IBM Gebruiksvoorwaarden – SaaS Specifieke Voorwaarden voor Aanbieding

IBM Application Security on Cloud

De Gebruiksvoorwaarden ("ToU") bestaan uit deze IBM Gebruiksvoorwaarden – SaaS Specifieke Voorwaarden voor Aanbieding ("SaaS Specifieke Voorwaarden voor Aanbieding") en een document met de titel IBM Gebruiksvoorwaarden – Algemene bepalingen ("Algemene Voorwaarden") dat beschikbaar is op de volgende URL: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

In geval van tegenstrijdigheid prevaleren de SaaS Specifieke Voorwaarden voor Aanbieding boven de Algemene Voorwaarden. Door de IBM SaaS te bestellen, te openen of te gebruiken, geeft Klant aan akkoord te gaan met de Gebruiksvoorwaarden.

De Gebruiksvoorwaarden worden beheerst door de IBM International Passport Advantage Overeenkomst, de IBM International Passport Advantage Express Overeenkomst of de IBM International Agreement for Selected IBM SaaS Offerings, zoals van toepassing ("Overeenkomst") en vormen samen met de Gebruiksvoorwaarden de volledige overeenkomst.

1. IBM SaaS

De volgende IBM SaaS-aanbiedingen worden gedekt door deze SaaS Specifieke Voorwaarden voor Aanbieding:

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

2. Maateenheden voor verschuldigde bedragen

De IBM SaaS wordt verkocht onder de volgende maateenheden voor verschuldigde bedragen, zoals gespecificeerd in het Transactiedocument:

a. **Job** – is een maateenheid onder welke de IBM SaaS kan worden verkregen. Een Job is een object binnen de IBM SaaS dat niet verder kan worden onderverdeeld en dat een rekenproces met inbegrip van alle subprocessen daarvan vertegenwoordigt. Er dienen voldoende gebruiksrechten te worden verworven ter dekking van het totaal aantal Jobs dat door de IBM SaaS wordt verwerkt of beheerd tijdens de meetperiode zoals aangegeven in het Bewijs van Gebruiksrecht of Transactiedocument van Klant.

b. **Applicatie Instance** – is een maateenheid onder welke de IBM SaaS kan worden verkregen. Er is een Applicatie Instance gebruiksrecht vereist voor elke instance van een Applicatie die verbonden is met de IBM SaaS. Indien een bepaalde Applicatie meerdere componenten heeft, elk daarvan een specifiek doel dient en/of een specifieke gebruikersbasis bedient, en elk daarvan kan worden verbonden met of beheerd door de IBM SaaS, wordt elke dergelijke component beschouwd als een afzonderlijke Applicatie. Bovendien worden test-, ontwikkelings-, staging- of productieomgevingen voor een Applicatie beschouwd als afzonderlijke instances van de Applicatie en is er voor elk daarvan een gebruiksrecht vereist. Meerdere Instances van een Applicatie in een enkele omgeving worden beschouwd als afzonderlijke instances van die Applicatie en voor elk van die instances is er een gebruiksrecht vereist. Er dienen voldoende gebruiksrechten te worden verworven ter dekking van het aantal Applicatie Instances dat tijdens de in het Bewijs van Gebruiksrecht of Transactiedocument van Klant aangegeven meetperiode is verbonden met de IBM SaaS.

   Voor het doel van deze IBM SaaS:

   - Voor Dynamic Testing: een via een publieke of private URL adresseerbare website. Elke Applicatie Instance geeft recht op een site van maximaal 1000 pagina's in een enkel domein.
   - Voor Static Testing: een in een enkele programmeertaal uitvoerbare code-eenheid. Elke Applicatie Instance geeft recht op het scannen van code-eenheden tot een maximum van 1.000.000 regels.
   - Voor Mobile Testing: een op een mobiel apparaat uitvoeren binaire code-eenheid. Elk afzonderlijk mobiel platform (bijv. iOS en Android) vormt een afzonderlijke Applicatie Instances.

c. **Instance** – is een maateenheid onder welke de IBM SaaS kan worden verkregen. Een Instance is de toegang tot een specifieke configuratie van de IBM SaaS. Er dienen voldoende gebruiksrechten te worden verworven voor elke Instance die beschikbaar is gesteld voor toegang en gebruik tijdens de in het Bewijs van Gebruiksrecht of Transactiedocument van Klant aangegeven meetperiode.

   Voor elk gebruiksrecht voor een Instance geldt er geen limiet wat betreft het aantal uitgevoerde Jobs of het aantal geleverde Applicatie Instances (verbonden Applicaties), met dien verstande echter dat er op geen enkel moment meer dan 30 Jobs gelijktijdig actief kunnen zijn.

d. **Engagement** – is een maateenheid onder welke de services kunnen verkregen. Een Engagement bestaat uit professionele en/of trainingsservices met betrekking tot de IBM SaaS. Er dienen voldoende gebruiksrechten te worden verworven ter dekking van elke Engagement.

3. Verschuldigde bedragen en facturering

Het verschuldigde bedrag voor de IBM SaaS wordt aangegeven in een Transactiedocument.

3.1 Verschuldigd bedrag voor een deel van een maand

Voor een deel van een maand kunnen er pro rato verschuldigde bedragen worden in rekening worden gebracht, zoals aangegeven in het Transactiedocument.

3.2 Verschuldigde bedragen bij overschrijding

Indien het feitelijke gebruik van de IBM SaaS tijdens de meetperiode het in het Bewijs van Gebruiksrecht gespecificeerde gebruik overschrijdt, wordt Klant voor de overschrijding gefactureerd zoals gespecificeerd in het Transactiedocument.

3.3 Verschuldigde bedragen voor setup

Klant wordt voor setup gefactureerd zoals aangegeven in het Transactiedocument.

4. Looptijd en verlengingsopties

De looptijd van de IBM SaaS begint op de datum waarop IBM Klant informeert omtrent diens toegang tot de IBM SaaS, zoals gedocumenteerd in het Bewijs van Gebruiksrecht. In het Bewijs van Gebruiksrecht wordt aangegeven of de IBM SaaS automatisch wordt verlengd, wordt voortgezet op basis van doorlopend gebruik, of eindigt aan het einde van de looptijd.

Bij automatische verlenging geldt dat de IBM SaaS automatisch met de in het Bewijs van Gebruiksrecht gespecificeerde looptijd wordt verlengd, tenzij Klant minimaal 30 dagen vóór het einde van looptijd schriftelijk opzegt.

Bij doorlopend gebruik blijft de IBM SaaS op maandelijkse basis beschikbaar, totdat Klant op een termijn van 30 dagen schriftelijk opzegt. Na die periode van 30 dagen blijft de IBM SaaS tot het einde van de kalendermaand beschikbaar.

5. Technische ondersteuning

Nadat Klant tijdens de Abonnementsperiode door IBM is ingelicht dat de IBM SaaS beschikbaar is, wordt er technische ondersteuning verleend via online forums en in de vorm van standaardondersteuning tijdens de periode waarin Klant verschuldigde bedragen in het kader van Betaling per Gebruik opbouwt. Vanuit IBM SaaS kan Klant een ondersteuningsticket indienen of een chatsessie openen voor assistentie. IBM zal het IBM Software as a Service Support Handbook ter beschikking stellen, met daarin contactgegevens voor technische ondersteuning en andere informatie en processen.

Severity	Definitie van severity	Doelstellingen inzake responstijd	Dekkingsuren voor responstijd
1	**Kritieke impact op bedrijfsvoering / service down:** Bepaalde bedrijfskritische functionaliteit of een cruciale interface werkt niet. Dit heeft gewoonlijk betrekking op een productie-omgeving en geeft aan dat het onmogelijk is toegang te krijgen tot de service, hetgeen kritieke gevolgen heeft voor de bedrijfsvoering. In deze situatie is onmiddellijk een oplossing vereist.	Binnen 1 uur	24x7

Severity	Definitie van severity	Doelstellingen inzake responstijd	Dekkingsuren voor responstijd
2	**Aanzienlijke impact op bedrijfsvoering:** Het gebruik van een bedrijfsfunctie of -voorziening van de service levert ernstige beperkingen op of Klant loopt het risico zakelijke deadlines te missen.	Binnen 2 kantooruren	Kantooruren, van maandag t/m vrijdag
3	**Kleinere impact op bedrijfsvoering:** Geeft aan dat de service of functie bruikbaar is en dat de impact op de bedrijfsvoering niet kritiek is.	Binnen vier kantooruren	Kantooruren, van maandag t/m vrijdag
4	**Minimale impact op bedrijfsvoering:** Een verzoek om informatie of een niet-technisch verzoek	Binnen 1 werkdag	Kantooruren, van maandag t/m vrijdag

5.1 Toegang tot gegevens van Klant

IBM is in staat zich toegang tot gegevens van Klant te verschaffen ten behoeve van het stellen van een diagnose bij problemen met de service, en het faciliteren van scans van de applicatie van Klant door de service. IBM zal zich uitsluitend toegang tot de gegevens verschaffen ten behoeve van het verhelpen van defecten of het verlenen van ondersteuning voor IBM-producten of -services.

6. Aanvullende bepalingen voor IBM SaaS-aanbiedingen

Beveiligingsscans sporen mogelijkerwijs niet alle beveiligingsrisico's in een applicatie op en zijn niet ontworpen of bedoeld voor gebruik in risicovolle omgevingen waarin een foutloze werking noodzakelijk is, zoals in vliegtuignavigatie, luchtverkeersleidingssystemen, wapensystemen, medische systemen voor de directe instandhouding van levensfuncties, nucleaire installaties, of enige andere toepassing waarin het niet opsporen van beveiligingsrisico's overlijden, letsel of fysieke schade tot gevolg kan hebben. Er wordt geen garantie gegeven dat beveiligingsscans ononderbroken en foutloos zullen werken.

De IBM SaaS kan worden gebruikt om Klant te helpen voldoen aan zijn verplichtingen inzake naleving van wet- en regelgeving (compliance), welke verplichtingen gebaseerd kunnen zijn op wetten, regelingen, normen of werkwijzen. Aanwijzingen, gebruiksadviezen of richtlijnen die door de Service worden verstrekt, vormen geen wettig, boekhoudkundig of professioneel advies en Klant wordt nadrukkelijk geadviseerd zelf deskundig advies in te winnen, juridisch of anderszins. Klant is als enige verantwoordelijk te garanderen dat Klant en de activiteiten, toepassingen en systemen van Klant voldoen aan de toepasselijke wetten, regelingen, normen en werkwijzen. Het gebruik van deze Service vormt geen garantie voor de naleving van enige wet, regeling, norm of werkwijze.

De IBM SaaS voert binnendringende en niet-binnendringende tests uit op de website en de web- of mobiele applicatie die Klant wil laten scannen. Pogingen computersystemen binnen te dringen of zich er toegang toe te verschaffen zijn bij wet verboden. Klant machtigt IBM de Services uit te voeren zoals hierin beschreven en verklaart dat de Services een geautoriseerde vorm van toegang tot de computersystemen van Klant zijn. IBM mag deze toestemmingsverklaring aan derden onthullen indien dit noodzakelijk wordt geacht voor het verlenen van de Services.

Het testen brengt bepaalde risico's met zich mee, met inbegrip van, maar niet beperkt tot de volgende:

a. de computersystemen van Klant kunnen tijdens het uitvoeren van applicaties onder de test "vastlopen", hetgeen kan leiden tot gegevensverlies of het tijdelijk niet beschikbaar zijn van de systemen;

b. de prestaties en doorvoer van de systemen van Klant, evenals de prestaties en doorvoer van bijbehorende routers en firewalls, kunnen tijdens de test tijdelijk verslechteren;

c. er kunnen buitensporige hoeveelheden logberichten worden gegenereerd, die uitzonderlijk veel schijfruimte innemen;

d. als gevolg van het onderzoeken van kwetsbaarheden kunnen er gegevens worden gewijzigd of gewist;

e. er kunnen door het inbraakdetectiesysteem alarms worden geactiveerd;

f. de verzending van e-mails kan worden gestart door de e-mailfunctie van de webapplicatie die wordt getest;

g. de IBM SaaS kan het verkeer van het bewaakte netwerk onderscheppen ten behoeve van de opsporing van events.

Tijdens testactiviteiten doet Klant afstand van alle door IBM op grond van een Service Level Agreement verleende rechten of schadevergoedingen met betrekking tot de websites of applicaties waarop de testactiviteiten betrekking hebben.

In geval Klant geverifieerde legitimatiegegevens voor aanmelding ("log-in") invoert voor de applicatie die onder de Service wordt getest, dient Klant uitsluitend legitimatiegegevens voor testaccounts in te voeren, niet voor productiegebruikers. Het gebruik van legitimatiegegevens van productiegebruikers kan ertoe leiden dat er via de Service persoonsgegevens worden verzonden.

De IBM SaaS kan worden geconfigureerd voor het scannen van productie-webapplicaties. Indien Klant het scantype instelt op "productie", voert de service volgens ontwerp scans uit op een wijze waarop de onderstaande risico's worden beperkt; in bepaalde situaties kan de IBM SaaS echter leiden tot achteruitgang van de performance of instabiliteit binnen de geteste productiesites en -infrastructuur. IBM geeft geen enkele garantie en doet geen enkele uitspraak met betrekking tot de geschiktheid van de IBM SaaS voor het scannen van productiesites.

HET IS DE VERANTWOORDELIJKHEID VAN KLANT TE BEPALEN OF DE SERVICE GESCHIKT EN VEILIG IS VOOR DE WEBSITE, WEBAPPLICATIE, MOBIELE APPLICATIE OF TECHNISCHE OMGEVING VAN KLANT.

De IBM SaaS is bedoeld voor het opsporen van een veelheid aan potentiële beveiligings- en complianceproblemen in mobiele en webapplicaties en in webservices. De Cloud Service onderzoekt niet alle kwetsbaarheden of compliancerisico's, en fungeert evenmin als barrière tegen aanvallen op de beveiliging. Beveiligingsrisico's, -regelingen en -standaarden veranderen voortdurend, en wellicht komen niet al dergelijke veranderingen tot uitdrukking in de Service. Klant is als enige verantwoordelijk voor de beveiliging en compliance van de webapplicaties, systemen en werknemers van Klant en voor eventuele herstelmaatregelen. Het is geheel aan Klant om te bepalen of de door de Service geleverde informatie al dan niet wordt gebruikt.

Pogingen computersystemen binnen te dringen of zich er toegang toe te verschaffen zijn bij wet verboden. KLANT GARANDEERT DAT HIJ DE SERVICE NIET GEBRUIKT VOOR HET SCANNEN VAN ENIGE WEBSITE EN/OF APPLICATIE ANDERS DAN DE WEBSITES EN/OF APPLICATIES DIE EIGENDOM ZIJN VAN KLANT OF DE WEBSITES EN/OF APPLICATIES WAARVOOR KLANT HET RECHT EN DE BEVOEGDHEID HEEFT ZE TE SCANNEN.

Voor de duidelijkheid: De in het artikel over gegevensbescherming van de IBM Gebruiksvoorwaarden – Algemene Voorwaarden beschreven content van Klant wordt ook geacht gegevens te bevatten die voor IBM toegankelijk kunnen worden tijdens Application Penetration Testing.

6.1 Systemen die eigendom zijn van een derde partij

Voor systemen (waar voor het doel van deze bepaling tevens applicaties en IP-adressen onder vallen) die eigendom zijn van een derde partij en die onder deze Gebruiksvoorwaarden worden onderworpen aan tests, gaat Klant ermee akkoord:

a. voordat IBM begint met de testactiviteiten op een systeem van een derde, een ondertekend schrijven van de eigenaar van elk systeem te zullen verkrijgen waarin IBM wordt gemachtigd om Services op dat systeem te verlenen en waarin wordt aangegeven dat de eigenaar akkoord gaat met de voorwaarden zoals vastgelegd in het gedeelte "Toestemming voor het uitvoeren van tests", en IBM een kopie van een dergelijke machtiging te zullen verstrekken;

b. als enige verantwoordelijk te zijn voor het aan de eigenaar van het systeem doorgeven van alle risico's en kwetsbaarheden die bij de op afstand uitgevoerde tests van IBM zijn gebleken; en

c. de uitwisseling van informatie tussen de eigenaar van het systeem en IBM te zullen regelen en faciliteren, voor zover noodzakelijk geacht door IBM.

Klant verklaart:

- IBM onverwijld in kennis te stellen steeds wanneer er een wijziging in de eigendom plaatsvindt van enig systeem waarop onder deze Gebruiksvoorwaarden tests worden uitgevoerd;
- de deliverables, of het feit dat IBM de Services heeft verleend, niet buiten de Onderneming van Klant te zullen onthullen zonder voorafgaande schriftelijke toestemming van IBM; en

- IBM volledig schadeloos te zullen stellen voor alle verliezen of schadevergoedingen die IBM oploopt als gevolg van niet-naleving door Klant van alle eisen in dit gedeelte getiteld "Systemen die eigendom zijn van een derde partij" en als gevolg van vorderingen van derden ingebracht tegen IBM of subcontractanten of agenten van IBM, voortvloeiend uit (a) het testen van de beveiligingsrisico's, andere risico's en kwetsbaarheden van de systemen die het onderwerp zijn van de tests onder deze Gebruiksvoorwaarden, (b) het aan Klant verstrekken van de resultaten van dergelijke tests, of (c) het gebruik of de openbaarmaking van dergelijke resultaten door Klant.

6.2 Cookies

Klant is zich ervan bewust en gaat ermee akkoord dat IBM, in het kader van de normale exploitatie en ondersteuning van de IBM SaaS, met behulp van tracerings- en andere technologie persoonsgegevens van Klant (uw werknemers en contractanten) kan verzamelen, verband houdend met het gebruik van de IBM SaaS. IBM doet dit ten behoeve van het verzamelen van gebruikscijfers en informatie over de effectiviteit van onze IBM SaaS, gericht op het verbeteren van de gebruikerservaring en/of het op maat toesnijden van interacties met Klant. Klant bevestigt toestemming te zullen verkrijgen of te hebben verkregen om IBM in staat te stellen de verzamelde persoonsgegevens, overeenkomstig de toepasselijke wetgeving, te verwerken voor de bovengenoemde doeleinden binnen IBM, andere IBM ondernemingen en hun onderaannemers, overal waar IBM en haar onderaannemers zakendoen. IBM zal voldoen aan verzoeken van werknemers en contractanten van Klant om de over hun verzamelde persoonsgegevens in te zien, bij te werken, te corrigeren en/of te wissen.

Als onderdeel van de IBM SaaS, waartoe rapportageactiviteiten behoren, zal IBM gedeïdentificeerde en/of samengevoegde informatie die vanuit de IBM SaaS is verzameld ("Beveiligingsgegevens" genaamd) opstellen en onderhouden. Klant noch andere individuen worden door de Beveiligingsgegevens geïdentificeerd, behoudens zoals vermeld onder lid (d), hieronder. Klant gaat er hierbij aanvullend mee akkoord dat IBM de Beveiligingsgegevens mag gebruiken en/of kopiëren, echter uitsluitend voor de volgende doeleinden:

a. het publiceren en/of distribueren van de Beveiligingsgegevens (bijvoorbeeld in compilaties en/of analyses met betrekking tot cybersecurity);

b. het ontwikkelen of verbeteren van producten of diensten;

c. het uitvoeren van onderzoek, intern of in samenwerking met derden; en

d. de wettige uitwisseling van informatie over bevestigde externe daders.

6.3 Profijt genietende locaties

Waar van toepassing worden de belastingen gebaseerd op de locatie(s) waarvan Klant aangeeft dat deze profijt geniet(en) van de IBM SaaS. Tenzij Klant IBM aanvullende informatie verstrekt, berekent IBM de belastingen op basis van het bedrijfsadres zoals dat bij het bestellen van een IBM SaaS bij IBM bekend is. Klant is verantwoordelijk voor het actueel houden van de desbetreffende informatie en voor het doorgeven van wijzigingen aan IBM.

6.4 Persoonsgegevens en gereguleerde content en services

Deze IBM SaaS is niet ontworpen op basis van specifieke beveiligingsvereisten voor gereguleerde content, zoals persoonsgegevens en gevoelige persoonsgegevens. Het is de verantwoordelijkheid van Klant te bepalen of deze IBM SaaS voldoet aan de eisen van Klant met betrekking tot het type content dat Klant in samenhang met de IBM SaaS gebruikt.

IBM treedt niet op als een door de overheid gereguleerde dienstverlener en heeft niet de bedoeling diensten te verlenen die door de overheid worden gereguleerd. Indien een overheidsinstantie eisen of verplichtingen oplegt met betrekking tot enige service die door IBM onder deze Gebruiksvoorwaarden wordt verleend, kan IBM: (a) op kosten van Klant producten wijzigen, terugplaatsen of vervangen, en/of (b) wijzigingen aanbrengen in de wijze waarop de services aan Klant worden verleend teneinde te voorkomen dat dergelijke eisen of verplichtingen aan IBM worden opgelegd (bijvoorbeeld door op te treden als agent van Klant ten behoeve van de aanschaf van dergelijke services van een derde partij).

Bijlage A

1. IBM Application Security on Cloud - Algemene beschrijving

Met IBM Application Security on Cloud heeft Klant de assistentie voor het opsporen van kwestbaarheden in de beveiliging (zoals SQL Injection, Cross-Site Scripting en Data Leakage) voor een veelheid aan applicaties op één plaats. De service omvat verschillende soorten scantechnieken voor applicatiebeveiliging, die elk de beveiligingsproblemen in de desbetreffende applicatie aangeven.

IBM Application Security on Cloud biedt de volgende mogelijkheden:

- Scanning van Mobiele Applicaties op kwetsbaarheden in de beveiliging. Dit gebeurt via dynamische (blackbox) en Interactieve (glassbox) technieken voor beveiligingsanalyse.
- Scanning van productie- of preproductiewebsites, dan wel publieke of op een besloten netwerk aanwezige websites op kwetsbaarheden in de beveiliging. Dit gebeurt via dynamische (blackbox) technieken voor beveiligingsanalyse.
- Scanning van de gegevensstromen binnen web- en desktopapplicaties op kwetsbaarheden in de beveiliging. Dit gebeurt via statische (whitebox) technieken voor beveiligingsanalyse.
- Gedetailleerde rapporten inzake kwetsbaarheden in de beveiliging, met zowel overkoepelende overzichten van de bevindingen als verbeteringsprocedures die door ontwikkelaars kunnen worden gevolgd.
- Integratie met diverse DevOps-platforms

1.1 IBM Application Analyzer

IBM Application Analyzer kan worden besteld per Applicatie Instance, per Job (scan) of in de vorm van een volledige Instance. IBM Application Analyzer maakt de volgende soorten scanning mogelijk:

- Dynamic Analyzer – Pre-productie- of productiewebsites testen via DAST-technieken
- Mobile Analyzer – Binaire iOS- of Android-bestanden testen via IAST-technieken
- Static Analyzer – Byte- of source-code data flow testen via via SAST-technieken

1.2 Set-Up Service

IBM Application Security on Cloud Consulting Services vormen een set-up serviceproduct voor Application Analyzer. De Service maakt gebruik van IBM consultants die begeleiding en assistentie verlenen bij het testen op, en aanpakken van, applicatierisico's. IBM Application Security on Cloud Consulting Services worden aangekocht in de vorm van blokken Engagements die in de hieronder uiteengezette aantallen kunnen worden besteed aan het aanvragen en gebruiken van de volgende specifieke services:

a. **Fast Start** [hiervoor is één (1) Engagement eenheid vereist]

De service Fast Start biedt expertise en begeleiding bij het werken met de test- en risicomanagementfuncties van Application Security on Cloud. Nadat Klant heeft bevestigd dat de login bij de portal van Application Security on Cloud is gelukt, belegt IBM een webvergadering van ten hoogste twee (2) uur om ten hoogste (2) actieve deelnemers onderricht te geven in elementaire configuraties en functies van AppSec op IBM SaaS, zoals de typen scans, het uitvoeren van scans, het doornemen van rapporten en het installeren van de bijbehorende tools en plug-ins. De service Fast Start is voltooid na de voltooiing van: (a) het educatieve webinar, (b) de installatie van de toepasselijke tools en plug-ins, en (c) de hulp aan Klant bij het opzetten en uitvoeren van diens eerste scan.

b. **Assessment Review** [hiervoor zijn twee (2) Engagement eenheden vereist]

De service Assessment Review biedt hulp bij het evalueren van een testresultaat, inclusief het begrijpen en stellen van prioriteiten bij de oplossing van kwetsbaarheden in de applicatie. IBM belegt een webvergadering van ten hoogste één (1) uur met twee (2) actieve deelnemers om een overzicht te geven van de aangetroffen kwetsbaarheden en de algehele beveiligingsrisico's van de applicatie, en om een gedetailleerde uiteenzetting te geven over de aangetroffen kwetsbaarheden in de applicatiebeveiliging, inclusief (1) de manier waarop de kwetsbaarheid is getest, (2) de manier waarop de kwetsbaarheden zijn gedetecteerd, (3) de risico's van elke kwetsbaarheid, en (4)

algemene aanbevelingen voor het verhelpen van de kwetsbaarheid. De evaluatie wordt uitsluitend gebaseerd op de testresultaten en is geen evaluatie van de broncode zelf. Klant evalueert de testresultaten eerst zelf en geeft voorafgaand aan de webvergadering tegenover IBM aan welk testresultaat hij geëvalueerd wil hebben. De service Assessment Review is voltooid na voltooiing van de webvergadering.

c. **Scan for Me** [hiervoor zijn vier (4) Engagement eenheden vereist]

De service Scan for Me behelst het beschikbaar stellen van een IBM application security expert die een scan configureert en uitvoert, de resultaten valideert en een rapport briefing houdt om de bevindingen te evalueren. Klant verleent een consultant van IBM toegang tot zijn ASoC omgeving ten behoeve van het configureren en uitvoeren van een scan, het valideren van de resultaten, het doen van aanbevelingen omtrent de prioriteit van oplossingen en het houden van een rapport briefing over de resultaten. IBM belegt een webvergadering van ten hoogste één (1) uur met twee (2) actieve deelnemers om een overzicht te geven van de aangetroffen kwetsbaarheden en de algehele beveiligingsrisico's van de applicatie, en om een gedetailleerde uiteenzetting te geven over de aangetroffen kwetsbaarheden in de applicatiebeveiliging, inclusief (1) de manier waarop de kwetsbaarheid is getest, (2) de manier waarop de kwetsbaarheden zijn gedetecteerd, (3) de risico's van elke kwetsbaarheid, en (4) algemene aanbevelingen voor het verhelpen van de kwetsbaarheid. Op verzoek zal IBM, tot maximaal 30 dagen na de eerste scan, een herscan uitvoeren met behulp van de oorspronkelijke scanconfiguratie (uitsluitend voor het verifiëren van beveiligingsfixes, niet voor het testen van nieuwe functionaliteit), de resultaten valideren en rapport uitbrengen aan Klant. De service Scan for Me is voltooid na voltooiing van de webvergadering voor het evalueren van de resultaten van de eerste scan of, indien van toepassing, de voltooiing van de door Klant aangevraagde herscan en de levering van het rapport van de herscan aan Klant.

d. **Advisor on Demand** [hiervoor zijn zeven (7) Engagement eenheden vereist]

De service Advisor on Demand geeft Klant ten hoogste twintig (20) uur de beschikking over een IBM consultant. Deze tijd kan worden besteed aan activiteiten samenhangend met de IBM SaaS. De IBM consultant verleent assistentie bij kwesties die specifiek te maken hebben met applicatiebeveiliging, met inbegrip van, maar niet beperkt tot, programmamanagement, prioriteitstelling voor beveiligingstests, oplossingsstrategieën, analyse van de broncode en reparatie van de broncode. IBM werkt samen met Klant aan beter inzicht en het opstellen van een projectplanning met specifieke eisen van Klant, inclusief projectdoelen, relevante technologieën, gewenste tijdslijnen, verwachte deliverables en geschat aantal service engagements voor Advisor on Demand. Klant dient toegang te verlenen tot de voor het verlenen van de services noodzakelijke applicaties, systemen en documentatie. De service Advisor on Demand is voltooid wanneer er ten hoogste 20 uur aan beveiligingsexpertise beschikbaar is gesteld en/of nadat de projectplanning en/of de in de projectplanning aangegeven deliverables zijn geleverd aan Klant.

e. **Application Penetration Testing**

Drie opties:

(1) **Compliance/Entry-Level Application Penetration Test**, bestaande uit ten hoogste veertig (40) uur de beschikking over een Consultant, met een focus op zogenoemde "single-step logic flaws" en eenvoudige versies van "injection flaws". Hiervoor zijn vijftien (15) Engagement eenheden vereist.

(2) **Standard Application Penetration Test**, bestaande uit ten hoogste zestig (60) uur de beschikking over een Consultant, met een bredere focus waarin ook zogenoemde "logic flaws in multi-step work flows", complexe versies van "injection flaws" en analyse van complexe datatypen een rol spelen. Hiervoor zijn eenentwintig (21) Engagement eenheden vereist.

(3) **Advanced Application Penetration Test** – Ten hoogste tachtig (80) uur de beschikking over een Consultant, met een bredere focus waarin ook reverse engineering van gecompileerde executables, ontleding van maatwerk netwerkprotocollen, diepgaande analyse van openbaar beschikbare libraries en frameworks een rol spelen. Hiervoor zijn zevenentwintig (27) Engagement eenheden vereist.

De service Application Oenetration Testing stelt een medewerker van IBM ter beschikking voor de test en exploitatie van een applicatie, de levering van een testrapport, en een rapport briefing om de bevindingen en bijbehorende risico's toe te lichten.

IBM organiseert een telefonisch projectinitialisatiegesprek van ten hoogste één (1) uur en met twee (2) actieve deelnemers teneinde de omgeving en organisatie van Klant door te nemen, met inbegrip van het applicatieplatform, de architectuur, de frameworks, de ondersteunende infrastructuur, reeds bekende beveiligingsproblemen met, of zorgen over de beveiliging van, de applicatie, voorlopige testplanning en noodcontactplan.

IBM voert de Application Penetrating Testing uit, met inbegrip van, maar niet beperkt tot: opsporing van gangbare kwetsbaarheden zoals SQL injection en cross-site scripting, beoordeling van de sterke en zwakke punten van de bestaande beveiligingsprocedures zoals inputvalidatie, authenticatie en autorisatie, controle op de juiste handhaving van business logic, validatie van het juiste gebruik van veilige protocollen, opsporing van "session handling flaws" en verificatie van de juiste beveiligingsprocedures voor login, wachtwoordrecovery, wachtwoordbeleid en andere gebruikersmanagementfuncties. De bevindingen worden gedocumenteerd in het Application Penetration Test Report. Ten behoeve van de rapport briefing organiseert IBM een webvergadering van ten hoogste één (1) uur. De service Application Penetration Test is voltooid wanneer het toegewezen aantal uren consultancy gebruikt is, de webvergadering is gehouden en het definitieve Application Penetration Test Report is geleverd aan Klant.

1.2.1 Verantwoordelijkheden voor Set-Up Services

IBM zal:

- Set-Up Services verlenen op basis van de door Klant aangekochte Engagement eenheden en zoals vastgelegd in het Bewijs van Gebruiksrecht; en
- de Set-Up Service hebben voltooid wanneer er aan de in Artikel 1.2 beschreven voltooiingscriteria is voldaan.

Klant verklaart:

- verantwoordelijk te zijn voor alle verschuldigde bedragen voor alle Engangement aanvragen die de tijdens de looptijd van het contract door Klant zijn ingediend;
- en erkent dat aangekochte Engagement eenheden moeten worden gebruikt binnen de initiële looptijd van het contract en dat deze eenheden vervallen indien ze op de einddatum van de looptijd van het contract niet zijn gebruikt; en
- ten minste 30 dagen vóór de einddatum van het abonnement een formeel verzoek voor alle Set-Up Services in gang te zetten.

IBM kan, bij het verlenen van welke Set-Up Service dan ook, informatie en redelijke medewerking van Klant verlangen. Het niet tijdig verstrekken van informatie of het niet tijdig verlenen van medewerking door Klant kan, zoals bepaald door IBM, leiden tot het in rekening brengen van Engagement eenheden zoals vereist voor de services, of tot vertraging in de verlening van de desbetreffende service.

Teneinde IBM in staat te stellen de tests zorgvuldig uit te voeren, verklaart Klant de instructies van IBM bij het voorbereiden en onderhouden van de omgeving voor de testperiode op te volgen.