

„IBM Application Security on Cloud“

Šiame Paslaugos apraše apibūdinta „Cloud Service“, kurią IBM pateikia Klientui. Klientas reiškia įmonę, jos įgaliotuosius vartotojus ir „Cloud Service“ gavėjus. Atitinkamas Pasiūlymas ir Teisių suteikimo dokumentas (TSD) pateikiami kaip atskiri Operacijų dokumentai.

1. „Cloud Service“

„IBM Application Security on Cloud“ suteikia vieną vietą, kuri padėtų Klientui nustatyti įvairių programų saugumo pažeidžiamumus (pvz., SQL įdėjimą, Scenarijų vykdymą keliose svetainėse ir Duomenų nutekėjimą). Ši paslauga apima įvairių tipų taikomųjų programų saugos žvalgyimo technikas, kurių kiekviena nustato tos taikomosios programos saugos problemas.

„IBM Application Security on Cloud“ teikia šias funkcines galimybes:

- Programų mobiliesiems žvalgyimą dėl saugos pažeidžiamumų. Tai atliekama naudojant interaktyviasias („glassbox“) saugos analizės technologijas.
- Gamybos ar priešgamybinių, viešų ar privačiojo tinklo Svetainių žvalgyimą dėl saugos pažeidžiamumų. Tai atliekama naudojant dinamines („blackbox“) saugos analizės technologijas.
- Duomenų srautų žiniatinklio ir kompiuterio taikomose programose žvalgyimą dėl saugos pažeidžiamumų. Tai atliekama naudojant statines („whitebox“) saugos analizės technologijas.
- Išsamias saugos pažeidžiamumų ataskaitas, apimančias aukšto lygio rezultatų suvestines ir taisymo veiksmus, kurių gali imtis kūrėjai.
- Integraciją su įvairiomis „DevOps“ platformomis.

1.1 „IBM Application Analyzer“

„IBM Application Analyzer“ galima užsisakyti Taikomosios programos egzemplioriui, Užduočiai (tikrinimui) arba kaip visą Egzempliorių ir atlikti toliau nurodytų tipų tikrinimus:

- „Dynamic Analyzer“ – tikrinti priešgamybines arba gamybos svetaines DAST metodais
- „Mobile Analyzer“ – tikrinti „iOS“ arba „Android“ dvejetainius IAST metodais
- „Static Analyzer“ – tikrinti baito arba šaltinio kodo duomenų srautą SAST metodais

1.2 Nustatymo paslauga

„IBM Application Security on Cloud Consulting Services“ – tai komerciniam naudojimui paruošta „Application Analyzer“ nustatymo paslauga. Paslauga apima IBM konsultantų teikiamas taikomosios programos rizikos tikrinimo ir tvarkymo rekomendacijas ir pagalbą. „IBM Application Security on Cloud Consulting Services“ įsigyjamoms kaip įsipareigojimų blokai, kuriuos galima išplėsti toliau nurodytomis apimtimis, kad būtų galima teikti užklausas ir naudotis toliau nurodytomis paslaugomis:

a. „Fast Start“ [naudojamas vienas (1) įsipareigojimo vienetas]

„Fast Start“ paslauga teikia „Application Security on Cloud“ tikrinimo ir rizikos valdymo funkcijų naudojimo žinias ir rekomendacijas. Kai Klientas patvirtina, kad sėkmingai prisijungė prie „Application Security on Cloud“ portalo, IBM surengs ne ilgesnę nei dviejų (2) valandų žiniatinklio konferenciją dviem (2) aktyviems dalyviams, kad išmokytų bazinių „AppSec“ konfigūracijų ir funkcijų „Cloud service“, įskaitant tikrinimo tipus, tikrinimų vykdymus, ataskaitų peržiūrą ir susijusių įrankių ir priedų diegimą. „Fast Start“ paslauga suteikiama užbaigus (a) kliento mokymo internetinį seminarą, (b) įdiegus atitinkamus įrankius ir priedus ir (c) padėjus Klientui nustatyti ir paleisti Kliento pirmąjį tikrinimą.

b. „Assessment Review“ [naudojami du (2) įsipareigojimo vienetai]

„Assessment Review“ paslauga padeda apžvelgti tikrinimo rezultatus, įskaitant supratimą ir taikomosios programos pažeidžiamumų šalinimo priemonių prioritetų nustatymą. IBM surengs ne ilgesnę nei vienos (1) valandos žiniatinklio konferenciją dviem (2) aktyviems dalyviams, kurio metu pateiks aptiktų pažeidžiamųjų ir taikomosios programos bendrosios saugos rizikos apžvalgą bei išsamiai aptars aptiktus taikomosios programos saugos pažeidžiamumus, įskaitant (1) tai, kaip pažeidžiamumas buvo tikrinamas, (2) kaip pažeidžiamumai buvo aptikti, (3) kokia kiekvieno pažeidžiamumo rizika, ir (4) pateiks bendrąsias taisymo rekomendacijas, kad padėtų pašalinti

pažeidžiamumą. Apžvalga bus pagrįsta išskirtinai tikrinimo rezultatais, šaltinio kodas nebus apžvelgiamas. Klientas peržiūrės tikrinimo rezultatus ir nustatys IBM peržiūrėti tikrinimo rezultatus prieš žiniatinklio konferenciją. „Assessment Review“ paslauga suteikiama užbaigus žiniatinklio konferenciją.

c. **„Scan for Me“** [naudojami keturi (4) įsipareigojimo vienetai]

„Scan for Me“ paslauga suteikia IBM taikomosios programos saugos specialistą, kuris konfigūruos ir vykdys tikrinimą, tikrins rezultatus ir parengs trumpą ataskaitą, kurioje apžvelgs tikrinimo duomenis. Klientas leis IBM konsultantui pasiekti „ASoC“ aplinką, kad galėtų konfigūruoti ir vykdyti tikrinimą, tikrinti rezultatus, teikti rekomendacijas dėl prioritetinių priemonių ir parengti trumpą ataskaitą, kurioje apžvelgtų tikrinimo duomenis. IBM surengs ne ilgesnę nei vienos (1) valandos žiniatinklio konferenciją dviem (2) aktyviems dalyviams, kurio metu pateiks aptiktų pažeidžiamųjų ir taikomosios programos bendrosios saugos rizikos apžvalgą bei išsamiai aptars aptiktus taikomosios programos saugos pažeidžiamumus, įskaitant (1) tai, kaip pažeidžiamumas buvo tikrinamas, (2) kaip pažeidžiamumai buvo aptikti, (3) kokia kiekvieno pažeidžiamumo rizika, ir (4) pateiks bendrąsias taisymo rekomendacijas, kad padėtų pašalinti pažeidžiamumą. Gavus prašymą ir ne vėliau nei per 30 dienų po pradinio tikrinimo IBM atliks pakartotinį tikrinimą, naudodama pradinę tikrinimo konfigūraciją, kad patikrintų tik saugos pataisymus, bet netikrins naujų funkcinių galimybių, netikrins rezultatų ir neteiks klientui ataskaitos. „Scan for Me“ paslauga suteikiama užbaigus žiniatinklio konferenciją, kurios metu apžvelgiami pradiniai tikrinimo rezultatai arba, jei taikoma, užbaigus pakartotinį tikrinimą, kurį atlikti paprašė Klientas, ir pateikus pakartotinio tikrinimo ataskaitą Klientui.

d. **„Advisor on Demand“** [naudojami septyni (7) įsipareigojimo vienetai]

„Advisor on Demand“ paslauga suteikia ne daugiau nei dvidešimt (20) valandų IBM konsultanto laiko, kurį galima naudoti su „Cloud Service“ susijusioms veikloms. IBM konsultantas padės specifiniais taikomosios programos saugos klausimais, įskaitant, bet neapsiribojant, programos valdymą, saugos tikrinimo prioritetų nustatymą, priemonių strategijas, šaltinio kodo analizę ir šaltinio kodo taisymą. IBM bendradarbiaus su Klientu, kad suprastų ir sukurtų projekto tvarkaraštį su konkrečiais Kliento reikalavimais, įskaitant projekto tikslus, atitinkamas technologijas, pageidaujamus terminus, tikėtinus rezultatus ir numatomą „Advisor on Demand“ paslaugos įsipareigojimų skaičių. Klientas privalo pateikti prieigą prie taikomųjų programų, sistemų ir dokumentacijos, reikalingų norint teikti paslaugas. „Advisor on Demand“ paslauga suteikiama, kai suteikiama ne daugiau nei 20 valandų konsultacijų saugos klausimais ir (arba) įvykdžius projekto tvarkaraštį ir (arba) pateikus projekto tvarkaraštyje dokumentuotus rezultatus Klientui.

e. **Taikomosios programos skverbties tikrinimas**

Trys parinktys:

- (1) **Atitiktis / bazinio lygmens taikomosios programos skverbties tikrinimas** apima ne daugiau nei (40) valandų Konsultanto laiko ir skirtas vieno veiksmo loginiams defektams bei ir įdėjimo defektų paprastesnėms versijoms. Naudojama penkiolika (15) įsipareigojimo vienetų.
- (2) **Standartinės taikomosios programos skverbties tikrinimas** apima ne daugiau nei šešiasdešimt (60) valandų Konsultanto laiko ir apima kelių veiksmų srautų loginius defektus, sudėtingas įdėjimo defektų versijas ir sudėtingų duomenų tipų analizę. Naudojamas dvidešimt vienas (21) įsipareigojimo vienetas.
- (3) **Išplėstinis taikomosios programos skverbties tikrinimas**
Ne daugiau nei aštuoniasdešimt (80) valandų Konsultanto laiko, apima kompiliuotų vykdomųjų elementų apgražos inžineriją, tinkintų tinklo protokolų analizę, viešai pasiekiamų bibliotekų ir struktūrų išsamią analizę. Naudojami dvidešimt septyni (27) įsipareigojimo vienetai.

Taikomosios programos skverbties tikrinimo paslauga suteikia IBM išteklius, skirtus taikomosios programos tikrinimui ir eksploatavimui, tikrinimo ataskaitos pateikimui ir trumpos ataskaitos, kurioje paaiškinami rezultatai ir susijusios rizikos, parengimui.

Dviem (2) aktyviems dalyviams IBM suteiks ne ilgesnį nei vienos (1) valandos projekto inicijavimo skambučių, skirtą Kliento aplinkos ir organizacijos apžvalgai, įskaitant taikomosios programos platformą, architektūrą, struktūras, palaikymo infrastruktūrą, žinomas saugos problemas arba problemas, susijusias su taikomąja programa, preliminariu tikrinimo tvarkaraščiu ir avarinio kontakto planu.

IBM atliks taikomosios programos skverbties tikrinimą, įskaitant, bet neapsiribojant: dažnai pasitaikančius pažeidžiamumus, pvz., SQL įdėjimo ir scenarijų vykdymo keliose svetainėse, esamų saugos valdiklių, pvz., įvesties tikrinimo, autentifikavimo ir autorizavimo, stipriųjų ir silpnųjų pusių įvertinimą, tinkamo verslo logikos realizavimo tikrinimą, tinkamo saugos protokolų naudojimo tikrinimą, seanso tvarkymo defektų identifikavimą ir prisijungimo, slaptažodžio atkūrimo, slaptažodžio politikos ir kitų vartotojo valdymo funkcijų tinkamų saugos valdiklių tikrinimą. Rezultatai bus dokumentuoti Taikomosios programos skverbties tikrinimo ataskaitoje. IBM parengs trumpą ataskaitą ir surengs ne ilgesnę nei vienos (1) valandos žiniatinklio konferenciją. Taikomosios programos skverbties tikrinimo paslauga suteikiama, kai išnaudojamas priskirtas konsultacijų laikas, surengiama žiniatinklio konferencija ir Klientui pateikiama galutinė Taikomosios programos skverbties tikrinimo ataskaita.

1.2.1 Nustatymo paslaugos įsipareigojimai

IBM:

- teikia Nustatymo paslaugas naudojant Kliento įsigytus įsipareigojimo vienetus Kliento užsakymo laikotarpiu; ir
- suteikia Nustatymo paslaugą, kai įvykdomi 1.2 skyriuje nurodyti užbaigimo kriterijai.

Klientas sutinka:

- prisiimti atsakomybę už visus mokesčius, susijusius su visomis įsipareigojimų užklausomis, kurias Klientas pateikia sutarties laikotarpiu;
- patvirtinti, kad įsigyti įsipareigojimų vienetai turi būti panaudoti per pradinį sutarties laikotarpį ir nustotos galioti, jeigu nebus panaudoti iki sutarties laikotarpio pabaigos datos; ir
- inicijuoti oficialią visų Nustatymo paslaugų užklausą mažiausiai 30 dienų prieš prenumeratos pabaigos datą.

Teikdama bet kurią Nustatymo paslaugą IBM gali pareikalauti iš Kliento informacijos ir pagrįstos pagalbos. Laiku negavus iš Kliento reikalaujamos informacijos arba pagalbos, už paslaugas gali būti taikomi IBM nustatyti įsipareigojimo vienetų mokesčiai arba sulaikytas atitinkamos paslaugos veikimas.

Tikrinimo laikotarpiu Klientas sutinka vykdyti aplinkos paruošimo ir palaikymo IBM instrukcijas, kad IBM galėtų tinkamai atlikti tikrinimą.

2. Saugos aprašas

Šiai „Cloud Service“ taikomi „IBM SaaS“ duomenų saugos ir privatumo principai, kurie pasiekiami <http://www.ibm.com/cloud/data-security>, ir visos kitos šiame skyriuje nurodytos papildomos sąlygos. Jokie IBM duomenų saugos ir privatumo principų pakeitimai nesumažins „Cloud Service“ saugos.

Ši „Cloud Service“ sukurta nesilaikantis specifinių tvarkomo turinio, pavyzdžiui, asmeninės informacijos arba slaptos asmeninės informacijos, saugos reikalavimų. Klientas yra atsakingas už nustatymą, ar ši „Cloud Service“ atitinka Kliento poreikius dėl to, kokio tipo turinį Klientas naudoja kartu su „Cloud Service“.

IBM nėra Federalinės ryšių komisijos (FCC) arba valstybinių reguliavimo institucijų („Valstybinis reguliuotojas“) reguliuojamų paslaugų teikėjas ir neketina teikti jokių FCC arba Valstybinio reguliuotojo reguliuojamų paslaugų. Jeigu FCC arba bet kuris Valstybinis reguliuotojas nustatys bet kokių IBM pagal šias sąlygas teikiamų paslaugų reguliavimo reikalavimus arba prievoles, IBM gali: (a) modifikuoti, keisti arba pakeisti produktus Kliento sąskaita ir (arba) (b) pakeisti tokių paslaugų teikimo būdą Klientui, kad išvengtų tokių reikalavimų ar prievolių taikymo IBM (pvz., veikti kaip Kliento agentas įsigyjant tokias paslaugas iš trečiosios šalies komunikacijos bendrovės).

3. Techninis palaikymas

Prenumeratos laikotarpiu ir po to, kai IBM praneša Klientui, kad suteikta prieiga prie „Cloud Service“, techninis palaikymas teikiamas internetiniuose forumuose ir kaip standartinis palaikymas laikotarpiu, kuriuo Klientas turi sumokėti mokesčius už naudojimą. Iš šio „Cloud Service“ Klientai gali pateikti palaikymo kortelę arba atidaryti pagalbos pokalbio sesiją. IBM pateiks „IBM Software as a Service Support Handbook“ (IBM Programinės įrangos kaip paslaugos palaikymo vadovą), kuriame nurodyta techninio palaikymo centro kontaktinė informacija, kita informacija ir procesai.

Sudėtingumo lygis	Sudėtingumo lygio apibrėžimas	Atsakymo laiko aprėptis	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.	24 x 7
2	Pastebimas poveikis verslui: Stipriai apribotas paslaugos verslo ypatybės arba funkcijos naudojimas arba Klientui atsiranda grėsmė pažeisti neveikiančio verslo galutinius terminus.	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

3.1 Prieiga prie Kliento duomenų

IBM galės pasiekti Kliento duomenis dėl paslaugos kylančių problemų diagnozavimo ir paslauga lengviau skenuos Kliento taikomąją programą. IBM pasieks duomenis tik klaidų taisymo arba IBM produktų ir paslaugų palaikymo teikimo tikslais.

4. Teisių suteikimo ir sąskaitų išrašymo informacija

4.1 Mokesčio apskaičiavimas

„Cloud Service“ pateikiama pagal mokesčių apskaitos metriką, nurodomą Operacijų dokumente:

- Darbas** – matavimo vienetas, kuriuo remiantis galima įsigyti „Cloud Service“. Darbas – tai Debesų kompiuterijos paslaugos objektas, kurio negalima smulkiau suskaidyti, reiškiantis skaičiavimo procesą, įskaitant visus jo antrinius procesus. Reikia įsigyti teises, kurių pakaktų bendram Darbų, apdorojamų ar valdomų naudojant Debesų kompiuterijos paslaugą, skaičiui matavimo laikotarpiu, nurodytu Kliento TSD arba Operacijų dokumente.
- Taikomosios programos egzempliorius** – tai matavimo vienetas, kuriuo remiantis galima įsigyti „Cloud Service“. Taikomosios programos egzemplioriaus teisės reikalingos kiekvienam prie „Cloud Service“ 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 „Cloud Service“ 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 „Cloud Service“ prijungtų Taikomosios programos egzempliorių skaičiui padengti matavimo laikotarpiu, nurodytu Kliento TSD arba Operacijų dokumente.

Šios „Cloud Service“ tikslais Taikomosios programos egzemplioriai yra iš eilės einantys atskiros taikomosios programos nuskaitymai, apibrėžti taip:

- Dinaminiam tikrinimui: svetainė pasiekama per viešuosius arba privačiuosius URL. Kiekvienas Egzempliorius suteikia teisę svetainei į 5 000 puslapių viename domene.
 - Statiniam tikrinimui: kodo, sukurto atskirai vykdymo aplinkai, vienetas. Kiekvienas Taikomosios programos egzempliorius suteikia kodo nuskaitymo vienetams teisę į 1 000 000 eilučių.
 - Mobiliajam tikrinimui: dvejetainio kodo vienetas, kurį galima vykdyti mobiliajame įrenginyje. Kiekviena atskira platforma mobiliesiems (pvz., „iOS“ ir „Android“) yra atskiras programos egzempliorius.
- Egzempliorius** – matavimo vienetas, kuriuo remiantis galima įsigyti „Cloud Service“. Egzempliorius yra prieiga prie konkrečios „Cloud Service“ konfigūracijos. Reikia įsigyti pakankamas teises, skirtas

kiekvienam „Cloud Service“ Egzemplioriui pasiekti ir naudoti matavimo laikotarpiu, nurodytu Kliento Teisių suteikimo dokumente (TSD) arba Operacijų dokumente.

Visų Egzempliorių teisės neriboja atliktų Darbų skaičiaus arba Taikomųjų programų egzempliorių (prijungtų Taikomųjų programų), jeigu bet kuriuo laiku vykdomų Darbų skaičius neviršys 30.

- d. **Įsipareigojimas** yra matavimo vienetas, pagal kurį galima gauti paslaugas. Įsipareigojimas apima specialistų ir (arba) mokymo paslaugas, susijusias su „Cloud Service“. Reikia įsigyti teises, kurių pakaktų kiekvienam Įsipareigojimui padengti.

4.2 Daliniai mėnesio mokesčiai

Dalinis mėnesio mokestis, kaip nurodyta Operacijų dokumente, gali būti nustatomas proporcingai.

4.3 Mokesčiai už perviršį

Jei faktinis „Cloud Service“ naudojimas matavimo laikotarpiu viršys TSD nurodytas teises, Klientas bus apmokestintas už perviršį, nustatytą pagal Operacijų dokumentą.

4.4 Nustatymo mokesčiai

Klientui bus taikomas mokestis už nustatymą, kaip nurodyta Operacijų dokumente.

5. Terminas ir atnaujinimo galimybės

„Cloud Service“ naudojimo terminas prasideda nuo dienos, kai IBM praneša Klientui, kad jis turi prieigą prie „Cloud Service“, kaip aprašyta TSD. TSD bus nurodyta, ar „Cloud Service“ bus atnaujinama automatiškai, naudojama nepertraukiamo naudojimo pagrindu ar nutraukiama laikotarpio pabaigoje.

Taikant automatinį atnaujinimą, jei Klientas mažiausiai prieš 30 dienų iki termino galiojimo pabaigos nepateikė prašymo raštu nebeatnaujinti, „Cloud Service“ bus automatiškai atnaujinta TSD nurodytam laikotarpiui.

Naudojant nuolat, „Cloud Service“ pasiekiamumas pratęsiamas kiekvieną mėnesį, kol Klientas prieš 30 dienų iki nutraukimo raštu pateiks prašymą nutraukti. Praėjus šiam 30 dienų laikotarpiui, „Cloud Service“ bus pasiekama iki kalendorinio mėnesio pabaigos.

6. Papildomos sąlygos

Saugos tikrinimai negali identifikuoti visų saugos rizikų taikomojoje programoje ir jie nėra skirti naudoti pavojingose aplinkose, kuriose būtinas veikimas be trikčių, įskaitant, be apribojimų, orlaivių navigacijos, oro eismo kontrolės sistemas, ginkluotės sistemas, gyvybės palaikymo sistemas, branduolinius objektus, arba bet kokias kitose taikymo aplinkose, kuriose, nepavykus identifikuoti saugos rizikų, galimos asmenų mirtys, sužeidimai ar žala nuosavybei. Neteikiama garantija, kad saugos tikrinimai veiks be trikčių ar be klaidų.

„Cloud Service“ galima naudoti kaip pagalbinę priemonę Klientui siekiant laikytis suderinamumo įsipareigojimų, kurie gali būti pagrįsti įstatymais, taisyklėmis, standartais ar praktikomis. Bet kokios „Cloud Service“ pateikiamos instrukcijos, siūlomas naudojimas ar patarimai nėra teisinė, apskaitos arba kitoks profesionalo patarimas, todėl Klientas įspėjamas konsultuotis su teisininku arba kitais ekspertais. Klientas išskirtinai atsakingas už tai, kad būtų užtikrintas Kliento ir Kliento veiklų, taikomųjų programų bei sistemų suderinamumas su visais taikomais įstatymais, taisyklėmis, standartais ir praktikomis. Šio „Cloud Service“ naudojimas negarantuoja suderinamumo su įstatymu, taisykle, standartu ar praktika.

„Cloud Service“ atlieka invazinius ir neinvazinius svetainės ir žiniatinklio arba taikomosios programos mobiliesiems, kurias Klientas pasirenka nuskaityti, patikrinimus. Tam tikri įstatymai draudžia be leidimo bandyti įsiskverbti į kompiuterių sistemas ar naudotis šių sistemų prieiga. Klientas įgalioja IBM teikti paslaugas, kaip aprašyta šiose sąlygose, ir patvirtina, kad Paslaugos apima įgaliojimą prieigą prie Kliento kompiuterinių sistemų. IBM gali atskleisti šį įgaliojimo suteikimą trečiajai šaliai, jei tai bus būtina teikiant Paslaugas.

Patikrinimas susijęs su tam tikra rizika, įskaitant, be apribojimų, toliau nurodytą riziką:

- a. Kliento kompiuterių sistemos, vykdydamos tikrinamas taikomas programas, gali užstrigti ir laikinai tapti nepasiekiamos arba gali būti prarasti duomenys;
- b. patikrinimo metu gali laikinai sumažėti Kliento sistemų ir susijusių maršruto parinktų bei ugniasienių efektyvumas ir našumas;
- c. gali būti sugeneruotas didelis žurnalo pranešimų kiekis, dėl to žurnalo failas gali užimti per daug disko vietos;

- d. dėl bandymo pažeidžiamumų gali būti pakeisti arba panaikinti duomenys;
- e. įsibrovimų aptikimo sistemos gali siųsti įspėjimus;
- f. tikrinamos žiniatinklio taikomosios programos el. pašto funkcija gali siųsti el. laiškus; ir
- g. „Cloud Service“, ieškodama įvykių, gali sukelti stebimo tinklo srauto trikdžių.

Atliekant bet kokius tikrinimo veiksmus, visų paslaugos lygio sutarties teisių arba priemonių, teikiamų IBM arba susijusių su tikrinamomis svetainėmis ar taikomosiomis programomis, atsisakoma.

Jeigu Klientui „Cloud Service“ reikia įvesti autentifikuotus prisijungimo prie bandomos taikomosios programos kredencialus, Klientas turėtų įvesti tik bandomųjų paskyrų, o ne gamybos vartotojų kredencialus. Naudojant gamybos vartotojų kredencialus per „Cloud Service“ gali būti perduoti asmens duomenys.

„Cloud Service“ galima konfigūruoti žvalgyti gamybos žiniatinklio taikomąsias programas. Kai Klientas nustato nuskaitymo tipą kaip „gamybos“, ši paslauga yra skirta atlikti nuskaitymą tokiu būdu, kad sumažėtų anksčiau išvardyta rizika; tačiau tam tikrose situacijose „Cloud Service“ gali pabloginti našumą arba sukelti nestabilumą tikrinamose gamybos vietose ir infrastruktūroje. IBM neteikia jokių garantijų ar pareiškimų dėl „Cloud Service“ tinkamumo gamybos vietoms nuskaityti.

KLIENTAS YRA ATSAKINGAS UŽ NUSTATYMĄ, AR „CLOUD SERVICE“ YRA TINKAMA ARBA SAUGI KLIENTO ŽINIATINKLIO SVETAINEI, ŽINIATINKLIO TAIKOMAJAI PROGRAMAI, TAIKOMAJAI PROGRAMAI MOBILIESIEMS ARBA TECHNINEI APLINKAI.

„Cloud Service“ skirta įvairioms potencialioms saugos ir reikalavimų laikymosi problemoms identifikuoti mobiliojo įrenginio ir žiniatinklio taikomosiuose 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 „Cloud Service“ gali būti įtraukti ne visi tokie pakeitimai. Tik Klientas yra atsakingas už Kliento žiniatinklio taikomosios programos, sistemų ir darbuotojų, taip pat bet kokių korekcinių veiksmų saugą ir reikalavimų laikymąsi. Ar naudoti „Cloud Service“ pateiktus duomenis, Klientas sprendžia tik savo nuožiūra.

Tam tikri įstatymai draudžia be leidimo bandyti įsiskverbti į kompiuterių sistemas ar naudotis šių sistemų prieiga. **KLIENTAS YRA ATSAKINGAS UŽ UŽTIKRINIMĄ, KAD KLIENTAS NENAUDOS „CLOUD SERVICE“ BET KOKIŲ ŽINIATINKLIO SVETAINIŲ IR (ARBA) TAIKOMŲJŲ PROGRAMŲ SKENAVIMUI, IŠSKYRUS KLIENTUI PRIKLAUSANČIAS ŽINIATINKLIO SVETAINES IR (ARBA) TAIKOMĄSIAS PROGRAMAS, TAIP PAT ŽINIATINKLIO SVETAINES IR (ARBA) TAIKOMĄSIAS PROGRAMAS, KURIAS SKENUOTI KLIENTUI SUTEIKTAS ĮGALIOJIMAS IR TEISĖ.**

Kad būtų aiškiau, laikoma, kad Kliento turinys, aprašytas dalies „Cloud Service“ Sutarties duomenų apsaugos skyriuje, taip pat apima duomenis, kuriuos IBM gali pasiekti Taikomosios programos skverbties tikrinimo metu.

6.1 Trečiajai šaliai priklausančios sistemos

Dėl trečiajai šaliai priklausančių sistemų (kurios šiose nuostatose apima, neapsiribojant, taikomąsias programas ir IP adresus), kurios bus tikrinamos, kaip aprašyta toliau, Klientas sutinka:

- a. kad prieš IBM inicijuojant trečiosios šalies sistemos tikrinimą, Klientas gaus kiekvienos sistemos savininko pasirašytą raštą, įgaliojantį IBM teikti Paslaugas toje sistemoje ir rodantį savininko sutikimą su toliau esančiame skyriuje „Permission to Perform Testing“ („Leidimas atlikti tikrinimą“) nurodytomis sąlygomis, ir pateiks IBM tokio įgaliojimo kopiją;
- b. prisiimti visą atsakomybę dėl sistemos savininko informavimo apie visas IBM nuotolinio tikrinimo metu šiose sistemose identifikuotas rizikas, pavojingas padėtis ir pažeidžiamumus; ir
- c. organizuoti ir palengvinti sistemos savininko ir IBM apsikeitimą informacija, jei, IBM nuomone, tai bus būtina.

Klientas sutinka:

- nedelsdamas informuoti IBM, jei pasikeistų kurios nors čia sistemos, tikrinamos pagal šias sąlygas, savininkas;
- be išankstinio IBM raštiško sutikimo neatskleisti pateikiamų elementų arba fakto, kad IBM teikė Paslaugas, už Kliento įmonės; ir
- visiškai atlyginti IBM bet kokią žalą arba įsiskolinimą, kurį IBM patirs dėl trečiosios šalies pretenzijų, atsiradusių Klientui nesilaikant šiame skyriuje „Trečiajai šaliai priklausančios sistemos“ nurodytų

reikalavimų ir dėl bet kokių trečiosios šalies šaukimų į teismą ar pretenzijų, pateiktų IBM arba IBM rangovams ar agentams, atsiradusių dėl (a) sistemų, kurios tikrinamos pagal šias sąlygas, saugos rizikų, pavojingų padėčių ar pažeidžiamumų tikrinimo, (b) tokio tikrinimo rezultatų pateikimo Klientui arba (c) tokių rezultatų Kliento naudojimo ar atskleidimo.

6.2 Slapukai

Klientas žino ir sutinka, kad „Cloud Service“ naudojimo ir palaikymo tikslais, naudodama sekimo ir kitas technologijas, IBM gali iš Kliento (jo 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 Klientu. Klientas patvirtina, kad gaus arba jau yra gavęs sutikimą leisti IBM tvarkyti surinktą asmens informaciją anksčiau nurodytais tikslais, laikantis taikomos teisės, IBM, kitose IBM įmonėse ir jų subrangovų vietose, kur IBM ir mūsų subrangovai vykdo veiklą. IBM vykdys Kliento darbuotojų ir rangovų pageidavimus pasiekti, naujinti, taisyti arba panaikinti jų surinktą asmens informaciją.

Kartu su „Cloud Service“ paslaugomis, kurios apima ataskaitų teikimą, IBM parengs ir tvarkys iš „Cloud Service“ surinktą informaciją, iš kurios buvo pašalinti identifikavimo duomenys ir (arba) kuri buvo sukaupta vienoje vietoje („Saugos duomenys“). Saugos duomenys neidentifikuos Kliento ar asmens, išskyrus atvejus, nurodytus toliau esančiame d punkte. Be to, Klientas sutinka, kad IBM gali naudoti ir (arba) kopijuoti Saugos duomenis tik šiais tikslais:

- a. publikuojant ir (arba) platinant Saugos duomenis (pvz., su kibernetine sauga susijusiuose rinkiniuose ir (arba) analizėse);
- b. kuriant arba tobulinant produktus ar paslaugas;
- c. atliekant vidinį arba trečiųjų šalių tyrimą ir
- d. teisėtai bendrinant trečiųjų šalių patvirtintą informaciją apie nusikaltėlius.

6.3 Įgalinimo programinė įranga

Ši „Cloud Service“ apima įgalinimo programinę įrangą, kurią galima naudoti tik kartu su Kliento naudojama „Cloud Service“ ir tik „Cloud Service“ naudojimo laikotarpiu.