

IBM QRadar Advisor with Watson

Ta opis storitve opisuje storitve, ki jih IBM zagotavlja naročniku. Naročnik pomeni in vključuje podjetje in njegove pooblaščen uporabnike ali prejemnike storitve v oblaku. Veljavna ponudba in dokazilo o upravičenosti sta zagotovljena v obliki ločenih transakcijskih dokumentov.

1. Storitev v oblaku

1.1 IBM QRadar Advisor with Watson Service

IBM QRadar Advisor with Watson razširja kognitivno analitiko v platformo QRadar Security Platform, pri čemer naročnikom in varnostnim analitikom omogoča hitro raziskovanje in odzivanje na grožnje. Uporablja obsežno znanje storitve Watson for Cyber Security ter nestrukturirane podatke (vključno z varnostnimi spletnimi mesti in raziskovalnimi študijami) in vzpostavlja povezave z incidenti, povezanimi z lokalno varnostjo. Na ta način lahko pomaga pri odkrivanju skritih groženj ter avtomatizira vpogleda, na podlagi katerih omogoči hitrejše odzivanje in izboljšano odločanje. QRadar Advisor with Watsono varnostnim analitikom omogoča pošiljanje dejanj, ki ogrožajo varnost, v storitev Watson, v kateri se s pomočjo baze znanja, ki vključuje več sto tisoč nestrukturiranih in strukturiranih podatkovnih virov, izvede odkrivanje grožnje, vpogled pa je nato preslikan nazaj v entiteto grožnje, povezano z izvornim dejanjem, ki ogroža varnost, kot so zlonamerne datoteke, sumljivi naslovi IP, tuje entitete ter razmerja med njimi. To je lahko še posebej koristno pri določanju, ali je dejanje, ki ogroža varnost, povezano z znano zlonamerno programsko opremo. Če je tako, potem storitev Watson poleg drugih vpogledov zagotovi ozadje za uporabljeno zlonamerno programsko opremo, uporabljene ranljivosti in obseg grožnje (vključno z dodatnimi potencialno ogroženimi končnimi točkami).

Storitev v oblaku od naročnika zahteva aktivno namestitev storitve IBM Security QRadar ter namestitev kode za omogočanje storitve v oblaku v tej namestitvi, da lahko naročnik dostopa do njenih funkcij. Storitev v oblaku vključuje 'mehko omejitev' za število poizvedb, povezanih z dejanji, ki ogrožajo varnosti, ki jih lahko naročnik pošlje v storitev v oblaku, in sicer petnajst (15) zahtev na dan na 1000 dogodkov na sekundo, za katere ima naročnik pooblastila. Poizvedbe, poslane zunaj tega obsega, bo storitev v oblaku sicer še vedno obdelala, vendar ne bodo imele enake visoke prednosti ter bodo vrnjene počasneje.

1.2 IBM QRadar Advisor with Watson Trial

IBM QRadar Advisor with Watson Trial ("preskusna storitev v oblaku") zagotavlja funkcije storitve IBM QRadar Advisor with Watson v obliki preskusne različice. Naročnikov dostop do preskusne storitve v oblaku je omejen na časovno obdobje, navedeno v transakcijskem dokumentu ali drugem dokumentu, pri čemer bo naročnikov dostop po preteku tega obdobja onemogočen. Naročnik lahko tekom preskusnega obdobja pošlje le največ 5 poizvedb, povezanih z dejanji, ki ogrožajo varnost. Preskusna storitev v oblaku je zagotovljena brez jamstva ter 'takšna, kot je', in naročnik jo lahko uporablja samo za notranje testiranje in neprodukcijsko uporabo. Odzivni časi na poizvedbe tekom preskusnega obdobja se lahko razlikujejo glede na trenutne ravni prometa.

2. Opis varnosti

Te storitev v oblaku so v skladu z IBM-ovimi načeli glede zaščite podatkov in zasebnosti za IBM-ovo programsko opremo kot storitev, ki so na voljo na spletnem mestu <http://www-03.ibm.com/software/sla/slabd.nsf/sla/dsp>, in vsemi drugimi določili v tem razdelku. Morebitne spremembe IBM-ovih načel glede zaščite podatkov in zasebnosti ne bodo zmanjšale stopnje varnosti storitev v oblaku.

Te storitve v oblaku se lahko uporabljajo za obdelavo izbrane vsebine z osebnimi podatki, če naročnik kot upravljavec podatkov presodi, da so tehnični in organizacijski varnostni ukrepi ustrezni glede na tveganje, ki ga predstavljata obdelava in vrsta podatkov, ki jih je treba zaščititi. Naročnik se zaveda, da te storitev v oblaku ne ponujajo funkcij za zaščito občutljivih osebnih podatkov ali podatkov, za katere veljajo dodatne regulativne zahteve. Naročnik potrjuje, da IBM ni seznanjen z vrstami podatkov, ki so vključeni v vsebino, in ne more oceniti ustreznosti storitev v oblaku ali zagotovljenih varnostnih ukrepov.

Storitev v oblaku omogoča naročniku vnos in upravljanje samo naslednje vsebine, ki morda vsebuje podatke, ki se lahko na podlagi veljavne zakonodaje o zasebnosti štejejo kot osebni podatki ("OP"):

- Ciljni/izvorni naslovi IP
- URL-ji
- Domene
- Razprševanje datotek

2.1 Varnostne funkcije in dolžnosti

Storitve v oblaku vključujejo naslednje varnostne funkcije:

Storitve v oblaku šifrirajo vsebino med prenosom podatkov med IBM-ovim omrežjem in naročnikovo nameščeno storitvijo IBM Security QRadar. Storitve v oblaku v času mirovanja ob čakanju na prenos podatkov vsebine ne šifrirajo.

Storitev v oblaku ne vzdržuje niti ne vztraja pri vhodni vsebini, ko je že izvedla svojo funkcijo v zvezi s temi podatki.

3. Tehnična podpora

Tehnična podpora za storitve v oblaku je na voljo prek e-pošte, spletnih forumov in spletnega sistema za poročanje o težavah, kot je opisano spodaj. Tehnična podpora je zagotovljena v okviru storitve v oblaku in ni na voljo kot ločena ponudba.

Resnost	Definicija resnosti	Ciljni odzivni čas	Kritje odzivnega časa
1	Odločilen vpliv na poslovanje/izpad storitve: Nedelovanje funkcije, ki je kritičnega pomena za poslovanje, ali izpad kritičnega vmesnika. To običajno velja za produkcijsko okolje in pomeni nezmožnost dostopanja do storitev, kar ima odločilen vpliv na delovanje. To stanje zahteva takojšnjo rešitev.	V roku 1 ure	24 ur na dan, 7 dni v tednu
2	Velik vpliv na poslovanje: Uporaba poslovne lastnosti ali funkcije storitve je zelo omejena oz. za naročnika obstaja nevarnost, da bo zamudil poslovne roke.	V roku 2 delovnih ur	Delovni čas od ponedeljka do petka
3	Manjši vpliv na poslovanje: Označuje, da je storitev ali funkcijo mogoče uporabljati in nima odločilnega vpliva na delovanje.	V roku 4 delovnih ur	Delovni čas od ponedeljka do petka)
4	Minimalen vpliv na poslovanje: Poizvedba ali netehnična zahteva.	V roku 1 delovnega dne	Delovni čas od ponedeljka do petka

Za naročnike, ki so sodelovali pri beta izdaji storitve v oblaku in še vedno uporabljajo različico 7.2.7 storitve QRadar Platform, nekaterih težav s tehnično podporo morda ne bo mogoče odpraviti. Ti naročniki bodo morali izvesti nadgradnjo na različico 7.2.8 in namestiti najnovejši popravek, da bodo lahko prejeli polno tehnično podporo.

4. Pooblastila in zaračunavanje

4.1 Metrike zaračunavanja

Storitev v oblaku je na voljo na podlagi naslednje metrike zaračunavanja, ki je določena v transakcijskem dokumentu:

- 100 dogodkov na sekundo** - je merska enota, na podlagi katere je mogoče pridobiti storitve v oblaku. Dogodek je pojavitev posebnega dogodka, ki ga obdela storitev v oblaku ali je povezan z njeno uporabo. Naročnik mora pridobiti zadostna pooblastila, da z njimi pokrije število dogodkov na sekundo, zaokroženo na najbližjo stotico, ki se zgodijo v meritvenem obdobju, navedenem v naročnikovem dokazilu o upravičenosti ali transakcijskem dokumentu.

5. Obdobje trajanja in možnosti podaljšanja

Obdobje trajanja storitev v oblaku se začne z dnem, ko IBM naročnika obvesti, da ima dostop do storitev v oblaku, navedene v dokazilu o upravičenosti. V dokazilu o upravičenosti bo navedeno, ali se storitve v oblaku podaljšajo samodejno, se nadaljujejo na podlagi neprekinjene uporabe ali se končajo ob izteku naročniškega obdobja.

Na podlagi samodejnega podaljšanja se bo naročnina na storitev v oblaku samodejno podaljševala v okviru naročniškega obdobja, navedenega v dokazilu o upravičenosti, razen če naročnik posreduje pisno obvestilo o prenehanju podaljšanja najmanj 90 dni pred iztekom naročniškega obdobja.

Na podlagi neprekinjene uporabe bo storitev v oblaku neprestano na voljo iz meseca v mesec, dokler naročnik ne posreduje pisnega obvestila o odpovedi z 90-dnevnim odpovednim rokom. Po izteku takega 90-dnevnega obdobja bo storitev v oblaku na voljo še do konca koledarskega meseca.

6. Podporna programska oprema.

Storitve v oblaku zahtevajo uporabo podporne programske opreme, ki jo naročnik prenese v svoje sisteme, da omogoči uporabo storitev v oblaku. Naročnik lahko podporno programsko opremo uporablja samo v povezavi z uporabo storitev v oblaku. Podporna programska oprema je zagotovljena "TAKŠNA, KOT JE".

Naročnik lahko podporno programsko opremo za storitev v oblaku prenese iz storitve IBM Security App Exchange na spletnem mestu <https://exchange.xforce.ibmcloud.com/hub>.

7. Dodatni pogoji

7.1 Splošno

Naročnik soglaša, da ga lahko IBM v oglaševalskih ali tržnih komunikacijah javno imenuje kot naročnika na storitve v oblaku.

7.2 Podporna programska oprema.

Storitve v oblaku zahtevajo uporabo podporne programske opreme, ki jo naročnik prenese v svoje sisteme, da omogoči uporabo storitev v oblaku. Naročnik lahko podporno programsko opremo uporablja samo v povezavi z uporabo storitev v oblaku. Podporna programska oprema je zagotovljena "TAKŠNA, KOT JE".

Naročnik lahko podporno programsko opremo za storitev v oblaku prenese iz storitve IBM Security App Exchange na spletnem mestu <https://exchange.xforce.ibmcloud.com/hub>.

7.3 Zakonita uporaba storitve v oblaku

Storitev v oblaku je zasnovan tako, da pomaga naročniku izboljšati svoje varnostno okolje in podatke. Za uporabo storitve v oblaku lahko veljajo različni zakoni in predpisi, vključno s tistimi glede zasebnosti, zaščite podatkov, zaposlitve in elektronske komunikacije ter shranjevanja. Storitve v oblaku se lahko uporabljajo samo za zakonite namene in na zakonit način. Naročnik soglaša, da bo uporabljal storitev v oblaku na podlagi veljavnih zakonov, predpisov in pravilnikov, pri čemer prevzema vso odgovornost za njihovo upoštevanje. Naročnik izjavlja, da bo/je pridobil vsa soglasja, dovoljenja ali licence, ki jih potrebuje za zakonito uporabo storitve v oblaku.

7.4 Potek storitve v oblaku

Do poteka ali prenehanja storitve v oblaku lahko naročnik uporablja vse funkcije poročanja ali izvoza storitve v oblaku za izvlačenje podatkov.

7.5 Varnostni podatki

Kot del storitev v oblaku, ki vključujejo poročanje, bo IBM pripravil in hranil anonimizirane in/ali združene podatke, zbrane iz storitev v oblaku ("varnostni podatki"). Varnostni podatki ne bodo razkrili identitete naročnika ali posameznikov, razen v primerih iz točke (d) spodaj. Naročnik prav tako soglaša, da IBM lahko uporabi in/ali kopira varnostne podatke le za naslednje namene:

- a. objavljanje in/ali distribucija varnostnih podatkov (npr. pri zbiranju in/ali analizi v povezavi s kibernetično varnostjo);
- b. razvijanje ali izboljševanje produktov ali storitev;
- c. izvajanje raziskav znotraj IBM-a ali v sodelovanju s tretjimi osebami; in
- d. zakonita skupna raba potrjenih podatkov o storilcu, ki je tretja oseba.