

# IBM Felhasználási Feltételek – SaaS Ajánlatra Vonatkozó Feltételek

---

## 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 jelen SaaS Ajánlatra Vonatkozó Feltételek az alábbi IBM SaaS ajánlatokra vonatkoznak:

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

### 2. Díjakkal kapcsolatos mérőszámok

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

- Feladat** – olyan mértékegység, amely alapján az IBM SaaS megvásárolható. A Feladat (Job) egy olyan objektum az IBM SaaS ajánlaton belül, amely nem osztható további részekre, és egy számítási folyamatot jelöl, beleértve annak részfolyamatait. Megfelelő felhasználási engedélyeket kell beszerezni annak érdekében, hogy az Ügyfél Felhasználási Engedélyében (PoE) vagy a Tranzakciós Dokumentumban meghatározott mérési időszakban az IBM SaaS által feldolgozott vagy kezelt Feladatok teljes számára kiterjedjen a feljogosítás.
- 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 jogosultság szükséges. Megfelelő jogosultságokat kell beszerezni, amelyek lefedik az IBM SaaS szolgáltatáshoz csatlakozó Alkalmazáspéldányok számát az Ügyfél PoE engedélyében vagy a Tranzakciós Dokumentumban meghatározott mérési időszak során.

A jelen IBM SaaS esetében:

- Dinamikus teszteléshez: egy nyilvános vagy privát URL-címen elérhető webhely. Az Alkalmazás minden egyes példánya feljogosít egy akár 1000 oldalt tartalmazó webhelyre egyetlen tartományon.
- Statikus teszteléshez: egy egyetlen programozási nyelven végrehajtható kódegység. Az Alkalmazás minden egyes példánya feljogosít akár 1 millió soros kódegységek vizsgálatára.
- Mobil teszteléshez: egy mobilkészítőn végrehajtható bináris kódegység. Minden egyes különböző mobilplatformhoz (például iOS és Android) az Alkalmazás egy külön példánya szükséges.

- c. **Példány** – olyan mértékegység, amely alapján az IBM SaaS megvásárolható. A Példány hozzáférést biztosít az IBM SaaS egy megadott konfigurációjához. Megfelelő jogosultságokat kell beszerezni az IBM SaaS minden egyes Példányához, amely az Ügyfél Felhasználási Engedélyében (PoE) vagy a Tranzakciós Dokumentumban meghatározott mérési időszak során hozzáférhető és használható.

Az egyes Példányjogosultságok esetén nem korlátozott a végrehajtható Feladatok vagy az Alkalmazáspéldányok (a csatlakoztatott Alkalmazások) száma, feltéve, hogy egyszerre legfeljebb 30 Feladat futtatható.

- d. **Részvétel** – olyan mértékegység, amely alapján a szolgáltatások megvásárolhatók. A Részvétel az IBM SaaS termékhez kapcsolódó szakmai és/vagy képzési szolgáltatásokból áll. Az egyes Részvételek biztosításához megfelelő jogosultságokat kell beszerezni.

### 3. Díjak és számlázás

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

#### 3.1 Részleges Havi Díjak

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

#### 3.2 Többlethasználat díjak

Ha a tényleges IBM SaaS használat a mérési időszak alatt meghaladja a Felhasználási Engedélyben meghatározott jogosultságot, az Ügyfélnek a Tranzakciós Dokumentumban meghatározottak szerint többlethasználati díjat kell fizetnie.

#### 3.3 Telepítési díjak

Az Ügyfélnek a Tranzakciós Dokumentumban meghatározott telepítési díjat kell kifizetnie.

### 4. Előfizetési időszak és Megújítási lehetőségek

Az IBM SaaS előfizetési időszaka azon a napon kezdődik, amikor az IBM értesíti az Ügyfelet, hogy hozzáféréssel rendelkezik az IBM SaaS termékhez, a Felhasználási Engedélyben (PoE) dokumentáltaknak megfelelően. A Felhasználási Engedély (PoE) határozza meg, hogy az IBM SaaS automatikusan megújul, folyamatos használat alapján folytatódik vagy megszűnik az előfizetési időszak végén.

Az automatikus megújulás esetében, amennyiben az Ügyfél nem kéri írásban a megújítás felfüggesztését az előfizetési időszak lejárat dátuma előtt legalább 30 nappal, az IBM SaaS automatikusan megújul a Felhasználási Engedélyben meghatározott időszakra.

Folyamatos használat esetén az IBM SaaS folyamatosan, hónapról hónapra elérhető, amíg az Ügyfél nem kéri 30 nappal korábban írásos értesítés formájában a megszüntetést. Az IBM SaaS a 30 napos időszak lejárat után a naptári hónap végéig elérhető marad.

### 5. 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 Használat alapú 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	<b>Kritikus üzleti hatás/szolgáltatásleállás:</b> Egy, az üzletmenet szempontjából kritikus fontosságú funkció nem működik, vagy egy kritikus fontosságú interfész 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)

Súlyosság	Súlyosság meghatározása	Válaszidő célértékei (RTO)	Válaszadási időablak (RTC)
2	<b>Jelentős üzleti hatás:</b> A szolgáltatás egyes üzleti jellemzői vagy a szolgáltatás egyes funkciói csak jelentős korlátozások mellett használhatók, vagy fennáll a veszély, hogy az Ügyfél nem tudja tartani az üzleti határidőket.	Munkaidőben 2 órán belül	Hétfőtől péntekig munkaidőben
3	<b>Kisebb mértékű üzleti hatás:</b> A szolgáltatás vagy a funkciók használhatók, és a probléma nincs kritikus hatással a működésre.	Munkaidőben 4 órán belül	Hétfőtől péntekig munkaidőben
4	<b>Minimális üzleti hatás:</b> Kérdés vagy nem műszaki jellegű kérés	1 munkanapon belül	Hétfőtől péntekig munkaidőben

## 5.1 Hozzáférés az Ügyfél adataihoz

Az IBM a szolgáltatással kapcsolatos 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.

## 6. Az IBM SaaS - Szoftver mint szolgáltatás ajánlat további feltételei

A biztonsági vizsgálatok nem feltétlenül azonosítják egy alkalmazás minden biztonsági kockázatát, továbbá nem arra tervezték és szánták azokat, hogy hibamentes működést igénylő, veszélyes környezetben működjenek, beleértve, de nem kizárólagosan a repülőgép-navigációs rendszereket, a légi irányítási vezérlőrendszereket, a fegyverrendszereket, a létfenntartó rendszereket, a nukleáris létesítményeket vagy bármely más alkalmazást, amely esetében a biztonsági kockázat azonosításának sikertelensége halálesethez, személyi sérüléshez vagy vagyoni kárhoz vezethet. Nem garantált, hogy a biztonsági vizsgálatok megszakítás nélkül vagy hibamentesen működnek.

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. Egyes jogszabályok tiltják a számítógépes rendszerekbe való bármilyen engedély nélküli behatolási vagy hozzáférési kísérletet. Az Ügyfél felhatalmazza az IBM vállalatot arra, hogy végrehajtsa az itt leírt Szolgáltatást, továbbá tudomásul veszi, hogy a Szolgáltatás az Ügyfél számítógépes rendszeréhez való jóváhagyott hozzáféréssel jár együtt. Az IBM közzéteheti ezt a megadott jóváhagyást harmadik fél számára, amennyiben azt szükségesnek ítéli a Szolgáltatás elvégzéséhez.

A tesztelés bizonyos kockázatokkal jár, amelyek korlátozás nélkül az alábbiak lehetnek:

- az Ügyfél a vizsgálat alatt álló alkalmazásokat futtató számítógépes rendszerei lefagyhatnak vagy összeomolhatnak, ami a rendszer ideiglenes elérhetetlenségét vagy adatvesztést eredményezhet;
- az Ügyfél rendszereinek teljesítménye és sebessége, valamint a társított útválasztók és tűzfalak teljesítménye és sebessége ideiglenesen csökkenhet a vizsgálat ideje alatt;
- túlzott mennyiségű naplóüzenet keletkezhet, ami a naplófájlok túlzott tárhelyfoglalását vonhatja maga után;
- adatok módosulhatnak vagy törölődhetnek a sérülékenységi tesztelés eredményeképp;
- a behatolásérzékelő rendszerek riasztásokat aktiválhatnak;
- a vizsgált webes alkalmazás e-mail szolgáltatása e-maileket küldhet;
- az IBM SaaS elfoghatja a megfigyelt hálózat forgalmát események keresése érdekében.

Az Ügyfél lemond minden, a tesztelés tárgyát képező webhelyhez vagy alkalmazáshoz kapcsolódó, az IBM által biztosított szolgáltatás-szint-megállapodási jogról vagy jogorvoslati lehetőségről bármely tesztelési tevékenység időtartama alatt.

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 felhasználóknak 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 ha az Ügyfél a vizsgálat típusát „termelésre” állítja, a fent felsorolt kockázatok csökkennek; azonban bizonyos esetekben az IBM SaaS a teljesítmény csökkenéséhez vagy instabilitáshoz vezethet a vizsgált termelési helyeken és infrastruktúrában. Az IBM semmilyen jótállást nem vállal és semmilyen nyilatkozatot nem tesz azzal kapcsolatban, hogy az IBM SaaS 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 ENGEDÉLLEL.**

A pontosság kedvéért: Az IBM Felhasználási Feltételek – Általános Feltételek adatvédelmi szakaszában leírt Ügyféltartalom is tartalmaz olyan adatokat, amelyek elérhetővé válnak az IBM számára az Alkalmazáspenetrációs tesztelés során.

## **6.1 Harmadik fél tulajdonába tartozó rendszerek**

Azon rendszerek esetében (amelyek a jelen rendelkezés tekintetében magukba foglalják, de nem kizárólagosan, az alkalmazásokat és IP-címeket), amelyek a tesztelés tárgyát fogják képezni és egy harmadik fél tulajdonában vannak, az Ügyfél beleegyezik, hogy:

- a. az IBM által harmadik felek rendszerén végzett tesztelés megkezdése előtt az Ügyfél aláírt engedélyt szerez be minden egyes rendszer tulajdonosától, amelyben feljogosítják az IBM vállalatot a Szolgáltatás elvégzésére az adott rendszeren, jelezve azt is, hogy a tulajdonos elfogadja a „Teszt végrehajtásának engedélyezése” című szakaszban meghatározott feltételeket, és az Ügyfél másolatot biztosít az IBM számára az ilyen engedélyről;
- b. kizárólagosan felelős azért, hogy bármely, az IBM távoli tesztelése által ezeken a rendszereken feltárt kockázatról, kitettségről és biztonsági résről tájékoztassa a rendszer tulajdonosát; és
- c. megszervezi és lebonyolítja az IBM által szükségesnek ítélt információcserét a rendszer tulajdonosa és az IBM között.

Az Ügyfél elfogadja a következőket:

- azonnal értesíti az IBM vállalatot, ha változik valamely, az itt hivatkozott tesztek által érintett rendszer tulajdonosa;
- az IBM előzetes, írásos engedélye nélkül nem adja át az Ügyfél vállalkozásán kívüli személyeknek az átadandó anyagokat vagy azt az információt, hogy az IBM nyújtotta a Szolgáltatást; és
- teljes mértékben kártalanítja az IBM vállalatot az IBM vállalatnál felmerülő bármely, harmadik felek követeléséből származó veszteség vagy felelősség tekintetében, amely az Ügyfél azon hibájából adódik, hogy nem teljesítette a jelen („Harmadik fél tulajdonába tartozó rendszerek” című) szakasz

kötelezettségeit, továbbá bármely, az IBM vagy annak alvállalkozóit és ügynökeit érintő, harmadik féltől származó idézés vagy követelés miatt, amely (a) a biztonsági rések teszteléséből, az itt foglalt tesztek tárgyát képező rendszerek kitérségéből vagy biztonsági réseiből, (b) az ilyen tesztek eredményeinek az Ügyfél felé történő átadásából vagy (c) az eredmények Ügyfél általi használatából vagy azok továbbadásából következik.

## 6.2 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.

A jelentéskészítési tevékenységet magukban foglaló IBM SaaS szolgáltatások keretében az IBM az IBM SaaS szolgáltatásból gyűjtött, személyek azonosítására alkalmatlan és/vagy összesített információkat készít és őriz meg („Biztonsági adatok” néven). A Biztonsági adatok nem azonosítják az Ügyfelet és az egyes személyeket az alábbi (d) pontban leírt eseteket kivéve. Az Ügyfél továbbá ezúton elfogadja, hogy az IBM használhatja és/vagy másolhatja a Biztonsági adatokat, kizárólag az alábbi célokra:

- a. a Biztonsági adatok közzététele és/vagy terjesztése (például a számítógépes biztonsággal kapcsolatos összeállításokban és/vagy elemzésekben);
- b. termékek és szolgáltatások fejlesztése és bővítése;
- c. szervezeten belül vagy harmadik felek útján megvalósuló kutatások; és
- d. harmadik felek adatainak jogszerű kiadása bizonyított elkövetők esetében.

## 6.3 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.

## 6.4 Személyes adatok és Szabályozás hatálya alá tartozó adatok és szolgáltatások

A jelen IBM SaaS tervezéséből fakadóan nem felel meg a szabályozott tartalmakra, például a személyes adatokra vagy bizalmas személyi adatokra vonatkozó biztonsági követelményeknek. Az Ügyfél a felelős annak meghatározásáért, hogy a jelen IBM SaaS megfelel-e az Ügyfél igényeinek az Ügyfél által az IBM SaaS termékkel használt tartalom típusára vonatkozóan.

Az IBM nem a Federal Communications Commission („FCC”) vagy az állami szabályozó hatóságok („Állami szabályozók”) által szabályozott szolgáltatóként működik, és nem áll szándékában az FCC vagy az Állami szabályozók hatáskörébe tartozó szolgáltatások biztosítása. Ha az FCC vagy az Állami szabályozók szabályozási követelményeket vagy kötelezettségeket vezetnek be az IBM itt foglalt szolgáltatásaival kapcsolatban, az IBM a következőket teheti: (a) módosíthat, lecserélhet vagy helyettesíthet termékeket az Ügyfél költségére és/vagy (b) módosíthatja a szolgáltatások biztosításának módját az Ügyfél részére az efféle követelmények vagy kötelezettségek az IBM részéről történő alkalmazásának elkerülése érdekében (például az Ügyfél képviselőjeként lép fel az ilyen szolgáltatások egy szállítójaként funkcionáló harmadik féltől való beszerzéséhez).

## „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, nyilvánosan elérhető vagy magánhálózaton található webhelyek vizsgálata biztonsági rések keresése céljából. 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

#### 1.1 IBM Application Analyzer

Az IBM Application Analyzer megrendelhető alkalmazáspéldányonként, feladatonként (vizsgálat) vagy teljes példányként, és az alábbi vizsgálatokat teszi lehetővé:

- Dinamikus elemzés – Termelés előtti és termelési webhelyek tesztelése DAST technikák segítségével
- Mobil elemzés – iOS vagy Android bináris kódok tesztelése IAST technikák segítségével
- Statikus elemzés – bájtt- vagy forráskód-adatfolyam tesztelése SAST technikák segítségével

#### 1.2 Telepítési szolgáltatás

Az IBM Application Security on Cloud Consulting Services az Application Analyzer egy termékké alakított telepítési szolgáltatása. A Szolgáltatás IBM szakértőket alkalmaz az alkalmazás kockázatainak tesztelésével és kezelésével kapcsolatos útmutatás és támogatás biztosítása érdekében. Az IBM Application Security on Cloud Consulting Services szolgáltatások Részvételi blokkok formájában vásárolhatók meg, amelyek felhasználhatók az alábbi szolgáltatások igénybevételére. Az adott szolgáltatás kérvényezéséhez az alábbiakban rögzített mennyiség szükséges:

##### a. **Fast Start** [Egy (1) Részvételi egységet igényel]

A Fast Start szolgáltatás szakértelmet és útmutatást biztosít az Application Security on Cloud szolgáltatás tesztelési és kockázatkezelési funkcióinak használatára vonatkozóan. Miután az Ügyfél megerősíti a sikeres bejelentkezést az Application Security on Cloud portálra, az IBM megtart egy legfeljebb két (2) órás webkonferenciát legfeljebb két (2) aktív résztvevő számára, amely során oktatást biztosít az alapvető AppSec IBM SaaS konfigurációkról és funkciókról, beleértve vizsgálati típusokat, a vizsgálatok futtatását, a jelentések áttekintését és a kapcsolódó eszközök és beépülő modulok telepítését. A Fast Start szolgáltatás teljesítése az (a) ügyfél oktatási webináriumának megtartása, (b) a megfelelő eszközök és beépülő modulok telepítése és (c) az Ügyfélnek az első vizsgálata beállításával és futtatásával kapcsolatban nyújtott segítség után tekinthető befejezettnek.

##### b. **Assessment Review** [Két (2) Részvételi egységet igényel]

Az Assessment Review szolgáltatás támogatást biztosít a teszteredmények áttekintéséhez, beleértve az alkalmazásban talált biztonsági rések helyreállításának megértését és a prioritások meghatározását. Az IBM biztosít egy legfeljebb egy (1) órás webkonferenciát legfeljebb két (2) aktív résztvevő számára, amely során áttekintést ad az alkalmazásban talált biztonsági résekről és az alkalmazás átfogó biztonsági kockázatairól, továbbá az alkalmazás megtalált biztonsági réseiről szóló részletes megbeszélés keretében ismerteti, (1) hogyan történt a biztonsági rések tesztelése,

(2) illetve a biztonsági rések észlelése, (3) milyen kockázatokat jelentenek az egyes biztonsági rések, valamint (4) általános megoldási javaslatokat ad az egyes biztonsági rések kijavításának segítésére. Az áttekintés kizárólag a teszt eredményén alapul, nem a forráskód áttekintésére irányul. Az Ügyfél a webkonferencia előtt áttekinti a teszteredményeket és megnevezi az IBM felé az áttekinteni kívánt teszteredményeket. Az Assessment Review szolgáltatás a webkonferenciával fejeződik be.

c. **Scan for Me** [Négy (4) Részvételi egységet igényel]

A Scan for Me szolgáltatás biztosít egy IBM alkalmazásbiztonsági szakértőt, aki beállítja és lefuttatja a vizsgálatot, kiértékeli az eredményeket, és levezet egy jelentésbemutatót az eredmények áttekintésére. Az Ügyfél lehetővé teszi egy IBM tanácsadó számára, hogy hozzáférjen az AsoC környezetéhez, aki így beállíthat és futtathat egy vizsgálatot, ellenőrizheti az eredményeket, ajánlásokat adhat a helyreállítás prioritásaival kapcsolatban, és jelentésbemutatót tarthat az eredményekről. Az IBM biztosít egy legfeljebb egy (1) órás webkonferenciát legfeljebb két (2) aktív résztvevő számára, amely során áttekintést ad az alkalmazásban talált biztonsági résekről és az alkalmazás átfogó biztonsági kockázatairól, továbbá az alkalmazás megtalált biztonsági réseiről szóló részletes megbeszélés keretében ismerteti, (1) hogyan történt a biztonsági rések tesztelése, (2) illetve a biztonsági rések észlelése, (3) milyen kockázatokat jelentenek az egyes biztonsági rések, valamint (4) általános megoldási javaslatokat ad az egyes biztonsági rések kijavításának segítésére. Kérés szerint és legfeljebb 30 nappal a kezdeti vizsgálat után az IBM az eredeti vizsgálati beállítások használatával végrehajt egy új vizsgálatot kizárólag a biztonsági javítások ellenőrzésének (nem pedig új funkciók tesztelésének) céljából, ellenőrzi az eredményeket, és jelentést készít az ügyfél számára. A Scan for Me szolgáltatás a webkonferenciával fejeződik be, amelyen áttekintik a kezdeti vizsgálat eredményeit, vagy az Ügyfél által esetlegesen kért, újból elvégzett vizsgálat teljesítésével és a megismételt vizsgálatról szóló jelentés az Ügyfél számára történő átadásával.

d. **Advisor on Demand** [Hét (7) Részvételi egységet igényel]

Az Advisor on Demand szolgáltatás akár húsz (20) órányi segítségnyújtást biztosít egy IBM tanácsadó részéről, amely az IBM SaaS termékhez kapcsolódó tevékenységekre fordítható. Az IBM tanácsadó támogatást nyújt az alkalmazásbiztonsági témákban, beleértve, de nem kizárólagosan a programfelügyeletet, a biztonsági tesztek sorrendjének meghatározását, a helyreállítási stratégiákat, a forráskódelemzést és a forráskódjavítást. Az IBM együttműködik az Ügyféllel egy, az Ügyfél speciális követelményeinek megfelelő projektütemterv értelmezésében és létrehozásában, beleértve a projekt céljait, a lényeges technológiákat, a kívánt határidőket, az elvárt átadandó anyagokat, valamint az Advisor on Demand szolgáltatás várható igénybevételének mértékét. Az Ügyfélnek hozzáférést kell biztosítania a szolgáltatás elvégzéséhez szükséges alkalmazásokhoz, rendszerekhez és dokumentációhoz. Az Advisor on Demand szolgáltatás akkor fejeződik be, ha az IBM legfeljebb 20 órányi biztonsági szaktanácsadást nyújtott az ügyfélnek, és/vagy a projektütemtervet és/vagy a projektütemtervben meghatározott, dokumentált átadandó anyagokat átadta az Ügyfélnek.

e. **Alkalmazáspenetrációs tesztelés**

Három lehetőség választható:

- (1) **Megfelelőségi/belépési szintű Alkalmazáspenetrációs teszt** – akár negyven (40) órányi szakértői tanácsadást tartalmaz, és az egylépéses logikai hibákra, valamint a beszűrési hibák egyszerű változataira összpontosít. Tizenöt (15) Részvételi egységet igényel.
- (2) **Normál Alkalmazáspenetrációs teszt** – akár hatvan (60) órányi szakértői tanácsadást tartalmaz, továbbá a többlépéses munkafolyamatokban előforduló logikai hibákkal, a beszűrési hibák összetett változataival és az összetett adattípusok elemzésével bővül a hatóköre. Huszonegy (21) Részvételi egységet igényel.
- (3) **Speciális Alkalmazáspenetrációs teszt** – akár nyolcvan (80) órányi szakértői tanácsadást tartalmaz, továbbá az összeállított futtatható fájlok visszafejtését, egyéni hálózati protokollok szétbontását és nyilvánosan elérhető könyvtárak és keretrendszerek átfogó elemzését is magában foglalja a hatóköre. Huszonhét (27) Részvételi egységet igényel.

Az alkalmazáspenetrációs tesztelési szolgáltatás IBM erőforrásokat biztosít egy alkalmazás tesztelésére és kihasználására, valamint magában foglalja egy tesztjelentés átadását és egy jelentésbemutatót, amely során ismerteti az eredményeket és az azokhoz kapcsolódó kockázatokat.

Az IBM biztosít egy legfeljebb egy (1) órás, két (2) aktív résztvevőt érintő projektindítási hívást az Ügyfél környezetének és szervezetének áttekintéséhez, beleértve az alkalmazásplatform, az architektúra, a keretrendszerek, a támogató infrastruktúra, az alkalmazást érintő ismert biztonsági problémák vagy aggályok, az előzetes tesztelési ütemterv és a sürgősségi kapcsolatfelvételi terv áttekintését.

Az IBM végrehajtja az alkalmazáspenetrációs tesztelést, beleértve, de nem kizárólagosan a következőket: gyakori biztonsági kockázatok azonosítása, mint például az SQL-beszúrás és a helyközi parancsfájlokat használó támadások, a meglévő biztonsági megoldások erősségeinek és gyenge pontjainak kiértékelése, mint például a bemeneti értékek ellenőrzése, hitelesítés és felhatalmazás, az üzleti logika megfelelő kikényszerítése, a biztonsági protokollok megfelelő használatának ellenőrzése, a munkamenet-kezelési hibák azonosítása, illetve a bejelentkezésnél, jelszó visszaállításánál, jelszavakra vonatkozó irányelveknél és egyéb felhasználófelügyeleti funkcióknál használt megfelelő biztonsági vezérlők ellenőrzése. Az eredményeket az Alkalmazáspenetrációs tesztjelentés fogja rögzíteni. Az IBM biztosít egy legfeljebb egy (1) órás webkonferenciát a jelentés bemutatásának céljából. Az Alkalmazáspenetrációs tesztelési szolgáltatás akkor fejeződik be, amikor felhasználták az összes elérhető tanácsadási időt, a webkonferencia lezajlott és a végső Alkalmazáspenetrációs tesztjelentést átadták az Ügyfélnek.

### 1.2.1 A Telepítési szolgáltatások kötelezettségei

Az IBM a következő tevékenységeket teljesíti:

- Telepítési szolgáltatásokat biztosít Részvételi egységekben, amelyeket az Ügyfél vásárol meg Felhasználási Engedélyenként; és
- teljesíti a Telepítési szolgáltatást, amikor az 1.2-es szakaszban leírt teljesítési feltételek teljesülnek.

Az Ügyfél elfogadja a következőket:

- felelősséget vállal a szerződési időszak alatt, az Ügyfél által létrehozott Részvételi kérelmekkel kapcsolatos költségekért;
- és elfogadja, hogy a megvásárolt Részvételi egységeket a kezdeti szerződési időtartam alatt kell felhasználni, a szerződés befejezési idejével a fel nem használt egységek lejárnak; és
- hivatalos kérelmet ad be minden Telepítési szolgáltatás esetén az előfizetés lejárta előtt legalább 30 nappal.

Bármely Telepítési Szolgáltatás elvégzése során az IBM információt és ésszerű együttműködést kérhet az Ügyféltől. A kért információk vagy együttműködés megfelelő időben történő biztosításának elmaradása esetében az Ügyfél, az IBM által meghatározott módon, Részvételi egységek megfizetésére kötelezhető, a szolgáltatások igénye vagy a megfelelő szolgáltatás teljesítményének késése alapján.

Annak érdekében, hogy az IBM a tesztelést megfelelően végezhesse el, az Ügyfél beleegyezik, hogy követi az IBM azon utasításait, amelyek a tesztelési időszak alatt szükséges környezet előkészítésére és fenntartására vonatkoznak.