„IBM Resilient Security Orchestration, Automation and Response on Cloud“

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

1. „Cloud Service“

„IBM Resilient Security Orchestration, Automation, and Response (SOAR) Platform on Cloud“ leidžia organizacijoms organizuoti ir automatizuoti su reagavimu į incidentą susijusius žmones, procesus ir technologiją.

„IBM Resilient SOAR Platform on Cloud“ racionalizuoja reagavimą į incidentą ir privatumo atsakymų valdymą, siekiant užtikrinti automatizuotą, spartesnį ir lankstesnį būdą organizacijoms reaguoti į įvykius ir incidentus. „Resilient SOAR Platform on Cloud“ suteikia pagrindą sėkmingai kibernetinei apsaugai, kuri leidžia organizacijoms:

- Kurti reagavimo planus, pagrįstus pramonės standartais ir geriausiomis praktikomis.
- Lengviau integruoti su saugos ir IT įrankiais, organizuoti reagavimą į įvykius ir incidentus.
- Bendradarbiauti organizacijoje, suteikiant įvairiems suinteresuotiesiems asmenims įrankius, skirtus savo vaidmenims ir užduotims atlikti, reaguojant į incidentus.

„IBM Resilient SOAR Platform“ skirta įvairaus dydžio ir sudėtingumo organizacijoms ir ją galima įsigyti su keliais pasirenkamais priedais. Klientui draudžiama naudoti galimybes, jei nenurodytos jų įsigytame pasiūlyme arba priede.

1.1 Pasiūlymai

Klientas gali rinktis iš toliau nurodytų galimų pasiūlymų.

1.1.1 „IBM Resilient SOAR Platform on Cloud“

„IBM Resilient SOAR Platform on Cloud Orchestration“ suteikia kibernetinės apsaugos pagrindą. Klientai gali kurti reagavimo planus, pagrįstus pramonės standartais ir geriausiomis praktikomis, lengvai integruoti su saugos ir IT įrankiais bei organizuoti reagavimą į įvykius ir incidentus. „Cloud Service“ palengvina bendradarbiavimą visoje organizacijoje, leidžia įvairiems dalyviams imtis savo vaidmens ir užduočių, kaip reagavimo į incidentą darbo dalį.

Saugos komandos gali bendradarbiauti reaguodamos į kibernetinės saugos įvykius ir incidentus, naudojant platformos specialiai sukurtas atvejo valdymo galimybes. „Dynamic Playbooks“ prisitaiko prie sparčiai kintančių atakų, o komandos gali greitai pakartoti procesus, kad pagerintų efektyvumą tinkant taisykles, duomenų laukus ir rodymo maketus. Modeliavimai padeda nuolat tobulinti reagavimo procesus. Įdėtieji ir diegiamieji integravimai leidžia papildyti duomenis renkant turinį, skirta saugos komandai priimti sprendimus ir organizuoti taisymo veiksmus, atsižvelgiant į įsigytų Veiksmų per mėnesį kiekį. El. pašto įdėjimas ir analizavimas leidžia lengvai eskaluoti iš kitų įrankių. Prieigą galima apsaugoti SAML autentifikavimu. Skaidrumo ir rizikos analizei padeda analizė ir ataskaitų teikimas. Šis pasiūlymas reikalingas visiems kitiems toliau nurodytiems priedams.

1.2 Pasirinktinės paslaugos

1.2.1 „IBM Resilient SOAR Platform Actions on Cloud“

„IBM Resilient SOAR Platform on Cloud Actions“ suteikia platformos organizavimo galimybes. Įdėtieji ir diegiamieji integravimai, įskaitant integravimus su įvairiomis grėsmių žvalgymo informacinėmis priemonėmis, užtikrina automatizuotą papildymą renkant turinį, skirtą saugos komandai priimti sprendimus ir organizuoti taisymo veiksmus.

1.2.2 „IBM Resilient SOAR Platform on Cloud Privacy“ priedas

„IBM Resilient SOAR Platform on Cloud Privacy“ leidžia Klientui įvertinti privatumo duomenų pažeidimus ir į juos reaguoti. Šio pasiūlymo sugeneruoti reagavimo planai pritaikomi pagal duomenų tipus, įrašų kiekius ir taikomas reguliavimo jurisdikcijas. Be to, Klientai gali pasiekti pasaulinių pranešimų apie

duomenų privatumo pažeidimus nuostatų įdėtąją žinių bazę, padedančią dar geriau pritaikyti reagavimo į incidentus planus.

1.2.3 „IBM Resilient SOAR Platform on Cloud Team Management“ priedas

„IBM Resilient SOAR Platform on Cloud Teams“ užtikrina kelių komandų vartotojų valdymą ir duomenų segregavimą. Slapta informacija laikoma taip, kad būtų pasiekiama tik tiems, kam reikia, apribojant prieigą prie darbo vietomis ir naudojant tinkamą vaidmenimis pagrįstą prieigos kontrolę. Vartotojų ir grupės valdymą galima supaprastinti vartotojo autorizavimui naudojant „Active Directory“. Be to, atskiras grupes galima konfigūruoti turėti savo Organizaciją.

1.2.4 „IBM Resilient SOAR Platform on Cloud MSSP“ priedas

„IBM Resilient SOAR Platform on Cloud MSSP“ suteikia atvejų valdymo, apdorojimo, tinkinimo ir instrukcijų valdymo galimybes keliose Organizacijose. Įvykius ir incidentus keliose Organizacijose galima peržiūrėti vienoje užklausoje, teikiant valdomos saugos paslaugos teikėjo (MSSP) analitikui išsamų vaizdą apie jo klientus. Instrukcijos su kiekvienos Organizacijos konfigūracija leidžia paprastai valdyti tiek standartizuotus, tiek tinkintus procesus.

1.2.5 „IBM Resilient SOAR Platform on Cloud Non-Production“ priedas

„IBM Resilient SOAR Platform on Cloud Non-Production“ yra atskiras „IBM Resilient SOAR 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.

1.3 Akceleravimo paslaugos

„IBM Security Expert Labs (SEL) for Resilient Services“ pasiūlymai yra nuotoliniu būdu teikiamos paslaugos, kuriomis skiriamas „Resilient“ eksperto laikas su „Resilient“ diegimu susijusioms architektūriniams ir diegimo konsultacijoms teikti. Bet kokių tokių Paslaugų būtinoji sąlyga yra „IBM Resilient Security, Orchestration and Response“ pasiūlymas, teikiamas kaip „Cloud Service“ arba kaip vietinė programinė įranga.

1.3.1 „IBM SEL for Resilient Base Starter Service“

IBM įsipareigoja per 5 dienas nuotoliniu būdu:

- padėti apibrėžti „IBM Security Resilient“ architektūrą;
- pateikti įdiegtą ir sukonfigūruotą „IBM Security Resilient“ (kai taikoma);
- surengti Analitikams ir Dizaineriams mokymą, kaip konfigūruoti ir naudoti Kliento turimus „Incident Response“ planus, atsižvelgiant į Kliento organizacijos pagrindinius reikalavimus;
- pateikti „IBM Security Resilient“ pagal Kliento organizacijų unikalius procesu sukonfigūruotas Instrukcijas;
- parodyti, kaip sekti apibrėžtus KPI ir Metriką, atsižvelgiant į Kliento organizacijų poreikius bei geriausią rinkos praktiką, ir
- nurodyti integravimo galimybes, kurios padėtų palaikyti, automatizuoti ir organizuoti visą procesą.

1.3.2 „IBM SEL for Resilient Premium Starter Service“

IBM įsipareigoja per 3 dienas nuotoliniu būdu:

- padėti apibrėžti „IBM Security Resilient“ architektūrą;
- įdiegti „IBM Security Resilient“ (kai taikoma);
- pirmą kartą sukonfigūruoti „IBM Security Resilient“ Kliento aplinkoje ir
- surengti Analitikams ir Dizaineriams mokymą, kaip konfigūruoti ir naudoti Kliento turimus „Incident Response“ planus, atsižvelgiant į jo organizacijos pagrindinius reikalavimus.

1.3.3 „IBM SEL for Resilient Additional Day“

Be „Base Starter Service“ ar „Premium Starter Service“ IBM nuotoliniu būdu atliks bet kokią 1 dienos su „IBM Security Resilient“ susijusią veiklą, dėl kurios buvo susitarta iš anksto. Pavyzdžiui:

- suteiks papildomą „IBM Security Resilient“ ar plėtinių (jei taikoma) diegimo arba konfigūravimo palaikymą;

- papildomai mokys Analitikus arba teiks jiems pagalbą, kad užtikrintų pasirengimą naudoti „IBM Security Resilient“ kaip Kliento pagrindinį SOAR sprendimą;
- instruktuos Dizainerius, kaip konfigūruoti ir naudoti savo Instrukcijas, kuriose atsispindėtų Kliento organizacijų pagrindiniai reikalavimai, arba
- atliks greitą „IBM Security Resilient“ aplinkos įvertinimą, kad galėtų rekomenduoti potencialias tobulintinas sritis.

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=A47500205B1911E6865BC3F213DB63F7

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.

- 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 „Cloud Services“.
- Lygiagretusis vartotojas – tai vartotojas, kuris vienu metu bet kokiu tiesioginiu arba netiesioginiu būdu (pavyzdžiui, naudodami tankinimo programą, įrenginį arba taikomųjų programų serverį) ir bet

kokiomis priemonėmis naudoja prieigą prie „Cloud Service“. Asmuo, kuris vienu metu naudojasi prieiga prie „Cloud Service“ kelis kartus, skaičiuojamas kaip vienas Lygiagretusis vartotojas.

- „Engagement“ yra profesionali arba mokymo paslauga, susijusi su „Cloud Services“.
- Elementas yra konkretaus elemento, kurį valdo ar apdoroja „Cloud Service“ arba kuris susijęs su jos naudojimu, atvejis. Šioje „Cloud Service“ Elementas yra Veiksmas. Veiksmas – „Cloud Service“ operacijų išdėstymas arba automatizavimo užklausos pateikimas kitai programinės įrangos programai.

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 Patikrinimas

Klientas i) palaikys ir gavęs prašymą teiks įrašus ir sistemos įrankių išvestį, kai tai pagrįstai bus reikalinga IBM ir jos nepriklausomam auditoriui, kad patikrintų, kaip Klientas laikosi šios Sutarties sąlygų, ir ii) nedelsdamas užsakys bei apmokės visas reikiamas teises pagal tuo metu IBM galiojančius tarifus ir kitus tokio patikrinimo metu nustatytus mokesčius bei prievoles, nurodytas IBM sąskaitoje faktūroje. Šie sąlygų laikymosi patikrinimo įsipareigojimai galioja „Cloud Service“ laikotarpį ir dvejus metus po jo.

5.2 Priedo papildomų teisių reikalavimas

Klientas privalo įsigyti vienodą skaičių tokio paties tipo tiek bazinių „Cloud Service“, tiek „Cloud Service“ Priedų.

5.3 Naudojimo apribojimai

Kiekvienas Klientas turi teisę pateikti daugiausia šimtą tūkstančių (100 000) Grėsmių paslaugos užklausų per mėnesį. Klientas sukuria Grėsmių paslaugos užklausą įtraukdamas į incidentą artefaktą, kai suaktyvinama jo Grėsmių paslauga. Po to dvi (2) dienas, kol incidentas atidarytas ir aktyvus, bus automatiškai generuojama nauja Grėsmių paslaugos užklausa.

Kiekvienas Klientas turi teisę sugeneruoti daugiausia šimtą (100) el. pašto pranešimų per dieną vienam Įgaliotajam / Lygiagrečiajam vartotojui. El. pašto pranešimus generuoja „Resilient“ platforma pagal Kliento valdomą konfigūraciją.

5.4 Papildoma duomenų apdorojimo ir apsaugos informacija

Kad būtų išvengta abejonių, „IBM Resilient SOAR Platform on Cloud“:

- nešifruoja neaktyvaus Turinio;
- nėra skirta jokių specialiųjų kategorijų asmens duomenims tvarkyti;
- tuščiuose teksto laukuose neturėtų įvesti jokių asmens duomenų, jei to neprašoma.

Išsami informacija apie šifravimą ir apdorojamų Asmens duomenų tipus pateikiama 2 skyriuje minimo Duomenų lapo URL adresu.

6. Pagrindinės sąlygos

6.1 Duomenų naudojimas

IBM nenaudos arba neatskleis rezultatų, gautų Klientui naudojant „Cloud Service“, 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.