IBM Resilient Security Orchestration, Automation and Response on Cloud

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

1. Storitev v oblaku

Platforma IBM Resilient Security Orchestration, Automation, and Response (SOAR) Platform on Cloud omogoča organizacijam orkestracijo in avtomatizacijo ljudi, procesov in tehnologije, ki so povezani z odzivi na dogodke.

IBM Resilient SOAR Platform on Cloud omogoča učinkovitejše upravljanje odzivov na dogodke in odzive na kršenje zasebnosti, kar zagotavlja samodejni, hitrejši in bolj prilagodljiv način, na katerega se organizacije odzovejo na dogodke in incidente. Platforma Resilient SOAR Platform on Cloud predstavlja osnovo za uspešno obrambo kibernetske varnosti, ki organizacijam omogoča:

- ustvarjanje načrtov za odzivanje na dogodke, ki temeljijo na panožnih standardih in najboljših praksah.
- enostavnejšo integracijo z zaščito in orodji IT ter usklajuje odzive na dogodke in incidente.
- sodelovanje znotraj organizacije, pri čemer različne deležnike opremi z orodji, ki jim omogočajo opravljanje njihove vloge in nalog pri odzivanju na dogodek.

Platforma IBM Resilient SOAR Platform je zasnovana za različno velike in kompleksne organizacije ter je na voljo z različnimi izbirnimi dodatki. Naročnik ne sme uporabljati zmožnosti, ki niso določene v ponudbi ali dodatkih, ki jih je kupil.

1.1 Ponudbe

Naročnik lahko izbira med naslednjimi razpoložljivimi ponudbami:

1.1.1 IBM Resilient SOAR Platform on Cloud

IBM Resilient SOAR Platform on Cloud Orchestration ponuja osnovo za obrambo kibernetske varnosti. Naročniki lahko ustvarjajo načrte za odzivanje na dogodke glede na panožne standarde in najboljše prakse, jih enostavno integrirajo z zaščito in orodji IT ter usklajujejo odzive na dogodke in incidente. Storitev v oblaku poenostavi sodelovanje znotraj organizacije in tako deležnikom omogoči opravljanje njihove vloge in nalog pri odzivanju na dogodek.

Ekipe za varnost lahko upravljajo z odzivanjem na dogodke kibernetske varnosti in sodelujejo pri njem prek namenskih zmožnosti za upravljanje primerov platforme. Dinamični postopkovni priročniki se prilagajajo hitro razvijajočim se napadom in tako lahko ekipe hitro ponovijo postopke ter s prilagajanjem postopkovnih priročnikov, podatkovnih polj in postavitev prikazov izboljšajo učinkovitost. Simulacije dodatno omogočajo izboljšanje postopkov za odzivanje. Vgrajene integracije, ki jih je možno namestiti, zagotavljajo obogatitev podatkov, ki zbira kontekst za odločanje ekipe za varnost, in omogoča usklajevanje sanacijskih dejanj v skladu s količino zakupljenih dejanj na mesec. Sprejemanje in razčlemba e-pošte zagotavlja lahko metodo za stopnjevanje z drugih orodij. Dostop je lahko zavarovan prek overjanja SAML. Analitika in poročanje dodatno izboljšata transparentnost in analizo tveganja. Ta ponudba je potrebna za vse ostale dodatke, navedene spodaj.

1.2 Izbirne storitve

1.2.1 IBM Resilient SOAR Platform Actions on Cloud

IBM Resilient SOAR Platform on Cloud Actions omogoča usklajevanje zmožnosti platforme. Vgrajene integracije, ki jih je možno namestiti, vključno z integracijami z viri informacij o grožnjah, zagotavljajo samodejno obogatitev za zbiranje konteksta za odločanje ekipe za varnost, kot tudi usklajevanje sanacijskih dejanj.

1.2.2 IBM Resilient SOAR Platform on Cloud Privacy Add-On

IBM Resilient SOAR Platform on Cloud Privacy omogoča naročnikom, da ocenijo in odgovorijo na kršitve zasebnih podatkov. Načrti za odzivanje, ki jih generira ta ponudba, se prilagodijo glede na vrste podatkov, količino evidenc in veljavne zakonske pristojnosti. Naročniki lahko dostopajo tudi do vgrajene zbirke

znanja o zakonodajnih obvestilih o kršitvah zasebnih podatkov, kar omogoča dodatno prilagoditev načrtov za odzivanje na dogodke.

1.2.3 Dodatek za IBM Resilient SOAR Platform on Cloud Team Management

Storitev IBM Resilient SOAR Platform on Cloud Teams zagotavlja upravljanje uporabnikov in segregacijo podatkov v več ekipah. Občutljive informacije se dodelijo po potrebi z omejevanjem dostopa do delovnega prostora in s prilagodljivimi nadzorom dostopa, ki temelji na vlogah. Upravljanje uporabnikov in skupin je lahko poenostavljeno s spodbujanjem storitve Active Directory za odobritev uporabnikov. Za ločene skupine lahko konfigurirate tudi njihovo lastno organizacijo.

1.2.4 Dodatek za IBM Resilient SOAR Platform on Cloud MSSP

Storitev IBM Resilient SOAR Platform on Cloud MSSP zagotavlja upravljanje primerov postopkov, prilagoditev in zmožnosti upravljanja postopkovnega priročnika v več organizacijah. Dogodke in incidente iz več organizacij si lahko ogledate v eni čakalni vrsti, kar omogoča analitiku MSSP (ponudnika upravljanih varnostnih storitev) celovit pregled nad strankami. Postopkovni priročniki s konfiguracijo na organizacijo zagotavljajo preprosto upravljanje standardiziranih in tudi prilagojenih postopkov.

1.2.5 Dodatek za IBM Resilient SOAR Platform on Cloud Non-Production

IBM Resilient SOAR Platform on Cloud Non-Production je ločen primerek platforme IBM Resilient SOAR Platform, ki ga lahko naročnik uporablja samo za notranje neprodukcijske dejavnosti, ki med drugim vključujejo preizkušanje, uglaševanje zmogljivosti, diagnosticiranje napak, notranje primerjalno preizkušanje, uprizarjanje dejavnosti za zagotavljanje kakovosti in/ali razvoj dodatkov ali razširitev za notranjo uporabo v storitvi v oblaku prek objavljenih aplikacijskih programerskih vmesnikov.

1.3 Pospeševalne storitve

Ponudbe IBM Security Expert Labs (SEL) for Resilient Services so oddaljeno zagotovljene storitve, ki zagotavljajo čas strokovnjaka Resilient za pomoč pri arhitekturi in uvedbi, povezani z postavitvijo storitev Resilient. Ponudba IBM Resilient Security, Orchestration and Response – kot storitev v oblaku ali kot programska oprema na mestu uporabe – je predpogoj za vse te storitve.

1.3.1 IBM SEL for Resilient Base Starter Service

V času 5-dnevne oddaljene uporabe bo IBM zagotovil:

- pomoč pri definiranju arhitekture IBM Security Resilient;
- namestitev in konfiguriranje IBM Security Resilient (kjer je to potrebno);
- usposabljanje za analitike in načrtovalce za konfiguriranje in uporabo naročnikovih trenutnih planov odziva na incidente, tako da odraža ključne zahteve naročnikove organizacije;
- za IBM Security Resilient konfigurirane postopkovne priročnike na osnovi enoličnih procesov naročnikovih organizacij;
- kako spremljati definirane ključne identifikatorje zmogljivosti in metrike v skladu s potrebami naročnikovih organizacij in najboljšimi praksami v panogi; in
- identificiral integracijske priložnosti za podporo, avtomatizacijo in uskladitev celovitega procesa.

1.3.2 IBM SEL for Resilient Premium Starter Service

V času 3-dnevne oddaljene uporabe bo IBM:

- pomagal definirati arhitekturo IBM Security Resilient;
- namestil IBM Security Resilient (kjer je to potrebno);
- začetno konfiguriral IBM Security Resilient v naročnikovem okolju; in
- usposobil analitike in načrtovalce za konfiguriranje in uporabo naročnikovih trenutnih planov odziva na incidente, tako da bodo odražali ključne zahteve njegovih organizacij.

1.3.3 IBM SEL for Resilient Additional Day

Poleg storitve Base ali Premium Starter bo v času enodnevne oddaljene uporabe IBM izvedel vse predhodno dogovorjene, z IBM Security Resilient povezane dejavnosti. Na primer:

- nadaljnja podporna namestitev ali konfiguracija IBM Security Resilient ali razširitev (kjer je to potrebno);

- nadaljnje usposabljanje ali podpora za analitike, da se zagotovi pripravljenost na uporabo IBM Security Resilient kot naročnikove ključne rešitve SOAR;
- vodenje načrtovalcev pri tem, kako konfigurirati in uporabiti "postopkovne priročnike", ki odražajo ključne zahteve naročnikovih organizacij; ali
- izvedba hitrega pregleda okolja IBM Security Resilient z namenom zagotavljanja priporočil glede morebitnih področij za izboljšanje.

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://www.ibm.com/dpa/dpl.

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=A47500205B1911E6865BC3F213DB63F7

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:

- Pooblaščeni uporabnik je edinstveni uporabnik, ki lahko dostopa do storitve v oblaku na kateri koli posreden ali neposreden način, prek katerega koli sredstva (na primer prek multipleksirnega programa, naprave ali aplikacijskega strežnika).
- Istočasni uporabnik je uporabnik, ki v določenem trenutku sočasno dostopa do storitve v oblaku na kakršenkoli posredni ali neposredni način (na premer prek programa, naprave ali aplikacijskega strežnika za multipleksiranje). Oseba, ki hkrati dostopa do storitve v oblaku večkrat, se šteje kot en sočasni uporabnik.
- Engagement je profesionalna ali izobraževalna storitev, povezana s storitvijo v oblaku.

- Postavka je primer določene postavke, ki jo upravlja ali obdela storitev v oblaku oz. je povezana z uporabo storitev v oblaku. Za namen te storitve v oblaku je postavka dejanje. Dejanje je orkestracija ali samodejna zahteva, ki jo storitev v oblaku sproži za drug program programske opreme.

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 Preverjanje

Naročnik bo i) hranil in na zahtevo posredoval zapise in produkte sistemskih orodij, kot je v razumni meri potrebno, da IBM in njegovi neodvisni revizorji preverjajo naročnikovo spoštovanje te pogodbe, ter bo ii) nemudoma naročil in plačal morebitna zahtevana pooblastila (vključno s povezano naročnino in podporo ali vzdrževanjem) po IBM-ovih tedaj veljavnih tarifah ter druge stroške in obveznosti, ugotovljene na podlagi takega preverjanja, kot jih IBM navede na računu. Te obveznosti v zvezi s preverjanjem skladnosti ostanejo v veljavi med obdobjem trajanja storitev v oblaku in dve leti po tem.

5.2 Dodatne zahteve za pooblastilo

Naročnik mora pridobiti enako število in enake vrste pooblastil za osnovne in morebitne dodatne storitve v oblaku.

5.3 Omejitve uporabe

Vsak naročnik lahko izvede največ sto tisoč (100.000) poizvedb v okviru storitve za ugotavljanje groženj na mesec. Naročnik lahko poizvedbo v okviru storitve za ugotavljanje groženj ustvari tako, da ob aktiviranju svoje storitve za ugotavljanje groženj incidentu doda nov artefakt. Nova poizvedba v okviru storitve za ugotavljanje groženj se bo samodejno ustvarila vsaka dva (2) dni po izvedbi takšne poizvedbe, dokler je incident odprt in aktiven.

Vsak naročnik lahko izvede največ sto (100) e-poštnih obvestil na dan na pooblaščenega/istočasnega uporabnika. E-poštna obvestila ustvari platforma Resilient glede na konfiguracijo, ki jo nadzira naročnik.

5.4 Dodatne informacije o obdelavi in varovanju podatkov

V izogib dvomu IBM Resilient SOAR Platform on Cloud:

- ne šifrira vsebine Content v mirovanju;
- ni zasnovana za obdelavo posebnih kategorij osebnih podatkov; in
- ni dovoljeno vnašati osebnih podatkov v polja s prostim besedilom, če se to ne zahteva.

Podrobne informacije glede šifriranja in vrstah osebnih podatkov, ki se jih obdeluje, so na voljo na URL-ju za podatkovni list, omenjen v zgornjem razdelku 2.

6. Prevladujoče določbe

6.1 Uporaba podatkov

IBM ne bo uporabil ali razkril rezultatov, ki izhajajo iz naročnikove uporabe storitev v oblaku, in so edinstveni za naročnikovo vsebino (Vpogledi) oziroma kako drugače omogočajo razpoznavo 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.