IBM QRadar on Cloud

Ta opis storitve opisuje storitev v oblaku. V ustreznih dokumentih o naročilu so navedene cene in dodatne podrobnosti o naročnikovem naročilu.

1. Storitev v oblaku

1.1 IBM QRadar on Cloud

Naročnik lahko izbira med naslednjimi razpoložljivimi ponudbami.

1.1.1 IBM QRadar on Cloud 100 EPS

Ponudba IBM QRadar on Cloud dostavlja napredno rešitev varnostnega obveščanja iz IBM-ovega oblaka na podlagi produkta IBM Security QRadar SIEM. Naročniku omogoča zbiranje, povezovanje in shranjevanje dogodkov, generiranih na mestu uporabe in v okoljih v oblaku, ter izvajanje upravljanja varnosti in tveganj, kot bi to dosegli z razmestitvijo produkta QRadar SIEM na mestu uporabe. Kot del te ponudbe IBM zagotavlja tudi nadzorovanje infrastrukture 24 ur na dan, 7 dni na teden in uveljavlja najnovejše popravke ravni programske opreme oziroma kritične popravke kadarkoli so na voljo.

Te storitve v oblaku vključujejo devetdeset (90) dni aktivne shrambe, ki omogoča iskanje.

1.2 Izbirne storitve

1.2.1 IBM QRadar on Cloud 1K EPS Temporary Upgrade

Nadgradnja storitve, ki zagotavlja zmogljivost dodatnih 1000 enot EPS za zbiranje in obdelavo dogodkov dnevnikov, vendar zgolj za začasno število mesecev. Naročnik lahko kupi več enot te nadgradnje, do največje stopnje EPS, ki jo ponudba lahko podpira. Namen tega dela je omogočiti naročniku, ki potrebuje kritje priložnosti med letom, ko poskoči uporaba, da lahko izpolni te zahteve z začasno nadgradnjo zmogljivosti. Ob koncu trajanja obdobja bo ta količina začasnega povečanja zmogljivosti odstranjena iz naročnikovega okolja.

1.2.2 IBM QRadar on Cloud Data Storage 100 EPS

Nadgradnja shrambe podatkov doda dodatni prostor za shranjevanje in razširi obdobje analize. Ta nadgradnja kapacitete naročnikom zagotavlja shranjene podatke za vsako kupljeno nadgradnjo 100 EPS za do 1 polno leto.

1.2.3 IBM QRadar on Cloud Flows Add-On

Omogoča integracijo z IBM QRadar SIEM in procesorji toka, kar zagotavlja vidnost 3. omrežne plasti in analizo toka, ki sta naročniku v pomoč pri zaznavanju, odkrivanju in odzivanju na dejavnosti v njegovem celotnem omrežju.

1.2.4 IBM QRadar on Cloud Vulnerability Management Add-On

Samodejno zazna in prepozna varnostne pomanjkljivosti omrežne naprave in aplikacije, doda kontekst in podpira prednostno obravnavo dejavnosti za odpravo ranljivosti in ublažitev.

1.2.5 IBM QRadar on Cloud Log Archival

Naročniku v naročniškem obdobju omogoča arhiviranje podatkov dogodka iz storitev v oblaku. IBM bo v sodelovanju z naročnikom napisal določene dogodke za shrambo objektov za arhivske namene. Na naročnikovo zahtevo bo IBM v roku treh (3) delovnih dni od prejema zahteve, ponovno vpel za do trideset (30) dni arhiviranih podatkov dogodka v naročnikov primerek storitev v oblaku. Ti podatki bodo naročniku na voljo 48 ur, nato pa bodo vrnjeni v arhivsko shrambo objektov. Naročnik lahko vsake tri mesece poda največ dve takšni zahtevi. Ta nadgradnja kapacitete naročnikom zagotavlja shranjene podatke za vsako kupljeno nadgradnjo 100 EPS za do 1 polno leto.

1.3 Acceleration Services

1.3.1 IBM QRadar on Cloud Optimization Service

Za to naročniško storitev na daljavo bo IBM organiziral sestanek z naročnikom, da ocenita trenutno stanje naročnikovega primerka storitev v oblaku, rezultate pa bo naročniku posredoval s poročilom QRadar on Cloud Health Status, ki bo navajalo področja, potrebna izboljšav, če obstajajo.

Poleg tega bo na naročnikovo zahtevo IBM naročniku v obdobju enega leta zagotovil do osem (8) dni katere koli od naslednjih svetovalnih storitev:

- Pomoč pri dodajanju dodatnih virov dnevnika storitvam v oblaku;
- Konfiguriranje dodatnih iskanj, poročil in nadzornih plošč;
- Izvedba dodatnega uglaševanja obstoječe namestitve QRadar in
- Zagotavljanje prenosa znanja o relevantnih zadevah v zvezi s QRadar.

1.3.2 Storitve nastavitve

Naslednje storitve nastavitve se zagotavljajo na daljavo in jih je mogoče naročiti posebej. Vsaka naročena storitev bo potekla (90) dni po nakupu, razen če je navedeno drugače, ne glede na to, ali so bile porabljene vse ure (če je ustrezno). Storitve bodo vključevale določenega vodjo sodelovanja z IBM, ki bo organiziral začetne klice.

1.3.3 IBM QRadar on Cloud Deployment Service

Ta storitev zagotavlja štirideset (40) ur strokovnih storitev, v okviru katerih bo IBM izvedel vse ali nekaj od naslednjega:

IBM bo opravil pregled arhitekture SIEM, ki bo trajal do šestnajst ur in v okviru katerega bo določil naročnikove zahteve za poročanje, ugotovitve pa bo naročniku posredoval v poročilu o arhitekturi rešitve, ki bo v pomoč pri določanju in podajanju naročnikovih zahtev.

To poročilo bo vključevalo:

- Zahteve za poročanje, ki jih določi naročnik in ki bodo v pomoč pri izpolnjevanju naročnikovih zahtev glede skladnosti, revizije in obveščanja o varnosti.
- Zahteve glede obveščanja o varnosti, primeri uporabe in aplikacije, pri uvedbi katerih lahko IBM pomaga (do deset (10) primerov uporabe in do dve (2) aplikaciji).
- Informacije na visoki ravni o naročnikovih virih dnevnika in poteka, ki bodo potrebne za podporo primerov uporabe.
- Priporočila glede omrežne infrastrukture, kot so požarni zidovi in vrata.

Na podlagi poročila o arhitekturi rešitve bo IBM izvedel naslednje naloge, odvisno od tega, koliko časa je še preostalo:

- Konfiguriral zbiranje dogodkov za do tri (3) primerke do desetih (10) tipov vira dnevnika v storitvah v oblaku. Ta dejavnost bo vključevala prenos znanja na ustrezno naročnikovo osebje, da bodo lahko po potrebi dodali več virov dnevnikov. Kot del te storitve bodo vključeni samo viri dnevnika, ki jih podpirajo standardni moduli QRadar Device Support Modules (DSM-ji).
- Začetno uglaševanje, ki vključuje a) aktivacijo pravil za takojšnjo uporabo, shranjenih iskanj, grafikonov in poročil akumuliranih časovnih nizov; b) določanje in odstranjevanje virov hrupa; in c) konfiguriranje shrambe brez povezave z NFS, CIFS ali iSCSI.
- Uvedba desetih (10) primerov uporabe in dveh (2) aplikacij iz IBM QRadar App Exchange, ki so dokumentirani v dokumentu o arhitekturi rešitve.

1.3.4 IBM QRadar on Cloud Custom Parser Service

Ta storitev bo zagotavljala razvoj enega samega, a prilagojenega razčlenjevalnika/uDSM za podporo naročnikovih nestandardnih tipov vira dnevnika, ki se pošljejo v storitve v oblaku, in vključuje naslednje naloge:

- Ustvarjanje prilagojenega razčlenjevalnika za en nestandarden tip vira dnevnika (delo se opravi na daljavo);
- Ustvarjanje, konfiguriranje in preslikava uDSM-ja;
- Namestitev in testiranje prilagojenega uDSM-ja; in

- Razčlemba do petindvajsetih tipov sporočil za vir dnevnika.

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) podaja dodatne informacije o varstvu podatkov za storitve v oblaku in možnosti v zvezi z vrstami vsebine, ki se lahko obdeluje, vključene delavnosti obdelave, funkcije varstva podatkov in podrobnosti glede hrambe in vračila vsebine. DPA velja v primeru in v obsegu, v katerem za osebne podatke, vključene v vsebino, velja Splošna uredba (EU) 2016/679 o varstvu podatkov (GDPR).

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

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 za uveljavljanje zahtevka in kako kontaktirati IBM v zvezi z razpoložljivostjo storitve, so v IBM-ovem pregledu podpore SaaS 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, odzivnimi časi in drugimi informacijami in procesi, najdete tako, da izberete storitev v oblaku v IBM vodniku za podporo, 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:

- Engagement je strokovna ali izobraževalna storitev, povezana s storitvijo v oblaku.
- Dogodki na sekundo so merska enota, ki pove, kakšno je bilo število pojavitev določenega dogodka na sekundo, ki ga obdelajo storitve v oblaku ali je povezan z uporabo teh storitev.
- Tokovi na minuto so merska enota, ki pove, kakšno je število tokov na minuto, ki jih upravljajo ali obdelajo storitve v oblaku. Tok je zapis komunikacije med dvema gostiteljema. Paketi, ki vsebujejo enak izvorni IP, ciljni IP, izvorna vrata, ciljna vrata in protokol, so združeni v en zapis toka.
- Sredstvo je materialni vir ali vrednostna postavka z enolično identifikacijo, do katere/-ga bodo dostopale storitve v oblaku ali ga/jo upravljale.

5. Dodatna določila

Za pogodbe o storitvi v oblaku (ali enakovredne osnovne sporazume), 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:

- Data Gateway – naročnik lahko namesti in uporablja samo do deset (10) primerkov programske opreme Data Gateway.

6. Prevladujoče določbe

6.1 Uporaba varnostnih podatkov

Naslednje določbe prevladajo nad vsemi določbami iz razdelka Vsebina in varstvo podatkov v osnovnih določbah storitve v oblaku, ki veljajo med pogodbenima strankama in morda določajo drugače: IBM sme zbirati indikatorje potencialne zlonamerne dejavnosti v naročnikovi vsebini ter jih uporabiti v kontekstih inteligentnega zaznavanja kibernetskih groženj, natančneje URL-je, naslove IP, domene in razpršitve datotek. IBM lahko nato obvesti naročnika, če ti kazalniki kažejo, da se je naročnikovo tveganje za kibernetske grožnje povečalo.