„IBM Financial Crimes Insight“

Šiame paslaugos apraše aprašoma „Cloud Service“. Taikomuose užsakymo dokumentuose pateikiama išsami informacija apie kainą ir papildoma informacija apie Kliento užsakymą.

1. „Cloud Service“

1.1 Pasiūlymai

Klientas gali rinktis iš toliau nurodytų galimų pasiūlymų.

1.1.1 „IBM Financial Crimes Insight“

Ši „Cloud Service“ pateikia bendrą infrastruktūrą ir bendrą paslaugų rinkinį, kuriuo naudojantis kuriami „Financial Crimes Insights“ pasiūlymai. „IBM Financial Crimes Insight“ teikia reikiamą integravimą tarp pasiūlymų, leidžiančių klientams pasinaudoti integruotų finansinių nusikaltimų pasiūlymų rinkinio teikiamu pranašumu.

„IBM Financial Crimes Insight“ yra būtinasis komponentas, teikiantis „Cloud Service“ egzempliorių.

1.1.2 „IBM Financial Crimes Insight Non-Production“

Ši „Cloud Service“ leidžia Klientui pasiekti „IBM Financial Crimes Insight Non-Production“ funkciją kaip debesies pasiūlymą.

1.1.3 „IBM Financial Crimes Insight BYOL“

Ši „Cloud Service“ leidžia Klientui pasiekti „IBM Financial Crimes Insight“ funkciją kaip debesies pasiūlymą. Norėdamas pasinaudoti „Bring your own licenses“ (BYOL) pasiūlymais, Klientas turi būti anksčiau įsigijęs atitinkamas susijusios IBM Programos licencijos teises. IBM Programa, reikalinga šiam „IBM Financial Crimes Insight BYOL“ pasiūlymui, yra „IBM Cloud Pak for Data Financial Crimes Insight“.

1.1.4 „IBM Financial Crimes Insight Non-Production BYOL“

Ši „Cloud Service“ leidžia Klientui pasiekti „IBM Financial Crimes Insight Non-Production“ funkciją kaip debesies pasiūlymą. Norėdamas pasinaudoti „Bring your own licenses“ (BYOL) pasiūlymais, Klientas turi būti anksčiau įsigijęs atitinkamas susijusios IBM Programos licencijos teises. IBM Programa, reikalinga šiam „IBM Financial Crimes Insight Non-Production BYOL“ pasiūlymui, yra „IBM Cloud Pak for Data Financial Crimes Insight for Non-Production Environment“.

1.1.5 „IBM Financial Crimes Insight for Entity Research Negative News API“

Šios „Cloud Service“ naudojamos kognityvinės kompiuterinės technologijos ir pažangi analizė padeda ieškoti nestruktūrinių naujienų ir medijos, analizuoti ir suskirstyti jas pagal prioritetus siekiant atskleisti galimą subjekto finansinio nusikaltimo riziką išvedant išfiltruotų ir surūšiuotų straipsnių sąrašą. Pasiūlymas organizacijoms teikiamas kaip API, kurią galima iškviesti arba įtraukti į darbo eigas ir procesus.

1.1.6 „IBM Financial Crimes Insight for Entity Research Enrichment API“

Ši „Cloud Service“ naudoja kognityvines kompiuterines technologijas duomenims iš struktūrinių šaltinių agreguoti, kas padeda organizacijoms suprasti daugiau apie subjektą, užtikrinant subjekto arba kliento įrašų atnaujinimą ir atskleidžiant galimą subjekto finansinio nusikaltimo riziką. Subjektai galėtų apimti klientus, sutarties šalis ir tiekėjus. Pasiūlymas organizacijoms teikiamas kaip API, kurią galima iškviesti arba įtraukti į darbo eigas ir procesus.

1.2 Pasirinktinės paslaugos

Kartu su „IBM Financial Crimes Insight“ arba „IBM Financial Crimes Insight Non-Production“ prenumerata Klientai taip pat turi prenumeruoti vieną iš šių „Cloud Service“ paslaugų:

1.2.1 „IBM Financial Crimes Insight for Anti-Money Laundering“

„IBM Financial Crimes Insight for Anti-Money Laundering“ („FCI for AML“) taikomi pažangios analizės lygiai siekiant stebėti finansinę veiklą ir padėti Klientui nustatyti subjektų polinkį plauti pinigus. Naudodama demografinius, elgsenos ir ryšių duomenis „FCI for AML“ padeda klientui vykdyti žinomų

rizikų peržiūros procesą ir taip pat gali padidinti rizikos draudimą teikdama paaiškinamas įžvalgas apie paslėptą riziką.

1.2.2 „IBM Financial Crimes Insight for Alert Triage – AML Transaction Monitoring“

Ši „Cloud Service“ naudoja istorinių atvejų duomenis, kontekstinių įrodymų duomenų sankaupas ir kompiuterio mokymosi galimybes, kad geriau suprastų subjekto riziką ir galėtų supaprastinti įspėjimų skubumo nustatymo procesą, sumažinti klaidingų pranešimų skaičių, paspartinti įspėjimo perdavimą ir pagerinti sprendimų priėmimą. Paslauga yra papildomas komponentas, papildantis Kliento institucijoje veikiančias sandorių stebėjimo ir atvejų valdymo sistemas.

1.2.3 „IBM Financial Crimes Insight for Alert Triage – Transaction List Screening“

Ši „Cloud Service“ papildo esamas sankcijų tikrinimo sistemas analizuodama operacijas, dėl kurių buvo gautas įspėjimas, naudodama konfigūruojamą, išplečiamą, API pagrįstą grandinę. Operacijos duomenys išvalomi, nagrinėjami ir tvarkomi, tada jie apdorojami naudojant euristikos ir kognityvines kompiuterines technikas. Rezultatai naudojami norint surinkti atitiktis, nustatyti klaidingai teigiamus rezultatus ir grąžinti informatyvias, tinkinamas įžvalgas.

1.2.4 „IBM Financial Crimes Insight for Entity Research“

Šios „Cloud Service“ naudojamos kognityvinės kompiuterinės technologijos padeda patikrinti, ištraukti ir susieti atitinkamą turinį iš struktūrizuotų ir nestruktūrizuotų duomenų šaltinių, siekiant pagerinti subjektų ir (arba) su bendradarbiavimu su jais susijusios rizikos supratimą ir sutrumpinti Kliento pažinimo (angl. „Know Your Customer“, KYC) veiksmų laiką. Sprendimas padeda automatizuoti ir standartizuoti iš įvairių duomenų šaltinių surinktos kliento informacijos paiešką ir analizę. Paslaugos tikslas – naudojant supaprastintą analizę ir patikrinimo veiklas pagerinti KYC įrašų kokybę bei patobulinti Kliento patirtį.

Klientas gali rinktis iš toliau nurodytų teisių parinkčių:

- „IBM Financial Crimes Insight for Entity Research – Enterprise“ – kiekvienu Įvykiu leidžiamas daugiau nei 5 susijusių šalių tyrimas.
- „IBM Financial Crimes Insight for Entity Research – Advanced“ – kiekvienu Įvykiu leidžiamas iki 5 susijusių šalių tyrimas.
- „IBM Financial Crimes Insight for Entity Research – Basic“ – kiekvienu Įvykiu leidžiamas iki 2 susijusių šalių tyrimas.

Susijusi šalis yra subjektas (organizacija arba asmuo), kurį reikia ištirti atliekant Pirminio tyrimo peržiūrą, kaip apibrėžta 4.1 skyriuje. Dažniausiai tai gali būti įgalioti pasirašantieji, pareigūnai, galutiniai naudos gavėjai, pirminė arba antrinė organizacija organizacijos schemoje. Siekiant išvengti abejonių, jei susijusi šalis yra subjektas, kurio asmenis arba asocijuotuosius narius reikia ištirti, kiekvienas asmuo arba asocijuotasis narys taip pat laikomas susijusia šalimi.

1.2.5 „IBM Financial Crimes Insight for Entity Research with Material Change“

Šios „Cloud Service“ naudojamos kognityvinės kompiuterinės technologijos padeda patikrinti, ištraukti ir susieti atitinkamą turinį iš struktūrizuotų ir nestruktūrizuotų duomenų šaltinių, siekiant pagerinti subjektų ir (arba) su bendradarbiavimu su jais susijusios rizikos supratimą ir sutrumpinti Kliento pažinimo (angl. „Know Your Customer“, KYC) veiksmų laiką. Sprendimas padeda automatizuoti ir standartizuoti iš įvairių duomenų šaltinių surinktos kliento informacijos paiešką ir analizę. Paslaugos tikslas – naudojant supaprastintą analizę ir patikrinimo veiklas pagerinti KYC įrašų kokybę bei patobulinti Kliento patirtį. Tai apima „Material Change“ funkciją, kuria leidžiama pagal tvarkaraštį stebėti, ar yra kokių nors subjektų medžiagos skirtumų, ir kuria pranešama analitikui, kad reikia atlikti peržiūrą.

Klientas gali rinktis iš toliau nurodytų teisių parinkčių:

- „IBM Financial Crimes Insight for Entity Research – Enterprise“ – kiekvienu Įvykiu leidžiamas daugiau nei 5 susijusių šalių tyrimas.
- „IBM Financial Crimes Insight for Entity Research – Advanced“ – kiekvienu Įvykiu leidžiamas iki 5 susijusių šalių tyrimas.
- „IBM Financial Crimes Insight for Entity Research – Basic“ – kiekvienu Įvykiu leidžiamas iki 2 susijusių šalių tyrimas.

Susijusi šalis yra subjektas (organizacija arba asmuo), kurį reikia ištirti atliekant Pirminio tyrimo peržiūrą, kaip apibrėžta 4.1 skyriuje. Dažniausiai tai gali būti įgalioti pasirašantieji, pareigūnai, galutiniai naudos gavėjai, pirminė arba antrinė organizacija organizacijos schemoje. Siekiant išvengti abejonių, jei susijusi

šalis yra subjektas, kurio asmenis arba asocijuotuosius narius reikia ištirti, kiekvienas asmuo arba asocijuotasis narys taip pat laikomas susijusia šalimi.

1.2.6 „IBM Financial Crimes Insight for Claims Fraud – Property and Casualty“

Ši „Cloud Service“ padeda organizacijoms analizuoti duomenis, siekiant nustatyti riziką, kurią sukelia jų klientų, medicininių paslaugų teikėjų ir kitų subjektų pateikiamos apgaulingos pretenzijos, valdyti visą tyrimo eigą ir teikti rezultatų ataskaitas.

1.2.7 „IBM Financial Crimes Insight for Claims Fraud – Investigation“

Ši „Cloud Service“ padeda organizacijoms valdyti visą įtartinų veiksmų ir galimų apgavysčių tyrimo eigą.

1.2.8 „IBM Electronic Communication Surveillance Analytics on Cloud“

Ši „Cloud Service“ – tai įrankis, skirtas padėti finansinių paslaugų institucijoms efektyviai analizuoti ir stebėti darbuotojų sąveikos duomenis keliais kanalais, siekiant aptikti įvairius įtartinų ryšių šablonus. Įrankis padeda aptikti įvairius sukčiavimo, susijusio su piktnaudžiavimu ir manipuliavimu rinka, šablonus. Įrankis naudoja natūralios kalbos apdorojimo galimybę, kad suprastų tekstinę informaciją ir, atsižvelgiant į kontekstą, atskirtų dviprasmiškus terminus. Be to, įrankyje naudojamos nuotaikos ir emocijų analizės galimybės, kurias galima pasitelkti atliekant ryšių analizę. Šios galimybės nėra skirtos naudoti ir nėra naudojamos asmenybės bruožams nustatyti. Ši analizė pateikiama bendrajam išvadų varikliui, padedantis susieti įvairias įžvalgas ir pateikia rizikos vertinimą atsakingiems pareigūnams.

1.2.9 „IBM Voice Surveillance Analytics on Cloud“

Ši „Cloud Service“ – tai įrankis, padedantis finansinių paslaugų institucijoms analizuoti ir stebėti darbuotojų bendravimą balsu įvairiais kanalais, siekiant aptikti įtartiną veiklą. Įrankyje naudojama „kalbos į tekstą“ technologija, skirta žmogaus balsui į rašytinius žodžius konvertuoti, išnaudojant įrenginio gebėjimą mokytis aptikti gramatinę ir kalbos struktūrą. Šis įrankis susieja „kalbos į tekstą“ rezultatus su išsamiais telefono sistemos sugeneruotais metaduomenimis ir tekstui pritaiko kalbėtojų paskirstymą, kad būtų galima lengvai ir greitai rasti ir paleisti dominančius pokalbius balsu. „Kalbos į testą“ rezultatai kartu su metaduomenimis pasiekiami Klientui aiškiai apibrėžtu formatu. Kaip papildoma parinktis įrankyje gali būti naudojamas natūralios kalbos apdorojimas, skirtas semantiniams metaduomenims iš turinio išgauti, ir lingvistinė analizė, skirta intonacijoms, nuotaikai ir emocijoms išgauti. Šios galimybės nėra skirtos naudoti ir nėra naudojamos asmenybės bruožams nustatyti. Visas „kalbos į tekstą“ pokalbis atliekamas „atmintyje“, kad nereikėtų laikyti dubliuotų failų ir transkripcijų, o po apdorojimo „Cloud“ nėra saugoma jokių balso duomenų.

1.2.10 „IBM Complaints Analytics on Cloud“

Ši „Cloud Service“ įgalina organizacijas atpažinti, kaupti ir skirstyti į kategorijas skundus, pareiškimus ir kitus veiklos elementus. Šis pasiūlymas pateikia įžvalgų apie kylančias problemas, kad būtų laikomasi reglamentų. Įrankyje naudojama pažangi analizė, kad būtų galima atpažinti ir analizuoti skundus, kurie tradicinėse sistemose būtų praleisti. Įrankis gali panaudoti struktūrinius ir nestruktūrinius duomenis, pvz., Kliento duomenis, el. laiškus, aptarnavimo pastabas, skundus socialinėje medijoje ir balso įrašus. Tada įrankyje naudojamos kognityvinės funkcijos, kad būtų galima sukaupti ir išplėsti skundų duomenis, siekiant identifikuoti sistemines grėsmes. Be to, taikomas dinaminis segmentavimas ir laiko sekos profiliavimas, norint stebėti ir numatyti pakeitimus bei tendencijas.

Norėdamas naudoti „IBM Complaints Analytics on Cloud“, Klientas taip pat turi prenumeruoti „IBM Electronic Communication Surveillance Analytics on Cloud“ arba „IBM Voice Surveillance Analytics on Cloud“.

1.2.11 „IBM Electronic Communication Surveillance Analytics on Cloud BYOL“

Ši „Cloud Service“ leidžia Klientui pasiekti „IBM Electronic Communication Surveillance Analytics on Cloud“ funkciją kaip debesies pasiūlymą. Norėdamas pasinaudoti „Bring your own licenses“ (BYOL) pasiūlymais, Klientas turi būti anksčiau įsigijęs atitinkamas susijusios IBM Programos licencijos teises. IBM Programa, reikalinga „IBM Electronic Communication Surveillance Analytics on Cloud BYOL“ pasiūlymui, yra „IBM Financial Crimes Insight for Conduct Surveillance Software – Electronic Communication“.

1.2.12 „IBM Voice Surveillance Analytics on Cloud BYOL“

Ši „Cloud Service“ leidžia Klientui pasiekti „IBM Voice Surveillance Analytics on Cloud“ funkciją kaip debesies pasiūlymą. Norėdamas pasinaudoti „Bring your own licenses“ (BYOL) pasiūlymais, Klientas turi būti anksčiau įsigijęs atitinkamas susijusios IBM Programos licencijos teises. IBM Programa, reikalinga

„IBM Voice Surveillance Analytics on Cloud BYOL“ pasiūlymui, yra „IBM Financial Crimes Insight for Conduct Surveillance Software – Voice“.

1.2.13 „IBM Complaints Analytics on Cloud BYOL“

Ši „Cloud Service“ leidžia Klientui pasiekti „IBM Complaints Analytics“ funkciją kaip debesies pasiūlymą. Norėdamas pasinaudoti „Bring your own licenses“ (BYOL) pasiūlymais, Klientas turi būti anksčiau įsigijęs atitinkamas susijusios IBM Programos licencijos teises. IBM Programa, reikalinga „IBM Complaints Analytics on Cloud BYOL“ pasiūlymui, yra „IBM Financial Crimes Insight for Conduct Surveillance Software – Complaint Analytics“.

1.3 Akceleravimo paslaugos

1.3.1 „IBM Financial Crimes Insight Set-up“

Tam, kad Klientas būtų pasirengęs naudoti atitinkamą „Cloud Service“, reikalingos šios sąrankos paslaugos:

- „IBM Financial Crimes Insight for Anti-Money Laundering Set-up“
- „IBM Financial Crimes Insight for Alert Triage – AML Transaction Monitoring Set-up“
- „IBM Financial Crimes Insight for Alert Triage – Transaction List Screening Set-up“
- „IBM Financial Crimes Insight for Entity Research – Enterprise Set-up“
- „IBM Financial Crimes Insight for Entity Research – Advanced Set-up“
- „IBM Financial Crimes Insight for Entity Research – Basic Set-up“
- „IBM Financial Crimes Insight for Entity Research with Material Change – Enterprise Set-up“
- „IBM Financial Crimes Insight for Entity Research with Material Change – Advanced Set-up“
- „IBM Financial Crimes Insight for Entity Research with Material Change – Basic Set-up“
- „IBM Financial Crimes Insight for Entity Research Negative News API Set-up“
- „IBM Financial Crimes Insight for Entity Research Enrichment API Set-up“
- „IBM Financial Crimes Insight for Claims Fraud – Property and Casualty Set-up“
- „IBM Financial Crimes Insight for Claims Fraud – Investigation Set-up“
- „IBM Surveillance Insight for Financial Services on Cloud Set-up“

2. Duomenų tvarkymo ir apsaugos duomenų lapai

Svetainėje http://ibm.com/dpa pateikiamame IBM Duomenų tvarkymo priede (DTP) ir toliau esančiose nuorodose pateikiamame (-uose) Duomenų tvarkymo bei apsaugos duomenų lape (-uose) (vadinamame (-uose) duomenų lapu (-ais) arba DTP įrodymu (-ais) pateikiama papildoma „Cloud Service“ duomenų apsaugos informacija ir jos apsaugos galimybės, susijusios su Turinio, kuris gali būti tvarkomas, tipais, atliekamais tvarkymo veiksmais, duomenų apsaugos funkcijomis ir Turinio saugojimo bei grąžinimo specifika. DTP taikomas asmeniniams duomenims, esantiems turinyje, jei (ir tik tokia apimtimi) taikomas i) Europos bendrasis duomenų apsaugos reglamentas (ES/2016/679) (BDAR) arba ii) kiti duomenų apsaugos teisės aktai, nurodyti http://www.ibm.com/dpa/dpl.

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=14BD7780D65B11E99EAFC519926DF897

3. Paslaugos lygiai ir techninis palaikymas

3.1 Paslaugos lygio sutartis

IBM teikia Klientui toliau nurodytus pasiekiamumo paslaugos lygio sutarties (PLS) įsipareigojimus. IBM taikys aukščiausią galimą kompensaciją, pagrįstą „Cloud Service“ kaupiamuoju pasiekiamumu, kaip nurodyta toliau esančioje lentelėje. Pasiekiamumo procentas apskaičiuojamas iš bendro minučių skaičiaus sutartinį mėnesį atėmus bendrą Paslaugos neveikimo minučių skaičių sutartinį mėnesį, gautą rezultatą padalijus iš bendro minučių skaičiaus sutartinį mėnesį. Paslaugos neveikimo apibrėžimas, prašymų pateikimo procesas ir informacija, kaip susisiekti su IBM dėl paslaugos pasiekiamumo problemų, pateikiama „IBM Cloud Service“ palaikymo vadove https://www.ibm.com/software/support/saas_support_overview.html.

Prieinamumas	Kreditas (% mėnesio prenumeratos mokesčio*)
Mažiau nei 99,9 %	2 %
Mažiau nei 99,0 %	5 %
Mažiau nei 95,0 %	10 %

* Prenumeratos mokestis yra teiginyje minimo mėnesio sutartinė kaina.

3.2 Techninė pagalba

„Cloud Service“ techninį palaikymą, įskaitant palaikymo kontaktinę informaciją, sudėtingumo lygius, pasiekiamumo palaikymo valandas, atsakymo laiką ir kitą palaikymo informaciją ir procesus rasite pasirinkę „Cloud Service“ IBM palaikymo vadove svetainėje https://www.ibm.com/support/home/pages/support-guide/.

4. Mokesčiai

4.1 Mokesčio apskaičiavimas

„Cloud Service“ mokesčio apskaičiavimas nurodytas Operacijų dokumente.

Šiai „Cloud Service“ taikomas toliau aprašytas mokesčio apskaičiavimas.

- „Engagement“ yra profesionali arba mokymo paslauga, susijusi su „Cloud Services“.
- Egzempliorius yra kiekviena prieiga prie konkrečios „Cloud Services“ konfigūracijos.
- Įvykis yra konkretaus įvykio, kurį apdoroja „Cloud Service“ arba kuris susijęs su „Cloud Services“ naudojimu, atvejis.
    - „IBM Financial Crimes Insight for Anti-Money Laundering“ Įvykis – tai 10 milijonų finansinių operacijų per vieną kalendorinį mėnesį.
    - „IBM Financial Crimes Insight for Claims Fraud – Property and Casualty“ ir „IBM Financial Crimes Insight for Claims – Investigation“ Įvykis – tai Pretenzijos atvejis. Pretenzija – tai instrukcijų, susijusių su oficialiu pareikalavimu organizacijai dėl dengiamų nuostolių arba įvykio padengimo ar kompensacijos, rinkinys.
    - „IBM Financial Crimes Insight for Alert Triage – AML Transaction Monitoring“ Įvykis – tai atskiras įspėjimas / įvykis, įdėtas į „Cloud Service“ iš pradinės sistemos per vieną kalendorinį mėnesį. Paprastai pradinė šaltinio sistema yra operacijų stebėjimo sistema arba atvejų valdymo sistema.
    - „IBM Financial Crimes Insight for Alert Triage – Transaction List Screening“ Įvykis – tai iki 1 000 atskirų įspėjimų, įdėtų į „Cloud Service“ iš pradinės sistemos per vieną kalendorinį mėnesį. Paprastai pradinė šaltinio sistema yra operacijų stebėjimo sistema arba atvejų valdymo sistema.
    - „IBM Financial Crimes Insight for Entity Research“ ir „IBM Financial Crimes Insight for Entity Research with Material Change“ Įvykis – tai bet koks per vieną kalendorinį mėnesį „Cloud Service“ apdorotas pirminis tyrimas, įskaitant identiškas pakartotines paieškas. Pirminis tyrimas – tai bet kuris įrašas, nesusietas kaip antrinis su kitu tyrimu. Antrinis subjektas yra susijusi šalis (kaip apibrėžta 1.2.5 skyriuje), kuriai jokiais būdais netaikomas pirminis tyrimas.
- Priskirtas dalyvis – tai privatus ar juridinis asmuo, turintis teisę dalyvauti bet kurioje „Cloud Services“ valdomoje arba stebimoje paslaugos teikimo programoje.
- Elementas yra konkretaus elemento, kurį valdo ar apdoroja „Cloud Service“ arba kuris susijęs su jos naudojimu, atvejis.
    - „IBM Voice Surveillance Analytics on Cloud“ Elementas yra viena Balso srauto, apdoroto „Cloud Service“, valanda per kalendorinę dieną. Balso srautas yra garso komunikacijos fiksavimas realiuoju laiku arba įrašomu formatu.
- API iškvieta – tai „Cloud Services“ iškvieta per programuojamąją sąsają.
- Subjekto ID yra unikalus bet kurio „Cloud Service“ subjekto identifikatorius.

5. Papildomos sąlygos

„Cloud Service“ sutartims (arba atitinkamoms debesies technologijomis pagrįstoms sutartims), vykdytoms iki 2019 m. sausio 1 d., taikomos sąlygos, pateikiamos https://www.ibm.com/acs.

5.1 Pagalbinės programos

„IBM Financial Crimes Insight“ ir „IBM Financial Crimes Insight Non-Production“ apima prieigą prie debesies aplinkoje įdiegtų tam tikrų programų („Pagalbinės programos“). Klientas šias Pagalbines programas gali naudoti tik kovos su sukčiavimu, finansiniais nusikaltimais ir nesąžiningais mokėjimais tikslu arba atliekant kitus veiksmus, skirtus tokiems veiksmams identifikuoti ir (arba) sukliudyti.

5.1.1 Konkrečioms Pagalbinėms programoms taikomi naudojimo apribojimai

Toliau nurodytos Pagalbinės programos pasiekiamos taikant šiuos apribojimus:

- „IBM Watson Studio“ – Teisės: 5 Lygiagretieji vartotojai
- „IBM Watson Machine Learning“ – Teisės: 50 Modelių
- „IBM Openscale“ – Teisės: 50 Modelių
- „IBM SPSS Modeler Premium“ – Teisės: 4 Įgaliotieji vartotojai
- „IBM SPSS Statistics Standard“ – Teisės: 4 Įgaliotieji vartotojai
- „Watson Explorer Advanced Edition“ – Teisės: X gigabaitų, kaip apibrėžta toliau.

  Klientui leidžiama analizuoti:

  - visą „Cloud Service“ saugykloje saugomą Turinį, skirtą naudoti su analizei neskirtais rinkiniais;
  - iki 10 gigabaitų „Cloud Service“ saugykloje nesaugomo Turinio, skirto naudoti su analizei neskirtais rinkiniais;
  - 100 gigabaitų „Cloud Service“ saugykloje saugomo Turinio, skirto naudoti su analizei skirtais rinkiniais.

    Analizės rinkiniai nurodo rinkinius, sukurtus „Watson Explorer annotation Administration Console“, „Watson Explorer Content Analytics Administration Console“ arba per API kaip „Turinio analizė“ arba „Analizė“ tipus.

    Ne analizės rinkiniai apima visą kitą Programos „Cloud Service“ analizuojamą turinį.
- „IBM InfoSphere DataStage – IBM InfoSphere DataStage and QualityStage Designer“ teisių suteikimas: 2 Įgaliotieji vartotojai
- „IBM Operational Decision Manager“ – teisių suteikimas: 1 milijonas taisyklių sprendimų per mėnesį ir 1 tūkstantis valdomų sprendimų artefaktų per mėnesį

Teisių apibrėžtys

a. Lygiagretusis vartotojas - tai asmuo, bet kuriuo metu naudojantis Pagalbine programa. Nepaisant to, ar asmuo vienu metu prieina prie Pagalbinės programos kelis kartus, jis skaičiuojamas kaip vienas Lygiagretusis vartotojas.

b. Modelis – tai matematinis modelis arba algoritmas, susijęs su pagrindiniais duomenimis arba duomenų generavimo procesu, naudojamu prognozėms Pagalbinėje programoje modeliuoti, aiškinti ir kurti.

c. Įgaliotasis vartotojas – tai unikalus vartotojas, kuriam bet kokiu tiesioginiu arba netiesioginiu būdu (pavyzdžiui, naudojant tankinimo programą, įrenginį arba taikomųjų programų serverį) ir bet kokiomis priemonėmis suteikiama teisė naudotis prieiga prie Pagalbinės programos.

d. Gigabaitas (GB) – tai 2 pakelta trisdešimtuoju laipsniu baitų duomenų, kurie yra apdorojami, analizuojami, naudojami, saugomi arba konfigūruojami Pagalbinėje programoje.

e. Mėnesiniai taisyklių sprendimai – tai iš taisyklių vykdymo serverio iškviesto taisyklių rinkinio rezultatas, kurį vykdo arba apdoroja Pagalbinė programa bet kurį kalendorinį mėnesį.

f. Kas mėnesį valdomi sprendimo artefaktai yra Pagalbinės programos valdomas subjektas bet kurį kalendorinį mėnesį.

5.2 „IBM Financial Crimes Insight BYOL“ taikomos sąlygos

Norėdamas pasinaudoti „Bring your own licenses“ (BYOL) pasiūlymais, Klientas turi būti anksčiau įsigijęs atitinkamas susijusios IBM Programos licencijos teises, nurodytas tolesnėje lentelėje. Kliento „BYOL SaaS“ teisės negali viršyti Kliento susijusios IBM Programos teisių toliau nurodytais santykiais.

BYOL pasiūlymas neapima susijusios IBM Programos prenumeratos ir palaikymo (S&S). Klientas pareiškia, kad yra įsigijęs taikomas Susijusios IBM programos (1) licencijos teises bei (2) S&S. BYOL pasiūlymo prenumeratos laikotarpiu Klientas turi išlaikyti dabartinę IBM Programos teisių, naudojamų kartu su BYOL pasiūlymo teisėmis, S&S. Tuo atveju, jei Kliento licencija naudoti susijusią IBM Programą arba susijusios IBM programos S&S nutraukiama, nebegalios ir Kliento teisė naudoti BYOL pasiūlymą.

Klientas gali toliau naudoti teises į susijusią IBM programą, kurios taikomos BYOL pasiūlymui naudoti diegiant susijusią IBM programą tuo pačiu metu, kai Klientas naudoja BYOL pasiūlymą toliau nurodytą laikotarpį („Lygiagrečiojo naudojimo laikotarpis“): Klientams, kurių prenumeratos terminas yra treji (3) metai, ne ilgiau nei devyniasdešimt (90) dienų nuo pradinės Kliento BYOL pasiūlymo prenumeratos pradžios; Klientams, kurių prenumeratos laikotarpis yra mažiau nei treji (3) metai arba ilgesnis, ne ilgiau nei vienus (1) metus nuo pradinės Kliento BYOL pasiūlymo prenumeratos pradžios. Pasibaigus Lygiagrečiojo naudojimo laikotarpiui, Kliento BYOL pasiūlymo naudojimo laikotarpiu Kliento susijusios IBM programos teisės, taikomos BYOL pasiūlymo naudojimui, yra sulaikomos ir Klientas nebegali naudoti šių teisių susijusiai IBM programai diegti (galimos nurodytos išimtys).

Tolesnėje lentelėje nurodytas susijusios IBM Programos teisių santykis, būtinas norint naudoti BYOL pasiūlymą laikantis nurodytos atitinkamos teisės. Klientui gavus BYOL pasiūlymą ir jo naudojimo laikotarpiu, Kliento teisės į susijusią IBM Programą ir taikomos BYOL pasiūlymo naudojimui, yra sulaikomos ir Klientas nebegali naudoti šių teisių diegdamas susietą IBM Programą (taikomos visos nurodytos išimtys).

Susijusi IBM programa	BYOL pasiūlymas	Santykis n/m*
„IBM Cloud Pak for Data Financial Crimes Insight“	„IBM Financial Crimes Insight BYOL“	Santykis: 1 Diegimas / 1 Egzempliorius
„IBM Cloud Pak for Data Financial Crimes Insight for Non-Production Environment“	„IBM Financial Crimes Insight Non-Production BYOL“	Santykis: 1 Diegimas / 1 Egzempliorius
„IBM Financial Crimes Insight for Conduct Surveillance Software – Electronic Communication“	„IBM Electronic Communication Surveillance Analytics on Cloud BYOL“	Kaupiamieji santykiai: 1 pakopa (1-100 IVV): ● 1 RVU / 1 Reikalavimus atitinkantis dalyvis 2 pakopa (101-235 IVV): ● 0,9 IVV / 1 Reikalavimus atitinkantis dalyvis 3 pakopa (236-435 IVV): ● 0,8 IVV / 1 Reikalavimus atitinkantis dalyvis 4 pakopa (436-585 IVV): ● 0,6 IVV / 1 Reikalavimus atitinkantis dalyvis 5 pakopa (586-835 IVV): ● 0,5 IVV / 1 Reikalavimus atitinkantis dalyvis 6 pakopa (836-1 135 IVV): ● 0,4 IVV / 1 Reikalavimus atitinkantis dalyvis 7 pakopa (daugiau nei 1 135 IVV): ● 0,3 IVV / 1 Reikalavimus atitinkantis dalyvis

Susijusi IBM programa	BYOL pasiūlymas	Santykis n/m*
„IBM Financial Crimes Insight for Conduct Surveillance Software – Voice“	„IBM Voice Surveillance Analytics on Cloud BYOL“	Kaupiamieji santykiai: 1 pakopa (1-100 IVV): ● 1 IVV / 1 Elementas 2 pakopa (101-235 IVV): ● 0,9 IVV / 1 Elementas 3 pakopa (236-435 IVV): ● 0,8 IVV / 1 Elementas 4 pakopa (436-585 IVV): ● 0,6 IVV / 1 Elementas 5 pakopa (586-835 IVV): ● 0,5 IVV / 1 Elementas 6 pakopa (836-1 135 IVV): ● 0,4 IVV / 1 Elementas 7 pakopa (daugiau nei 1 135 IVV): ● 0,3 IVV / 1 Elementas
„IBM Financial Crimes Insight for Conduct Surveillance Software – Complaint Analytics“	„IBM Complaints Analytics on Cloud BYOL“	Kaupiamieji santykiai: 1 pakopa (1-100 IVV): ● 5 IVV / 1 Subjekto ID 2 pakopa (101-235 IVV): ● 4,5 IVV / 1 Subjekto ID 3 pakopa (236-435 IVV): ● 4 IVV / 1 Subjekto ID 4 pakopa (436-585 IVV): ● 3 IVV / 1 Subjekto ID 5 pakopa (586-835 IVV): ● 2,5 IVV / 1 Subjekto ID 6 pakopa (836-1 135 IVV): ● 2 IVV / 1 Subjekto ID 7 pakopa (daugiau nei 1 135 IVV): ● 1,5 IVV / 1 Subjekto ID

* „Santykis n/m“ reiškia, kad kiekvienam susietos IBM programos nurodytos metrikos teisių skaičiui (n) Klientas gali taikyti tas teises nurodytam BYOL pasiūlymo metrikos teisių skaičiui (m). Jei konvertuojant iš Susijusių IBM programų į BYOL pasiūlymą gaunamas ne sveikasis skaičius, apvalinama iki artimiausio sveikojo skaičiaus.

1 pavyzdys:

710 IVV Reikalavimus atitinkančiam dalyviui (EPS)

(Taikoma „IBM Trade Surveillance Analytics“ ir „IBM Electronic Communication Surveillance Analytics“)

1 pakopa: jeigu 710>100, tuomet 100/1 = 100 EPS

2 pakopa: jei 710>235, tuomet (235-100)/0,9 = +150 EPS

3 pakopa: jei 710>435, tuomet (435-235)/0,8 = +250 EPS

4 pakopa: jei 710>585, tuomet (585-435)/0,6 = +250 EPS

5 pakopa: jei 710>835 ? ne, tuomet (710-585)/0,5 = +250 EPS

Iš viso EPS: 100 + 150 + 250 + 250 + 250 = 1000 EPS

2 pavyzdys:

250 IVV (100 000/pak.) Subjekto ID (500 000/pak.)

(Taikoma „IBM Complaints Analytics“)

1 pakopa: jei 250>100, tuomet 100/5 = 20 Subjekto ID

2 pakopa: jei 250>235, tuomet (235-100)/4,5 = +30 Subjekto ID

3 pakopa: jei 250>435 ? ne, tuomet (250-235)/4 = +3,75 Subjekto ID

Iš viso EPS: 20 + 30 + 3,75 = 53,75 Subjekto ID, apvalinama iki 54 Subjekto ID

Tikrinimas: 250 IVV = 269 Ištekliai * 100 000 turimo paketo dydis / 500 000 paketo dydis „SaaS“ = 53,75, apvalinama iki 54 Subjekto ID

5.3 Trečiosios šalies turinys

Klientas pripažįsta, kad gauti ir ataskaitose nurodyti paieškos rezultatai, sugeneruoti kaip šiame dokumente aprašytų „Cloud Services“ dalis („Paieškos rezultatai“), gali apimti duomenis arba Turinį, priklausantį trečiosioms šalims, ir kad IBM neparduoda arbe neteikia jokių Paieškos rezultatų arba Turinio licencijų ar kitų teisių. Klientas sutinka, kad jis vienintelis atsako už bet kokių ir visų tokių licencijų, teisių ir leidimų iš atitinkamų trečiųjų šalių gavimą (ir turi juos gauti prieš pradedamas naudoti bet kurias šiame dokumente aprašytas „Cloud Services“), kaip tai yra būtina pagal tokiems Paieškos rezultatams, skirtiems Klientui arba IBM Kliento vardu, taikomus įstatymus Paieškos rezultatams naudoti, laikyti, saugoti, apdoroti, atkurti arba pritaikyti. Klientas įgalioja IBM ir jos susijusias įmones bei rangovus Kliento vardu pasiekti, atkurti, pritaikyti arba kitaip apdoroti trečiosios šalies duomenų šaltinius (įskaitant bet kokius duomenis arba Turinį, esantį Paieškos rezultatuose arba gautą iš jų), susijusius su šiame dokumente nurodytomis „Cloud Services“. Šiame 5.3 skyriuje nustatyta, kad Turinį sudaro bet koks autoriaus teisių saugomas kūrinys, duomenys, vaizdai, programinė įranga arba informacija, kurią Klientas arba jo įgaliotieji vartotojai pateikia, suteikia teisę pasiekti arba įtraukia į „Cloud Service“.

5.4 „Cloud Service“ galiojimo laikas

Iki „Cloud Service“ paslaugos galiojimo pabaigos ar nutraukimo Klientas gali gauti duomenų naudodamas bet kokias pateiktas „Cloud Service“ ataskaitų ir eksportavimo funkcijas. Pasirinktinio duomenų išgavimo paslaugos teikiamos pagal atskirą sutartį.

Per 30 dienų nuo „Cloud Service“ paslaugos galiojimo pabaigos ar nutraukimo, gavusi užklausą iš Kliento, IBM grąžins elektroninę Kliento turinio kopiją vietinės taikomosios programos formatu.