„IBM Cloud Service“ aprašas

„IBM Security AppScan Mobile Analyzer“

Toliau pateiktas jūsų Užsakymo Paslaugų aprašas:

1. „Cloud Service“

„Cloud Service“ pasiūlymas aprašytas toliau ir tiksliai nurodytas pasirinktų taikomų pasiūlymų Užsakymo dokumente. Užsakymo dokumentą sudarys pateiktas Pasiūlymas ir Teisių suteikimo dokumentas (TSD), patvirtinantis „Cloud Services“ pradžios datą ir terminą. Sąskaitų siuntimas prasidės nuo „Cloud Service“ teikimo pradžios.

1.1 „IBM Security AppScan Mobile Analyzer“

Ši paslauga identifikuoja saugos problemas „Android“ taikomųjų programų mobiliesiems kodo lygiu. Ji leidžia kūrėjui nuskaityti saugos pažeidžiamumus nepateikiant taikomosios programos išeitinio kodo. Baigus nuskaitymą paslauga sugeneruoja saugos ataskaitą, į kurią įtraukia išsamią informaciją apie aptiktus pažeidžiamumus, potencialią taikomosios programos mobiliesiems saugos riziką, kurią kelia šie pažeidžiamumai, ir pasiūlymus, kaip juos pašalinti.

2. Saugos aprašas

2.1 Saugos strategijos

IBM turi informacijos apsaugos komandą ir palaiko privatumo bei saugos politiką, kuri yra pateikiama IBM darbuotojams. IBM reikalauja, kad darbuotojai, teikiantys IBM duomenų centrų palaikymą, dalyvautų privatumo ir saugos mokymuose. IBM saugos strategijos ir standartai kasmet peržiūrimi ir iš naujo įvertinami. Su IBM sauga susiję įvykiai valdomi pagal išsamią reagavimo į įvykius procedūrą.

2.2 Prieigos valdymas

Jei reikia, prieiga prie kliento duomenų, laikantis pareigų atskyrimo principo, leidžiama tik įgaliotiesiems IBM palaikymo atstovams ir aptarnavimo operacijų personalui. IBM darbuotojai naudoja dviejų veiksnių tarpinio šliuzo valdymo pagrindinio kompiuterio autentifikavimą. Visi prieigos prie klientų duomenų ryšio kanalai yra užšifruoti.

2.3 Paslaugos vientisumas ir prieinamumas

Operacinių sistemų ir taikomųjų programų programinės įrangos modifikavimus reguliuoja IBM keitimų valdymo procesas. Užkardos taisyklių keitimams taip pat taikomas keitimų valdymo procesas, o prieš diegiant juos peržiūri IBM saugos darbuotojai. Duomenų centrą IBM stebi 24 valandas per parą, 7 dienas per savaitę. Siekiant nustatyti ir pašalinti galimas sistemos saugos spragas, vidaus ir išorės pažeidžiamumo tikrinimą reguliariai atlieka įgaliotieji administratoriai ir teikėjai (trečiosios šalys). Visuose IBM duomenų centruose naudojamos kenkėjiškų programų aptikimo (antivirusinė, įsilaužimo aptikimo, pažeidžiamumo tikrinimo ir įsilaužimo prevencijos) sistemos. IBM duomenų centro tarnybos palaiko įvairius duomenų perdavimo viešaisiais tinklais informacijos pateikimo protokolus. Pavyzdžiui, HTTPS / SFTP / FTPS / S/MIME ir VPN tarp darbo vietų. Atskiroje saugykloje skirta saugoti atsarginė duomenų kopija prieš transportavimą užšifruojama.

2.4 Veiklos registravimas

IBM pildo savo veiklos sistemose, taikomosiose programose, duomenų saugyklose, tarpinėje įrangoje ir tinklo infrastruktūros įrenginiuose, kuriuose galima konfigūruoti ir kurie yra konfigūruoti registruoti veiklą, žurnalus. Siekiant sumažinti klastojimo riziką ir užtikrinti centralizuotą analizę, įspėjimų bei ataskaitų teikimą, veiksmai realiuoju laiku registruojami centrinio žurnalo saugyklose. Siekiant išvengti klastojimo, duomenys pasirašomi. Realiuoju laiku analizuojant žurnalus ir reguliariai pateikiant analizės ataskaitas nustatomi netinkamos veiklos atvejai. Eksploatuojantis personalas įspėjamas apie anomalijas ir, jei reikia, kreipiasi į 24 x 7 pagal iškvietimą pasiekiamą saugos specialistą.

2.5 Fizinė sauga

IBM laikosi fizinės saugos standartų, skirtų neteisėtai fizinei prieigai prie IBM duomenų centrų apriboti. Duomenų centruose yra tik ribotos prieigos vietos, kurios kontroliuojamos taikant dviejų veiksnių autentifikavimą ir stebimos stebėjimo kameromis. Įeiti leidžiama tik įgaliotajam personalui, turinčiam patvirtintą įėjimo leidimą. Vykdantysis personalas patikrina patvirtinimą ir išduoda prieigos leidimą,

suteikiantį reikiamą prieigą. Tokius leidimus gavę darbuotojai privalo atiduoti kitus prieigos leidimus ir lankydamiesi gali turėti tik duomenų centro prieigos leidimą. Leidimų naudojimas registruojamas. Įeinantys į patalpas ne IBM lankytojai registruojami ir lydimi visose patalpose. Pristatymo vietos, krovimo rampos ir kitos vietos, per kurias į patalpas gali patekti asmenys be leidimų, kontroliuojamos ir izoliuotos.

2.6 Atitikimas

IBM kasmet atestuoja privatumo praktikas, kad atitiktų JAV Prekybos departamento „Saugaus uosto“ programos principus dėl pranešimų, pasirinkimo, tolesnio perdavimo, prieigos ir tikslumo, saugos ir priežiūros bei reikalavimų vykdymo. IBM kasmet gamybos duomenų centruose atlieka standartines „SSAE 16“ audito (arba jį atitinkančias) procedūras. IBM peržiūri, ar su sauga ir privatumu susijusios veiklos atitinka IBM verslo reikalavimus. Siekdama laikytis informacijos saugos politikų, IBM reguliariai atlieka vertinimus ir auditus. IBM darbuotojai ir tiekėjų darbuotojai kasmet dalyvauja darbuotojų saugos mokymuose. Darbuotojams kasmet primenami jų darbo tikslai ir atsakomybė laikytis verslo etikos, konfidencialumo ir IBM saugos įsipareigojimų.

3. Teisių suteikimo ir sąskaitų išrašymo informacija

3.1 Mokesčio apskaičiavimas

„Cloud Service“ pateikiama pagal šią mokesčių apskaičiavimo metriką, kaip nurodyta Užsakymo dokumente:

- Taikomosios programos egzempliorius yra matavimo vienetas, kuriuo remiantis galima įsigyti „IBM SaaS“. Taikomosios programos egzemplioriaus teisės reikalingos kiekvienam prie „IBM SaaS“ prijungtam Taikomosios programos egzemplioriui. Jeigu Taikomojoje programoje yra keli komponentai ir kiekvienas iš jų skirtas kitam tikslui ir (arba) vartotojų bazei ir kiekvieną iš jų galima prijungti prie „IBM SaaS“ arba valdyti ją naudojant, kiekvienas toks komponentas laikomas atskira Taikomąja programa. Be to, Taikomosios programos tikrinimo, kūrimo, parengimo ir gamybos aplinkos laikomos atskirais Taikomosios programos egzemplioriais ir kiekvienai jų reikia turėti teises. Keli Taikomosios programos egzemplioriai vienoje aplinkoje laikomi atskirais Taikomosios programos egzemplioriais ir kiekvienam iš jų reikia turėti teises. Reikia įsigyti teises, pakankamas prie „IBM SaaS“ prijungtų Taikomosios programos egzempliorių skaičiui padengti matavimo laikotarpiu, nurodytu Kliento Teisių suteikimo dokumente (TSD) arba Operacijų dokumente.

3.2 Mokesčiai ir sąskaitų išrašymas

Mokėtina suma už „Cloud Service“ nurodoma Užsakymo dokumente.

3.3 Einamasis mokėjimas

Už einamojo mokėjimo parinktis sąskaitos pagal Operacijų dokumente nurodytą tarifą bus išrašomos kitą mėnesį po to, kai pasinaudojama paslauga.

4. Techninis palaikymas

„Cloud Service“ techninis palaikymas įtrauktas į prenumeratos laikotarpį.

Palaikymo tarnybos darbo valandos:

Informacijos apie darbo valandas, internetines pranešimo apie problemą sistemas ir kitas techninio palaikymo ryšio priemones bei procesus pateikta „IBM Software as a Service Support Handbook“ (IBM Programinės įrangos kaip paslaugos palaikymo vadove).

Palaikymas ne darbo valandomis:

Palaikymas ne darbo valandomis (ne įprastomis, anksčiau nurodytomis, darbo valandomis) teikiamas tik dėl 1 sudėtingumo lygio problemų darbo dienomis, savaitgaliais ir švenčių dienomis. Jei problema yra 1 sudėtingumo lygio, klientas privalo būti pasiekiamas visą parą (24X7), kad padėtų diagnozuoti problemas. Kitu atveju problemos sudėtingumo lygis bus sumažintas iki 2.

4.1 Pagalba forume

Visiems „Cloud Service“ klientams teikiama pagalba forume, kurį reguliariai stebi IBM palaikymo atstovai ir kūrėjai.

a. Užduokite klausimus:

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

b. Peržiūrėkite dabartinius įrašus:

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

4.2 Standartinis palaikymas

Standartinis palaikymas galimas laikotarpiu, kuriuo klientai turi sumokėti Einamojo mokėjimo mokesčius. Iš „Cloud Service“ klientai gali pateikti palaikymo kortelę arba atidaryti pagalbos pokalbio sesiją. Jei reikia daugiau informacijos apie palaikymo procedūras, peržiūrėkite IBM palaikymo žiniatinklio portalą https://support.ibmcloud.com arba „IBM SaaS“ programinės įrangos palaikymo vadovą http://www.ibm.com/software/support/acceleratedvalue/SaaS_Handbook_V18.pdf.

Sudėtingumo lygis	Sudėtingumo lygio apibrėžimas	atsakymo laiko tikslai	Atsakymo laiko aprėptis
1	**Kritinis poveikis verslui / neveikianti paslauga:** Neveikia svarbi verslo funkcija arba sugedusi svarbi sąsaja. Paprastai taikoma gamybos aplinkoje ir rodo negalėjimą pasiekti paslaugas, dėl kurio atsiranda rimtas poveikis operacijoms. Ši padėtis reikalauja neatidėliotino sprendimo.	Per 1 val.	27 x 7
2	**Pastebimas poveikis verslui:** itin apribotas paslaugų įmonės teikiamos paslaugos priemonių arba funkcijų naudojimas arba jūs galite nespėti atlikti darbo iki nustatyto termino.	Per 2 darbo valandas	Pir.–penkt. darbo valandomis
3	**Nedidelis poveikis verslui:** Nurodo naudojamą paslaugą arba funkciją be kritinio poveikio operacijoms.	Per 4 darbo valandas	Pir.–penkt. darbo valandomis
4	**Minimalus poveikis verslui:** Užklausa arba ne techninė užklausa	Per 1 darbo dieną	Pir.–penkt. darbo valandomis

5. „Saugaus uosto“ nuostatų laikymasis

IBM neapibrėžė šios „Cloud Service“ atitikties pagal JAV–ES ir JAV–Šveicarijos Saugaus uosto programų reikalavimus.

6. Papildoma informacija

„Cloud Service“ skirta įvairioms potencialioms saugos ir reikalavimų laikymosi problemoms identifikuoti mobiliesiems, skirtose taikomosiose programose ir žiniatinklio paslaugose. Programa netikrina visų pažeidžiamumų ar reikalavimų nesilaikymo atvejų, taip pat neveikia kaip saugos atakų užkarda. Saugos grėsmės, reglamentai ir standartai nuolat keičiasi, todėl į Paslaugą gali būti įtraukti ne visi tokie pakeitimai. Tik Klientas yra atsakingas už Kliento taikomosios programos mobiliesiems, sistemų ir darbuotojų, taip pat bet kokių taisomojo pobūdžio veiksmų saugą ir reikalavimų laikymąsi. Ar naudoti Paslaugos pateiktus duomenis, Klientas sprendžia tik savo nuožiūra.

6.1 Naudos gavimo vietos

Kai taikoma, mokesčiai yra pagrįsti vieta (-omis), kurią (-ias) jūs nurodote kaip gaunančią (-ias) naudą iš „Cloud Services“. IBM taikys mokesčius pagal „Cloud Service“ užsakymo metu nurodytą verslo adresą kaip pagrindinę naudos gavimo vietą, nebent IBM pateiksite papildomos informacijos. Jūs esate atsakingi už tokios informacijos atnaujinimą ir IBM informavimą apie visus pakeitimus.

6.2 Slapukai

Jūs žinote ir sutinkate, kad „Cloud Service“ naudojimo ir palaikymo tikslais, naudodama sekimo ir kitas technologijas, IBM gali iš jūsų (jūsų darbuotojų ir rangovų) rinkti su „Cloud Service“ naudojimu susijusią asmens informaciją. IBM renka naudojimo statistinius duomenis ir informaciją apie „Cloud Service“ efektyvumą, kad galėtų gerinti vartotojų patirtį ir (arba) pritaikyti bendravimą su jumis. Jūs patvirtinate, kad gausite arba jau esate gavę sutikimą leisti IBM apdoroti surinktą asmens informaciją anksčiau nurodytais tikslais, laikantis taikomų įstatymų, IBM, kitose IBM įmonėse ir jų subrangovų vietose, kur IBM ir mūsų subrangovai vykdo veiklą. IBM vykdys jūsų darbuotojų ir rangovų pageidavimus pasiekti, naujinti, taisyti arba panaikinti jų surinktą asmens informaciją.