IBM Resilient Incident Response Platform On Cloud

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

1. Cloud Service

Služba IBM Resilient Incident Response Platform on Cloud poskytuje dynamické akční plány (od malwaru přes útoky typu DDoS až po ztráty zařízení), stejně tak jako doporučené postupy obecné reakce na incidenty. Tato znalostní báze slouží jako průvodce týmu Zákazníka pro reakce na incidenty a je možné ji nakonfigurovat podle jedinečných provozních procedur Zákazníka.

Prostřednictvím produktu IBM Resilient Incident Response Platform on Cloud mohou týmy své reakce na incidenty přímo spravovat a v tomto prostředí spolupracovat. Produkt IBM Resilient Incident Response Platform na rozdíl od systémů vytváření požadavků na podporu (tiketů) a jiných obecných nástrojů IT umožňuje úplnou konfiguraci a byl vytvořen speciálně pro účely reakcí na incidenty. Prostřednictvím prakticky neomezených analýz, přizpůsobitelných panelů dashboard a výkonných funkcí pro tvorbu sestav mají vyšší manažeři přístup ke všem klíčovým informacím.

Produkt IBM Resilient Incident Response Platform byl navržen pro organizace nejrůznějších velikostí i uspořádání a nabízí se v několika verzích s možností samostatného objednávání:

1.1 IBM Resilient Incident Response Platform Enterprise on Cloud

Produkt IBM Resilient Incident Response Platform Enterprise on Cloud představuje řešení služby Cloud Service navržené pro velké a různorodé systémy nejvýznamnějších podniků. Představuje základnu pro plánování, správu a zmírňování reakcí u různých organizací a různých typů incidentů. Uživatelé mohou vytvářet plány reakce na incidenty na základě oborových standardů a doporučených postupů; dále mohou sledovat průběh incidentů až do jejich vyřešení. Služba Cloud Service usnadňuje jednotnou spolupráci napříč celou organizací, a umožňuje tak různým zainteresovaným osobám realizovat jejich role i úlohy v rámci reakcí na incidenty. Produkt umožňuje i simulaci incidentů za účelem testování plánů reakce, zjišťování případných mezer a zlepšování celého procesu reakce. Doplňování incidentů a artefaktů se automatizuje díky vestavěné integraci různých analytických zdrojů externích hrozeb. Služba Cloud Service zahrnuje znalostní bázi globálních předpisů pro oznamování případů porušení ochrany dat, což usnadňuje další přizpůsobení plánů reakce na incidenty. Data je také možné slučovat z existujících bezpečnostních a IT systémů za účelem poskytování informací prakticky v reálném čase. V rámci služby Cloud Service je možné automatizovat, optimalizovat nebo odlaďovat nejrůznější úlohy i bez zapojení vlastního vývoje. Zákazník si musí pořídit nejméně jedno (1) oprávnění k Instanci a jednoho (1) Oprávněného uživatele pro tuto službu.

1.2 IBM Resilient Incident Response Platform Standard on Cloud

Produkt IBM Resilient Incident Response Platform Standard on Cloud představuje řešení služby Cloud Service navržené k řešení požadavků reakce na incidenty malých až středních podniků. Nabízí přibližně stejné funkce jako produkt IBM Resilient Incident Response Platform Enterprise on Cloud, s výjimkou následujících vlastností a funkcí, které Zákazník nemá povoleno využívat: předpisy týkající se porušení ochrany dat, automatizace/koordinace, analytické zdroje hrozeb, vlastní zdroje hrozeb a integrace LDAP. Zákazník si musí pořídit nejméně jedno (1) oprávnění k Instanci a jednoho (1) Oprávněného uživatele pro tuto službu.

1.3 Volitelné služby

1.3.1 IBM Resilient Incident Response Platform Enterprise for Non-Production Environment on Cloud

Produkt IBM Resilient Incident Response Platform Enterprise for Non-Production Environment on Cloud představuje samostatnou instanci služby IBM Resilient Incident Response Platform, kterou je Zákazník oprávněn využívat výhradně v rámci interních neproduktivních aktivit, včetně - nikoli však pouze - testování, ladění výkonu, diagnostiky chyb, interních benchmarkových testů, aktivit souvisejících se zajištěním jakosti anebo vývojem interně používaných doplňků nebo rozšíření nabídky Cloud Service s využitím zveřejněných rozhraní API.

1.4 Vzdálené služby

Následující Vzdálené služby je možné objednávat samostatně, přičemž platnost každé z těchto služeb vyprší devadesát (90) dnů od data zakoupení bez ohledu na to, zda byly vyčerpány všechny služby, na které má Zákazník nárok (je-li relevantní):

1.4.1 IBM Resilient Incident Response Platform Integration for Cloud

Tato nabídka obsahuje integrační služby k propojení služby Cloud Service se souvisejícími systémy zabezpečení a řízení na základě předem definované integrace. K jednomu Oprávnění se vztahuje pouze jedna integrace s jedním systémem. Níže jsou uvedeny integrace dostupné k nastavení touto Vzdálenou službou:

- **Integrace s produktem QRadar**

  Tato integrace umožňuje produktu QRadar automaticky (nebo ručně) odesílat do služby Cloud Service výstrahy o porušení v podobě nových incidentů. Zahrnuje obousměrnou synchronizaci poznámek, událostí uzavření a dat k novým výstrahám o porušení.

- **Integrace s produktem HP Arcsight**

  Pomocí této integrace mohou uživatelé produktu ArcSight ručně (nebo automaticky) odesílat podrobnosti událostí Arcsight do služby Cloud Service v podobě nových incidentů, resp. přidávat artefakty do existujících incidentů.

- **Integrace s produktem Splunk**

  Tato integrace umožňuje produktu Splunk automaticky odesílat do služby Cloud Service výstrahy v podobě incidentů. Dotazy na Splunk může zákazník spouštět i přímo z webového rozhraní služby Cloud Service.

- **Integrace s produktem ServiceNow**

  Prostřednictvím této integrace mohou uživatelé produktu ServiceNow vytvářet incidenty ve službě Cloud Service; uživatelé služby Cloud Service pak mohou vytvářet tikety v produktu ServiceNow. Mezi oběma systémy se dále replikují aktualizace tiketů nebo incidentů.

- **Integrace s produktem JIRA**

  Prostřednictvím této integrace mohou uživatelé produktu JIRA vytvářet incidenty ve službě Cloud Service na základě tiketů JIRA; uživatelé služby Cloud Service pak mohou vytvářet tikety v produktu JIRA. Mezi oběma systémy se dále replikují aktualizace tiketů nebo incidentů.

1.4.2 IBM Resilient Incident Response Platform Design Session for Cloud

Tato služba obsahuje konzultační služby s cílem optimalizovat instanci služby Cloud Service u Zákazníka. Konzultanti IBM ve spolupráci se Zákazníkem slučují existující Zákazníkovy procesy reakce na incidenty až pro tři (3) různé typy incidentů, upřesňují tyto procesy na základě aktuálních doporučených postupů v daném odvětví a podle možností služby Cloud Service, a dále radí Zákazníkovi s konfigurací služby Cloud Service za účelem implementace těchto postupů.

2. Popis zabezpečení

Tato služba Cloud Service splňuje zásady IBM pro zabezpečení dat a ochranu soukromí IBM SaaS, které jsou k dispozici na adrese http://www.ibm.com/cloud/data-security, a další dodatečné podmínky uvedené v této části. Jakákoli změna zásad zabezpečení a ochrany soukromí IBM nesníží zabezpečení služby Cloud Service.

Tato služba Cloud Service není navržena podle žádných konkrétních požadavků na zabezpečení pro regulovaný obsah, například pro osobní údaje nebo citlivé osobní informace. Zákazník nese odpovědnost za určení toho, zda tato služba Cloud Service uspokojuje potřeby Zákazníka s ohledem na typ obsahu, který Zákazník ve spojitosti se službou Cloud Service používá.

3. Smlouva o úrovni služeb

IBM poskytuje pro službu Cloud Service následující dohodu o úrovni služeb, jak je uvedeno v Dokumentu o oprávnění (Proof of Entitlement). Dohoda o úrovni služeb nepředstavuje záruku. Dohoda o úrovni služeb je k dispozici pouze pro Zákazníka a vztahuje se pouze na používání v produktivních prostředích.

3.1 Kredity za porušení úrovně dostupnosti služeb

Zákazník musí u IBM střediska technické podpory zaregistrovat požadavek na podporu se Závažností 1 do 24 hodin od okamžiku, kdy poprvé zjistil, že událost měla dopad na dostupnost služby Cloud Service. Zákazník musí s IBM přiměřeně spolupracovat při diagnostice a řešení problémů.

Nárok na požadavek podpory za nesplnění dohody o úrovni služeb musí být předložen do tří pracovních dní od konce smluvního měsíčního období. Kompenzací za platný nárok týkající se smlouvy o úrovni služeb bude kredit vydaný oproti budoucí faktuře za Cloud Service na základě doby, během které nebylo zpracování produktivního systému pro Cloud Service k dispozici ("Odstávka"). Odstávka se měří od okamžiku, kdy Zákazník nahlásí událost, do okamžiku obnovení Cloud Service a nezahrnuje čas související s plánovanou nebo nahlášenou odstávkou v rámci údržby, příčinami mimo kontrolu IBM, problémy s obsahem, technologií Zákazníka nebo třetí osoby, návrhy nebo pokyny, nepodporovanými konfiguracemi systému a platformami nebo jinými chybami Zákazníka či incidentem zabezpečení způsobeným Zákazníkem nebo testováním zabezpečení Zákazníka. IBM bude aplikovat nejvyšší použitelnou kompenzaci vycházející ze souhrnné dostupnosti služby Cloud Service dosažené během každého smluvního měsíčního období, jak je uvedeno v tabulce níže. Celková kompenzace vztahující se k jakémukoliv smluvnímu měsíčnímu období nesmí přesáhnout deset procent z jedné dvanáctiny (1/12) ročního poplatku za službu Cloud Service.

3.2 Úrovně služeb

Dostupnost služby Cloud Service v průběhu smluvního měsíčního období

Dostupnost v průběhu smluvního měsíčního období	**Kompenzace (% měsíčního registračního poplatku* za smluvní měsíční období, za které je uplatňován nárok)**
99,5 %	2 %
98 %	5 %
96 %	10 %

* Pokud byla služba Cloud Service získána od Obchodního partnera IBM, bude měsíční registrační poplatek vypočítán na základě aktuálního ceníku pro Cloud Service, který je platný pro smluvní měsíční období, na které se nárok vztahuje, se slevou 50 %. IBM Zákazníkovi přímo poskytne slevu.

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.

Příklad: 500 minut celkové Odstávky za smluvní měsíční období

Celkem 43 200 minut za 30denní Smluvní měsíční období - 500 minut Odstávky = 42 700 minut _____ Celkem 43 200 minut	= Kredity za porušení úrovně dostupnosti služeb = 2 % pro 98,8% dostupnost během Smluvního měsíčního období

4. 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. Technická podpora je k dispozici v běžné pracovní době od 9:00 do 18:00 vých. času (kromě svátků).

Závažnost	Definice Závažnosti	Cílové hodnoty doby odezvy během hodin podpory
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
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)
3	**Mírný dopad na obchodní činnost:** Službu nebo funkčnost lze používat a dopad na provoz není kritický.	Do čtyř hodin (v průběhu pracovní doby)
4	**Minimální dopad na obchodní činnost:** Dotaz nebo netechnický požadavek.	Do jednoho pracovního dne

5. Oprávnění a informace o fakturaci

5.1 Metriky poplatků

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

a. **Instance** – je měrnou jednotkou, na jejímž základě lze získat Cloud Service. Instance je přístup ke specifické konfiguraci služby Cloud Service. Pro každou Instanci Cloud Service zpřístupněnou a používanou během období měření uvedeného v Zákazníkově Dokumentu o oprávnění (Proof of Entitlement) nebo Transakčním dokumentu Zákazníka je nutno získat dostatečný počet oprávnění.

b. **Oprávněný uživatel** – je měrnou jednotkou, na jejímž základě lze získat Cloud Service. Zákazník je povinen získat samostatná, vyhrazená oprávnění pro každého jedinečného Oprávněného uživatele, kterému byl udělen přístup ke službě Cloud Service jakýmkoli způsobem přímo či nepřímo (například prostřednictvím multiplexovacího programu, zařízení nebo aplikačního serveru). Je nutno získat dostatečný počet oprávnění, který bude pokrývat počet Oprávněných uživatelů, kterým byl udělen přístup ke službě Cloud Service během období měření uvedeného v Dokumentu o oprávnění (Proof of Entitlement) nebo v Transakčním dokumentu Zákazníka.

c. **Sjednaná služba** – je měrnou jednotkou, na jejímž základě lze získat služby. Sjednaná služba sestává z odborných služeb a/nebo ze služeb v oblasti vzdělávání týkajících se služby Cloud Service. Je nutno získat dostatečný počet oprávnění, který bude pokrývat každou Sjednanou službu.

5.2 Poplatky za překročení limitu

Pokud skutečné užívání služby Cloud Service Zákazníkem během období měření překročí oprávnění uvedená v Dokumentu o oprávnění (Proof of Entitlement), bude Zákazníkovi takové překročení limitu účtováno v souladu s Transakčním dokumentem.

5.3 Poplatky za vzdálené služby

Vzdálené služby lze zakoupit na základě metriky Sjednané služby a budou fakturovány za sazbu uvedenou v Transakčním dokumentu.

6. 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 90 dní před datem ukončení období písemné oznámení o záměru nabídku neobnovit, bude Cloud Service automaticky obnovena na období uvedené v Dokumentu o oprávnění (Proof of Entitlement).

V případě průběžného používání bude 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.

7. Dodatečné podmínky

7.1 Obecná ustanovení

Zákazník souhlasí s tím, že IBM je oprávněna Zákazníka veřejně označovat jako odběratele služeb Cloud Service v reklamních nebo v marketingových sděleních.

7.2 Služba Compliance Management Cloud Service

Tato služba Cloud Service může Zákazníkovi pomoci zajistit dodržování závazků, jež pro něj mohou vyplývat z právních předpisů, norem nebo postupů. Zákazník bere na vědomí a souhlasí s tím, že jakékoli pokyny, informace týkající se doporučeného užívání nebo jiné pokyny, které Zákazník získá prostřednictvím služby Cloud Service, nepředstavují právní, účetní nebo jinou odbornou radu, přičemž Zákazník by si měl zajistit vlastní právní, účetní nebo jinou odbornou konzultaci. Zákazník rovněž souhlasí s tím, že nese výhradní odpovědnost za dodržování všech příslušných právních předpisů, nařízení, standardů a postupů. Totéž platí pro všechny jeho činnosti, aplikace a systémy. Užívání služby Cloud Service nezaručuje soulad s požadavky právních předpisů, nařízení, standardů nebo postupů.

7.3 Použití Cloud Service v souladu s právními předpisy

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 Zabezpečení dat

V rámci služby Cloud Service, která zahrnuje činnosti vytváření sestav, bude IBM připravovat a uchovávat neidentifikované a/nebo agregované informace shromážděné ze služby Cloud Service ("Data zabezpečení"). S výjimkou ustanovení (d) níže nebudou Data zabezpečení identifikovat Zákazníka ani jiné 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.

7.5 Soubory cookie

Zákazník si je vědom skutečnosti a vyjadřuje svůj souhlas s tím, že IBM smí v rámci své běžné činnosti a podpory služby Cloud Service od Zákazníka (jeho zaměstnanců a smluvních partnerů) shromažďovat osobní údaje týkající se užívání služby Cloud Service prostřednictvím sledovacích a jiných technologií. IBM tak činí za účelem získání statistik užívání a informací o efektivitě naší služby Cloud Service, které IBM umožní zlepšit zkušenosti uživatelů nebo přizpůsobit vzájemné interakce se Zákazníkem. Zákazník potvrzuje, že získá nebo získal souhlas, který IBM uděluje oprávnění zpracovávat, v souladu s příslušnými právními předpisy, shromážděné osobní údaje pro výše uvedené účely v rámci IBM, jiných společností IBM a jejích subdodavatelů, kdekoli IBM a její subdodavatelé provádějí obchodní činnost. IBM vyhoví požadavkům zaměstnanců a smluvních partnerů Zákazníka, pokud jde o přístup, aktualizaci, opravu nebo vymazání jejich shromážděných osobních údajů.