„IBM Resilient Incident Response Platform 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 Resilient Incident Response Platform on Cloud“ suteikia dinaminių veiksmų planus (nuo kenkėjiškos programinės įrangos ir „DDoS“ iki prarastų įrenginių) ir geriausią bendro reagavimo į incidentus praktiką. Kliento komanda naudoja šią žinių bazę reaguodama į incidentus ir ji gali būti sukonfigūruota Kliento unikaliose darbo procedūrose.

Reagavimo į incidentus komandos gali valdyti ir bendradarbiauti reaguodamos tiesiogiai „IBM Resilient Incident Response Platform on Cloud“. Priešingai nei naudojant kortelių sistemas ar kitus bendrojo pobūdžio IT įrankius, „IBM Resilient Incident Response Platform“ yra visiškai sukonfigūruota ir sukurta reaguoti į incidentus. Išsami analizė, tinkinami stebėjimo skydai ir patikimos ataskaitų funkcijos leidžia vyresniesiems vadovams pateikti svarbiausią informaciją.

„IBM Resilient Incident Response Platform“ sukurta įvairaus dydžio ir sudėtingumo organizacijoms ir yra galimos kelios, atskirai užsakomos versijos:

1.1 „IBM Resilient Incident Response Platform Enterprise on Cloud“

„IBM Resilient Incident Response Platform Enterprise on Cloud“ yra „Cloud Service“ sprendimas, sukurtas didžiųjų įmonių didelės ir įvairioms sistemoms. Jis siūlo pagrindą, skirtą organizacijų reagavimui planuoti, valdyti ir incidentų tipams mažinti. Vartotojai gali sukirti reagavimo planus pagal pramonės šakos standartus ir geriausias praktikas bei stebėti incidentus iki sprendimo. „Cloud Service“ padeda koncentruoti bendradarbiavimą visoje organizacijoje, leidžia įvairiems dalyviams imtis savo vaidmens ir užduočių, kaip reagavimo į incidentą darbo dalį. Taip pat galima atlikti incidentų modeliavimus, padedančius komandoms testuoti reagavimo planus, identifikuoti spragas ir patikslinti reagavimo procesus. Įdėtieji integravimai su įvairių išorinių grėsmių informacijos santraukomis automatizuoja incidentų ir artefaktų patobulinimus. „Cloud Service“ sudaro visuotinių duomenų privatumo pažeidimo pranešimo nuostatų žinių bazė, kuri padeda pagerinti reagavimo į incidentus planus. Duomenis galima sintetinti iš esamų saugos ir IT sistemų siekiant pateikti informaciją beveik realiuoju laiku. „Cloud Service“ galima automatizuoti, racionalizuoti ar tiksliai suderinti įvairias užduotis, taigi nereikia vykdyti pasirinktinio kūrimo. Klientas turi įsigyti bent 1 šios paslaugos Egzemplioriaus teises ir 1 Įgaliotojo vartotojo teises.

1.2 „IBM Resilient Incident Response Platform Standard on Cloud“

„IBM Resilient Incident Response Platform Standard on Cloud“ yra „Cloud Service“ sprendimas, sukurtas vidutinių ir mažų įmonių reagavimo į įvykius poreikiams patenkinti. Jis siūlo daugelį tų pačių funkcijų, kaip „IBM Resilient Incident Response Platform Enterprise on Cloud“, išskyrus šias funkcijas, kurių Klientui neleidžiama naudoti: privatumo pažeidimo nuostatos, automatizavimas / suderinimas, žinių apie grėsmes sklaidos kanalai, pasirinktiniai grėsmių sklaidos kanalai ir LDAP integracija. Klientas turi įsigyti bent 1 šios paslaugos Egzemplioriaus teises ir 1 Įgaliotojo vartotojo teises.

1.3 Pasirinktinės paslaugos

1.3.1 „IBM Resilient Incident Response Platform Enterprise for Non-Production Environment on Cloud“

„IBM Resilient Incident Response Platform Enterprise for Non-Production Environment on Cloud“ yra atskiras IBM Resilient Incident Response Platform“ egzempliorius, kurį Klientas gali naudoti tik ne gamybos vidiniams veiksmams atlikti, įskaitant, bet neapsiribojant, tikrinimą, veikimo reguliavimą, trikčių diagnozavimą, vidinį kontrolinį testą, parengimo kokybės užtikrinimo veiksmus ir (arba) viduje naudojamų „Cloud Service“ priedų ar plėtinių kūrimą, naudojant paskelbtas taikomųjų programų programavimo sąsajas.

1.4 Nuotolinės paslaugos

Toliau nurodytos Nuotolinės paslaugos yra užsakomos atskirai ir kiekvienos iš jų galiojimas baigiasi po devyniasdešimties (90) dienų nuo pardavimo, nepaisant to, ar buvo išnaudotos visos valandos (jei taikoma):

1.4.1 „IBM Resilient Incident Response Platform Integration for Cloud“

Šis pasiūlymas suteikia integracijos paslaugas, sujungiančias „Cloud Service“ su susijusiomis saugos ir valdymo sistemomis naudojant iš anksto sukurtą integraciją. Vienam Įsipareigojimui bus nustatyta tik viena integracija su viena sistema. Toliau pateiktos šios Nuotolinės paslaugos galimos nustatyti integracijos:

- **Integravimas su „QRadar“**

  Ši integracija įgalins „QRadar“ automatiniu arba neautomatiniu būdu pateikti pažeidimus į „Cloud Service“ kaip naujus incidentus. Tai apima dvikryptį pastabų, uždarymo įvykių ir naujų pažeidimų duomenų sinchronizavimą.

- **Integravimas su „HP Arcsight“**

  Ši integracija leis „ArcSight“ vartotojams neautomatiniu arba automatiniu būdu pateikti „Arcsight“ įvykių informaciją į „Cloud Service“ kaip naujus incidentus arba į esamus incidentus įtraukti artefaktų.

- **Integravimas su „Splunk“**

  Ši integracija leis „Splunk“ automatiškai pateikti įspėjimus „Cloud Service“ kaip incidentus. Klientas taip pat gali „Splunk“ užklausas vykdyti tiesiogiai iš „Cloud Service“ žiniatinklio sąsajos.

- **Integravimas su „ServiceNow“**

  Ši integracija leis „ServiceNow“ vartotojams kurti incidentus „Cloud Service“, o „Cloud Service“ vartotojams kurti kvitus „ServiceNow“. Kvitų ar incidentų naujinimai taip pat replikuojami tarp sistemų.

- **Integravimas su JIRA**

  Ši integracija leis JIRA vartotojams kurti incidentus „Cloud Service“, pagrįstus JIRA kvitais, o „Cloud Service“ vartotojams kurti kvitus JIRA. Kvitų ar incidentų naujinimai taip pat replikuojami tarp sistemų.

1.4.2 „IBM Resilient Incident Response Platform Design Session for Cloud“

Ši paslauga suteikia konsultacinį įsipareigojimą padėti Klientui optimizuoti „Cloud Service“ egzempliorių. IBM konsultantai dirba su Klientu, kad sujungtų ne daugiau kaip trijų (3) skirtingų tipų reagavimo į incidentus procesus, juos ištobulintų pagal tuo metu geriausias pramonės šakos praktikas ir „Cloud Service“ funkcijas ir patartų Klientui, kaip konfigūruoti „Cloud Service“ norint šiuos procesus įgyvendinti.

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 pricipų pakeitimai nesumažins „Cloud Service“ saugos.

Ši „Cloud Service“ sukurta nesilaikantis specifinių tvarkomo turinio, pavyzdžiui, asmeninės informacijos arba slaptos asmeninės informacijos, saugos reikalavimų. Kliento atsakomybė yra nustatyti, ar ši „Cloud Service“ atitinka Kliento poreikius atsižvelgiant į tai, kokio tipo turinį Klientas naudoja kartu su „Cloud Service“.

3. Paslaugos lygio sutartis

IBM užtikrina toliau nurodytus „Cloud Service“ pasiekiamumo paslaugos lygio sutarties (PLS) įsipareigojimus, kaip nurodyta TSD. PLS neteikia garantijų. PLS yra pasiekiama Klientui ir yra skirta naudoti tik gamybos aplinkose.

3.1 Pasiekiamumo kreditai

Sužinojęs, kad įvykis paveikė „Cloud Service“ pasiekiamumą, Klientas turi per 24 valandas IBM techninio palaikymo centre užregistruoti 1 sudėtingumo lygio palaikymo kortelę. Klientas turi, kiek gali, padėti IBM diagnozuoti problemą ir ją išspręsti.

Palaikymo kortelės pretenzija dėl PLS sąlygų nesilaikymo turi būti pateikta per tris darbo dienas nuo sutartinio mėnesio pabaigos. Kompensacija už pagrįstą PLS pretenziją bus suteikta kaip kreditas būsimoje „Cloud Service“ sąskaitoje faktūroje, atsižvelgiant į laikotarpį, per kurį „Cloud Service“ gamybos sistema buvo nepasiekiama („Prastova“). Prastova skaičiuojama nuo tada, kai Klientas praneša apie įvykį, iki tada, kai „Cloud Service“ atkuriama. Ji neapima laiko, susijusio su paslaugos teikimo nutraukimu dėl suplanuotos arba informuotos techninės priežiūros, dėl nuo IBM nepriklausančių priežasčių,

problemų, susijusių su Kliento ar trečiosios šalies turiniu, technologijomis, dizainu ar instrukcijomis, nepalaikomų sistemų konfigūracijų ir platformų ar kitų Kliento klaidų arba Kliento sukeltų saugos problemų ar Kliento saugos tikrinimo. IBM taikys aukščiausią galimą kompensaciją, pagrįstą kiekvieno sutartinio mėnesio „Cloud Service“ kaupiamuoju pasiekiamumu, kaip nurodyta toliau esančioje lentelėje. Bendra kompensacijos suma, atsižvelgiant į bet kurį sutartinį mėnesį, negali neviršyti 10 procentų vienos dvyliktosios (1/12) metinio mokesčio už „Cloud Service“ dalies.

3.2 Paslaugų lygiai

„Cloud Service“ pasiekiamumas per sutartinį mėnesį

Pasiekiamumas per sutartinį mėnesį	**Kompensacija (% mėnesinio prenumeratos mokesčio* už „Audio Conferencing for Connections Meetings“ sutartinį mėnesį, kuris yra pretenzijos dalykas)**
99,5 %	2 %
98 %	5 %
96 %	10 %

* Jei „Cloud Service“ buvo įsigyta iš IBM verslo partnerio, mėnesio prenumeratos mokestis bus apskaičiuojamas, atsižvelgiant į tuo metu galiojančiame kainoraštyje nurodytą „Cloud Service“ kainą, kuri galioja pretenzijoje nurodytą sutartinį mėnesį, pritaikant 50 % nuolaidą. IBM suteiks nuolaidą Klientui tiesiogiai.

Pasiekiamumas, išreikštas procentine išraiška, apskaičiuojamas iš bendro minučių skaičiaus sutartinį mėnesį atėmus bendrą Prastovų minučių skaičių sutartinį mėnesį, gautą rezultatą padalijus iš bendro minučių skaičiaus sutartinį mėnesį.

Pavyzdžiui, sutartinį mėnesį iš viso buvo 500 Prastovos min.

Iš viso sutartinį mėnesį, kurį sudarė 30 dienų, buvo 43 200 min. - 500 min. Prastovų = 42 700 min. _____ Iš viso 43 200 minučių	= 2 % Pasiekiamumo kredito už 98,8 % pasiekiamumo per sutartinį mėnesį

4. Techninis palaikymas

„Cloud Service“ techninis palaikymas teikiamas el. paštu, internetiniuose forumuose ir internetinėje pranešimo apie problemas sistemoje. Techninis palaikymas įtrauktas į „Cloud Service“ ir kaip atskiras pasiūlymas neteikiamas. Techninis palaikymas teikiamas įprastomis darbo valandomis 9–18 val. Rytų laiko juostos laiku, išskyrus švenčių dienas.

Sudėtingumo lygis	**Sudėtingumo lygio apibrėžimas**	**Atsakymo laiko tikslai palaikymo valandomis**
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.
2	**Pastebimas poveikis verslui:** Itin apribotas paslaugos priemonės arba funkcijos naudojimas arba Klientas gali nespėti atlikti darbo iki nustatyto termino.	Per 2 darbo valandas
3	**Nedidelis poveikis verslui:** Nurodo, kad paslaugą ar funkciją galima naudoti ir nėra kritinio poveikio operacijoms.	Per 4 darbo valandas

Sudėtingumo lygis	Sudėtingumo lygio apibrėžimas	Atsakymo laiko tikslai palaikymo valandomis
4	**Minimalus poveikis verslui:** Užklausa arba ne techninio pobūdžio užklausa.	Per 1 darbo dieną

5. Teisių suteikimo ir sąskaitų išrašymo informacija

5.1 Mokesčio apskaičiavimas

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

a. **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 TSD arba Operacijų dokumente.

b. **Įgaliotasis vartotojas** – matavimo vienetas, kuriuo remiantis galima įsigyti „Cloud Service“. Klientas privalo įsigyti atskiras, priskirtas kiekvienam unikaliam Įgaliotajam vartotojui, suteiktos prieigos prie „Cloud Service“ teises. Prieiga gali būti suteikta bet kokiu tiesioginiu arba netiesioginiu būdu (pavyzdžiui, naudojant tankinimo programą, įrangą arba taikomųjų programų serverį) ir bet kokiomis priemonėmis. Reikia įsigyti teises, pakankamas Įgaliotųjų vartotojų, kuriems suteikta prieiga prie „Cloud Service“, skaičiui padengti matavimo laikotarpiu, nurodytu Kliento TSD arba Operacijų dokumente.

c. **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.

5.2 Mokesčiai už perviršį

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

5.3 Nuotolinių paslaugų mokesčiai

Nuotolinės paslaugos įsigyjamos pagal Įsipareigojimo metriką, o sąskaitos bus išrašomos užsakymo metu pagal Operacijų dokumente nurodytą įkainį.

6. 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 90 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 90 dienų iki nutraukimo raštu pateiks prašymą nutraukti. Praėjus 90 dienų laikotarpiui, „Cloud Service“ bus pasiekiama iki kalendorinio mėnesio pabaigos.

7. Papildomos sąlygos

7.1 Bendrosios nuostatos

Klientas sutinka, kad spaudoje ar rinkodaros informacijoje IBM gali Klientą viešai vadinti „Cloud Services“ prenumeratoriumi.

7.2 Suderinamumo valdymo „Cloud Service“

„Cloud Service“ galima naudoti kaip pagalbinę priemonę Klientui siekiant laikytis suderinamumo įsipareigojimų, kurie gali būti pagrįsti įstatymais, taisyklėmis, standartais ar praktikomis. Klientas pripažįsta ir sutinka, kad bet kokios „Cloud Service“ pateikiamos instrukcijos, siūlomas pritaikymas ar patarimai nėra teisiniai, apskaitos arba kitokio pobūdžio profesionalūs patarimai, todėl Klientas įspėjamas konsultuotis su teisininku, finansininku arba kitais specialistais. Klientas sutinka, kad yra išskirtinai

atsakingas, kad būtų užtikrintas Kliento ir Kliento veiklų, taikomųjų programų bei sistemų suderinamumas su visais taikomais įstatymais, taisyklėmis, standartais ir praktikomis. „Cloud Service“ naudojimas negarantuoja suderinamumo su įstatymu, taisykle, standartu ar praktika.

7.3 Teisėtas „Cloud Service“ naudojimas

„Cloud Service“ padeda Klientui patobulinti saugos aplinką ir duomenis. Naudojant „Cloud Service“, gali būti taikomi įvairūs teisės aktai ir taisyklės, įskaitant susijusias su privatumu, duomenų apsauga, darbo santykiais ir elektroniniais ryšiais bei saugyklomis. „Cloud Service“ galima naudoti tik teisėtais tikslais ir teisėtu būdu. Klientas sutinka naudoti „Cloud Service“ laikydamasis taikomų teisės aktų, taisyklių ir politikos nuostatų ir prisiima už tai visą atsakomybę. Klientas pareiškia, kad gaus arba gavo visus teisėtam „Cloud Service“ naudojimui reikalingus sutikimus, leidimus arba licencijas.

7.4 Saugos duomenys

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.

7.5 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 asmeninę informaciją.