IBM Resilient Security Orchestration, Automation and Response on Cloud

Uraian Layanan ini menguraikan Layanan Cloud. Dokumen pemesanan yang berlaku memberikan penentuan harga dan rincian tambahan tentang pemesanan Klien.

1. Layanan Cloud

IBM Resilient Security Orchestration, Automation, and Response (SOAR) Platform on Cloud memungkinkan organisasi untuk mengatur dan mengotomatiskan orang-orang, proses, dan teknologi yang terkait dengan tanggapan insiden.

IBM Resilient SOAR Platform on Cloud mengefisiensikan manajemen tanggapan insiden dan tanggapan privasi untuk menyampaikan cara yang diotomatiskan, lebih cepat, dan lebih fleksibel bagi organisasi untuk bereaksi terhadap peristiwa dan insiden. Resilient SOAR Platform on Cloud menyampaikan dasar pertahanan keamanan dunia maya yang sukses yang memungkinkan organisasi untuk:

- Membuat rencana tanggapan yang didasarkan pada standar industri dan praktik terbaik.
- Berintegrasi secara lebih mudah dengan alat keamanan dan TI, dan mengatur tanggapan terhadap peristiwa dan insiden.
- Berkolaborasi di seluruh organisasi, melengkapi berbagai pemangku kepentingan dengan alat untuk menjalankan peran dan tugas mereka sebagai bagian dari upaya tanggap insiden.

IBM Resilient SOAR Platform dirancang untuk organisasi dengan berbagai ukuran dan kompleksitas dan dapat dibeli dengan beberapa add-on opsional. Klien tidak diizinkan menggunakan kemampuan kecuali yang ditentukan dalam tawaran atau add-on yang telah mereka beli.

1.1 Tawaran

Klien dapat memilih dari tawaran berikut yang tersedia:

1.1.1 IBM Resilient SOAR Platform on Cloud

IBM Resilient SOAR Platform on Cloud Orchestration menawarkan dasar pertahanan keamanan dunia maya. Klien dapat membuat rencana tanggapan berdasarkan standar industri dan praktik terbaik, berintegrasi dengan alat keamanan dan TI dengan mudah, dan mengatur tanggapan terhadap peristiwa dan insiden. Layanan Cloud ini memfasilitasi kolaborasi di seluruh organisasi, memungkinkan berbagai pemangku kepentingan untuk menjalankan peran dan tugas mereka sebagai bagian dari upaya tanggap insiden.

Tim keamanan dapat berkolaborasi pada peristiwa dan insiden keamanan dunia maya menggunakan kemampuan manajemen kasus yang dibuat dengan tujuan pada platform. Dynamic Playbook beradaptasi dengan serangan yang berkembang dengan cepat, dan tim dapat dengan cepat mengulangi proses untuk meningkatkan keefektifan dengan menyesuaikan playbook, bidang data, dan tata letak tampilan. Selanjutnya simulasi membantu penyempurnaan proses tanggapan. Integrasi bawaan dan dapat dipasang memberikan pengayaan data guna mengumpulkan konteks untuk pembuatan keputusan tim keamanan dan memungkinkan pengaturan tindakan remediasi, sesuai dengan kuantitas Tindakan per Bulan yang dibeli. Penyerapan (ingestion) dan penguraian email memberikan metode yang ringan untuk meningkatkan dari alat lain. Akses dapat diamankan melalui otentikasi SAML. Analisis transparansi dan risiko dibantu dengan analitik dan pelaporan. Tawaran ini diperlukan untuk semua add-on lain di bawah ini.

1.2 Layanan Opsional

1.2.1 IBM Resilient SOAR Platform Actions on Cloud

IBM Resilient SOAR Platform on Cloud Actions memungkinkan kemampuan pengaturan platform. Integrasi bawaan dan dapat dipasang, termasuk integrasi dengan berbagai umpan inteligensi ancaman, memberikan pengayaan yang diotomatiskan guna mengumpulkan konteks untuk pembuatan keputusan tim keamanan serta pengaturan tindakan remediasi.

1.2.2 IBM Resilient SOAR Platform on Cloud Privacy Add-On

IBM Resilient SOAR Platform on Cloud Privacy memungkinkan Klien untuk menilai dan menanggapi pelanggaran data privasi. Rencana tanggapan yang dibuat melalui tawaran ini beradaptasi terhadap tipe data, kuantitas catatan, dan yurisdiksi peraturan yang berlaku. Klien juga dapat mengakses pengetahuan bawaan mengenai regulasi pemberitahuan pelanggaran kerahasiaan data global yang membantu untuk menyesuaikan rencana tanggapan insiden mereka lebih lanjut.

1.2.3 IBM Resilient SOAR Platform on Cloud Team Management Add-On

IBM Resilient SOAR Platform on Cloud Teams memberikan kepada pengguna pengelolaan dan pemisahan data dalam beberapa tim. Informasi sensitif disimpan dengan basis kebutuhan untuk mengetahui melalui pembatasan akses dengan Workspaces dan dengan pengendalian akses berbasis peran yang dapat disesuaikan. Pengelolaan pengguna dan grup dapat disederhanakan dengan memanfaatkan Direktori Aktif untuk otorisasi pengguna. Grup yang terpisah juga dapat dikonfigurasi untuk memiliki Organisasi milik mereka sendiri.

1.2.4 IBM Resilient SOAR Platform on Cloud MSSP Add-On

IBM Resilient SOAR Platform on Cloud MSSP memberikan kemampuan pengelolaan kasus, proses, penyesuaian, dan pengelolaan playbook di beberapa Organisasi. Peristiwa dan insiden dari beberapa Organisasi dapat ditampilkan dalam antrean tunggal, menyediakan ahli analisis penyedia layanan keamanan terkelola (MSSP) dengan tampilan pelanggan mereka yang komprehensif. Playbook dengan konfigurasi per Organisasi memberikan pengelolaan yang sederhana pada proses yang distandardisasikan dan disesuaikan.

1.2.5 IBM Resilient SOAR Platform on Cloud Non-Production Add-On

IBM Resilient SOAR Platform on Cloud Non-Production adalah mesin virtual terpisah dari IBM Resilient SOAR Platform yang dapat digunakan oleh Klien hanya untuk aktivitas non-produksi internal, termasuk namun tidak terbatas pada pengujian, penyesuaian kinerja, diagnosis kecacatan, penentuan tolok ukur internal, stating, aktivitas uji mutu, dan/atau pengembangan tambahan atau ekstensi yang digunakan secara internal pada Layanan Cloud menggunakan antarmuka pemrograman aplikasi yang dipublikasikan.

1.3 Layanan Percepatan

Tawaran IBM Security Expert Labs (SEL) for Resilient Services adalah layanan yang disampaikan dari jarak jauh yang memberikan waktu pakar Resilient untuk panduan implementasi dan arsitektural yang terkait dengan penyebaran Resilient. Tawaran IBM Resilient Security, Orchestration and Response – baik sebagai Layanan Cloud atau sebagai perangkat lunak di lokasi – adalah prasyarat untuk setiap Layanan ini.

1.3.1 IBM SEL for Resilient Base Starter Service

Dalam 5 hari pengikatan jarak jauh, IBM akan memberikan:

- bantuan menentukan arsitektur IBM Security Resilient;
- IBM Security Resilient yang dipasang & dikonfigurasikan (jika berlaku);
- pelatihan bagi Analis dan Desainer untuk mengonfigurasi dan menggunakan rencana Incident Response terbaru milik Klien, yang menunjukkan persyaratan kunci organisasi Klien;
- IBM Security Resilient configured Playbooks yang didasarkan pada proses unik organisasi Klien;
- cara melacak KPI dan Metrik yang ditentukan menurut kebutuhan organisasi Klien dan praktik terbaik industri; serta
- mengidentifikasi peluang integrasi guna mendukung, mengotomatiskan, dan mengatur proses menyeluruh.

1.3.2 IBM SEL for Resilient Premium Starter Service

Dalam 3 hari pengikatan jarak jauh, IBM akan:

- membantu menentukan arsitektur IBM Security Resilient;
- memasang IBM Security Resilient (jika berlaku);
- mengonfigurasi awal IBM Security Resilient pada lingkungan Klien; dan

- melatih Analis dan Desainer untuk mengonfigurasi dan menggunakan rencana Incident Response terbaru milik Klien, yang menunjukkan persyaratan kunci organisasinya.

1.3.3 IBM SEL for Resilient Additional Day

Selain layanan Starter Base atau Premium, dalam 1 hari pengikatan jarak jauh, IBM akan menjalankan setiap aktivitas terkait IBM Security Resilient, yang akan disetujui sebelumnya. Contohnya:

- dukungan lebih lanjut untuk pemasangan atau konfigurasi IBM Security Resilient atau ekstensi (jika berlaku);
- pelatihan atau dukungan lebih lanjut untuk Analis guna memastikan kesiapan untuk menggunakan IBM Security Resilient sebagai solusi SOAR kunci Klien;
- memandu Desainer tentang cara mengonfigurasi dan menggunakan 'Playbook' mereka sendiri yang menunjukkan persyaratan kunci organisasi Klien; atau
- menjalankan pemindaian cepat atas lingkungan IBM Security Resilient untuk menyarankan area peningkatan potensial.

2. Lembar Data Perlindungan dan Pemrosesan Data

Adendum Pemrosesan Data IBM di http://ibm.com/dpa (Data Processing Addendum - "DPA") dan Lembar(-Lembar) Data Perlindungan dan Pemrosesan Data (disebut sebagai lembar(-lembar) data atau Ekshibit(-Ekshibit) DPA) dalam tautan di bawah memberikan informasi perlindungan data tambahan untuk Layanan Cloud dan opsinya sehubungan dengan tipe Konten yang dapat diproses, aktivitas pemrosesan yang terlibat, fitur perlindungan data, serta pokok-pokok mengenai retensi dan pengembalian Konten. DPA tersebut berlaku untuk data pribadi yang terkandung dalam Konten, apabila dan sejauh i) Regulasi Perlindungan Data Umum Eropa (EU/2016/679) (European General Data Protection Regulation - "GDPR"); atau ii) peraturan perundang-undangan perlindungan data lainnya yang ditetapkan di http://www.ibm.com/dpa/dpl berlaku.

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=A47500205B1911E6865BC3F213DB63F7

3. Tingkat Layanan dan Dukungan Teknis

3.1 Perjanjian Tingkat Layanan

IBM memberikan perjanjian tingkat layanan (SLA) ketersediaan berikut kepada Klien. IBM akan memberlakukan kompensasi yang berlaku yang paling tinggi berdasarkan ketersediaan kumulatif Layanan Cloud sebagaimana yang ditunjukkan dalam tabel di bawah. Persentase ketersediaan dihitung sebagai total jumlah menit dalam suatu bulan masa kontrak, dikurangi total jumlah menit Layanan Berhenti dalam bulan masa kontrak, dibagi dengan total jumlah menit dalam bulan masa kontrak. Definisi Layanan Berhenti, proses klaim dan cara menghubungi IBM terkait permasalahan ketersediaan layanan berada pada buku petunjuk dukungan Layanan Cloud IBM di https://www.ibm.com/software/support/saas_support_overview.html.

Ketersediaan	Kredit (% biaya langganan bulanan*)
Kurang dari 99,9%	2%
Kurang dari 99,0%	5%
Kurang dari 95,0%	10%

* Biaya langganan adalah harga pada masa kontrak untuk bulan yang sesuai dengan klaim.

3.2 Dukungan Teknis

Dukungan teknis untuk Layanan Cloud, termasuk rincian kontak dukungan, level tingkat permasalahan, jam dukungan ketersediaan, waktu tanggapan, dan informasi serta proses dukungan lain, ditemukan dengan memilih Layanan Cloud dalam panduan dukungan IBM yang tersedia di https://www.ibm.com/support/home/pages/support-guide/.

4. Biaya

4.1 Metrik Biaya

Metrik(-metrik) biaya untuk Layanan Cloud ditetapkan dalam Dokumen Transaksi.

Metrik biaya berikut berlaku untuk Layanan Cloud ini:

- Pengguna yang sah adalah pengguna khusus yang diberi wewenang untuk mengakses Layanan Cloud dengan cara apa pun secara langsung atau tidak langsung (misalnya, melalui program, perangkat, atau server aplikasi multipleks) melalui sarana apa pun.
- Pengguna dengan Akses Bersamaan adalah pengguna yang secara bersama-sama mengakses Layanan Cloud dengan cara apa pun secara langsung atau tidak langsung (misalnya, melalui program multipleks, perangkat, atau server aplikasi) kapan pun dalam satu waktu. Individu yang sedang mengakses Layanan Cloud beberapa kali secara serentak, hanya diperhitungkan sebagai Pengguna dengan Akses Bersamaan tunggal.
- Pengikatan adalah layanan pelatihan atau profesional yang berkaitan dengan Layanan Cloud.
- Item adalah kejadian dari suatu item spesifik yang dikelola oleh, diproses oleh, atau yang berkaitan dengan penggunaan Layanan Cloud. Untuk tujuan Layanan Cloud ini, Item adalah suatu Tindakan. Suatu Tindakan adalah permintaan pengaturan atau otomatisasi yang dibuat oleh Layanan Cloud ke program perangkat lunak lain.

5. Syarat-syarat Tambahan

Untuk Perjanjian Layanan Cloud (atau perjanjian cloud dasar yang setara) yang ditandatangani sebelum tanggal 1 Januari 2019, syarat-syarat yang tersedia di https://www.ibm.com/acs adalah yang berlaku.

5.1 Verifikasi

Klien akan i) memelihara, dan memberikan berdasarkan permintaan, catatan, dan output peralatan sistem, sebagaimana yang diperlukan secara wajar bagi IBM dan auditor independennya untuk memverifikasi kepatuhan Klien terhadap Perjanjian, dan ii) segera memesan dan membayar untuk kepemilikan yang diperlukan sesuai dengan tarif IBM yang berlaku saat itu dan untuk biaya serta tanggung jawab lain yang ditentukan sebagai hasil dari verifikasi tersebut, sebagaimana yang ditetapkan oleh IBM dalam tagihan. Kewajiban verifikasi kepatuhan ini akan tetap berlaku selama jangka waktu Layanan Cloud dan selama dua tahun kemudian.

5.2 Persyaratan Kepemilikan Add-On

Klien harus memperoleh jumlah yang setara dan tipe kepemilikan atas Layanan Cloud dasar dan Add-On.

5.3 Pembatasan pada Penggunaan

Setiap Klien berhak untuk membuat maksimum seratus ribu (100.000) kueri Layanan Ancaman per bulan. Klien membuat kueri Layanan Ancaman dengan menambahkan artefak ke suatu insiden saat Layanan Ancaman mereka telah diaktifkan. Untuk setiap dua (2) hari setelahnya, apabila insiden tersebut tetap terbuka dan aktif, kueri Layanan Ancaman baru akan dibuat secara otomatis.

Setiap Klien berhak untuk membuat maksimum seratus (100) email pemberitahuan per hari per Pengguna yang Sah/dengan Akses Bersamaan. Email pemberitahuan dibuat oleh platform Resilient berdasarkan konfigurasi yang dikontrol oleh Klien.

5.4 Informasi Pemrosesan dan Perlindungan Data Tambahan

Untuk menghindari keraguan, IBM Resilient SOAR Platform on Cloud:

- tidak mengenkripsi Konten saat berada di penyimpanan (at rest);
- tidak dirancang untuk memproses setiap Kategori Data Pribadi Khusus; dan
- seharusnya tidak memasukkan data pribadi ke dalam bidang teks bebas jika tidak diminta.

Informasi rinci mengenai enkripsi dan tipe Data Pribadi yang diproses dapat ditemukan di url untuk Lembar Data yang direferensikan pada Pasal 2 di atas.

6. Syarat-syarat Utama

6.1 Penggunaan Data

IBM tidak akan menggunakan atau mengungkapkan hasil yang timbul dari penggunaan Klien atas Layanan Cloud yang khusus untuk Konten Klien (Wawasan) atau, jika tidak, yang mengidentifikasi Klien. Namun demikian, IBM akan menggunakan Konten dan informasi lainnya yang dihasilkan dari Konten sebagai bagian dari Layanan Cloud untuk tujuan peningkatan Layanan Cloud. IBM juga dapat membagikan pengidentifikasi ancaman dan informasi keamanan lainnya yang disematkan dalam Konten untuk tujuan perlindungan dan deteksi ancaman.

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 Inggris dan bahasa Indonesia. 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.