

„IBM QRadar Advisor with Watson“

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

1. „Cloud Service“

„IBM QRadar Advisor with Watson“ išplečia kognityvinę analizę į „QRadar Security Platform“, padeda Klientams ir saugos analitikams tirti grėsmes ir į jas reaguoti. Ji išnaudoja „Watson for Cyber Security“ žinių visumą, prisijungusi prie nestruktūrizuotų duomenų (įskaitant saugos svetaines, interneto dienoraščius, tyrimo dokumentus ir kt.) ir susiejusi tarpusavyje vietos saugos incidentus. Taip galima atskleisti paslėptas grėsmes ir automatizavus įžvalgas reaguoti ir priimti sprendimus. „QRadar Advisor with Watson“ suteikia galimybę saugos analitikui siųsti saugos pažeidimus „Watson“ ir aptikti grėsmę naudojantis šimtų tūkstančių nestruktūrizuotų ir struktūrizuotų duomenų šaltinių duomenų baze ir susiejant juos su grėsmių atvejais, susijusiais su originaliu saugos pažeidimu, pvz., kenkėjiškais failais, įtartinais IP adresais, sukčiavimo subjektais ir jų ryšiais. Tai gali būti ypač naudinga nustatant, ar saugos pažeidimas susijęs su žinoma kenkėjiškos programos kampanija. Jei taip, „Watson“ kartu su kitomis įžvalgomis teikia naudojamų kenkėjiškų programų, pažeidžiamumo išnaudojimo ir grėsmių aprėpties (įskaitant papildomus galimai paveiktus galutinius taškus) įžvalgas.

1.1 Pasiūlymai

Klientas gali rinktis iš toliau nurodytų galimų pasiūlymų.

1.1.1 „IBM QRadar Advisor with Watson“

„IBM QRadar Advisor with Watson“ reikalauja, kad Klientas turėtų aktyvią „IBM QRadar“ įdiegtą vietinėje sistemoje arba debesijos aplinkoje ir būtų įdiegęs joje „Cloud Service“ įgalinimo programinę įrangą, kad galėtų pasiekti funkcinę galimybę. Kai „Cloud Service“ teisės suteikiamos pagal įvykius per sekundę, nustatyta saugos pažeidimų užklausa, kurias Klientas gali siųsti „Cloud Service“, skaičiaus riba – po 1,5 užklauskos per dieną 100 įvykių per sekundę (suapvalinus iki artimiausios užklauskos), kurių teisę Klientas turi. Kai „Cloud Service“ teisės suteikiamos pagal Valdomą virtualųjį serverį (VVS), nustatyta saugos pažeidimų užklausa, kurias Klientas gali siųsti „Cloud Service“, skaičiaus riba – po 15 užklauskos per dieną 100 VVS, kurių teisę Klientas turi. Šį skaičių viršijančių Užklauskų prioritetą bus panaikintas ir likusią dienos dalį jos nebus apdorojamos „Cloud Service“.

1.1.2 „IBM QRadar Advisor with Watson – Enterprise“

„IBM QRadar Advisor with Watson – Enterprise“ geriausiai tinka didelio saugos operacijų centro (SOC) diegimams, kurie paprastai viršija du šimtus penkiasdešimt tūkstančių įvykių per sekundę ar daugiau. Norėdamas pasiekti „Cloud Service“ funkcijas, „Cloud Service“ įgalinimo programinę įrangą Klientas turi įdiegti atskirai įsigytoje „IBM QRadar“ įdiegtyje. „IBM QRadar Advisor with Watson – Enterprise“ galima įsigyti pagal Egzemplioriumi pagrįstą metriką, kuri nepriklauso nuo Kliento „IBM QRadar“ diegimo apimtys. Bet kuriuo nurodytu metu Klientas gali pateikti daugiausia 25 paraiškas iš eilės.

1.1.3 „IBM QRadar Advisor with Watson – Starter Pack“

„IBM QRadar Advisor with Watson – Starter Pack“ yra skirta pirmą kartą besinaudojantiems „QRadar Advisor with Watson“. Ši „Cloud Service“ turi visas „QRadar Advisor with Watson“ funkcijas, kaip aprašyta anksčiau pateiktame 1.1.1 skyriuje, tačiau ji prieinama tik Klientui pirmą kartą įsigijus „QRadar Advisor with Watson“ ir nėra atnaujinama.

1.2 Pasirinktinės paslaugos

1.2.1 „IBM QRadar Advisor with Watson – Test Environment“

„IBM QRadar Advisor with Watson – Test Environment“ yra skirta Klientams, kurie nori diegti „Cloud Service“ savo vidinėje testavimo aplinkoje. Ją galima naudoti tik ne gamybos testavimo tikslais. Kartu su „IBM QRadar Advisor with Watson – Test Environment“ turi būti naudojama gamybos lygio „Cloud Service“ prenumerata.

1.3 Akceleravimo paslaugos

1.3.1 „IBM QRadar Advisor with Watson Advanced Services“

Kaip šios nuotoliniu būdu teikiamos prenumeratos paslaugos dalį IBM teiks Klientui bet kurią iš toliau nurodytų konsultacinių paslaugų iki 5 dienų per vienerių metų laikotarpį:

- Kliento SOC proceso, įskaitant tyrimą ir (arba) reagavimo į incidentą procesą, vertinimą;
- pakartotinį reagavimo į nuorodų rinkinius vertinimą;
- automatinės didelio masto pažeidimų analizės koregavimą;
- atvejo kūrimo naudojimą;
- rekomendacijų dėl SOC proceso keitimų, kurie apima „QRadar Advisor with Watson“, teikimą;
- gairių, kaip tinkamai suprasti ir įtraukti duomenis iš „QRadar Advisor with Watson“ į esamus Kliento procesus, teikimą;
- žinių susijusiomis „QRadar Advisor with Watson“ temomis perdavimą.

PASTABA. Toliau nurodytos veiklos gali būti įtrauktos į šią paslaugą remiantis Kliento „QRadar“ diegimo būseną:

- Kliento „QRadar“ diegimo būklės patikra;
- papildomas esamo „QRadar“ diegimo reguliavimas;
- pagalba įtraukiant papildomus žurnalų šaltinius į Kliento „QRadar“ diegimą.

1.3.2 „IBM QRadar Advisor with Watson Basic Setup Service“

Ši sąrankos paslauga teikiama nuotoliniu būdu ir apima keturiasdešimt (40) valandų profesionalių paslaugų, kurių galiojimas baigsis po devyniasdešimties (90) dienų nuo pirkimo, jei nėra numatyta kitaip, neatsižvelgiant į tai, ar buvo išnaudotos visos valandos (jei taikoma). Į paslaugas įtrauktas paskirtas IBM įsipareigojimų vadovas, kuris planuos pradinį skambučių.

IBM atliks kelis arba visus toliau nurodytus darbus:

- Kliento SOC proceso, įskaitant tyrimą ir (arba) reagavimo į incidentą procesą, vertinimą;
- „QRadar Advisor with Watson“ diegimą Kliento aplinkoje;
 - „QRadar Advisor with Watson“ diegimą;
 - vieningų ypatybių susiejimą su „QRadar Advisor with Watson“;
 - reagavimo į nuorodų rinkinius vykdymą;
 - automatinės didelio masto pažeidimų analizės koregavimą;
 - atvejo rekomendacijų naudojimą;
 - rekomendacijų dėl SOC proceso keitimų, kurie apima „QRadar Advisor with Watson“, teikimą.

1.3.3 „IBM QRadar Advisor with Watson Quick Setup Service“

Ši sąrankos paslauga skirta Klientams, naudojančioms mažiau nei 5 000 įvykių per sekundę (IPS).

Teikiant šią nuotoliniu būdu teikiamą paslaugą, IBM teiks Klientui bet kurią iš toliau nurodytų konsultacinių paslaugų (arba jų derinį) iki 16 valandų per 90 dienų laikotarpį:

- „QRadar Advisor with Watson“ diegimas.
- „QRadar Advisor with Watson“ teisių valdymas.
- „QRadar Advisor with Watson“ konfigūravimas, kuris gali apimti:
 - saugaus tarpinio serverio konfigūravimą,
 - „X-Force“ apsikeitimo kredencialų pateikimą,
 - įgaliojimų paslaugos atpažinimo ženklų kūrimas,
 - analizės rezultatų saugojimo išlaikymo strategijos konfigūravimas,
 - pasirinktinio įvykio ypatybių susiejimas,
 - nuorodos rinkinių eksportavimas,
 - intelektualusis grėsmių susiejimas,

- turto identifikavimo konfigūravimas,
- naudojimo optimizavimas.
- Automatinis pažeidimo tyrimas ir rezultatai (bent vieno naudojimo atvejo demonstravimas).
- Įžvalgų tyrimas naudojant ryšių diagramą.

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://ibm.com/dpa/dpl>.

<https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=0B439290AB5011E6BE74C84817AAB206>

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.

- Įvykis per sekundę (IPS) yra konkretaus IPS, kurį apdoroja „Cloud Service“ arba kuris susijęs su „Cloud Services“ naudojimu, atvejis. Šioje „Cloud Service“ įvykiai per sekundę yra tie, įvykiai, kuriuos surenka ir apdoroja Kliento „IBM QRadar“ diegimas.
- Egzempliorius yra kiekviena prieiga prie konkrečios „Cloud Services“ konfigūracijos.
- „Engagement“ yra profesionali arba mokymo paslauga, susijusi su „Cloud Services“.

- Valdomąjį virtualųjį serverį (VVS) sudaro procesoriai, atmintis ir įvesties / išvesties funkcinės galimybės, kurios vykdo reikiamas procedūras, komandas arba taikomas programas, kurias valdo „Cloud Services“.

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 Įgalinimo programinė įranga

„Cloud Service“ yra ši įgalinimo programinė įranga:

- „IBM QRadar with Watson App“ (<https://exchange.xforce.ibmcloud.com/hub>)

5.2 Teisėtai „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 teisėtai 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 teisėtai „Cloud Service“ naudojimui reikalingus sutikimus, leidimus arba licencijas.

6. Pagrindinės sąlygos

6.1 Duomenų naudojimas

Toliau nurodytas teiginys laikomas svarbesniu už bet kuriuos jam prieštaraujančius pagrindinių „Cloud Service“ sąlygų tarp šalių Turinio ir Duomenų apsaugos skyriuose nurodytus teiginius: IBM nenaudos arba neatskleis Klientui naudojant „Cloud Service“ gautų rezultatų, kurie yra unikalūs Kliento Turinio (Įžvalgų) rezultatai ar kitaip identifikuoja Klientą. Tačiau IBM naudos Turinį ir kitą informaciją, gautą iš Turinio (išskyrus „Insights“) kaip „Cloud Service“ dalį, „Cloud Service“ tobulinimo tikslais. IBM taip pat gali bendrai naudoti grėsmių identifikatorius ir kitą saugos informaciją, įdėtą į Turinį grėsmių aptikimo ir apsaugos tikslais.