

IBM X-Force Threat Intelligence

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

1. Storitev v oblaku

IBM X-Force Threat Intelligence zagotavlja programski dostop do platforme IBM X-Force Exchange prek API-ja RESTful, ki informacije vrne v obliki zapisa JavaScript Object Notation (JSON). Storitve v oblaku prav tako podpirajo standarda Structured Threat Information eXpression (STIX) in Trusted Automated eXchange of Indicator Information (TAXII). Storitve v oblaku so zasnovane za zagotavljanje naslednjih glavnih zmožnosti za pomoč uporabniku:

- a. Dostop do informacij o določenih poizvedbah o varnosti, znanih pod imenom "zbirke", ki vsebujejo nestrukturirano in strukturirano vsebino.
- b. Dostop do opisov vrste dogodka (npr. zlonamerna programska oprema, kršitve v zvezi s podatki ali ranljivost) in povezanih ugotovitev, ki se nanašajo na dogodek.
- c. Pridobitev posodobljenih in celovitih podatkov o indikatorjih groženj, ki so najpogosteje izhodišče za nadaljnje raziskave, in o kontekstu za razumevanje teh indikatorjev.
- d. Integracija podatkov (kot je določeno spodaj) z naročnikovimi ponudbami za uporabo informacij o grožnjah.

1.1 Ponudbe

Naročnik lahko izbira med naslednjimi razpoložljivimi ponudbami:

1.1.1 IBM X-Force Exchange Commercial API

IBM X-Force Exchange Commercial Application Programming Interface (API) omogoča uporabnikom avtomatizacijo porabe podatkov o grožnjah iz IBM X-Force Exchange, IBM-ove platforme v oblaku za skupno rabo informacij o grožnjah. Ponudba se prodaja v paketih po deset tisoč postavk.

1.1.2 IBM X-Force Exchange Commercial API Enterprise

IBM X-Force Exchange Commercial Application Programming Interface (API) Enterprise omogoča uporabnikom avtomatizacijo porabe podatkov o grožnjah iz IBM X-Force Exchange, IBM-ove platforme v oblaku za skupno rabo informacij o grožnjah. Ponudba se prodaja po primerku. En primerek zagotavlja neomejen dostop do IP-ja in URL-ja po virih kategorij, poročilih IP in URL in virih ranljivosti ter virih TAXII. Zahteve za indikatorje, ki jih ni mogoče najti na platformi X-Force Exchange, so omejene na 100.000 postavk na mesec.

1.1.3 IBM Advanced Threat Protection Feed by X-Force

IBM Advanced Threat Protection Feed by X-Force uporabnikom zagotavlja definiran nabor dejavnih indikatorjev za neposredno vnašanje v varnostna orodja in rešitve. Vir zagotavlja dostop do dejavnih indikatorjev grožnje (IP-jev in URL-jev), analitično izpeljanih indikatorjev grožnje in naših indikatorjev zgodnjega opozorila za DNS. Viri so na voljo v več formatih, ki vključujejo: STIX/TAXII, JSON, besedilni seznam in CSV.

1.1.4 Threat Intelligence Insights Standard for IBM Cloud Pak for Security

Ta storitev v oblaku je na voljo brezplačno in naročnikom ponuja zmožnost integracije temeljnih podatkov o grožnjah in omogočanje funkcij znotraj aplikacije Threat Intelligence Insights v Cloud Pak for Security. Naročniki s tem paketom pridobijo dostop do brezplačne plasti vsebine X-Force Threat Intelligence, ki vključuje svetovalce in grožnje X-Force ter povezane indikatorje ogroženosti (IP-je, URL-je, ranljivosti in razpršilne vrednosti). Poleg tega lahko naročniki izvajajo ročno zmožnost Am-I-Affected ter z njo poiščejo in identificirajo zlonamerne grožnje v svojem okolju. Aplikacija IBM Security Threat Intelligence Insights, ki je na voljo kot del izdelka IBM Cloud Pak for Security, je predpogoj za to storitev v oblaku.

1.1.5 Threat Intelligence Insights Advanced for IBM Cloud Pak for Security

Threat Intelligence Insights Advanced for IBM Cloud Pak for Security je vrhunski paket, ki naročnikom ponuja zmožnost, da aplikaciji Threat Intelligence Insights v Cloud Pak for Security dodajo naslednjo

generacijo podatkov o grožnjah in zmožnosti storitve X-Force. Napredna vsebina s podatki o grožnjah, ki jo ureja IBM-ova ekipa za analizo incidentov in odzivanje nanje (IRIS), vključuje dostop do poglobljenih analiz in poročil o zlonamerni programski opremi, skupinah groženj, dejavnostih groženj in panogah, priporočil za popraviljanje, indikatorjev ogroženosti in drugega. Paket Advanced naročnikom omogoča tudi neprekinjeno in samodejno izvajanje zmožnosti Am-I-Affected, ki proaktivno nastavlja prioriteto in identificira ustrezne grožnje v okolju uporabnika. Aplikacija IBM Security Threat Intelligence Insights, ki je na voljo kot del izdelka IBM Cloud Pak for Security, je predpogoj za to storitev v oblaku.

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=1ECC13601F5911E69AAAC4D0C72C126B>

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 pogodbeno 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:

- Primerek je vsak dostop do določene konfiguracije storitev v oblaku.
- Postavka je primer določene postavke, ki jo upravlja ali obdelava storitev v oblaku oz. je povezana z uporabo storitev v oblaku. Pri tej storitvi je postavka vsak rezultat, ki ga vrne ena poizvedba.
- Upravljeni 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 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 Podatki

5.2.1 Opredelitev pojmov

Storitev v oblaku vključuje uporabo ali dostop do IBM-ovih podatkov in podatkov skupnosti. IBM zagotavlja podatke in vse vsebine tretjih oseb, ki so na voljo prek storitve v oblaku, brez kakršnih koli garancij in ne odgovarja za nobene izgube, ki jih utrpi naročnik kot rezultat dostopanja do podatkov ali vsebin tretje osebe oziroma njihove uporabe. Veljajo naslednje definicije:

- a. **Podatki** pomenijo katerekoli informacije, vsebino, datoteke, besedilo, grafiko, programsko opremo, kodo, sporočila, izhodne podatke iskalnih poizvedb, vhodne podatke iskalnih poizvedb, vsebino forumov, načine ali druga gradiva, ki so dostopna prek storitve v oblaku.
- b. **IBM-ovi podatki** pomenijo podatke, ki jih IBM da naročniku na voljo prek storitve v oblaku, razen podatkov skupnosti. IBM, njegovi dajalci licenc ali njegovi dobavitelji zadržijo vse pravice, pravni naslov in interes glede IBM-ovih podatkov.
- c. **Podatki skupnosti** pomenijo podatke, ki so naročniku dani na voljo prek storitve v oblaku s strani drugih uporabnikov storitve v oblaku.

5.2.2 IBM-ovi podatki

IBM podeljuje naročniku omejeno, neizključno, neprenosljivo licenco za dostop do podatkov in njihovo uporabo prek storitev v oblaku izključno - (i) za naročnikovo osebno uporabo za podporo naročnikove raziskave in preiskave groženj ali (ii) za namene integracije IBM-ovih podatkov v naročnikove ponudbe. Naročnik ne sme podvajati ali poskušati podvajati večjih delov ali celotne vsebine IBM-ovih podatkov ali storitev v oblaku. Naročnik mora upoštevati vsa obvestila, informacije in omejitve o avtorskih pravicah, ki so del katerihkoli IBM-ovih podatkov ali so takšnim podatkom priložene, prav tako naročnik ne sme iz IBM-ovih podatkov odstraniti nobenega besedila, obvestila o avtorskih pravicah ali drugih obvestil o lastništvu. Naročnik ne sme zaobiti ali poskusiti zaobiti katerih koli omejitev dostopa, povezanih s storitvami v oblaku.

Če naročnik vključi IBM-ove podatke v svoje ponudbe, bo naročnik v svoji pogodbi s končnim uporabnikom: (a) omejil skupno odgovornost naročnika in njegovih neodvisnih dobaviteljev za neposredno škodo na primeren znesek ter zavrnil vsakršno odgovornost za posledično in drugo posredno škodo ter predpostavljena jamstva neodvisnih dobaviteljev; (b) zahteval od naročnikovega končnega uporabnika, da poda kakršne koli zahtevke, ki izhajajo iz pogodbe s končnim uporabnikom, izključno proti naročniku, (c) prepovedal uporabo podatkov ločeno od naročnikovih proizvodov in storitev; in (d) prepovedal podlicenciranje ali kakšno drugačno nadaljnje distribuiranje podatkov.

Če naročnik vključi IBM-ove podatke v svoje ponudbe, bo naročnik poleg škode, za katero je morda odgovoren na podlagi veljavne zakonodaje ali določb pogodbe, branil IBM, mu povrnil škodo in prevzel odgovornost namesto njega v zvezi s kakršnimi koli zahtevki tretjih oseb zaradi: (a) neupoštevanja določb iz prejšnjega odstavka; ali (b) zagotovil, izjav, zahtevkov ali jamstev v zvezi z IBM-ovimi podatki, ki jih ni odobril IBM.

Razen kot je izrecno navedeno zgoraj, naročnik IBM-ovih podatkov ne sme kopirati, spreminjati, reproducirati, prenašati, prodajati, ponujati za prodajo, izposojati, dajati v najem, licencirati, zanje izdajati podlicenc, jih ponovno distribuirati ali kako drugače dajati na voljo tretjim osebam.

5.2.3 Podatki skupnosti

Naročnik je odgovoren za svojo interakcijo z drugimi uporabniki storitev v oblaku, vključno z dostopanjem do podatkov skupnosti. Določene podatke skupnosti je mogoče deliti v zbirki ali grožnji. V zvezi z javno

dostopnimi podatki skupnosti je lastnik podatkov podelil uporabnikom storitve v oblaku neizključno, po vsem svetu veljavno plačano pravico in licenco za uporabo, kopiranje, reproduciranje, spreminjanje in/ali izdelavo izpeljanih del in distribuiranje takšnih podatkov skupnosti ali njihovih delov (javna licenca). Če naročnik kopira, reproducira, distribuira ali kako drugače da na voljo podatke skupnosti v skladu z javno licenco, mora naročnik prispevati k podatkom skupnosti. Naročnik lahko podatke, ki so mu dani na voljo v zbirki ali grožnji, uporablja izključno za lastno notranjo in nekomercialno uporabo. Naročniku bodo morda prikazani podatki skupnosti, ki kršijo IBM-ove pravilnike, ta opis storitev oz. so drugače žaljivi.

Podatki skupnosti vključujejo informacije o profilu uporabnika drugih uporabnikov storitve v oblaku. Naročnik ne sme pridobivati podatkov z rudarjenjem, kopirati ali drugače uporabljati informacij o profilu za katerikoli drug namen, razen za komuniciranje z drugimi uporabniki storitev v oblaku o informacijah o grožnjah.

Podatki skupnosti lahko vključujejo povezave do spletnih mest, ki jih IBM ne upravlja. IBM ne odgovarja za vsebino, produkte, gradiva ali prakse (vključno s praksami glede zasebnosti) takih spletnih mest. Naročnik razume, da je lahko z dostopom do podatkov skupnosti izpostavljen spletnim mestom tretjih oseb, za katere morda meni, da so žaljiva, nespodobna ali drugače sporna.

Če naročnik meni, da podatki vključujejo osebne podatke, ki so nepravilni ali bi jih bilo treba odstraniti, se lahko obrne na IBM prek funkcije Contribute (Prispevaj) v možnosti X-Force IP Report.

6. Prevladujoče določbe

6.1 Podobdelovalec Cloudflare, Inc.

Naslednje prevlada pri morebitnih nasprotnih določbah v načelih glede varstva podatkov in zasebnosti za storitve v oblaku med pogodbenima strankama: ta storitev v oblaku uporablja Cloudflare, Inc. kot enega izmed svojih podobdelovalcev vsebine. Cloudflare obdeluje vsebino v nešifrirani obliki za optimizacijo dostave v storitev v oblaku. Cloudflare je s PCI združljiv ponudnik storitev ravni 1, ki je v postopku pridobivanja skladnosti s standardi ISO 27001 in SOC 2. (Pojasnilo: celotna storitev v oblaku ni združljiva s PCI).