# „IBM QRadar on Cloud“

Šis Paslaugos aprašas apibūdina „Cloud Service“. Taikomuose užsakymo dokumentuose pateikiama išsami informacija apie kainą ir papildoma informacija apie Kliento užsakymą.

## 1. „Cloud Service“

### 1.1 „IBM QRadar on Cloud“

Klientas gali rinktis iš toliau nurodytų galimų pasiūlymų.

#### 1.1.1 „IBM QRadar on Cloud 100 EPS“

„IBM QRadar on Cloud“ pasiūlymas teikia išplėstinį saugos informacijos sprendimą iš „IBM Cloud“, pagrįsto „IBM Security QRadar SIEM“ produktu. Jis leidžia Klientams rinkti, susieti ir saugoti vietinėje ir debesies aplinkose sugeneruotus įvykius, taip pat valdyti saugą ir grėsmę taip, kaip jie tai darytų naudodami vietoje įdiegtą „QRadar SIEM“ produktą. Kartu su pasiūlymu IBM taip pat pateikia infrastruktūros stebėjimo visą parą galimybę ir pritaiko naujausią programinės įrangos lygį arba svarbias pataisas, kai tokių yra.

Ši „Cloud Service“ apima devyniasdešimt (90) dienų aktyvios, iešką palaikančios saugyklos.

### 1.2 Pasirinktinės paslaugos

#### 1.2.1 „IBM QRadar on Cloud 1K EPS Temporary Upgrade“

Paslaugos naujinimas, suteikiantis papildomą 1 000 ĮPS talpą žurnalo įvykiams rinkti ir apdoroti, bet tik laikinam mėnesių skaičiui. Klientas gali įsigyti kelis šio naujinimo vienetus, bet ne daugiau nei didžiausias ĮPS lygis, kurį pasiūlymas gali palaikyti. Šios dalies tikslas – įgalinti Klientą, kuriam reikia padengti įvykius per metinius „piko“ laikotarpius, kad jis atitiktų tuos reikalavimus, pasinaudodamas laikinu talpos padidinimu. Laikotarpio pabaigoje šios laikinos talpos padidinti kiekiai bus pašalinti iš Kliento aplinkos.

#### 1.2.2 „IBM QRadar on Cloud Data Storage 100 EPS“

Atnaujinus duomenų saugyklą, pridedama papildomos saugyklos vietos ir išplečiamas analizės laikotarpis. Talpos padidinimas suteikia klientams galimybę už kiekvieną 100 EPS padidinimą saugoti duomenis iki 1 pilnų metų.

#### 1.2.3 „IBM QRadar on Cloud Flows Add-On“

Integruojama su „IBM QRadar SIEM“ ir srauto procesoriais, kad būtų galima užtikrinti „Layer 3“ tinklo matomumą ir srauto analizę, o Klientas galėtų aptikti, nustatyti ir atsakyti į Kliento tinkle atliekamus veiksmus.

#### 1.2.4 „IBM QRadar on Cloud Vulnerability Management Add-On“

Aktyviai aptinka ir nustato tinklo įrenginio ir taikomosios programos saugos silpnąsias vietas, prideda konteksto ir palaiko taisymo bei rizikos mažinimo prioritetų nustatymo veiksmus.

#### 1.2.5 „IBM QRadar on Cloud Log Archival“

Leidžia Klientui prenumeratos laikotarpiu archyvuoti įvykių duomenis iš „Cloud Service“. IBM bendradarbiaus su Klientu įrašant nurodytus įvykius į objektų saugyklą archyvavimo tikslais. Klientui pageidaujant, IBM perkels iki trisdešimties (30) dienų vertės suarchyvuotų įvykių duomenų į Kliento „Cloud Service“ egzempliorių per tris (3) darbo dienas nuo tokio prašymo pateikimo. Tokie duomenys bus pasiekiami Klientui 48 val. Po to jie bus grąžinti į archyvuojamų objektų saugyklą. Klientas gali pateikti du prašymus per trijų mėnesių laikotarpį.Talpos padidinimas suteikia klientams galimybę už kiekvieną 100 EPS padidinimą saugoti duomenis iki 1 pilnų metų.

### 1.3 Akceleravimo paslaugos

#### 1.3.1 „IBM QRadar on Cloud Optimization Service“

Dėl šios nuotoliniu būdu teikiamos prenumeratos paslaugos IBM rengs su Klientu apžvalgos susitikimus, kad būtų įvertinta esama Kliento „Cloud Service“ egzemplioriaus sveikata ir Klientui būtų pateikti rezultatai „QRadar on Cloud“ sveikatos būklės ataskaitoje, nurodant tobulintinas sritis, jei tokių yra.

Be to, Kliento prašymu IBM teiks Klientui bet kurią iš toliau nurodytų konsultacinių paslaugų iki aštuonių (8) dienų per vienerių metų laikotarpį:

- pagalba įtraukiant papildomus žurnalų šaltinius į „Cloud Service“;
- papildomų ieškų, ataskaitų ir ataskaitų sričių konfigūravimas;
- papildomas esamo „QRadar“ diegimo reguliavimas ir
- žinių susijusiomis „QRadar“ temomis perdavimas.

### 1.3.2 Nustatymo paslaugos

Toliau nurodytos sąrankos paslaugos yra teikiamos nuotoliniu būdu ir užsakomos atskirai. Kiekvienos užsakytos paslaugos 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 pradinius skambučius.

### 1.3.3 „IBM QRadar on Cloud Deployment Service“

Ši paslauga teikia keturiasdešimt (40) valandų profesionalių paslaugų, kurių metu IBM atliks kelis arba visus iš šių veiksmų:

IBM atliks iki šešiolikos valandų SIEM architektūros apžvalgą, kad apibrėžtų Kliento ataskaitų teikimo reikalavimus, ir pateiks gautus rezultatus Klientui sprendimo architektūros ataskaitoje, kuri padės apibrėžti ir užfiksuoti Kliento reikalavimus.

Į šią ataskaitą bus įtraukta:

- Kliento apibrėžti ataskaitų teikimo reikalavimai, padedantys laikytis Kliento atitikties, audito ir saugos informacijos reikalavimų.
- Saugos informacijos reikalavimai, naudojimo atvejai ir programos, kurias IBM gali padėti įdiegti (iki dešimties (10) naudojimo atvejų ir iki dviejų (2) programų).
- Aukšto lygio informacija apie Kliento žurnalų ir srautų šaltinius, kurių reikės siekiant palaikyti naudojimo atvejus.
- Tinklo infrastruktūros sprendimai, pvz., užkardos ir prievadai.

Atsižvelgdama į sprendimo architektūros ataskaitą, jei liks laiko, IBM atliks šias užduotis:

- Sukonfigūruos „Cloud Service“ įvykių rinkinį daugiausia trims (3) iki dešimties (10) žurnalų šaltinių tipų egzemplioriams. Ši veikla apims žinių perdavimą atitinkamam Kliento personalui, kad jie prireikus galėtų įtraukti daugiau žurnalų šaltinių. Su šia paslauga bus įtraukti tik standartinių „QRadar“ įrenginių palaikymo modulių (DSM) palaikomi žurnalų šaltiniai.
- Pradinis reguliavimas, apimantis a) jau parengtų taisyklių, įrašytų ieškų, sukauptų laiko sekų diagramų ir ataskaitų aktyvinimą, b) triukšmo šaltinių nustatymą ir pašalinimą ir c) neprisijungus naudojamos saugyklos konfigūravimą per NFS, CIFS ar iSCSI.
- Dešimties (10) naudojimo atvejų ir dviejų (2) programų diegimą iš „IBM QRadar App Exchange“, aprašyto sprendimo architektūros dokumente.

### 1.3.4 „IBM QRadar on Cloud Custom Parser Service“

Teikiant šią paslaugą, bus sukurtas vienas pasirinktinis analizatorius / „uDSM“, kuris palaikys Kliento nestandartinius žurnalų šaltinių, siunčiamų į „Cloud Service“, tipus. Paslauga apima tokias užduotis:

- pasirinktinio analizatoriaus sukūrimas vienam nestandartiniam žurnalo šaltinio tipui (darbas atliekamas nuotoliniu būdu);
- „uDSM“ kūrimas, konfigūravimas ir susiejimas;
- pasirinktinio „uDSM“ diegimas ir tikrinimas bei
- iki dvidešimt penkių pranešimų tipų viename žurnalo šaltinyje analizavimas.

## 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) duomenu 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, jei (ir tik tokia apimtimi) Turinyje esantiems asmens duomenims taikomas Europos Bendrasis duomenų apsaugos reglamentas (ES/2016/679) (GDPR).

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=FB0F42F0750011E6865BC3F213DB63F7

# 3. Paslaugos lygiai ir techninis palaikymas

## 3.1 Paslaugos lygio sutartis

IBM pateikia 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 Neveikiančios paslaugos minučių skaičių sutartinį mėnesį, gautą rezultatą padalijus iš bendro minučių skaičiaus sutartinį mėnesį. Neveikiančios paslaugos apibrėžimas, pretenzijos pateikimo procesas ir informacija, kaip susisiekti su IBM dėl paslaugos pasiekiamumo problemų, pateikiama IBM „SaaS“ palaikymo apžvalgoje, kurią galima rasti adresu 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 – tai sutarta mėnesio kaina, dėl kurios teikiama pretenzija.

## 3.2 Techninė pagalba

„Cloud Service“ techninis palaikymas, įskaitant palaikymo centro kontaktinę informaciją, palaikymo teikimo valandas, atsakymo laiką ir kitą su palaikymu susijusią informaciją bei procesus, galima rasti IBM palaikymo vadove, pateikiamame adresu https://www.ibm.com/support/home/pages/support-guide/, pasirinkus „Cloud Service“.

# 4. Mokesčiai

## 4.1 Mokesčio apskaičiavimas

„Cloud Service“ mokesčio apskaičiavimas nurodytas Operacijų dokumente.

Šiai „Cloud Service“ taikomas toliau aprašytas mokesčio apskaičiavimas.

- Įsipareigojimas yra profesionali arba mokymo paslauga, susijusi su „Cloud Services“.
- Įvykis per sekundę yra konkrečių įvykių, kuriuos apdoroja „Cloud Service“ arba kurie susiję su „Cloud Service“ naudojimu, skaičius per sekundę.
- Srautai per minutę yra srautų, kuriuos valdo arba apdoroja „Cloud Service“, skaičius per minutę. Srautas yra ryšių tarp dviejų pagrindinių kompiuterių įrašas. Paketai, kuriuose yra tas pats šaltinio IP, paskirties IP, šaltinio prievadas, paskirties prievadas ir protokolas, sujungiami į vieną Srauto įrašą.
- Turtas – tai unikaliai identifikuojamas „Cloud Service“ pasiekiamas ar valdytinas materialusis išteklius arba vertę turintis daiktas.

# 5. Papildomos sąlygos

„Cloud Service“ sutartims (arba atitinkamoms pagrindinėms debesies sutartims) įvykdytoms 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:

- Duomenų šliuzas – Klientas gali diegti ir naudoti daugiausia dešimt (10) Duomenų šliuzo kopijų.

# 6. Pagrindinės sąlygos

## 6.1 Saugos duomenų naudojimas

Toliau išdėstytos sąlygos turi aukštesnę galią nei bet kurios, prieštaraujančios bazinių „Cloud Service“ sąlygų Turinio ir duomenų apsaugos skyriaus sąlygoms tarp šalių: IBM gali rinkti potencialios kenkėjiškos veiklos indikatorius Kliento turinyje, kad galėtų naudoti juos gynybos nuo kibernetinių atakų įžvalgų kontekste, ypač URL, IP adresus, domenus ir failų maišas. IBM, savo ruožtu, gali pranešti Klientui, jei jam kyla didesnė kibernetinių atakų grėsmė.