IBM Application Security on Cloud

A Felhasználási Feltételeket („Felhasználási Feltételek”) a jelen IBM Felhasználási Feltételek – SaaS Ajánlatra Vonatkozó Feltételek („SaaS Ajánlatra Vonatkozó Feltételek”) és az IBM Felhasználási Feltételek – Általános Feltételek („Általános Feltételek”) című dokumentum alkotja, amely a következő URL-címen érhető el: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

Abban az esetben, ha ellentmondás merül fel, a SaaS Ajánlatra Vonatkozó Feltételek elsőbbséget élveznek az Általános Feltételekkel szemben. Az IBM SaaS megrendelésével, elérésével vagy használatával az Ügyfél elfogadja a Felhasználási Feltételeket.

A jelen Felhasználási Feltételeket a vonatkozó IBM Nemzetközi Passport Advantage Megállapodás, az IBM Nemzetközi Passport Advantage Express Megállapodás vagy az IBM Nemzetközi Megállapodás Kijelölt IBM SaaS Ajánlatokhoz („Megállapodás”) feltételei szabályozzák, és a Felhasználási Feltételekkel együtt ezek alkotják a teljes megállapodást.

1. IBM SaaS (Szoftver mint Szolgáltatás)

A következő IBM SaaS (szoftver mint szolgáltatás) ajánlatokra ezen SaaS Speciális Ajánlati Feltételek érvényesek:

- IBM Application Security Analyzer

2. Díjakkal kapcsolatos mérőszámok

Az IBM SaaS értékesítése a következő díjszabási egységek egyike szerint történik, a Tranzakciós Dokumentumban meghatározottak szerint:

a. **Alkalmazáspéldány** – olyan mértékegység, amely alapján az IBM SaaS megvásárolható. Az Alkalmazás minden olyan példányához Alkalmazáspéldány-jogosítvány szükséges, amely csatlakozik az IBM SaaS szolgáltatáshoz. Amennyiben az Alkalmazás több összetevőt tartalmaz, amelyek mindegyike külön célt és/vagy felhasználói bázist szolgál ki, és amelyek mindegyike csatlakoztatható az IBM SaaS szolgáltatáshoz vagy kezelhető az által, az ilyen összetevők mindegyike külön alkalmazásnak tekintendő. Emellett az Alkalmazások tesztelési, fejlesztési, állomásoztatási, illetve üzemi környezetei az Alkalmazás egy-egy külön példányának tekintendők, és ezek mindegyikéhez külön jogosítvány szükséges. Az Alkalmazás külön példányainak tekintendő az egyetlen környezetben lévő több Alkalmazáspéldány, és ezek mindegyikéhez is külön jogosítvány szükséges. Megfelelő jogosultságokat kell beszerezni, amelyek lefedik az IBM SaaS szolgáltatáshoz csatlakozó Alkalmazáspéldányok számát az Ügyfél Felhasználási Engedélyében (PoE) vagy a Tranzakciós Dokumentumban meghatározott mérési időszak során.

b. **Hozzáférés** – olyan mértékegység, amely alapján az IBM SaaS megvásárolható. A Hozzáférés az IBM SaaS használatára vonatkozó jogosultságokat jelenti. Az Ügyfélnek egyszeri Hozzáférési jogosultságot kell beszereznie az IBM SaaS az Ügyfél Felhasználási Engedélyében (PoE) vagy a Tranzakciós Dokumentumban meghatározott mérési időszak során történő használatához.

3. Díjak és számlázás

Az IBM SaaS termékért fizetendő összeg egy Tranzakciós Dokumentumban van meghatározva.

3.1 Használatalapú fizetés

A Használatalapú fizetés számlázása a Tranzakciós Dokumentumban meghatározott díjszabás szerint, a szolgáltatás használatát követő hónapban történik.

3.2 Részleges Havi Díj

A Tranzakciós Dokumentumban meghatározottak alapján részleges havi díj állapítható meg előzetesen.

4. Technikai Támogatás

Az Előfizetési Időszak alatt és azt követően, hogy az IBM értesíti az Ügyfelet arról, hogy az IBM SaaS elérhető, a technikai támogatás online fórumok útján és alapszintű támogatásként érhető el azon időszak alatt, amely során az Ügyfelet Használatalapú fizetési (Pay per Use) díjak terhelik. Az IBM SaaS szolgáltatáson belülről az Ügyfelek hibajegyet nyújthatnak be, vagy egy csevegési munkamenet megnyitásával csevegésben kérhetnek segítséget. Az IBM rendelkezésre bocsátja az IBM

Szolgáltatásként kínált szoftver Támogatási kézikönyvet, amely a technikai támogatás kapcsolati információit, illetve egyéb információkat és folyamatokat tartalmaz.

Súlyosság	Súlyosság meghatározása	Válaszidő célértékei (RTO)	Válaszadási időablak (RTC)
1	**Kritikus üzleti hatás/szolgáltatásleállás:** Egy, az üzletmenet szempontjából kritikus fontosságú funkció nem működik, vagy egy kritikus fontosságú felület meghibásodott. Ez általában a termelési környezetben fordul elő, és azt jelzi, hogy nem lehet hozzáférni a szolgáltatásokhoz, ez pedig kritikus hatással van a működésre. Ez az állapot azonnali megoldást igényel.	1 órán belül	A hét 7 napján, napi 24 órában (7x24)
2	**Jelentős üzleti hatás:** A szolgáltatás egyes üzleti jellemzői vagy a szolgáltatás egyes funkciói csak jelentős korlátozások mellett használhatóak, vagy fennáll a veszély, hogy az üzleti határidők az esemény miatt nem tarthatók.	Munkaidőben 2 órán belül	Hétfőtől péntekig munkaidőben
3	**Kisebb mértékű üzleti hatás:** A szolgáltatás vagy a funkciók használhatók, és a probléma nincs kritikus hatással a működésre.	Munkaidőben 4 órán belül	Hétfőtől péntekig munkaidőben
4	**Minimális üzleti hatás:** Kérdés vagy nem műszaki jellegű kérés	1 munkanapon belül	Hétfőtől péntekig munkaidőben

4.1 Hozzáférés az Ügyfél adataihoz

Az IBM a szolgáltatással kapcsolatosan felmerülő hibák diagnosztizálása és az Ügyfél alkalmazásának a szolgáltatás általi vizsgálata érdekében hozzáférhet az Ügyfél adataihoz. Az IBM az adatokhoz kizárólag a hibák javítása, illetve az IBM termékek és szolgáltatások támogatásának biztosítása érdekében fér hozzá.

5. Az IBM SaaS - Szoftver mint szolgáltatás ajánlat további feltételei

A Biztonsági vizsgálatok nem feltétlenül képesek az összes biztonsági kockázatot azonosítani az egyes alkalmazásokban.

Az IBM SaaS az Ügyfél jogszabályokon, rendeleteken, szabványokon vagy gyakorlaton alapuló kötelezettségeinek betartásában nyújthat segítséget. A Szolgáltatás által biztosított utasítások, használati javaslat vagy útmutatás nem minősülnek jogi, könyvelési vagy egyéb szakmai tanácsnak, és az Ügyfélnek saját jogi vagy egyéb tanácsadóval kell rendelkeznie. Kizárólag az Ügyfél felelőssége annak biztosítása, hogy az Ügyfél, valamint tevékenységei, alkalmazásai és rendszerei megfeleljenek a vonatkozó jogszabályoknak, szabályozásoknak, szabványoknak és gyakorlatoknak. A Szolgáltatás használata nem garantálja a jogszabályoknak, rendeleteknek, szabványoknak vagy gyakorlatnak való megfelelést.

Az IBM SaaS invazív és nem invazív vizsgálatokat végez az Ügyfél által vizsgálatnak alávetett webhelyen és webes vagy mobilalkalmazáson, amely vizsgálat bizonyos kockázatokkal járhat, beleértve korlátozás nélkül a következőket:

a. az Ügyfél a vizsgálat alatt álló alkalmazásokat futtató számítógépes rendszerei lefagyhatnak vagy összeomolhatnak, ami a rendszer ideiglenes elérhetetlenségét vagy adatvesztést eredményezhet;

b. az Ügyfél rendszereinek teljesítménye és sebessége, valamint a társított útválasztók és tűzfalak teljesítménye és sebessége ideiglenesen csökkenhet a vizsgálat ideje alatt;

c. túlzott mennyiségű naplóüzenet keletkezhet, ami a naplófájlok túlzott tárhelyfoglalását vonhatja maga után;

d. adatok módosulhatnak vagy törlődhetnek a sérülékenységi tesztelés eredményeképp;

e. a behatolásérzékelő rendszerek riasztásokat aktiválhatnak;

f. a vizsgált webes alkalmazás e-mail szolgáltatása e-maileket küldhet;

és

g. a felhőszolgáltatás elfoghatja a megfigyelt hálózat forgalmát események után kutatva.

Abban az esetben, ha az Ügyfél a vizsgálat alatt álló alkalmazás hitelesített bejelentkezési adatait beviszi a Szolgáltatásba, az Ügyfél az ilyen hitelesítő adatokat kizárólag a tesztfiókokhoz adja meg, a termelési felhasználókhoz ne. A termelési felhasználók hitelesítő adatainak használata személyes adatok átvitelét eredményezheti a Szolgáltatáson keresztül.

Az IBM SaaS konfigurálható termelési webes alkalmazások vizsgálatára. A szolgáltatás úgy lett kialakítva, hogy amennyiben az Ügyfél a vizsgálat típusát „termelésre" állítja, a fent felsorolt kockázatok csökkennek; mindazonáltal bizonyos esetekben a Felhőszolgáltatás a teljesítmény csökkenéséhez vagy instabilitáshoz vezethet a vizsgált termelési helyeken és infrastruktúrában. Az IBM semmilyen jótállást, sem szavatosságot nem vállal és semmilyen nyilatkozatot nem tesz azzal kapcsolatban, hogy a Felhőszolgáltatás használata termelési helyek vizsgálatára alkalmas.

AZ ÜGYFÉL FELELŐSSÉGE MEGÁLLAPÍTANI, HOGY A SZOLGÁLTATÁS MEGFELELŐ VAGY BIZTONSÁGOS-E AZ ÜGYFÉL WEBHELYE, WEBES ALKALMAZÁSA, MOBILALKALMAZÁSA VAGY MŰSZAKI KÖRNYEZETE SZÁMÁRA.

Az IBM SaaS alkalmas számos potenciális biztonsági és megfelelőségi probléma a mobil- és webes alkalmazásokban és a webszolgáltatásokban való azonosítására. Nem teszteli az összes biztonsági rést vagy megfelelőségi kockázatot, és nem akadályozza meg a biztonsági rendszerre irányuló támadásokat. A biztonsági fenyegetések, szabályozások és szabványok folyamatosan változnak, és a Szolgáltatás nem feltétlenül alkalmazkodik minden ilyen természetű változáshoz. Az Ügyfél webes alkalmazásának, rendszereinek és alkalmazottainak biztonságáért és megfelelőségéért, valamint a helyreállító műveletek végrehajtásáért kizárólag az Ügyfél felelős. Az Ügyfél saját belátása szerint használhatja fel vagy mellőzheti a Szolgáltatás által biztosított információkat.

Egyes jogszabályok tiltják a számítógépes rendszerekbe való bármilyen engedély nélküli behatolási vagy hozzáférési kísérletet. AZ ÜGYFÉL FELELŐSSÉGE BIZTOSÍTANI, HOGY AZ ÜGYFÉL A SZOLGÁLTATÁST NEM HASZNÁLJA OLYAN WEBHELYEK ÉS/VAGY ALKALMAZÁSOK VIZSGÁLATÁRA, AMELY WEBHELYEK ÉS/VAGY ALKALMAZÁSOK NEM KÉPEZIK AZ ÜGYFÉL TULAJDONÁT, VAGY AMELYEK VIZSGÁLATÁRA NEM JOGOSULT VAGY RENDELKEZIK ENGEDÉLLYEL.

5.2 Sütik (cookie)

Az Ügyfél tudatában van és elfogadja, hogy az IBM az IBM SaaS ajánlat normál működésének és támogatásának részeként nyomon követés és egyéb technológiák révén az IBM SaaS felhasználásához kapcsolódó személyes információkat gyűjthet az Ügyfélről (annak alkalmazottairól és alvállalkozóiról). Az IBM használati statisztikák és az IBM SaaS ajánlat hatékonyságával kapcsolatos információk begyűjtése érdekében végzi ezt a tevékenységet, amelynek célja a felhasználói élmény javítása és/vagy az interakcióknak az Ügyfél igényeihez való igazítása. Az Ügyfél ezúton megerősíti, hogy megszerzi vagy megszerezte a szükséges hozzájárulásokat annak engedélyezéséhez, hogy az IBM a fenti célokra feldolgozza a gyűjtött személyes információkat az IBM vállalaton belül, más IBM vállalatokban, valamint ezek alvállalkozói által a saját vagy alvállalkozói üzletmenetének részeként, a vonatkozó jogszabályoknak megfelelően. Az IBM teljesíti az Ügyfél alkalmazottaitól és alvállalkozóitól származó, a gyűjtött személyes információk elérésére, frissítésére, javítására vagy törlésére irányuló kéréseket.

5.3 Származtatott előnyökkel járó helyszínek

Adott esetben az Ügyfél által az IBM SaaS termék használatából származó haszon realizálásának helyeként megjelölt hely(ek) alapján kell adót fizetni. Az IBM a felsorolt üzleti címek alapján alkalmazza az adókat az IBM SaaS rendelésekor az elsődleges előnyben részesülő helyen, hacsak az Ügyfél külön információkat nem bocsát az IBM rendelkezésére. Az Ügyfél felelősséggel tartozik azért, hogy az erre vonatkozó információkat naprakészen tartsa, és tájékoztassa az IBM vállalatot az esetleges változtatásokról.

„A” Függelék

1. Az IBM Application Security on Cloud általános leírása

Az IBM Application Security on Cloud segítségével az Ügyfél egyetlen helyen azonosíthatja a különféle alkalmazások biztonsági hiányosságait (például az SQL-injektálást, a helyközi, parancsfájlt alkalmazó támadásokat és az adatszivárgást). A szolgáltatás az alkalmazások biztonsági ellenőrzési technikáinak különféle típusait tartalmazza, amelyek mindegyike azonosítja az adott alkalmazás biztonsági hibáit.

Az IBM Application Security on Cloud a következő képességeket biztosítja:

- Mobilalkalmazások biztonsági hiányosságainak ellenőrzése. Ez dinamikus (fekete dobozos – blackbox) és interaktív (üveg dobozos – glass box) biztonsági elemzési technológiákkal történik.
- Termelési és termelés előtti webhelyek biztonsági hiányosságainak ellenőrzése. Ez dinamikus (fekete dobozos – blackbox) biztonsági elemzési technikákkal történik.
- Webes és asztali alkalmazásokon belüli adatfolyamok biztonsági hiányosságainak ellenőrzése. Ez statikus (fehér dobozos – whitebox) biztonsági elemzési technikákkal történik.
- Biztonsági hiányosságokkal kapcsolatos részletes jelentések, amelyek az eredmények magas szintű összegzéseit és a fejlesztők által követhető helyreállítási lépéseket tartalmazzák.
- Integráció különböző DevOps platformokkal (például: Maven és IBM UrbanCode)