Popis služeb IBM Cloud Service

IBM Security AppScan Mobile Analyzer

Níže je uveden Popis služeb pro Vaši Objednávku:

1. Cloud Service

Nabídka Cloud Service pro vybrané způsobilé nabídky je popsána níže a je specifikována v Objednávce. Objednávka bude zahrnovat předkládanou Cenovou nabídku a Dokument o oprávnění (Proof of Entitlement) uvádějící datum zahájení a smluvní období pro služby Cloud Service. Fakturace bude zahájena po poskytnutí služby Cloud Service.

1.1 IBM Security AppScan Mobile Analyzer

Tato služba identifikuje záležitosti zabezpečení na úrovni kódu mobilních aplikací pro systém Android. Umožňuje vývojáři vyhledávat ohrožení zabezpečení bez potřeby zadání zdrojového kódu aplikace. Na konci vyhledávání služba vygeneruje report zabezpečení, který zahrnuje podrobnosti o zjištěných ohroženích zabezpečení, možných bezpečnostních rizicích mobilní aplikace způsobených těmito ohroženími a návrh, jak tento stav opravit.

2. Popis zabezpečení

2.1 Zásady zabezpečení

IBM má tým pro zabezpečení informací a dodržuje zásady v oblasti zabezpečení a ochrany soukromí a seznamuje s nimi své zaměstnance. IBM vyžaduje, aby zaměstnanci, kteří poskytují podporu datovým střediskům, byli proškoleni v oblasti zabezpečení a ochrany soukromí. Zásady a standardy IBM v oblasti zabezpečení jsou každoročně přezkoumávány a přehodnocovány. Bezpečnostní incidenty IBM jsou zpracovávány v souladu s komplexním postupem reagování na incidenty.

2.2 Řízení přístupu

Přístup k datům Zákazníka, je-li vyžadován, je umožněn pouze oprávněným zástupcům podpory a pracovníkům servisu IBM v souladu s principy segregace povinností. Ve vztahu k hostiteli pro mezilehlého správce "brány" používají pracovníci IBM dvouúrovňové ověření. Při přístupu k datům Zákazníka se pro všechna připojení používají šifrované kanály.

2.3 Integrita a dostupnost služeb

Úpravy operačního systému a aplikačního softwaru se řídí procesem řízení změn IBM. Změny v nastavení brány firewall rovněž podléhají procesu řízení změn a před implementací jsou přezkoumávány bezpečnostními pracovníky IBM. IBM monitoruje datová střediska 24 hodin denně, 7 dní v týdnu. Na podporu detekce a řešení potenciálního ohrožení zabezpečení systému je oprávněnými administrátory a dodavateli, kteří jsou třetími stranami, prováděno pravidelné interní i externí skenování ohrožení zabezpečení. Ve všech datových střediscích IBM jsou používány systémy na detekci malwaru (antivirové programy, detekce neoprávněného vniknutí a ochrana před ním, skenování ohrožení zabezpečení). Služby datových středisek IBM podporují řadu doručovacích protokolů pro přenos dat prostřednictvím veřejných sítí. Jedná se například o HTTPS/SFTP/FTPS/S/MIME a site-to-site VPN. Zálohovaná data určená pro uložení mimo pracoviště jsou před přenosem šifrována.

2.4 Protokolování aktivit

IBM uchovává protokoly aktivit pro systémy, aplikace, datová úložiště, middleware a zařízení síťové infrastruktury, které umožňují protokolovat aktivitu a jsou pro tento účel nakonfigurovány. Aktivita je protokolována v reálném čase do centrálních úložišť protokolů, což umožňuje minimalizovat pravděpodobnost neoprávněných zásahů, umožňuje centrální provádění analýzy, zasílání výstražných zpráv a tvorbu reportů. Aby se zabránilo neoprávněným zásahům, jsou data opatřena podpisem. Analýza protokolů se provádí v reálném čase prostřednictvím pravidelných analytických reportů umožňujících detekci abnormálního chování. Operátoři jsou upozorňováni na anomálie a v případě potřeby mohou 24 hodin denně, 7 dní v týdnu telefonicky kontaktovat bezpečnostního specialistu.

2.5 Fyzické zabezpečení

IBM dodržuje standardy v oblasti fyzického zabezpečení, jejichž účelem je omezení neoprávněného fyzického přístupu do datových středisek IBM. Přístup do datových středisek je možný pouze omezenými přístupovými body, pro něž platí režim dvouúrovňového ověření a které jsou monitorovány sledovacími kamerami. Přístup je umožněn pouze oprávněným pracovníkům s povoleným přístupem. Operátoři ověří povolení k přístupu a vydají přístupovou kartu umožňující nezbytný přístup. Zaměstnanci, jimž byly vydány takové přístupové karty, musí odevzdat ostatní přístupové karty a po dobu jejich činnosti smí mít u sebe pouze přístupové karty pro přístup do datového střediska. Používání přístupových karet je evidováno. Návštěvníci, kteří nejsou pracovníky IBM, jsou při vstupu do budovy zaregistrováni a po budovách se pohybují v doprovodu. Zásobovací a nakládací oblasti a další místa, jimiž mohou do prostor vniknout neoprávněné osoby, jsou hlídány a izolovány.

2.6 Dodržování požadavků

IBM certifikuje své postupy v oblasti ochrany soukromí vždy jednou ročně z hlediska souladu se zásadami U.S. Department of Commerce's Safe Harbor Principles: Notice, Choice, Onward Transfer, Access and Accuracy, Security, and Oversight/Enforcement. IBM provádí ve svých datových střediscích vždy jednou ročně audit dle odvětvového standardu SSAE 16 (nebo ekvivalentní audit). IBM přezkoumává činnosti související se zabezpečením a ochranou soukromí z hlediska dodržování obchodních požadavků IBM. IBM pravidelně provádí hodnocení a prověřování, jejichž cílem je ověřit dodržování zásad zabezpečení informací. Zaměstnanci IBM a dodavatelů absolvují jednou ročně školení pro zaměstnance zaměřené na zabezpečení a zvyšování povědomí o zabezpečení. Zaměstnancům jsou vždy jednou ročně připomínány jejich pracovní cíle a povinnosti ohledně dodržování etického obchodního chování, ochrany důvěrných informací a závazků IBM v oblasti zabezpečení.

3. Oprávnění a informace o fakturaci

3.1 Metriky poplatků

Cloud Service je dostupná na základě níže uvedené metriky poplatků, jak je uvedeno v Objednávce.

- Instance aplikace je měrnou jednotkou, na jejímž základě lze získat IBM SaaS. Pro každou Aplikaci připojenou k IBM SaaS je vyžadováno oprávnění Instance aplikace. Pokud má Aplikace více komponent, každá z nich slouží k jinému účelu nebo jiné uživatelské základně a každá z nich může být připojena k nabídce IBM SaaS nebo může být nabídkou spravována, považuje se každá taková komponenta za samostatnou Aplikaci. Navíc testovací, vývojové, fázovací a produktivní prostředí Aplikace se považují za samostatné instance Aplikace a každé toto prostředí musí mít oprávnění. Více instancí Aplikace v jednom prostředí se považuje za samostatné instance Aplikace a musí mít oprávnění. Je nutno získat dostatečný počet Oprávnění, který bude pokrývat počet Instancí aplikace připojených k IBM SaaS během období měření uvedeného v Dokumentu o oprávnění (Proof of Entitlement) nebo v Transakčním dokumentu Zákazníka.

3.2 Poplatky a fakturace

Výše platby za službu Cloud Service je specifikována v Objednávce.

3.3 Pay as you Go

Volby Pay as you Go budou fakturovány v měsíci následujícím po použití služby, a to za sazbu uvedenou v Transakčním dokumentu.

4. Technická podpora

Technická podpora pro Cloud Service je poskytována během Období registrace.

Provozní doba podpory je následující:

Informace o hodinách dostupnosti, online systémech pro hlášení problémů a ostatních nástrojích a procesech komunikace s technickou podporou naleznete v příručce IBM Software as a Service Support Handbook.

Podpora po pracovní době

Podpora po pracovní době (mimo výše uvedenou řádnou provozní dobu) je dostupná během pracovních dní, víkendů a státních svátků pouze pro problémy se Závažností 1. Problémy se Závažností 1 vyžadují, aby byl klient 24 hodin denně, 7 dní v týdnu k dispozici a mohl poskytnout pomoc při diagnostice problémů. Není-li tato podmínka splněna, je Závažnost 1 změněna na Závažnost 2.

4.1 Fórum podpory

Všichni klienti služby Cloud Service mají k dispozici fórum podpory, které je pravidelně sledováno zástupci podpory a vývojáři IBM.

a. Ptejte se:

https://developer.ibm.com/answers/questions/ask/?topics=appscan-mobile-analyzer

b. Procházejte aktuální příspěvky:

https://developer.ibm.com/answers/topics/appscan-mobile-analyzer/

4.2 Standardní podpora

Standardní podpora je poskytována během období, ve kterém jsou klientovi účtovány poplatky Pay as you Go. Ze služby Cloud Service mohou klienti odeslat tiket podpory nebo zahájit relaci konverzace a požádat o asistenci. Další informace o postupech podpory naleznete na webovém portále podpory IBM na adrese https://support.ibmcloud.com nebo v příručce IBM SaaS Software Support Handbook na adrese: http://www.ibm.com/software/support/acceleratedvalue/SaaS_Handbook_V18.pdf.

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 hodin, 7 dní v týdnu
2	**Významný dopad na obchodní činnost:** Obchodní komponenty nebo funkce služby jsou, pokud jde o jejich užívání, vážně omezeny nebo hrozí nedodržení obchodních termínů.	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

5. Soulad s Pravidly Safe Harbor

IBM se nevyjádřila, zda tato služba Cloud Service odpovídá požadavkům Pravidel Safe Harbor, která se týkají shromažďování, používání a uchovávání dat z Evropské unie a Švýcarska.

6. Další informace

Tato služba Cloud Service je určena k identifikaci širokého spektra potenciálních problémů týkajících se zabezpečení a dodržování právních předpisů v oblasti mobilních aplikací a mobilních webových služeb. Netestuje všechna ohrožení zabezpečení nebo všechna rizika v oblasti dodržování právních předpisů, ani nefunguje jako bariéra proti útokům na zabezpečení. Bezpečnostní rizika, regulace a standardy se průběžně mění a Služba nemůže všechny takové změny zohledňovat. Zákazník odpovídá za zabezpečení svých mobilních aplikací, systémů a zaměstnanců a za dodržování právních předpisů a rovněž za jakékoli nápravné akce samostatně. Záleží výhradně na uvážení Zákazníka, zda bude, či nebude využívat jakékoli informace poskytnuté Službou.

6.1 Lokality, v nichž jsou využívány výhody

V případech, kdy je to relevantní, budou daně založeny na lokalitě(ách), kterou(é) jste uvedli jako místo, kde využíváte výhod služeb Cloud Service. IBM uplatní daně na základě obchodní adresy, která byla při objednání služby Cloud Service uvedena jako primární lokalita pro využívání výhod, ledaže byste IBM poskytli doplňující informace. Nesete odpovědnost za aktualizaci takových informací a za informování IBM o jakýchkoli změnách.

6.2 Soubory cookie

Jste si vědomi a souhlasíte, že IBM smí v rámci své běžné obchodní činnosti a podpory služby Cloud Service od Vás (Vašich 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 a/nebo přizpůsobit vzájemné interakce. Potvrzujete, že získáte nebo jste získali souhlas, který IBM povoluje 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 Vašich zaměstnanců a smluvních partnerů, pokud jde o přístup, aktualizaci, opravu nebo vymazání jejich shromážděných osobních údajů.