Syarat-syarat Penggunaan IBM – Syarat-syarat Tawaran Spesifik SaaS

IBM Application Security on Cloud

Syarat-syarat Penggunaan ("ToU") terdiri dari Syarat-syarat Penggunaan IBM – Syarat-syarat Tawaran Spesifik SaaS ("Syarat-syarat Tawaran Spesifik SaaS") ini dan sebuah dokumen berjudul Syarat-syarat Penggunaan IBM – Syarat-syarat Umum ("Syarat-syarat Umum") yang tersedia di URL berikut: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

Apabila terdapat ketidaksesuaian, Syarat-syarat Tawaran Spesifik SaaS akan berlaku di atas Syarat-syarat Umum. Dengan memesan, mengakses, atau menggunakan SaaS IBM, Klien menyetujui ToU.

ToU diatur oleh Perjanjian Keuntungan Paspor Internasional IBM, Perjanjian Ekspres Keuntungan Paspor Internasional IBM, atau Perjanjian Internasional IBM untuk Tawaran SaaS IBM Terpilih, sebagaimana yang berlaku ("Perjanjian") dan bersama dengan ToU merupakan perjanjian yang lengkap.

1. SaaS IBM

Tawaran SaaS IBM berikut dicakup oleh Syarat-syarat Tawaran Spesifik SaaS ini:

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

2. Metrik Biaya

SaaS IBM dijual berdasarkan metrik biaya berikut, sebagaimana yang ditetapkan dalam Dokumen Transaksi:

a. **Pekerjaan** – adalah suatu unit ukuran yang olehnya SaaS IBM dapat diperoleh. Suatu Pekerjaan merupakan suatu objek di dalam SaaS IBM yang tidak dapat dibagi lagi dan mewakili proses komputasi termasuk seluruh sub-prosesnya. Kepemilikan yang memadai harus diperoleh untuk mencakup total jumlah Pekerjaan yang diproses atau dikelola oleh SaaS IBM selama periode pengukuran yang ditetapkan dalam Bukti Kepemilikan (PoE) atau Dokumen Transaksi Klien.

b. **Mesin Virtual Aplikasi** – adalah suatu unit ukuran yang olehnya SaaS IBM dapat diperoleh. Kepemilikan atas Mesin Virtual Aplikasi diperlukan untuk setiap mesin virtual Aplikasi yang terhubung ke SaaS IBM. Apabila suatu Aplikasi memiliki beberapa komponen, yang masing-masing memiliki tujuan dan/atau dasar pengguna yang berbeda, dan masing-masing komponen dapat dihubungkan ke atau dikelola oleh SaaS IBM, masing-masing komponen tersebut dianggap sebagai Aplikasi yang terpisah. Selain itu, lingkungan pengujian, pengembangan, *staging*, dan produksi untuk suatu Aplikasi masing-masing dianggap sebagai mesin virtual terpisah dari Aplikasi dan masing-masing harus mempunyai kepemilikan. Beberapa Mesin Virtual Aplikasi dalam suatu lingkungan tunggal masing-masing dianggap sebagai mesin virtual terpisah dari Aplikasi tersebut dan masing-masing harus mempunyai kepemilikan. Kepemilikan yang memadai harus diperoleh untuk mencakup jumlah Mesin Virtual Aplikasi yang terhubung ke SaaS IBM selama periode pengukuran yang ditetapkan dalam PoE atau Dokumen Transaksi Klien.

   Untuk tujuan SaaS IBM ini:

   - Untuk Pengujian Dinamis: situs web yang dapat ditemukan melalui URL pribadi atau publik. Setiap Mesin Virtual Aplikasi memiliki situs dengan hingga 1.000 halaman dalam suatu domain tunggal.
   - Untuk Pengujian Statik: suatu unit kode yang dapat dijalankan dalam suatu bahasa pemrograman tunggal. Setiap Mesin Virtual Aplikasi memiliki unit pemindaian kode hingga 1.000.000 jalur.
   - Untuk Pengujian Mobile: suatu unit kode biner yang dapat dijalankan pada perangkat mobile. Setiap platform mobile yang berbeda (misalnya, iOS dan Android) merupakan Mesin Virtual Aplikasi yang berbeda.

c. **Mesin Virtual** – adalah suatu unit ukuran yang olehnya SaaS IBM dapat diperoleh. Suatu Mesin Virtual adalah akses ke suatu konfigurasi spesifik dari SaaS IBM. Kepemilikan yang memadai harus diperoleh untuk setiap Mesin Virtual SaaS IBM yang tersedia untuk akses dan penggunaan selama

periode pengukuran yang ditetapkan dalam Bukti Kepemilikan (PoE) atau Dokumen Transaksi Klien.

Untuk setiap kepemilikan Mesin Virtual, tidak ada batas untuk jumlah Pekerjaan yang dilakukan atau Mesin Virtual Aplikasi (Aplikasi yang terhubung), namun dengan ketentuan bahwa, tidak lebih dari 30 Pekerjaan dapat dijalankan pada suatu waktu tertentu.

d. **Pengikatan** – adalah suatu unit ukuran yang olehnya layanan-layanan dapat diperoleh. Suatu Pengikatan terdiri atas layanan profesional dan/atau pelatihan yang berkaitan dengan SaaS IBM. Kepemilikan yang memadai harus diperoleh untuk mencakup setiap Pengikatan.

3. Biaya dan Penagihan

Jumlah yang harus dibayarkan untuk SaaS IBM ditetapkan dalam Dokumen Transaksi.

3.1 Biaya Pertengahan Bulan (*Partial Month Charges*)

Biaya pertengahan bulan sebagaimana yang ditetapkan dalam Dokumen Transaksi dapat dinilai secara pro-rata.

3.2 Biaya untuk Kelebihan Penggunaan

Apabila penggunaan yang sebenarnya atas SaaS IBM selama periode pengukuran melampaui kepemilikan yang ditetapkan dalam PoE, maka Klien akan ditagih untuk kelebihan penggunaan tersebut sebagaimana yang ditetapkan dalam Dokumen Transaksi.

3.3 Biaya Pengaturan

Klien akan dikenai biaya untuk pengaturan seperti yang ditetapkan dalam Dokumen Transaksi.

4. Jangka Waktu dan Opsi Pembaruan

Jangka waktu SaaS IBM dimulai pada tanggal ketika IBM memberi tahu Klien mengenai akses mereka ke SaaS IBM, sebagaimana yang didokumentasikan dalam PoE. PoE akan menetapkan apakah SaaS IBM memperbarui secara otomatis, berlanjut berdasarkan penggunaan berkelanjutan, atau berakhir pada akhir jangka waktu.

Untuk pembaruan otomatis, kecuali apabila Klien memberikan pemberitahuan tertulis untuk tidak memperbarui setidaknya 30 hari sebelum tanggal habis masa berlakunya jangka waktu, SaaS IBM akan secara otomatis memperbarui untuk jangka waktu yang ditetapkan dalam PoE.

Untuk penggunaan berkelanjutan, SaaS IBM akan terus tersedia dengan basis per bulan hingga Klien memberikan pemberitahuan tertulis 30 hari sebelumnya mengenai pengakhiran. SaaS IBM akan tetap tersedia hingga akhir bulan kalender setelah periode 30 hari tersebut.

5. Dukungan Teknis

Selama Periode Langganan dan setelah IBM memberi tahu Klien bahwa akses ke Saas IBM tersedia, dukungan teknis diberikan melalui forum online dan sebagai dukungan standar selama periode waktu di mana Klien dikenai biaya Bayar per Penggunaan (Pay per Use). Dari dalam SaaS IBM, Klien dapat mengajukan tiket dukungan atau membuka sesi obrolan untuk mendapatkan bantuan. IBM akan menyediakan Buku Petunjuk Dukungan Perangkat Lunak sebagai Layanan IBM yang memberikan informasi kontak dukungan teknis serta informasi dan proses lain.

Tingkat Permasalahan	Definisi Tingkat Permasalahan	Sasaran Waktu Tanggapan	Cakupan Waktu Tanggapan
1	**Pengaruh bisnis penting/layanan bermasalah:** Fungsi penting bisnis tidak dapat beroperasi atau antarmuka penting telah gagal. Hal ini biasanya berlaku pada lingkungan produksi dan mengindikasikan ketidakmampuan untuk mengakses layanan yang berpengaruh penting pada pengoperasian. Kondisi ini memerlukan suatu solusi yang mendesak.	Dalam 1 jam	24x7
2	**Pengaruh bisnis yang signifikan:** Suatu fitur bisnis layanan atau fungsi dari layanan sangat terbatas dalam penggunaannya atau Klien berisiko melewati tenggat waktu bisnis.	Dalam 2 jam kerja	Jam kerja S-J

Tingkat Permasalahan	Definisi Tingkat Permasalahan	Sasaran Waktu Tanggapan	Cakupan Waktu Tanggapan
3	**Pengaruh bisnis minor:** Mengindikasikan fungsi atau layanan dapat digunakan dan tidak berpengaruh penting terhadap pengoperasian.	Dalam 4 jam kerja	Jam kerja S-J
4	**Pengaruh bisnis minimum:** Pertanyaan atau permintaan non-teknis	Dalam 1 hari kerja	Jam kerja S-J

5.1 Akses ke Data Klien

IBM akan dapat mengakses data Klien untuk tujuan mendiagnosis masalah yang terjadi dengan layanan, dan memfasilitasi pemindaian aplikasi Klien oleh layanan. IBM akan mengakses data hanya untuk tujuan memperbaiki kecacatan atau menyediakan dukungan untuk layanan atau produk IBM.

6. Syarat-syarat Tambahan Tawaran SaaS IBM

Pemindaian keamanan tidak dapat mengidentifikasi semua risiko keamanan dalam suatu aplikasi, dan juga tidak dirancang atau dimaksudkan untuk penggunaan dalam lingkungan yang berbahaya yang memerlukan pengoperasian bebas kesalahan, termasuk namun tidak terbatas pada navigasi penerbangan, sistem kendali lalu lintas udara, sistem persenjataan, sistem pendukung kehidupan, fasilitas nuklir, atau aplikasi lain apa pun di mana kegagalan untuk mengidentifikasi risiko keamanan dapat menyebabkan kematian, cedera pribadi, atau kerusakan properti. Pemindaian keamanan tidak dijamin akan beroperasi tanpa interupsi atau bebas kesalahan.

SaaS IBM dapat digunakan untuk membantu Klien memenuhi kewajiban kepatuhan, yang dapat didasarkan pada peraturan perundang-undangan, regulasi, standar atau kebiasaan umum. Setiap petunjuk, anjuran penggunaan, atau panduan yang diberikan oleh Layanan bukan merupakan advis hukum, akuntansi, atau advis profesional lainnya, dan Klien diperingatkan untuk mendapatkan nasihat ahli hukum atau ahli lainnya sendiri. Klien sepenuhnya bertanggung jawab untuk memastikan bahwa Klien serta aktivitas, aplikasi, dan sistem Klien mematuhi seluruh peraturan perundang-undangan, regulasi, standar, dan kebiasaan umum yang berlaku. Penggunaan Layanan ini tidak menjamin kepatuhan terhadap setiap peraturan perundang-undangan, regulasi, standar atau kebiasaan umum.

SaaS IBM melakukan pengujian invasif dan non-invasif pada situs web dan aplikasi web atau mobile yang dipilih Klien untuk dipindai. Peraturan perundang-undangan tertentu melarang setiap upaya yang tidak sah untuk memasuki atau mengakses sistem komputer. Klien mengizinkan IBM untuk menjalankan Layanan seperti yang diuraikan dalam perjanjian ini dan mengakui bahwa Layanan merupakan akses yang sah ke sistem komputer Klien. IBM dapat mengungkapkan pemberian wewenang ini ke pihak ketiga jika dianggap perlu untuk menjalankan Layanan.

Pengujian memiliki risiko tertentu, termasuk namun tidak terbatas pada batasan berikut ini:

a. sistem komputer Klien saat menjalankan aplikasi yang diuji dapat terhenti (hang) atau terganggu (*crash*), yang mengakibatkan sistem tidak tersedia untuk sementara atau hilangnya data;

b. kinerja dan *throughput* sistem Klien, serta kinerja dan *throughput* dari *router* dan *firewall* terkait, dapat diturunkan (*degraded*) sementara selama pengujian;

c. jumlah pesan catatan (*log messages*) yang berlebihan dapat dihasilkan, mengakibatkan penggunaan ruang *disk* file catatan (*log file*) yang berlebih;

d. data dapat diubah atau dihapus sebagai akibat dari pemeriksaan terhadap kerentanan;

e. alarm dapat dipicu oleh sistem deteksi intrusi;

f. email dapat dipicu oleh fungsi email dari aplikasi web yang sedang diuji;

g. SaaS IBM dapat menghalangi lalu lintas jaringan yang dipantau untuk tujuan mencari peristiwa.

Hak perjanjian tingkat layanan atau ganti rugi apa pun yang diberikan oleh IBM dan berkaitan dengan situs web atau aplikasi yang diuji akan diabaikan selama aktivitas pengujian apa pun.

Apabila Klien memasukkan kredensial log-in yang telah diotentikasi untuk aplikasi yang diuji ke dalam Layanan, Klien harus memasukkan kredensial tersebut hanya untuk akun pengujian dan bukan untuk pengguna produksi. Penggunaan kredensial pengguna produksi dapat mengakibatkan data pribadi ditransmisikan melalui Layanan.

SaaS IBM dapat dikonfigurasikan untuk memindai aplikasi web produksi. Saat Klien menetapkan jenis pemindaian sebagai "produksi", layanan dirancang untuk menjalankan pemindaian dengan cara yang mengurangi risiko-risiko yang tercantum di atas; namun demikian, dalam situasi tertentu, SaaS IBM dapat mengakibatkan penurunan kinerja atau ketidakstabilan dalam infrastruktur dan situs-situs produksi yang diuji. IBM tidak membuat jaminan atau pernyataan apa pun sehubungan dengan kesesuaian penggunaan SaaS IBM untuk memindai situs produksi.

KLIEN BERTANGGUNG JAWAB UNTUK MENENTUKAN APAKAH LAYANAN TELAH SESUAI ATAU AMAN UNTUK SITUS WEB, APLIKASI WEB, APLIKASI MOBILE, ATAU LINGKUNGAN TEKNIS KLIEN.

SaaS IBM dirancang untuk mengidentifikasi berbagai potensi masalah keamanan dan kepatuhan dalam aplikasi web dan mobile serta layanan web. Layanan ini tidak menguji semua risiko kerentanan atau kepatuhan, ataupun bertindak sebagai penghalang terhadap serangan keamanan. Ancaman keamanan, regulasi, dan standar terus-menerus berubah, dan Layanan ini tidak dapat merefleksikan semua perubahan tersebut. Keamanan dan kepatuhan aplikasi web, sistem dan karyawan Klien, serta tindakan perbaikan apa pun, merupakan tanggung jawab Klien sepenuhnya. Atas kebijakannya sendiri Klien dapat menggunakan atau tidak menggunakan informasi apa pun yang diberikan oleh Layanan.

Peraturan perundang-undangan tertentu melarang setiap upaya yang tidak sah untuk memasuki atau mengakses sistem komputer. KLIEN BERTANGGUNG JAWAB UNTUK MEMASTIKAN BAHWA KLIEN TIDAK MENGGUNAKAN LAYANAN UNTUK MEMINDAI SITUS WEB DAN/ATAU APLIKASI APA PUN SELAIN SITUS WEB DAN/ATAU APLIKASI YANG DIMILIKI OLEH KLIEN ATAU YANG UNTUKNYA KLIEN MEMILIKI HAK DAN OTORITAS UNTUK MEMINDAI.

Agar lebih jelas, konten Klien yang diuraikan dalam pasal perlindungan data pada Syarat-syarat Penggunaan IBM – Syarat-syarat Umum juga dianggap mencakup data yang dapat diakses oleh IBM selama Pengujian Penetrasi Aplikasi.

6.1 Sistem yang Dimiliki oleh Pihak Ketiga

Untuk sistem (yang untuk tujuan penyediaan ini mencakup namun tidak terbatas pada aplikasi dan alamat IP) yang dimiliki oleh pihak ketiga yang akan menjadi subjek pengujian berdasarkan perjanjian ini, Klien menyetujui:

a. bahwa sebelum IBM memulai pengujian pada sistem pihak ketiga, Klien memperoleh surat bertanda tangan dari pemilik setiap sistem yang mengizinkan IBM untuk memberikan Layanan pada sistem tersebut, dan mengindikasikan persetujuan pemilik atas ketentuan yang tercantum dalam pasal yang berjudul "Izin untuk Menjalankan Pengujian" dan untuk memberikan salinan otorisasi tersebut kepada IBM;

b. bertanggung jawab sepenuhnya untuk mengkomunikasikan risiko, eksposur, dan kerentanan apa pun yang teridentifikasi dalam sistem ini oleh pengujian jarak jauh IBM kepada pemilik sistem; dan

c. untuk mengatur dan memfasilitasi pertukaran informasi antara pemilik sistem dan IBM sebagaimana dianggap perlu oleh IBM.

Klien menyetujui:

- untuk segera memberi tahu IBM jika terdapat perubahan pada kepemilikan sistem apa pun yang menjadi subjek pengujian berdasarkan perjanjian ini;
- tidak mengungkapkan materi yang disampaikan, atau fakta bahwa IBM menjalankan Layanan, di luar Perusahaan Klien tanpa persetujuan tertulis sebelumnya dari IBM; dan
- untuk memberikan ganti rugi kepada IBM sepenuhnya atas kehilangan atau tanggung jawab apa pun yang dibebankan oleh IBM karena klaim pihak ketiga yang timbul karena kegagalan Klien untuk mematuhi persyaratan pasal yang berjudul, "Sistem yang Dimiliki oleh Pihak Ketiga" ini dan untuk surat panggilan pengadilan atau klaim pihak ketiga apa pun terhadap IBM atau subkontraktor atau agen IBM yang timbul karena (a) pengujian risiko keamanan, eksposur atau kerentanan sistem yang merupakan subjek pengujian berdasarkan perjanjian ini, (b) memberikan hasil pengujian tersebut kepada Klien, atau (c) penggunaan atau pengungkapan Klien atas hasil tersebut.

6.2 Cookies

Klien menyadari dan menyetujui bahwa IBM dapat, sebagai bagian dari dukungan dan operasi normal atas SaaS IBM, mengumpulkan informasi pribadi dari Klien (karyawan dan kontraktor Anda) terkait dengan penggunaan SaaS IBM, melalui pelacakan dan teknologi lainnya. IBM melakukan hal tersebut untuk mengumpulkan statistik penggunaan dan informasi mengenai keefektifan SaaS IBM kami untuk tujuan meningkatkan pengalaman pengguna dan/atau menyesuaikan interaksi dengan Klien. Klien

mengonfirmasi bahwa pihaknya akan atau telah memperoleh persetujuan untuk mengizinkan IBM memproses informasi pribadi yang dikumpulkan untuk tujuan di atas dalam IBM, perusahaan IBM lainnya dan subkontraktor mereka, di mana pun kami dan subkontraktor kami melakukan bisnis, sesuai dengan hukum yang berlaku. IBM akan mematuhi permintaan dari karyawan dan kontraktor Klien untuk mengakses, memperbarui, memperbaiki, atau menghapus informasi pribadi mereka yang dikumpulkan.

Sebagai bagian dari SaaS IBM, yang mencakup aktivitas pelaporan, IBM akan mempersiapkan dan mengelola informasi yang di de-identifikasi dan/atau agregat yang dikumpulkan dari SaaS IBM (disebut "Data Keamanan"). Data Keamanan tidak akan mengidentifikasi Klien, atau individu, kecuali sebagaimana yang ditentukan dalam butir (d) di bawah ini. Selain itu, dalam hal ini Klien setuju bahwa IBM dapat menggunakan dan/atau menyalin Data Keamanan hanya untuk tujuan berikut:

a. memublikasikan dan/atau mendistribusikan Data Keamanan (misalnya dalam kompilasi dan/atau analisis yang terkait dengan keamanan dunia maya);

b. mengembangkan atau meningkatkan produk atau layanan;

c. menjalankan penelitian secara internal atau dengan pihak ketiga; dan

d. pembagian yang sah secara hukum atas informasi pelaku kejahatan pihak ketiga yang dikonfirmasi.

6.3 Lokasi Manfaat yang Diperoleh

Apabila berlaku, pajak didasarkan pada lokasi(-lokasi) yang diidentifikasi oleh Klien sebagai penerima manfaat dari SaaS IBM. IBM akan menerapkan pajak berdasarkan alamat bisnis yang dicantumkan pada saat memesan SaaS IBM sebagai lokasi manfaat utama kecuali apabila Klien memberikan informasi tambahan kepada IBM. Klien bertanggung jawab untuk tetap memperbarui informasi tersebut dan menyampaikan setiap perubahan kepada IBM.

6.4 Informasi Pribadi dan Konten dan Layanan yang Diatur

SaaS IBM ini tidak dirancang untuk persyaratan keamanan spesifik apa pun untuk konten yang diatur, seperti informasi pribadi atau informasi pribadi yang sensitif. Klien bertanggung jawab untuk menentukan apakah SaaS IBM ini memenuhi kebutuhan Klien terkait dengan jenis konten yang digunakan oleh Klien dalam hubungannya dengan SaaS IBM.

IBM tidak beroperasi sebagai penyedia layanan yang diatur oleh Komisi Komunikasi Federal (*Federal Communications Commission* - "FCC") atau otoritas pengaturan negara bagian ("Regulator Negara Bagian"), dan tidak bermaksud untuk memberikan layanan apa pun yang diatur oleh FCC atau Regulator Negara Bagian. Jika FCC atau Regulator Negara Bagian mana pun membebankan kewajiban atau persyaratan pengaturan pada layanan apa pun yang diberikan oleh IBM berdasarkan perjanjian ini, IBM dapat: (a) memodifikasi, mengganti, atau mencadangkan produk dengan biaya yang ditanggung oleh Klien, dan/atau (b) mengubah cara layanan tersebut diberikan kepada Klien untuk menghindari pelaksanaan persyaratan atau kewajiban tersebut pada IBM (misalnya, dengan bertindak sebagai agen Klien untuk mendapatkan layanan tersebut dari angkutan umum pihak ketiga).

Apendiks A

1. Deskripsi Umum IBM Application Security on Cloud

IBM Application Security on Cloud memberikan suatu tempat tunggal untuk membantu Klien dalam mengidentifikasi kerentanan keamanan (seperti Injeksi SQL, Scripting Lintas Situs (*Cross-Site Scripting*), dan Kebocoran Data) untuk berbagai aplikasi. Layanan mencakup berbagai jenis teknik pemindaian keamanan aplikasi, yang masing-masing mengidentifikasi masalah keamanan dalam aplikasi tersebut.

IBM Application Security on Cloud memberikan kemampuan berikut:

- Memindai Aplikasi Mobile untuk kerentanan keamanan. Hal ini dilakukan melalui teknologi analisis keamanan dinamis (*blackbox*) dan Interaktif (*glassbox*).
- Memindai situs Web produksi atau pra-produksi di jaringan publik atau pribadi, untuk kerentanan keamanan. Hal ini dilakukan melalui teknik analisis keamanan dinamis (*blackbox*).
- Memindai alur data dalam aplikasi Web dan Desktop untuk kerentanan keamanan. Hal ini dilakukan melalui teknik analisis keamanan statis (*whitebox*).
- Laporan kerentanan keamanan terperinci yang mencakup ringkasan tingkat tinggi tentang temuan dan langkah-langkah perbaikan yang dapat dilakukan oleh para pengembang.
- Integrasi dengan berbagai platform DevOps

1.1 IBM Application Analyzer

IBM Application Analyzer dapat dipesan per Mesin Virtual Aplikasi, per Pekerjaan (pindai), atau sebagai Mesin Virtual lengkap dan memungkinkan tipe pemindaian berikut ini:

- Penganalisis Dinamis (Dynamic Analyzer) – Menguji situs web pra-produksi atau produksi dengan teknik DAST
- Penganalisis Mobile (Mobile Analyzer) – Menguji biner iOS atau Android dengan teknik IAST
- Penganalisis Statik (Static Analyzer) – Menguji arus data bita- atau kode sumber dengan teknik SAST

1.2 Layanan Pengaturan

IBM Application Security on Cloud Consulting Services adalah layanan pengaturan yang dapat diproduksi untuk Application Analyzer. Layanan tersebut menggunakan konsultan IBM untuk memberikan panduan dan bantuan dengan pengujian dan pengelolaan risiko aplikasi. IBM Application Security on Cloud Consulting Services dibeli sebagai blok Pengikatan yang dapat ditambah pada kuantitas yang tercantum di bawah ini untuk permintaan dan penggunaan layanan spesifik berikut ini:

a. **Mulai Cepat** [Menggunakan satu (1) unit Pengikatan]

Layanan Mulai Cepat memberikan keahlian dan panduan untuk menggunakan fitur pengujian dan pengelolaan risiko Application Security on Cloud. Setelah Klien mengkonfirmasi berhasil login ke portal Application Security on Cloud, IBM akan memfasilitasi konferensi web untuk hingga dua (2) jam dan dua (2) peserta aktif guna memberikan pendidikan mengenai AppSec dasar pada fungsi dan konfigurasi SaaS IBM termasuk mengenai tipe pindai, menjalankan pemindaian, meninjau laporan dan memasang peralatan dan plug-in terkait. Layanan Mulai Cepat selesai setelah penyelesaian terhadap (a) webinar pendidikan klien, (b) pemasangan peralatan dan plug-in yang dapat dipakai, dan (c) membantu Klien untuk mengatur dan menjalankan pemindaian pertama Klien.

b. **Peninjauan Penilaian** [Menggunakan dua (2) unit Pengikatan]

Layanan Peninjauan Penilaian memberikan bantuan peninjauan hasil pengujian, termasuk memahami dan memprioritaskan perbaikan pada kerentanan dalam aplikasi. IBM akan memfasilitasi konferensi web untuk hingga satu (1) jam dan dua (2) peserta aktif untuk memberikan ikhtisar mengenai kerentanan yang ditemukan dan keseluruhan risiko aplikasi keamanan dan diskusi terperinci pada kerentanan keamanan aplikasi yang ditemukan termasuk (1) cara untuk menguji kerentanan, (2) cara mendeteksi kerentanan, (3) risiko setiap kerentanan, dan (4) memberikan rekomendasi perbaikan umum untuk membantu memperbaiki kerentanan. Peninjauan hanya akan berdasarkan pada hasil pengujian dan bukan merupakan peninjauan atas kode sumber

itu sendiri. Klien akan meninjau hasil pengujian dan akan mengidentifikasi kepada IBM mengenai hasil pengujian untuk peninjauan sebelum konferensi web. Layanan Peninjauan Penilaian selesai setelah penyelesaian konferensi web.

c. **Pindai untuk Saya** [Menggunakan empat (4) unit Pengikatan]

Layanan Pindai untuk Saya menyediakan seorang ahli keamanan aplikasi IBM yang akan mengkonfigurasi dan menjalankan pemindaian, memvalidasi hasil, dan menjalankan pengarahan singkat laporan untuk meninjau temuan. Klien akan mengizinkan konsultan IBM untuk mengakses lingkungan ASoC-nya untuk mengkonfigurasi dan menjalankan pemindaian, memvalidasi hasil, memberikan rekomendasi pada prioritas perbaikan, dan menjalankan pengarahan singkat laporan mengenai hasil. IBM akan memfasilitasi konferensi web untuk hingga satu (1) jam dan dua (2) peserta aktif untuk memberikan ikhtisar mengenai kerentanan yang ditemukan dan keseluruhan risiko aplikasi keamanan dan diskusi terperinci pada kerentanan keamanan aplikasi yang ditemukan termasuk (1) cara untuk menguji kerentanan, (2) cara mendeteksi kerentanan, (3) risiko setiap kerentanan, dan (4) memberikan rekomendasi perbaikan umum untuk membantu memperbaiki kerentanan. Jika diminta, dan sebelum 30 hari setelah pemindaian awal, IBM akan menyediakan pemindaian ulang dengan menggunakan konfigurasi pemindaian awal hanya untuk memverifikasi perbaikan keamanan, tidak untuk menguji fungsionalitas baru, memvalidasi hasil dan mengirim laporan kepada klien. Layanan Pindai untuk Saya selesai setelah penyelesaian konferensi web untuk meninjau hasil pemindaian awal atau, jika berlaku, penyelesaian pemindaian ulang seperti yang diminta oleh Klien dan mengirimkan laporan pemindaian ulang kepada Klien.

d. **Penasihat berdasarkan Permintaan** [Menggunakan tujuh (7) unit Pengikatan]

Layanan Penasihat berdasarkan Permintaan memberikan hingga dua puluh (20) jam waktu konsultasi IBM yang dapat digunakan untuk aktivitas terkait dengan SaaS IBM. Konsultan IBM akan membantu dengan topik spesifik keamanan aplikasi, termasuk, namun tidak terbatas pada, pengelolaan program, prioritas pengujian keamanan, strategi perbaikan, analisis kode sumber dan perbaikan kode sumber. IBM akan bekerja dengan Klien untuk memahami dan membuat suatu skedul proyek dengan persyaratan Klien yang spesifik, termasuk sasaran proyek, teknologi yang sesuai, lini waktu yang diinginkan, materi yang disampaikan yang diharapkan, dan perkiraan jumlah pengikatan layanan Penasihat berdasarkan Permintaan. Klien harus memberikan akses ke aplikasi, sistem dan dokumentasi penting yang diperlukan untuk menjalankan layanan. Layanan Penasihat berdasarkan Permintaan selesai setelah 20 jam keahlian keamanan telah dilaksanakan dan/atau setelah skedul proyek dan/atau materi yang disampaikan terdokumentasi yang ditentukan dalam skedul proyek telah dikirim kepada Klien.

e. **Pengujian Penetrasi Aplikasi**

Tiga Opsi:

(1) **Pengujian Penetrasi Aplikasi Tingkat Awal/Pemenuhan**, yang mencakup hingga empat puluh (40) jam waktu Konsultasi, dan fokus pada kesalahan logika Langkah-tunggal, dan versi yang Lebih Sederhana atas kesalahan injeksi. Menggunakan lima belas (15) unit Pengikatan.

(2) **Pengujian Penetrasi Aplikasi Standar**, yang mencakup hingga enam puluh (60) jam waktu Konsultasi, dan memperluas fokus untuk mencakup kesalahan Logika dalam alur kerja multi-langkah, versi Kompleks atas kesalahan injeksi dan Analisis tipe data kompleks. Menggunakan dua puluh satu (21) unit Pengikatan.

(3) **Pengujian Penetrasi Aplikasi Lanjutan** – Hingga delapan puluh (80) jam waktu Konsultasi, dan memperluas fokus untuk mencakup teknik Pemutar balik dari program yang dapat dijalankan yang terkompilasi, Pemotongan protokol jaringan kustom, analisis Mendalam atas kerangka kerja dan pustaka yang tersedia secara publik. Menggunakan dua puluh tujuh (27) unit Pengikatan.

Layanan pengujian penetrasi aplikasi memberikan sumber daya IBM untuk menjalankan pengujian dan eksploitasi aplikasi, pengiriman laporan pengujian, dan pengarahan singkat laporan untuk menjelaskan temuan dan risiko terkait.

IBM akan memfasilitasi panggilan awal proyek untuk hingga satu (1) jam dan dua (2) peserta aktif untuk meninjau lingkungan dan organisasi Klien, termasuk platform aplikasi, arsitektur, kerangka kerja, infrastruktur pendukung, masalah keamanan yang diketahui atau persoalan terkait dengan aplikasi, skedul pengujian awal dan rencana kontak darurat.

IBM akan mengadakan pengujian penetrasi aplikasi termasuk, namun tidak terbatas pada: identifikasi kerentanan umum seperti injeksi SQL dan penulisan skrip lintas situs, penilaian keunggulan dan kelemahan pengendali keamanan yang ada seperti validasi input, otentikasi, dan otorisasi, memeriksa pelaksanaan logika bisnis yang sesuai, validasi penggunaan protokol keamanan yang sesuai, identifikasi kesalahan penanganan sesi, dan verifikasi pengendalian keamanan yang sesuai pada login, pembaruan kata sandi, kebijakan kata sandi, dan fungsi pengelolaan pengguna lainnya. Temuan akan didokumentasikan dalam Laporan Pengujian Penetrasi Aplikasi. IBM akan memfasilitasi konferensi web untuk pengarahan singkat laporan selama hingga satu (1) jam. Layanan Pengujian Penetrasi Aplikasi selesai saat waktu konsultasi yang diberikan telah digunakan, konferensi web telah dijalankan dan Laporan Pengujian Penetrasi Aplikasi akhir telah dikirimkan kepada Klien.

1.2.1 Tanggung Jawab Layanan Pengaturan

IBM akan:

- memberikan Layanan Pengaturan dengan menggunakan unit Pengikatan yang dibeli oleh Klien dan per POE; dan
- telah menyelesaikan Layanan Pengaturan saat kriteria penyelesaian yang diuraikan dalam Pasal 1.2 telah selesai.

Klien menyetujui:

- untuk bertanggung jawab atas semua biaya terkait dengan semua permintaan Pengikatan yang dibuat oleh Klien selama jangka waktu kontrak;
- dan memahami, bahwa unit Pengikatan yang dibeli harus digunakan dalam jangka waktu kontrak awal dan berakhir jika tidak digunakan hingga tanggal akhir periode kontrak; dan
- untuk mengajukan permintaan resmi untuk semua Layanan Pengaturan dalam jangka waktu 30 hari sebelum tanggal akhir langganan.

Dalam kinerja Layanan Pengaturan apa pun, IBM dapat meminta informasi dan kerja sama yang wajar dari Klien. Kegagalan Klien untuk memberikan informasi atau kerja sama yang diminta pada waktu yang tepat dapat, seperti yang ditentukan oleh IBM, mengakibatkan biaya pada unit Pengikatan seperti yang diwajibkan oleh layanan atau keterlambatan pada kinerja layanan yang berlaku.

Agar IBM dapat menjalankan pengujian dengan akurat, Klien menyetujui untuk mematuhi instruksi IBM dalam mempersiapkan dan mengelola lingkungan selama periode pengujian.

This document is made in the English and Indonesian languages. To the extent permitted by the prevailing law, the English language of this document will prevail in the case of any inconsistencies or differences of interpretation with the Indonesian language text of this document.

Dokumen ini dibuat dalam bahasa Indonesia dan bahasa Inggris. Sepanjang diperbolehkan oleh hukum yang berlaku, dalam hal terdapat ketidaksesuaian atau perbedaan penafsiran dengan teks bahasa Indonesia dari dokumen ini, maka teks dalam bahasa Inggris yang akan berlaku.