IBM QRadar Advisor with Watson

Ta opis storitve opisuje storitev v oblaku. Ustrezni dokumenti o naročilu nudijo cene in dodatne podrobnosti o naročnikovem naročilu.

1. Storitev v oblaku

IBM QRadar Advisor with Watson razširja kognitivno analitiko na QRadar Security Platform in naročnikom ter varnostnim analitikom pomaga pri preiskovanju in odzivanju 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. Tako lahko pomaga pri odkrivanju skritih groženj in avtomatizaciji vpogledov za boljše odzive in odločanje. QRadar Advisor with Watson 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 izvirnim 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).

1.1 Ponudbe

Naročnik lahko izbira med naslednjimi razpoložljivimi ponudbami.

1.1.1 IBM QRadar Advisor with Watson

Za IBM QRadar Advisor with Watson mora naročnik imeti aktivno razmestitev IBM QRadar, bodisi v lokalnem okolju na mestu uporabe bodisi v oblaku, in imeti nameščeno podporno programsko opremo storitve v oblaku v tej postavitvi, da lahko naročnik dostopa do njene funkcionalnosti. Ko je storitev v oblaku upravičena na podlagi dogodkov na sekundo, vsebuje omejitev poizvedb varnostnih prekrškov, ki jih lahko naročnik pošlje storitvi v oblaku s stopnjo 1,5 poizvedbe na dan na 100 dogodkov na sekundo (zaokroženo navzgor na najbližjo poizvedbo), do katerih je upravičen naročnik. Ko je storitev v oblaku upravičena na podlagi upravljanega navideznega strežnika (MVS), vsebuje omejitev števila poizvedb varnostnih prekrškov, ki jih lahko naročnik pošlje storitvi v oblaku s stopnjo 15 poizvedb na dan na 100 MVS, do katerih je upravičen naročnik. Poslanim poizvedbam, ki presegajo to omejitev, se zmanjša prioriteta in jih storitev v oblaku preostanek dneva ne bo obdelala.

1.1.2 IBM QRadar Advisor with Watson – Enterprise

IBM QRadar Advisor with Watson – Enterprise je najbolj primerna za razmestitve v velikih centrih za varnostne operacije (SOC), ki običajno presegajo dvesto petdeset tisoč dogodkov na sekundo ali več. Naročnik mora namestiti podporno programsko opremo storitve v oblaku v svojo ločeno pridobljeno razmestitev IBM QRadar za dostop do funkcionalnosti storitve v oblaku. IBM QRadar Advisor with Watson – Enterprise je na voljo na osnovi metrike zaračunavanja, ki temelji na primerku in ki ni odvisna od obsega naročnikove razmestitve IBM QRadar. Naročnik je v kateremkoli danem trenutku omejen na 25 poizvedb v čakalni vrsti.

1.1.3 IBM QRadar Advisor with Watson – Starter Pack

IBM QRadar Advisor with Watson – Starter Pack je namenjen uporabnikom, ki prvič uporabljajo QRadar Advisor with Watson. Ta storitev v oblaku ima polno funkcionalnost storitve QRadar Advisor with Watson, kot je opisana v zgornjem razdelku 1.1.1, vendar je na voljo samo kot naročnikov prvi nakup storitve QRadar Advisor with Watson, in se ne obnavlja.

1.2 Izbirne storitve

1.2.1 IBM QRadar Advisor with Watson – Test Environment

IBM QRadar Advisor with Watson – Test Environment je namenjena naročnikom, ki želijo razmestiti storitve v oblaku v svojem internem preizkusnem okolju, in jo je mogoče uporabiti samo za

neprodukcijske namene preizkušanja. IBM QRadar Advisor with Watson – Test Environment je treba dopolniti z naročnino na produkcijske storitve v oblaku.

1.3 Pospeševalne storitve

1.3.1 IBM QRadar Advisor with Watson Advanced Services

Za to naročniško storitev na daljavo bo IBM naročniku zagotavljal katero koli od naslednjih svetovalnih storitev za največ 5 dni v obdobju 1 leta:

- Ocena naročnikovega procesa SOC, vključno s procesom preiskovanja in/ali odzivanja na dogodke;
- Ponovna ocena odziva referenčnih naborov;
- Prilagajanje samodejne analize za prekrške velikih razsežnosti;
- Razvoj primerov uporabe;
- Zagotavljanje priporočil za spremembe procesa SOC, ki vključujejo QRadar Advisor with Watson;
- Podajanje navodil za čim bolj učinkovito razumevanje in vključevanje podatkov iz storitve QRadar Advisor with Watson v naročnikove obstoječe procese;
- Zagotavljanje prenosa znanja o relevantnih subjektih QRadar Advisor with Watson.

OPOMBA: v to storitev je na podlagi statusa naročnikove razmestitve QRadar mogoče vključiti naslednje dejavnosti:

- Izvajanje preverjanje zdravja naročnikove razmestitve QRadar;
- Izvajanje dodatnega uglaševanja obstoječe naročnikove razmestitve QRadar;
- Pomoč pri dodajanju dodatnih izvorov dnevnika v naročnikovo razmestitev QRadar.

1.3.2 IBM QRadar Advisor with Watson Basic Setup Service

Ta storitev nastavitve je storitev na daljavo in vključuje štirideset (40) ur strokovnih storitev, ki potečejo v devetdesetih (90) dneh od nakupa, če ni drugače navedeno, ne glede na to, ali so bile izkoriščene vse ure (če je primerno). Storitve bodo vključevale določenega vodjo sodelovanja z IBM, ki bo organiziral začetne klice.

IBM bo izvedel nekaj ali vse od spodaj naštetega:

- Ocena naročnikovega procesa SOC, vključno s procesom preiskovanja in/ali odzivanja na dogodke;
- Uvedba storitve QRadar Advisor with Watson v naročnikovo okolje:
    - Namestitev storitve Install QRadar Advisor with Watson;
    - Preslikava enotnih lastnosti v QRadar Advisor with Watson;
    - Uvedba odziva referenčnih naborov;
    - Prilagajanje samodejne analize za prekrške velikih razsežnosti;
    - Usmeritve glede navodil uporabe;
    - Zagotavljanje priporočil za spremembe procesa SOC, ki vključujejo QRadar Advisor with Watson.

1.3.3 IBM QRadar Advisor with Watson Quick Setup Service

Ta storitev nastavitve je namenjena naročnikom z manj kot 5000 dogodki na sekundo (EPS).

Za to storitev na daljavo bo IBM naročniku zagotavljal katero koli od naslednjih svetovalnih storitev (ali kombinacijo teh) za največ 16 ur v obdobju 90 dni:

- Namestitev QRadar Advisor with Watson.
- Upravljanje dovoljenj za QRadar Advisor with Watson.
- Konfiguracija QRadar Advisor with Watson, ki lahko vključuje:
    - konfiguracijo varnega strežnika proxy;
    - predložitev poverilnic X-Force za izmenjavo;
    - ustvarjanje avtoriziranih žetonov za storitev;
    - konfiguriranje načel zadržanja za shrambo rezultatov analiz;

- preslikavo lastnosti dogodkov po meri;
- izvoz referenčnih naborov;
- preslikavo obveščanja o grožnjah;
- konfiguracijo identifikacije sredstev;
- optimizacijo uporabe;

- samodejno preiskovanje prekrškov in rezultate (vsaj ena predstavitev primera uporabe).
- Raziskovanje vpogledov z grafikonom razmerij.

2. Podatkovni listi za obdelavo in varstvo podatkov

IBM-ov dodatek k obdelavi podatkov http://ibm.com/dpa (DPA) in podatkovni list za obdelavo in varstvo podatkov (podatkovni list) podajata dodatne informacije o varstvu podatkov za storitve v oblaku in možnosti v zvezi z vrstami vsebine, ki se lahko obdeluje, vključene dejavnosti obdelave, funkcije varstva podatkov in podrobnosti glede hrambe in vračila vsebine. DPA velja za osebne podatke, ki jih zajema vsebina, če in v obsegu, v katerem veljajo i) Splošna uredba EU o varstvu podatkov (EU/2016/679) (GDPR); ali ii) drugi zakoni o varstvu podatkov, navedeni na spletni strani http://ibm.com/dpa/dpl.

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

3. Ravni storitve in tehnična podpora

3.1 Pogodba o ravni storitev

IBM naročniku zagotavlja naslednjo pogodbo o ravni storitev za razpoložljivost (SLA). IBM bo priznal najvišje veljavno nadomestilo na podlagi zbirne razpoložljivosti storitve v oblaku, kot je prikazano v spodnji tabeli. Razpoložljivost, izražena v odstotkih, se izračuna kot skupno število minut v pogodbenem mesecu, zmanjšano za skupno število minut nerazpoložljivosti v pogodbenem mesecu, deljeno s skupnim številom minut v pogodbenem mesecu. Definicija nerazpoložljivosti storitve, postopek pritožbe in kako kontaktirati IBM v zvezi z razpoložljivostjo storitve, so v IBM-ovem pregledu podpore za storitev v oblaku na naslovu https://www.ibm.com/software/support/saas_support_overview.html.

Razpoložljivost	Dobropis (% mesečne naročnine*)
Manj kot 99,9 %	2 %
Manj kot 99,0 %	5 %
Manj kot 95,0 %	10 %

* Naročnina je pogodbena cena za mesec, na katerega se nanaša zahtevek.

3.2 Tehnična podpora

Tehnično podporo za storitev v oblaku, vključno s kontaktnimi podatki podpore, stopnjami resnosti, časom razpoložljivosti podpore, odzivnim časom in drugimi informacijami ter procesi naročnik najde tako, da izbere storitev v oblaku v storitvi IBM Support, ki je na voljo na https://www.ibm.com/support/home/pages/support-guide/.

4. Stroški

4.1 Metrike zaračunavanja

Metrike zaračunavanja za storitev v oblaku so podane v transakcijskem dokumentu.

Za to storitev v oblaku se uporabljajo naslednje metrike zaračunavanja:

- Dogodek na sekundo (EPS) je pojav določenega EPS-ja, ki ga obdelajo storitve v oblaku ali je povezan z uporabo teh storitev. Za namen te storitve v oblaku so dogodki na sekundo tisti dogodki, ki jih zbere in obdeluje naročnikova razmestitev IBM QRadar.
- Primerek je vsak dostop do določene konfiguracije storitev v oblaku.
- Engagement je profesionalna ali izobraževalna storitev, povezana s storitvijo v oblaku.

- Upravljani navidezni strežnik je sestavljen iz procesnih enot, zmožnosti pomnilnika in vhodnih/izhodnih zmožnosti, ki izvajajo zahtevane postopke, ukaze ali aplikacije, ki jih upravljajo storitve v oblaku.

5. Dodatna določila

Za pogodbe o storitvi v oblaku (ali enakovredne osnovne pogodbe), podpisane pred 1. januarjem 2019, veljajo pogoji, ki so na voljo na https://www.ibm.com/acs.

5.1 Podporna programska oprema

Storitev v oblaku vsebuje naslednjo podporno programsko opremo:

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

5.2 Zakonita uporaba storitev 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 o zasebnosti, varstvu podatkov, zaposlovanju in elektronskih komunikacijah ter shranjevanju. 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.

6. Prevladujoče določbe

6.1 Uporaba podatkov

Naslednje prevlada pri morebitnih nasprotnih določbah v razdelku o vsebini in varstvu podatkov osnovnih pogojev za storitev v oblaku med pogodbenima strankama: IBM ne bo uporabil ali razkril rezultatov, ki izhajajo iz naročnikove uporabe storitve v oblaku in so edinstveni za naročnikovo vsebino (vpogledi) oziroma na kak drug način identificirajo naročnika. IBM pa bo vsebino in druge informacije, ki izhajajo iz vsebine (razen za vpoglede), uporabil kot del storitve v oblaku za namen izboljšanja storitve v oblaku. Prav tako lahko IBM deli identifikatorje groženj in druge varnostne podatke, vdelane v vsebino, za namene zaznavanja groženj in varovanja.