strukturer, understøttende infrastruktur, kendte sikkerhedsproblemer eller bekymringer i forbindelse med applikationen, foreløbig testplan og plan for kontakt i nødsituationer.

IBM gennemfører Applikation Penetration-testen, herunder f.eks.: Identificering af almindelige sårbarheder såsom SQL-injektion og scripting på tværs af websteder, vurdering af styrker og svagheder ved de eksisterende sikkerhedskontroller såsom validering af input, autentificering og autorisation, tjek af korrekt brug af forretningslogik, validering af korrekt brug af sikre protokoller, identificering af fejl i sessionsbehandlingen og verificering af korrekte sikkerhedskontroller i

forbindelse med login, gendannelse af kodeord, kodeordspolitik og andre brugeradministrationsfunktioner. Resultaterne dokumenteres i Applikation Penetration-testrapporten. IBM forestår et webmøde med orientering om rapporten på op til en time. Applikation Penetration-testserviceydelsen er gennemført, når den tildelte rådgivningstid er brugt, webmødet er afholdt, og den endelige Applikation Penetration-testrapport er leveret til Kunden.

1.2.1 Ansvar i forbindelse med Opsætningsserviceydelser

IBM skal:

- levere Opsætningsserviceydelser ved brug af de Engagements-enheder, som Kunden har købt, og ifølge beviset for brugsret, og
- have gennemført en Opsætningsserviceydelse, når kriterierne for gennemførelse, der er beskrevet i afsnit1.2, er gennemført.

Kunden er indforstået med:

- at være ansvarlig for alle betalinger i forbindelse med alle Engagementsanmodninger, som Kunden foretager i aftaleperioden
- og anerkender, at de købte Engagements-enheder skal bruges i den første aftaleperiode, og at de udløber, hvis de ikke er brugt på datoen for aftaleperiodens udløb, samt
- at indlede en formel anmodning om alle Opsætningsydelser senest 30 dage før abonnementets udløbsdato.

Ved udførelsen af enhver Opsætningsserviceydelse kan IBM anmode Kunden om oplysninger og rimeligt samarbejde. Hvis Kunden ikke rettidigt leverer de oplysninger eller det samarbejde, som IBM har anmodet om, kan dette resultere i Engagementenhedsbetalinger i det omfang, serviceydelserne eller forsinkelsen i udførelsen af den pågældende serviceydelse kræver det. Sådanne betalinger fastsættes af IBM.

For at IBM kan udføre testen nøjagtigt, er Kunden indforstået med at følge IBM's anvisninger i forbindelse med klargøring og vedligeholdelse af miljøet i testperioden.