IBM Trusteer Pinpoint Detect

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

1. Usługa Przetwarzania w Chmurze

IBM Trusteer Pinpoint to usługa przetwarzania w chmurze zaprojektowana z myślą o zapewnieniu kolejnej warstwy ochrony. Celem tej usługi jest wykrywanie szkodliwego oprogramowania, przypadków wyłudzania informacji i ataków polegających na przejęciu kontroli nad urządzeniem oraz ograniczanie skutków takich działań. Usługę Trusteer Pinpoint można zintegrować z Biznesowymi i/lub Indywidualnymi Aplikacjami Klienta, w odniesieniu do których Klient dokonał subskrypcji ochrony i procesów zapobiegania oszustwom dostępnych w ramach Usług Przetwarzania w Chmurze.

W skład niniejszej Usługi Przetwarzania w Chmurze wchodzą następujące komponenty:

a. Trusteer Management Application (TMA) i Trustboard

   TMA to tradycyjna aplikacja do zarządzania Trusteer, umożliwiająca Klientom ocenę i klasyfikację alertów. Trustboard jest nowszą aplikacją do zarządzania, używaną przede wszystkim do celów badawczych. Klienci mogą w dowolnym momencie zdecydować się na korzystanie z aplikacji TMA lub Trustboard. Aplikacje TMA i Trustboard są udostępnianie w środowisku IBM Trusteer utrzymywanym w chmurze, za pośrednictwem którego Klient (oraz nieograniczona liczba upoważnionych członków jego personelu) może: (i) wyświetlać i pobierać niektóre raporty z danymi o zdarzeniach i oceny ryzyka oraz (ii) wyświetlać, subskrybować i konfigurować dostarczanie generowanych w ramach usługi Pinpoint kanałów informacyjnych na temat zagrożeń. Usługi IBM Trusteer Pinpoint Detect i IBM Trusteer Pinpoint Verify są używane w ramach logowania do usług TMA i Trustboard.

b. Skrypt WWW i/lub interfejsy API

   Narzędzia do zainstalowania w serwisie WWW w celu uzyskania dostępu do Usługi Przetwarzania w Chmurze, jej testowania lub używania.

„Sesja” to interakcja między Aplikacją Klienta (WWW lub mobilną) a Usługą Przetwarzania w Chmurze, generująca co najmniej jedną analizę ryzyka w czasie rzeczywistym. Sesję mierzy się od momentu rozpoczęcia do momentu zakończenia interakcji. Za koniec interakcji uważane jest jedno z następujących zdarzeń:

- zresetowanie interakcji w zwykłym trybie wylogowania z aplikacji;
- zamknięcie przeglądarki, aplikacji lub karty;
- usunięcie informacji cookie;
- przekroczenie limitu czasu.

Sesja może obejmować dowolną liczbę czynności, takich jak logowanie, przeglądanie, obsługa kasowa, konfiguracja płatności i inne działania zdefiniowane w Aplikacji Klienta. Dla uniknięcia wątpliwości wyjaśnia się, że na potrzeby niniejszej Usługi Przetwarzania w Chmurze jedno Połączenie (zdefiniowane poniżej) odpowiada jednej Sesji.

1.1 Produkty oferowane

Klient może dokonać wyboru spośród następujących produktów oferowanych.

1.1.1 IBM Trusteer Pinpoint Detect Standard for Retail i/lub IBM Trusteer Pinpoint Detect Standard for Business

Ta Usługa Przetwarzania w Chmurze łączy usługi IBM Trusteer Pinpoint Criminal Detection oraz IBM Trusteer Pinpoint Malware Detection w ramach jednego skonsolidowanego rozwiązania.

Rozwiązanie to umożliwia wykrywanie szkodliwego oprogramowania i/lub podejrzanych działań związanych z przejmowaniem kont w przeglądarkach, które łączą się z Aplikacją Biznesową lub Aplikacją Indywidualną. Wykrywanie odbywa się bez użycia oprogramowania klienckiego, z wykorzystaniem mechanizmów pozwalających wykryć identyfikator urządzenia oraz przypadki wyłudzania informacji i kradzieży danych uwierzytelniających przez szkodliwe oprogramowanie. Usługi IBM Trusteer Pinpoint

zapewniają kolejną warstwę ochrony. Ich celem jest wykrywanie prób przejęcia konta oraz dostarczanie bezpośrednio Klientowi (za pośrednictwem rodzimej przeglądarki lub aplikacji Klienta dla urządzeń mobilnych) wyników analizy ryzyka w odniesieniu do przeglądarek i urządzeń mobilnych uzyskujących dostęp do Aplikacji Biznesowej lub Aplikacji Indywidualnej. Usług tych można używać również do uzyskiwania zdalnego dostępu przez personel w celu oceny ryzyka generowanego przez zarządzane i niezarządzane urządzenia.

W ramach tej Usługi Przetwarzania w Chmurze jest świadczone wsparcie Premium (zgodnie z definicją podaną poniżej w paragrafie Wsparcie techniczne).

Usługa jest sprzedawana w pakietach po 100 Uprawnionych Uczestników lub 100 Połączeń.

1.1.2 IBM Trusteer Pinpoint Detect Premium for Retail i/lub IBM Trusteer Pinpoint Detect Premium for Business

Ta Usługa Przetwarzania w Chmurze łączy usługi IBM Trusteer Pinpoint Criminal Detection oraz IBM Trusteer Pinpoint Malware Detection w ramach jednego skonsolidowanego rozwiązania.

Rozwiązanie to umożliwia wykrywanie szkodliwego oprogramowania i/lub podejrzanych działań związanych z przejmowaniem kont w przeglądarkach, które łączą się z Aplikacją Biznesową lub Aplikacją Indywidualną. Wykrywanie odbywa się bez użycia oprogramowania klienckiego, z wykorzystaniem mechanizmów pozwalających wykryć identyfikator urządzenia oraz przypadki wyłudzania informacji i kradzieży danych uwierzytelniających przez szkodliwe oprogramowanie. Usługi IBM Trusteer Pinpoint zapewniają kolejną warstwę ochrony. Ich celem jest wykrywanie prób przejęcia konta oraz dostarczanie bezpośrednio Klientowi (za pośrednictwem rodzimej przeglądarki lub aplikacji Klienta dla urządzeń mobilnych) wyników analizy ryzyka dotyczącej przeglądarek i urządzeń mobilnych uzyskujących dostęp do Aplikacji Biznesowej lub Aplikacji Indywidualnej.

Oferta obejmuje rozwiązanie o rozszerzonym zakresie funkcji i usług, takich jak rozszerzone usługi wdrażania i konfigurowania, dostosowane strategie bezpieczeństwa, usługi badania incydentów itp. Klient uzyskuje dostęp do usług wdrażania z wykorzystaniem współużytkowanych zasobów dla każdej aplikacji w wymiarze 200 godzin oraz usług analizy bezpieczeństwa, również z wykorzystaniem współużytkowanych zasobów, w maksymalnym wymiarze 200 godzin dla każdej aplikacji po jej skonfigurowaniu. Usługi bieżące obejmują 20 godzin wdrażania i serwisowania dla każdej aplikacji rocznie oraz 100 godzin badań w dziedzinie bezpieczeństwa dla każdej aplikacji rocznie. Każda dodatkowa czynność będzie podlegać opłacie.

Usługa Pinpoint Detect może wykorzystywać transakcje zarówno z kanałów mobilnych, jak i kanałów WWW. W przypadku transakcji mobilnych stosowana jest usługa Pinpoint nabywana według Połączeń. Niniejsza Usługa Przetwarzania w Chmurze obejmuje ochronę jednej Aplikacji. W odniesieniu do każdej kolejnej Aplikacji Klient powinien uzyskać uprawnienia objęte opcją IBM Trusteer Pinpoint Detect Premium Additional Applications.

Ta Usługa Przetwarzania w Chmurze obejmuje wsparcie na poziomie Premium.

Usługi IBM Trusteer Pinpoint Detect Premium for Retail oraz Business są sprzedawane w pakietach po 100 Uprawnionych Uczestników. Usługa IBM Trusteer Pinpoint Detect Premium jest sprzedawana w pakietach po 100 Połączeń. Jeśli Klient wybierze opcję zakupu według Połączeń, to opłata za Dodatkową Aplikację będzie naliczana począwszy od pierwszej aplikacji.

Pinpoint Detect Policy Manager

Funkcja Policy Manager wchodzi w skład usługi Pinpoint Detect Premium i jest udostępniana w środowisku IBM Trusteer utrzymywanym w chmurze, za pośrednictwem którego Klient (oraz nieograniczona liczba upoważnionych członków personelu) może: (i) projektować, testować i wdrażać w środowisku produkcyjnym logikę wykrywania oszustw; (ii) projektować raporty i panele kontrolne oraz (iii) wyświetlać, konfigurować i ustalać strategie bezpieczeństwa oraz strategie związane z wykrywaniem budzącej podejrzenia aktywności w Aplikacji klienta.

W celu aktywacji funkcji Policy Manager i zaawansowanego wsparcia obowiązkowego niezbędne są usługi konsultacji. Szczegółowe informacje o usługach konsultacji zostaną podane w osobnym zakresie prac.

W przypadku aktywacji funkcji Policy Manager IBM zastrzega sobie prawo do uzyskiwania dostępu do środowiska Klienta w celu świadczenia wsparcia w zakresie dostosowywania strategii Klienta w taki sposób, aby usunąć poważne problemy wynikające ze zmian takich strategii.

Klient zobowiązuje się zapewnić ochronę wszelkich danych udostępnianych za pośrednictwem funkcji Policy Manager przed niewłaściwym użytkowaniem.

Jeśli zostanie aktywowana funkcja Policy Manager, Klient musi wykonywać instrukcje IBM dotyczące konfiguracji reguł zgodnie z opisem podanym w dokumentacji. Klient potwierdza, że IBM nie ponosi odpowiedzialności za sytuacje spowodowane nieprzestrzeganiem tych zaleceń przez Klienta.

Wszelkie problemy polegające na pogorszeniu stabilności lub dostępności usługi, które wynikają z błędnej konfiguracji funkcji Policy Manager przez Klienta, są wyłączone z czasu Przestoju wykorzystywanego w obliczeniach na potrzeby umowy dotyczącej poziomu usług.

1.1.3 IBM Trusteer Pinpoint Detect for Connections

Celem tej Usługi Przetwarzania w Chmurze zapewniającej ochronę jest wykrywanie prób przejęcia konta oraz dostarczanie (za pośrednictwem rodzimej przeglądarki lub aplikacji Klienta dla urządzeń mobilnych) wyników analizy ryzyka/zaufania dotyczącej przeglądarek i urządzeń mobilnych uzyskujących dostęp do Aplikacji Biznesowej lub Aplikacji Indywidualnej. Rozwiązanie to analizuje urządzenie, połączenia i zachowanie użytkownika końcowego na podstawie różnych wskaźników ryzyka oraz porównuje wyniki tej analizy z historią użytkownika, co pozwala na wykrycie podejrzanych sposobów używania urządzenia.

Usługa Przetwarzania w Chmurze może wykorzystywać połączenia zarówno z kanałów mobilnych, jak i kanałów WWW. W ramach usługi IBM Trusteer Pinpoint Detect Użytkownikowi przysługuje uprawnienie do pakietu IBM Trusteer Mobile SDK, o ile ma to zastosowanie.

Usługa Przetwarzania w Chmurze jest sprzedawana w pakietach po 100 Połączeń rocznie.

1.1.4 IBM Trusteer Pinpoint Detect Bundle

Ta Usługa Przetwarzania w Chmurze jest oparta na rozwiązaniach IBM Trusteer Pinpoint Detect, IBM Trusteer Mobile SDK i IBM Trusteer Rapport. Celem tej Usługi Przetwarzania w Chmurze zapewniającej ochronę jest wykrywanie prób przejęcia konta oraz dostarczanie (za pośrednictwem rodzimej przeglądarki lub aplikacji Klienta dla urządzeń mobilnych) wyników analizy ryzyka/zaufania dotyczącej przeglądarek i urządzeń mobilnych uzyskujących dostęp do Aplikacji Biznesowej lub Aplikacji Indywidualnej. Rozwiązanie to analizuje urządzenie, połączenia i zachowanie użytkownika końcowego na podstawie różnych wskaźników ryzyka oraz porównuje wyniki tej analizy z historią użytkownika, co pozwala na wykrycie podejrzanych sposobów używania urządzenia.

Usługę tę można nabyć według liczby Aktywnych Użytkowników.

Usługa Przetwarzania w Chmurze może wykorzystywać połączenia zarówno z kanałów mobilnych, jak i kanałów WWW. Usługa IBM Trusteer Pinpoint Detect obejmuje dostęp do pakietu IBM Trusteer Mobile SDK.

Usługa IBM Trusteer Pinpoint Detect Bundle obejmuje dostęp do usługi IBM Trusteer Rapport. O ile IBM nie określi inaczej na piśmie, dostęp ten nie obejmuje Ekranu Powitalnego Trusteer i usługi IBM Trusteer Rapport Mandatory Service.

IBM Trusteer Mobile SDK

Usługi Przetwarzania w Chmurze IBM Trusteer Mobile SDK zostały zaprojektowane z myślą o wprowadzeniu kolejnej warstwy ochrony, tak aby zapewnić bezpieczny dostęp w sieci WWW do Aplikacji Biznesowych i/lub Indywidualnych Klienta, w odniesieniu do których Klient dokonał subskrypcji Usług Przetwarzania w Chmurze w zakresie ochrony, oceny ryzyka dotyczącego urządzeń mobilnych oraz zabezpieczenia przed wyłudzaniem informacji metodą pharming. Mechanizm wykrywania bezpiecznych sieci Wi-Fi jest dostępny tylko dla platform z systemem operacyjnym Android.

Usługi Przetwarzania w Chmurze IBM Trusteer Mobile SDK zawierają prawnie zastrzeżony pakiet narzędzi do tworzenia oprogramowania dla urządzeń mobilnych („SDK”). Jest to pakiet oprogramowania zawierający dokumentację, prawnie zastrzeżone biblioteki programistyczne oraz inne powiązane pliki i elementy określane nazwą „biblioteka IBM Trusteer dla urządzeń mobilnych”, a także „komponent środowiska wykonawczego” lub „Element Podlegający Redystrybucji”, czyli prawnie zastrzeżony kod wygenerowany przez pakiet IBM Trusteer Mobile SDK, który można osadzać w autonomicznych, chronionych aplikacjach Klienta dla urządzeń mobilnych z systemem operacyjnym iOS lub Android (oraz integrować z takimi aplikacjami), w odniesieniu do których Klient dokonał subskrypcji ochrony dostępnej w ramach Usług Przetwarzania w Chmurze („Zintegrowana przez Klienta Aplikacja dla Urządzeń Mobilnych”).

Klient może:

a. wykorzystywać pakiet IBM Trusteer Mobile SDK do użytku wewnętrznego, wyłącznie na potrzeby opracowywania Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych;

b. osadzić Element Podlegający Redystrybucji (wyłącznie w postaci kodu wynikowego) w Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych, tak aby stanowił on integralną, nieodłączną część tej aplikacji, przy czym każdy fragment Elementu Podlegającego Redystrybucji zmodyfikowany lub wbudowany zgodnie z niniejszą licencją będzie podlegał niniejszemu Opisowi Usług;

c. prowadzić sprzedaż i dystrybucję Elementu Podlegającego Redystrybucji przeznaczonego do pobrania na urządzenia mobilne Uprawnionych Uczestników lub do pobrania przez posiadacza Urządzenia Klienckiego, pod następującymi warunkami:

   - Z wyjątkiem przypadków wyraźnie dozwolonych w niniejszej Umowie, Klient nie ma prawa (1) używać, kopiować, modyfikować ani dystrybuować pakietu SDK; (2) deasemblować, dekompilować ani przeprowadzać translacji pakietu SDK innymi metodami (z wyjątkiem przypadków wyraźnie dozwolonych przez przepisy prawa bez możliwości ich wyłączenia w ramach umowy); (3) udzielać dalszych licencji, wypożyczać lub wydzierżawiać pakietu SDK; (4) usuwać żadnych plików z informacjami o prawach autorskich ani plików informacyjnych zawartych w Elemencie Podlegającym Redystrybucji; (5) używać tej samej nazwy ścieżki, która została użyta w oryginalnych plikach/modułach Elementu Podlegającego Redystrybucji; (6) używać nazw ani znaków towarowych IBM oraz jego licencjodawców i dystrybutorów w powiązaniu ze sprzedażą Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych bez uprzedniej pisemnej zgody IBM lub odpowiedniego licencjodawcy bądź dystrybutora.
   - Element Podlegający Redystrybucji musi pozostać nierozłącznie zintegrowany ze Zintegrowaną przez Klienta Aplikacją dla Urządzeń Mobilnych; ponadto musi mieć wyłącznie postać kodu wynikowego i spełniać wszystkie wytyczne, instrukcje i specyfikacje zawarte w pakiecie SDK i jego dokumentacji. Umowa licencyjna z użytkownikiem końcowym Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych musi zawierać zapis informujący użytkownika końcowego, że Elementu Podlegającego Redystrybucji nie wolno i) używać do jakichkolwiek innych celów niż umożliwienie działania Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych, ii) kopiować (z wyjątkiem tworzenia kopii zapasowej), iii) przeznaczać do dalszej dystrybucji lub przekazywać, iv) deasemblować, dekompilować ani w inny sposób poddawać translacji, o ile nie zezwalają na to przepisy prawa bez możliwości ich wyłączenia w ramach umowy. Umowa licencyjna zawarta przez Klienta musi chronić prawa IBM w stopniu co najmniej równoważnym warunkom niniejszej Umowy.
   - Pakiet SDK może być wdrażany tylko w ramach wewnętrznych testów programistycznych i jednostkowych prowadzonych przez Klienta na urządzeniach mobilnych określonych przez Klienta jako testowe. Klient nie jest upoważniony do używania pakietu SDK w celu przetwarzania lub symulowania obciążeń produkcyjnych ani testowania skalowalności jakiegokolwiek kodu, programu lub systemu. Klient nie jest uprawniony do używania jakiejkolwiek części pakietu SDK do innych celów.

Klient ponosi wyłączną odpowiedzialność za tworzenie i testowanie Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych oraz za świadczenie wsparcia dla niej. Klient odpowiada za świadczenie pełnego zakresu usług pomocy technicznej w odniesieniu do Zintegrowanej przez Klienta Aplikacji dla Urządzeń Mobilnych oraz wszelkich modyfikacji w Elemencie Podlegającym Redystrybucji, wprowadzonych przez Klienta w sposób dozwolony w niniejszym dokumencie.

Klient może zainstalować Elementy Podlegające Redystrybucji oraz pakiet IBM Security Mobile SDK i używać ich wyłącznie po to, aby ułatwić sobie korzystanie z Usług Przetwarzania w Chmurze.

IBM nie gwarantuje, że aplikacje lub dane wyjściowe wytworzone z użyciem narzędzi mobilnych wchodzących w skład pakietu IBM Security Mobile SDK będą zgodne operacyjnie, kompatybilne lub zdolne funkcjonować w połączeniu z konkretnym systemem operacyjnym platformy mobilnej lub konkretnym urządzeniem mobilnym.

Komponenty Źródłowe i Materiały Przykładowe – usługa IBM Trusteer Mobile SDK może zawierać pewne komponenty w formie kodu źródłowego (zwane dalej „Komponentami Źródłowymi”) i inne materiały określane jako Materiały Przykładowe. Klient ma prawo kopiować i modyfikować Komponenty Źródłowe i Materiały Przykładowe wyłącznie do użytku wewnętrznego pod warunkiem, że takie użycie materiałów jest objęte uprawnieniami licencyjnymi określonymi niniejszą Umową, jednak z zastrzeżeniem, że Klient

nie może zmieniać ani usuwać jakichkolwiek informacji i uwag dotyczących praw autorskich zawartych w Komponentach Źródłowych lub Materiałach Przykładowych. IBM udostępnia Komponenty Źródłowe i Materiały Przykładowe bez zobowiązania do wsparcia oraz W STANIE, W JAKIM SIĘ ZNAJDUJĄ („AS IS"). Zastrzeżenie: Komponenty Źródłowe i Materiały Przykładowe są dostarczane wyłącznie jako przykład sposobu wdrażania Produktu Osadzanego w rozwiązaniu CIMA. Komponenty Źródłowe i Materiały Przykładowe mogą być niezgodne ze środowiskiem programistycznym Klienta. Ponadto Klient ponosi wyłączną odpowiedzialność za testowanie i wdrażanie Produktu Osadzanego w rozwiązaniu CIMA.

Dalsze postanowienia umieszczone w niniejszym paragrafie mają zastosowanie, jeśli Usługi Przetwarzania w Chmurze opisane w niniejszym dokumencie są świadczone przez podmiot inny niż International Business Machines Corporation, spółka zarejestrowana w Nowym Jorku (zwana dalej „IBM Corporation"). Prawa do pakietu SDK i Elementu Podlegającego Redystrybucji opisanych niniejszym dokumencie są udzielane przez IBM Corporation. W ramach niniejszej Umowy IBM występuje jako dystrybutor dostarczający pakiet SDK i Element Podlegający Redystrybucji i ponosi odpowiedzialność za egzekwowanie warunków oraz spełnianie wszelkich zobowiązań dotyczących takiego pakietu SDK i Elementu Podlegającego Redystrybucji, a niniejsza Umowa nie daje Klientowi żadnej podstawy roszczeniowej wobec IBM Corporation. Klient zrzeka się wszelkich roszczeń i podstaw roszczeniowych wobec IBM Corporation, a w odniesieniu do wszelkich praw, odszkodowań i zadośćuczynień związanych z pakietem SDK i Elementem Podlegającym Redystrybucji zobowiązuje się kontaktować wyłącznie z IBM.

IBM Trusteer Rapport

Oferta Trusteer Rapport zapewnia warstwę ochrony przed wyłudzaniem informacji i przed szkodliwym oprogramowaniem typu MitB (ang. Man in the Browser). Usługa ta wykorzystuje sieć kilkudziesięciu milionów punktów końcowych rozmieszczonych na wszystkich kontynentach, aby gromadzić dane analityczne o aktywnych atakach skierowanych przeciwko organizacjom z całego świata, a polegających na wyłudzaniu informacji lub posługiwaniu się szkodliwym oprogramowaniem. W usłudze IBM Trusteer Rapport zastosowano algorytmy analizy zachowania, których celem jest blokowanie ataków związanych z wyłudzaniem informacji oraz zapobieganie instalowaniu i działaniu poszczególnych odmian szkodliwego oprogramowania typu MitB.

Niniejsza oferta Usług Przetwarzania w Chmurze obejmuje następujące komponenty:

a. Skrypt WWW

   Skrypt, który umożliwia dostęp do serwisu WWW w celu uzyskania dostępu do Usługi Przetwarzania w Chmurze, jej testowania lub używania.

1.2 Usługi Opcjonalne

W przypadku Usług Przetwarzania w Chmurze wymienionych w tym paragrafie wymaganiem wstępnym jest uzyskanie uprawnienia do usługi IBM Trusteer Pinpoint Detect Premium, IBM Trusteer Pinpoint Detect Standard, IBM Trusteer Pinpoint for Connections lub IBM Trusteer Pinpoint Detect Bundle.

1.2.1 IBM Trusteer Pinpoint Detect Standard Application

Termin „Aplikacja Klienta" oznacza Aplikację WWW i/lub Aplikację Mobilną. Aplikacja WWW udostępnia wszystkie funkcje oferowane Uprawnionym Uczestnikom Klienta na wielu stronach WWW, z ekranu logowania lub identyfikacji. Funkcje te są monitorowane z konsoli usługi Trusteer jako jedna Aplikacja (aplikacja Trusteer Management Application). Aplikacja Mobilna udostępnia wszystkie funkcje oferowane Uprawnionym Uczestnikom Klienta w jednym oprogramowaniu, które można pobrać ze sklepu z aplikacjami („sklepu"), z ekranu logowania lub identyfikacji. Funkcje te są monitorowane z konsoli usługi Trusteer jako jedna Aplikacja (aplikacja Trusteer Management Application).

Integracja usługi IBM Trusteer Pinpoint wymaga uprawnienia do aplikacji IBM Trusteer Pinpoint Application dla każdej Aplikacji.

- Wdrożenie usługi IBM Trusteer Pinpoint Detect Standard wymaga nabycia uprawnień IBM Trusteer Pinpoint Detect Standard Application w odniesieniu do każdej Aplikacji.

1.2.2 IBM Trusteer Pinpoint Detect Premium Application

Termin „Aplikacja Klienta" oznacza Aplikację WWW i/lub Aplikację Mobilną. Aplikacja WWW udostępnia wszystkie funkcje oferowane Uprawnionym Uczestnikom Klienta na wielu stronach WWW, z ekranu logowania lub identyfikacji. Funkcje te są monitorowane z konsoli usługi Trusteer jako jedna Aplikacja (aplikacja Trusteer Management Application). Aplikacja Mobilna udostępnia wszystkie funkcje oferowane

Uprawnionym Uczestnikom Klienta w jednym oprogramowaniu, które można pobrać ze sklepu z aplikacjami („sklepu”), z ekranu logowania lub identyfikacji. Funkcje te są monitorowane z konsoli usługi Trusteer jako jedna Aplikacja (aplikacja Trusteer Management Application).

Oferta obejmuje dostęp do usług wdrażania z wykorzystaniem współużytkowanych zasobów dla każdej aplikacji w wymiarze 200 godzin oraz usług analizy bezpieczeństwa, również z wykorzystaniem współużytkowanych zasobów, w maksymalnym wymiarze 200 godzin dla każdej aplikacji przy jej konfigurowaniu. Usługi bieżące obejmują 20 godzin wdrażania i serwisowania dla każdej aplikacji rocznie oraz 100 godzin badań w dziedzinie bezpieczeństwa dla każdej aplikacji rocznie.

- Wdrożenie usługi IBM Trusteer Pinpoint Premium wymaga nabycia uprawnień IBM Trusteer Pinpoint Detect Premium Application w odniesieniu do każdej Aplikacji.

1.2.3 IBM Trusteer New Account Fraud for Retail i/lub IBM Trusteer New Account Fraud for Business

Usługa ta, dostępna dla subskrybentów usługi Pinpoint, została zaprojektowana z myślą o wykrywaniu nieprawidłowości, oznaczaniu podejrzanych działań oraz wczesnym generowaniu alertów podczas tworzenia nowych kont. Monitoruje ona nowe konta w celu rozpoznawania nowych działań mogących wskazywać na oszustwa, związanych z tworzeniem profili kont osób młodych oraz operacjami na kontach. Usługa generuje wczesne ostrzeżenia wskazujące, że takie nowe konto może być założone na podstawioną osobę lub wykorzystane w celu dokonywania oszustw, i przekazuje te ostrzeżenia za pośrednictwem raportów dotyczących używania usługi, dostępnych w aplikacji TMA.

Usługi IBM Trusteer New Account Fraud for Retail i IBM Trusteer New Account Fraud for Business można nabywać w pakietach po 10 Wywołań API.

1.2.4 IBM Trusteer Digital Content Pack for Retail i/lub IBM Trusteer Digital Content Pack for Business

Usługa IBM Trusteer Digital Content Pack umożliwia analitykom ds. bezpieczeństwa integrowanie nowych modeli przeciwdziałania oszustwom oraz zapewnia pełne wsparcie podczas tworzenia i modyfikowania doraźnych modeli reagowania na coraz bardziej zaawansowane zagrożenia. Obejmuje obszerny zbiór reguł, danych analitycznych i strategii, które można nabyć jako dodatkową i integralną część rozwiązania. Digital Content Pack pozwala na jeszcze ściślejszą integrację między funkcjami zapobiegania oszustwom cyfrowym oferowanymi przez Trusteer a kanałami płatności bezgotówkowych IBM Safer Payments. Dzięki wykorzystaniu wbudowanych reguł i specyficznej logiki biznesowej usługa Digital Content Pack umożliwia bankom i innym instytucjom finansowym rozszerzanie istniejących funkcji wykrywania oszustw i zapobiegania im.

Usługa IBM Trusteer Digital Content Pack for Retail jest dostępna w pakietach po 100 Uprawnionych Uczestników, a usługa IBM Trusteer Digital Content Pack for Business – w pakietach po 10 Uprawnionych Uczestników.

W przypadku integrowania usługi Digital Content Pack z rozwiązaniami Pinpoint Detect oraz IBM Safer Payments, a także w przypadku usług wymagających szczególnej uwagi niezbędne są usługi konsultacji. Usługi konsultacji nabywa się osobno, na podstawie odrębnego zakresu prac.

1.2.5 IBM Trusteer Pinpoint Malware Detection

W przypadku wykrycia szkodliwego oprogramowania w ramach Usług Przetwarzania w Chmurze IBM Trusteer Pinpoint Malware Detection II Klient jest zobowiązany postępować zgodnie z Podręcznikiem sprawdzonych procedur Pinpoint. Z Usług Przetwarzania w Chmurze IBM Trusteer Pinpoint Malware Detection II należy korzystać w taki sposób, aby nie wpływać na zachowanie Uprawnionych Uczestników tuż po wykryciu szkodliwego oprogramowania lub przejęcia konta, gdyż mogłoby to umożliwić innym osobom powiązanie czynności wykonanych przez Klienta z użyciem Usług Przetwarzania w Chmurze IBM Trusteer Pinpoint (dotyczy to np. powiadomień, komunikatów, blokowania urządzeń lub blokowania dostępu do Aplikacji Biznesowej i/lub Aplikacji Indywidualnej tuż po wykryciu szkodliwego oprogramowania lub przejęcia konta).

1.2.6 Oferty IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business i/lub IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail i/lub IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business i/lub IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail

Oparta na ofercie IBM Trusteer Pinpoint Malware Detection nowa oferta IBM Security Pinpoint Malware Detection II ułatwia standaryzowanie opłat związanych z ochroną wielu Aplikacji i zastępuje opłaty jednorazowe przy dodawaniu Aplikacji.

Wykrywanie przeglądarek łączących się z Aplikacją Biznesową i/lub Indywidualną, które są zawirusowane szkodliwym oprogramowaniem typu MitB ukierunkowanym na transakcje finansowe (mechanizm ten działa bez oprogramowania klienckiego). Usługi Przetwarzania w Chmurze IBM Trusteer Pinpoint Malware Detection zapewniają dodatkową warstwę ochrony, a ich celem jest wyposażenie organizacji w narzędzia, które pozwalają koncentrować się na procesach zapobiegania oszustwom opartym na szkodliwym oprogramowaniu. Jest to możliwe dzięki dostarczaniu Klientowi ocen i alertów dotyczących obecności szkodliwego oprogramowania typu MitB ukierunkowanego na transakcje finansowe.

a. Dane o zdarzeniach

   Klient (oraz nieograniczona liczba upoważnionych członków jego personelu) może korzystać z aplikacji TMA, aby otrzymywać dane o zdarzeniach wygenerowane w wyniku elektronicznych interakcji Uprawnionych Uczestników z jedną bądź wieloma Aplikacjami Biznesowymi i/lub Indywidualnymi Klienta.

b. Wydanie Advanced Edition

   Wydania Advanced Edition for Business i/lub Advanced Edition for Retail oferują dodatkową warstwę ochrony i wykrywania dostosowaną i skorygowaną pod kątem struktury Aplikacji Biznesowych i/lub Indywidualnych Klienta oraz przepływów między nimi. Ponadto wydania te można dostosowywać do konkretnych schematów zagrożeń, jakim podlega Klient, oraz wbudowywać w różne obszary Aplikacji Biznesowych i/lub Indywidualnych Klienta.

   Wydanie Advanced Edition jest oferowane Klientowi przy minimalnej wielkości zamówienia obejmującej 100 tys. Uprawnionych Uczestników wersji Indywidualnej lub 10 tys. Uprawnionych Uczestników wersji Biznesowej, czyli 1000 pakietów po 100 Uprawnionych Uczestników wersji Indywidualnej lub 1000 pakietów po 10 Uprawnionych Uczestników wersji Biznesowej.

c. Wydanie Standard Edition

   Wydania Standard Edition for Business i/lub Standard Edition for Retail to przeznaczone do szybkiego wdrożenia rozwiązania, które zapewniają podstawową funkcjonalność Usługi Przetwarzania w Chmurze opisanej w niniejszym dokumencie.

Niniejsza Usługa Przetwarzania w Chmurze obejmuje ochronę jednej Aplikacji. W odniesieniu do każdej kolejnej Aplikacji Klient musi uzyskać uprawnienia objęte opcją IBM Trusteer Pinpoint Malware Detection Additional Applications.

1.2.7 Opcjonalne dodatkowe Usługi Przetwarzania w Chmurze dla ofert IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail, IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail, IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business i/lub IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business

- W przypadku Usługi Przetwarzania w Chmurze IBM Trusteer Rapport Remediation for Retail wymaganiem wstępnym jest subskrypcja oferty IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail lub IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail.
- W przypadku Usługi Przetwarzania w Chmurze IBM Trusteer Rapport Remediation for Business wymaganiem wstępnym jest subskrypcja oferty IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business lub IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business.

1.2.8 IBM Trusteer Pinpoint Criminal Detection for Business i/lub IBM Trusteer Pinpoint Criminal Detection for Retail

Usługa ta umożliwia wykrywanie podejrzanych działań związanych z przejmowaniem kont w przeglądarkach, które łączą się z Aplikacją Biznesową lub Aplikacją Indywidualną. Wykrywanie odbywa się bez użycia oprogramowania klienckiego, z wykorzystaniem mechanizmów pozwalających wykryć identyfikator urządzenia oraz przypadki wyłudzania informacji i kradzieży danych uwierzytelniających przez szkodliwe oprogramowanie. Usługi Przetwarzania w Chmurze IBM Trusteer Pinpoint Criminal Detection zapewniają kolejną warstwę ochrony. Ich celem jest wykrywanie prób przejęcia konta oraz dostarczanie bezpośrednio Klientowi (za pośrednictwem rodzimej przeglądarki lub aplikacji mobilnej Klienta) wyników analizy ryzyka dotyczącej przeglądarek i urządzeń mobilnych uzyskujących dostęp do Aplikacji Biznesowej lub Aplikacji Indywidualnej.

a. Dane o zdarzeniach

Klienci mogą w dowolnym momencie zdecydować się na korzystanie z aplikacji TMA lub Trustboard. Klient (oraz nieograniczona liczba upoważnionych członków jego personelu) może korzystać z aplikacji TMA lub Trustboard, aby otrzymywać dane o zdarzeniach wygenerowane w wyniku elektronicznych interakcji Uprawnionych Uczestników z jedną bądź wieloma Aplikacjami Biznesowymi i/lub Indywidualnymi Klienta, w odniesieniu do których Klient dokonał subskrypcji ochrony dostępnej w ramach Usług Przetwarzania w Chmurze. Alternatywnie Klient ma do dyspozycji tryb dostarczania danych o zdarzeniach z wykorzystaniem interfejsu API zaplecza.

1.2.9 IBM Trusteer Pinpoint Criminal Detection II for Business i/lub IBM Trusteer Pinpoint Criminal Detection II for Retail

Oparta na ofercie IBM Trusteer Pinpoint Criminal Detection nowa oferta IBM Security Pinpoint Criminal Detection II ułatwia standaryzowanie opłat związanych z ochroną wielu Aplikacji i zastępuje opłaty jednorazowe przy dodawaniu Aplikacji.

Usługa ta umożliwia wykrywanie podejrzanych działań związanych z przejmowaniem kont w przeglądarkach, które łączą się z Aplikacją Biznesową lub Aplikacją Indywidualną. Wykrywanie odbywa się bez użycia oprogramowania klienckiego, z wykorzystaniem mechanizmów pozwalających wykryć identyfikator urządzenia oraz przypadki wyłudzania informacji i kradzieży danych uwierzytelniających przez szkodliwe oprogramowanie. Usługi Przetwarzania w Chmurze IBM Trusteer Pinpoint Criminal Detection II zapewniają kolejną warstwę ochrony. Ich celem jest wykrywanie prób przejęcia konta oraz dostarczanie bezpośrednio Klientowi (za pośrednictwem rodzimej przeglądarki lub aplikacji mobilnej Klienta) wyników analizy ryzyka dotyczącej przeglądarek i urządzeń mobilnych uzyskujących dostęp do Aplikacji Biznesowej lub Aplikacji Indywidualnej.

a. Dane o zdarzeniach

Klienci mogą w dowolnym momencie zdecydować się na korzystanie z aplikacji TMA lub Trustboard. Klient (oraz nieograniczona liczba upoważnionych członków jego personelu) może korzystać z aplikacji TMA lub Trustboard, aby otrzymywać dane o zdarzeniach wygenerowane w wyniku elektronicznych interakcji Uprawnionych Uczestników z jedną bądź wieloma Aplikacjami Biznesowymi i/lub Indywidualnymi Klienta, w odniesieniu do których Klient dokonał subskrypcji ochrony dostępnej w ramach Usług Przetwarzania w Chmurze. Alternatywnie Klient ma do dyspozycji tryb dostarczania danych o zdarzeniach z wykorzystaniem interfejsu API zaplecza.

Niniejsza Usługa Przetwarzania w Chmurze obejmuje ochronę jednej Aplikacji. W odniesieniu do każdej kolejnej Aplikacji Klient powinien uzyskać uprawnienia objęte opcją IBM Trusteer Pinpoint Criminal Detection Additional Applications.

1.2.10 Oferty IBM Trusteer Rapport Remediation for Retail i/lub IBM Trusteer Rapport Remediation for Business

Celem usług IBM Trusteer Rapport Remediation for Retail i IBM Trusteer Rapport Remediation for Business jest zbadanie, zneutralizowanie, zablokowanie i usunięcie szkodliwego oprogramowania typu MitB z zawirusowanych urządzeń (komputerów PC/MAC) Uprawnionych Uczestników w firmie Klienta, którzy doraźnie uzyskują dostęp do Aplikacji Klienta. Wykryte przypadki zawirusowania szkodliwym oprogramowaniem typu MitB są uwzględniane w danych o zdarzeniach dostarczanych przez usługę IBM Trusteer Pinpoint Malware Detection. Klient musi posiadać aktualną subskrypcję usługi IBM Trusteer Pinpoint Malware Detection II faktycznie uruchomionej w ramach Aplikacji Klienta. Klient może korzystać z niniejszej Usługi Przetwarzania w Chmurze wyłącznie w powiązaniu z Uprawnionymi Uczestnikami uzyskującymi dostęp do Aplikacji Klienta. Ponadto niniejsza Usługa Przetwarzania w Chmurze może być używana tylko jako narzędzie, którego celem jest doraźne zbadanie i naprawienie konkretnego zawirusowanego urządzenia (komputera PC/MAC). Usługa IBM Trusteer Rapport Remediation musi działać na urządzeniu Uprawnionego Uczestnika (komputerze PC/MAC), którego dotyczy zagrożenie. Ponadto Uprawniony Uczestnik, którego dotyczy zagrożenie, musi zaakceptować warunki Umowy Licencyjnej z Użytkownikiem Końcowym i przynajmniej raz uwierzytelnić się w jednej lub wielu Aplikacjach Klienta, przy czym stosowana przez Klienta konfiguracja musi obejmować gromadzenie ID użytkowników. W celu uniknięcia wątpliwości zaznacza się, że niniejsza oferta Usług Przetwarzania w Chmurze nie obejmuje prawa do używania Ekranu Powitalnego Trusteer i/lub do promowania Oprogramowania Klienckiego Posiadacza Konta jakimikolwiek innymi metodami w całej grupie Uprawnionych Uczestników z firmy Klienta. Na potrzeby niniejszego Opisu Usługi Posiadacz Konta to użytkownik końcowy z firmy Klienta, który zainstalował klienckie oprogramowanie pomocnicze, zaakceptował Umowę Licencyjną z Użytkownikiem Końcowym oraz co najmniej raz uwierzytelnił się w

posiadanej przez Klienta Aplikacji Indywidualnej lub Biznesowej, w odniesieniu do której Klient dokonał subskrypcji ochrony dostępnej w ramach Usługi Przetwarzania w Chmurze. Oprogramowanie Klienckie Posiadacza Konta to klienckie oprogramowanie pomocnicze IBM Trusteer Rapport lub dowolne inne klienckie oprogramowanie pomocnicze dostarczane w ramach subskrypcji niektórych Usług Przetwarzania w Chmurze i przeznaczone do zainstalowania na urządzeniu użytkownika końcowego.

1.2.11 Oferty IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail i/lub IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

- Aby wdrożyć ofertę IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail lub IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail w odniesieniu do dowolnej dodatkowej Aplikacji Indywidualnej oprócz pierwszej Aplikacji, należy nabyć uprawnienia do oferty IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail.
- Aby wdrożyć ofertę IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business lub IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business w odniesieniu do dowolnej dodatkowej Aplikacji Biznesowej oprócz pierwszej Aplikacji, należy nabyć uprawnienia do oferty IBM Trusteer Pinpoint Malware Detection Additional Applications for Business.

1.2.12 Oferty IBM Trusteer Rapport for Mitigation for Retail i/lub IBM Trusteer Rapport for Mitigation for Business

- Usługa IBM Trusteer Rapport for Mitigation for Retail służy do badania, neutralizowania, blokowania i usuwania szkodliwego oprogramowania z zainfekowanych urządzeń (komputerów PC/MAC) Uprawnionych Uczestników w firmie Klienta, którzy uzyskują doraźnie dostęp do Aplikacji Indywidualnej Klienta. Dotyczy to przypadków zainfekowania szkodliwym oprogramowaniem wykrywanych na podstawie danych o zdarzeniach dostarczanych przez usługę IBM Trusteer Pinpoint Detect Premium lub IBM Trusteer Pinpoint Detect Standard. Klient musi posiadać bieżącą subskrypcję usługi IBM Trusteer Pinpoint Detect Premium lub IBM Trusteer Pinpoint Detect Standard, działającą w danym momencie w ramach Aplikacji Indywidualnej Klienta. Klient może korzystać z niniejszej Usługi Przetwarzania w Chmurze wyłącznie w powiązaniu z Uprawnionymi Uczestnikami uzyskującymi dostęp do Aplikacji Indywidualnej Klienta. Ponadto niniejsza Usługa Przetwarzania w Chmurze może być używana tylko jako narzędzie, którego celem jest doraźne zbadanie i naprawienie konkretnego zawirusowanego urządzenia (komputera PC/MAC). Usługa IBM Trusteer Rapport for Mitigation for Retail musi być faktycznie uruchomiona na urządzeniu Uprawnionego Uczestnika (komputerze PC/MAC), którego dotyczy zagrożenie. Ponadto Uprawniony Uczestnik, którego dotyczy zagrożenie, musi zaakceptować warunki Umowy Licencyjnej z Użytkownikiem Końcowym i przynajmniej raz uwierzytelnić się w jednej lub kilku Aplikacjach Indywidualnych Klienta, a stosowana przez Klienta konfiguracja musi obejmować gromadzenie identyfikatorów użytkowników. W celu uniknięcia wątpliwości zaznacza się, że niniejsza Usługa Przetwarzania w Chmurze nie obejmuje prawa do używania Ekranu Powitalnego Trusteer i/lub do promowania Oprogramowania Klienckiego Posiadacza Konta jakimikolwiek innymi metodami w całej grupie Uprawnionych Uczestników z firmy Klienta.
- Usługa IBM Trusteer Rapport for Mitigation for Business służy do badania, neutralizowania, blokowania i usuwania szkodliwego oprogramowania z zainfekowanych urządzeń (komputerów PC/MAC) Uprawnionych Uczestników w firmie Klienta, którzy uzyskują doraźnie dostęp do Aplikacji Biznesowej Klienta. Dotyczy to przypadków zainfekowania szkodliwym oprogramowaniem wykrywanych na podstawie danych o zdarzeniach dostarczanych przez usługę IBM Trusteer Pinpoint Detect Premium lub IBM Trusteer Pinpoint Detect Standard. Klient musi posiadać bieżącą subskrypcję usługi IBM Trusteer Pinpoint Detect Premium lub IBM Trusteer Pinpoint Detect Standard, działającą w danym momencie w ramach Aplikacji Biznesowej Klienta. Klient może korzystać z niniejszej Usługi Przetwarzania w Chmurze wyłącznie w powiązaniu z Uprawnionymi Uczestnikami uzyskującymi dostęp do Aplikacji Biznesowej Klienta. Ponadto niniejsza Usługa Przetwarzania w Chmurze może być używana tylko jako narzędzie, którego celem jest doraźne zbadanie i naprawienie konkretnego zawirusowanego urządzenia (komputera PC/MAC). Usługa IBM Trusteer Rapport for Mitigation for Business musi być faktycznie uruchomiona na urządzeniu Uprawnionego Uczestnika (komputerze PC/MAC), którego dotyczy zagrożenie. Ponadto Uprawniony Uczestnik, którego dotyczy zagrożenie, musi zaakceptować warunki Umowy Licencyjnej z Użytkownikiem Końcowym i przynajmniej raz uwierzytelnić się w jednej lub kilku Aplikacjach Biznesowych Klienta, a stosowana przez Klienta konfiguracja musi obejmować gromadzenie identyfikatorów użytkowników. W celu uniknięcia wątpliwości zaznacza się, że niniejsza Usługa Przetwarzania w Chmurze nie obejmuje prawa do używania Ekranu Powitalnego

Trusteer i/lub do promowania Oprogramowania Klienckiego Posiadacza Konta jakimikolwiek innymi metodami w całej grupie Uprawnionych Uczestników z firmy Klienta.

1.2.13 IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail i/lub IBM Trusteer Pinpoint Detect Standard Additional Applications for Business

- Aby wdrożyć ofertę IBM Trusteer Pinpoint Detect Standard for Retail w odniesieniu do dowolnej dodatkowej Aplikacji Indywidualnej oprócz pierwszej Aplikacji, należy nabyć uprawnienia do oferty IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail.
- Aby wdrożyć ofertę IBM Trusteer Pinpoint Detect Standard for Business w odniesieniu do dowolnej dodatkowej Aplikacji Biznesowej oprócz pierwszej Aplikacji, należy nabyć uprawnienia do oferty IBM Trusteer Pinpoint Detect Standard Additional Applications for Business.

1.2.14 IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail i/lub IBM Trusteer Pinpoint Detect Premium Additional Applications for Business

Oferta obejmuje dostęp do usług wdrażania z wykorzystaniem współużytkowanych zasobów dla każdej aplikacji w wymiarze 200 godzin oraz usług analizy bezpieczeństwa, również z wykorzystaniem współużytkowanych zasobów, w maksymalnym wymiarze 200 godzin dla każdej aplikacji przy jej konfigurowaniu. Usługi bieżące obejmują 20 godzin wdrażania i serwisowania dla każdej aplikacji rocznie oraz 100 godzin badań w dziedzinie bezpieczeństwa dla każdej aplikacji rocznie.

- Aby wdrożyć ofertę IBM Trusteer Pinpoint Premium for Retail w odniesieniu do dowolnej dodatkowej Aplikacji Indywidualnej oprócz pierwszej Aplikacji, należy nabyć uprawnienia do oferty IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail.
- Aby wdrożyć ofertę IBM Trusteer Pinpoint Premium for Business w odniesieniu do dowolnej dodatkowej Aplikacji Biznesowej oprócz pierwszej Aplikacji, należy nabyć uprawnienia do oferty IBM Trusteer Pinpoint Detect Premium Additional Applications for Business.

1.2.15 IBM Trusteer Pinpoint Detect Standard for Retail Premium Support i/lub IBM Trusteer Pinpoint Detect Standard for Business Premium Support

Klienci, którzy nabywają Usługę Przetwarzania w Chmurze Pinpoint Detect Standard, mogą również nabyć usługi wsparcia Premium. Zakres usług wsparcia Premium został określony poniżej w paragrafie 4.

1.2.16 IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect

Aby nabyć subskrypcję na tę Usługę Przetwarzania w Chmurze, Klient musi już posiadać subskrypcję usługi IBM Trusteer Pinpoint Detect.

Ta Usługa Przetwarzania w Chmurze rozszerza usługę IBM Trusteer Pinpoint Detect, udostępniając dodatkowe informacje i kontekst w związku z numerami telefonów komórkowych przekazanymi do jednej z tych Usług Przetwarzania w Chmurze. Ułatwia to ocenę ryzyka oszustwa zachodzącego w danej sesji. Klient może wysyłać do Usługi Przetwarzania w Chmurze zapytania dotyczące charakterystyki danego numeru telefonu komórkowego, na przykład informacji o operatorze powiązanych z tym numerem.

Dane dotyczące numerów telefonów komórkowych udostępnione przez tę Usługę Przetwarzania w Chmurze („Analiza Danych Komórkowych”) mogą być wykorzystywane wyłącznie do celów wewnętrznych Klienta i przechowywane nie dłużej niż 30 (trzydzieści) dni. Po upływie tego okresu Klient musi wysłać do Usługi Przetwarzania w Chmurze ponowne zapytanie o ten sam numer telefonu komórkowego, aby uzyskać Analizę Danych Komórkowych na jego temat; niedozwolone jest ponowne wykorzystywanie Analizy Danych Komórkowych uzyskanych w ramach poprzedniego zapytania. Klient nie jest uprawniony do buforowania Analizy Danych Komórkowych w sposób inny niż określony powyżej, a także do jej ponownego wykorzystywania ani używania w całości lub w części w połączeniu z funkcjami eksploracji danych lub w celu archiwizacji jakiejkolwiek jej części.

1.3 Usługi przyspieszające

1.3.1 Oferty IBM Trusteer Pinpoint Detect Standard Redeployment i/lub IBM Trusteer Pinpoint Detect Premium Redeployment

Klienci, którzy przydzielają Aplikacje bankowości elektronicznej do innych zadań w okresie świadczenia usługi i na skutek tego wymagają wprowadzenia zmian we wdrożonych usługach IBM Trusteer Pinpoint Detect, powinni nabyć usługę IBM Trusteer Pinpoint Detect Redeployment.

Przyczyną przydzielenia do innych zadań może być zmiana domeny Aplikacji lub adresu URL hosta, przekształcanie Aplikacji elektronicznej pod kątem nowej technologii, przejście na nową platformę bankowości elektronicznej lub dodanie nowego strumienia logowania do istniejącej Aplikacji.

W sześciomiesięcznym okresie przejściowym związanym z przydzieleniem do innych zadań Klient jest uprawniony do używania dodatkowych Aplikacji, z których każda przypada na jedną wcześniej zasubskrybowaną Aplikację i działa niezależnie od niej.

1.3.2 IBM Trusteer Pinpoint Malware Detection Redeployment

Klienci, którzy przydzielają Aplikacje bankowości elektronicznej do innych zadań w okresie świadczenia usługi i na skutek tego wymagają wprowadzenia zmian we wdrożonej usłudze IBM Trusteer Pinpoint Malware Detection II, powinni nabyć usługę IBM Trusteer Pinpoint Malware Detection Redeployment.

Przyczyną przydzielenia do innych zadań może być zmiana domeny Aplikacji lub adresu URL hosta, przekształcanie Aplikacji elektronicznej pod kątem nowej technologii, przejście na nową platformę bankowości elektronicznej lub dodanie nowego strumienia logowania do istniejącej Aplikacji.

W sześciomiesięcznym okresie przejściowym związanym z przydzieleniem do innych zadań Klient jest uprawniony do używania dodatkowych Aplikacji, z których każda przypada na jedną wcześniej zasubskrybowaną Aplikację i działa niezależnie od niej.

IBM Trusteer Pinpoint Malware Detection Additional Applications: Wdrożenie usługi IBM Trusteer Pinpoint Malware Detection II Standard Edition lub IBM Trusteer Pinpoint Malware Detection II Advanced Edition w odniesieniu do dowolnej dodatkowej Aplikacji oprócz pierwszej Aplikacji wymaga nabycia uprawnienia do usługi IBM Trusteer Pinpoint Malware Detection Additional Applications.

1.3.3 IBM Trusteer Pinpoint Criminal Detection Redeployment

Klienci, którzy przydzielają Aplikacje bankowości elektronicznej do innych zadań w okresie świadczenia usługi i na skutek tego wymagają wprowadzenia zmian we wdrożonej Usłudze Przetwarzania w Chmurze IBM Trusteer Pinpoint Criminal Detection, powinni nabyć usługę IBM Trusteer Pinpoint Criminal Detection Redeployment.

Przyczyną przydzielenia do innych zadań może być zmiana domeny Aplikacji lub adresu URL hosta, przekształcanie Aplikacji elektronicznej pod kątem nowej technologii, przejście na nową platformę bankowości elektronicznej lub dodanie nowego strumienia logowania do istniejącej Aplikacji.

W sześciomiesięcznym okresie przejściowym związanym z przydzieleniem do innych zadań Klient jest uprawniony do używania dodatkowych Aplikacji, z których każda przypada na jedną wcześniej zasubskrybowaną Aplikację i działa niezależnie od niej.

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://ibm.com/dpa/dpl, to w zakresie, w jakim przepisy te mają zastosowanie do danych osobowych uwzględnionych w Zawartości, obowiązuje DPD.

Dla uniknięcia wątpliwości wyjaśnia się, że w Specyfikacjach Technicznych wymienione są zwykle wszystkie lokalizacje, w których IBM (w tym ewentualni podwykonawcy IBM jako podmiotu przetwarzającego będący osobami trzecimi) udostępnia i przetwarza Dane Osobowe, niezależnie od centrum przetwarzania danych, z którego usługi są wdrażane. Lista lokalizacji udostępniających i przetwarzających Dane Osobowe, powiązanych z centrum przetwarzania danych, z którego usługi są wdrażane, znajduje się w paragrafie 5.2 (Informacje o dodatkowych miejscach przetwarzania).

IBM Trusteer Pinpoint Criminal Detect

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402489853624

IBM Trusteer Pinpoint Detect

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=3D3DA0C0E5F711E5A3808DA17FABE9B1

IBM Trusteer Pinpoint Malware Detection

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402489595035

IBM Trusteer Mobile SDK

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402492847439

IBM Trusteer Rapport

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=1402483908375

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).

Wsparcie Premium:

Subskrypcja Wsparcia Premium jest dostępna dla Usługi Przetwarzania w Chmurze za dodatkową opłatą i zapewnia następujące udogodnienia:

- Wsparcie jest świadczone przez całą dobę we wszystkie dni tygodnia bez względu na poziom istotności.
- Klienci mogą kontaktować się bezpośrednio ze wsparciem drogą telefoniczną lub zamawiając oddzwonienie.
- Klienci i Uprawnieni Uczestnicy mogą wprowadzać zgłoszenia problemów w postaci elektronicznej zgodnie ze szczegółowym opisem w „Podręczniku wsparcia dla usługi IBM Software as a Service (SaaS)".
- Klient może uzyskiwać dostęp do powiadomień, dokumentów, raportów z wdrożeń i często zadawanych pytań w Portalu Obsługi Klienta pod adresem: http://www.ibm.com/software/security/trusteer/support/.

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:

- Przedsięwzięcie to usługa specjalistyczna lub szkoleniowa związana z Usługami Przetwarzania w Chmurze.
- Uprawniony Uczestnik to osoba lub podmiot uprawniony do uczestnictwa w dowolnym programie świadczenia usługi zarządzanym lub monitorowanym za pomocą Usług Przetwarzania w Chmurze.
    - Aktywny Użytkownik to unikalna osoba, która uzyskuje dostęp do Usługi Przetwarzania w Chmurze w jakikolwiek sposób, bezpośrednio lub pośrednio (na przykład przez program multipleksujący, urządzenie lub serwer aplikacji), przy użyciu dowolnych środków.
- W przypadku usługi IBM Trusteer Pinpoint Detect Bundle Aktywnym Użytkownikiem jest unikalna osoba, która uzyskuje dostęp do Usług Przetwarzania w Chmurze w jakikolwiek sposób przynajmniej jednokrotnie w ostatnim 12-miesięcznym okresie (przed jego upływem).
- Aplikacja to jednoznacznie nazwany program utworzony, udostępniony lub używany przez Usługi Przetwarzania w Chmurze.
- Wywołanie API oznacza odwołanie do Usług Przetwarzania w Chmurze za pośrednictwem interfejsu programowania.
- Połączenie to łącze lub powiązanie z bazą danych, aplikacją, serwerem lub innym typem urządzenia, które zostały udostępnione dla Usługi Przetwarzania w Chmurze.

4.2 Opłaty za Usługi Zdalne

Usługa zdalna traci ważność po upływie 90 dni od daty zakupu niezależnie od tego, czy usługa zdalna została wykorzystana.

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 Umowa Licencyjna z Użytkownikiem Końcowym i podstawa przetwarzania danych Podmiotów Danych

Do Usług Przetwarzania w Chmurze IBM Trusteer Rapport (w tym do usługi Rapport Remediation lub Rapport for Mitigation, jeśli została ona wdrożona w powiązaniu z Usługami Przetwarzania w Chmurze Pinpoint) ma zastosowanie następująca reguła: O ile nie uzgodniono inaczej, zgodnie z podstawą przetwarzania, którą Klient określił w sposób niezależny, Klient upoważnia IBM do udostępniania Umowy Licencyjnej z Użytkownikiem Końcowym dostępnej pod adresem https://trusteer.secure.force.com/PKB/articles/en_US/FAQ/RAPPORT-DATA-PRIVACY-NOTICE-AND-END-USER-LICENSE-AGREEMENT-EULA, w celach związanych z gromadzeniem i przetwarzaniem przez IBM informacji niezbędnych do świadczenia Usług Przetwarzania w Chmurze.

Ponadto Użytkownik upoważnia IBM (jako podmiot przetwarzający dane Przedsiębiorstwa Sponsorującego Użytkownika) do używania Programu w celu gromadzenia danych dotyczących szkodliwego oprogramowania oraz artefaktów szkodliwego oprogramowania, tzn. plików związanych ze szkodliwymi działaniami lub nieprawidłowościami w funkcjonowaniu Programu. IBM nie będzie wykorzystywać Programu do pozyskiwania plików, które zawierają dane osobowe Użytkownika. Zgromadzone pliki mogą jednak zawierać dane osobowe, które zostały pobrane przez szkodliwe oprogramowanie bez zgody Użytkownika. IBM: 1) niezwłocznie usunie wszelkie pliki, które nie są potrzebne do celów takiej analizy; 2) zachowa potrzebne pliki tylko na czas takiej analizy, w żadnym przypadku nie dłużej niż przez trzy miesiące.

5.2 Informacje o dodatkowych miejscach przetwarzania

Udostępnianie i przetwarzanie Danych Osobowych, również przez ewentualnych podwykonawców podmiotu przetwarzającego będących osobami trzecimi, którzy zostali wyszczególnieni w Specyfikacji Technicznej, będzie się odbywać w całości w następujących miejscach:

W przypadku wszystkich usług świadczonych za pośrednictwem centrum przetwarzania danych w Niemczech IBM ograniczy udostępnianie i przetwarzanie Danych Osobowych do kraju Podmiotu IBM zawierającego Umowę oraz następujących krajów: Niemcy, Izrael, Irlandia i Holandia.

W przypadku wszystkich usług świadczonych za pośrednictwem centrum przetwarzania danych w Japonii IBM ograniczy udostępnianie i przetwarzanie Danych Osobowych do kraju Podmiotu IBM zawierającego Umowę oraz następujących krajów: Japonia, Izrael i Irlandia.

W przypadku wszystkich usług świadczonych za pośrednictwem centrum przetwarzania danych w Stanach Zjednoczonych IBM ograniczy udostępnianie i przetwarzanie Danych Osobowych do kraju Podmiotu IBM zawierającego Umowę oraz następujących krajów: Stany Zjednoczone, Izrael, Irlandia, Singapur i Australia.

Oprócz powyższych lokalizacji dla wszystkich usług świadczonych przez centra przetwarzania danych w Niemczech, Japonii i Stanach Zjednoczonych (1) dane dotyczące wsparcia mogą być udostępniane lub przetwarzane w Niemczech i Francji przez firmę Salesforce.Com będącą zewnętrznym podwykonawcą IBM jako podmiotu przetwarzającego; (2) w przypadku Klientów, którzy wybrali opcję wysyłania danych do dostawców rozwiązania Mobile Carrier Intelligence, Dane Osobowe mogą być przechowywane i przetwarzane w krajach odpowiednich zewnętrznych podwykonawców podmiotu przetwarzającego, wyszczególnionych w Specyfikacji Technicznej. Bez względu na stanowiące inaczej warunki Specyfikacji Technicznej zewnętrzni podwykonawcy podmiotu przetwarzającego, o których mowa w klauzuli (2) poprzedniego zdania, mogą nie spełniać norm ISO 27001 lub SOC2.

Usługi wsparcia i serwisowania kont IBM Trusteer mogą być również udostępniane w razie potrzeby, w miarę dostępności odpowiedniego personelu IBM, lokalizacji Klienta oraz centrum przetwarzania danych, w którym przechowywane są odpowiednie dane.

5.3 Dane Posiadacza Konta

Dla uniknięcia wątpliwości wyjaśnia się, że jeśli istnieje więcej niż jeden Klient IBM powiązany z Oprogramowaniem Klienckim Posiadacza Konta konkretnego Posiadacza Konta (tacy Klienci IBM będą dalej zwani „Klientami Afiliowanymi"), a IBM świadczy takim Klientom Afiliowanym usługi, które są przedmiotem niniejszego Opisu Usługi, za pośrednictwem centrów przetwarzania danych w różnych regionach, to wówczas dane Posiadacza Konta mogą być przetwarzane w dowolnych lokalizacjach powiązanych z każdym takim centrum przetwarzania danych zgodnie z paragrafem 5.2.

5.4 Zintegrowane rozwiązania

Dla uniknięcia wątpliwości precyzuje się, że różne produkty oferowane w ramach marki Trusteer mogą stanowić zintegrowane rozwiązanie. W związku z tym, jeśli Klient przestanie korzystać z jednej z takich Usług Przetwarzania w Chmurze, IBM może zatrzymać Dane Klienta w celu świadczenia mu pozostałych Usług Przetwarzania w Chmurze zgodnie z niniejszym Opisem Usługi, a także innych usług Trusteer zgodnie z opisami mającymi do nich zastosowanie.

5.5 Oprogramowanie pomocnicze

Usługa Przetwarzania w Chmurze zawiera następujące oprogramowanie pomocnicze:

- IBM Rapport Agents

5.6 Sprawdzone procedury dotyczące rozwiązań Pinpoint

W przypadku wykrycia szkodliwego oprogramowania lub wykrycia przejęcia konta Klient jest zobowiązany postępować zgodnie z „Podręcznikiem sprawdzonych procedur dotyczących rozwiązań Pinpoint". Z Usług Przetwarzania w Chmurze IBM Trusteer Pinpoint Detect należy korzystać w taki sposób, aby nie wpływać w żaden sposób na zachowanie Uprawnionych Uczestników tuż po wykryciu szkodliwego oprogramowania lub przejęcia konta, gdyż mogłoby to umożliwić innym osobom powiązanie czynności wykonanych przez Klienta z użyciem usług IBM Trusteer Pinpoint (dotyczy to np. powiadomień, komunikatów, blokowania urządzeń lub blokowania dostępu do Aplikacji Biznesowej i/lub Aplikacji Indywidualnej tuż po wykryciu szkodliwego oprogramowania lub przejęcia konta).

5.7 Dane gromadzone w związku z wdrażaniem usługi

Wdrożenie Usługi Przetwarzania w Chmurze może wymagać od Klienta przekazania IBM określonych danych. Dane te nie mogą obejmować informacji, które umożliwiają zidentyfikowanie konkretnej osoby fizycznej lub które mogą być powiązane z konkretną osobą fizyczną. Więcej wytycznych dotyczących danych przekazywanych IBM w związku z wdrożeniem usługi znajduje się w „Wytycznych dotyczących wdrażania usługi Trusteer", które zostaną udostępnione Klientowi.

6. Warunki unieważniające

6.1 Wykorzystanie danych

Następujące postanowienie ma znaczenie rozstrzygające w przypadku, gdy którekolwiek z postanowień paragrafu „Ochrona Zawartości i Danych" warunków podstawowych dotyczących Usługi Przetwarzania w Chmurze, które zostały uzgodnione między Stronami, jest z nim sprzeczne: 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.