IBM QRadar Advisor with Watson

Tento Popis služby popisuje službu , kterou IBM poskytuje Zákazníkovi. Pojem "Zákazník" označuje a zahrnuje společnost, její autorizované uživatele nebo příjemce služby Cloud Service. Příslušná Cenová nabídka a Dokument o oprávnění (Proof of Entitlement) jsou poskytnuty ve formě samostatných Transakčních dokumentů.

1. Cloud Service

1.1 IBM QRadar Advisor with Watson Service

IBM QRadar Advisor with Watson rozšiřuje kognitivní analytiku platformy QRadar Security Platform, která zákazníkům a analytikům zabezpečení pomáhá rychle 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 rychlejší reakci a zlepšené 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 hrozících 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).

Služba Cloud Service vyžaduje, aby měl Zákazník aktivní nasazení IBM Security QRadar a nainstalován aktivační kód služby Cloud Service pro příslušné nasazení, aby měl Zákazník k této funkci přístup. Služba Cloud Service zahrnuje "měkké limity" pro počet dotazů na narušení zabezpečení, které smí Zákazník zasílat do služby Cloud Service, v sazbě patnácti (15) dotazů denně na 1000 Událostí za sekundu, na něž má Zákazník nárok. Dotazy zaslané nad tento limit budou službou Cloud Service zpracovány, nicméně nebudou mít prioritu a reakce bude zaslána nižší rychlostí.

1.2 IBM QRadar Advisor with Watson Trial

IBM QRadar Advisor with Watson Trial ("Trial Cloud Service") nabízí funkce IBM QRadar Advisor with Watson v rámci zkušebního období. Přístup Zákazníka ke službě Trial Cloud Service bude fungovat po dobu stanovenou v Transakčním dokumentu nebo jiné dokumentaci a po jejím uplynutí přístup Zákazníka skončí. Zákazník je rovněž během zkušebního období oprávněn zasílat maximálně 5 dotazů na narušení zabezpečení denně. Služba Trial Cloud Service se poskytuje bez záruky, "jak je" a Zákazník ji smí využívat výhradně pro interní testování a neproduktivní použití. Doba reakce na dotazy se může během zkušebního období lišit v závislosti na úrovni provozu.

2. Popis zabezpečení

Tato Cloud Service splňuje zásady zabezpečení dat a ochrany soukromí IBM, které jsou k dispozici na adrese http://www-03.ibm.com/software/sla/sladb.nsf/sla/dsp, a další dodatečné podmínky uvedené v této části. Jakákoli změna zásad zabezpečení a ochrany soukromí IBM nesníží zabezpečení služby Cloud Service.

Tuto službu Cloud Service lze využívat ke zpracovávání vybraného obsahu, který zahrnuje osobní údaje, pokud Zákazník jako správce dat rozhodne, že technické a organizační bezpečnostní opatření jsou přiměřená rizikům spojeným se zpracováním a povahou dat, které je třeba chránit. Zákazník uznává, že tato služba Cloud Service nenabízí funkce pro ochranu citlivých osobních údajů nebo údajů, na něž se vztahují další regulační požadavky. Zákazník potvrzuje, že společnost IBM nezná typy údajů, které byly zahrnuty do obsahu, a že neprovádí posouzení vhodnosti služby Cloud Service nebo uplatněných bezpečnostních ochran.

Služba Cloud Service umožní Zákazníkovi zadávat a spravovat pouze následující obsah, přičemž některé jeho části mohou být v souladu se zákony o ochraně osobních údajů považovány za osobní údaje ("OÚ"):

- Cílová/Zdrojová adresa IP
- URL
- Domény

- Hašování souboru

2.1 Funkce zabezpečení a odpovědnost

Služba Cloud Service zahrnuje následující bezpečnostní funkce:

Služba Cloud Service šifruje obsah během přenosu dat mezi sítí společnosti IBM a nasazením IBM Security QRadar Zákazníka. Služba Cloud Service nešifruje obsah, je-li nečinná a čeká na přenos dat.

Služba Cloud Service neuchovává ani neukládá zadaný obsah po provedení své funkce s příslušnými daty.

3. Technická podpora

Technická podpora pro službu Cloud Service je poskytována prostřednictvím e-mailu, online fór a online systému hlášení problémů. Technická podpora je nabízena se službou Cloud Service a není dostupná jako samostatná nabídka.

Závažnost	Definice Závažnosti	Cílové hodnoty doby odezvy	Pokrytí doby odezvy
1	**Kritický dopad na obchodní činnost/selhání služby:** Funkčnost, která je rozhodující pro obchodní činnost, není provozuschopná nebo došlo k selhání kritického rozhraní. Tato Závažnost se obvykle vztahuje na produktivní prostředí a označuje neschopnost přístupu ke službám, která má za následek kritický dopad na provoz. Tento stav vyžaduje okamžité řešení.	Do jedné hodiny	24 x 7
2	**Významný dopad na obchodní činnost:** Komponenta nebo funkce služby je, pokud jde o užívání, vážně omezena nebo hrozí nedodržení obchodních termínů Zákazníka.	Do dvou hodin (v průběhu pracovní doby)	Pondělí až pátek, v průběhu pracovní doby
3	**Mírný dopad na obchodní činnost:** Službu nebo funkčnost lze používat a dopad na provoz není kritický.	Do čtyř hodin (v průběhu pracovní doby)	Pondělí až pátek, v průběhu pracovní doby
4	**Minimální dopad na obchodní činnost:** Dotaz nebo netechnický požadavek.	Do jednoho pracovního dne	Pondělí až pátek, v průběhu pracovní doby

Pro Zákazníky, kteří se podíleli na beta testování služby Cloud Service a dosud používají verzi 7.2.7 QRadar Platform, nemusí být možné vyřešit některé problémy technické podpory a tito Zákazníci budou muset provést upgrade na 7.2.8 a nainstalovat nejnovější opravu, aby získali plnou technickou podporu.

4. Oprávnění a informace o fakturaci

4.1 Metriky poplatků

Služba Cloud Service je poskytována v rámci metriky poplatků uvedené v Transakčním dokumentu:

a. **100 událostí za sekundu** – je měrnou jednotkou, na jejímž základě lze získat Cloud Service. Událost je výskyt specifické události, která je zpracovávána nebo souvisí s použitím služby Cloud Service. Je nutno získat dostatečný počet oprávnění na pokrytí počtu Událostí za sekundu zaokrouhleno nahoru na celé stovky, k nimž dojde během období měření stanoveného v Dokumentu o oprávnění (Proof of Entitlement) nebo Transakčním dokumentu.

5. Smluvní období a možnost obnovení

Smluvní období pro poskytování služby Cloud Service začíná datem, kdy IBM Zákazníkovi oznámí, že mu byl udělen přístup ke službě Cloud Service, jak je uvedeno v Dokumentu o oprávnění (Proof of Entitlement). Dokument o oprávnění určí, zda se Cloud Service obnovuje automaticky, je používána nepřetržitě, nebo zda je po uplynutí smluvního období ukončena.

V případě automatického obnovení platí, že pokud Zákazník neposkytne alespoň 90 dní před datem ukončení období písemné oznámení o záměru nabídku neobnovit, bude služba Cloud Service automaticky obnovena na období uvedené v Dokumentu o oprávnění (Proof of Entitlement).

V případě průběžného používání bude služba Cloud Service dále dostupná na měsíční bázi, dokud Zákazník neposkytne 90 dní předem písemnou výpověď. Po ukončení takového 90denního období zůstane služba Cloud Service k dispozici do konce kalendářního měsíce.

6. Aktivační software

Služba Cloud Service vyžaduje použití aktivačního softwaru, který si Zákazník stáhne do svých systémů pro usnadnění používání služeb Cloud Service. Zákazník je oprávněn používat aktivační software výhradně ve spojení s užíváním služby Cloud Service. Aktivační software se poskytuje "tak, jak je".

Aktivační software pro službu Cloud Service je Zákazníkovi k dispozici ke stažení z aplikace IBM Security App Exchange na adrese https://exchange.xforce.ibmcloud.com/hub.

7. Dodatečné podmínky

7.1 Obecné

Zákazník souhlasí, že IBM může Zákazníka veřejně označovat jako odběratele služby Cloud Service v reklamních nebo marketingových sděleních.

7.2 Aktivační software

Služba Cloud Service vyžaduje použití aktivačního softwaru, který si Zákazník stáhne do svých systémů pro usnadnění používání služeb Cloud Service. Zákazník je oprávněn používat aktivační software výhradně ve spojení s užíváním služby Cloud Service. Aktivační software se poskytuje "tak, jak je".

Aktivační software pro službu Cloud Service je Zákazníkovi k dispozici ke stažení z aplikace IBM Security App Exchange na adrese https://exchange.xforce.ibmcloud.com/hub.

7.3 Použití Cloud Service v souladu se zákony

Účelem Cloud Service je pomoct 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 uchovávání. 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.

7.4 Uplynutí doby platnosti služby Cloud Service

Před uplynutím doby platnosti nebo ukončením služby Cloud Service může Zákazník používat libovolné funkce reportingu nebo exportu služby Cloud Service k extrahování dat.

7.5 Zabezpečení dat

V rámci služby Cloud Service, která zahrnuje činnosti vytváření sestav, bude IBM připravovat a uchovávat neidentifikované anebo agregované informace shromážděné ze služby Cloud Service ("Data zabezpečení"). S výjimkou ustanovení v bodě (d) níže nebudou Data zabezpečení identifikovat Zákazníka ani jiné fyzické osoby. Zákazník dále vyjadřuje souhlas s tím, že IBM je oprávněna používat anebo kopírovat Data zabezpečení pouze k následujícím účelům:

a. Publikování anebo distribuce Dat zabezpečení (např. v kompilacích anebo analýzách týkajících se kybernetické bezpečnosti).

b. vývoj a vylepšení produktů nebo služeb;

c. interní výzkum nebo výzkum realizovaný se třetími osobami; a

d. sdílení informací o potvrzeném pachateli, který je třetí osobou, v souladu se zákonem.