

IBM QRadar Advisor with Watson

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

1. Cloud Service

IBM QRadar Advisor with Watson rozšiřuje kognitivní analytiku platformy QRadar Security Platform, která Zákazníkům a analytikům zabezpečení pomáhá vyšetřit hrozby a reagovat na ně. Rozšiřuje korpus Watson o znalostní korpus Cyber Security, který se zaměřuje na nestrukturovaná data (včetně například webových stránek zabezpečení, blogů a výzkumných zpráv) a korelaci s místními incidenty zabezpečení. To může pomoci odhalit skryté hrozby a automaticky vytvořit přehled pro reakci a rozhodování. QRadar Advisor with Watson umožňuje analytikům zabezpečení zasílat narušení zajištění službě Watson pro provádění zjišťování hrozeb s využitím znalostní báze stovek tisíc nestrukturovaných a strukturovaných dat a jejich zpětného mapování z hlediska hrozcích subjektů souvisejících s původním narušením zabezpečení, jako jsou škodlivé soubory, podezřelé adresy IP, výstražné subjekty a vztahy mezi nimi. To může být mimořádně přínosné při stanovení, zda je narušení zabezpečení spojeno se známou malwarovou kampaní či nikoliv. Pokud tomu tak je, Watson poskytne kromě jiných i informace o použitém malwaru, zjištěných slabých místech a rozsahu hrozby (včetně dalších potenciálně zasažených koncových bodů).

1.1 Nabídky

Zákazník si může vybrat z následujících dostupných nabídek.

1.1.1 IBM QRadar Advisor with Watson

QRadar Advisor with Watson vyžaduje, aby měl Zákazník aktivní nasazení IBM QRadar, buď v lokálním prostředí, nebo nasazení v cloudu, a nainstalován aktivační software služby Cloud Service pro příslušné nasazení za účelem přístupu Zákazníka k této funkci. Pokud je oprávnění ke službě Cloud Service zakoupeno podle Událostí za sekundu, obsahuje limit pro počet dotazů na narušení zabezpečení, které smí Zákazník zasílat do služby Cloud Service v sazbě 1,5 dotazu denně na 100 Událostí za sekundu (zaokrouhleno nahoru na nejbližší dotaz), na něž má Zákazník nárok. Pokud je oprávnění ke službě Cloud Service zakoupeno podle Managed Virtual Server (MVS), obsahuje limit pro počet dotazů na narušení zabezpečení, které smí Zákazník zasílat do služby Cloud Service v sazbě 15 dotazů denně na 100 MVS, na něž má Zákazník nárok. Dotazy zaslané nad rámec tohoto limitu nebudou mít udělenou prioritu a služba Cloud Service se po zbytek daného dne nemusí zpracovat.

1.1.2 IBM QRadar Advisor with Watson – Enterprise

IBM QRadar Advisor with Watson – Enterprise nejlépe vyhovuje velkým nasazením operačních středisek zabezpečení (SOC), která obecně překračují dvě stě padesát tisíc Událostí za sekundu či více. Zákazník je povinen instalovat aktivační software služby Cloud Service na svá příslušná zakoupená nasazení IBM QRadar, aby získal přístup k funkcím služby Cloud Service. IBM QRadar Advisor with Watson – Enterprise je k dispozici na základě účtovací metriky vycházející z Instance, která není závislá na rozsahu nasazení IBM QRadar u Zákazníka. Zákazník je omezen na 25 dotazů ve frontě v kterémkoliv daném okamžiku.

1.1.3 IBM QRadar Advisor with Watson – Starter Pack

IBM QRadar Advisor with Watson – Starter Pack je určen pro začínající uživatele QRadar Advisor with Watson. Tato služba Cloud Service má veškeré funkce QRadar Advisor with Watson, jak je popsáno v Části 1.1.1 výše, ale pro Zákazníky je k dispozici pouze jako první nákup produktu QRadar Advisor with Watson, a nejde ji prodloužit.

1.2 Volitelné služby

1.2.1 IBM QRadar Advisor with Watson – Test Environment

IBM QRadar Advisor with Watson – Test Environment je určena Zákazníkům, kteří si přejí nasadit službu Cloud Service ve svém interním testovacím prostředí, a lze ji využívat výhradně pro neproduktivní

testovací účely. IBM QRadar Advisor with Watson – Test Environment musí být doplněna registrací služby Cloud Service pro produktivní úroveň.

1.3 Akcelerační služby

1.3.1 IBM QRadar Advisor with Watson Advanced Services

Pro tuto vzdáleně poskytovanou službu registrace společnost IBM poskytne kterékoliv z následujících konzultačních služeb Zákazníkovi po dobu až 5 dní během 1 roku:

- Vyhodnocení procesu SOC Zákazníka, včetně procesu vyšetřování a/nebo odezvy na incident;
- Opakované vyhodnocení odezvy referenčních sad;
- Úprava automatické analýzy pro porušení velkého rozsahu;
- Vypracování případu použití;
- Poskytnutí doporučení pro změny procesu SOC, které budou zahrnovat QRadar Advisor with Watson;
- Poskytnutí vedení ohledně postupu co nejefektivnějšího pochopení a zabudování dat z QRadar Advisor with Watson do stávajících procesů Zákazníka;
- Poskytnutí přenosu znalostí na příslušné subjekty QRadar Advisor with Watson.

POZNÁMKA: Následující činnosti mohou být součástí této služby na základě stavu nasazení QRadar Zákazníkem:

- Provedení kontroly stavu nasazení QRadar Zákazníkem;
- Provedení dodatečného ladění stávajícího nasazení QRadar;
- Pomoc s přidáním dalších zdrojů protokolu k nasazení QRadar Zákazníka;

1.3.2 IBM QRadar Advisor with Watson Basic Setup Service

Tato služba nastavení je poskytována vzdáleně a zahrnuje čtyřicet (40) hodin profesionálních služeb, jejichž platnost vyprší devadesát (90) dní od zakoupení, pokud nebude uvedeno jinak, a to bez ohledu na to, zda byly (v příslušných případech) využity veškeré hodiny. Služby budou zahrnovat jmenovaného Správce podpory IBM, který naplánuje veškeré zahajovací hovory.

IBM poskytne některé nebo všechny následující položky:

- Vyhodnocení procesu SOC Zákazníka, včetně procesu vyšetřování a/nebo odezvy na incident;
- Implementace QRadar Advisor with Watson do prostředí Zákazníka:
 - Instalace QRadar Advisor with Watson;
 - Mapování jednotlivých vlastností do QRadar Advisor with Watson;
 - Implementace odezvy referenčních sad;
 - Úprava automatické analýzy pro porušení velkého rozsahu;
 - Vedení pro případy využití;
 - Poskytnutí doporučení pro změny procesu SOC, které budou zahrnovat QRadar Advisor with Watson.

1.3.3 IBM QRadar Advisor with Watson Quick Setup Service

Tato služba nastavení je určena pro Zákazníky s méně než 5 000 událostmi za sekundu (EPS).

Pro tuto vzdáleně poskytovanou službu IBM poskytne kterékoliv z následujících konzultačních služeb (nebo jejich kombinaci) Zákazníkovi po dobu až 16 hodin během 90denního období:

- Instalace QRadar Advisor with Watson.
- Správa oprávnění pro QRadar Advisor with Watson.
- Konfigurace QRadar Advisor with Watson, která může zahrnovat:
 - konfiguraci zabezpečeného serveru proxy;
 - odesílání výměnných přihlašovacích údajů X-Force;
 - vytvoření tokenů oprávněných služeb;
 - konfiguraci pravidel uchovávání pro ukládání výsledků analýzy;

- mapování vlastností vlastní události;
- export referenčních sad;
- mapování informační služby o hrozbách;
- konfiguraci identifikace aktiv;
- optimalizaci využití;
- automatické vyšetřování a výsledky výstrah o porušení pravidel (minimálně jedna ukázka příkladu použití);
- prozkoumání náhledu s grafem vztahů.

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/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=0B439290AB5011E6BE74C84817AAB206>

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.

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, úrovni 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:

- Událost za sekundu je výskyt specifické události (EPS), která je zpracovávána službami Cloud Services nebo souvisí s použitím služeb Cloud Services. Pro účely této služby Cloud Service jsou

Událostmi za sekundu takové Události, které jsou shromážděny a zpracovány nasazením IBM QRadar Zákazníkem.

- Instance je každý přístup ke specifické konfiguraci služeb Cloud Services.
- Sjednaná služba je profesionální nebo školicí služba související se službami Cloud Services.
- 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 Aktivační software

Služba Cloud Service obsahuje následující Aktivační software:

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

5.2 Použití Cloud Service v souladu se zákony

Účelem Cloud Service je pomoci Zákazníkovi zlepšit jeho prostředí a data zabezpečení. Použití Cloud Service může implikovat různé právní předpisy, včetně předpisů týkajících se soukromí, ochrany dat, zaměstnání a elektronické komunikace a uchování. Službu Cloud Service lze používat pouze zákonným způsobem a pro účely, které jsou v souladu se zákonem. Zákazník se zavazuje, že službu Cloud Service bude používat v souladu s platnými právními předpisy a zásadami, a v této souvislosti přebírá veškerou odpovědnost. Zákazník vyjadřuje souhlas s tím, že získal nebo získá všechny souhlasy, oprávnění nebo licence nutné k používání Cloud Service v souladu se zákony.

6. Přednostní podmínky

6.1 Využití údajů

Dále uvedené má přednost v případě rozporu s částí Ochrana obsahu a údajů v základních podmínkách služby Cloud Service mezi stranami: IBM nepoužije ani nesdělí výsledky pocházející z používání služby Cloud Service Zákazníkem, které jsou jedinečné vzhledem k Obsahu Zákazníka (Poznatky) nebo jinak identifikují Zákazníka. Společnost IBM však bude používat Obsah a další informace, které vyplynou z Obsahu (kromě Insights) v průběhu poskytování služby Cloud Service, pro účely vylepšování služby Cloud Service. IBM může rovněž sdílet identifikátory hrozeb a další bezpečnostní informace vložené do Obsahu pro účely detekce hrozeb a ochranu.