IBM Application Security on Cloud

Käyttöehdot (ToU-ehdot) koostuvat tästä asiakirjasta IBM:n käyttöehdot – SaaS-tuotteita koskevat ehdot (SaaS-tuotteita koskevat ehdot) ja asiakirjasta IBM:n käyttöehdot – Yleiset ehdot (Yleiset ehdot), joka on saatavana seuraavasta URL-osoitteesta: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

Mahdollisissa ristiriitatilanteissa SaaS-tuotteita koskevat ehdot ovat etusijalla Yleisiin ehtoihin nähden. Asiakas hyväksyy ToU-ehdot tilaamalla tai ottamalla käyttöön IBM SaaS -tuotteen.

ToU-ehtoja koskevat soveltuvin osin IBM:n kansainvälisen Passport Advantage -sopimuksen, IBM:n kansainvälisen Passport Advantage Express -sopimuksen tai IBM:n kansainvälisen Valikoituja IBM Software as a Service (SaaS) -tuotteita koskevan sopimuksen (Sopimus) ehdot, jotka yhdessä ToU-ehtojen kanssa muodostavat kokonaissopimuksen.

1. IBM SaaS

Nämä SaaS-tuotteita koskevat ehdot koskevat seuraavia IBM SaaS -tuotteita:

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

2. Maksujen mittayksiköt

IBM SaaS -tuotteen myynnissä sovelletaan yhtä seuraavista mittayksiköistä Sopimusasiakirjassa määritetyllä tavalla:

a. **Työ** on mittayksikkö, jonka mukaan IBM SaaS -tuotteen voi hankkia. Työ on IBM SaaS -tuotteen yksikkö, jota ei voi jakaa edelleen osiin ja joka kuvaa laskentaprosessia kaikkine aliprosesseineen. Käyttöoikeuksia on hankittava määrä, joka vastaa IBM SaaS -tuotteen mittauskauden aikana käsittelemien tai hallitsemien Töiden kokonaismäärää. Mittauskausi on määritetty Asiakkaan Käyttölupatodistuksessa (PoE) tai Sopimusasiakirjassa.

b. **Sovellusilmentymä** on mittayksikkö, jonka mukaan IBM SaaS -tuotteen voi hankkia. Sovellusilmentymän käyttöoikeus on pakollinen kutakin IBM SaaS -tuotteeseen yhdistettyä Sovelluksen ilmentymää kohden. Jos Sovelluksessa on useita komponentteja, joista kullakin on erillinen tarkoituksensa ja/tai käyttäjäjoukkonsa ja joista kukin voidaan yhdistää IBM SaaS -tuotteeseen tai asettaa sen hallintaan, jokainen tällainen komponentti katsotaan erilliseksi sovellukseksi. Lisäksi testaus-, kehitys-, välivaihe- ja tuotantoympäristössä ajettavat Sovellukset katsotaan Sovelluksen erillisiksi ilmentymiksi, joilla tulee olla oma käyttöoikeutensa. Tietyssä ympäristössä ajettavat useat Sovellusilmentymät katsotaan Sovelluksen erillisiksi ilmentymiksi, joilla tulee olla käyttöoikeus. Käyttöoikeuksia on hankittava määrä, joka vastaa mittauskauden aikana IBM SaaS -tuotteeseen yhdistettyjen Sovellusilmentymien määrää. Mittauskausi on määritetty Asiakkaan Käyttölupatodistuksessa (PoE) tai Sopimusasiakirjassa.

   Tämän IBM SaaS -tuotteen yhteydessä:

   - Dynaaminen testaus: julkisen tai yksityisen URL-osoitteen avulla osoitettava verkkosivusto. Kukin Sovellusilmentymä antaa oikeuden yhdessä verkkotunnuksessa toimivaan sivustoon, jossa on enintään 1 000 sivua.
   - Staattinen testaus: koodikokonaisuus, joka on ajettavissa yhdellä ohjelmointikielellä. Kukin Sovellusilmentymä antaa oikeuden enintään 1 000 000 rivin koodikokonaisuuksien lukemiseen.
   - Mobiilitestaus: binaarikoodikokonaisuus, joka on ajettavissa mobiililaitteessa. Kukin erillinen mobiiliympäristö (esimerkiksi iOS ja Android) muodostaa erillisen Sovellusilmentymän.

c. **Ilmentymä** on mittayksikkö, jonka mukaan IBM SaaS -tuotteen voi hankkia. Ilmentymällä tarkoitetaan IBM SaaS -tuotteen tietyn kokoonpanon käyttöä. Kutakin käytettäväksi saatettavaa tai käytettävää IBM SaaS -tuotteen Ilmentymää varten on hankittava riittävä määrä käyttöoikeuksia Asiakkaan Käyttölupatodistuksessa (PoE) tai Sopimusasiakirjassa määritetyn mittauskauden ajaksi.

   Ilmentymän käyttöoikeutta kohden ei ole ajettavien Töiden eikä Sovellusilmentymien (yhdistettyjen Sovellusten) määrää koskevaa rajoitusta, mutta samaan aikaan ajossa olevien Töiden enimmäismäärä on kuitenkin 30.

d. **Palvelutapahtuma** on mittayksikkö, jonka mukaan palveluja voi hankkia. Palvelutapahtuma tarkoittaa IBM SaaS -tuotteeseen liittyviä asiantuntija- ja/tai koulutuspalveluja. Käyttöoikeuksia on hankittava kutakin Palvelutapahtumaa vastaava määrä.

3. Maksut ja laskutus

IBM SaaS -tuotteesta perittävä maksu määritetään Sopimusasiakirjassa.

3.1 Osittaiset kuukausimaksut

Sopimusasiakirjassa määritetty osittainen kuukausimaksu voidaan laskea suhteellisesti jaetun hinnan perusteella.

3.2 Ylitysmaksut

Jos toteutunut IBM SaaS -tuotteen käyttö ylittää Käyttölupatodistuksessa määritetyn käyttöoikeuksien määrän mittauskauden aikana, ylitys veloitetaan Asiakkaalta Sopimusasiakirjassa määritetyllä tavalla.

3.3 Asennuspalvelun maksut

Asiakasta veloitetaan asennuksesta Sopimusasiakirjassa määritetyllä tavalla.

4. Sopimuskausi ja uusimisvaihtoehdot

IBM SaaS -tuotteen sopimuskausi alkaa päivänä, jolloin IBM ilmoittaa Asiakkaalle, että tämä voi käyttää Käyttölupatodistuksessa mainittua IBM SaaS -tuotetta. Käyttölupatodistuksessa määritetään, uusiutuuko IBM SaaS -tilaus automaattisesti, jatkuuko se jatkuvana käyttönä vai päättyykö tilaus tilauskauden päättyessä.

Jos käytössä on automaattinen uusiutuminen, IBM SaaS -tilaus uusiutuu automaattisesti Käyttölupatodistuksessa määritetyn tilauskauden ajaksi, ellei Asiakas ilmoita kirjallisesti tilauksen uusimatta jättämisestä vähintään 30 päivää ennen tilauskauden päättymispäivämäärää.

Jos käytössä on jatkuva käyttö, IBM SaaS -tuote pysyy käytettävissä kuukausi kerrallaan, kunnes Asiakas ilmoittaa kirjallisesti tilauksen päättämisestä vähintään 30 päivää ennen haluttua päättämishetkeä. IBM SaaS -tuote pysyy käytössä sen kalenterikuukauden loppuun, jolloin kyseinen 30 päivän jakso päättyy.

5. Tekninen tuki

Sen jälkeen, kun IBM on ilmoittanut Asiakkaalle, että IBM SaaS -tuote on käytettävissä, teknistä tukea toimitetaan Tilauskauden aikana verkon keskusteluryhmissä ja vakiotukena sinä aikana, jolta Asiakkaalla on Käyttöön perustuvia maksuja. IBM SaaS -tuotteessa Asiakkaat voivat lähettää tukipyyntöjä tai pyytää apua verkkokeskusteluistunnossa. IBM antaa käyttöön IBM Software as a Service Support Handbook -tukioppaan, joka sisältää muiden tietojen ja prosessikuvausten ohella myös teknisen tuen yhteystiedot.

Vakavuustaso	Vakavuustason määritelmä	Vastausaikatavoitteet	Vastausajan voimassaolo
1	**Liiketoiminnan kannalta olennainen häiriö tai palvelun käyttökatko:** Liiketoiminnan kannalta olennaiset toiminnot eivät ole käytettävissä, tai tärkeä käyttöliittymä ei toimi. Tämä koskee tavallisesti tuotantoympäristöä ja merkitsee sitä, että palvelujen käytön epäonnistuminen haittaa toimintaa vakavasti. Tilanteeseen tarvitaan ratkaisu heti.	Yhden (1) tunnin kuluessa	24 x 7
2	**Merkittävä vaikutus liiketoimintaan:** Liiketoimintaan liittyvä palvelun ominaisuus tai toiminto toimii vakavan vajavaisesti, tai Asiakas on vaarassa ylittää liiketoimintaan liittyviä määräaikoja.	Kahden (2) tunnin kuluessa normaalina työaikana	Maanantaista perjantaihin normaalina työaikana
3	**Vähäinen vaikutus liiketoimintaan:** Merkitsee, että palvelu tai toiminto on käyttökelpoinen eikä häiriön vaikutus toimintaan ole vakava.	Neljän (4) tunnin kuluessa normaalina työaikana	Maanantaista perjantaihin normaalina työaikana

Vakavuustaso	Vakavuustason määritelmä	Vastausaikatavoitteet	Vastausajan voimassaolo
4	**Pieni vaikutus liiketoimintaan:** Tiedustelu tai muu kuin tekninen pyyntö	Yhden (1) työpäivän kuluessa	Maanantaista perjantaihin normaalina työaikana

5.1 Asiakkaan tietojen käyttö

IBM saa käyttää Asiakkaan tietoja selvittääkseen palveluun liittyvien ongelmien syitä sekä helpottaakseen palvelun tekemiä Asiakkaan sovellukseen kohdistuvia tarkistuksia. IBM käyttää tietoja ainoastaan vikojen korjaukseen tai toimittaakseen IBM-tuotteisiin tai -ohjelmiin liittyvää tukipalvelua.

6. IBM SaaS -tuotteiden lisäehdot

Tietoturvatarkistukset eivät välttämättä tunnista kaikkia sovellukseen sisältyviä tietoturvauhkia, eikä niitä ole suunniteltu eikä tarkoitettu käytettäviksi riskialttiissa ympäristöissä, joissa toiminnan on oltava ehdottoman varmaa. Tällaisia ympäristöjä (niihin rajoittumatta) ovat esimerkiksi ilma-alusten ohjausjärjestelmät, lennonjohtojärjestelmät, asejärjestelmät, elvytyslaitteet, ydinvoimalaitokset ja muut sovellukset, joissa turvallisuusriskin havaitsematta jääminen voi johtaa kuolemaan tai henkilö- tai omaisuusvahinkoon. Tietoturvatarkistusten ei taata toimivan keskeytyksittä ja virheittä.

Asiakkaan on mahdollista käyttää IBM SaaS -tuotetta apuna vaatimustenmukaisuuteen liittyvien velvoitteiden täyttämisessä. Velvoitteet voivat perustua lakeihin, säädöksiin, standardeihin tai käytäntöihin. Mitään Palvelun antamia ohjeita tai ehdottamia käyttötapoja ei ole tarkoitettu lainopillisiksi, kirjanpitoon liittyviksi tai muiksi asiantuntijan neuvoiksi, ja Asiakasta kehotetaan hankkimaan omat lainopilliset ja muut neuvonantajansa. Asiakas vastaa yksin sen varmistamisesta, että Asiakas ja Asiakkaan toimet, sovellukset ja järjestelmät vastaavat kaikkien sovellettavien lakien, säädösten, standardien ja käytäntöjen vaatimuksia. Tämän Palvelun käyttö ei takaa lakien, säädösten, standardien ja käytäntöjen vaatimustenmukaisuutta.

IBM SaaS -tuote tekee Asiakkaan tarkistettaviksi valitsemille Web-sivustoille sekä Web- ja mobiilisovelluksille sisäisiä ja ulkoisia testejä. Tietyt lait kieltävät kaikki luvattomat tietokonejärjestelmiin kohdistuvat tunkeutumis- tai käyttöyritykset. Asiakas myöntää IBM:lle valtuudet toteuttaa Palvelut tässä kuvatulla tavalla ja myöntää IBM:lle käyttöoikeuden Asiakkaan tietokonejärjestelmiin Palvelujen toimitusta varten. IBM voi luovuttaa tämän valtuutuksen kolmannelle osapuolelle, jos se on Palvelujen toimituksen kannalta välttämätöntä.

Testaukseen sisältyy tiettyjä riskejä, näihin rajoittumatta muun muassa seuraavia:

a. Asiakkaan tietokonejärjestelmät, joissa on ajossa testattavia sovelluksia, voivat lakata vastaamasta tai kaatua, mistä voi olla seurauksena järjestelmän tilapäinen käyttökeskeytys tai tietojen katoaminen

b. Asiakkaan järjestelmien sekä niihin liittyvien reitittimien ja palomuurien suorituskyky ja siirtonopeus voivat tilapäisesti heiketä testauksen aikana

c. testaus voi tuottaa huomattavan määrän lokisanomia, mistä voi aiheutua lokitiedostojen liiallista levytilan kulutusta

d. haavoittuvuuksien luotaus voi muuttaa tai poistaa tietoja

e. tunkeutumisen tunnistusjärjestelmät saattavat aktivoida hälytyksiä

f. testattavan Web-sovelluksen sähköpostitoiminto saattaa aktivoitua lähettämään sähköpostiviestejä

g. IBM SaaS -tuote voi pysäyttää valvottavan verkon liikenteen etsiäkseen tapahtumia.

Mitkään palvelutasosopimuksiin liittyvät oikeudet ja IBM:n korjaustoimet, jotka koskevat testattavia verkkosivustoja tai sovelluksia, eivät ole voimassa minkään testaustoiminnan aikana.

Jos Asiakas antaa Palveluun testattavan sovelluksen todennetut sisäänkirjauksen valtuustiedot, Asiakkaan tulee käyttää ainoastaan testitilien valtuustietoja, ei tuotantokäyttöön tarkoitettujen käyttäjätilien valtuustietoja. Jos käytetään tuotantokäyttöön tarkoitettujen käyttäjätilien valtuustietoja, Palvelun välityksellä voi siirtyä henkilötietoja.

IBM SaaS -tuote voidaan määrittää tarkistamaan tuotantokäytössä olevia Web-sovelluksia. Jos Asiakas valitsee tuotantokäyttöön kohdistuvan tarkistuslajin, Palvelu tekee tarkistukset tavalla, joka vähentää edellä mainittuja riskejä, mutta joissakin tilanteissa IBM SaaS -tuote kuitenkin aiheuttaa testattavissa

tuotantokäytön sivustoissa ja infrastruktuurissa suorituskyvyn heikkenemistä tai epävakautta. IBM ei anna mitään takuita tai lausumia IBM SaaS -tuotteen soveltuvuudesta käytettäväksi tuotantosivustojen tarkistukseen.

ASIAKAS VASTAA SEN SELVITTÄMISESTÄ, ONKO PALVELU TARKOITUKSENMUKAINEN JA TURVALLINEN ASIAKKAAN WEB-SIVUSTOLLE, WEB-SOVELLUKSILLE, MOBIILISOVELLUKSILLE JA TEKNISELLE YMPÄRISTÖLLE.

IBM SaaS -tuote on suunniteltu tunnistamaan lukuisia erilaisia mobiili- ja Web-sovelluksiin sekä Web-palveluihin liittyviä mahdollisia tietoturva- ja vaatimustenmukaisuusongelmia. Palvelu ei testaa kohteita kaikkien haavoittuvuuksien ja vaatimustenmukaisuuteen liittyvien riskien varalta, eikä se myöskään toimi suojana tietoturvaan kohdistuvia hyökkäyksiä vastaan. Tietoturvaan liittyvät uhkat, säädökset ja standardit muuttuvat jatkuvasti, eikä Palvelu välttämättä mukaudu kaikkiin tällaisiin muutoksiin. Asiakkaan Web-sovelluksen, järjestelmien ja työntekijöiden tietoturva ja vaatimustenmukaisuus sekä näihin liittyvät korjaustoimet ovat yksin Asiakkaan vastuulla. Palvelun tuottamien tietojen käyttö tai käyttämättä jättäminen perustuu yksinomaan Asiakkaan omaan harkintaan.

Tietyt lait kieltävät kaikki luvattomat tietokonejärjestelmiin kohdistuvat tunkeutumis- tai käyttöyritykset. ASIAKAS VASTAA SEN VARMISTAMISESTA, ETTÄ ASIAKAS EI KÄYTÄ PALVELUA MUIDEN KUIN SELLAISTEN WEB-SIVUSTOJEN JA/TAI SOVELLUSTEN TARKISTUKSEEN, JOTKA ASIAKAS OMISTAA TAI JOIDEN TARKISTUKSEEN ASIAKKAALLA ON OIKEUDET JA VALTUUDET.

Selvyyden vuoksi todetaan, että IBM:n käyttöehdot – Yleiset ehdot -ehtojen tietosuojaa käsittelevässä kohdassa kuvatun Asiakkaan sisällön katsotaan sisältävän tietoja, jotka voivat olla IBM:n käytettävissä Sovelluksen haavoittuvuustestauksen aikana.

6.1 Kolmannen osapuolen omistamat järjestelmät

Testauksen kohteena olevien kolmannen osapuolen omistamien järjestelmien (jotka tässä ehdossa tarkoittavat niihin rajoittumatta myös sovelluksia ja IP-osoitteita) osalta Asiakas hyväksyy seuraavat ehdot:

a. Ennen kuin IBM aloittaa testauksen kolmannen osapuolen järjestelmässä, Asiakas hankkii kunkin järjestelmän omistajalta allekirjoitetun luvan, jossa annetaan IBM:lle valtuudet toimittaa Palveluja kyseisessä järjestelmässä sekä ilmaistaan omistajan hyväksyntä kohdassa Permission to Perform Testing esitetyille ehdoille. Lisäksi Asiakas toimittaa IBM:lle tällaisen valtuutuksen kopion.

b. Asiakas vastaa yksin näissä järjestelmissä IBM:n etätestien tuloksena havaittujen uhkien, riskien ja haavoittuvuuksien tiedottamisesta järjestelmän omistajalle.

c. Asiakas järjestää mahdollisuuden järjestelmän omistajan ja IBM:n väliseen tietojenvaihtoon, jos IBM pitää sitä välttämättömänä.

Asiakas sitoutuu

- tiedottamaan IBM:lle heti minkä tahansa testauksen kohteena olevan järjestelmän omistussuhteen muutoksesta
- ilman IBM:ltä etukäteen saatua kirjallista suostumusta olemaan luovuttamatta toimitettavaa aineistoa ja paljastamatta Asiakkaan Konsernin ulkopuolelle sitä, että IBM on toimittanut Palvelut
- hyvittämään IBM:lle täysimääräisinä sellaisista kolmannen osapuolen vaateista IBM:lle mahdollisesti aiheutuvat menetykset tai korvausvastuut, joiden syynä on Asiakkaan laiminlyönti tässä kohdassa (Kolmannen osapuolen omistamat järjestelmät) esitettyjen vaatimusten noudattamisessa, sekä mahdolliset kolmannen osapuolen IBM:ää tai IBM:n alihankkijoita tai edustajia vastaan esittämät haasteet tai vaateet, joiden syynä on (a) tietoturvauhkien, riskien ja haavoittuvuuksien testaus testauksen kohteena olevissa järjestelmissä, (b) tällaisen testauksen tulosten toimitus Asiakkaalle tai (c) se, että Asiakas käyttää tuloksia hyväkseen tai paljastaa ne.

6.2 Evästeet

Asiakas on tietoinen siitä ja hyväksyy sen, että IBM voi normaalina IBM SaaS -palvelun toimintaan ja tukeen kuuluvana toimenpiteenä kerätä Asiakkaalta IBM SaaS -palvelun käyttöön liittyviä henkilötietoja (jotka voivat koskea Asiakkaan työntekijöitä ja alihankkijoita) seurannan ja muiden tekniikoiden avulla. Näin tehdessään IBM kerää käyttötilastoja ja tietoja IBM SaaS -palvelun tehokkuudesta parantaakseen käyttökokemusta ja mukauttaakseen vuorovaikutustaan Asiakkaan kanssa. Asiakas vahvistaa hankkivansa tai hankkineensa hyväksynnän sille, että IBM voi käsitellä kerättyjä henkilötietoja voimassa olevan lainsäädännön mukaisesti IBM:n sisäisesti tai muiden IBM-yhtiöiden ja niiden alihankkijoiden

välityksellä kaikkialla, missä IBM alihankkijoineen toimii. IBM noudattaa Asiakkaan työntekijöiden ja alihankkijoiden pyyntöjä tarkastella, päivittää, korjata tai poistaa heistä kerättyjä henkilötietoja.

Raportointitoimintoja sisältävän IBM SaaS -tuotteen osana IBM valmistelee ja ylläpitää IBM SaaS -tuotteesta kerättyjä tunnistustiedoista puhdistettuja tietoja ja/tai koostetietoja (Tietoturvatiedot). Tietoturvatietojen perusteella ei voi tunnistaa Asiakasta eikä yksittäisiä henkilöitä muutoin kuin jäljempänä kohdassa (d) mainitussa tapauksessa. Asiakas hyväksyy lisäksi sen, että IBM saa käyttää ja/tai kopioida Tietoturvatietoja ainoastaan seuraaviin tarkoituksiin:

a. Tietoturvatietojen julkaisu ja/tai jakelu (esimerkiksi kyberturvallisuuteen liittyvissä koosteissa tai analyyseissa)

b. tuotteiden tai palvelujen kehittäminen ja parantaminen

c. sisäisesti tai yhdessä kolmannen osapuolen kanssa tehdyt tutkimukset

d. kolmannen osapuolen rikoksentekijän tietojen lainmukainen ilmoittaminen.

6.3 Johdannaishyötyjen sijainnit

Verotus perustuu soveltuvin osin sijainteihin, joiden Asiakas määrittää hyötyvän IBM SaaS -tuotteesta. IBM soveltaa verotusta IBM SaaS -tuotteen tilauksen yhteydessä annetun liiketoimintaosoitteen perusteella ja käyttää kyseistä osoitetta ensisijaisena hyötyvänä sijaintina, ellei Asiakas toimita IBM:lle lisätietoja. Asiakas vastaa siitä, että kyseiset tiedot ovat ajan tasalla ja että mahdolliset muutokset toimitetaan IBM:lle.

6.4 Henkilötiedot, säännelty sisältö ja palvelut

Tätä IBM SaaS -tuotetta ei ole suunniteltu minkään tiettyjen sellaisten suojausvaatimusten mukaiseksi, jotka koskevat säänneltyä sisältöä, esimerkiksi henkilötietoja tai arkaluonteisia henkilötietoja. Asiakas vastaa sen selvittämisestä, täyttääkö tämä IBM SaaS -tuote Asiakkaan tarpeet sen sisällön lajin suhteen, jota Asiakas käyttää IBM SaaS -tuotteessa.

IBM ei toimi sellaisten palvelujen toimittajana, joita säätelee Yhdysvaltojen telehallintovirasto (FCC) tai valtion valvontaviranomainen (Valtion sääntelyviranomainen), eikä IBM myöskään aio toimittaa mitään palveluja, joita säätelee FCC tai Valtion sääntelyviranomainen. Jos FCC tai Valtion sääntelyviranomainen määrää mille tahansa IBM:n tämän sopimuksen perusteella toimittamille palveluille lakisääteisiä vaatimuksia tai velvoitteita, IBM voi (a) muokata, vaihtaa tai korvata tuotteita Asiakkaan kustannuksella ja/tai (b) muuttaa palvelujen toimitustapaa Asiakkaalle välttääkseen vaatimusten tai velvoitteiden soveltamisen IBM:ään (esimerkiksi toimimalla Asiakkaan edustajana ja hankkimalla palvelut kolmannen osapuolen telelaitokselta).

Liite A

1. IBM Application Security on Cloud -tuotteen yleiskuvaus

IBM Application Security on Cloud on keskitetty ratkaisu, jonka avulla Asiakas voi tunnistaa tietoturvauhkia (kuten SQL-injektion, sivustojen väliset komentosarjat ja tietovuodot) monista eri sovelluksista. Palvelu sisältää monia erilaisia sovellusten tietoturvan tarkistustekniikoita, joista kukin tunnistaa kyseisen sovelluksen tietoturvaongelmia.

IBM Application Security on Cloud sisältää seuraavat toiminnot:

- Tietoturvauhkien etsintä mobiilisovelluksista. Tämä toteutetaan dynaamisten (blackbox) ja vuorovaikutteisten (glassbox) tietoturvan analyysitekniikoiden avulla.
- Tietoturva-aukkojen etsintä tuotanto- tai esituotantotilassa olevista, julkisesti käsiteltävissä olevista tai yksityisissä verkoissa sijaitsevista Web-sivustoista. Tämä toteutetaan dynaamisten (blackbox) tietoturvan analyysitekniikoiden avulla.
- Tietoturva-aukkojen etsintä Web- ja työasemasovellusten tietovirroista. Tämä toteutetaan staattisten (whitebox) tietoturvan analyysitekniikoiden avulla.
- Kehittäjät voivat seurata yksityiskohtaisia tietoturva-aukkoraportteja, jotka sisältävät sekä ylätason tiivistelmät löydöksistä että korjaustoimet.
- Integrointi moniin DevOps-käyttöympäristöihin.

1.1 IBM Application Analyzer

IBM Application Analyzer -tuotteen voi tilata Sovellusilmentymänä, Työkohtaisena (tarkistuskohtaisena) ilmentymänä tai täytenä Ilmentymänä. Tuotteen avulla voi tehdä seuraavia tarkistuksia:

- Dynamic Analyzer – esituotanto- tai tuotantovaiheen verkkosivustojen testaus DAST-tekniikoilla
- Mobile Analyzer – iOS- tai Android-binaarikoodin testaus IAST-tekniikoilla
- Static Analyzer – tavu- tai lähdekooditietovirran testaus SAST-tekniikoilla.

1.2 Asennuspalvelu

IBM Application Security on Cloud Consulting Services on Application Analyzer -tuotetta varten kehitetty asennuspalvelu. Palvelussa IBM:n konsultit opastavat ja avustavat sovelluksiin liittyvien uhkien testauksessa ja hallinnassa. IBM Application Security on Cloud Consulting Services -palvelut hankitaan Palvelutapahtumien paketteina, joita voi käyttää jäljempänä esitettyjen määrien mukaisesti seuraavia palveluja varten:

a. **Fast Start -palvelu** [kuluttaa yhden (1) Palvelutapahtuma-yksikön]

Fast Start -palvelussa Asiakas saa Application Security on Cloud -tuotteen testaus- ja riskienhallintaominaisuuksien käytössä tarvittavaa asiantuntemusta ja opastusta. Kun Asiakas on vahvistanut onnistuneen kirjautumisen Application Security on Cloud -portaaliin, IBM auttaa järjestämään enintään kaksi (2) tuntia kestävän, kahden (2) aktiivisen osanottajan välisen verkkoneuvottelun, jonka aiheena on peruskoulutus AppSec on IBM SaaS -kokoonpanoihin ja -toimintoihin. Näitä ovat esimerkiksi tarkistuslajit, tarkistusten ajo, raporttien arviointi sekä ympäristöön liittyvien työkalujen ja lisäosien asennus. Fast Start -palvelu päättyy, (a) kun Asiakasta on koulutettu verkkoseminaarissa, (b) kun asianmukaiset työkalut ja lisäosat on asennettu ja (c) kun Asiakasta on avustettu määrittämään ja ajamaan Asiakkaan ensimmäinen tarkistus.

b. **Assessment Review -palvelu** [kuluttaa kaksi (2) Palvelutapahtuma-yksikköä]

Assessment Review -palvelussa Asiakasta autetaan arvioimaan testitulosta sekä ymmärtämään ja priorisoimaan sovelluksen haavoittuvuuksien edellyttämiä korjaustoimia. IBM auttaa järjestämään enintään yhden (1) tunnin kestävän, kahden (2) aktiivisen osanottajan välisen verkkoneuvottelun, jonka aiheena ovat löydettyjen haavoittuvuuksien yleiskuvaus ja sovelluksen aiheuttama kokonaistietoturvauhka. Lisäksi keskustellaan yksityiskohtaisesti löydetyistä sovelluksen tietoturva-aukoista muun muassa seuraavista näkökulmista: (1) miten haavoittuvuutta testattiin, (2) miten haavoittuvuudet havaittiin, (3) millaisen riskin kukin haavoittuvuus aiheuttaa ja (4) mitkä ovat haavoittuvuuden korjaamista koskevat yleiset suositukset. Arviointi perustuu ainoastaan testitulokseen, eikä kyseessä ole itse lähdekoodin arviointi. Asiakas arvioi testituloksen ja osoittaa

IBM:lle arvioitavan testituloksen ennen verkkoneuvottelua. Assessment Review -palvelu päättyy, kun verkkoneuvottelu on pidetty.

c. **Scan for Me -palvelu** [kuluttaa neljä (4) Palvelutapahtuma-yksikköä]

Scan for Me -palvelussa IBM:n sovellustietoturva-asiantuntija määrittää ja ajaa tarkistuksen, tarkistaa tulokset ja arvioi löydökset pitämässään raportin selostustilaisuudessa. Asiakas antaa IBM:n konsultille käyttöoikeuden Asiakkaan ASoC-ympäristöön, jotta konsultti voi määrittää ja ajaa tarkistuksen, tarkistaa tulokset, antaa korjaustoimien priorisointiin liittyviä suosituksia ja pitää tuloksia esittelevän raportin selostustilaisuuden. IBM auttaa järjestämään enintään yhden (1) tunnin kestävän, kahden (2) aktiivisen osanottajan välisen verkkoneuvottelun, jonka aiheena ovat löydettyjen haavoittuvuuksien yleiskuvaus ja sovelluksen aiheuttama kokonaistietoturvauhka. Lisäksi keskustellaan yksityiskohtaisesti löydetyistä sovelluksen tietoturva-aukoista muun muassa seuraavista näkökulmista: (1) miten haavoittuvuutta testattiin, (2) miten haavoittuvuudet havaittiin, (3) millaisen riskin kukin haavoittuvuus aiheuttaa ja (4) mitkä ovat haavoittuvuuden korjaamista koskevat yleiset suositukset. IBM tekee pyydettäessä ja enintään 30 päivää alkuperäisen tarkistuksen jälkeen uuden tarkistuksen, jossa käytetään alkuperäistä tarkistusmääritystä ja tarkistetaan ainoastaan suojauskorjaukset, tarkistetaan tulokset ja toimitetaan raportti Asiakkaalle. Uusintatarkistuksessa ei testata uusia toimintoja. Scan for Me -palvelu päättyy, kun alkuperäisen tarkistuksen tuloksia arvioiva verkkoneuvottelu on pidetty tai kun Asiakkaan pyytämä uusintatarkistus on tehty ja sen raportti toimitettu Asiakkaalle.

d. **Advisor on Demand -palvelu** [kuluttaa seitsemän (7) Palvelutapahtuma-yksikköä]

Advisor on Demand -palvelu sisältää enintään kaksikymmentä (20) tuntia IBM:n konsultin aikaa, joka voidaan käyttää IBM SaaS -tuotteeseen liittyviin toimiin. IBM:n konsultti auttaa sovelluksen tietoturvaan liittyvissä aiheissa, joita voivat olla niihin rajoittumatta ohjelman hallinta, tietoturvatestauksen priorisointi, korjaustoimia koskevat strategiat, lähdekoodin analysointi ja lähdekoodin korjaus. IBM tekee yhteistyötä Asiakkaan kanssa laatiakseen Asiakkaan erityisvaatimusten mukaisen projektiaikataulun, jossa otetaan huomioon esimerkiksi projektin tavoitteet, asiaankuuluvat tekniikat, halutut etenemisaikataulut, odotuksenmukainen toimitettava aineisto sekä Advisor on Demand -palvelutapahtumien arvioitu määrä. Asiakkaan on annettava käyttöoikeudet palvelujen toimituksessa tarvittaviin sovelluksiin, järjestelmiin ja asiakirjoihin. Advisor on Demand -palvelut päättyvät, kun enintään 20 tuntia tietoturva-asiantuntijan apua on toimitettu ja/tai kun projektiaikataulu ja/tai projektiaikataulussa määritetty ja dokumentoitu toimitettava aineisto on toimitettu Asiakkaalle.

e. **Sovelluksen haavoittuvuustestaus**

Kolme vaihtoehtoa:

(1) **Yhteensopivuuteen keskittyvä / perustason sovelluksen haavoittuvuustesti**, joka sisältää enintään neljäkymmentä (40) tuntia Konsultin aikaa ja jossa keskitytään yksivaiheisen logiikan virheisiin ja yksinkertaisiin koodi-injektion mahdollistaviin virheisiin. Kuluttaa viisitoista (15) Palvelutapahtuma-yksikköä.

(2) **Vakiomuotoinen sovelluksen haavoittuvuustesti**, joka sisältää enintään kuusikymmentä (60) tuntia Konsultin aikaa ja jossa keskitytään myös monivaiheisten käsittelyreittien logiikkavirheisiin sekä monimutkaisiin koodi-injektion mahdollistaviin virheisiin ja monimutkaisten tietolajien analysointiin. Kuluttaa kaksikymmentäyksi (21) Palvelutapahtuma-yksikköä.

(3) **Kehittynyt sovelluksen haavoittuvuustesti**, joka sisältää enintään kahdeksankymmentä (80) tuntia Konsultin aikaa ja jossa lisäksi keskitytään käännettyjen ohjelmatiedostojen purkamiseen, mukautettujen verkkoyhteyskäytäntöjen huolelliseen tarkasteluun ja yleisesti saatavilla olevien kirjastojen ja käyttöympäristöjen syvälliseen analysointiin. Kuluttaa kaksikymmentäseitsemän (27) Palvelutapahtuma-yksikköä.

Sovelluksen haavoittuvuuden testauspalvelussa IBM:n resurssi testaa sovelluksen haavoittuvuuksien varalta, toimittaa Asiakkaalle testiraportin ja pitää raportin selostustilaisuuden, jossa esitellään löydökset ja niihin liittyvät uhkat.

IBM auttaa järjestämään enintään yhden (1) tunnin kestävän, kahden (2) aktiivisen osanottajan välisen projektin aloituspuhelun, jossa arvioidaan Asiakkaan ympäristö ja organisaatio, mukaan lukien sovelluskäyttöympäristö, arkkitehtuuri, käyttöympäristöt, tuki-infrastruktuuri, sovellukseen

liittyvät tunnetut tietoturvaongelmat tai huolenaiheet, alustava testausaikataulu ja hätätilanteiden yhteydenottosuunnitelma.

IBM tekee sovelluksen haavoittuvuustestauksen, joka sisältää niihin rajoittumatta esimerkiksi seuraavat tehtävät: tavallisten haavoittuvuuksien tunnistus (esimerkiksi SQL-injektio ja sivustojen väliset komentosarjat), nykyisten suojausmekanismien (esimerkiksi syötteen tarkistuksen, todennuksen ja valtuutuksen) vahvuuksien ja heikkouksien arviointi, liiketoimintalogiikan asianmukaisen toteutumisen tarkistus, suojattujen yhteyskäytäntöjen asianmukaisen käytön tarkistus, istuntojen käsittelyn virheiden tunnistus sekä sen varmistaminen, että asianmukaiset suojausmekanismit ovat käytössä sisäänkirjauksessa, salasanan palautuksessa, salasanakäytännöissä ja muissa käyttäjien hallintatoiminnoissa. Löydökset kirjataan sovelluksen haavoittuvuustestin raporttiin. IBM auttaa järjestämään enintään yhden (1) tunnin kestävän verkkoneuvottelun raportin selostustilaisuutta varten. Sovelluksen haavoittuvuuden testauspalvelu päättyy, kun siihen osoitettu konsultointiaika on käytetty, verkkoneuvottelu pidetty ja lopullinen sovelluksen haavoittuvuustestin raportti toimitettu Asiakkaalle.

1.2.1 Asennuspalveluihin liittyvät velvollisuudet

IBM

- toimittaa Asennuspalvelut Käyttölupatodistuksen mukaisesti käyttämällä Asiakkaan hankkimia Palvelutapahtuma-yksikköjä
- on toimittanut Asennuspalvelut, kun kohdassa 1.2 kuvatut valmistumiskriteerit on täytetty.

Asiakas sitoutuu

- vastaamaan kaikkiin Asiakkaan sopimuskauden aikana esittämiin Palvelutapahtuma-pyyntöihin liittyvistä kaikista maksuista
- siihen, että hankitut Palvelutapahtuma-yksiköt on käytettävä ensimmäisen sopimuskauden aikana ja että sopimuskauden päättymispäivään mennessä käyttämättömät Palvelutapahtuma-yksiköt vanhenevat
- esittämään kaikista Asennuspalveluista muodollisen pyynnön vähintään 30 päivää ennen tilauksen päättymispäivää.

IBM voi pyytää Asiakkaalta minkä tahansa Asennuspalvelun toimituksen yhteydessä tietoja ja kohtuullista yhteistyötä. Jos Asiakas ei toimita pyydettyjä tietoja tai osallistu pyydettyyn yhteistyöhön viipymättä, seurauksena voi IBM:n harkinnan mukaan olla palvelujen tarpeiden mukaisia Palvelutapahtuma-yksikkömaksuja tai asiaankuuluvan palvelun viivästyminen.

Jotta IBM voi toteuttaa testauksen virheettömästi, Asiakas sitoutuu testauskauden aikana noudattamaan IBM:n ohjeita ympäristön valmistelussa ja ylläpidossa.