

IBM Application Security on Cloud

Kullanım Koşulları, bu IBM Kullanım Koşulları – Hizmet Olarak Sunulan Yazılıma Özgü Olanak Koşullarından (“Hizmet Olarak Sunulan Yazılıma Özgü Olanak Koşulları”) ve aşağıdaki URL adresinde bulunan IBM Kullanım Koşulları - Genel Koşullardan (“Genel Koşullar”) oluşur: <http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/>.

Çelişki durumunda, Hizmet Olarak Sunulan Yazılıma Özgü Olanak Koşulları, Genel Koşullara göre öncelikli olarak uygulanır. Müşteri, IBM Hizmet Olarak Sunulan Yazılımına erişerek ya da IBM Hizmet Olarak Sunulan Yazılımını kullanarak veya sipariş ederek bu Kullanım Koşullarını kabul etmiş olur.

Kullanım Koşulları, uygulanabilir olduğu şekilde, IBM Uluslararası Passport Advantage Sözleşmesine, IBM Uluslararası Passport Advantage Express Sözleşmesine veya Seçilmiş IBM Hizmet Olarak Sunulan Yazılımı İçin IBM Uluslararası Sözleşmesine (“Sözleşme”) tabidir ve Kullanım Koşulları, bunlar ile birlikte taraflar arasındaki sözleşmenin tamamını oluşturur.

1. IBM Hizmet Olarak Sunulan Yazılımları

Aşağıdaki IBM Hizmet Olarak Sunulan Yazılımları, Hizmet Olarak Sunulan Yazılıma Özgü Olanak Koşulları kapsamında yer alır:

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

2. Ücret Ölçüleri

IBM Hizmet Olarak Sunulan Yazılımı, İşlem Belgesinde belirtilen şekilde aşağıdaki ücret ölçülerinden biri kapsamında satılır:

- İş** – IBM Hizmet Olarak Sunulan Yazılımının edinilebileceği bir ölçü birimidir. IBM Hizmet Olarak Sunulan Yazılımı içinde yer alan ve daha fazla bölünemeyen bir nesne olan iş, tüm alt süreçleri de dahil olmak üzere, bir bilgi işlem sürecini temsil eder. Müşteri, Yetki Belgesinde veya İşlem Belgesinde belirtilen ölçüm süresi boyunca IBM Hizmet Olarak Sunulan Yazılımı tarafından işleme konan ya da yönetilen toplam İş sayısını kapsamaya yetecek sayıda yetki edinmelidir.
- Uygulama Eşgörünümlü** – IBM Hizmet Olarak Sunulan Yazılımının edinilebileceği bir ölçü birimidir. IBM Hizmet Olarak Sunulan Yazılımına bağlı olan bir Uygulamanın her bir eşgörünümlü için bir Uygulama Eşgörünümlü yetkisi edinilmelidir. Bir Uygulamanın çok sayıda bileşeni varsa, ayrı bir amaca ve/veya kullanıcı tabanına hizmet veren ve IBM Hizmet Olarak Sunulan Yazılımına bağlanabilen ya da bu olanak tarafından yönetilen her bileşen ayrı bir Uygulama olarak kabul edilir. Ayrıca, bir Uygulama için test, geliştirme, hazırlık ve üretim ortamlarının her biri Uygulamanın ayrı eşgörünümlüleri olarak kabul edilir ve her biri için bir yetki edinilmelidir. Tek bir ortamdaki çok sayıda Uygulama Eşgörünümlünün her biri, Uygulamanın ayrı eşgörünümlüleri olarak kabul edilir ve her biri için ayrı bir yetki edinilmelidir. Müşterinin, Yetki Belgesinde ya da İşlem Belgesinde belirtilen ölçüm süresi boyunca IBM Hizmet Olarak Sunulan Yazılımına bağlanan Uygulama Eşgörünümlü sayısını kapsamaya yetecek sayıda Yetki edinmesi gerekir.

IBM Hizmet Olarak Sunulan Yazılımının amaçları doğrultusunda:

- Dinamik Testler için: genel veya özel URL aracılığıyla adreslenebilen bir web sitesi. Her Uygulama Eşgörünümlü, tek bir etki alanında en fazla 1.000 sayfalık bir site için yetki verir.
 - Statik Testler için: tek bir programlama dilinde yürütülebilir kod birimidir. Her Uygulama Eşgörünümlü, 1.000.000 satıra kadar kod birimlerini tarama yetkisi verir.
 - Mobil Testler için: mobil aygıt üzerinde yürütülebilir ikili kod birimidir. Her farklı mobil platform (örn: iOS ve Android) farklı Uygulama Eşgörünümlüleri oluşturur.
- Eşgörünümlü**, IBM Hizmet Olarak Sunulan Yazılımının edinilebileceği bir ölçü birimidir. Bir Eşgörünümlü IBM Hizmet Olarak Sunulan Yazılımının belirli bir yapılandırmasına erişimdir. Müşterinin Yetki Belgesinde veya İşlem Belgesinde belirtilen ölçüm süresi boyunca erişilmesine ve kullanılmasına imkan tanıyan her IBM Hizmet Olarak Sunulan Yazılımı Eşgörünümlü için yeterli sayıda yetki edinilmelidir.

Her Eşgörünüm yetkisi için, gerçekleştirilen İş veya Uygulama Eşgörünümü (bağlı Uygulamalar) sayısında bir sınır yoktur, ancak aynı anda en fazla 30 İş çalıştırılabilir.

- d. **Taahhüt** - hizmetlerin edinilebileceği bir ölçü birimidir. Taahhüt, IBM Hizmet Olarak Sunulan Yazılımıyla ilişkili profesyonel hizmetlerden ve/veya eğitim hizmetlerinden oluşur. Her Taahhüdü kapsamaya yetecek sayıda yetki edinilmelidir.

3. Ücretler ve Faturalama

IBM Hizmet Olarak Sunulan Yazılımı için ödenecek tutar bir İşlem Belgesinde belirtilmiştir.

3.1 Kısmi Aylık Ücretler

Bir kısmi aylık ücret, İşlem Belgesinde belirtilmiş olduğu şekilde, oranlanmış olarak değerlendirilebilir.

3.2 Limit Aşımı Ücretleri

Ölçüm süresi boyunca IBM Hizmet Olarak Sunulan Yazılımının gerçek kullanımı Yetki Belgesinde belirtilen yetkiyi aşarsa, limit aşımı miktarı İşlem Belgesinde belirtilen şekilde Müşteriye fatura edilecektir.

3.3 Kurulum Ücretleri

Müşteriye, İşlem Belgesinde belirtildiği şekilde fatura düzenlenecektir.

4. Süre ve Yenileme Seçenekleri

IBM Hizmet Olarak Sunulan Yazılımının süresi, Yetki Belgesinde belgelenmiş olduğu şekilde, IBM Hizmet Olarak Sunulan Yazılımına erişiminin sağlandığı IBM tarafından Müşteriye bildirildiği tarihte başlar. Yetki Belgesinde IBM Hizmet Olarak Sunulan Yazılımının, otomatik olarak mı yenileneceği, sürekli kullanım esasına göre mi işleneceği yoksa belirlenen sürenin sonunda sona mı ereceği belirtilir.

Otomatik yenileme için: müşteri, sürenin sona erme tarihinden en az otuz (30) gün önce yazılı olarak olanağı kullanımını yenilemeyeceğini bildirmediği sürece, IBM Hizmet Olarak Sunulan Yazılımı, Yetki Belgesinde belirtilen süreye uygun olarak kendiliğinden yenilenir.

Sürekli kullanım için: müşteri, sürenin sona erme tarihinden otuz (30) gün önce yazılı olarak olanağı kullanımını sona erdireceğine ilişkin bildirim gönderinceye kadar, IBM Hizmet Olarak Sunulan Yazılımı, aylık kullanım esasına göre kullanılmaya devam eder. IBM Hizmet Olarak Sunulan Yazılımı, otuz (30) günlük bu bildirim süresinin sona ermesini izleyen takvim ayının sonuna kadar kullanılmaya devam edilebilir.

5. Teknik Destek

Abonelik Süresi boyunca ve IBM Hizmet Olarak Sunulan Yazılımına erişiminin etkinleştirildiği IBM tarafından Müşteriye bildirildikten sonra, teknik destek çevrimiçi forumlar aracılığıyla sağlanırken standart destek de Müşteri için Kullandığın Kadar Öde (Pay per Use) ücretlerinin geçerli olduğu süre boyunca sağlanır. Müşteri, IBM Hizmet Olarak Sunulan Yazılımının içinden bir destek bildirim kaydı gönderebilir ya da yardım almak için bir sohbet oturumu açabilir. IBM, teknik destek iletişim bilgilerini ve diğer bilgi ve süreçleri içeren IBM Hizmet Olarak Sunulan Yazılım Desteği El Kitabı'nı sağlayacaktır.

Önem Derecesi	Önem Derecesi Tanımı	Yanıt Süresi Hedefleri	Yanıt Süresi Kapsamı
1	Kritik iş etkisi/hizmet kesintisi: İş açısından kritik önem taşıyan işlevsellik kullanılabilir durumda değildir veya kritik bir arabirimde hata oluşmuştur. Bu durum genellikle bir üretim ortamı için geçerlidir ve hizmetlere erişilemediğini, bunun da operasyonlar üzerinde kritik bir etki yarattığını ifade eder. Bu durum, derhal çözüm sağlanmasını gerektirir.	1 saat içinde	7x24
2	Önemli iş etkisi: Hizmetin bir iş özelliğinin ya da işlevinin kullanımı önemli ölçüde kısıtlanmıştır ya da Müşteri iş teslim tarihlerine uyamama riski ile karşı karşıya bulunmaktadır.	2 iş saati içinde	P-C mesai saatleri

Önem Derecesi	Önem Derecesi Tanımı	Yanıt Süresi Hedefleri	Yanıt Süresi Kapsamı
3	Önemsiz iş etkisi: Hizmetin ya da işlevselliğin kullanılabilir olduğunu ve operasyonlar üzerinde kritik bir etkisinin bulunmadığını ifade eder.	4 iş saati içinde	P-C mesai saatleri
4	Asgari iş etkisi: Bir sorgu ya da teknik olmayan bir taleptir.	1 iş günü içinde	P-C mesai saatleri

5.1 Müşteri Verilerine Erişim

IBM, hizmete ilişkin sorunların tanınması ve Müşterinin uygulamasında hizmet tarafından tarama yapılmasını kolaylaştırmak amacıyla Müşteri verilerine erişebilecektir. IBM, verilere yalnızca kusurların giderilmesi ya da IBM ürünleri veya hizmetleri için destek sağlanması amaçlarıyla erişecektir.

6. IBM Hizmet Olarak Sunulan Yazılımı Olanına İlişkin Ek Koşullar

Güvenlik taramaları, bir uygulama içindeki tüm güvenlik risklerini belirleyemeyebilir. Ayrıca, bu taramalar; güvenlik risklerinin belirlenememesi durumunda ölüm, kişisel yaralanma veya maddi zarara yol açabileceği hava taşıtı seyrüseferi, hava trafik kontrol sistemleri, silah sistemleri, yaşam destek sistemleri, nükleer tesisler veya diğer tüm uygulamalar dahil, fakat tümü bunlarla sınırlı olmamak kaydıyla hatalara karşı güvenli çalışma gerektiren tehlikeli ortamlarda kullanılmak üzere tasarlanmamış veya bu şekilde kullanılması amaçlanmamıştır. Güvenlik taramalarının, kesintisiz veya hatasız olarak çalışacağı garanti edilmemektedir.

IBM Hizmet Olarak Sunulan Yazılımı olanağı Müşterinin, yasalar, düzenlemeler, standartlar ya da günlük uygulamaları esas alan uyumluluk yükümlülüklerini yerine getirmesinde Müşteriye yardımcı olmak üzere kullanılabilir. Bu Hizmet tarafından sağlanan herhangi bir yönerge, önerilen kullanım veya rehberlik, yasal, muhasebeyle ilişkili ya da diğer bir profesyonel danışmanlık niteliğinde değildir ve Müşteri, kendisi için hukuki veya diğer uzmanlık konularına ilişkin danışmanlık alması için uyarılır. Müşterinin ve Müşteri etkinliklerinin, uygulamalarının ve sistemlerinin geçerli tüm yasalara, yasal düzenlemelere, standartlara ve uygulamalara uygun olmasını sağlamaktan yalnızca Müşteri sorumludur. Bu Hizmetin kullanımı, herhangi bir yasaya, yasal düzenlemeye, standarda veya uygulamaya uygunluğu garanti etmez.

IBM Hizmet Olarak Sunulan Yazılımı, Müşterinin taramayı seçtiği web sitesi ve web uygulaması veya mobil uygulama üzerinde yayılımcı (invasive) ve yayılımcı olmayan (non-invasive) testler gerçekleştirir. Belirli yasalar, bilgisayar sistemlerine herhangi bir yetkisiz giriş teşebbüsünü ya da erişimi yasaklamaktadır. Müşteri, Hizmetleri burada açıklandığı şekilde yerine getirmesi için IBM'e yetki verir ve Hizmetlerin, Müşterinin bilgisayar sistemlerine yetkili erişimi içerdiğini onaylar. IBM, Hizmetleri gerçekleştirmek için gerekli görmesi halinde, bu yetkilendirmeyi üçüncü taraflara açıklayabilir.

Testler, aşağıdakiler de dahil, ancak tamamı bunlarla sınırlı olmamak üzere belirli riskler taşımaktadır.

- Müşterinin bilgisayar sistemleri, test edilen uygulamaların çalıştırılması sırasında kilitlenebilir ya da çökebilir ve bu da sistemin geçici olarak kullanılamamasına ya da veri kaybına yol açabilir;
- Müşteri sistemlerinin performansı ve veri çıkışı, aynı zamanda ilgili yönlendiricilerin ve güvenlik duvarlarının performansı ve veri çıkışı, test sırasında geçici olarak düşebilir;
- Çok yüksek miktarda günlük iletisi oluşturulabilir ve bu da çok yüksek miktarda günlük dosyası disk alanı tüketimi ile sonuçlanabilir;
- Güvenlik açıklarının algılanması sonucunda veriler değiştirilebilir ya da silinebilir;
- İzinsiz giriş saptama sistemleri tarafından alarmlar tetiklenebilir;
- Test edilen Web uygulamasının e-posta işlevi tarafından e-postalar tetiklenebilir;
- IBM Hizmet Olarak Sunulan Yazılımı, olayları aramak amacıyla, izlenmekte olan ağın trafiğini durdurabilir.

Herhangi bir test etkinliği sırasında testlere tabi olan web siteleri veya uygulamalar ile ilgili olan ve IBM tarafından sağlanan herhangi bir hizmet seviyesi sözleşmesine ilişkin haklardan ve yasal yollardan feragat edilir.

Test edilmekte olan uygulama için kimlik doğrulaması gerçekleştirilmiş oturum açma kimlik bilgilerinin Müşteri tarafından Hizmete girilmesi durumunda, Müşteri bu kimlik bilgilerini üretim kullanıcıları için değil,

yalnızca test hesapları için girmelidir. Üretim kullanıcısı kimlik bilgilerinin kullanılması, kişisel verilerin bu Hizmet aracılığıyla aktarılmasına neden olabilir.

IBM Hizmet Olarak Sunulan Yazılımı Olanağı, üretimde kullanılan web uygulamalarını tarayacak şekilde yapılandırılabilir. Müşteri, tarama tipini "üretim" olarak ayarladığında, hizmet, taramaları yukarıda listelenen riskleri azaltacak şekilde gerçekleştirmek üzere tasarlanır, ancak belirli durumlarda IBM Hizmet Olarak Sunulan Yazılımı test edilen üretim sitelerinde veya altyapılarında performans düşüşüne veya dengesizliklere yol açabilir. IBM, IBM Hizmet Olarak Sunulan Yazılımının üretim sitelerini taramak üzere kullanılması için uygun olduğuna ilişkin hiçbir garanti vermez ve beyanda bulunmaz.

HİZMETİN, MÜŞTERİNİN WEB SİTESİ, WEB UYGULAMASI, MOBİL UYGULAMASI YA DA TEKNİK ORTAMI İÇİN UYGUN YA DA GÜVENLİ OLUP OLMADIĞININ BELİRLENMESİ MÜŞTERİNİN SORUMLULUĞUNDADIR.

IBM Hizmet Olarak Sunulan Yazılımı Olanağı, mobil uygulamadaki ve web uygulamaları ve hizmetlerindeki bir dizi potansiyel güvenlik ve uyumluluk sorunlarını belirlemek üzere tasarlanmıştır. Bu olanak, tüm güvenlik açıklarını ya da uygunluk risklerini test etmez ya da güvenlik saldırıları için bir engel olarak hizmet vermez. Güvenlik tehditleri, yasal düzenlemeleri ve standartları sürekli olarak değişmektedir ve bu Hizmet bu değişikliklerin tamamını yansıtmayabilir. Müşterinin Web uygulamasının, sistemlerinin ve çalışanlarının güvenliği ve uyumluluğu ile herhangi bir çözüm etkinliği yalnızca Müşterinin sorumluluğundadır. Hizmet kapsamında sağlanan bilgileri kullanmak veya kullanmamak yalnızca Müşterinin takdirindedir.

Belirli yasalar, bilgisayar sistemlerine herhangi bir yetkisiz giriş teşebbüsünü ya da erişimi yasaklamaktadır. MÜŞTERİNİN HİZMETİ, KENDİSİNE AİT WEB SİTELERİ VE/VEYA UYGULAMALAR HARİCİNDEKİ YA DA TARAMA HAKKINA VE YETKİSİNE SAHİP OLDUĞU WEB SİTELERİ VE/VEYA UYGULAMALAR HARİCİNDEKİ HERHANGİ BİR WEB SİTESİNİN VE/VEYA UYGULAMANIN TARANMASI İÇİN KULLANMAMASININ SAĞLANMASINDAN MÜŞTERİ SORUMLUDUR.

Herhangi bir şüpheye mahal vermemek adına, IBM Kullanım Koşulları - Genel Koşullar belgesinin veri koruma bölümünde açıklanan Müşteri içeriğinin, Uygulama Sızma Testleri sırasında IBM tarafından erişilebilir hale gelebilecek verileri de içerebilecektir.

6.1 Üçüncü Kişilerin Mülkiyetinde Olan Sistemler

Müşteri, üçüncü kişilerin mülkiyetinde olan ve burada tanımlanan testlere tabi tutulacak sistemler (bu hükmün amacı doğrultusunda uygulamaları ve IP adreslerini kapsar, ancak tamamı bunlarla sınırlı değildir) için aşağıdakileri kabul eder:

- Müşteri, üçüncü kişilere ait bir sistem üzerinde IBM testlere başlamadan önce, her sistemin sahibinden IBM'in Hizmetleri anılan sistem üzerinde sağlanmasına yetki veren ve sistem sahibinin "Testleri Gerçekleştirme İzni" (Permission to Perform Testing) başlıklı bölümde belirtilen koşulları kabul ettiğini belirten imzalı bir mektup alacak ve bu yetkinin bir kopyasını IBM'e sağlayacaktır;
- IBM'in uzaktan yürüttüğü testlerin sonucunda bu sistemlerde saptanan tüm riskleri, açığa çıkarma işlemlerini ve güvenlik açıklarını sistem sahibine bildirmekten tek başına sorumlu olacaktır.
- IBM tarafından gerekli görüldüğü şekilde, sistem sahibi ile IBM arasındaki bilgi alışverişini düzenleyecek ve yürütecektir.

Müşteri aşağıdakileri kabul eder:

- Bu belgede tanımlanan testlere tabi tutulan herhangi bir sistemin sahipliğinde ortaya çıkacak değişiklikleri derhal IBM'e bildirecektir;
- Herhangi bir teslim edilecek malzemeyi veya Hizmetlerin IBM tarafından gerçekleştirildiğini, IBM'in önceden yazılı izni olmaksızın Müşterinin Teşebbüsü dışında açıklamayacaktır; ve
- Müşterinin "Üçüncü Kişilerin Mülkiyetinde Olan Sistemler" başlıklı bu bölümde yer alan şartlara uymaması nedeniyle ileri sürülen üçüncü kişi iddiaları ve (a) burada tanımlanan testlere tabi tutulan sistemlerin güvenlik riskleri, izinsiz erişim olanakları ya da güvenlik açıkları açısından test edilmesi, (b) bu testlerin sonuçlarının Müşteriye sağlanması ya da (c) Müşterinin bu sonuçları kullanması ya da açıklaması nedeniyle üçüncü kişilerce IBM'e ya da IBM'in alt yüklenicileri ya da araçlarına yönelik açılan davalar ya da ileri sürülen iddialar nedeniyle IBM'in karşı karşıya kalacağı zararların ya da yükümlülüklerin tamamı için IBM'i tazmin edecektir.

6.2 Tanımlama Bilgileri

Müşteri, IBM'in, IBM Hizmet Olarak Sunulan Yazılımının normal işletimi ve desteklenmesi kapsamında, takip ve diğer teknolojiler aracılığıyla Müşteriden (çalışanlarından ve yüklenicilerinden) IBM Hizmet Olarak Sunulan Yazılımının kullanımına ilişkin kişisel veriler toplayabileceğini bildiğini ve bu verilerin toplanmasını kabul eder. IBM, bunu kullanıcı deneyiminin iyileştirilmesi ve/veya Müşteriyle olan etkileşimlerin kişiselleştirilmesi amacıyla IBM Hizmet Olarak Sunulan Yazılımının etkinliğine ilişkin kullanım istatistikleri ve bilgileri toplamak için yapmaktadır. Müşteri, IBM'in toplanan kişisel verileri, yukarıda belirtilen amaç uyarınca IBM, diğer IBM şirketleri ve bunların alt yüklenicileri içerisinde, IBM'in ve alt yüklenicilerinin iş yaptıkları herhangi bir yerde, uygulanabilir olan hukuka uygun olarak işlemesi için izin alacağını ya da almış olduğunu doğrular. IBM, Müşteri çalışanlarının ve yüklenicilerinin toplanan kişisel verilere erişmeye, bunların güncellenmesine, düzeltilmesine ya da silinmesine ilişkin taleplerini karşılayacaktır.

IBM, raporlama etkinliklerini içeren IBM Hizmet Olarak Sunulan Yazılımının kapsamında, IBM Hizmet Olarak Sunulan Yazılımından toplanan önceden anonim hale getirilen ve/veya bir araya getirilen bilgileri ("Güvenlik Verileri") hazırlayacak ve sağlayacaktır. Güvenlik Verileri, Müşteriyi veya aşağıda (d) bölümünde sağlananlar dışındaki bir kişiyi tanımlamayacaktır. Müşteri, bu belgede ayrıca IBM'in Güvenlik Verilerini yalnızca aşağıdaki amaçlarla kullanabileceğini ve/veya kopyalayabileceğini kabul eder:

- Güvenlik Verilerinin yayınlanması ve/veya dağıtılması (örneğin; siber güvenlikle ilgili derlemelerde ve/veya analizlerde)
- Ürün veya hizmetlerin geliştirilmesi veya iyileştirilmesi
- Dahili olarak veya üçüncü kişilerle birlikte araştırma yürütülmesi; ve
- Doğrulanmış üçüncü kişi fail bilgilerinin yasalara uygun olarak paylaşılması.

6.3 Türetilen Yararlanma Lokasyonları

Geçerli olduğunda, vergiler hesaplanırken Müşterinin IBM Hizmet Olarak Sunulan Yazılımından yararlandığını belirttiği lokasyon(lar) esas alınacaktır. IBM, Müşteri tarafından IBM'e ek bilgiler sağlanmadıkça, IBM Hizmet Olarak Sunulan Yazılımı sipariş edilirken belirtilen iş adresini birincil Yararlanma lokasyonu varsayarak vergileri uygulayacaktır. Anılan bilgilerin güncel tutulmasından ve herhangi bir değişikliğin IBM'e sağlanmasından Müşteri sorumludur.

6.4 Kişisel Veriler ve Yasal Düzenlemeye Tabi İçerik ve Hizmetler

Bu IBM Hizmet Olarak Sunulan Yazılımı, kişisel veriler veya özel nitelikli kişisel veriler gibi yasal düzenlemeye tabi içeriğe ilişkin hiçbir özel güvenlik gereksinimine uygun olarak tasarlanmamıştır. IBM Hizmet Olarak Sunulan Yazılımının Müşteri tarafından IBM Hizmet Olarak Sunulan Yazılımı ile bağlantılı olarak kullanılan içeriğin türü açısından Müşterinin gereksinimlerini karşılayıp karşılamadığını belirlemekten Müşteri sorumludur.

IBM, Federal İletişim Komisyonu ("FCC") veya eyalet denetim kurumları ("Eyalet Denetleyicileri") tarafından denetlenen hizmetlerin sağlayıcısı olarak faaliyet göstermemektedir ve FCC ya da Eyalet Denetleyicileri tarafından denetlenen herhangi bir hizmet sağlama amacı gütmeyiz. IBM, FCC'nin veya herhangi bir Eyalet Denetleyicisinin, IBM tarafından bu Hizmet Bildirimi kapsamında sağlanan hizmetlerle ilgili yasal gereksinimler veya yükümlülükler yürürlüğe koyması durumunda, bu tür gereksinimlerin veya yükümlülüklerin IBM için geçerli olmaması amacıyla, (a) Müşterinin maliyetinde olmak üzere ürünleri değiştirebilir, ürünlerde değişiklik yapabilir veya ürünler yerine başka ürünler kullanabilir, ve/veya (b) söz konusu hizmetlerin Müşteriye sağlanma şeklini değiştirebilir (örneğin, söz konusu hizmetlerin bir üçüncü kişi genel taşıyıcıdan temin edilmesi için bir Müşteri aracı olarak çalışarak).

IBM Kullanım Koşulları – IBM Hizmet Olarak Sunulan Yazılımına İlişkin Belirtiler

Ek A

1. IBM Application Security on Cloud Genel Tanımı

IBM Application Security on Cloud, Müşteriye çeşitli uygulamalar için güvenlik açıklarının (SQL enjeksiyonu, Siteler Arası Komut Dosyası Oluşturma [Cross-Site Scripting] ve Veri Sızması [Data Leakage] gibi) belirlenmesinde yardımcı olacak tek bir yer sağlar. Bu hizmet çeşitli türlerde uygulama güvenliğini tarama tekniklerini içerir. Bu tekniklerin her biri ilgili uygulamadaki güvenlik sorunları belirler.

IBM Application Security on Cloud aşağıdaki yetenekleri sağlar:

- Güvenlik açıkları için Mobil Uygulamaların taranması. Bu tarama işlemi, Dinamik (kara kutu [blackbox]) ve Etkileşimli (cam kutu [glassbox]) güvenlik analizi teknolojileri kullanılarak gerçekleştirilir.
- Güvenlik açıkları için, genel kullanıma yönelik olan veya özel ağda bulunan üretim veya üretim öncesi Web sitelerinin taranması. Bu tarama işlemi, Dinamik (kara kutu (blackbox)) güvenlik analizi teknikleri kullanılarak gerçekleştirilir.
- Güvenlik açıkları için Web ve Masaüstü uygulamalarındaki veri akışlarının taranması. Bu tarama işlemi, Statik (beyaz kutu [whitebox]) güvenlik analizi teknikleri kullanılarak gerçekleştirilir.
- Hem bulguların genel özetlerini hem de geliştiriciler tarafından izlenebilecek olan açıkları giderme adımlarını içeren ayrıntılı güvenlik açığı raporları.
- Çeşitli DevOps platformlarıyla bütünleştirme.

1.1 IBM Application Analyzer

IBM Application Analyzer, Uygulama Örneği başına her İş (tarama) için veya Tam Eşgörünüm olarak sipariş edilebilir ve aşağıdaki tarama türlerini sağlar:

- Dynamic Analyzer – Dinamik Uygulama Güvenliği Testi (DAST) teknikleri aracılığıyla teste ilişkin üretim öncesi veya üretim web siteleri
- Mobile Analyzer – Etkileşimli Uygulama Güvenliği Testleri (IAST) aracılığıyla teste ilişkin iOS veya Android ikili kodları
- Static Analyzer – Statik Uygulama Güvenliği Testi (SAST) aracılığıyla test baytı veya kaynak koduna ilişkin veri akışı

1.2 Kurulum Hizmeti

IBM Application Security on Cloud Consulting Services, Application Analyzer için ürün haline getirilmiş bir kurulum hizmetidir. Hizmette, test ve yönetim uygulama riskinde rehberlik ve yardım sağlamak için IBM danışmanlık kullanılır. IBM Application Security on Cloud Consulting Services, aşağıdaki belirli hizmetleri talep etmek ve kullanmak amacıyla, aşağıda belirtilen miktarlarda genişletilebilecek Taahhüt Blokları olarak satın alınır.

a. Hızlı Başlangıç [Bir (1) Taahhüt birimini kullanır]

Hızlı Başlangıç hizmeti, Application Security on Cloud ürününün test ve risk yönetimi özelliklerini kullanmak için uzmanlık ve rehberlik sağlar. Müşteri, Application Security on Cloud portalına başarılı şekilde oturum açtıktan sonra, IBM, tarama türleri, taramaların çalıştırılması, raporların incelenmesi ve ilgili araç ve eklentilerin kurulması dahil, IBM Hizmet Olarak Sunulan Yazılımına ilişkin yapılandırmalar ve işlevler hakkında temel AppSec eğitimi sağlamak amacıyla, iki (2) etkin katılımcı için iki (2) saat boyunca web konferansı gerçekleştirecektir. Hızlı Başlangıç hizmeti, aşağıda belirtilenler tamamlandıktan sonra tamamlanmış sayılacaktır: (a) müşteri eğitim web semineri, (b) geçerli araç ve eklentilerin kurulması ve (c) Müşterinin ilk taramasını kurup çalıştırmasına yardımcı olunması.

b. Değerlendirme İncelemesi [İki (2) Taahhüt birimini kullanır]

Değerlendirme İncelemesi hizmeti, uygulamadaki güvenlik açıklarının giderilmesini öncelik sırasına koyma ve anlamaya yönelik yardım dahil olmak üzere, test sonucunun incelenmesine yönelik yardım sağlar. IBM, saptanan güvenlik açıklarına ilişkin genel bakışı, uygulamaya ilişkin genel

güvenlik riskini ve aşağıdakileri içeren uygulama güvenlik açıklarına ilişkin ayrıntılı bir tartışma sağlamak amacıyla, iki (2) etkin katılımcı için iki (2) saat boyunca web konferansı gerçekleştirecektir: (1) güvenlik açığının nasıl test edildiği, (2) güvenlik açıklarının nasıl saptandığı, (3) her güvenlik açığı riskinin ne olduğu ve (4) güvenlik açığını gidermek için genel düzeltme önerilerinin sağlanması. İnceleme, yalnızca test sonucuna dayalı olacak ve kaynak koduna ilişkin bir inceleme niteliğinde olmayacaktır. Müşteri, test sonucunu inceleyecek ve web konferansından önce test sonucunu incelemesi için IBM'e tanımlayacaktır. Değerlendirme İncelemesi hizmeti, web konferansı tamamlandıktan sonra tamamlanmış olacaktır.

c. **Benim İçin Tara (Scan for Me)** [Dört (4) Taahhüt birimini kullanır]

Benim İçin Tara (Scan for Me) hizmeti, bir IBM uygulama güvenliği uzmanı sağlayacaktır. Bu uzman, bir taramayı yapılandırıp yürütecek, sonuçları doğrulayacak ve bulguları incelemek için rapora ilişkin bilgilendirme yürütecektir. Müşteri; tarama yürütmek, sonuçları doğrulamak, çözümün öncelik sırasına konulmasıyla ilgili öneriler sağlamak ve sonuçlara ilişkin rapor bilgilendirmesi yürütmek için IBM danışmanına ASoC ortamına erişme olanağı tanıyacaktır. IBM, saptanan güvenlik açıklarına ilişkin genel bakışı, uygulamaya ilişkin genel güvenlik riskini ve aşağıdakileri içeren uygulama güvenlik açıklarına ilişkin ayrıntılı bir tartışma sağlamak amacıyla, iki (2) etkin katılımcı için bir (1) saat boyunca web konferansı gerçekleştirecektir: (1) güvenlik açığının nasıl test edildiği, (2) güvenlik açıklarının nasıl saptandığı, (3) her güvenlik açığı riskinin ne olduğu ve (4) güvenlik açığını gidermek için genel düzeltme önerilerinin sağlanması. IBM, talep üzerine ve ilk taramanın ardından en fazla 30 gün boyunca, yeni işlevleri test etmek yerine yalnızca güvenlik düzeltmelerini ve sonuçları doğrulamak ve müşteriye rapor sunmak amacıyla, başlangıçtaki tarama yapılandırmasını kullanarak yeniden tarama yapacaktır. Benim İçin Tara (Scan for Me) hizmeti, ilk tarama sonuçlarını incelemeye yönelik web konferansının tamamlanmasından sonra veya geçerliyse, yeniden taramanın Müşteri tarafından tamamlanmasından ve yeniden tarama raporunun Müşteriye teslim edilmesinden sonra tamamlanmış olacaktır.

d. **İsteğe Bağlı Danışman (Advisor on Demand)** [Yedi (7) Taahhüt birimini kullanır.]

İsteğe Bağlı Danışman (Advisor on Demand) hizmeti, 20 saate kadar IBM danışmanı süresi sağlayacaktır. Bu süre, IBM Hizmet Olarak Sunulan Yazılımıyla ilgili etkinlikler için kullanılabilir. IBM danışmanı; program yönetimi, güvenlik testlerinin öncelik sırasına konması, düzeltme stratejileri, kaynak kodu analizi ve kaynak kodu onarımı dahil ancak tümü bunlarla sınırlı olmamak üzere, uygulama güvenliğine ilişkin belirli konularda yardımcı olacaktır. IBM; proje hedefleri, ilgili teknolojiler, istenen zaman çizelgeleri, beklenen teslim edilecek malzemeler ve tahmini sayıda İsteğe Bağlı Danışman (Advisor on Demand) hizmet taahhütleri dahil olmak üzere, belirli Müşteri gereksinimlerini içeren bir proje planını anlamak ve oluşturmak için Müşteri ile birlikte çalışacaktır. Müşteri, hizmetleri gerçekleştirmek için gereken uygulamalara, sistemlere ve belgelere erişim sağlamalıdır. İsteğe Bağlı Danışman (Advisor on Demand) hizmeti, 20 saatlik güvenlik uzmanlığı verildiğinde ve/veya proje planı ve/veya proje planında tanımlanan teslim edilecek malzemeler Müşteriye teslim edildikten sonra tamamlanmış olacaktır.

e. **Uygulama Sızma Testleri**

Üç seçenek:

- (1) **Uygunluk/Başlangıç Seviyesinde Uygulama Sızma Testi**, en fazla kırk (40) saatlik Danışmanlık içerir ve tek adımlı mantık hatalarına ve enjeksiyon hatalarına odaklanır. On beş (15) Taahhüt birimini kullanır.
- (2) **Standard Uygulama Sızma Testi**, en fazla altmış (60) saatlik Danışmanlık içerir ve odak noktasını; çok adımlı iş akışlarını, enjeksiyon hatalarının Karmaşık sürümlerini ve karmaşık veri türlerinin Analizini içerecek şekilde genişletir. Yirmi bir (21) Taahhüt birimini kullanır.
- (3) **Gelişmiş Uygulama Sızma Testi**, – en fazla seksen (80) saatlik Danışmanlık içerir odak noktasını; derlenebilir ve yürütülebilir ögelere ilişkin tersine mühendislik, özel ağ protokollerinin bölümlere ayrılması, genel kullanıma açık kitaplıklara ve çerçevelere ilişkin derinlemesine analizi içerecek şekilde genişletir. Yirmi yedi (27) Taahhüt birimini kullanır.

Uygulama güvenlik test açığı testleri hizmeti; uygulamaya ilişkin test ve kullanım gerçekleştirmek, test raporu sunmak ve bulguları ve ilgili riskleri açıklamak için bir rapor bilgilendirmesi sunmak amacıyla bir IBM kaynağı sağlar.

IBM, Müşterinin ortamını ve kuruluşunu incelemek için en fazla bir (1) saat boyunca, iki (2) etkin katılımcıya yönelik bir proje başlatma çağrısı gerçekleştirecektir. Bu çağrı; uygulama platformu,

mimari, çerçeveler ve destekleyici altyapının yanı sıra uygulamaya, ön test planına ve acil durum iletişim planına ilişkin bilinen güvenlik sorunlarını veya endişelerini içerecektir.

IBM, aşağıda belirtilenler dahil ancak bunlarla sınırlı olmamak üzere uygulama sızma testleri yürütecektir: SQL enjeksiyonu ve siteler arası komut dosyası oluşturma gibi ortak güvenlik açıklarının saptanması, girdi doğrulaması, kimlik doğrulaması ve yetkilendirme gibi mevcut güvenlik denetimlerinin güçlü ve zayıf yönlerinin değerlendirilmesi, iş mantığının uygun şekilde uygulanmasına yönelik denetim, güvenli protokollerin uygun şekilde kullanıldığının doğrulanması, oturum işleme hatalarının belirlenmesi, oturum açma, şifre kurtarma, şifre ilkesi ve diğer kullanıcı yönetimi işlevlerine yönelik uygun güvenlik denetimlerinin doğrulanması. Bulgular, Uygulama Sızma Test Raporunda belgelenecektir. IBM, en fazla bir (1) saatlik rapor bilgilendirmesine yönelik web konferansı düzenleyecektir. Uygulama Sızma Testi hizmeti; ayrılan danışmanlık süresi kullanıldığında, web konferansı yürütüldüğünde ve son Uygulama Sızma Testi Raporu Müşteriye teslim edildiğinde tamamlanmış olacaktır.

1.2.1 Kurulum Hizmetlerine İlişkin Sorumluluklar

IBM aşağıdakileri gerçekleştirecektir:

- Müşteri tarafından Yetki Belgesine göre satın alınan Taahhüt birimlerini kullanarak, Kurulum Hizmetlerini sağlayacaktır; ve
- Bölüm 1.2'de açıklanan tamamlanma kriterleri tamamlandığında, Kurulum Hizmetini tamamlamış olacaktır.

Müşteri aşağıdakileri kabul eder:

- sözleşme süresince Müşteri tarafından yapılan tüm Taahhüt talepleriyle ilgili tüm ücretlerden sorumlu olmayı;
- ve satın alınan Taahhüt birimlerinin, ilk sözleşmesi süresi içinde kullanılması gerektiğini ve sözleşme süresinin sona erme tarihi itibarıyla kullanılmaması durumunda bu birimlerin süresinin sona ereceğini kabul eder; ve
- aboneliğin sona erme tarihinden en az 30 gün önce tüm Kurulum Hizmetleri için resmi bir talepte bulunmayı.

IBM, herhangi bir Kurulum Hizmetini gerçekleştirmeden önce Müşteriden bilgi ve makul işbirliği talebinde bulunabilir. Talep edilen bilgilerin veya işbirliğinin, Müşteri tarafından zamanında sağlanmaması, IBM'in belirlediği şekilde, hizmetlerin gerektirdiği Taahhüt birimi ücretlerine veya geçerli hizmetin gecikmesine yol açabilir.

Müşteri, IBM'in testleri doğru şekilde gerçekleştirmesi için, teste yönelik ortam hazırlamaya ve korumaya yönelik yönergelere uymayı kabul eder.

Kabul eden:

Müşteri Şirketinin Ticari Unvanı adına ("**Müşteri**")

İmza _____

Yetkili imza

Unvan:

İsim (el yazısı veya daktiloyla):

Tarih:

Müşteri Numarası:

Müşteri Adresi:

Kabul eden:

<İlgili IBM Şirketinin Ticari Unvanı adına> ("**IBM**")

İmza _____

Yetkili imza

Unvan:

İsim (el yazısı veya daktiloyla):

Tarih:

Sözleşme Numarası:

IBM Adresi: