IBM Bulut Hizmeti Tanımı

IBM Security AppScan Mobile Analyzer

Müşterinin siparişine ilişkin Hizmet Tanımı aşağıda belirtildiği gibidir:

1. Bulut Hizmeti

Bulut Hizmeti olanağı aşağıda açıklanmıştır ve seçilen yetki verilmiş olanaklara ilişkin bir Sipariş Belgesinde belirtilmiştir. Sipariş Belgesi, sağlanan Fiyat Teklifinden ve Bulut Hizmetlerinin başlangıç tarihi ile süresini teyit eden Yetki Belgesinden oluşacaktır. Faturalandırma, Bulut Hizmetinin tahsis edilmesinin ardından başlayacaktır.

1.1 IBM Security AppScan Mobile Analyzer

Bu hizmet, güvenlik sorunlarını Android mobil uygulamaların kod düzeyinde belirler. Ayrıca, bir geliştiricinin, uygulama kaynak kodunun sağlanmasına gerek kalmadan güvenlik açıkları için tarama yapmasını da sağlar. Bu taramanın sonunda hizmet bir güvenlik raporu oluşturur. Bu raporda, saptanan güvenlik açıklarının ayrıntıları, mobil uygulamada bu güvenlik açıklarından kaynaklanan olası güvenlik riskleri ve bunların nasıl düzeltileceğine ilişkin öneriler yer alır.

2. Güvenlik Açıklaması

2.1 Güvenlik İlkeleri

IBM, IBM çalışanlarına duyurulan gizlilik ve güvenlik ilkeleri uygulamaktadır ve aynı zamanda bir bilgi güvenliği ekibine sahiptir. IBM, IBM veri merkezlerini destekleyen personelin gizlilik ve güvenlik eğitimi almasını gerektirmektedir. IBM güvenlik ilkeleri ve standartları, yıllık olarak incelenmekte ve yeniden değerlendirilmektedir. IBM güvenlik olayları, kapsamlı bir olay müdahale prosedürü uyarınca ele alınmaktadır.

2.2 Erişim Denetimi

Müşteri verilerine erişime, gerekli ise, görevlerin ayrılığı ilkelerine göre yalnızca yetkili IBM destek temsilcileri ve hizmet operasyonları personeli tarafından izin verilir. IBM personeli, bir ara "ağ geçidi" yönetim anabilgisayarına erişmek için iki etkenli kimlik doğrulaması kullanmaktadır. Müşteri verilerine erişim için kullanılan tüm bağlantılar, şifrelenmiş kanallardır.

2.3 Hizmetin Bütünlüğü ve Kullanılabilirliği

İşletim sistemlerinde ve uygulama yazılımlarında yapılacak değişiklikler, IBM'in değişiklik yönetimi süreci aracılığıyla yönetilir. Güvenlik duvarı kurallarındaki değişiklikler de değişiklik yönetimi sürecine tabidir ve uygulanmadan önce IBM güvenlik personeli tarafından incelenir. IBM, veri merkezini 7 gün 24 saat izler. Potansiyel sistem güvenliği açıklarının tespit edilmesine ve çözülmesine yardımcı olması için yetkili sistem yöneticileri ve üçüncü kişi satıcı firmalar tarafından düzenli olarak dahili ve harici güvenlik açığı taraması gerçekleştirilmektedir. Tüm IBM veri merkezlerinde kötü amaçlı yazılım saptama (virüs önleme, izinsiz giriş saptama, güvenlik açığı taraması ve izinsiz giriş önleme) sistemleri kullanılmaktadır. IBM'in veri merkezi hizmetleri, verilerin halka açık ağlar üzerinden aktarılmasına ilişkin olarak çeşitli bilgi iletimi iletişim kurallarını desteklemektedir. Örnekler arasında HTTPS/SFTP/FTPS/S/MIME ve siteler arası VPN yer almaktadır. Uzak konumda depolanmak üzere oluşturulan yedek veriler, aktarılmadan önce şifrelenir.

2.4 Etkinliklerin Günlüğe Kaydedilmesi

IBM, etkinlikleri günlüğe kaydetme yeteneğine sahip ve kaydetmek üzere yapılandırılmış sistemler, uygulamalar, veri havuzları, ara katman yazılımları ve ağ altyapısı aygıtları için etkinliklerinin günlüklerini tutmaktadır. Yetkisiz müdahale olasılığının en düşük seviyeye indirgenmesi ve merkezi analize, uyarı oluşturmaya ve raporlamaya olanak sağlanması için etkinlikler gerçek zamanlı olarak merkezi günlük havuzlarına kaydedilmektedir. Yetkisiz müdahalenin önlenmesi için verilere imza eklenir. Anormal davranışların saptanması için, günlükler gerçek zamanlı olarak ve düzenli analiz raporları aracılığıyla analiz edilir. Anormallikler operasyon personeline bildirilir ve gerekli olması halinde 7 gün 24 saat nöbet esasına göre çalışan bir güvenlik uzmanı ile iletişim kurulur.

2.5 Fiziksel Güvenlik

IBM, IBM veri merkezlerine yetkisiz fiziksel erişimi kısıtlamak üzere tasarlanmış fiziksel güvenlik standartları uygulamaktadır. Veri merkezlerinde yalnızca sınırlı erişim noktaları vardır ve bunlar, iki etkenli kimlik doğrulama tarafından kontrol edilir ve güvenlik kameraları tarafından izlenir. Yalnızca erişimi onaylanmış yetkili personelin erişimine izin verilmektedir. Operasyon personeli, onayı doğrulamaktadır ve gerekli erişim yetkisini sağlayan bir erişim kartı düzenlemektedir. Anılan kartların sağlandığı çalışanlar, diğer erişim kartlarını iade etmeli ve etkinlikleri süresince yalnızca veri merkezi erişim kartına sahip olmalıdır. Erişim kartlarının kullanımı günlüğe kaydedilmektedir. IBM dışı ziyaretçiler, tesislere girişleri sırasında kaydedilmekte ve tesislerde bulundukları süre boyunca kendilerine eşlik edilmektedir. Teslimat alanları, yükleme platformları ve yetkisiz kişilerin binaya girebileceği diğer noktalar denetlenir ve ayrıştırılmıştır.

2.6 Uyumluluk

IBM, ABD Ticaret Bakanlığı'nın Safe Harbor: Bildirim, Tercih, Üçüncü Kişilere Bilgi Açıklama, Erişim ve Doğruluk, Güvenlik ve Denetim/Uygulama ilkeleri uyarınca gizlilik uygulamalarını her yıl tasdik etmektedir. IBM, üretim veri merkezlerinde yıllık olarak sektör standardına uygun SSAE 16 denetimleri (ya da bunların eşdeğeri) gerçekleştirmektedir. IBM, güvenlik ve gizlilik ile bağlantılı etkinlikleri IBM'in iş gereksinimlerine uygunluk açısından incelemektedir. IBM, bilgi güvenliği ilkelerine uygunluğu doğrulamak için düzenli olarak değerlendirmeler ve denetimler gerçekleştirmektedir. IBM çalışanları ile satıcı firma çalışanları, yıllık olarak iş gücü güvenliği ve farkındalık eğitimi almaktadır. İş hedefleri ile etik iş adabına, gizliliğe ve IBM'in güvenlik yükümlülüklerine uyma sorumlulukları, personele yıllık olarak hatırlatılmaktadır.

3. Yetki ve Faturalandırma Bilgileri

3.1 Ücret Ölçümleri

Bulut Hizmeti, Sipariş Belgesinde belirtilen aşağıdaki ücretlendirme ölçülerinden biri uyarınca sağlanmaktadır:

- Uygulama Eşgörünümü, IBM Hizmet Olarak Sunulan Yazılımlar olanağının edinilebileceği ölçüm sistemidir. IBM Hizmet Olarak Sunulan Yazılım olanağına bağlı olan bir Uygulamanın her bir eşgörünümü için bir Uygulama Eşgörünümü 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 eşgörünümleri olarak kabul edilir ve her biri için bir yetki edinilmelidir. Aynı ortamdaki çok sayıda Uygulama eşgörünümünün her biri, Uygulamanın ayrı eşgörünümleri olarak kabul edilir ve her biri için ayrı bir yetki edinilmelidir. Müşteri, Yetki Belgesinde (PoE) ya da İşlem Belgesinde belirtilen ölçüm süresi boyunca IBM Hizmet Olarak Sunulan Yazılımına bağlanan Uygulama eşgörünümü sayısını karşılamak için yeterli sayıda yetki edinmelidir.

3.2 Ücretler ve Faturalama

Bulut Hizmeti için ödenecek tutar bir Sipariş Belgesinde belirtilmiştir.

3.3 Kullandığın Kadar Öde

Kullandığın Kadar Öde seçenekleri, hizmetin kullanıldığı ayı takip eden ayda, İşlem Belgesinde belirtilen tarifeye uygun olarak fatura edilecektir.

4. Teknik Destek

Bulut Hizmeti için, abonelik süresi boyunca teknik destek sağlanacaktır.

Destek Çalışma Saatleri aşağıdaki gibidir:

Hizmetlerin sağlanacağı saatlere, çevrimiçi sorun bildirimi sistemlerine ve diğer teknik destek iletişim araçlarına ve süreçlerine ilişkin bilgiler, IBM Hizmet Olarak Sunulan Yazılım Desteği El Kitabında açıklanmıştır.

Mesai Saatleri Dışında Destek:

Mesai Saatleri Dışında Destek (yukarıda belirtilen normal çalışma saatleri dışında), yalnızca Önem Derecesi 1 olan sorunlar için iş günlerinde, hafta sonlarında ve resmi tatil günlerinde sağlanacaktır. Önem Derecesi 1 olan sorunlar, Müşterinin 7 gün 24 saat boyunca sorunların teşhis edilmesinde yardımcı olmak üzere hazır bulunmasını gerektirir; aksi takdirde, bu sorunlar önem derecesi 2 şeklinde değiştirilecektir.

4.1 Forum Desteği

Tüm Bulut Hizmeti müşterilerine, IBM destek temsilcileri ve geliştiricileri tarafından düzenli olarak izlenen forum desteği sağlanmaktadır.

a. Soruların Sorulması:

https://developer.ibm.com/answers/questions/ask/?topics=appscan-mobile-analyzer

b. Güncel Gönderilerin Görüntülenmesi:

https://developer.ibm.com/answers/topics/appscan-mobile-analyzer/

4.2 Standart Destek

Standart destek, Müşterinin Kullandığın Kadar Öde esasına göre ücretlendirildiği zaman aralığında kullanılabilir. Müşteriler, Bulut Hizmetinin içerisinden bir sorun bildirimi gönderebilir ya da destek için bir sohbet oturumu başlatabilir. Destek prosedürlerine ilişkin daha fazla bilgi için lütfen aşağıdaki adreste yer alan IBM destek Web portalını ziyaret edin: https://support.ibmcloud.com ya da aşağıdaki adreste yer alan IBM Hizmet Olarak Sunulan Yazılım Destek El Kitabına bakın: http://www.ibm.com/software/support/acceleratedvalue/SaaS_Handbook_V18.pdf.

Önem Derecesi	Önem Derecesi Tanımı	Yanıt Süresi Hedefleri	Yanıt Süresi Kapsamı
1	**Kritik iş etkisi/hizmet devre dışı:** 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 etmektedir. Bu durum, derhal çözüm sağlanmasını gerektirmektedir.	1 saat içinde	7x24
2	**Önemli iş etkisi:** Hizmetin bir iş özelliğinin ya da işlevinin kullanımı önemli ölçüde kısıtlanmıştır ya da iş terminlerine uyamama riski ile karşı karşıya bulunulmaktadır.	2 iş saati içinde	P-C mesai saatleri
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. Safe Harbor Uygunluğu

IBM, bu Bulut Hizmetinin ABD-AB ve ABD-İsviçre Safe Harbor Çerçevelerine uygunluğunu belirlememiştir.

6. Ek Bilgiler

Bulut Hizmeti, mobil uygulamalardaki ve mobil Web hizmetlerindeki çeşitli potansiyel güvenlik ve mevzuata uygunluk sorunlarını belirlemek üzere tasarlanmıştır. Tüm güvenlik açıklarını ya da uygunluk risklerini test etmez ya da güvenlik saldırıları için bir engel olarak hizmet vermez. Güvenlik tehditleri, mevzuatı ve standartları sürekli olarak değişmektedir ve bu Hizmet bu değişikliklerin tamamını yansıtmayabilir. Müşterinin mobil uygulamasının, sistemlerinin ve çalışanlarının güvenliği ve mevzuata uygunluğu ile herhangi bir çözüm etkinliği yalnızca Müşterinin sorumluluğundadır. Hizmet kapsamında sağlanan bilgileri kullanmak veya kullanmamak yalnızca Müşterinin takdirindedir.

6.1 Türetilen Yararlanma Lokasyonları

Geçerli olduğunda, vergiler hesaplanırken Müşterinin Bulut Hizmetlerinden yararlandığını belirttiği lokasyon(lar) esas alınacaktır. IBM, Müşteri tarafından IBM'e ek bilgiler sağlanmadıkça, bir Bulut Hizmeti sipariş edilirken belirtilen iş adresini birincil Yararlanma lokasyonu varsayarak vergileri bu adrese uygun

olarak uygulayacaktır. Anılan bilgilerin güncel tutulması ve herhangi bir değişikliğin IBM'e bildirilmesi Müşterinin sorumluluğundadır.

6.2 Tanımlama Bilgileri

Müşteri, IBM'in Bulut Hizmetinin normal işletimi ve desteklenmesi kapsamında, takip ve diğer teknolojiler aracılığıyla kendisinden (çalışanlarından ve yüklenicilerinden) Bulut Hizmetinin kullanımına ilişkin kişisel bilgiler toplayabileceğini bildiğini ve bu bilgilerin toplanmasına izin verdiğini kabul eder. IBM, bunu kullanıcı deneyiminin iyileştirilmesi ve/veya Müşteriyle olan etkileşimlerin kişiselleştirilmesi amacıyla Bulut Hizmetinin etkinliğine ilişkin kullanım istatistikleri ve bilgileri toplamak için yapmaktadır. Müşteri, IBM'in toplanan kişisel bilgileri, yukarıda belirtilen amaç uyarınca IBM, diğer IBM şirketleri ve bunların alt yüklenicileri içerisinde, IBM'in ve alt yüklenicilerinin iş yaptıkları herhangi bir yerde, geçerli yasalara uygun olarak işlemesi için izin alacağını ya da almış olduğunu doğrular. IBM, Müşteri çalışanlarının ve yüklenicilerinin toplanan kişisel bilgilere erişmeye, bunların güncellenmesine, düzeltilmesine ya da silinmesine ilişkin taleplerini karşılayacaktır.