IBM Resilient Security Orchestration, Automation and Response on Cloud

Niniejszy opis dotyczy Usługi Przetwarzania w Chmurze. Odpowiednie dokumenty zamówienia zawierają ceny i dodatkowe informacje dotyczące zamówienia Klienta.

1. Usługa Przetwarzania w Chmurze

Usługa IBM Resilient Security Orchestration, Automation, and Response (SOAR) Platform on Cloud umożliwia organizacjom orkiestrację i automatyzację działań osób oraz procesów i technologii związanych z reagowaniem na incydenty.

IBM Resilient SOAR Platform on Cloud upraszcza reagowanie na incydenty i przypadki naruszenia prywatności. Dzięki tej usłudze organizacje mogą reagować na zdarzenia i incydenty w sposób zautomatyzowany, szybszy i bardziej elastyczny. Resilient SOAR Platform on Cloud zapewnia podstawę skutecznej ochrony przed zagrożeniami cybernetycznymi i umożliwia organizacjom:

- tworzenie planów reagowania na podstawie standardów branżowych i sprawdzonych procedur;
- łatwiejszą integrację z narzędziami zabezpieczającymi i informatycznymi oraz koordynowanie reakcji na zdarzenia i incydenty;
- centralizację współpracy w całej organizacji oraz wyposażenie różnych interesariuszy w narzędzia, które pozwolą im występować w odpowiednich rolach i realizować zadania związane z reagowaniem na incydenty.

Usługa IBM Resilient SOAR Platform została zaprojektowana z myślą o organizacjach różnej wielkości i o różnym stopniu złożoności. Można ją nabyć z różnymi opcjonalnymi programami dodatkowymi. Klient nie jest uprawniony do korzystania z możliwości, które nie zostały określone w nabytej ofercie lub programie dodatkowym.

1.1 Produkty oferowane

Klient może dokonać wyboru spośród następujących produktów oferowanych:

1.1.1 IBM Resilient SOAR Platform on Cloud

Usługa IBM Resilient SOAR Platform on Cloud Orchestration zapewnia podstawę ochrony przed zagrożeniami cybernetycznymi. Klienci mogą tworzyć plany reagowania oparte na standardach branżowych i sprawdzonych procedurach oraz łatwo integrować te plany z narzędziami zabezpieczającymi i informatycznymi, a także koordynować reakcje na zdarzenia i incydenty. Usługa Przetwarzania w Chmurze pozwala scentralizować współpracę w ramach organizacji, umożliwiając różnym interesariuszom występowanie w odpowiednich rolach oraz realizację zadań związanych z reakcją na incydenty.

Zespoły odpowiedzialne za bezpieczeństwo mogą ze sobą współpracować w przypadku wystąpienia zdarzeń i incydentów dotyczących cyberbezpieczeństwa, wykorzystując dostępne funkcje zarządzania przypadkami utworzone w konkretnym celu. Dynamiczne scenariusze działań dostosowują się do szybko rozwijających się ataków, a zespoły mogą szybko przeprowadzać iterację procesów i zwiększać ich efektywność poprzez odpowiednie modyfikowanie scenariuszy działań, pól danych i układów wyświetlaczy. W dalszym doskonaleniu procesów reagowania pomagają symulacje. Wbudowane i instalowane elementy zintegrowane umożliwiają wzbogacenie danych w celu uzyskania kontekstu, który pomaga zespołom ds. bezpieczeństwa w podejmowaniu decyzji oraz koordynowaniu stosowania środków zaradczych zgodnie z nabytą liczbą Działań na Miesiąc. Pozyskiwanie i analizowanie wiadomości e-mail jest prostą metodą eskalacji problemów z innych narzędzi. Dostęp do systemu może być zabezpieczony za pomocą uwierzytelniania SAML. Analiza danych i raportowanie zwiększają przejrzystość i ułatwiają ocenę ryzyka. Niniejsza oferta jest wymagana dla wszystkich określonych poniżej programów dodatkowych.

1.2 Usługi Opcjonalne

1.2.1 IBM Resilient SOAR Platform Actions on Cloud

Usługa IBM Resilient SOAR Platform on Cloud Actions aktywuje funkcje orkiestracji platformy. Wbudowane i instalowane elementy zintegrowane, w tym kanały dostarczające informacje analityczne o

zagrożeniach, zapewniają automatyczne wzbogacanie danych. Dzięki temu zespoły odpowiedzialne za bezpieczeństwo zyskują kontekst, który ułatwia im podejmowanie decyzji oraz koordynowanie działań naprawczych.

1.2.2 IBM Resilient SOAR Platform on Cloud Privacy Add-On

Usługa IBM Resilient SOAR Platform on Cloud Privacy umożliwia Klientom ocenę przypadków naruszenia ochrony danych oraz reagowanie na te przypadki. Plany reagowania wygenerowane przez tę usługę są dostosowane do typów danych, liczby rekordów oraz obowiązujących przepisów prawnych. Klienci mają również dostęp do wbudowanej bazy wiedzy, która zawiera przepisy z całego świata dotyczące powiadamiania o naruszeniach ochrony danych, dzięki czemu można jeszcze bardziej szczegółowo opracować plany reagowania.

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

Usługa IBM Resilient SOAR Platform on Cloud Teams umożliwia zarządzanie użytkownikami i segregację danych w wielu zespołach. Informacje wrażliwe są przechowywane zgodnie z rzeczywistymi potrzebami, a dostęp do nich jest ograniczany na podstawie obszarów roboczych oraz dostosowywalnych metod kontroli dostępu opartych na rolach. Zarządzanie użytkownikami i grupami można uprościć dzięki wykorzystaniu usługi Active Directory do uwierzytelniania użytkowników. Można również skonfigurować odrębne grupy w taki sposób, aby każda z nich miała własną organizację.

1.2.4 IBM Resilient SOAR Platform on Cloud MSSP Add-On

Usługa IBM Resilient SOAR Platform on Cloud MSSP umożliwia zarządzanie przypadkami, procesami, dostosowaniami i scenariuszami działania w wielu organizacjach. Zdarzenia i incydenty dotyczące wielu organizacji można przeglądać w jednej kolejce, dzięki czemu analitycy z firm świadczących zarządzane usługi zabezpieczeń uzyskują kompleksowy widok danych swoich klientów. Scenariusze działań przygotowane dla każdej z organizacji umożliwiają proste zarządzanie procesami standardowymi i dostosowanymi.

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

Usługa IBM Resilient SOAR Platform on Cloud Non-Production to odrębna instancja platformy IBM Resilient SOAR Response Platform, która może być używana wyłącznie w wewnętrznej działalności pozaprodukcyjnej Klienta, a w szczególności do testowania, dostrajania wydajności, diagnozowania błędów, wykonywania wewnętrznych testów porównawczych, określania czynności z zakresu zapewniania jakości i/lub programowania dodatków lub rozszerzeń do Usługi Przetwarzania w Chmurze przeznaczonych do użytku wewnętrznego za pomocą opublikowanych aplikacyjnych interfejsów programistycznych.

1.3 Usługi przyspieszające

IBM Security Expert Labs (SEL) for Resilient Services to świadczone zdalnie usługi eksperta ds. rozwiązań Resilient w zakresie architektury i implementacji, związane z wdrażaniem rozwiązań Resilient. Wymaganiem wstępnym dla tej usługi jest korzystanie z oferty IBM Resilient Security, Orchestration and Response w postaci Usługi Przetwarzania w Chmurze lub oprogramowania instalowanego lokalnie.

1.3.1 IBM SEL for Resilient Base Starter Service

W ramach realizowanego zdalnie 5-dniowego przedsięwzięcia IBM:

- udzieli pomocy w definiowaniu architektury IBM Security Resilient;
- udostępni zainstalowane i skonfigurowane oprogramowanie IBM Security Resilient (jeśli ma zastosowanie);
- zapewni szkolenie dla analityków i projektantów w zakresie konfigurowania i używania bieżących planów Klienta związanych z reagowaniem na incydenty, odzwierciedlających główne wymagania jednostek organizacyjnych Klienta;
- udostępni skonfigurowane przez zespół IBM Security Resilient scenariusze działań oparte na specyficznych procesach jednostek organizacyjnych Klienta;
- określi sposoby śledzenia zdefiniowanych Wskaźników KPI i Metryk zgodnie z potrzebami jednostek organizacyjnych Klienta i sprawdzonymi procedurami branżowymi;
- zidentyfikuje możliwości integracji w celu wsparcia, automatyzacji i koordynacji kompleksowego procesu.

1.3.2 IBM SEL for Resilient Premium Starter Service

W ramach realizowanego zdalnie 3-dniowego przedsięwzięcia IBM:

- udzieli pomocy w definiowaniu architektury IBM Security Resilient;
- zainstaluje oprogramowanie IBM Security Resilient (jeśli ma zastosowanie);
- wstępnie skonfiguruje oprogramowanie IBM Security Resilient w środowisku Klienta;
- przeszkoli analityków i projektantów w zakresie konfigurowania i używania bieżących planów Klienta związanych z reagowaniem na incydenty, odzwierciedlających główne wymagania jednostek organizacyjnych Klienta.

1.3.3 IBM SEL for Resilient Additional Day

W uzupełnieniu usługi Base Starter lub Premium Starter w ramach realizowanego zdalnie jednodniowego przedsięwzięcia IBM wykona dowolne działania związane z oprogramowaniem IBM Security Resilient o uzgodnionym wcześniej zakresie, na przykład:

- udzieli dodatkowego wsparcia w zakresie instalacji i konfiguracji oprogramowania IBM Security Resilient lub jego rozszerzeń (jeśli ma zastosowanie);
- przeprowadzi dalsze szkolenie i udzieli dodatkowego wsparcia analitykom w celu zapewnienia gotowości do używania rozwiązania IBM Security Resilient jako głównego rozwiązania SOAR Klienta;
- udzieli projektantom porad w zakresie konfigurowania i używania własnych scenariuszy działań odzwierciedlających główne wymagania jednostek organizacyjnych Klienta;
- wykona szybkie skanowanie środowiska IBM Security Resilient w celu opracowania zaleceń dotyczących potencjalnych obszarów do udoskonalenia.

2. Specyfikacje techniczne dotyczące przetwarzania i ochrony danych

Dodatek IBM dotyczący Przetwarzania Danych dostępny pod adresem http://ibm.com/dpa (dalej „DPD”) oraz Specyfikacja Techniczna dotycząca Przetwarzania i Ochrony Danych (dalej „Specyfikacja Techniczna” lub „Załącznik Szczegółowy do DPD”) dostępna za pośrednictwem zamieszczonych poniżej odsyłaczy zawierają dodatkowe informacje na temat ochrony danych dla Usług Przetwarzania w Chmurze oraz ich opcji. Informacje te precyzują, jakie rodzaje Zawartości mogą być przetwarzane przez daną Usługę, jakie czynności przetwarzania są realizowane, jakie są opcje ochrony danych, a także jakie są szczegółowe zasady przechowywania i zwrotu Zawartości. Jeśli do Zawartości stosuje się i) ogólne rozporządzenie o ochronie danych (RODO – UE/2016/679) lub ii) inne regulacje dotyczące ochrony danych osobowych określone pod adresem http://www.ibm.com/dpa/dpl, to w zakresie, w jakim przepisy te mają zastosowanie do danych osobowych uwzględnionych w Zawartości, obowiązuje DPD.

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

3. Poziomy Usług i wsparcie techniczne

3.1 Umowa dotycząca Poziomu Usług

IBM udostępnia Klientowi przedstawioną poniżej Umowę dotyczącą Poziomu Usług („SLA”). IBM naliczy najwyższe obowiązujące wyrównanie na podstawie łącznej dostępności Usługi Przetwarzania w Chmurze, zgodnie z poniższą tabelą. Dostępność wyrażona procentowo jest równa ilorazowi łącznej liczby minut w danym miesiącu obowiązywania umowy, pomniejszonej o łączną liczbę minut Wyłączenia Usługi w tym miesiącu, oraz łącznej liczby minut w tym miesiącu. Definicja Wyłączenia Usługi, opis procesu zgłaszania reklamacji oraz opis sposobu kontaktowania się z IBM w sprawach związanych z dostępnością usług znajdują się w podręczniku wsparcia dla Usługi Przetwarzania w Chmurze IBM pod adresem https://www.ibm.com/software/support/saas_support_overview.html.

Dostępność	Uznanie (% miesięcznej opłaty za subskrypcję*)
Poniżej 99,9%	2%
Poniżej 99,0%	5%
Poniżej 95,0%	10%

* Opłata za subskrypcję oznacza cenę w miesiącu obowiązywania umowy, którego dotyczy reklamacja.

3.2 Wsparcie techniczne

Informacje o wsparciu technicznym dla Usługi Przetwarzania w Chmurze, w tym dane kontaktowe, poziomy istotności, godziny świadczenia usług, czasy reakcji oraz inne informacje i procesy, można znaleźć w podręczniku wsparcia IBM, dostępnym pod adresem https://www.ibm.com/support/home/pages/support-guide/ (należy wybrać odpowiednią Usługę Przetwarzania w Chmurze).

4. Opłaty

4.1 Opłaty rozliczeniowe

Opłaty rozliczeniowe za Usługę Przetwarzania w Chmurze są określone w Dokumencie Transakcyjnym.

Przy sprzedaży niniejszej Usługi Przetwarzania w Chmurze wysokość opłat rozliczeniowych jest ustalana na podstawie jednej z następujących miar:

- Autoryzowany Użytkownik to unikalny użytkownik, który ma prawo dostępu do Usługi Przetwarzania w Chmurze w jakikolwiek sposób, bezpośrednio lub pośrednio (na przykład przez program multipleksujący, urządzenie lub serwer aplikacji), przy użyciu dowolnych środków.
- Jednocześnie Pracujący Użytkownik to każdy z użytkowników, którzy w dowolnym określonym momencie uzyskują równoczesny dostęp do Usługi Przetwarzania w Chmurze w jakikolwiek sposób, bezpośrednio lub pośrednio (na przykład przez program multipleksujący, urządzenie lub serwer aplikacji). Osoba, która uzyskuje równoczesny dostęp do Usługi Przetwarzania w Chmurze wielokrotnie, jest traktowana jako pojedynczy Jednocześnie Pracujący Użytkownik.
- Przedsięwzięcie to usługa specjalistyczna lub szkoleniowa związana z Usługami Przetwarzania w Chmurze.
- Element oznacza wystąpienie określonego elementu, który jest przetwarzany lub zarządzany przez Usługę Przetwarzania w Chmurze bądź związany z jej używaniem. Na potrzeby niniejszej Usługi Przetwarzania w Chmurze Element oznacza Działanie. Działanie to żądanie orkiestracji lub automatyzacji wysłane przez Usługę Przetwarzania w Chmurze do innego oprogramowania.

5. Warunki dodatkowe

Dla Umów o Usługi Przetwarzania w Chmurze (lub podstawowych umów o usługi przetwarzania w chmurze będących ich odpowiednikami) zawartych przed 1 stycznia 2019 r. mają zastosowanie warunki zamieszczone pod adresem https://www.ibm.com/acs.

5.1 Weryfikacja

Klient będzie i) prowadzić i na żądanie dostarczać rekordy i dane wyjściowe narzędzi systemowych w zakresie niezbędnym dla IBM i jego niezależnych rewidentów w celu zweryfikowania, czy Klient przestrzega Umowy, oraz ii) niezwłocznie zamawiać i opłacać wszelkie niezbędne uprawnienia według cen obowiązujących w danym czasie, a także uiszczać inne opłaty oraz spełniać inne zobowiązania stwierdzone w wyniku takiej weryfikacji, zgodnie z fakturą wystawioną przez IBM. Takie zobowiązania w zakresie weryfikacji zgodności pozostają w mocy przez cały okres świadczenia Usługi Przetwarzania w Chmurze i przez dwa lata po jego zakończeniu.

5.2 Wymóg nabycia uprawnienia do programu dodatkowego

Klient musi nabyć tyle samo uprawnień tego samego typu dla podstawowej i dodatkowej Usługi Przetwarzania w Chmurze.

5.3 Ograniczenia dotyczące używania

Każdy Klient jest uprawniony do maksymalnie 100 000 (stu tysięcy) zapytań dotyczących Usługi Analizy Zagrożeń w miesiącu. Klient tworzy zapytanie w Usłudze Analizy Zagrożeń poprzez dodanie artefaktu do incydentu po aktywowaniu tej usługi. Następnie w okresie, w którym incydent pozostanie otwarty i aktywny, co 2 (dwa) dni będzie automatycznie generowane nowe zapytanie w Usłudze Analizy Zagrożeń.

Każdy Klient jest uprawniony do maksymalnie 100 (stu) powiadomień e-mail dziennie na każdego Autoryzowanego / Jednocześnie Pracującego Użytkownika. Powiadomienia e-mail są generowane przez platformę Resilient na podstawie konfiguracji kontrolowanej przez Klienta.

5.4 Dodatkowe informacje dotyczące przetwarzania i ochrony danych

Dla uniknięcia wątpliwości zaznacza się, że usługa IBM Resilient SOAR Platform on Cloud podlega następującym ograniczeniom:

- usługa nie szyfruje Zawartości w stanie spoczynku;
- usługa nie została zaprojektowana z myślą o przetwarzaniu jakichkolwiek szczególnych kategorii Danych Osobowych;
- w ramach usługi nie należy wprowadzać danych osobowych do pól pełnotekstowych, jeśli dane takie nie są wymagane.

Szczegółowe informacje dotyczące szyfrowania i rodzaju przetwarzanych Danych Osobowych można znaleźć pod adresem URL wskazanym dla Specyfikacji Technicznej przywoływanej w paragrafie 2.

6. Warunki unieważniające

6.1 Wykorzystanie danych

IBM nie będzie wykorzystywać ani ujawniać rezultatów używania Usługi Przetwarzania w Chmurze przez Klienta, które występują wyłącznie w Zawartości (Rezultatach) Klienta lub w inny sposób umożliwiają jego identyfikację. IBM będzie jednak wykorzystywać Zawartość oraz inne oparte na niej informacje (z wyjątkiem Rezultatów) w ramach Usługi Przetwarzania w Chmurze w celu jej usprawnienia. IBM może również udostępniać identyfikatory zagrożeń i inne informacje dotyczące bezpieczeństwa osadzone w Zawartości na potrzeby wykrywania zagrożeń i ochrony przed nimi.