IBM Resilient Security Orchestration, Automation and Response on Cloud

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 Resilient Security Orchestration, Automation, and Response (SOAR) Platform on Cloud umožňuje organizacím koordinovat a automatizovat lidi, procesy a technologie, které souvisejí s reakcí na incidenty.

IBM Resilient SOAR Platform on Cloud zefektivňuje reakci na incidenty a řízení reakce ochrany soukromí pro zajištění automatizovaného, rychlejšího a flexibilnějšího způsobu reakce organizací na události a incidenty. Resilient SOAR Platform on Cloud poskytuje základy pro úspěšnou obranu kybernetické bezpečnosti, která organizacím umožňuje:

- vytvářet plány odezvy vycházející z odvětvových standardů a doporučených postupů,
- jednodušeji integrovat se zabezpečením a nástroji IT, stejně jako koordinovat reakce na události a nehody,
- spolupracovat napříč organizací a poskytovat zainteresovaným stranám nástroje nezbytné pro plnění jejich rolí a úkolů v rámci snahy reakce na incident.

IBM Resilient SOAR Platform je určena organizacím různé velikosti a složitosti a lze ji zakoupit s několika dalšími volitelnými doplňky. Zákazník není oprávněn používat funkce, pokud nejsou specifikovány v zakoupené nabídce nebo doplňku.

1.1 Nabídky

Zákazník si může vybrat z následujících dostupných nabídek:

1.1.1 IBM Resilient SOAR Platform on Cloud

IBM Resilient SOAR Platform on Cloud Orchestration nabízí základ pro obranu kybernetické bezpečnosti. Zákazníci mohou vytvářet plány reakce na základně odvětvových standardů a doporučených postupů, jednoduše je integrovat se zabezpečením a IT nástroji a koordinovat reakce na události a incidenty. Služba Cloud Service usnadňuje spolupráci napříč organizací a umožňuje jednotlivým zainteresovaným stranám plnit jejich role a úkoly v rámci snah o reakci na incident.

Bezpečnostní týmy mohou spolupracovat na událostech a incidentech kybernetické bezpečnosti s využitím funkcí řízení případu platformy, které byly vytvořeny k tomuto účelu. Dynamic Playbooks se rychle přizpůsobuje rychle se rozvíjejícím útokům a týmy dovedou rychle iterovat procesy a zlepšit efektivitu přizpůsobením playbooků, datových polí a rozvržení zobrazení. Simulace dále pomáhají ve zpřesnění procesů reakce. Zabudované a instalovatelné doplňky poskytují obohacení dat pro získání dalšího kontextu pro rozhodování bezpečnostních týmů a umožnění koordinace akcí v souladu se zakoupeným množstvím Akcí za měsíc. Příjem a syntaktická analýza e-mailů poskytuje odlehčenou metodu eskalace z dalších nástrojů. Přístup lze zajistit ověřením SAML. Analýza transparentnosti a rizik využívá pomoci analytiky a vytváření sestav. Tato nabídka se vyžaduje pro všechny níže uvedené doplňky.

1.2 Volitelné služby

1.2.1 IBM Resilient SOAR Platform Actions on Cloud

IBM Resilient SOAR Platform on Cloud Actions umožňuje funkce koordinace platformy. Zabudované a instalovatelné doplňky včetně doplnění o různé kanály zpravodajských služeb ohledně hrozeb poskytuje automatizované obohacení pro zjištění kontextu pro rozhodování bezpečnostního týmu, stejně jako koordinaci nápravných kroků.

1.2.2 IBM Resilient SOAR Platform on Cloud Privacy Add-On

IBM Resilient SOAR Platform on Cloud Privacy umožňuje Zákazníkům hodnotit narušení ochrany osobních údajů a reagovat na ně. Plány reakce vygenerované touto nabídkou se přizpůsobí typům dat, množství záznamů a příslušným regulačním jurisdikcím. Zákazník rovněž získá přístup k zabudované

databázi znalostí báze globálních předpisů pro oznamování případů porušení ochrany dat, což usnadňuje další přizpůsobení plánů reakce na incidenty.

1.2.3 IBM Resilient SOAR Platform on Cloud Team Management Add-On

IBM Resilient SOAR Platform on Cloud Teams zajišťuje řízení uživatelů a segregaci dat napříč různými týmy. Citlivé informace jsou uchovávány na bázi potřeby s omezením přístupu s pomocí Pracovních míst a nastavitelnou kontrolou přístupu dle rolí. Správu uživatelů a skupin lze zjednodušit využitím Active Directory pro ověření uživatelů. Lze rovněž konfigurovat samostatné skupiny s jejich vlastní Organizací.

1.2.4 IBM Resilient SOAR Platform on Cloud MSSP Add-On

IBM Resilient SOAR Platform on Cloud MSSP zajišťuje správu případu, procesy, přizpůsobení a funkce správy playbooku napříč několika Organizacemi. Události a incidenty z vícero Organizací lze zobrazovat v rámci jediné fronty, což poskytuje analytikům Managed security service provider (MSSP) komplexní přehled o jejich zákaznících. Playbooky s konfigurací pro Organizaci nabízejí jednoduchou správu standardizovaných i přizpůsobených procesů.

1.2.5 IBM Resilient SOAR Platform on Cloud Non-Production Add-On

IBM Resilient SOAR Platform on Cloud Non-Production představuje samostatnou instanci služby IBM Resilient SOAR Platform, kterou je Zákazník oprávněn využívat výhradně v rámci interních neproduktivních aktivit, včetně například 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 programování aplikací.

1.3 Akcelerační služby

Nabídky IBM Security Expert Labs (SEL) for Resilient Services jsou vzdáleně poskytované služby, které poskytují čas odborníků na Resilient pro vedení v oblasti architektury a implementace související s nasazením Resilient. Nabídka IBM Resilient Security, Orchestration and Response – buď formou služby Cloud Service, nebo jako software na místě – je předpokladem pro kteroukoliv z těchto služeb.

1.3.1 IBM SEL for Resilient Base Starter Service

V rámci 5denní vzdálené spolupráce IBM poskytne:

- pomoc při definování architektury IBM Security Resilient;
- nainstalovanou & nakonfigurovanou IBM Security Resilient (v příslušných případech);
- školení pro Analytiky a Návrháře pro konfiguraci a používání aktuálních plánů reakce Zákazníka, které odrážejí klíčové požadavky organizace Zákazníka;
- konfigurované návody k použití IBM Security Resilient na základě jedinečných procesů organizací Zákazníka;
- způsoby sledování definovaných KPI a Metrik v souladu s potřebami organizací Zákazníka a doporučenými postupy v oboru; a
- identifikaci příležitostí k integraci pro podporu, automatizaci a optimalizaci celkového procesu.

1.3.2 IBM SEL for Resilient Premium Starter Service

V rámci 3denní vzdálené spolupráce IBM poskytne:

- pomoc při definování architektury IBM Security Resilient;
- instalaci IBM Security Resilient (v příslušných případech);
- počáteční konfiguraci IBM Security Resilient v prostředí Zákazníka; a
- školení pro Analytiky a Návrháře pro konfiguraci a používání aktuálních plánů reakce Zákazníka, které odrážejí klíčové požadavky jeho organizace.

1.3.3 IBM SEL for Resilient Additional Day

Navíc kromě služeb zahrnutých ve variantách Base nebo Premium Starter, společnost IBM v rámci 1denní vzdálené spolupráce provede veškeré činnosti související s IBM Security Resilient, které budou předem sjednány. Například:

- další podporu pro instalaci nebo konfiguraci IBM Security Resilient nebo rozšíření (v příslušných případech);

- další školení Analytiků pro zajištění připravenosti na použití IBM Security Resilient jako klíčového řešení SOAR Zákazníka;
- vedení Návrhářů o tom, jak konfigurovat a používat jejich vlastní "návody k použití", které budou odrážet klíčové požadavky organizací Zákazníka; nebo
- provedení rychlého skenování prostředí IBM Security Resilient pro doporučení případných oblastí s potenciálem zlepšení.

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 na osobní údaje zahrnuté v Obsahu, pokud se uplatní i) Evropské obecné nařízení o ochraně údajů (EU/2016/679) (GDPR); nebo ii) jiné právní předpisy o ochraně údajů uvedené na adrese http://www.ibm.com/dpa/dpl.

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=A47500205B1911E6865BC3F213DB63F7

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, 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:

- Oprávněný uživatel je jedinečný uživatel, který má oprávnění pro přístup ke službám Cloud Services jakýmkoliv způsobem přímo či nepřímo (například prostřednictvím multiplexovacího programu, zařízení nebo aplikačního serveru) libovolnými prostředky.
- Souběžný uživatel je počet uživatelů, kteří v určitém časovém okamžiku jakýmkoliv způsobem přímo či nepřímo (například prostřednictvím multiplexovacího programu, zařízení nebo aplikačního serveru) souběžně přistupují ke službě Cloud Service. Osoba, která souběžně přistupuje ke službě Cloud Service vícekrát, se počítá za jediného Souběžného uživatele.

- Sjednaná služba je profesionální nebo školicí služba související se službami Cloud Services.
- Položka je výskyt specifické položky, která je spravována či zpracovávána službou Cloud Service nebo souvisí s použitím služby Cloud Service. Pro účely této služby Cloud Service je Položkou Akce. Akce je koordinace nebo automatický požadavek vytvořený službou Cloud Service na jiný softwarový program.

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 Požadavek na dodatečné oprávnění

Zákazník je povinen získat stejný počet a typ oprávnění jak pro základní, tak pro jakoukoliv doplňkovou službu Cloud Service.

5.3 Omezení používání

Každý Zákazník je oprávněn zaslat maximálně jedno sto tisíc (100 000) dotazů na Službu hrozeb za měsíc. Zákazník vytvoří dotaz na Službu hrozeb doplněním artefaktu k incidentu po aktivaci Služby hrozeb. Pro každé dva (2) dny poté, co bude incident otevřený a aktivní, se automaticky vygeneruje nový dotaz Služby hrozeb.

Každý Zákazník je oprávněn vygenerovat maximálně jedno sto (100) oznamovacích e-mailů za den pro každého Oprávněného/Souběžného uživatele. Oznamovací e-maily jsou generovány spolehlivou platformou na základě konfigurace kontrolované Zákazníkem.

5.4 Další zpracování dat a ochrana informací

Aby se zabránilo pochybnostem, platforma IBM Resilient SOAR Platform on Cloud:

- nešifruje neaktivní Obsah (data v klidu);
- není navržena pro zpracovávání jakýchkoliv Speciálních kategorií Osobních údajů; a
- neměla by mít ve volných textových polích osobní údaje, pokud to není vyžadováno.

Podrobné informace ohledně šifrování a typů zpracovávaných Osobních údajů najdete na adrese url pro Datový list, na který se odkazuje v části 2 výše.

6. Přednostní podmínky

6.1 Využití údajů

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.