

## IBM X-Force Threat Intelligence

Tento Popis služby stanovuje podmínky služby Cloud Service. Příslušné dokumenty objednávky poskytují podrobnosti o ceně a další podrobnosti o objednavce Zákazníka.

### 1. Cloud Service

IBM X-Force Threat Intelligence poskytuje programový přístup k IBM X-Force Exchange prostřednictvím rozhraní RESTful API, které vrací informace ve formátu JavaScript Object Notation (JSON). Služba Cloud Service dále podporuje standardy Structured Threat Information eXpression (STIX) a Trusted Automated eXchange of Indicator Information (TAXII). Služba Cloud Service je určena k poskytování následujících klíčových funkcí, které pomáhají uživateli:

- a. Přistupovat k informacím o konkrétních šetřeních v oblasti zabezpečení, známým jako "kolekce", které zahrnují nestruturovaný i strukturovaný obsah.
- b. Přistupovat k popisům typu incidentu (jako je malware, narušení dat nebo ohrožení zabezpečení) i k souvisejícím pozorovatelným veličinám, které se týkají konkrétního incidentu.
- c. Získat aktuální a komplexní informace pro různé indikátory hrozeb, které jsou často výchozím bodem pro další výzkum, a kontext k pochopení těchto indikátorů.
- d. Integrovat Data (definovaná níže) s nabídkami Zákazníka, které využívají informace o hrozbách.

#### 1.1 Nabídky

Zákazník si může vybrat z následujících dostupných nabídek:

##### 1.1.1 IBM X-Force Exchange Commercial API

Služba IBM X-Force Exchange Commercial Application Programming Interface (API) umožňuje uživatelům automatizovat využívání informací o hrozbách z IBM X-Force Exchange, cloudové platformy pro sdílení informací o hrozbách od IBM. Nabídka se prodává v balíčcích po Deseti tisících položkách.

##### 1.1.2 IBM X-Force Exchange Commercial API Enterprise

IBM X-Force Exchange Commercial Application Programming Interface (API) Enterprise umožňuje uživatelům automatizovat využívání informací o hrozbách z IBM X-Force Exchange, cloudové platformy pro sdílení informací o hrozbách od IBM. Nabídka se prodává na základě Instancí. Jedna Instance poskytuje neomezený přístup k IP a URL podle kanálů kategorií, sestavám IP a URL a kanálům ohrožení zabezpečení, stejně jako ke všem kanálům TAXII. Požadavky na indikátory, které nebudou v X-Force Exchange nalezeny, jsou omezeny na 100 000 Položek měsíčně.

##### 1.1.3 IBM Advanced Threat Protection Feed by X-Force

IBM Advanced Threat Protection Feed by X-Force nabízí uživatelům definovanou sadu bezprostředně použitelných indikátorů pro přímý import do bezpečnostních nástrojů a řešení. Tento informační kanál nabízí přístup k bezprostředně použitelným indikátorům narušení (IP a URL), indikátorům narušení odvozeným analytiky a našim indikátorům včasného varování pro DNS (DNS Early Warning). Informační kanály jsou dostupné v různých formátech: STIX/TAXII, JSON, Textový seznam a CSV.

##### 1.1.4 Threat Intelligence Insights Standard for IBM Cloud Pak for Security

Tato služba Cloud Service je k dispozici bezplatně a Zákazníkům nabízí možnost integrovat základní zpravodajství o hrozbách a povolit funkce v rámci aplikace Threat Intelligence Insights na Cloud Pak for Security. Prostřednictvím tohoto balíčku Zákazník získá přístup k bezplatné vrstvě obsahu X-Force Threat Intelligence, a to včetně X-Force Advisories, Threats a souvisejících IOC (IP, URL, zranitelnost, haš). Navíc může Zákazník spustit manuální možnost Am-I-Affected pro vyhledání a identifikaci škodlivých hrozeb v jeho prostředí. Aplikace IBM Security Threat Intelligence Insights dostupná v rámci IBM Cloud Pak for Security je předpokladem pro tuto službu Cloud Service.

##### 1.1.5 Threat Intelligence Insights Advanced for IBM Cloud Pak for Security

Threat Intelligence Insights Advanced for IBM Cloud Pak for Security je prémiový balíček, který Zákazníkům nabízí možnost přidat zpravodajství o hrozbách a funkce příští generace X-Force do aplikace Threat Intelligence Insights na Cloud Pak for Security. Pokročilý obsah zpravodajství o hrozbách

zajišťovaný týmem reakce na incidenty a analytickým týmem IBM zahrnuje přístup k hloubkovým analytickým zprávám o malwaru, skupinách hrozeb, ohrožující činnosti a oboru, doporučení pro nápravu, indikátory kompromisu (IOC) a mnoho dalšího. Pokročilý balíček rovněž umožňuje Zákazníkům souvisle a automaticky spustit možnost Am-I-Affected, která proaktivně stanovuje priority a identifikuje relevantní hrozby v prostředí uživatele. Aplikace IBM Security Threat Intelligence Insights dostupná v rámci IBM Cloud Pak for Security je předpokladem pro tuto službu Cloud Service.

## 2. Datové listy ochrany a zpracování údajů

Dodatek o zpracování údajů (Data Processing Addendum, DPA) společnosti IBM na adrese <http://ibm.com/dpa> a Datový list zpracování a ochrany údajů (označováno jako Datový list nebo Dodatek DPA) v odkazech níže poskytují další informace o ochraně údajů pro služby Cloud Services a volby týkající se typů Obsahu, které lze zpracovat, využívaných činností vztahujících se ke zpracování, funkcí ochrany údajů a specifických aspektů uchovávání a vrácení Obsahu. Dodatek DPA se uplatní, pokud se na osobní údaje zahrnuté v Obsahu vztahuje/í i) Evropské obecné nařízení o ochraně údajů (EU/2016/679) (GDPR); nebo ii) jiné zákony o ochraně údajů uvedené na adrese <http://ibm.com/dpa/dpl>.  
<https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1ECC13601F5911E69AAAC4D0C72C126B>

## 3. Úrovně služby a Technická podpora

### 3.1 Dohoda o úrovni služeb

IBM poskytuje Zákazníkovi pro dostupnost následující Dohodu o úrovni služeb (SLA). IBM uplatní nejvyšší použitelnou kompenzaci vycházející ze souhrnné dostupnosti služby Cloud Service, jak je uvedeno v tabulce níže. Procento dostupnosti se vypočítá jako celkový počet minut v rámci smluvního měsíčního období minus celkový počet minut Odstávky za smluvní měsíční období, děleno celkovým počtem minut za smluvní měsíční období. Definice Odstávky, proces uplatňování nároku a pokyny, jak kontaktovat IBM ohledně problémů s dostupností služby, jsou uvedeny na stránkách IBM v příručce Cloud Service Support Guide na adrese [https://www.ibm.com/software/support/saas\\_support\\_overview.html](https://www.ibm.com/software/support/saas_support_overview.html).

Dostupnosti služeb	Dobropis (% měsíčního registračního poplatku*)
Méně než 99,9 %	2 %
Méně než 99,0 %	5 %
Méně než 95,0 %	10 %

\* Registrační poplatek je smluvní cena za měsíc, za který je uplatňován nárok.

### 3.2 Technická podpora

Informace o technické podpoře pro službu Cloud Service, včetně kontaktních údajů na podporu, úrovní závažnosti, hodin dostupnosti podpory, dob odezvy a dalších informací a procesů podpory, lze zjistit výběrem služby Cloud Service v příručce podpory IBM na adrese <https://www.ibm.com/support/home/pages/support-guide/>.

## 4. Poplatky

### 4.1 Metriky poplatků

Metriky poplatků za službu Cloud Service jsou uvedeny v Transakčním dokumentu.

Na tuto službu Cloud Service se uplatní následující metriky poplatků:

- Instance je každý přístup ke specifické konfiguraci služeb Cloud Services.
- Položka je výskyt specifické položky, která je spravována či zpracovávána službou Cloud Service nebo souvisí s použitím služby Cloud Service. Pro tuto službu je Položka každý výsledek vrácený z jednoho dotazu.
- Spravovaný virtuální server (MVS) sestává z procesních jednotek, paměti a I/O funkcí a provádí požadované postupy, příkazy nebo aplikace spravované službami Cloud Services.

## 5. Dodatečné podmínky

Na Smlouvy o službě Cloud Service (nebo ekvivalentní smlouvy o základním cloudu) uzavřené před 1. lednem 2019 se vztahují podmínky dostupné na adrese <https://www.ibm.com/acs>.

### 5.1 Ověření

Zákazník i) povede a na vyžádání poskytne záznamy a výstupy ze systémových nástrojů v rozsahu přiměřeně potřebném pro IBM a jejího nezávislého auditora pro účely kontroly dodržování této Smlouvy ze strany Zákazníka a ii) neprodleně objedná a uhradí veškerá požadovaná oprávnění dle příslušné aktuální sazby IBM a uhradí i další poplatky a závazky stanovené na základě výsledků takového ověření, které IBM uvede na faktuře. Tyto povinnosti vzniklé v souvislosti s kontrolou dodržování podmínek jsou a budou účinné po dobu poskytování služby Cloud Service a ještě dva roky poté.

### 5.2 Data

#### 5.2.1 Definice

Služba Cloud Service zahrnuje používání Dat IBM i Dat komunity a přístup k nim. IBM poskytuje Data a veškerý dostupný obsah třetích osob prostřednictvím služby Cloud Service bez záruk jakéhokoliv druhu a nenese odpovědnost za případné ztráty, které Zákazníkovi vzniknou v důsledku přístupu k Datům či obsahu třetích osob nebo jejich použití. Platí následující definice:

- a. **Data** – znamená jakékoli informace, obsah, soubory, text, grafiku, software, kód, zprávy, výstup z dotazů vyhledávání, vstup pro dotazy vyhledávání, obsah diskusních fór, metody nebo jiné materiály přístupné prostřednictvím služby Cloud Service.
- b. **Data IBM** – znamená Data zpřístupněná Zákazníkovi od IBM prostřednictvím služby Cloud Service, s výjimkou Dat komunity. IBM, její poskytovatelé licencí nebo dodavatelé si zachovávají všechna práva, nároky a tituly k Datům IBM.
- c. **Data komunity** – znamená Data zpřístupněná Zákazníkovi prostřednictvím služby Cloud Service ostatními uživateli Cloud Service.

#### 5.2.2 Data IBM

IBM udílí Zákazníkovi omezenou, nevýhradní, nepřenosnou licenci pro přístup k Datům IBM a jejich užívání výhradně prostřednictvím služby Cloud Service – (i) výhradně pro osobní využití Zákazníka na podporu výzkumu a vyšetřování hrozeb Zákazníka, nebo (ii) pro účely integrace Dat IBM do nabídek Zákazníka. Zákazník nesmí provádět duplikaci významných částí nebo celého obsahu Dat IBM nebo služby Cloud Service ani se o ni pokoušet. Zákazník musí dodržovat všechny informace, oznámení a omezení týkající se autorských práv obsažené v Datech IBM nebo k nim připojené a nesmí odebrat žádný text ani sdělení o autorských právech či jiných vlastnických právech obsažené v Datech IBM. Zákazníkovi není dovoleno obcházet jakákoli omezení přístupu související se službou Cloud Service nebo se o to pokoušet.

Pokud Zákazník začlení Data IBM do svých nabídek, je Zákazník povinen ve své smlouvě s koncovým uživatelem: (a) omezit kolektivní odpovědnost Zákazníka a jeho nezávislých dodavatelů za přímé škody na přiměřenou částku a vyloučit veškerou odpovědnost za následné nebo jiné nepřímé škody, stejně jako odvozené záruky za nezávislé dodavatele; (b) požadovat, aby koncový uživatel Zákazníka uplatňoval případné nároky vyplývající ze smlouvy s koncovým uživatelem výhradně vůči Zákazníkovi; (c) zakázat používání Dat odděleně od produktu Zákazníka nebo jeho služeb; a (d) zakázat poskytování podlicencí nebo jakoukoliv další distribuci Dat.

Pokud Zákazník začlení Data IBM do svých nabídek, pak mimo škody, za které může Zákazník nést odpovědnost v souladu s platnými předpisy nebo podmínkami Smlouvy, bude Zákazník IBM bránit, chránit a odškodnit ji v případě veškerých nároků třetí osoby vyplývajících: (a) z nedodržení podmínek předchozího odstavce; nebo (b) ze závazků, prohlášení, nároků nebo záruk týkajících se Dat IBM, které IBM neschválila.

Není-li výše výslovně uvedeno jinak, Zákazník nesmí kopírovat, měnit, rozmnožovat, přenášet, prodávat, nabízet k prodeji, pronajímat, poskytovat na leasing, licencovat, sublicencovat, opakovaně distribuovat ani jinak zpřístupňovat Data IBM třetím osobám.

### 5.2.3 Data komunity

Zákazník nese odpovědnost za své interakce s ostatními uživateli služby Cloud Service, včetně přístupu k Datům komunity. Určitá Data mohou být sdílena v Kolekci nebo Hrozbě. S ohledem na veřejně dostupná Data komunity vlastník Dat udílí uživatelům služby Cloud Service nevýhradní, celosvětově platné, zcela uhrazené právo a licenci k užívání, kopírování, rozmnožování, úpravám anebo distribuci Dat komunity nebo jejich částí a k vytváření odvozených děl z těchto Dat komunity (Veřejná licence). Pokud Zákazník kopíruje, rozmnožuje, distribuuje nebo jinak zpřístupňuje Data komunity v souladu s Veřejnou licencí, musí pro taková Data komunity poskytnout atribuci. Zákazník smí Data zpřístupněná v Kolekci nebo Hrozbě použít pouze pro své interní nekomerční využití. Zákazník se může setkat s Daty komunity, která porušují zásady IBM, tento Popis služby nebo jsou jinak urážlivá.

Data komunity mohou zahrnovat informace o uživatelském profilu ostatních uživatelů Cloud Service. Zákazník nesmí dolovat, kopírovat ani jinak využívat informace profilu k jinému účelu než ke komunikaci s ostatními uživateli Cloud Service, a to v souvislosti s informacemi o hrozbách.

Data komunity mohou zahrnovat odkazy na weby, které neprovozuje IBM. IBM nenese odpovědnost za obsah, produkty, materiály či postupy (včetně postupů týkajících se osobních údajů) těchto webů. Zákazník bere na vědomí, že přístupem k Datům komunity může být vystaven webům třetích stran, které pro něj mohou být urážlivé, nevhodné nebo jinak nepřijatelné.

Pokud se Zákazník domnívá, že Data zahrnují osobní údaje, které jsou nesprávné nebo by měly být odstraněny z jiného důvodu, může se obrátit na společnost IBM prostřednictvím funkce Příspěvků v rámci X-Force IP Report.

## 6. Přednostní podmínky

### 6.1 Cloudflare, Inc. Subprocessor

Níže uvedené má přednost před případnými odlišnými ustanoveními Zásad zabezpečení dat a ochrany osobních údajů pro služby Cloud Services mezi smluvními stranami: Tato služba Cloud Service využívá Cloudflare, Inc. jako jednoho ze svých dílčích zpracovatelů Obsahu. Cloudflare zpracovává Obsah v nešifrované formě s cílem optimalizovat poskytování služby Cloud Service. Cloudflare splňuje podmínky PCI jako poskytovatel služeb 1. úrovně a je v procesu získání certifikace podle ISO 27001 a SOC 2. (Pro vyloučení pochybností se uvádí, že celková služba Cloud Service není v souladu s PCI.)