IBM Trusteer Fraud Protection

Στην παρούσα Περιγραφή Υπηρεσιών περιγράφεται η Υπηρεσία Cloud που παρέχεται από την IBM στον Πελάτη. Με τον όρο "Πελάτης" νοούνται το συμβαλλόμενο μέρος, οι εξουσιοδοτημένοι χρήστες του και οι αποδέκτες της Υπηρεσίας Cloud. Η αντίστοιχη Προσφορά Τιμής (Quotation) και η Απόδειξη Δικαιώματος (Proof of Entitlement - "PoE") παρέχονται ως χωριστά Έγγραφα Συναλλαγών.

1. Υπηρεσία Cloud

Οι ακόλουθες Υπηρεσίες Cloud καλύπτονται από την παρούσα Περιγραφή Υπηρεσιών:

Υπηρεσίες Cloud για το Rapport:

- IBM Trusteer Rapport for Business
- IBM Trusteer Rapport for Business Premium Support
- IBM Trusteer Rapport for Retail
- IBM Trusteer Rapport for Retail Premium Support
- IBM Trusteer Rapport II for Business
- IBM Trusteer Rapport II for Retail
- IBM Trusteer Rapport Fraud Feeds for Business
- IBM Trusteer Rapport Fraud Feeds for Business Premium Support
- IBM Trusteer Rapport Fraud Feeds for Retail
- IBM Trusteer Rapport Fraud Feeds for Retail Premium Support
- IBM Trusteer Rapport Phishing Protection for Business
- IBM Trusteer Rapport Phishing Protection for Business Premium Support
- IBM Trusteer Rapport Phishing Protection for Retail
- IBM Trusteer Rapport Phishing Protection for Retail Premium Support
- IBM Trusteer Rapport Mandatory Service for Business
- IBM Trusteer Rapport Mandatory Service for Retail
- IBM Trusteer Rapport Additional Applications For Retail
- IBM Trusteer Rapport Additional Applications For Business
- IBM Trusteer Rapport Large Redeployment
- IBM Trusteer Rapport Small Redeployment

Υπηρεσίες Cloud για το Pinpoint:

- IBM Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Trusteer Pinpoint Malware Detection for Business Standard Edition Premium Support
- IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition Premium Support
- IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition Premium Support
- IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition Premium Support
- IBM Trusteer Pinpoint Criminal Detection for Business
- IBM Trusteer Pinpoint Criminal Detection for Business Premium Support
- IBM Trusteer Pinpoint Criminal Detection for Retail
- IBM Trusteer Pinpoint Criminal Detection for Retail Premium Support
- IBM Trusteer Pinpoint Carbon Copy for Business

- IBM Trusteer Pinpoint Carbon Copy for Business Premium Support
- IBM Trusteer Pinpoint Carbon Copy for Retail
- IBM Trusteer Pinpoint Carbon Copy for Retail Premium Support
- IBM Trusteer Rapport Remediation for Retail
- IBM Trusteer Rapport Remediation for Retail Premium Support
- IBM Trusteer Pinpoint Criminal Detection II for Business
- IBM Trusteer Pinpoint Criminal Detection II for Retail
- IBM Trusteer Pinpoint Malware Detection II for Business Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Advanced Edition
- IBM Trusteer Rapport Remediation for Business
- IBM Trusteer Rapport Remediation for Business Premium Support
- IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail
- IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Business
- IBM Trusteer Pinpoint Malware Detection Redeployment
- IBM Trusteer Pinpoint Criminal Detection Redeployment
- IBM Trusteer Pinpoint Detect Standard for Business
- IBM Trusteer Pinpoint Detect Premium for Business
- IBM Trusteer Pinpoint Detect Standard Additional Applications for Business
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Business
- IBM Trusteer Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- IBM Trusteer Rapport for Mitigation for Retail
- IBM Trusteer Rapport for Mitigation for Retail Premium Support
- IBM Trusteer Rapport for Mitigation for Business
- IBM Trusteer Rapport for Mitigation for Business Premium Support
- IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Standard with access management integration for Retail
- IBM Trusteer Pinpoint Detect Standard with access management integration for Business
- IBM Trusteer Pinpoint Detect Premium with access management integration for Retail
- IBM Trusteer Pinpoint Detect Premium with access management integration for Business
- IBM Trusteer Pinpoint Detect Standard Redeployment
- IBM Trusteer Pinpoint Detect Premium Redeployment
- IBM Trusteer Pinpoint Detect Standard For Retail Premium Support
- IBM Trusteer Pinpoint Detect Standard For Business Premium Support

Υπηρεσίες Cloud για το Mobile:

- IBM Trusteer Mobile SDK for Business
- IBM Trusteer Mobile SDK for Retail
- IBM Trusteer Mobile Browser for Business
- IBM Trusteer Mobile Browser for Business Premium Support

- IBM Trusteer Mobile Browser for Retail
- IBM Trusteer Mobile Browser for Retail Premium Support

1.1 Υπηρεσίες Cloud για Επιχειρηματική και Λιανική Χρήση

Οι Υπηρεσίες Cloud για το IBM Trusteer παρέχονται για χρήση με συγκεκριμένα είδη Εφαρμογών. Μια Εφαρμογή ορίζεται ως ένα από τα ακόλουθα είδη: Λιανικής ή Επιχειρηματική. Διατίθενται χωριστές προσφορές για Εφαρμογές Λιανικής και για Επιχειρηματικές Εφαρμογές.

α. Μια Εφαρμογή Λιανικής ορίζεται ως μια εφαρμογή online τραπεζικών συναλλαγών, μια εφαρμογή για φορητές συσκευές ή μια εφαρμογή e-commerce που έχει σχεδιαστεί για την εξυπηρέτηση πελατών. Η ισχύουσα πολιτική του Πελάτη μπορεί να κατηγοριοποιεί ορισμένες μικρές επιχειρήσεις ως επιχειρήσεις που δικαιούνται να αποκτούν πρόσβαση μέσω εφαρμογών λιανικής.

β. Μια Επιχειρηματική Εφαρμογή ορίζεται ως μια εφαρμογή online τραπεζικών συναλλαγών, μια εφαρμογή για φορητές συσκευές ή μια εφαρμογή e-commerce που έχει σχεδιαστεί για την εξυπηρέτηση εταιρειών, φορέων ή αντίστοιχων νομικών προσώπων ή ως μια εφαρμογή που δεν κατηγοριοποιείται ως Εφαρμογή Λιανικής.

1.1.1 Υπηρεσίες Cloud για Επιχειρηματική Χρήση

- IBM Trusteer Rapport for Business
- IBM Trusteer Rapport II for Business
- IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Business Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Business Advanced Edition
- IBM Trusteer Pinpoint Malware Detection II for Business Standard Edition
- IBM Trusteer Pinpoint Criminal Detection II for Business
- IBM Trusteer Pinpoint Criminal Detection for Business
- IBM Trusteer Mobile SDK for Business
- IBM Trusteer Mobile Browser for Business
- IBM Trusteer Pinpoint Detect Standard for Business
- IBM Trusteer Pinpoint Detect Premium for Business
- IBM Trusteer Pinpoint Detect Standard with access management integration for Business
- IBM Trusteer Pinpoint Detect Premium with access management integration for Business

1.1.2 Υπηρεσίες Cloud για Λιανική Χρήση

- IBM Trusteer Rapport for Retail
- IBM Trusteer Rapport II for Retail
- IBM Trusteer Pinpoint Criminal Detection for Retail
- IBM Trusteer Pinpoint Criminal Detection II for Retail
- IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition
- IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Advanced Edition
- IBM Trusteer Pinpoint Malware Detection II for Retail Standard Edition
- IBM Trusteer Pinpoint Detect Standard for Retail
- IBM Trusteer Pinpoint Detect Premium for Retail
- IBM Trusteer Pinpoint Detect Standard with access management integration for Retail
- IBM Trusteer Pinpoint Detect Premium with access management integration for Retail
- IBM Trusteer Mobile SDK for Retail
- IBM Trusteer Mobile Browser for Retail

Για κάθε μία από τις Υπηρεσίες Cloud για Επιχειρηματική και Λιανική Χρήση, διατίθεται ένα αντίστοιχο προϊόν Υποστήριξης επιπέδου Premium έναντι πρόσθετης χρέωσης, με την εξαίρεση των Υπηρεσιών Cloud IBM Trusteer Mobile SDK.

1.1.3 Πρόσθετες Υπηρεσίες Cloud για το IBM Trusteer Rapport

α. Πρόσθετες Υπηρεσίες Cloud που διατίθενται για το IBM Trusteer Rapport for Business:

- IBM Trusteer Rapport Fraud Feeds for Business
- IBM Trusteer Rapport Phishing Protection for Business
- IBM Trusteer Rapport Mandatory Service for Business
- IBM Trusteer Rapport Additional Applications For Business

β. Πρόσθετες Υπηρεσίες Cloud που διατίθενται για το IBM Trusteer Rapport for Retail:

- IBM Trusteer Rapport Fraud Feeds for Retail
- IBM Trusteer Rapport Phishing Protection for Retail
- IBM Trusteer Rapport Mandatory Service for Retail
- IBM Trusteer Rapport Additional Applications For Retail

Για κάθε μία από τις πρόσθετες (add-on) Επιχειρηματικές υπηρεσίες και υπηρεσίες Λιανικής για τις Υπηρεσίες Cloud IBM Trusteer Rapport, με την εξαίρεση των πρόσθετων υπηρεσιών IBM Trusteer Rapport Mandatory Service, διατίθεται ένα αντίστοιχο προϊόν Υποστήριξης επιπέδου Premium έναντι πρόσθετης χρέωσης.

Μια συνδρομή για το IBM Trusteer Rapport for Business ή το IBM Trusteer Rapport for Retail αποτελεί απαραίτητη προϋπόθεση για την απόκτηση οποιασδήποτε από τις αντίστοιχες πρόσθετες Υπηρεσίες Cloud που αναφέρονται στο παρόν άρθρο.

1.1.4 Πρόσθετες Υπηρεσίας Cloud για το IBM Trusteer Pinpoint Malware Detection ή/και το IBM Trusteer Pinpoint Malware Detection II

α. Πρόσθετες Υπηρεσίες Cloud που διατίθενται για το IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition ή το IBM Trusteer Pinpoint Malware Detection for Business Standard Edition ή για το IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business ή το IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business:

- IBM Trusteer Pinpoint Carbon Copy for Business
- IBM Trusteer Rapport Remediation for Business
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

β. Πρόσθετες Υπηρεσίες Cloud που διατίθενται για το IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition ή το IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition ή για το IBM Trusteer Pinpoint Malware Detection II for Business Advanced Edition ή το IBM Trusteer Pinpoint Malware Detection II for Business Standard Edition:

- IBM Trusteer Pinpoint Carbon Copy for Retail
- IBM Trusteer Rapport Remediation for Retail
- IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail

Διατίθεται Υποστήριξη επιπέδου Premium για συγκεκριμένες προσφορές, όπως ορίζεται στο παρόν έγγραφο. Μια συνδρομή για το IBM Trusteer Pinpoint Malware Detection for Business ή το IBM Trusteer Pinpoint Malware Detection for Retail ή για το IBM Trusteer Pinpoint Malware Detection II for Business ή το IBM Trusteer Pinpoint Malware Detection II for Retail αποτελεί απαραίτητη προϋπόθεση για την απόκτηση οποιασδήποτε από τις αντίστοιχες πρόσθετες Υπηρεσίες Cloud που αναφέρονται στο παρόν άρθρο.

1.1.5 Πρόσθετες Υπηρεσίες Cloud για το IBM Trusteer Pinpoint Criminal Detection ή/και το IBM Trusteer Pinpoint Criminal Detection II

α. Πρόσθετες Υπηρεσίες Cloud που διατίθενται για το IBM Trusteer Pinpoint Criminal Detection for Business ή το IBM Trusteer Pinpoint Criminal Detection II:

- IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business

β. Πρόσθετες Υπηρεσίες Cloud που διατίθενται για το IBM Trusteer Pinpoint Criminal Detection for Retail ή/και το IBM Trusteer Pinpoint Criminal Detection II for Retail:

- IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail

Διατίθεται Υποστήριξη επιπέδου Premium για συγκεκριμένες προσφορές, όπως ορίζεται στο παρόν έγγραφο.

Μια συνδρομή για το IBM Trusteer Pinpoint Criminal Detection for Business ή το IBM Trusteer Pinpoint Criminal Detection for Retail ή για το IBM Trusteer Pinpoint Criminal Detection II for Business ή το IBM Trusteer Pinpoint Criminal Detection II for Retail αποτελεί απαραίτητη προϋπόθεση για την απόκτηση οποιασδήποτε από τις αντίστοιχες πρόσθετες Υπηρεσίες Cloud που αναφέρονται στο παρόν άρθρο.

1.1.6 Πρόσθετες Υπηρεσίες Cloud για το IBM Trusteer Pinpoint Detect Standard ή/και το IBM Trusteer Pinpoint Detect Premium ή/και το IBM Security Pinpoint Detect Standard with access management integration ή/και το IBM Security Detect Premium with access management integration

α. Πρόσθετες Υπηρεσίες Cloud που διατίθενται για το IBM Trusteer Detect Standard for Business ή/και το IBM Trusteer Pinpoint Detect Premium for Business ή/και το IBM Security Pinpoint Detect Standard with access management integration for Business ή/και το IBM Security Detect Premium with access management integration for Business:

- IBM Trusteer Pinpoint Detect Standard Additional Applications for Business
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Business

β. Πρόσθετες Υπηρεσίες Cloud που διατίθενται για το IBM Trusteer Detect Standard for Retail ή/και το IBM Trusteer Pinpoint Detect Premium for Retail ή/και το IBM Security Pinpoint Detect Standard with access management integration for Retail ή/και το IBM Security Detect Premium with access management integration for Retail:

- IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail
- IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail

Μια συνδρομή για το IBM Trusteer Detect Standard ή το IBM Trusteer Pinpoint Detect Premium ή για το IBM Security Pinpoint Detect Standard with access management integration ή το IBM Security Detect Premium with access management integration αποτελεί απαραίτητη προϋπόθεση για την απόκτηση οποιασδήποτε από τις αντίστοιχες πρόσθετες Υπηρεσίες Cloud που αναφέρονται στο παρόν άρθρο.

1.1.7 Άλλες Πρόσθετες Υπηρεσίες Cloud

Οποιαδήποτε πρόσθετη συνδρομή Υπηρεσίας Cloud επιπλέον των ανωτέρω βασικών συνδρομών η οποία δεν αναφέρεται στο παρόν άρθρο, είτε είναι επί του παρόντος διαθέσιμη είτε βρίσκεται υπό ανάπτυξη, δεν θεωρείται ενημέρωση και πρέπει να χορηγείται χωριστά.

1.2 Ορισμοί

Κάτοχος Λογαριασμού (Account Holder) – ο τελικός χρήστης του Πελάτη, ο οποίος έχει εγκαταστήσει το λογισμικό ενεργοποίησης πελάτη, έχει αποδεχθεί τη σύμβαση άδειας χρήσης τελικού χρήστη ("Σύμβαση EULA") και έχει ταυτοποιηθεί τουλάχιστον μία φορά στην Εφαρμογή Λιανικής ή στην Επιχειρηματική Εφαρμογή του Πελάτη για την οποία ο Πελάτης έχει προμηθευτεί συνδρομή για την κάλυψη της εν λόγω Εφαρμογής από Υπηρεσίες Cloud.

Λογισμικό Πελάτη για Κάτοχο Λογαριασμού (Account Holder Client Software) – το λογισμικό ενεργοποίησης πελάτη IBM Trusteer Rapport, το λογισμικό ενεργοποίησης πελάτη IBM Trusteer Mobile Browser ή οποιοδήποτε άλλο λογισμικό ενεργοποίησης πελάτη που παρέχεται με ορισμένες Υπηρεσίες Cloud για εγκατάσταση στη συσκευή του τελικού χρήστη.

Οθόνη Εκκίνησης Trusteer (Trusteer Splash) – η οθόνη εκκίνησης που παρέχεται στον Πελάτη βάσει των διαθέσιμων προτύπων οθονών εκκίνησης.

Σελίδα Προσγείωσης (Landing Page) – η φιλοξενούμενη από την IBM σελίδα που παρέχεται στον Πελάτη με την οθόνη εκκίνησης και το μεταφορτώσιμο Λογισμικό Πελάτη για Κάτοχο Λογαριασμού.

2. Υπηρεσίες Cloud για το IBM Trusteer Rapport

2.1 IBM Trusteer Rapport for Retail ή/και IBM Trusteer Rapport for Business ("Trusteer Rapport")

Το Trusteer Rapport παρέχει ένα επίπεδο προστασίας έναντι επιθέσεων τύπου phishing και επιβλαβούς κώδικα MitB (Man-in-the-Browser). Χρησιμοποιώντας ένα δίκτυο αποτελούμενο από δεκάδες εκατομμύρια τελικά σημεία ανά τον κόσμο, το IBM Trusteer Rapport συλλέγει πληροφορίες για ενεργές επιθέσεις phishing και επιβλαβούς κώδικα έναντι οργανισμών σε παγκόσμια κλίμακα. Το IBM Trusteer

Rapport εφαρμόζει αλγορίθμους συμπεριφοράς με σκοπό την αποτροπή επιθέσεων phishing και την παρεμπόδιση της εγκατάστασης και λειτουργίας επιβλαβούς κώδικα MitB.

Αυτή η Υπηρεσία Cloud χρησιμοποιεί ένα μετρικό σύστημα χρέωσης βάσει Δικαιούμενων Συμμετεχόντων. Η Επιχειρηματική προσφορά πωλείται σε πακέτα των 10 Δικαιούμενων Συμμετεχόντων. Η προσφορά Λιανικής πωλείται σε πακέτα των 100 Δικαιούμενων Συμμετεχόντων.

Αυτή η Υπηρεσία Cloud περιλαμβάνει τα ακόλουθα στοιχεία:

α. Trusteer Management Application ("TMA"):

Το TMA διατίθεται στο φιλοξενούμενο στο cloud περιβάλλον του IBM Trusteer, μέσω του οποίου ο Πελάτης (και απεριόριστος αριθμός μελών του εξουσιοδοτημένου προσωπικού του) μπορούν: (i) να εξετάζουν και να μεταφορτώνουν (download) αναφορές δεδομένων περιστατικών και εκτιμήσεις κινδύνων, (ii) να εξετάζουν την παραμετροποποίηση του λογισμικού ενεργοποίησης πελάτη που παραχωρείται βάσει μιας σύμβασης άδειας χρήσης τελικού χρήστη ("Σύμβαση EULA"), χωρίς χρέωση, στους Δικαιούμενους Συμμετέχοντες του Πελάτη, και να το καθιστούν διαθέσιμο για μεταφόρτωση στους υπολογιστές και στις φορητές συσκευές (PC/MACs) των Δικαιούμενων Συμμετεχόντων. Το εν λόγω λογισμικό είναι επίσης γνωστό ως Trusteer Rapport software suite ("Λογισμικό Πελάτη για Κάτοχο Λογαριασμού"). Ο Πελάτης επιτρέπεται να διαθέτει το Λογισμικό Πελάτη για Κάτοχο Λογαριασμού στην αγορά μόνο μέσω της Οθόνης Εκκίνησης Trusteer ή του Report API, και ο Πελάτης δεν επιτρέπεται να χρησιμοποιεί το Λογισμικό Πελάτη για Κάτοχο Λογαριασμού για τις εσωτερικές λειτουργίες της επιχείρησής του ή για χρήση (με την εξαίρεση της προσωπικής χρήσης) από τους υπαλλήλους του.

β. Web Script:

Για πρόσβαση σε έναν ιστότοπο για τους σκοπούς της πρόσβασης ή χρήσης της Υπηρεσίας Cloud.

γ. Δεδομένα Περιστατικών:

Ο Πελάτης (και απεριόριστος αριθμός μελών του εξουσιοδοτημένου προσωπικού του) μπορούν να χρησιμοποιούν το TMA για τη λήψη δεδομένων περιστατικών που δημιουργήθηκαν από το Λογισμικό Πελάτη για Κάτοχο Λογαριασμού ως αποτέλεσμα των online συναλλαγών του Κατόχου Λογαριασμού με την Επιχειρηματική Εφαρμογή ή την Εφαρμογή Λιανικής για την οποία ο Πελάτης έχει προμηθευτεί συνδρομή για την κάλυψη της εν λόγω Εφαρμογής από Υπηρεσίες Cloud. Τα δεδομένα περιστατικών θα λαμβάνονται από το Λογισμικό Πελάτη για Κάτοχο Λογαριασμού που εκτελείται στις συσκευές των Δικαιούμενων Συμμετεχόντων, οι οποίοι θα έχουν αποδεχθεί τη Σύμβαση EULA, θα έχουν ταυτοποιηθεί τουλάχιστον μία φορά στην Επιχειρηματική Εφαρμογή ή στην Εφαρμογή Λιανικής του Πελάτη, ενώ η παραμετροποίηση του Πελάτη πρέπει να περιλαμβάνει τη συλλογή ταυτοτήτων χρήστη (user IDs).

δ. Οθόνη Εκκίνησης Trusteer:

Η Οθόνη Εκκίνησης Trusteer (Trusteer Splash) αποτελεί μια πλατφόρμα μάρκετινγκ μέσω της οποίας προωθείται το Λογισμικό Πελάτη για Κάτοχο Λογαριασμού στους Δικαιούμενους Συμμετέχοντες που αποκτούν πρόσβαση στις Επιχειρηματικές Εφαρμογές ή/και στις Εφαρμογές Λιανικής του Πελάτη για τις οποίες ο Πελάτης έχει προμηθευτεί συνδρομή για την κάλυψη των εν λόγω Εφαρμογών από Υπηρεσίες Cloud. Ο Πελάτης μπορεί να επιλέξει κάποιο από τα διαθέσιμα Πρότυπα Οθονών Εκκίνησης. Επίσης μπορεί να συνάψει χωριστή σύμβαση ή περιγραφή έργου για την παροχή ειδικά προσαρμοσμένης οθόνης εκκίνησης.

Ο Πελάτης μπορεί να συμφωνήσει στην παροχή των δικών του εμπορικών σημάτων, λογοτύπων και εικονιδίων για χρήση σε συνάρτηση με το TMA, αποκλειστικά για την εμφάνισή τους στην Οθόνη Εκκίνησης Trusteer, στις οθόνες του Λογισμικού Πελάτη για Κάτοχο Λογαριασμού ή στις σελίδες προσγείωσης που φιλοξενούνται από την IBM και στον ιστότοπο του IBM Trusteer. Οποιαδήποτε χρήση των παρεχόμενων εμπορικών σημάτων, λογοτύπων ή εικονιδίων θα γίνεται σύμφωνα με τις εύλογες πολιτικές της IBM αναφορικά με τη διαφήμιση και τη χρήση εμπορικών σημάτων.

Ο Πελάτης πρέπει να προμηθευτεί συνδρομή για την Υπηρεσία Cloud IBM Trusteer Rapport Mandatory Service εάν ο Πελάτης επιθυμεί να προβεί σε οποιουδήποτε είδους υποχρεωτική εγκατάσταση του Λογισμικού Πελάτη για Κάτοχο Λογαριασμού.

Στην υποχρεωτική εγκατάσταση του Λογισμικού Πελάτη για Κάτοχο Λογαριασμού περιλαμβάνεται, ενδεικτικά και όχι περιοριστικά, οποιοδήποτε είδος υποχρεωτικής εγκατάστασης από οποιονδήποτε μηχανισμό ή μέσο μέσω του οποίου ένας Δικαιούμενος Συμμετέχων υποχρεούται άμεσα ή έμμεσα να μεταφορτώσει το Λογισμικό Πελάτη για Κάτοχο Λογαριασμού, ή οποιαδήποτε μέθοδος, εργαλείο,

διαδικασία, συμφωνία ή μηχανισμός που δεν δημιουργήθηκε ή εγκρίθηκε από την IBM, που δημιουργήθηκε για την παράκαμψη των απαιτήσεων απόκτησης άδειας χρήσης για την εν λόγω υποχρεωτική εγκατάσταση του Λογισμικού Πελάτη για Κάτοχο Λογαριασμού.

2.2 IBM Trusteer Rapport II for Retail ή/και IBM Trusteer Rapport II for Business ("Trusteer Rapport II")

Η Υπηρεσία Cloud Trusteer Rapport II αποτελεί μια νέα εκδοχή του IBM Trusteer Rapport που βοηθά στην τυποποίηση των χρεώσεων που σχετίζονται με την προστασία περισσότερων από μία Εφαρμογών και αντικαθιστά τις εφάπαξ χρεώσεις που επιβάλλονται κατά την προσθήκη Εφαρμογών.

Το Trusteer Rapport II παρέχει ένα επίπεδο προστασίας έναντι επιθέσεων τύπου phishing και επιβλαβούς κώδικα MitB (Man-in-the-Browser). Χρησιμοποιώντας ένα δίκτυο αποτελούμενο από δεκάδες εκατομμύρια τελικά σημεία ανά τον κόσμο, το IBM Trusteer Rapport συλλέγει πληροφορίες για ενεργές επιθέσεις phishing και επιβλαβούς κώδικα έναντι οργανισμών σε παγκόσμια κλίμακα. Το IBM Trusteer Rapport εφαρμόζει αλγορίθμους συμπεριφοράς με σκοπό την αποτροπή επιθέσεων phishing και την παρεμπόδιση της εγκατάστασης και λειτουργίας επιβλαβούς κώδικα MitB.

Τα δικαιώματα χρήσης αυτής της Υπηρεσίας Cloud υπόκεινται στο μετρικό σύστημα χρέωσης βάσει Δικαιούμενων Συμμετεχόντων. Η Επιχειρηματική προσφορά πωλείται σε πακέτα των 10 Δικαιούμενων Συμμετεχόντων. Η προσφορά Λιανικής πωλείται σε πακέτα των 100 Δικαιούμενων Συμμετεχόντων.

Αυτή η Υπηρεσία Cloud περιλαμβάνει τα ακόλουθα στοιχεία:

α. Trusteer Management Application ("TMA"):

Το TMA διατίθεται στο φιλοξενούμενο στο cloud περιβάλλον του IBM Trusteer, μέσω του οποίου ο Πελάτης (και απεριόριστος αριθμός μελών του εξουσιοδοτημένου προσωπικού του) μπορούν: (i) να εξετάζουν και να μεταφορτώνουν (download) αναφορές δεδομένων περιστατικών και εκτιμήσεις κινδύνων, (ii) να εξετάζουν την παραμετροποποίηση του λογισμικού ενεργοποίησης πελάτη που παραχωρείται βάσει μιας σύμβασης άδειας χρήσης τελικού χρήστη ("Σύμβαση EULA"), χωρίς χρέωση, στους Δικαιούμενους Συμμετέχοντες του Πελάτη, και να το καθιστούν διαθέσιμο για μεταφόρτωση στους υπολογιστές και στις φορητές συσκευές (PC/MACs) των Δικαιούμενων Συμμετεχόντων. Το εν λόγω λογισμικό είναι επίσης γνωστό ως Trusteer Rapport software suite ("Λογισμικό Πελάτη για Κάτοχο Λογαριασμού"). Ο Πελάτης επιτρέπεται να διαθέτει το Λογισμικό Πελάτη για Κάτοχο Λογαριασμού στην αγορά μόνο μέσω της Οθόνης Εκκίνησης Trusteer ή του Report API, και ο Πελάτης δεν επιτρέπεται να χρησιμοποιεί το Λογισμικό Πελάτη για Κάτοχο Λογαριασμού για τις εσωτερικές λειτουργίες της επιχείρησής του ή για χρήση (με την εξαίρεση της προσωπικής χρήσης) από τους υπαλλήλους του.

β. Web Script:

Για πρόσβαση σε έναν ιστότοπο για τους σκοπούς της πρόσβασης ή χρήσης της Υπηρεσίας Cloud.

γ. Δεδομένα Περιστατικών:

Ο Πελάτης (και απεριόριστος αριθμός μελών του εξουσιοδοτημένου προσωπικού του) μπορούν να χρησιμοποιούν το TMA για τη λήψη δεδομένων περιστατικών που δημιουργήθηκαν από το Λογισμικό Πελάτη για Κάτοχο Λογαριασμού ως αποτέλεσμα των online συναλλαγών του Κατόχου Λογαριασμού με την Επιχειρηματική Εφαρμογή ή την Εφαρμογή Λιανικής για την οποία ο Πελάτης έχει προμηθευτεί συνδρομή για την κάλυψη της εν λόγω Εφαρμογής από Υπηρεσίες Cloud. Τα δεδομένα περιστατικών θα λαμβάνονται από το Λογισμικό Πελάτη για Κάτοχο Λογαριασμού που εκτελείται στις συσκευές των Δικαιούμενων Συμμετεχόντων, οι οποίοι θα έχουν αποδεχθεί τη Σύμβαση EULA, θα έχουν ταυτοποιηθεί τουλάχιστον μία φορά στην Επιχειρηματική Εφαρμογή ή στην Εφαρμογή Λιανικής του Πελάτη, ενώ η παραμετροποίηση του Πελάτη πρέπει να περιλαμβάνει τη συλλογή ταυτοτήτων χρήστη (user IDs).

δ. Οθόνη Εκκίνησης Trusteer:

Η Οθόνη Εκκίνησης Trusteer (Trusteer Splash) αποτελεί μια πλατφόρμα μάρκετινγκ μέσω της οποίας προωθείται το Λογισμικό Πελάτη για Κάτοχο Λογαριασμού στους Δικαιούμενους Συμμετέχοντες που αποκτούν πρόσβαση στις Επιχειρηματικές Εφαρμογές ή/και στις Εφαρμογές Λιανικής του Πελάτη για τις οποίες ο Πελάτης έχει προμηθευτεί συνδρομή για την κάλυψη των εν λόγω Εφαρμογών από Υπηρεσίες Cloud. Ο Πελάτης μπορεί να επιλέξει κάποιο από τα διαθέσιμα Πρότυπα Οθονών Εκκίνησης. Επίσης μπορεί να συνάψει χωριστή σύμβαση ή περιγραφή έργου για την παροχή ειδικά προσαρμοσμένης οθόνης εκκίνησης.

Ο Πελάτης μπορεί να συμφωνήσει στην παροχή των δικών του εμπορικών σημάτων, λογοτύπων και εικονιδίων για χρήση σε συνάρτηση με το TMA, αποκλειστικά για την εμφάνισή τους στην Οθόνη Εκκίνησης Trusteer, στις οθόνες του Λογισμικού Πελάτη για Κάτοχο Λογαριασμού ή στις σελίδες προσγείωσης που φιλοξενούνται από την IBM και στον ιστότοπο του IBM Trusteer. Οποιαδήποτε χρήση των παρεχόμενων εμπορικών σημάτων, λογοτύπων ή εικονιδίων θα γίνεται σύμφωνα με τις εύλογες πολιτικές της IBM αναφορικά με τη διαφήμιση και τη χρήση εμπορικών σημάτων.

Ο Πελάτης πρέπει να προμηθευτεί συνδρομή για την Υπηρεσία Cloud IBM Trusteer Rapport Mandatory Service εάν ο Πελάτης επιθυμεί να προβεί σε οποιουδήποτε είδους υποχρεωτική εγκατάσταση του Λογισμικού Πελάτη για Κάτοχο Λογαριασμού.

Στην υποχρεωτική εγκατάσταση του Λογισμικού Πελάτη για Κάτοχο Λογαριασμού περιλαμβάνεται, ενδεικτικά και όχι περιοριστικά, οποιοδήποτε είδος υποχρεωτικής εγκατάστασης από οποιονδήποτε μηχανισμό ή μέσο μέσω του οποίου ένας Δικαιούμενος Συμμετέχων υποχρεούται άμεσα ή έμμεσα να μεταφορτώσει το Λογισμικό Πελάτη για Κάτοχο Λογαριασμού, ή οποιαδήποτε μέθοδος, εργαλείο, διαδικασία, συμφωνία ή μηχανισμός που δεν δημιουργήθηκε ή εγκρίθηκε από την IBM, που δημιουργήθηκε για την παράκαμψη των απαιτήσεων απόκτησης άδειας χρήσης για την εν λόγω υποχρεωτική εγκατάσταση του Λογισμικού Πελάτη για Κάτοχο Λογαριασμού.

Το Trusteer Rapport II for Business ή/και το Trusteer Rapport II for Retail περιλαμβάνει προστασία για μία Εφαρμογή. Για κάθε πρόσθετη Εφαρμογή, ο Πελάτης πρέπει να αποκτήσει δικαίωμα χρήσης του IBM Trusteer Rapport Additional Applications.

2.3 Προαιρετικές Πρόσθετες Υπηρεσίες Cloud για το IBM Trusteer Rapport for Business ή/και το IBM Trusteer Rapport for Retail ή/και το IBM Trusteer Rapport II for Business ή/και το IBM Trusteer Rapport II for Retail

Μια συνδρομή για τις Υπηρεσίες Cloud για το IBM Trusteer Rapport ή το IBM Trusteer Rapport II αποτελεί απαραίτητη προϋπόθεση για την απόκτηση συνδρομής για οποιαδήποτε από τις ακόλουθες Υπηρεσίες Cloud. Εάν η Υπηρεσία Cloud προσδιορίζεται ως υπηρεσία "for Business" (για Επιχειρηματική Χρήση), τότε οι πρόσθετες Υπηρεσίες Cloud που αποκτά ο Πελάτης πρέπει επίσης να προσδιορίζονται ως υπηρεσίες "for Business". Εάν η Υπηρεσία Cloud προσδιορίζεται ως υπηρεσία "for Retail" (για Λιανική Χρήση), τότε οι πρόσθετες Υπηρεσίες Cloud που αποκτά ο Πελάτης πρέπει επίσης να προσδιορίζονται ως υπηρεσίες "for Retail". Ο Πελάτης θα λαμβάνει δεδομένα περιστατικών από Δικαιούμενους Συμμετέχοντες που χρησιμοποιούν το Λογισμικό Πελάτη για Κάτοχο Λογαριασμού και έχουν αποδεχθεί τη Σύμβαση EULA, έχουν ταυτοποιηθεί τουλάχιστον μία φορά στην (στις) Επιχειρηματική(-ές) Εφαρμογή(-ές) ή Εφαρμογή(-ές) Λιανικής του Πελάτη, ενώ η παραμετροποίηση του Πελάτη πρέπει να περιλαμβάνει τη συλλογή ταυτοτήτων χρήστη (user IDs).

2.3.1 IBM Trusteer Rapport Fraud Feeds for Business ή/και IBM Trusteer Rapport Fraud Feeds for Retail

Όταν ο Πελάτης προμηθευτεί συνδρομή για αυτή την πρόσθετη Υπηρεσία Cloud, ο Πελάτης (και απεριόριστος αριθμός μελών του εξουσιοδοτημένου προσωπικού του) μπορούν να κάνουν χρήση του TMA για να εγγραφούν ως συνδρομητές, να εξετάζουν και να παραμετροποιούν την παράδοση τροφοδοσιών δεδομένων απειλών (threat feeds) που παράγονται από την Υπηρεσία Cloud για το Trusteer Report. Οι τροφοδοσίες αυτές μπορούν να σταλούν μέσω email σε καθορισμένες διευθύνσεις email ή μέσω SFTP με τη μορφή αρχείων κειμένου.

2.3.2 IBM Trusteer Rapport Phishing Protection for Business ή/και IBM Trusteer Rapport Phishing Protection for Retail

Ο Πελάτης (και απεριόριστος αριθμός μελών του εξουσιοδοτημένου προσωπικού του) μπορούν να χρησιμοποιούν το TMA για τη λήψη ειδοποιήσεων για δεδομένα περιστατικών που σχετίζονται με την υποβολή στοιχείων ταυτότητας για τη σύνδεση του Κατόχου Λογαριασμού σε έναν ιστότοπο για τον οποίο υπάρχουν υποψίες ότι χρησιμοποιείται για phishing ή άλλες μορφές απάτης. Ενδέχεται να υπάρχουν έγκυρες online εφαρμογές (URL) που χαρακτηρίζονται εσφαλμένα ως ιστότοποι phishing και η Υπηρεσία Cloud μπορεί να προειδοποιήσει τους Κατόχους Λογαριασμών ότι ένας έγκυρος ιστότοπος είναι ιστότοπος phishing. Σε τέτοιες περιπτώσεις, ο Πελάτης πρέπει να ενημερώσει την IBM ότι πρόκειται για σφάλμα και η IBM θα διορθώσει το εν λόγω σφάλμα. Πρόκειται για αποκλειστικό μέσο επανόρθωσης που παρέχεται στον Πελάτη για το εν λόγω σφάλμα.

2.3.3 IBM Trusteer Rapport Mandatory Service for Business ή/και IBM Trusteer Rapport Mandatory Service for Retail

Ο Πελάτης επιτρέπεται να χρησιμοποιεί μια περίπτωση χρήσης της πλατφόρμας μάρκετινγκ Trusteer Splash ώστε να παρέχει τη δυνατότητα μεταφόρτωσης του Λογισμικού Πελάτη για Κάτοχο Λογαριασμού

από Δικαιούμενους Συμμετέχοντες που αποκτούν πρόσβαση στις Επιχειρηματικές Εφαρμογές ή/και Εφαρμογές Λιανικής του Πελάτη για τις οποίες ο Πελάτης έχει προμηθευτεί συνδρομή για την κάλυψη των εν λόγω Εφαρμογών από Υπηρεσίες Cloud.

Μια συνδρομή για το IBM Trusteer Rapport Premium Support αποτελεί απαραίτητη προϋπόθεση για την απόκτηση συνδρομής για το IBM Security Rapport Mandatory Service for Business.

Μια συνδρομή για το IBM Trusteer Rapport Premium Support for Retail αποτελεί απαραίτητη προϋπόθεση για την απόκτηση συνδρομής για το IBM Security Rapport Mandatory Service for Retail.

Ο Πελάτης επιτρέπεται να εφαρμόζει τις πρόσθετες λειτουργίες του IBM Trusteer Rapport Mandatory Service μόνο εάν παραγγέλθηκαν και παραμετροποιήθηκαν για χρήση με την Επιχειρηματική Εφαρμογή ή την Εφαρμογή Λιανικής του Πελάτη για την οποία ο Πελάτης προμηθεύτηκε συνδρομή για την κάλυψη της εν λόγω Εφαρμογής από Υπηρεσίες Cloud.

2.3.4 IBM Trusteer Rapport Large Redeployment ή/και IBM Trusteer Rapport Small Redeployment

Οι Πελάτες που προβαίνουν στην εκ νέου υλοποίηση (redeployment) των Εφαρμογών online τραπεζικών συναλλαγών τους κατά τη διάρκεια της περιόδου ισχύος της υπηρεσίας και στη συνέχεια απαιτούν την πραγματοποίηση αλλαγών στην εν λόγω νέα υλοποίηση του IBM Trusteer Rapport ή του IBM Trusteer Rapport II, θα πρέπει να αγοράσουν την Υπηρεσία Cloud για το IBM Trusteer Rapport Redeployment.

Η εκ νέου υλοποίηση μπορεί να είναι απαραίτητη επειδή ο Πελάτης άλλαξε τον τομέα (domain) ή τη διεύθυνση URL της Εφαρμογής, τροποποίησε την οθόνη εκκίνησης ή μετέφερε την Εφαρμογή σε μια νέα πλατφόρμα online τραπεζικών συναλλαγών.

Κατά τη διάρκεια της περιόδου μετάβασης 6 μηνών για την εκ νέου υλοποίηση, ο Πελάτης δικαιούται την εκτέλεση πρόσθετων Εφαρμογών, σε μια σχέση μία προς μία, επιπλέον των Εφαρμογών για τις οποίες έχει προμηθευτεί συνδρομή.

Το IBM Trusteer Rapport Large Redeployment προορίζεται για περιβάλλοντα με περισσότερους από 20.000 χρήστες, ενώ το IBM Trusteer Rapport Small Redeployment προορίζεται για μικρότερα περιβάλλοντα με 20.000 το πολύ χρήστες.

2.3.5 IBM Trusteer Rapport Additional Applications for Business ή/και IBM Trusteer Rapport Additional Applications for Retail

Για το IBM Trusteer Rapport II for Business, προϋπόθεση για την υλοποίηση σε οποιαδήποτε πρόσθετη Επιχειρηματική Εφαρμογή επιπλέον της πρώτης Εφαρμογής είναι η απόκτηση δικαιώματος χρήσης της Υπηρεσίας Cloud για το IBM Trusteer Rapport Additional Applications for Business. Για το IBM Trusteer Rapport II for Retail, προϋπόθεση για την υλοποίηση σε οποιαδήποτε πρόσθετη Εφαρμογή Λιανικής επιπλέον της πρώτης Εφαρμογής είναι η απόκτηση δικαιώματος χρήσης της Υπηρεσίας Cloud για το IBM Trusteer Rapport Additional Applications for Retail.

3. Υπηρεσίες Cloud για το IBM Trusteer Pinpoint

Το IBM Trusteer Pinpoint είναι μια βασιζόμενη στο cloud υπηρεσία που έχει σχεδιαστεί για την παροχή ενός πρόσθετου επιπέδου προστασίας και στοχεύει στον εντοπισμό και την αποτροπή επιθέσεων επιβλαβούς κώδικα, phishing και οικειοποίησης λογαριασμού (account takeover). Το Trusteer Pinpoint μπορεί να ενσωματωθεί στις Επιχειρηματικές Εφαρμογές ή/και Εφαρμογές Λιανικής του Πελάτη για τις οποίες έχει προμηθευτεί συνδρομή για την κάλυψη των εν λόγω Εφαρμογών από Υπηρεσίες Cloud και τις αντίστοιχες διαδικασίες καταπολέμησης απάτης.

Αυτή η Υπηρεσία Cloud περιλαμβάνει τα ακόλουθα στοιχεία:

α. TMA:

Το TMA διατίθεται στο φιλοξενούμενο στο cloud περιβάλλον του IBM Trusteer, μέσω του οποίου ο Πελάτης (και απεριόριστος αριθμός μελών του εξουσιοδοτημένου προσωπικού του) μπορούν: (i) να εξετάζουν και να μεταφορτώνουν (download) αναφορές ορισμένων δεδομένων περιστατικών και εκτιμήσεις κινδύνων, και (ii) να εγγραφούν ως συνδρομητές, να εξετάζουν και να παραμετροποιούν την παράδοση τροφοδοσιών δεδομένων απειλών (threat feeds) που παράγονται από τις προσφορές Pinpoint.

β. Web Script ή/και APIs:

Για υλοποίηση σε έναν ιστότοπο για τους σκοπούς της πρόσβασης ή χρήσης της Υπηρεσίας Cloud.

3.1 Βέλτιστες πρακτικές για το IBM Trusteer Pinpoint Malware Detection και το IBM Trusteer Pinpoint Criminal Detection

Σε περίπτωση που εντοπιστεί επιβλαβής κώδικας από μια Υπηρεσία Cloud IBM Trusteer Pinpoint Malware Detection ή IBM Trusteer Pinpoint Malware Detection II ή εντοπιστούν απόπειρες οικειοποίησης λογαριασμού (account takeover) από μια Υπηρεσία Cloud IBM Trusteer Pinpoint Criminal Detection ή IBM Trusteer Pinpoint Criminal Detection II, ο Πελάτης πρέπει να ακολουθεί τις οδηγίες που παρέχονται στο εγχειρίδιο Pinpoint Best Practices Guide. Μη χρησιμοποιείτε τις Υπηρεσίες Cloud IBM Trusteer Pinpoint Malware Detection ή IBM Trusteer Pinpoint Malware Detection II ή τις Υπηρεσίες Cloud IBM Trusteer Pinpoint Criminal Detection ή IBM Trusteer Pinpoint Criminal Detection II με οποιονδήποτε τρόπο που επηρεάζει τη γενική εμπειρία του Δικαιούμενου Συμμετέχοντος αμέσως μετά τον εντοπισμό επιβλαβούς κώδικα ή απόπειρας οικειοποίησης λογαριασμού (account takeover), παρέχοντας έτσι σε άλλους τη δυνατότητα να συσχετίσουν τις ενέργειες του Πελάτη με την εκ μέρους του χρήση Υπηρεσιών Cloud IBM Trusteer Pinpoint (π.χ. αποστολή ειδοποιήσεων ή μηνυμάτων, φραγή συσκευών, φραγή της πρόσβασης στην Επιχειρηματική Εφαρμογή ή/και στην Εφαρμογή Λιανικής αμέσως μετά τον εντοπισμό επιβλαβούς κώδικα ή απόπειρας οικειοποίησης λογαριασμού).

3.2 IBM Trusteer Pinpoint Criminal Detection for Business ή/και IBM Trusteer Pinpoint Criminal Detection for Retail

Εντοπισμός, χωρίς τη χρήση λογισμικού πελάτη, ύποπτων δραστηριοτήτων οικειοποίησης λογαριασμού από προγράμματα πλοήγησης που συνδέονται σε μια Επιχειρηματική Εφαρμογή ή Εφαρμογή Λιανικής, χρησιμοποιώντας τη ταυτότητα συσκευής (device ID) και τεχνικές εντοπισμού phishing και κλοπής στοιχείων ταυτότητας μέσω επιβλαβούς κώδικα. Οι Υπηρεσίες Cloud για το IBM Trusteer Pinpoint Criminal Detection παρέχουν ένα πρόσθετο επίπεδο προστασίας και στοχεύουν στον εντοπισμό προσπαθειών οικειοποίησης λογαριασμού (account takeover) και στην παράδοση, απευθείας στον Πελάτη, βαθμολογικών στοιχείων εκτίμησης κινδύνων για προγράμματα πλοήγησης ή φορητές συσκευές (με χρήση του τοπικού προγράμματος πλοήγησης ή της εφαρμογής του Πελάτη για φορητές συσκευές) που αποκτούν πρόσβαση σε μια Επιχειρηματική Εφαρμογή ή Εφαρμογή Λιανικής.

α. Δεδομένα Περιστατικών:

Ο Πελάτης (και απεριόριστος αριθμός μελών του εξουσιοδοτημένου προσωπικού του) μπορούν να χρησιμοποιούν το TMA για τη λήψη δεδομένων περιστατικών που προκύπτουν από online συναλλαγές Δικαιούμενων Συμμετεχόντων με την (τις) Επιχειρηματική(-ές) Εφαρμογή(-ές) ή Εφαρμογή(-ές) Λιανικής του Πελάτη για την (τις) οποία(-ες) ο Πελάτης έχει προμηθευτεί συνδρομή για την κάλυψή της (τους) από τις Υπηρεσίες Cloud. Εναλλακτικά, ο Πελάτης μπορεί να λαμβάνει τα δεδομένα περιστατικών μέσω ενός API παρασκηνιακής παράδοσης.

3.3 IBM Trusteer Pinpoint Criminal Detection II for Business ή/και IBM Trusteer Pinpoint Criminal Detection II for Retail

Το IBM Trusteer Pinpoint Criminal Detection II αποτελεί μια νέα εκδοχή του IBM Trusteer Pinpoint Criminal Detection που βοηθά στην τυποποίηση των χρεώσεων που σχετίζονται με την προστασία περισσότερων από μία Εφαρμογών και αντικαθιστά τις εφάπαξ χρεώσεις που επιβάλλονται κατά την προσθήκη Εφαρμογών.

Εντοπισμός, χωρίς τη χρήση λογισμικού πελάτη, ύποπτων δραστηριοτήτων οικειοποίησης λογαριασμού από προγράμματα πλοήγησης που συνδέονται σε μια Επιχειρηματική Εφαρμογή ή Εφαρμογή Λιανικής, χρησιμοποιώντας τη ταυτότητα συσκευής (device ID) και τεχνικές εντοπισμού phishing και κλοπής στοιχείων ταυτότητας μέσω επιβλαβούς κώδικα. Οι Υπηρεσίες Cloud για το IBM Trusteer Pinpoint Criminal Detection II παρέχουν ένα πρόσθετο επίπεδο προστασίας και στοχεύουν στον εντοπισμό απόπειρων οικειοποίησης λογαριασμού (account takeover) και στην παράδοση, απευθείας στον Πελάτη, βαθμολογικών στοιχείων εκτίμησης κινδύνων για προγράμματα πλοήγησης ή φορητές συσκευές (με χρήση του τοπικού προγράμματος πλοήγησης ή της εφαρμογής του πελάτη για φορητές συσκευές) που αποκτούν πρόσβαση σε μια Επιχειρηματική Εφαρμογή ή Εφαρμογή Λιανικής.

α. Δεδομένα Περιστατικών:

Ο Πελάτης (και απεριόριστος αριθμός μελών του εξουσιοδοτημένου προσωπικού του) μπορούν να χρησιμοποιούν το TMA για τη λήψη δεδομένων περιστατικών που προκύπτουν από online συναλλαγές Δικαιούμενων Συμμετεχόντων με την (τις) Επιχειρηματική(-ές) Εφαρμογή(-ές) ή Εφαρμογή(-ές) Λιανικής του Πελάτη για την (τις) οποία(-ες) ο Πελάτης έχει προμηθευτεί συνδρομή για την κάλυψή της (τους) από τις Υπηρεσίες Cloud. Εναλλακτικά, ο Πελάτης μπορεί να λαμβάνει τα δεδομένα περιστατικών μέσω ενός API παρασκηνιακής παράδοσης.

Αυτή η Υπηρεσία Cloud παρέχει προστασία για μία Εφαρμογή. Για κάθε πρόσθετη Εφαρμογή, ο Πελάτης πρέπει να αποκτήσει δικαίωμα χρήσης του IBM Trusteer Pinpoint Criminal Detection Additional Applications.

3.4 IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition ή/και IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition ή/και IBM Trusteer Pinpoint Malware Detection for Business Standard Edition ή/και IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition

Εντοπισμός μολυσμένων με επιβλαβή χρηματοοικονομικό κώδικα MitB (Man in the Browser) προγραμμάτων πλοήγησης (browsers) που συνδέονται σε μια Επιχειρηματική Εφαρμογή ή/και Εφαρμογή Λιανικής. Οι Υπηρεσίες Cloud για το IBM Trusteer Pinpoint Malware Detection παρέχουν ένα πρόσθετο επίπεδο προστασίας που επιτρέπει στους οργανισμούς να επικεντρώνονται σε διαδικασίες καταπολέμησης απάτης που βασίζονται στην εκτίμηση κινδύνων επιβλαβούς κώδικα παρέχοντας στον Πελάτη αξιολογήσεις και προειδοποιήσεις αναφορικά με την παρουσία επιβλαβούς χρηματοοικονομικού κώδικα MitB.

α. Δεδομένα Περιστατικών:

Ο Πελάτης (και απεριόριστος αριθμός μελών του εξουσιοδοτημένου προσωπικού του) μπορούν να χρησιμοποιούν το TMA για τη λήψη δεδομένων περιστατικών που προκύπτουν από online συναλλαγές Δικαιούμενων Συμμετεχόντων με την (τις) Επιχειρηματική(-ές) Εφαρμογή(-ές) ή Εφαρμογή(-ές) Λιανικής του Πελάτη.

β. Έκδοση Advanced:

Οι Εκδόσεις Advanced για Επιχειρηματική (for Business) ή/και για Λιανική Χρήση (for Retail) παρέχουν ένα πρόσθετο επίπεδο εντοπισμού και προστασίας που αναπροσαρμόζεται και ρυθμίζεται για τη συγκεκριμένη δομή και ροή των Επιχειρηματικών Εφαρμογών ή/και Εφαρμογών Λιανικής του Πελάτη, και μπορούν να προσαρμοστούν για το συγκεκριμένο τοπίο απειλών που αντιμετωπίζει ο Πελάτης. Μπορεί να ενσωματωθεί σε διάφορα σημεία των Επιχειρηματικών Εφαρμογών ή/και Εφαρμογών Λιανικής του Πελάτη.

Η Έκδοση Advanced προσφέρεται στον Πελάτη με 100K Δικαιούμενους Συμμετέχοντες ως ελάχιστη ποσότητα για Λιανική Χρήση ή 10K Δικαιούμενους Συμμετέχοντες ως ελάχιστη ποσότητα για Επιχειρηματική Χρήση. Πρόκειται για 1000 πακέτα των 100 Δικαιούμενων Συμμετεχόντων για Λιανική Χρήση ή 1000 πακέτα των 10 Δικαιούμενων Συμμετεχόντων για Επιχειρηματική Χρήση.

γ. Έκδοση Standard:

Η Έκδοση Standard για Επιχειρηματική Χρήση (for Business) ή για Λιανική Χρήση (for Retail) είναι μια άμεσα υλοποιήσιμη λύση που παρέχει τις κύριες λειτουργίες αυτής της Υπηρεσίας Cloud, όπως περιγράφεται στο παρόν.

3.5 IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business ή/και IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail ή/και IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business ή/και IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail

Το IBM Trusteer Pinpoint Malware Detection II αποτελεί μια νέα εκδοχή του IBM Trusteer Pinpoint Malware Detection που βοηθά στην τυποποίηση των χρεώσεων που σχετίζονται με την προστασία περισσότερων από μία Εφαρμογών και αντικαθιστά τις εφάπαξ χρεώσεις που επιβάλλονται κατά την προσθήκη Εφαρμογών.

Εντοπισμός μολυσμένων με επιβλαβή χρηματοοικονομικό κώδικα MitB (Man in the Browser) προγραμμάτων πλοήγησης (browsers) που συνδέονται σε μια Επιχειρηματική Εφαρμογή ή/και Εφαρμογή Λιανικής. Οι Υπηρεσίες Cloud για το IBM Trusteer Pinpoint Malware Detection παρέχουν ένα πρόσθετο επίπεδο προστασίας που επιτρέπει στους οργανισμούς να επικεντρώνονται σε διαδικασίες καταπολέμησης απάτης που βασίζονται στην εκτίμηση κινδύνων επιβλαβούς κώδικα παρέχοντας στον Πελάτη αξιολογήσεις και προειδοποιήσεις αναφορικά με την παρουσία επιβλαβούς χρηματοοικονομικού κώδικα MitB.

α. Δεδομένα Περιστατικών:

Ο Πελάτης (και απεριόριστος αριθμός μελών του εξουσιοδοτημένου προσωπικού του) μπορούν να χρησιμοποιούν το TMA για τη λήψη δεδομένων περιστατικών που προκύπτουν από online

συναλλαγές Δικαιούμενων Συμμετεχόντων με την (τις) Επιχειρηματική(-ές) Εφαρμογή(-ές) ή Εφαρμογή(-ές) Λιανικής του Πελάτη.

β. Έκδοση Advanced:

Οι Εκδόσεις Advanced για Επιχειρηματική (for Business) ή/και για Λιανική Χρήση (for Retail) παρέχουν ένα πρόσθετο επίπεδο εντοπισμού και προστασίας που αναπροσαρμόζεται και ρυθμίζεται για τη συγκεκριμένη δομή και ροή των Επιχειρηματικών Εφαρμογών ή/και Εφαρμογών Λιανικής του Πελάτη, και μπορούν να προσαρμοστούν για το συγκεκριμένο τοπίο απειλών που αντιμετωπίζει ο Πελάτης. Μπορεί να ενσωματωθεί σε διάφορα σημεία των Επιχειρηματικών Εφαρμογών ή/και Εφαρμογών Λιανικής του Πελάτη.

Η Έκδοση Advanced προσφέρεται στον Πελάτη με 100K Δικαιούμενους Συμμετέχοντες ως ελάχιστη ποσότητα για Λιανική Χρήση ή 10K Δικαιούμενους Συμμετέχοντες ως ελάχιστη ποσότητα για Επιχειρηματική Χρήση. Πρόκειται για 1000 πακέτα των 100 Δικαιούμενων Συμμετεχόντων για Λιανική Χρήση ή 1000 πακέτα των 10 Δικαιούμενων Συμμετεχόντων για Επιχειρηματική Χρήση.

γ. Έκδοση Standard:

Η Έκδοση Standard για Επιχειρηματική Χρήση (for Business) ή για Λιανική Χρήση (for Retail) είναι μια άμεσα υλοποιήσιμη λύση που παρέχει τις κύριες λειτουργίες αυτής της Υπηρεσίας Cloud, όπως περιγράφεται στο παρόν.

Αυτή η Υπηρεσία Cloud παρέχει προστασία για μία Εφαρμογή. Για κάθε πρόσθετη Εφαρμογή, ο Πελάτης πρέπει να αποκτήσει δικαίωμα χρήσης του IBM Trusteer Pinpoint Malware Detection Additional Applications.

3.6 Προαιρετικές Πρόσθετες Υπηρεσίες Cloud για το IBM Trusteer Pinpoint Malware Detection for Business Advanced Edition ή/και το IBM Trusteer Pinpoint Malware Detection for Retail Advanced Edition ή/και το IBM Trusteer Pinpoint Malware Detection for Business Standard Edition ή/και το IBM Trusteer Pinpoint Malware Detection for Retail Standard Edition ή/και το IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail ή/και το IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business ή/και το IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail ή/και το IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business

- Απαραίτητη προϋπόθεση για την Υπηρεσία Cloud για το IBM Trusteer Rapport Remediation for Retail είναι η απόκτηση συνδρομής για το IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail ή το IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail ή το IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail ή το IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail.
- Απαραίτητη προϋπόθεση για την Υπηρεσία Cloud για το IBM Trusteer Rapport Remediation for Business είναι η απόκτηση συνδρομής για το IBM Trusteer Pinpoint Malware Detection Standard Edition for Business ή το IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business ή το IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business ή το IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business.
- Απαραίτητη προϋπόθεση για την προσφορά IBM Trusteer Pinpoint Carbon Copy for Retail, είναι η απόκτηση συνδρομής για το IBM Trusteer Pinpoint Malware Detection Standard Edition for Retail ή το IBM Trusteer Pinpoint Malware Detection Advanced Edition for Retail ή το IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail ή το IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail.
- Απαραίτητη προϋπόθεση για την προσφορά IBM Trusteer Pinpoint Carbon Copy for Business είναι η απόκτηση συνδρομής για το IBM Trusteer Pinpoint Malware Detection Standard Edition for Business ή το IBM Trusteer Pinpoint Malware Detection Advanced Edition for Business ή το IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business ή το IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business.

3.6.1 IBM Trusteer Pinpoint Carbon Copy for Business ή/και IBM Trusteer Pinpoint Carbon Copy for Retail

Οι προσφορές IBM Trusteer Pinpoint Carbon Copy έχουν σχεδιαστεί για την παροχή ενός πρόσθετου επιπέδου προστασίας, καθώς περιλαμβάνουν μια υπηρεσία παρακολούθησης που επιτρέπει τον εντοπισμό περιστατικών υποκλοπής στοιχείων ταυτότητας Δικαιούμενων Συμμετεχόντων από επιθέσεις

phishing στις Επιχειρηματικές Εφαρμογές ή/και Εφαρμογές Λιανικής του Πελάτη για τις οποίες ο Πελάτης έχει προμηθευτεί συνδρομή για την κάλυψη των εν λόγω Εφαρμογών από προσφορές Υπηρεσιών Cloud.

3.6.2 IBM Trusteer Rapport Remediation for Retail ή/και IBM Trusteer Rapport Remediation for Business

Το IBM Trusteer Rapport Remediation for Retail και το IBM Trusteer Rapport Remediation for Business στοχεύουν στη διερεύνηση, αντιμετώπιση, αποτροπή και αφαίρεση μολύνσεων από επιβλαβή κώδικα MitB (Man-in-the-Browser) από μολυσμένες συσκευές (PC/MACs) Δικαιούμενων Συμμετεχόντων του Πελάτη που αποκτούν πρόσβαση στην Εφαρμογή του Πελάτη σε περιστασιακή βάση, σε περίπτωση που έχουν εντοπιστεί τέτοιες μολύνσεις από επιβλαβή κώδικα MitB στα δεδομένα περιστατικών του IBM Trusteer Pinpoint Malware Detection. Ο Πελάτης πρέπει να διαθέτει μια ισχύουσα συνδρομή για το IBM Trusteer Pinpoint Malware Detection ή το IBM Trusteer Pinpoint Malware Detection II που εκτελείται στην Εφαρμογή του Πελάτη. Ο Πελάτης επιτρέπεται να χρησιμοποιεί αυτή την προσφορά Υπηρεσίας Cloud μόνο σε συνάρτηση με Δικαιούμενους Συμμετέχοντες που αποκτούν πρόσβαση στην Εφαρμογή του Πελάτη, και αποκλειστικά ως εργαλείο που στοχεύει στη διερεύνηση και αντιμετώπιση μιας συγκεκριμένης μολυσμένης συσκευής (PC/MAC) σε περιστασιακή βάση. Το IBM Trusteer Rapport Remediation πρέπει να εκτελείται πράγματι στην εν λόγω συσκευή (PC/MAC) του Δικαιούμενου Συμμετέχοντος και ο εν λόγω Δικαιούμενος Συμμετέχων πρέπει να αποδεχθεί τη Σύμβαση EULA, να ταυτοποιηθεί τουλάχιστον μία φορά στην Εφαρμογή του Πελάτη, ενώ η παραμετροποίηση του Πελάτη πρέπει να περιλαμβάνει τη συλλογή ταυτοτήτων χρηστών (user IDs). Για την αποφυγή οποιωνδήποτε αμφιβολιών, αυτή η προσφορά Υπηρεσίας Cloud δεν περιλαμβάνει το δικαίωμα χρήσης της Οθόνης Εκκίνησης Trusteer (Trusteer Splash) ή/και προώθησης του Λογισμικού Πελάτη για Κάτοχο Λογαριασμού με οποιονδήποτε άλλο τρόπο στην κοινότητα των Δικαιούμενων Συμμετεχόντων του Πελάτη.

3.6.3 IBM Trusteer Pinpoint Malware Detection Redeployment

Οι Πελάτες που προβαίνουν στην εκ νέου υλοποίηση (redeployment) των Εφαρμογών online τραπεζικών συναλλαγών τους κατά τη διάρκεια της περιόδου ισχύος της υπηρεσίας και στη συνέχεια απαιτούν την πραγματοποίηση αλλαγών στην εν λόγω νέα υλοποίηση του IBM Trusteer Pinpoint Malware Detection ή/και του IBM Trusteer Pinpoint Malware Detection II, θα πρέπει να αγοράσουν το IBM Trusteer Pinpoint Malware Detection Redeployment.

Η εκ νέου υλοποίηση μπορεί να είναι απαραίτητη επειδή ο Πελάτης άλλαξε τον τομέα (domain) ή τη διεύθυνση URL της Εφαρμογής, μετέτρεψε την online Εφαρμογή σε κάποια νέα τεχνολογία, μετέφερε την Εφαρμογή σε μια νέα πλατφόρμα online τραπεζικών συναλλαγών ή πρόσθεσε μια νέα ροή σύνδεσης χρηστών στην Εφαρμογή.

Κατά τη διάρκεια της περιόδου μετάβασης 6 μηνών για την εκ νέου υλοποίηση, ο Πελάτης δικαιούται την εκτέλεση πρόσθετων Εφαρμογών, σε μια σχέση μία προς μία, επιπλέον των Εφαρμογών για τις οποίες έχει προμηθευτεί συνδρομή.

3.6.4 IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail ή/και IBM Trusteer Pinpoint Malware Detection Additional Applications for Business

Για το IBM Trusteer Pinpoint Malware Detection Standard Edition II for Business ή το IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Business, προϋπόθεση για την υλοποίηση σε οποιαδήποτε πρόσθετη Επιχειρηματική Εφαρμογή επιπλέον της πρώτης Εφαρμογής είναι η απόκτηση δικαιώματος χρήσης του IBM Trusteer Pinpoint Malware Detection Additional Applications for Business. Για το IBM Trusteer Pinpoint Malware Detection Standard Edition II for Retail ή το IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail, προϋπόθεση για την υλοποίηση σε οποιαδήποτε πρόσθετη Εφαρμογή Λιανικής επιπλέον της πρώτης Εφαρμογής είναι η απόκτηση δικαιώματος χρήσης του IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail.

3.7 Προαιρετικές Πρόσθετες Υπηρεσίες Cloud για το IBM Trusteer Pinpoint Criminal Detection for Business ή/και το IBM Trusteer Pinpoint Criminal Detection for Retail ή/και το IBM Trusteer Pinpoint Criminal Detection II for Business ή/και το IBM Trusteer Pinpoint Criminal Detection II for Retail

3.7.1 IBM Trusteer Pinpoint Criminal Detection Redeployment

Οι Πελάτες που προβαίνουν στην εκ νέου υλοποίηση (redeployment) των Εφαρμογών online τραπεζικών συναλλαγών τους κατά τη διάρκεια της περιόδου ισχύος της υπηρεσίας και στη συνέχεια απαιτούν την πραγματοποίηση αλλαγών στην εν λόγω νέα υλοποίηση της Υπηρεσίας Cloud για το IBM Trusteer Pinpoint Criminal Detection, θα πρέπει να αγοράσουν το IBM Trusteer Pinpoint Criminal Detection Redeployment.

Η εκ νέου υλοποίηση μπορεί να είναι απαραίτητη επειδή ο Πελάτης άλλαξε τον τομέα (domain) ή τη διεύθυνση URL της Εφαρμογής, μετέτρεψε την online Εφαρμογή σε κάποια νέα τεχνολογία, μετέφερε την Εφαρμογή σε μια νέα πλατφόρμα online τραπεζικών συναλλαγών ή πρόσθεσε μια νέα ροή σύνδεσης χρηστών στην Εφαρμογή.

Κατά τη διάρκεια της περιόδου μετάβασης 6 μηνών για την εκ νέου υλοποίηση, ο Πελάτης δικαιούται την εκτέλεση πρόσθετων Εφαρμογών, σε μια σχέση μία προς μία, επιπλέον των Εφαρμογών για τις οποίες έχει προμηθευτεί συνδρομή.

3.7.2 IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business ή/και IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail

Για το IBM Trusteer Pinpoint Criminal Detection II for Business, προϋπόθεση για την υλοποίηση σε οποιαδήποτε πρόσθετη Επιχειρηματική Εφαρμογή επιπλέον της πρώτης Εφαρμογής είναι η απόκτηση δικαιώματος χρήσης του IBM Trusteer Pinpoint Criminal Detection Additional Applications for Business. Για το IBM Trusteer Pinpoint Criminal Detection II for Retail, προϋπόθεση για την υλοποίηση σε οποιαδήποτε πρόσθετη Εφαρμογή Λιανικής επιπλέον της πρώτης Εφαρμογής είναι η απόκτηση δικαιώματος χρήσης του IBM Trusteer Pinpoint Criminal Detection Additional Applications for Retail.

4. IBM Trusteer Fraud Protection Suite

Το IBM Trusteer Fraud Protection Suite ("Πακέτο") είναι μια συλλογή βασιζόμενων στο cloud υπηρεσιών που έχουν σχεδιαστεί για την παροχή ενός πρόσθετου επιπέδου προστασίας από απάτες. Οι υπηρεσίες του Πακέτου μπορούν να ενοποιηθούν με πρόσθετα προϊόντα IBM για την παροχή μιας λύσης διαχείρισης κύκλου ζωής. Το Πακέτο περιλαμβάνει τις ακόλουθες βασιζόμενες στο cloud υπηρεσίες:

- Το IBM Trusteer Pinpoint Detect που στοχεύει στον εντοπισμό και την αποτροπή επιθέσεων επιβλαβούς κώδικα, phishing και οικειοποίησης λογαριασμών (account takeover). Το Trusteer Pinpoint Detect μπορεί να ενσωματωθεί στις Επιχειρηματικές Εφαρμογές ή/και Εφαρμογές Λιανικής του Πελάτη για τις οποίες ο Πελάτης έχει προμηθευτεί συνδρομή για την κάλυψή τους από την Υπηρεσία Cloud και τις διαδικασίες καταπολέμησης απάτης.
- Το IBM Trusteer Rapport for Mitigation που στοχεύει στην αποκατάσταση και την προστασία των μολυσμένων τελικών στοιχείων.

Οι Υπηρεσίες Cloud περιλαμβάνουν:

α. TMA:

Το TMA διατίθεται στο φιλοξενούμενο στο cloud περιβάλλον του IBM Trusteer, μέσω του οποίου ο Πελάτης (και απεριόριστος αριθμός μελών του εξουσιοδοτημένου προσωπικού του) μπορούν: (i) να λαμβάνουν αναφορές δεδομένων περιστατικών και εκτιμήσεις κινδύνων, και (ii) να εξετάζουν, να παραμετροποιούν και να ορίζουν πολιτικές ασφάλειας και πολιτικές αναφορικά με τη δημιουργία αναφορών δεδομένων περιστατικών.

β. Δεδομένα Περιστατικών:

Ο Πελάτης (και απεριόριστος αριθμός μελών του εξουσιοδοτημένου προσωπικού του) μπορούν να χρησιμοποιούν το TMA για τη λήψη δεδομένων περιστατικών που προκύπτουν από online συναλλαγές Δικαιούμενων Συμμετεχόντων με την (τις) Επιχειρηματική(-ές) Εφαρμογή(-ές) ή Εφαρμογή(-ές) Λιανικής του Πελάτη για την (τις) οποία(-ες) ο Πελάτης έχει προμηθευτεί συνδρομή για την κάλυψή της (τους) από τις Υπηρεσίες Cloud. Εναλλακτικά, ο Πελάτης μπορεί να λαμβάνει τα δεδομένα περιστατικών μέσω ενός API παρασκηνιακής παράδοσης.

γ. Web Script ή/και APIs:

Για υλοποίηση σε έναν ιστότοπο για τους σκοπούς της πρόσβασης ή χρήσης της Υπηρεσίας Cloud.

Βέλτιστες πρακτικές Pinpoint

Σε περίπτωση που εντοπιστεί επιβλαβής κώδικας ή εντοπιστούν απόπειρες οικειοποίησης λογαριασμού (account takeover), ο Πελάτης πρέπει να ακολουθεί τις οδηγίες που παρέχονται στο εγχειρίδιο Pinpoint Best Practices Guide. Μη χρησιμοποιείτε τις Υπηρεσίες Cloud για το IBM Trusteer Pinpoint Detect με οποιονδήποτε τρόπο ο οποίος επηρεάζει τη γενική εμπειρία του Δικαιούμενου Συμμετέχοντος αμέσως μετά τον εντοπισμό επιβλαβούς κώδικα ή απόπειρας οικειοποίησης λογαριασμού (account takeover), παρέχοντας έτσι σε άλλους τη δυνατότητα να συσχετίσουν τις ενέργειες του Πελάτη με την εκ μέρους του χρήση προσφορών IBM Trusteer Pinpoint Detect (π.χ. αποστολή ειδοποιήσεων ή μηνυμάτων, φραγή συσκευών, φραγή της πρόσβασης στην Επιχειρηματική Εφαρμογή ή/και στην Εφαρμογή Λιανικής αμέσως μετά τον εντοπισμό επιβλαβούς κώδικα ή απόπειρας οικειοποίησης λογαριασμού).

4.1 IBM Trusteer Pinpoint Detect Standard for Business ή/και IBM Trusteer Pinpoint Detect Standard for Retail

Αυτή η Υπηρεσία Cloud συνδυάζει τα προϊόντα IBM Trusteer Pinpoint Criminal Detection και IBM Security Trusteer Pinpoint Malware Detection σε μία ενοποιημένη λύση.

Η λύση υποστηρίζει τον εντοπισμό, χωρίς τη χρήση λογισμικού πελάτη, επιβλαβούς κώδικα ή/και ύποπτων δραστηριοτήτων οικειοποίησης λογαριασμών από προγράμματα πλοήγησης που συνδέονται σε μια Επιχειρηματική Εφαρμογή ή Εφαρμογή Λιανικής, χρησιμοποιώντας την ταυτότητα συσκευής (device ID), τεχνικές εντοπισμού phishing και τεχνικές εντοπισμού κλοπής στοιχείων ταυτότητας μέσω επιβλαβούς κώδικα. Οι προσφορές IBM Trusteer Pinpoint παρέχουν ένα πρόσθετο επίπεδο προστασίας και στοχεύουν στον εντοπισμό προσπαθειών οικειοποίησης λογαριασμών (account takeover) και στην παράδοση, απευθείας στον Πελάτη, βαθμολογικών στοιχείων εκτίμησης κινδύνων για τα προγράμματα πλοήγησης ή τις φορητές συσκευές (με χρήση του τοπικού προγράμματος πλοήγησης ή της εφαρμογής του πελάτη για φορητές συσκευές) που αποκτούν πρόσβαση σε μια Επιχειρηματική Εφαρμογή ή Εφαρμογή Λιανικής.

Αυτή η Υπηρεσία Cloud περιλαμβάνει την παροχή υποστήριξης επιπέδου Standard (όπως ορίζεται στο άρθρο "Τεχνική Υποστήριξη" παρακάτω). Για την παροχή υποστήριξης επιπέδου Premium, ο Πελάτης πρέπει να προμηθευτεί το Detect Premium.

Αυτή η Υπηρεσία Cloud παρέχει προστασία για μία Εφαρμογή. Για κάθε πρόσθετη Εφαρμογή, ο Πελάτης πρέπει να αποκτήσει δικαίωμα χρήσης του IBM Trusteer Pinpoint Detect Standard Additional Applications.

4.2 IBM Trusteer Pinpoint Detect Premium for Business ή/και IBM Trusteer Pinpoint Detect Premium for Retail

Αυτή η Υπηρεσία Cloud συνδυάζει τα προϊόντα IBM Trusteer Pinpoint Criminal Detection και IBM Trusteer Pinpoint Malware Detection σε μία ενοποιημένη λύση που μπορεί να ενσωματωθεί εύκολα στο περιβάλλον σας.

Η λύση υποστηρίζει τον εντοπισμό, χωρίς τη χρήση λογισμικού πελάτη, επιβλαβούς κώδικα ή/και ύποπτων δραστηριοτήτων οικειοποίησης λογαριασμών από προγράμματα πλοήγησης που συνδέονται σε μια Επιχειρηματική Εφαρμογή ή Εφαρμογή Λιανικής, χρησιμοποιώντας την ταυτότητα συσκευής (device ID), τεχνικές εντοπισμού phishing και τεχνικές εντοπισμού κλοπής στοιχείων ταυτότητας μέσω επιβλαβούς κώδικα. Οι προσφορές IBM Trusteer Pinpoint παρέχουν ένα πρόσθετο επίπεδο προστασίας και στοχεύουν στον εντοπισμό προσπαθειών οικειοποίησης λογαριασμών (account takeover) και στην παράδοση, απευθείας στον Πελάτη, βαθμολογικών στοιχείων εκτίμησης κινδύνων για τα προγράμματα πλοήγησης ή τις φορητές συσκευές (με χρήση του τοπικού προγράμματος πλοήγησης ή της εφαρμογής του πελάτη για φορητές συσκευές) που αποκτούν πρόσβαση σε μια Επιχειρηματική Εφαρμογή ή Εφαρμογή Λιανικής.

Η υπηρεσία περιλαμβάνει βελτιωμένες λειτουργίες και υπηρεσίες, συμπεριλαμβανομένων διευρυμένων υπηρεσιών υλοποίησης και προετοιμασίας, προσαρμοσμένες πολιτικές ασφάλειας, υπηρεσίες διερεύνησης και άλλες υπηρεσίες.

Αυτή η Υπηρεσία Cloud παρέχει προστασία για μία Εφαρμογή. Για κάθε πρόσθετη Εφαρμογή, ο Πελάτης πρέπει να αποκτήσει δικαίωμα χρήσης του IBM Trusteer Pinpoint Detect Premium Additional Applications.

Αυτή η Υπηρεσία Cloud περιλαμβάνει την παροχή υποστήριξης επιπέδου Premium.

Pinpoint Detect Policy Manager:

Το Policy Manager περιλαμβάνεται στην υπηρεσία Pinpoint Detect Premium και καθίσταται διαθέσιμο στο φιλοξενούμενο στο cloud περιβάλλον του IBM Trusteer, μέσω του οποίου ο Πελάτης (και απεριόριστος αριθμός μελών του εξουσιοδοτημένου προσωπικού του) μπορούν: (i) να σχεδιάζουν, να δοκιμάζουν και να εφαρμόζουν στο περιβάλλον παραγωγής τη λογική για τον εντοπισμό δραστηριοτήτων απάτης, (ii) να σχεδιάζουν αναφορές και χειριστήρια (dashboards), και (iii) να εξετάζουν, να παραμετροποιούν και να ορίζουν πολιτικές ασφάλειας και πολιτικές για τον εντοπισμό ύποπτων δραστηριοτήτων στις Εφαρμογές του Πελάτη.

Απαιτούνται συμβουλευτικές υπηρεσίες για την ενεργοποίηση της λειτουργίας Policy Manager και για επιπλέον υποστήριξη που απαιτεί εις βάθος ανάλυση. Οι συμβουλευτικές υπηρεσίες θα περιγράφονται χωριστά σε μια Περιγραφή Έργου.

Μετά την ενεργοποίηση του Policy Manager, η IBM διατηρεί το δικαίωμα να αποκτά πρόσβαση στο περιβάλλον του Πελάτη προκειμένου να υποστηρίζει τον Πελάτη στην αναπροσαρμογή των πολιτικών του Πελάτη για την επίλυση σοβαρών ζητημάτων που απορρέουν από αλλαγές πολιτικής.

Ο Πελάτης δεσμεύεται ότι θα μεριμνά για την προστασία δεδομένων που εκτίθενται μέσω του Policy Manager από αθέμιτη χρήση.

Αφού ενεργοποιηθεί η λειτουργία Policy Manager, ο Πελάτης πρέπει να ακολουθεί τις κατευθυντήριες γραμμές της IBM για τον ορισμό κανόνων, όπως αυτές περιγράφονται στη σχετική τεκμηρίωση. Ο Πελάτης αποδέχεται ότι η IBM δεν φέρει ευθύνη για οποιεσδήποτε επιπτώσεις της μη συμμόρφωσης του Πελάτη με τις εν λόγω συστάσεις.

Τυχόν ζητήματα σταθερότητας ή/και υποβάθμισης υπηρεσιών τα οποία μπορεί να απορρέουν από την ακατάλληλη παραμετροποίηση της λειτουργίας Policy Manager από τον Πελάτη δεν θα θεωρούνται Χρόνος Διακοπής Λειτουργίας κατά τους υπολογισμούς αναφορικά με την επίτευξη των στόχων των αντίστοιχων συμβάσεων SLA.

4.3 IBM Trusteer Pinpoint Detect Standard with access management integration for Business ή/και IBM Trusteer Pinpoint Detect Standard with access management integration for Retail

Η Υπηρεσία Cloud για το IBM Trusteer Pinpoint Detect Standard with access management integration περιλαμβάνει τις λειτουργίες του IBM Security Pinpoint Detect Standard που περιγράφονται στο ανωτέρω άρθρο 4.1.

Το IBM Trusteer Pinpoint Detect Standard with access management integration χρησιμοποιείται όταν αγοραστεί με ένα σύστημα διαχείρισης πρόσβασης όπως π.χ. το IBM Security Access Management ("ISAM"). Όταν αγοραστεί με το ISAM θα πρέπει να ενεργοποιηθούν και οι δύο προσφορές. Αυτή η προσφορά περιλαμβάνει την επιλογή ενοποίησης με το σύστημα διαχείρισης πρόσβασης. Δεν περιλαμβάνει το δικαίωμα χρήσης του συστήματος διαχείρισης πρόσβασης.

Αυτή η προσφορά παρέχει προστασία για μία Εφαρμογή. Για κάθε πρόσθετη Εφαρμογή, ο Πελάτης πρέπει να αποκτήσει δικαίωμα χρήσης του IBM Trusteer Pinpoint Detect Standard Additional Applications.

Αυτή η Υπηρεσία Cloud περιλαμβάνει την παροχή υποστήριξης επιπέδου Standard (όπως ορίζεται στο άρθρο "Τεχνική Υποστήριξη"). IBM Trusteer Pinpoint Detect Premium with access management integration for Business ή/και IBM Trusteer Pinpoint Detect Premium with access management integration for Retail

Η Υπηρεσία Cloud για το IBM Trusteer Pinpoint Detect Premium with access management integration περιλαμβάνει τις λειτουργίες του IBM Security Pinpoint Detect Premium που περιγράφονται στο ανωτέρω άρθρο 4.2, καθώς και την επιλογή ενοποίησης με το σύστημα διαχείρισης πρόσβασης (access management system).

Το IBM Trusteer Pinpoint Detect Premium with access management integration χρησιμοποιείται όταν αγοραστεί με ένα σύστημα διαχείρισης πρόσβασης όπως π.χ. το IBM Security Access Management ("ISAM"). Όταν αγοραστεί με το ISAM θα πρέπει να ενεργοποιηθούν και οι δύο προσφορές. Αυτή η Υπηρεσία Cloud περιλαμβάνει την επιλογή ενοποίησης με το σύστημα διαχείρισης πρόσβασης. Δεν περιλαμβάνει το δικαίωμα χρήσης του συστήματος διαχείρισης πρόσβασης.

Αυτή η Υπηρεσία Cloud παρέχει προστασία για μία Εφαρμογή. Για κάθε πρόσθετη Εφαρμογή, ο Πελάτης πρέπει να αποκτήσει δικαίωμα χρήσης του IBM Trusteer Pinpoint Detect Premium Additional Applications.

Αυτή η προσφορά περιλαμβάνει την παροχή υποστήριξης επιπέδου Premium.

4.4 Προαιρετικές υπηρεσίες για το IBM Trusteer Pinpoint Detect Standard ή/και το IBM Trusteer Pinpoint Detect Premium

Για τις Υπηρεσίες Cloud σε αυτό το άρθρο, απαιτείται η απόκτηση δικαιώματος χρήσης του IBM Trusteer Pinpoint Detect Premium for Retail ή του IBM Trusteer Pinpoint Detect Standard for Retail.

4.5 IBM Trusteer Rapport for Mitigation for Retail ή/και IBM Trusteer Rapport for Mitigation for Business

Το IBM Trusteer Rapport for Mitigation στοχεύει στη διερεύνηση, αντιμετώπιση, αποτροπή και αφαίρεση μολύνσεων από επιβλαβή κώδικα από μολυσμένες συσκευές (PC/MAC) Δικαιούμενων Συμμετεχόντων του Πελάτη που αποκτούν πρόσβαση στην Εφαρμογή Λιανικής του Πελάτη σε περιστασιακή βάση,

εφόσον έχουν εντοπιστεί τέτοιες μολύνσεις από επιβλαβή κώδικα στα δεδομένα περιστατικών του IBM Trusteer Pinpoint Detect Premium ή του IBM Trusteer Pinpoint Detect Standard. Ο Πελάτης πρέπει να διαθέτει μια ισχύουσα συνδρομή για το IBM Trusteer Pinpoint Detect Premium ή το IBM Trusteer Pinpoint Detect Standard που εκτελείται στην Εφαρμογή Λιανικής του Πελάτη. Ο Πελάτης επιτρέπεται να χρησιμοποιεί αυτή την Υπηρεσία Cloud μόνο σε συνάρτηση με Δικαιούμενους Συμμετέχοντες που αποκτούν πρόσβαση στην Εφαρμογή Λιανικής του Πελάτη, και αποκλειστικά ως εργαλείο που στοχεύει στη διερεύνηση και αντιμετώπιση μιας συγκεκριμένης μολυσμένης συσκευής (PC/MAC) σε περιστασιακή βάση. Το IBM Trusteer Rapport for Mitigation for Retail πρέπει να εκτελείται πράγματι στην εν λόγω συσκευή (PC/MAC) του Δικαιούμενου Συμμετέχοντος και ο εν λόγω Δικαιούμενος Συμμετέχων πρέπει να αποδεχθεί τη Σύμβαση EULA, να ταυτοποιηθεί τουλάχιστον μία φορά στην Εφαρμογή Λιανικής του Πελάτη, ενώ η παραμετροποίηση του Πελάτη πρέπει να περιλαμβάνει τη συλλογή ταυτοτήτων χρηστών (user IDs). Για την αποφυγή οποιωνδήποτε αμφιβολιών, αυτή η Υπηρεσία Cloud δεν περιλαμβάνει το δικαίωμα χρήσης της Οθόνης Εκκίνησης Trusteer (Trusteer Splash) ή/και προώθησης του Λογισμικού Πελάτη για Κάτοχο Λογαριασμού με οποιονδήποτε άλλο τρόπο στην κοινότητα των Δικαιούμενων Συμμετεχόντων του Πελάτη.

4.5.1 IBM Trusteer Pinpoint Detect Standard Additional Applications for Business ή/και IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail ή/και IBM Trusteer Pinpoint Detect Premium Additional Applications for Business ή/και IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail

Για το IBM Trusteer Pinpoint Detect Standard for Business, προϋπόθεση για την υλοποίηση σε οποιαδήποτε πρόσθετη Επιχειρηματική Εφαρμογή επιπλέον της πρώτης Εφαρμογής είναι η απόκτηση δικαιώματος χρήσης του IBM Trusteer Pinpoint Detect Standard Additional Applications for Business.

Για το IBM Trusteer Pinpoint Detect Standard for Retail, προϋπόθεση για την υλοποίηση σε οποιαδήποτε πρόσθετη Εφαρμογή Λιανικής επιπλέον της πρώτης Εφαρμογής είναι η απόκτηση δικαιώματος χρήσης του IBM Trusteer Pinpoint Detect Standard Additional Applications for Retail.

Για το IBM Trusteer Pinpoint Premium for Business, προϋπόθεση για την υλοποίηση σε οποιαδήποτε πρόσθετη Επιχειρηματική Εφαρμογή επιπλέον της πρώτης Εφαρμογής είναι η απόκτηση δικαιώματος χρήσης του IBM Trusteer Pinpoint Detect Premium Additional Applications for Business.

Για το IBM Trusteer Pinpoint Premium for Retail, προϋπόθεση για την υλοποίηση σε οποιαδήποτε πρόσθετη Εφαρμογή Λιανικής επιπλέον της πρώτης Εφαρμογής είναι η απόκτηση δικαιώματος χρήσης του IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail.

4.5.2 IBM Trusteer Pinpoint Detect Standard Redeployment ή/και IBM Trusteer Pinpoint Detect Premium Redeployment

Οι Πελάτες που προβαίνουν στην εκ νέου υλοποίηση (redeployment) των Εφαρμογών online τραπεζικών συναλλαγών τους κατά τη διάρκεια της περιόδου ισχύος της υπηρεσίας και στη συνέχεια απαιτούν την πραγματοποίηση αλλαγών στην εν λόγω νέα υλοποίηση του IBM Trusteer Pinpoint Detect, θα πρέπει να αγοράσουν το IBM Trusteer Pinpoint Detect Redeployment.

Η εκ νέου υλοποίηση μπορεί να είναι απαραίτητη επειδή ο Πελάτης άλλαξε τον τομέα (domain) ή τη διεύθυνση URL της Εφαρμογής, μετέτρεψε την online Εφαρμογή σε κάποια νέα τεχνολογία, μετέφερε την Εφαρμογή σε μια νέα πλατφόρμα online τραπεζικών συναλλαγών ή πρόσθεσε μια νέα ροή σύνδεσης χρηστών στην Εφαρμογή.

Κατά τη διάρκεια της περιόδου μετάβασης 6 μηνών για την εκ νέου υλοποίηση, ο Πελάτης δικαιούται την εκτέλεση πρόσθετων Εφαρμογών, σε μια σχέση μία προς μία, επιπλέον των Εφαρμογών για τις οποίες έχει προμηθευτεί συνδρομή.

5. Υπηρεσίες Cloud για το IBM Trusteer Mobile

5.1 IBM Trusteer Mobile Browser for Business ή/και IBM Trusteer Mobile Browser for Retail

Το IBM Trusteer Mobile Browser έχει σχεδιαστεί για την παροχή ενός πρόσθετου επιπέδου προστασίας που στοχεύει στην παροχή ασφαλούς online πρόσβασης των φορητών συσκευών των Δικαιούμενων Συμμετεχόντων στις Επιχειρηματικές Εφαρμογές ή Εφαρμογές Λιανικής του Πελάτη για τις οποίες ο Πελάτης έχει προμηθευτεί συνδρομή για την κάλυψη των εν λόγω Εφαρμογών από Υπηρεσίες Cloud. Επίσης παρέχουν τη δυνατότητα αποτίμησης κινδύνων για τις φορητές συσκευές του Πελάτη και προστασία από επιθέσεις phishing. Ο εντοπισμός ασφαλών δικτύων Wi-Fi διατίθεται μόνο για πλατφόρμες Android. Για τους σκοπούς της παρούσας Υπηρεσίας Cloud, στις "φορητές συσκευές" περιλαμβάνονται μόνο τα κινητά τηλέφωνα και οι συσκευές tablet, ενώ δεν περιλαμβάνονται οι φορητοί υπολογιστές PC ή Mac.

Μέσω του TMA, ο Πελάτης μπορεί να λαμβάνει δεδομένα περιστατικών, αναλύσεις και στατιστικά στοιχεία αναφορικά με τις Συσκευές των Δικαιούμενων Συμμετεχόντων οι οποίοι: (i) έχουν μεταφορτώσει το Λογισμικό Πελάτη για Κάτοχο Λογαριασμού, μια εφαρμογή που παραχωρείται βάσει μιας σύμβασης άδειας χρήσης τελικού χρήστη ("Σύμβαση EULA"), χωρίς χρέωση, στο κοινό και καθίσταται διαθέσιμη για μεταφόρτωση στις φορητές συσκευές των Δικαιούμενων Συμμετεχόντων, και (ii) έχουν αποδεχθεί τους όρους της Σύμβασης EULA και έχουν ταυτοποιηθεί τουλάχιστον μία φορά στις Επιχειρηματικές Εφαρμογές ή Εφαρμογές Λιανικής για τις οποίες ο Πελάτης έχει προμηθευτεί συνδρομή για την κάλυψη των εν λόγω Εφαρμογών από Υπηρεσίες Cloud. Ο Πελάτης επιτρέπεται να διαθέτει το Λογισμικό Πελάτη για Κάτοχο Λογαριασμού στην αγορά μόνο μέσω της Οθόνης Εκκίνησης Trusteer και δεν επιτρέπεται να χρησιμοποιεί το Λογισμικό Πελάτη για Κάτοχο Λογαριασμού για τις εσωτερικές λειτουργίες της επιχείρησής του.

α. Δεδομένα Περιστατικών:

Ο Πελάτης (και απεριόριστος αριθμός μελών του εξουσιοδοτημένου προσωπικού του) μπορούν να χρησιμοποιούν το TMA για τη λήψη δεδομένων περιστατικών που προκύπτουν από online συναλλαγές φορητών συσκευών με τις Επιχειρηματικές Εφαρμογές ή Εφαρμογές Λιανικής του Πελάτη για τις οποίες ο Πελάτης έχει προμηθευτεί συνδρομή για την κάλυψη των εν λόγω Εφαρμογών από Υπηρεσίες Cloud.

β. Οθόνη Εκκίνησης Trusteer:

Η Οθόνη Εκκίνησης Trusteer (Trusteer Splash) αποτελεί μια πλατφόρμα μάρκετινγκ μέσω της οποίας προωθείται το Λογισμικό Πελάτη για Κάτοχο Λογαριασμού στους Δικαιούμενους Συμμετέχοντες που αποκτούν πρόσβαση στις Επιχειρηματικές Εφαρμογές ή/και στις Εφαρμογές Λιανικής του Πελάτη για τις οποίες ο Πελάτης έχει προμηθευτεί συνδρομή για την κάλυψη των εν λόγω Εφαρμογών από Υπηρεσίες Cloud. Ο Πελάτης μπορεί να επιλέξει κάποιο από τα διαθέσιμα πρότυπα οθονών εκκίνησης ("Splash Templates"). Επίσης μπορεί να συνάψει χωριστή σύμβαση ή περιγραφή έργου για την παροχή ειδικά προσαρμοσμένης οθόνης εκκίνησης.

Ο Πελάτης μπορεί να συμφωνήσει στην παροχή των δικών του εμπορικών σημάτων, λογοτύπων και εικονιδίων για χρήση σε συνάρτηση με το TMA, αποκλειστικά για την εμφάνισή τους στην Οθόνη Εκκίνησης Trusteer, στις οθόνες του Λογισμικού Πελάτη για Κάτοχο Λογαριασμού ή στις σελίδες προσγείωσης που φιλοξενούνται από την IBM ή στον ιστότοπο του IBM Trusteer. Οποιαδήποτε χρήση των παρεχόμενων εμπορικών σημάτων, λογοτύπων ή εικονιδίων θα γίνεται σύμφωνα με τις εύλογες πολιτικές της IBM αναφορικά με τη διαφήμιση και τη χρήση εμπορικών σημάτων.

5.2 IBM Trusteer Mobile SDK for Business ή/και IBM Trusteer Mobile SDK for Retail

Οι Υπηρεσίες Cloud για το IBM Trusteer Mobile SDK έχουν σχεδιαστεί για την παροχή ενός πρόσθετου επιπέδου ασφάλειας που εξασφαλίζει την ασφαλή διαδικτυακή πρόσβαση στις Επιχειρηματικές Εφαρμογές ή/και Εφαρμογές Λιανικής του Πελάτη για τις οποίες ο Πελάτης έχει αποκτήσει συνδρομή για την κάλυψη των εν λόγω Εφαρμογών από Υπηρεσίες Cloud. Επίσης παρέχουν τη δυνατότητα αποτίμησης κινδύνων για τις συσκευές του Πελάτη και προστασία από επιθέσεις pharming. Ο εντοπισμός ασφαλών δικτύων Wi-Fi διατίθεται μόνο για πλατφόρμες Android.

Οι Υπηρεσίες Cloud για το IBM Trusteer Mobile SDK περιλαμβάνουν ένα ιδιόκτητο SDK (software developer's kit - "SDK") για την ανάπτυξη λογισμικού για φορητές συσκευές, ένα πακέτο λογισμικού που περιέχει τεκμηρίωση, ιδιόκτητες βιβλιοθήκες λογισμικού προγραμματισμού και άλλα σχετικά αρχεία και στοιχεία, επίσης γνωστό ως "IBM Trusteer mobile library" (Βιβλιοθήκη του IBM Trusteer για φορητές συσκευές) ή ως "Run-time Component" (Λειτουργικό Τμήμα Περιβάλλοντος Εκτέλεσης) ή "Redistributable" (Αναδιανεμητέος Κώδικας), μια ιδιόκτητη ενότητα κώδικα που δημιουργήθηκε με το IBM Trusteer Mobile SDK και μπορεί να ενσωματωθεί και να ενοποιηθεί με μεμονωμένες προστατευόμενες εφαρμογές του Πελάτη για φορητές συσκευές iOS ή Android για τις οποίες ο Πελάτης έχει προμηθευτεί συνδρομή για την κάλυψη των εν λόγω Εφαρμογών από Υπηρεσίες Cloud ("Ενιαία Εφαρμογή του Πελάτη για Φορητές Συσκευές").

Το IBM Trusteer Mobile SDK for Retail διατίθεται σε πακέτα των 100 Δικαιούμενων Συμμετεχόντων ή σε πακέτα των 100 Συσκευών Πελάτη, ενώ το IBM Trusteer Mobile SDK for Business διατίθεται σε πακέτα των 10 Δικαιούμενων Συμμετεχόντων ή σε πακέτα των 10 Συσκευών Πελάτη.

Μέσω του TMA, ο Πελάτης (και ένας απεριόριστος αριθμός εξουσιοδοτημένων μελών του προσωπικού του) μπορεί να λαμβάνει αναφορές δεδομένων συμβάντων και εκτιμήσεις τάσεων κινδύνων. Μέσω της Ενιαίας Εφαρμογής του Πελάτη για Φορητές Συσκευές, ο Πελάτης μπορεί να λαμβάνει δεδομένα ανάλυσης κινδύνων και πληροφορίες για φορητές συσκευές των Δικαιούμενων Συμμετεχόντων που έχουν

μεταφορτώσει (downloaded) την Ενιαία Εφαρμογή του Πελάτη για Φορητές Συσκευές, επιτρέποντας έτσι στον Πελάτη να καταρτίσει μια πολιτική καταπολέμησης απάτης που επιβάλλει τη λήψη μέτρων για την αντιμετώπιση των εν λόγω κινδύνων. Για τους σκοπούς αυτής της προσφοράς, στις "φορητές συσκευές" περιλαμβάνονται μόνο υποστηριζόμενα κινητά τηλέφωνα και συσκευές tablet, και όχι υπολογιστές PC ή MAC.

Ο Πελάτης μπορεί να προβαίνει στις εξής ενέργειες:

α. Εσωτερική χρήση του IBM Trusteer Mobile SDK αποκλειστικά για το σκοπό της ανάπτυξης της Ενιαίας Εφαρμογής του Πελάτη για Φορητές Συσκευές.

β. Ενσωμάτωση του Αναδιανεμητέου Κώδικα (αποκλειστικά σε μορφή κώδικα αντικειμένου) ως αναπόσπαστου, δομικού στοιχείου στην Ενιαία Εφαρμογή του Πελάτη για Φορητές Συσκευές. Οποιοδήποτε τροποποιημένο ή συγχωνευμένο τμήμα του Αναδιανεμητέου Κώδικα που υπόκειται σε αυτή τη χορήγηση άδειας χρήσης θα διέπεται από τους όρους της παρούσας Περιγραφής Υπηρεσιών, και

γ. Προώθηση και διανομή του Αναδιανεμητέου Κώδικα για μεταφόρτωση σε φορητές συσκευές Δικαιούμενων Συμμετεχόντων ή σε Συσκευές Πελάτη, υπό την προϋπόθεση ότι:

- Εκτός εάν επιτρέπεται ρητώς στην παρούσα Σύμβαση, ο Πελάτης δεν επιτρέπεται να προβαίνει (1) στη χρήση, αντιγραφή, τροποποίηση ή διανομή του SDK, (2) στην αντίστροφη συμβολομετάφραση (reverse assemble), αντίστροφη μεταγλώττιση (reverse compile) ή κατά άλλον τρόπο μετάφραση ή αποσυμπίληση (reverse engineer) του SDK, παρά μόνο στο βαθμό που επιτρέπεται ρητώς από το νόμο χωρίς τη δυνατότητα συμβατικής παραίτησης από αυτό το δικαίωμα, (3) στην ενοικίαση ή εκμίσθωση του SDK ή στην παραχώρηση περαιτέρω αδειών χρήσης (sublicense) του SDK, (4) στην αφαίρεση αρχείων πνευματικών δικαιωμάτων ή ειδοποιήσεων που περιέχονται στον Αναδιανεμητέο Κώδικα, (5) στη χρήση του ίδιου ονόματος διαδρομής (path name) με τα πρωτότυπα αρχεία/ενότητες του Αναδιανεμητέου Κώδικα, και (6) στη χρήση επωνυμιών και εμπορικών σημάτων της IBM, των χορηγούντων τις άδειες χρήσης της ή των διανομέων της σε συνάρτηση με την προώθηση της Ενιαίας Εφαρμογής του Πελάτη για Φορητές Συσκευές χωρίς την προηγούμενη έγγραφη συναίνεση της IBM ή του εν λόγω διανομέα ή χορηγούντος άδειες χρήσης.
- Ο Αναδιανεμητέος Κώδικας πρέπει να παραμείνει ενσωματωμένος ως αναπόσπαστο στοιχείο στην Ενιαία Εφαρμογή του Πελάτη για Φορητές Συσκευές. Ο Αναδιανεμητέος Κώδικας πρέπει να βρίσκεται σε μορφή κώδικα αντικειμένου (object code) μόνο και να συμμορφώνεται με όλες τις κατευθυντήριες γραμμές, οδηγίες και προδιαγραφές που παρέχονται στο SDK και στην αντίστοιχη τεκμηρίωση. Στη σύμβαση άδειας χρήσης με τον τελικό χρήστη της Ενιαίας Εφαρμογής του Πελάτη για Φορητές Συσκευές, ο τελικός χρήστης πρέπει να ειδοποιείται ότι ο Διανεμητέος Κώδικας δεν επιτρέπεται i) να χρησιμοποιείται για οποιονδήποτε άλλο σκοπό παρά μόνο για να καθιστά δυνατή τη χρήση της Ενιαίας Εφαρμογής του Πελάτη για Φορητές Συσκευές, ii) να αντιγράφεται (παρά μόνο για λόγους εφεδρικής αποθήκευσης), iii) να διανέμεται ή να διαβιβάζεται περαιτέρω, ή iv) να υφίσταται αντίστροφη συμβολομετάφραση (reverse assembly), αντίστροφη μεταγλώττιση (reverse compilation) ή άλλου είδους μετάφραση, παρά μόνο στο βαθμό που επιτρέπεται ρητώς εκ του νόμου χωρίς δυνατότητα συμβατικής παραίτησης από αυτό το δικαίωμα. Η σύμβαση άδειας χρήσης του Πελάτη πρέπει να παρέχει τουλάχιστον ισοδύναμη προστασία των δικαιωμάτων της IBM με αυτή που παρέχεται από τους όρους της παρούσας Σύμβασης.
- Το SDK επιτρέπεται να εγκατασταθεί μόνο ως τμήμα του περιβάλλοντος εσωτερικής ανάπτυξης και διενέργειας δοκιμών σε επίπεδο μονάδας (unit testing) του Πελάτη στις καθορισμένες φορητές συσκευές διενέργειας δοκιμών του Πελάτη. Ο Πελάτης δεν είναι εξουσιοδοτημένος να χρησιμοποιεί το SDK για την επεξεργασία φορτίων εργασίας του περιβάλλοντος παραγωγής, την προσομοίωση φορτίων εργασίας του περιβάλλοντος παραγωγής ή τη δοκιμή της επεκτασιμότητας (scalability) οποιουδήποτε κώδικα, εφαρμογής ή συστήματος. Ο Πελάτης δεν είναι εξουσιοδοτημένος να χρησιμοποιεί οποιοδήποτε τμήμα του SDK για οποιονδήποτε άλλο σκοπό.

Ο Πελάτης είναι αποκλειστικά υπεύθυνος για την ανάπτυξη, δοκιμή και υποστήριξη της Ενιαίας Εφαρμογής του Πελάτη για Φορητές Συσκευές. Ο Πελάτης είναι υπεύθυνος για την παροχή οποιασδήποτε τεχνικής υποστήριξης για την Ενιαία Εφαρμογή του Πελάτη για Φορητές Συσκευές, καθώς και για οποιεσδήποτε τροποποιήσεις στον Αναδιανεμητέο Κώδικα που πραγματοποιήθηκαν από τον Πελάτη, όπως προβλέπεται στο παρόν έγγραφο.

Ο Πελάτης είναι εξουσιοδοτημένος να εγκαθιστά και να χρησιμοποιεί το Αναδιανεμητέο Κώδικα και το IBM Security Mobile SDK αποκλειστικά για την υποστήριξη της εκ μέρους του χρήσης των Υπηρεσιών Cloud.

Η IBM έχει διενεργήσει δοκιμές με δείγματα εφαρμογών χρησιμοποιώντας τα εργαλεία για φορητές συσκευές που παρέχονται στο IBM Trusteer Mobile SDK ("Εργαλεία για Φορητές Συσκευές" (Mobile Tools)) προκειμένου να προσδιοριστεί αν οι εν λόγω εφαρμογές εκτελούνται σωστά σε ορισμένες εκδοχές πλατφορμών λειτουργικών συστημάτων για φορητές συσκευές της Apple (iOS), της Google (Android) και άλλων (από κοινού "Πλατφόρμες Λειτουργικών Συστημάτων για Φορητές Συσκευές" (Mobile OS Platforms)). Όμως, οι Πλατφόρμες Λειτουργικών Συστημάτων για Φορητές Συσκευές παρέχονται από τρίτους, δεν βρίσκονται υπό τον έλεγχο της IBM και υπόκεινται σε αλλαγή χωρίς ειδοποίηση προς την IBM. Για το λόγο αυτό και παρά τα όσα προβλέπονται περί του αντιθέτου, η IBM δεν εγγυάται ότι οποιεσδήποτε εφαρμογές ή άλλα αποτελέσματα που δημιουργούνται με χρήση των Εργαλείων για Φορητές Συσκευές θα εκτελούνται σωστά, θα συνεργάζονται ή θα είναι συμβατά με οποιεσδήποτε Πλατφόρμες Λειτουργικών Συστημάτων για Φορητές Συσκευές ή με οποιεσδήποτε φορητές συσκευές.

Λειτουργικά Τμήματα Πηγαίου Κώδικα και Υλικά Δειγμάτων - Το IBM Trusteer Mobile SDK μπορεί να περιλαμβάνει ορισμένα λειτουργικά τμήματα σε μορφή πηγαίου κώδικα ("Λειτουργικά Τμήματα Πηγαίου Κώδικα") και άλλα υλικά που προσδιορίζονται ως Υλικά Δειγμάτων. Ο Πελάτης επιτρέπεται να αντιγράψει και να τροποποιήσει Λειτουργικά Τμήματα Πηγαίου Κώδικα και Υλικά Δειγμάτων μόνο για σκοπούς εσωτερικής χρήσης, υπό την προϋπόθεση ότι η εν λόγω χρήση γίνεται εντός των ορίων των δικαιωμάτων χρήσης που χορηγούνται βάσει της παρούσας Σύμβασης, και υπό την προϋπόθεση ότι ο Πελάτης δεν προβαίνει στην τροποποίηση ή διαγραφή οποιωνδήποτε πληροφοριών ή ειδοποιήσεων περί πνευματικών δικαιωμάτων που περιέχονται στα Λειτουργικά Τμήματα Πηγαίου Κώδικα και στα Υλικά Δειγμάτων. Η IBM παρέχει τα Λειτουργικά Τμήματα Πηγαίου Κώδικα και τα Υλικά Δειγμάτων χωρίς υποχρέωση υποστήριξης και "ΩΣ ΕΧΟΥΝ", ΧΩΡΙΣ ΚΑΝΕΝΟΣ ΕΙΔΟΥΣ ΕΓΓΥΗΣΗ, ΡΗΤΗ Ή ΣΙΩΠΗΡΗ, ΣΥΜΠΕΡΙΛΑΜΒΑΝΟΜΕΝΗΣ ΤΗΣ ΕΓΓΥΗΣΗΣ ΤΙΤΛΟΥ ΚΥΡΙΟΤΗΤΑΣ, ΜΗ ΠΑΡΑΒΙΑΣΗΣ ΔΙΚΑΙΩΜΑΤΩΝ Ή ΥΠΑΡΞΗΣ ΑΞΙΩΣΕΩΝ ΤΡΙΤΩΝ ΚΑΙ ΤΩΝ ΣΙΩΠΗΡΩΝ ΕΓΓΥΗΣΕΩΝ ΚΑΙ ΠΡΟΫΠΟΘΕΣΕΩΝ ΕΜΠΟΡΕΥΣΙΜΟΤΗΤΑΣ ΚΑΙ ΚΑΤΑΛΛΗΛΟΤΗΤΑΣ ΓΙΑ ΣΥΓΚΕΚΡΙΜΕΝΟ ΣΚΟΠΟ. Σημειώνεται ότι τα Λειτουργικά Τμήματα Πηγαίου Κώδικα ή τα Υλικά Δειγμάτων παρέχονται μόνο ώστε να χρησιμοποιούνται ως παραδείγματα υλοποίησης των εν λόγω στοιχείων στο CIMA. Τα Λειτουργικά Τμήματα Πηγαίου Κώδικα ή τα Υλικά Δειγμάτων ενδέχεται να μην είναι συμβατά με το περιβάλλον ανάπτυξης λογισμικού του Πελάτη και ο Πελάτης είναι αποκλειστικά υπεύθυνος για τη δοκιμή και την υλοποίηση των εν λόγω στοιχείων στο CIMA του.

Ο Πελάτης συμφωνεί να δημιουργεί, να τηρεί και να παρέχει στην IBM και τους ελεγκτές της ακριβή έγγραφα στοιχεία, αποτελέσματα εργαλείων του συστήματος και άλλα δεδομένα του συστήματος τα οποία επαρκούν προκείμενου να παράσχουν επαλήθευση, η οποία θα υπόκειται σε έλεγχο, ότι η χρήση του IBM Trusteer Mobile SDK από τον Πελάτη συμμορφώνεται με την παρούσα Περιγραφή Υπηρεσιών.

6. Υποστήριξη επιπέδου Premium (Premium Support)

Ο Πελάτης δικαιούται να λαμβάνει Υποστήριξη επιπέδου Premium μόνο για τις Υπηρεσίες Cloud για τις οποίες ο Πελάτης έχει προμηθευτεί συνδρομή για την αντίστοιχη προσφορά Premium Support.

7. Υλοποίηση του IBM Trusteer Fraud Protection

Για κάθε Εφαρμογή για την οποία ο Πελάτης προμηθεύεται συνδρομή, η βασική συνδρομή του Πελάτη περιλαμβάνει τις απαιτούμενες δραστηριότητες ετοιμασίας (setup) και αρχικής εγκατάστασης στο IBM Trusteer cloud, στις οποίες περιλαμβάνονται η αρχική εκκίνηση, η παραμετροποίηση, η χρήση προτύπου οθόνης εκκίνησης (Splash Template), η διενέργεια δοκιμών και η εκπαίδευση.

Στις δραστηριότητες υλοποίησης δεν περιλαμβάνονται οι δραστηριότητες που απαιτούνται για τις Εφαρμογές ή τα συστήματα του Πελάτη.

Η φάση της υλοποίησης των διαφόρων Υπηρεσιών Cloud έχει σχεδιαστεί για να ολοκληρωθεί εντός των χρονικών πλαισίων που περιγράφονται στους αντίστοιχους οδηγούς υλοποίησης.

Η ολοκλήρωση αυτών των φάσεων υλοποίησης εντός της καθορισμένης χρονικής προθεσμίας εξαρτάται από την πλήρη δέσμευση και συμμετοχή της διοίκησης και του προσωπικού του Πελάτη. Ο Πελάτης πρέπει να παρέχει εγκαίρως τις απαιτούμενες πληροφορίες. Η αποδοτικότητα της IBM θα εξαρτάται από την έγκαιρη παροχή πληροφοριών και την έγκαιρη λήψη αποφάσεων από τον Πελάτη και οποιαδήποτε καθυστέρηση μπορεί να συνεπάγεται πρόσθετες δαπάνες ή/και καθυστέρηση στην ολοκλήρωση αυτών των υπηρεσιών υλοποίησης.

Για κάθε Εφαρμογή για την οποία ο Πελάτης προμηθεύεται συνδρομή, η βασική συνδρομή του Πελάτη περιλαμβάνει τις απαιτούμενες δραστηριότητες ετοιμασίας (setup) και αρχικής εγκατάστασης στο IBM Trusteer cloud, στις οποίες περιλαμβάνονται η αρχική εκκίνηση, η παραμετροποίηση, η χρήση προτύπου οθόνης εκκίνησης (Splash Template), η διενέργεια δοκιμών και η εκπαίδευση.

Η συνδρομή του Πελάτη περιλαμβάνει την υποστήριξη και δοκιμή για τις σελίδες στην εν λόγω εφαρμογή του Πελάτη που θα έχουν χαρακτηριστεί ως προτεινόμενες από την IBM κατά την αρχική υλοποίηση. Η IBM δεν είναι υπεύθυνη για: (i) τη μερική υλοποίηση, (ii) την επιλογή του Πελάτη να μην υλοποιήσει τις Υπηρεσίες Cloud της IBM όπως συνιστάται από την IBM, (iii) την επιλογή του Πελάτη να πραγματοποιήσει ο ίδιος την υλοποίηση, την προετοιμασία και τη δοκιμή, (iv) τη μερική υλοποίηση ή προστασία που οφείλεται στην παροχή ανεπαρκών πληροφοριών από τον Πελάτη. Μπορεί να συναφθεί χωριστή σύμβαση για πρόσθετες υπηρεσίες, συμπεριλαμβανομένων δραστηριοτήτων υλοποίησης πέρα από την αρχική υλοποίηση, έναντι πρόσθετης χρέωσης.

8. Προστασία Προσωπικών Δεδομένων και Ασφάλεια Δεδομένων

Αυτή η Υπηρεσία Cloud συμμορφώνεται με τις βασικές αρχές προστασίας και ασφάλειας δεδομένων για Cloud, οι οποίες καθίστανται διαθέσιμες στην ιστοσελίδα http://www.ibm.com/cloud/data-security και με οποιουσδήποτε πρόσθετους όρους προβλέπονται στο παρόν άρθρο. Τυχόν αλλαγές στις βασικές αρχές ασφάλειας δεδομένων της IBM δεν θα υποβαθμίζουν την ασφάλεια της Υπηρεσίας Cloud.

Αυτή η Υπηρεσία Cloud μπορεί να χρησιμοποιηθεί για την επεξεργασία περιεχομένου που περιλαμβάνει δεδομένα προσωπικού χαρακτήρα σε περίπτωση που ο Πελάτης, ως υπεύθυνος επεξεργασίας δεδομένων (data controller), κρίνει ότι τα υφιστάμενα τεχνικά και οργανωτικά μέτρα ασφαλείας είναι κατάλληλα για την αντιμετώπιση των κινδύνων που απορρέουν από την επεξεργασία και τη φύση των προς προστασία δεδομένων. Ο Πελάτης αναγνωρίζει ότι αυτή η Υπηρεσία Cloud δεν παρέχει λειτουργίες για την προστασία ευαίσθητων δεδομένων προσωπικού χαρακτήρα ή δεδομένων που υπόκεινται σε πρόσθετες κανονιστικές απαιτήσεις.

Αυτή η Υπηρεσία Cloud περιλαμβάνεται στην πιστοποίηση της IBM για την Ασπίδα Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Privacy Shield), η οποία ισχύει σε περίπτωση που ο Πελάτης επιλέξει την "φιλοξενία" της Υπηρεσίας Cloud σε ένα κέντρο πληροφοριακών συστημάτων που βρίσκεται στις Ηνωμένες Πολιτείες, και υπόκειται στην Πολιτική Προστασίας Δεδομένων Προσωπικού Χαρακτήρα της IBM σύμφωνα με την Ασπίδα Προστασίας (IBM Privacy Shield Privacy Policy), η οποία καθίσταται διαθέσιμη στην ιστοσελίδα http://www.ibm.com/privacy/details/us/en/privacy_shield.html.

8.1 Λειτουργίες Ασφάλειας και Υποχρεώσεις

Η Υπηρεσία Cloud παρέχει τις ακόλουθες λειτουργίες ασφάλειας:

Η Υπηρεσία Cloud κρυπτογραφεί περιεχόμενο κατά τη μετάδοση δεδομένων από και προς το δίκτυο της IBM και καθώς βρίσκεται σε κατάσταση αναμονής για τη μετάδοση δεδομένων από το τελικό σημείο.

8.2 Νόμιμη Χρήση και Συναίνεση

Νόμιμη Χρήση

Η χρήση αυτής της Υπηρεσίας Cloud μπορεί να υπόκειται σε διάφορους νόμους ή κανονισμούς. Η Υπηρεσία Cloud επιτρέπεται να χρησιμοποιείται μόνο για νόμιμους σκοπούς και με νόμιμο τρόπο. Ο Πελάτης συμφωνεί να χρησιμοποιεί την Υπηρεσία Cloud σύμφωνα με τους ισχύοντες νόμους, κανονισμούς και πολιτικές και αναλαμβάνει την πλήρη ευθύνη για τη συμμόρφωση με τους εν λόγω νόμους, κανονισμούς και πολιτικές.

Εξουσιοδότηση για τη Συλλογή και Επεξεργασία Δεδομένων

Η Υπηρεσία Cloud θα συλλέγει πληροφορίες από Δικαιούμενους Συμμετέχοντες και Συσκευές Πελάτη που αλληλεπιδρούν με τις Επιχειρηματικές Εφαρμογές ή τις Εφαρμογές Λιανικής για τις οποίες ο Πελάτης έχει προμηθευτεί συνδρομή για την κάλυψή τους από Υπηρεσίες Cloud. Η Υπηρεσία Cloud συλλέγει πληροφορίες οι οποίες, είτε μεμονωμένες είτε σε συνδυασμό, μπορεί να θεωρούνται Δεδομένα Προσωπικού Χαρακτήρα σε ορισμένες δικαιοδοσίες. Δεδομένα Προσωπικού Χαρακτήρα (Personal Data) είναι οποιεσδήποτε πληροφορίες που μπορούν να χρησιμοποιηθούν για τον προσδιορισμό της ταυτότητας ενός συγκεκριμένου ατόμου, όπως π.χ. ένα όνομα, μια διεύθυνση email, μια διεύθυνση οικίας ή ένας αριθμός τηλεφώνου, οι οποίες παρέχονται στην IBM για την αποθήκευση, επεξεργασία ή διαβίβασή τους για λογαριασμό του Πελάτη.

Οι πρακτικές συλλογής και επεξεργασίας δεδομένων μπορεί να ενημερώνονται με σκοπό τη βελτίωση της λειτουργικότητας της Υπηρεσίας Cloud. Ένα έγγραφο στο οποίο παρέχεται μια πλήρης περιγραφή των πρακτικών συλλογής και επεξεργασίας δεδομένων ενημερώνεται όποτε είναι απαραίτητο και διατίθεται

κατόπιν σχετικού αιτήματος του Πελάτη. Ο Πελάτης εξουσιοδοτεί την IBM να συλλέγει αυτές τις πληροφορίες και να τις επεξεργάζεται σύμφωνα με τις διατάξεις του άρθρου Διασυνοριακές Διαβιβάσεις και του άρθου Προστασία Δεδομένων Προσωπικού Χαρακτήρα της παρούσας Περιγραφής Υπηρεσιών.

Για προσφορές IBM Trusteer που περιλαμβάνουν το Trusteer Management Application (TMA):

Τα ακόλουθα δεδομένα συλλέγονται και αποθηκεύονται στο Trusteer Management Application (TMA) για διαχειριστές του TMA από την επιχείρηση-χορηγό: διεύθυνση email (ως όνομα σύνδεσης), κωδικός πρόσβασης σε κατακερματισμένη (hashed) μορφή, όνομα, επώνυμο, επαγγελματικός τίτλος και τμήμα.

Για Υπηρεσίες Cloud για το IBM Trusteer Pinpoint:

Στα δεδομένα που συλλέγονται μπορεί να περιλαμβάνονται τα εξής:

- προσδιοριστικά χρηστών ή τελικών σημείων όπως π.χ ταυτότητες χρήστη (user IDs) κρυπτογραφημένες ή κατακερματισμένες μέσω μονόδρομων συναρτήσεων κατακερματισμού (one-way hash), ταυτότητας PUID (Persistent User ID), κλειδιά Report Agent Key και ταυτότητες συνεδριών πελατών (Customer Session IDs),
- δεδομένα που σχετίζονται με την προστατευόμενη εφαρμογή, όπως π.χ. συγκεκριμένα χαρακτηριστικά/στοιχεία από την εφαρμογή online τραπεζικών συναλλαγών του πελάτη όπως αυτά εμφανίζονται στο πρόγραμμα πλοήγησης του τελικού χρήστη, επισκέψεις σε ιστοσελίδες και ιστορικό πλοήγησης,
- πληροφορίες εγκατεστημένου περιβάλλοντος λογισμικού, χαρακτηριστικά και ρυθμίσεις προγράμματος οδήγησης και συσκευής και μήκος ιστορικού προγράμματος πλοήγησης,
- πληροφορίες υλικού εξοπλισμού και αποτύπωμα χρόνου,
- κεφαλίδες (headers) προγράμματος πλοήγησης και δεδομένα πρωτοκόλλων επικοινωνίας, όπως π.χ. διευθύνσεις IP χρηστών, cookies, κεφαλίδες διευθύνσεων αναφοράς και άλλες κεφαλίδες HTTP,
- δεδομένα κίνησης ποντικιού των τελικών χρηστών, όπως π.χ. οι συντεταγμένες του δείκτη του ποντικιού, η κίνηση της ροδέλας κύλισης (ή αντίστοιχου μηχανισμού) και το αποτύπωμα χρόνου κατά την αλληλεπίδραση των τελικών χρηστών με την εφαρμογή online τραπεζικών συναλλαγών του Πελάτη,
- ιστότοποι "ηλεκτρονικού ψαρέματος" (phishing) και πληροφορίες που υποβάλλονται σε τέτοιους ιστοτόπους, και
- κατ' αποκλειστική επιλογή του Πελάτη, δεδομένα συναλλαγών (ποσό συναλλαγών, νόμισμα συναλλαγών και κωδικοί προορισμού, κατακερματισμένες μέσω μονόδρομων συναρτήσεων κατακερματισμού ταυτότητες τραπεζών προορισμού, κατακερματισμένες μέσω μονόδρομων συναρτήσεων κατακερματισμού ταυτότητες λογαριασμών προορισμού, δυαδικές τιμές στις περιπτώσεις νέων δικαιούχων πληρωμής, και ημερομηνία/ώρα) και, προαιρετικά, δεδομένα βαθμών κινδύνου.
- κατ' αποκλειστική επιλογή του Πελάτη, ρυθμοί πληκτρολόγησης ή σειρές πληκτρολόγησης που χρησιμοποιούνται από τον τελικό χρήστη για την καταχώρηση ενός ονόματος χρήστη, ενός κωδικού πρόσβασης ή άλλου κειμένου (άλλα όχι τα ίδια τα γράμματα, οι αριθμοί ή οι ειδικοί χαρακτήρες, και χωρίς να υπάρχει η δυνατότητα διάκρισης του ονόματος χρήστη ή του κωδικού πρόσβασης).

Όταν το Policy Manager είναι ενεργοποιημένο, ο Πελάτης φέρει την αποκλειστική ευθύνη για τη χρήση οποιωνδήποτε εκτεταμένων δεδομένων (extended data). Η IBM συνιστά τον κατακερματισμό (hash) ή κρυπτογράφηση δεδομένων που μπορεί να θεωρούνται πληροφορίες από τις οποίες μπορεί να προκύψει η ταυτότητα συγκεκριμένων προσώπων.

Ο Πελάτης κατανοεί και συμφωνεί ότι η IBM δεν συλλέγει, αποθηκεύει διαχειρίζεται ή τηρεί τα επίσημα βιβλία ή/και αρχεία του Πελάτη.

Σε περίπτωση που ο Πελάτης προμηθευτεί μια συνδρομή για την προσφορά IBM Trusteer Rapport for Remediation ή σε περίπτωση παροχής υποστήριξης για μια προσφορά Pinpoint, η IBM μπορεί να προτείνει την εγκατάσταση του Λογισμικού Πελάτη για Κάτοχο Λογαριασμού Trusteer Rapport σε μια μηχανή ενός Δικαιούμενου Συμμετέχοντα για τη διερεύνηση πιθανής μόλυνσης από επιβλαβή κώδικα. Τα δεδομένα που συλλέγονται για τις προσφορές Trusteer Report αναφέρονται παρακάτω.

Για Υπηρεσίες Cloud για το IBM Trusteer Rapport (συμπεριλαμβανομένης της προσφοράς Rapport for Remediation ή Rapport for Mitigation όταν υλοποιηθεί σε συνάρτηση με τις προσφορές Pinpoint):

Στα δεδομένα που συλλέγονται μπορεί να περιλαμβάνονται τα εξής:

- διευθύνσεις URL και διευθύνσεις IP (Internet Protocol) ιστοτόπων που επισκέπτεται ένας Κάτοχος Λογαριασμού και οι οποίοι κρίνονται από την IBM ως δυνητικά κακόβουλοι ή εκμεταλλευτικοί ή ως ιστότοποι "ηλεκτρονικού ψαρέματος" (phishing), μαζί με πληροφορίες για τη φύση των δυνητικών απειλών που εντοπίστηκαν,
- διευθύνσεις URL και διευθύνσεις IP ιστοτόπων που επισκέπτεται ο Κάτοχος Λογαριασμού οι οποίοι ελέγχονται από την Πελάτη και προστατεύονται από την Υπηρεσία Cloud, όπως π.χ. ιστότοποι online τραπεζικών συναλλαγών, και διευθύνσεις IP του Κατόχου Λογαρισμού,
- πληροφορίες για τον υλικό εξοπλισμό, τα λειτουργικά συστήματα, το λογισμικό εφαρμογών, τον περιφερειακό εξοπλισμό, την παραμετροποίηση ασφάλειας, τις ρυθμίσεις συστήματος και τις δικτυακές συνδέσεις του τελικού σημείου, καθώς και η ταυτότητα, το όνομα, τα δείγματα χρήσης (use patterns) και άλλες αναγνωρίσιμες πληροφορίες του τελικού σημείου,
- πληροφορίες σχετικά με την εγκατάσταση και λειτουργία του προγράμματος, την ταυτότητα του προγράμματος, την έκδοση του προγράμματος, τα περιστατικά ασφάλειας που παράγονται από το τελικό σημείο, και πληροφορίες για τα σφάλματα του προγράμματος,
- στατιστικά στοιχεία χρήσης και στατιστικές πληροφορίες για τις απειλές που εντοπίστηκαν από το πρόγραμμα, αρχεία καταγραφής που περιέχουν πληροφορίες για περιστατικά τερματισμού της λειτουργίας του προγράμματος πλοήγησης, πληροφορίες για την ημερομηνία και ώρα μόλυνσης, και πληροφορίες για τη φύση των απειλών και δυσλειτουργιών που εντοπίστηκαν,
- επιχειρηματικός δεσμός με τον Πελάτη, αναφερόμενος επίσης ως Επιχείρηση-Χορηγός. Δημιουργείται ένας επιχειρηματικός δεσμός όταν ένας τελικός χρήστης μεταφορτώσει (download) το Rapport από τον ιστότοπο του Πελάτη, επιλέξει ένα συγκεκριμένο Πελάτη κατά τη μεταφόρτωση του Report από τον ιστότοπο υποστήριξης της Trusteer ή συνδεθεί στην τραπεζική εφαρμογή του Πελάτη. Ένας τελικός χρήστης μπορεί να έχει περισσότερους από έναν επιχειρηματικούς δεσμούς του Πελάτη.
- ένα αντίγραφο της κρυπτογραφημένης ταυτότητας χρήστη (User ID) που χρησιμοποιεί ο Κάτοχος Λογαριασμού για την επικοινωνία με τον Πελάτη (προαιρετικά),
- ένα κρυπτογραφημένο αντίγραφο του αριθμού πιστωτικής κάρτας που καταχωρεί ο Κάτοχος Λογαριασμού στην ιστοσελίδα ενός ιστοτόπου αφού ενημερωθεί από το πρόγραμμα ότι ο εν λόγω ιστότοπος κρίνεται επικίνδυνος,
- αρχεία και άλλες πληροφορίες από το τελικό σημείο για τα οποία το εξειδικευμένο προσωπικό ασφάλειας της IBM υποπτεύεται ότι σχετίζονται με επιβλαβή κώδικα ή άλλες κακόβουλες δραστηριότητες, ή τα οποία μπορεί να σχετίζονται με μια γενική δυσλειτουργία του προγράμματος, και
- προσωπικές πληροφορίες επικοινωνίας, όπως π.χ. ονόματα και διευθύνσεις email, που συλλέγονται όταν ο τελικός χρήστης επικοινωνήσει με την υπηρεσία υποστήριξης.

Για Υπηρεσίες Cloud για το IBM Trusteer Mobile SDK και το IBM Trusteer Mobile Browser:

Στα δεδομένα που συλλέγονται μπορεί να περιλαμβάνονται τα εξής:

- προσδιοριστικά χρηστών, όπως π.χ. ταυτότητες χρήστη (user IDs) κρυπτογραφημένες ή κατακερματισμένες μέσω μονόδρομων συναρτήσεων κατακερματισμού (one-way hash),
- πληροφορίες συσκευών, όπως π.χ. διεύθυνση IP, κατακερματισμένη (hashed) ταυτότητα συσκευής, αποτύπωμα χρόνου, τιμές MD5 εγκατεστημένων πακέτων και άλλες πληροφορίες για τον υλικό εξοπλισμό και το λογισμικό της συσκευής,
- αριθμός έκδοσης και ημερομηνία εγκατάστασης του Mobile SDK ή του Mobile Browser,
- επισκέψεις σε προστατευόμενες εφαρμογές,
- επιχειρηματικοί δεσμοί του Πελάτη, και
- δεδομένα αναφορικά με κινδύνους για τη συσκευή (π.χ. παρουσία επιβλαβούς κώδικα, εφαρμογών root hider, κατάσταση κρυπτογράφησης Wi-Fi, το εάν η συσκευή έχει υποστεί jailbreaking, κ.ο.κ.),

- ιχνηλασία στοίβας τερματισμού λειτουργίας (crash stack trace, στην περίπτωση απροσδόκητου τερματισμού της λειτουργίας της εφαρμογής),
- δεδομένα κατασκευής τηλεφώνου (π.χ. μοντέλο, κατασκευαστής),
- αλληλεπιδράσεις τελικών χρηστών στην οθόνη αφής, όπως π.χ. οι συντεταγμένες x, y, η περιοχή αφής και το είδος ενέργειας (πάνω, κάτω και μετακίνηση),
- δεδομένα αισθητήρων κίνησης, κατανάλωση ενέργειας/πόρων, ρυθμίσεις σύνδεσης, δεδομένα αισθητήρων περιβάλλοντος χώρου όπως π.χ. θερμοκρασία, φως και ατμοσφαιρική πίεση, και γενικές ρυθμίσεις συσκευής (ένταση ήχου, ένταση κουδουνίσματος, φωτεινότητα οθόνης κ.ο.κ.).

8.3 Ενημερωμένη Συναίνεση από τα Πρόσωπα στα οποία αναφέρονται τα Δεδομένα

Για Υπηρεσίες Cloud για το IBM Trusteer Pinpoint και το IBM Trusteer Mobile SDK:

Ο Πελάτης συμφωνεί ότι έχει αποκτήσει ή θα αποκτήσει οποιεσδήποτε απαιτούμενες πλήρως ενημερωμένες συναινέσεις, άδειες ή δικαιώματα χρήσης προκειμένου να καθίσταται δυνατή η νόμιμη χρήση της Υπηρεσίας Cloud και να επιτρέπεται η συλλογή και επεξεργασία των πληροφοριών από την IBM μέσω των Υπηρεσιών Cloud.

Για Υπηρεσίες Cloud IBM Trusteer Rapport (συμπεριλαμβανομένου του Rapport for Remediation ή του Rapport for Mitigation όταν υλοποιηθεί σε συνάρτηση με τις Υπηρεσίες Cloud για το Pinpoint), και για Υπηρεσίες Cloud IBM Trusteer Mobile Browser:

Ο Πελάτης εξουσιοδοτεί την IBM να αποκτήσει τις απαιτούμενες πλήρως ενημερωμένες συναινέσεις προκειμένου να καθίσταται δυνατή η νόμιμη χρήση της Υπηρεσίας Cloud και η συλλογή και επεξεργασία των πληροφοριών, όπως περιγράφεται στη Σύμβαση Άδειας Χρήσης Τελικού Χρήστη που διατίθεται στην ιστοσελίδα https://www.trusteer.com/support/end-user-license-agreement. Σε περίπτωση που ο Πελάτης αποφασίσει ότι ο ίδιος (και όχι η IBM) αναλαμβάνει την επικοινωνία με τους τελικούς χρήστες αναφορικά με τις απαιτούμενες συναινέσεις, ο Πελάτης συμφωνεί ότι έχει αποκτήσει ή θα αποκτήσει οποιεσδήποτε απαιτούμενες πλήρως ενημερωμένες συναινέσεις, άδειες ή δικαιώματα χρήσης προκειμένου να καθίσταται δυνατή η νόμιμη χρήση της Υπηρεσίας Cloud και να επιτρέπεται η συλλογή και επεξεργασία των πληροφοριών από την IBM ως εκτελούντα την επεξεργασία δεδομένων (data processor) του Πελάτη μέσω της Υπηρεσίας Cloud.

8.4 Χρήση Δεδομένων Ασφάλειας

Στο πλαίσιο της Υπηρεσίας Cloud, η οποία περιλαμβάνει δραστηριότητες δημιουργίας αναφορών, η IBM θα προετοιμάζει και θα διατηρεί πληροφορίες μη περιέχουσες στοιχεία προσδιορισμού ταυτότητας ή/και συγκεντρωτικές πληροφορίες που συλλέγονται από την Υπηρεσία Cloud ("Δεδομένα Ασφάλειας"). Τα Δεδομένα Ασφάλειας δεν θα προσδιορίζουν την ταυτότητα του Πελάτη, των Δικαιούμενων Συμμετεχόντων του ή οποιουδήποτε μεμονωμένου προσώπου, με εξαίρεση την περίπτωση που περιγράφεται στο στοιχείο (δ) παρακάτω. Ο Πελάτης συμφωνεί ότι η IBM μπορεί για απεριόριστο χρονικό διάστημα να χρησιμοποιεί ή/και να αντιγράφει τα Δεδομένα Ασφάλειας μόνο για τους ακόλουθους σκοπούς:

α. δημοσίευση ή/και διανομή των Δεδομένων Ασφάλειας (π.χ. σε συλλογές ή/και αναλύσεις που σχετίζονται με την ασφάλεια στον κυβερνοχώρο),

β. ανάπτυξη ή βελτίωση προϊόντων ή υπηρεσιών,

γ. διεξαγωγή ερευνητικών δραστηριοτήτων είτε εσωτερικά είτε σε συνεργασία με τρίτους,

δ. κοινοποίηση πληροφοριών τρίτων με αποδεδειγμένη παραβατική δραστηριότητα, και

ε. χρήση κανόνων από το Policy Manager από τους οποίους έχουν αφαιρεθεί τα όποια στοιχεία προσδιορισμού ταυτότητας.

8.5 Διασυνοριακές Διαβιβάσεις

Ο Πελάτης συμφωνεί ότι η IBM μπορεί να προβαίνει στην επεξεργασία του περιεχομένου, συμπεριλαμβανομένων οποιωνδήποτε Δεδομένων Προσωπικού Χαρακτήρα, όπως αυτά ορίζονται στο ανωτέρω άρθρο Νόμιμη Χρήση και Συναίνεση, σύμφωνα με τους ισχύοντες νόμους και απαιτήσεις, διαμέσου κρατικών συνόρων μέσω εκτελούντων την επεξεργασία (processors) και υπεργολάβων επεξεργασίας (sub-processors) στις ακόλουθες χώρες εκτός του Ευρωπαϊκού Οικονομικού Χώρου και χώρες που θεωρούνται από την Ευρωπαϊκή Επιτροπή ως χώρες που παρέχουν επαρκή επίπεδα προστασίας: στις ΗΠΑ.

8.6 Προστασία Δεδομένων Προσωπικού Χαρακτήρα

Εάν ο Πελάτης καταστήσει Δεδομένα Προσωπικού Χαρακτήρα διαθέσιμα στην Υπηρεσία Cloud στα Κράτη-Μέλη της ΕΕ, στην Ισλανδία, στο Λιχτενστάιν, στη Νορβηγία ή στην Ελβετία, ή εάν ο Πελάτης έχει Δικαιούμενους Συμμετέχοντες ή Συσκευές Πελάτη στις εν λόγω χώρες, τότε ο Πελάτης ως μοναδικός υπεύθυνος επεξεργασίας (controller) ορίζει την IBM ως εκτελούντα την επεξεργασία (processor) για την επεξεργασία (ως οι εν λόγω όροι ορίζονται στην Οδηγία 95/46/ΕΚ της ΕΕ) Δεδομένων Προσωπικού Χαρακτήρα. Η IBM θα επεξεργάζεται τέτοια Δεδομένα Προσωπικού Χαρακτήρα μόνο στο βαθμό που απαιτείται για να καταστεί διαθέσιμη η προσφορά Υπηρεσίας Cloud σύμφωνα με τις δημοσιευμένες από την IBM περιγραφές Υπηρεσιών Cloud και ο Πελάτης συμφωνεί ότι η εν λόγω επεξεργασία γίνεται σύμφωνα με τις δικές του οδηγίες. Η IBM θα παρέχει εύλογη εκ των προτέρων ειδοποίηση μέσω της Πύλης Πελατών (Customer Portal) εάν η IBM προβεί σε ουσιώδη αλλαγή στην τοποθεσία επεξεργασίας ή στον τρόπο προστασίας Δεδομένων Προσωπικού Χαρακτήρα στο πλαίσιο της Υπηρεσίας Cloud. Ο Πελάτης μπορεί να διακόψει την τρέχουσα περίοδο συνδρομής της εν λόγω Υπηρεσίας Cloud, παρέχοντας έγγραφη ειδοποίηση στην IBM εντός τριάντα (30) ημερών από την ημερομηνία κατά την οποία η IBM κοινοποιεί την εν λόγω αλλαγή στον Πελάτη.

Τα συμβαλλόμενα μέρη ή οι αντίστοιχες συνδεδεμένες με αυτά εταιρείες μπορούν να προβούν στη σύναψη χωριστών, πρότυπων συμβάσεων με Πρότυπες Ρήτρες της ΕΕ, χωρίς τροποποιήσεις, υπό τους αντίστοιχους ρόλους τους σύμφωνα με την Απόφαση 2010/87/ΕΕ της ΕΚ, έχοντας αφαιρέσει τις προαιρετικές ρήτρες. Οποιεσδήποτε διαφορές ή ευθύνες απορρέουν από τις εν λόγω συμβάσεις, ακόμα και σε περίπτωση που οι εν λόγω έχουν συναφθεί από συνδεδεμένες με τα συμβαλλόμενα μέρη εταιρείες, θα αντιμετωπίζονται από τα συμβαλλόμενα μέρη σαν να πρόκειται για διαφορά ή ευθύνη που προέκυψε ανάμεσα στα συμβαλλόμενα μέρη βάσει των όρων της παρούσας Σύμβασης.

α. Ο Πελάτης συμφωνεί ότι για υπηρεσίες που παρέχονται μέσω του Γερμανικού κέντρου πληροφοριακών συστημάτων, όπως ορίζεται κατά τη διαδικασία αρχικής παροχής του IBM SaaS, η IBM μπορεί να προβαίνει στην επεξεργασία περιεχομένου, συμπεριλαμβανομένων οποιωνδήποτε Δεδομένων Προσωπικού Χαρακτήρα, διαμέσου κρατικών συνόρων μέσω των ακόλουθων εκτελούντων την επεξεργασία (processors) και υπεργολάβων επεξεργασίας (sub-processors):

Όνομα Εκτελούντος την Επεξεργασία/Υπεργολάβου Επεξεργασίας	Ρόλος (Εκτελών την Επεξεργασία ή Υπεργολάβος Επεξεργασίας)	Τοποθεσία
Συμβαλλόμενο νομικό πρόσωπο IBM	Εκτελών την Επεξεργασία	Όπως δηλώνεται στο Έγγραφο Συναλλαγής
Amazon Web Services (Γερμανία)	Υπεργολάβος Επεξεργασίας	Γερμανία
IBM Ireland Ltd.	Εκτελών την Επεξεργασία	Ιρλανδία
IBM Israel Ltd.	Εκτελών την Επεξεργασία	Ισραήλ

Για υπηρεσίες που παρέχονται μέσω του κέντρου πληροφοριακών συστημάτων στη Γερμανία, ορισμένες υπηρεσίες υποστήριξης πελατών μπορεί να παρέχονται από υπαλλήλους της Trusteer που έχουν την έδρα τους σε κάποια χώρα της Ευρωπαϊκής Ένωσης.

β. Ο Πελάτης συμφωνεί ότι για υπηρεσίες που παρέχονται μέσω του Ιαπωνικού κέντρου πληροφοριακών συστημάτων, όπως ορίζεται κατά τη διαδικασία αρχικής παροχής του IBM SaaS, η IBM μπορεί να προβαίνει στην επεξεργασία περιεχομένου, συμπεριλαμβανομένων οποιωνδήποτε Δεδομένων Προσωπικού Χαρακτήρα, διαμέσου κρατικών συνόρων μέσω των ακόλουθων εκτελούντων την επεξεργασία (processors) και υπεργολάβων επεξεργασίας (sub-processors):

Όνομα Εκτελούντος την Επεξεργασία/Υπεργολάβου Επεξεργασίας	Ρόλος (Εκτελών την Επεξεργασία ή Υπεργολάβος Επεξεργασίας)	Τοποθεσία
Συμβαλλόμενο νομικό πρόσωπο IBM	Εκτελών την Επεξεργασία	Ιαπωνία, όπως δηλώνεται στο Έγγραφο Συναλλαγής
Amazon Web Services (Ιαπωνία)	Υπεργολάβος Επεξεργασίας	Ιαπωνία
IBM Ireland Ltd.	Εκτελών την Επεξεργασία	Ιρλανδία
IBM Israel Ltd.	Εκτελών την Επεξεργασία	Ισραήλ

γ. Ο Πελάτης συμφωνεί ότι για υπηρεσίες που παρέχονται μέσω του κέντρου πληροφοριακών συστημάτων στις ΗΠΑ, η IBM μπορεί να προβαίνει στην επεξεργασία περιεχομένου, συμπεριλαμβανομένων οποιωνδήποτε Δεδομένων Προσωπικού Χαρακτήρα, διαμέσου κρατικών συνόρων μέσω των ακόλουθων εκτελούντων την επεξεργασία (processors) και υπεργολάβων επεξεργασίας (sub-processors):

Όνομα Εκτελούντος την Επεξεργασία/Υπεργολάβου Επεξεργασίας	Ρόλος (Εκτελών την Επεξεργασία ή Υπεργολάβος Επεξεργασίας)	Τοποθεσία
Συμβαλλόμενο νομικό πρόσωπο IBM	Εκτελών την Επεξεργασία	Όπως δηλώνεται στο Έγγραφο Συναλλαγής
Amazon Web Services LLC	Υπεργολάβος Επεξεργασίας	Ηνωμένες Πολιτείες
IBM Ireland Ltd.	Εκτελών την Επεξεργασία	Ιρλανδία
IBM Israel Ltd.	Εκτελών την Επεξεργασία	Ισραήλ
IBM Corp	Εκτελών την Επεξεργασία	Ηνωμένες Πολιτείες

δ. Για τις παρεχόμενες υπηρεσίες μέσω των κέντρων πληροφοριακών συστημάτων που παρατίθενται στο ανωτέρω Άρθρο 8.5.γ, η IBM μπορεί να προβαίνει στην επεξεργασία μέσω ενός ή περισσοτέρων από τους ακόλουθους υπεργολάβους επεξεργασίας (sub-processors), όπως ορίζεται κατά τη διαδικασία αρχικής παροχής του IBM SaaS:

Όνομα Εκτελούντος την Επεξεργασία/Υπεργολάβου Επεξεργασίας	Ρόλος (Εκτελών την Επεξεργασία ή Υπεργολάβος Επεξεργασίας)	Τοποθεσία
Amazon Web Services (Αυστραλία)	Υπεργολάβος Επεξεργασίας	Αυστραλία
Amazon Web Services (Σιγκαπούρη)	Υπεργολάβος Επεξεργασίας	Σιγκαπούρη
Amazon Web Services (Ιρλανδία)	Υπεργολάβος Επεξεργασίας	Ιρλανδία

ε. Ο Πελάτης συμφωνεί ότι η IBM μπορεί, κατόπιν σχετικής ειδοποίησης μέσω της Πύλης Πελατών (Customer Portal), να μεταφέρει την επεξεργασία από την Amazon Web Services στα κέντρα πληροφοριακών συστημάτων της IBM. Η IBM μπορεί επίσης, κατόπιν σχετικής ειδοποίησης μέσω της Πύλης Πελατών, να μεταβάλει τις παραπάνω λίστες υπεργολάβων επεξεργασίας.

στ. Τα δεδομένα του Κατόχου Λογαριασμού θα υποβάλλονται σε επεξεργασία στην περιοχή από την οποία ο Κάτοχος Λογαριασμού εγκατέστησε αρχικά το Λογισμικό Πελάτη για Κάτοχο Λογαριασμού. Αυτό μπορεί να σημαίνει ότι το περιεχόμενο του Κατόχου Λογαριασμού μπορεί να υποβάλλεται σε επεξεργασία τόσο στην περιοχή προέλευσης του λογισμικού όσο και στην περιοχή που θα συμφωνηθεί με τον πελάτη.

ζ. Τα δεδομένα υποστήριξης πελατών αποθηκεύονται σε έναν εξυπηρετητή cloud της Salesforce.com στην Ιρλανδία.

η. Διευκρινίζεται ότι, δεδομένου ότι το Trusteer Fraud Protection αποτελεί μια ολοκληρωμένη λύση, σε περίπτωση που ο Πελάτης προβεί στη διακοπή οποιασδήποτε από αυτές τις Υπηρεσίες Cloud, η IBM μπορεί να διατηρήσει τα δεδομένα του Πελάτη για τους σκοπούς της παροχής των υπολοίπων Υπηρεσιών Cloud στον Πελάτη βάσει της παρούσας Περιγραφής Υπηρεσιών.

9. Σύμβαση Επιπέδου Παροχής Υπηρεσιών

Η IBM παρέχει την ακόλουθη σύμβαση επιπέδου παροχής υπηρεσιών ("SLA") αναφορικά με τη διαθεσιμότητα της Υπηρεσίας Cloud, όπως καθορίζεται σε μια Απόδειξη Δικαιώματος. Η Σύμβαση SLA δεν συνιστά εγγύηση. Η Σύμβαση SLA είναι διαθέσιμη μόνο στον Πελάτη και ισχύει μόνο για τη χρήση σε περιβάλλοντα παραγωγής.

9.1 Πιστώσεις Διαθεσιμότητας

Ο Πελάτης πρέπει να υποβάλει ένα δελτίο υποστήριξης για Ζήτημα Κρισιμότητας 1 στο Help Desk τεχνικής υποστήριξης της IBM, εντός 24 ωρών από τη στιγμή που ο Πελάτης παρατηρεί για πρώτη φορά ότι προέκυψε ένα συμβάν που έχει επιπτώσεις στη διαθεσιμότητα της Υπηρεσίας Cloud. Ο Πελάτης πρέπει εύλογα να βοηθά την IBM στη διάγνωση και επίλυση προβλημάτων.

Μια αξίωση βάσει δελτίου υποστήριξης για τη μη ανταπόκριση στις απαιτήσεις μιας Σύμβασης SLA πρέπει να υποβάλλεται εντός τριών εργάσιμων ημερών από το τέλος του συμβατικού μήνα. Η αποζημίωση για μια έγκυρη αξίωση μη ανταπόκρισης στις απαιτήσεις μιας Σύμβασης SLA θα συνίσταται σε μια πίστωση έναντι ενός μελλοντικού τιμολογίου για την Υπηρεσία Cloud η οποία θα βασίζεται στη διάρκεια του χρονικού διαστήματος κατά το οποίο δεν ήταν διαθέσιμη η δυνατότητα επεξεργασίας στο σύστημα παραγωγής της Υπηρεσίας Cloud ("Χρόνος Διακοπής Λειτουργίας"). Ο Χρόνος Διακοπής Λειτουργίας μετράται από τη χρονική στιγμή που ο Πελάτης αναφέρει το συμβάν έως τη χρονική στιγμή που αποκαθίσταται η Υπηρεσία Cloud και δεν περιλαμβάνει το χρόνο που σχετίζεται με μια προγραμματισμένη ή ανακοινωθείσα διακοπή λειτουργίας για σκοπούς συντήρησης, αιτίες πέραν από τον έλεγχο της IBM, προβλήματα με το περιεχόμενο ή την τεχνολογία, το σχεδιασμό ή τις οδηγίες του Πελάτη ή τρίτων, μη υποστηριζόμενες διατάξεις συστημάτων και πλατφορμών ή άλλα σφάλματα του Πελάτη, ή προκληθέντα από τον Πελάτη περιστατικά ασφάλειας ή δοκιμές ασφάλειας του Πελάτη. Η IBM θα παρέχει την υψηλότερη ισχύουσα αποζημίωση με βάση τη σωρευτική διαθεσιμότητα της Υπηρεσίας Cloud κατά τη διάρκεια κάθε Συμβατικού Μήνα, όπως αναφέρεται στον παρακάτω πίνακα. Η συνολική αποζημίωση που παρέχεται για οποιονδήποτε συμβατικό μήνα δεν μπορεί να υπερβαίνει το 10 τοις εκατό (10%) του εν δωδέκατου (1/12) της ετήσιας χρέωσης για την Υπηρεσία Cloud.

9.2 Επίπεδα Παροχής Υπηρεσιών

Διαθεσιμότητα της Υπηρεσίας Cloud κατά τη διάρκεια ενός συμβατικού μήνα

Διαθεσιμότητα κατά τη διάρκεια ενός Συμβατικού Μήνα	**Αποζημίωση (% της μηνιαίας χρέωσης συνδρομής* για το συμβατικό μήνα που αποτελεί αντικείμενο αξίωσης)**
< 99,5%	2%
< 98,0%	5%
< 96,0%	10%

* Εάν η Υπηρεσία Cloud αποκτήθηκε από έναν Εμπορικό Συνεργάτη της IBM, η μηνιαία χρέωση συνδρομής θα βασίζεται στην εκάστοτε ισχύουσα τιμή καταλόγου της Υπηρεσίας Cloud για το συμβατικό μήνα που αποτελεί αντικείμενο αξίωσης, με έκπτωση 50%. Η IBM θα προβαίνει σε μια άμεση επιστροφή χρημάτων στον Πελάτη.

Τα Επίπεδα Παροχής Υπηρεσιών και οι αντίστοιχες Πιστώσεις Υπηρεσιών μετρώνται χωριστά ανά Υπηρεσία Cloud και ανά Εφαρμογή Πελάτη.

Κατά τον υπολογισμό πιστώσεων SLA για Υπηρεσίες Cloud που βασίζονται σε δικαιώματα χρήσης Εφαρμογών, η Διαθεσιμότητα θα υπολογίζεται βάσει των παρακάτω κατευθυντήριων γραμμών:

- Σε κάθε Εφαρμογή θα αποδίδεται ένα ειδικό βάρος που θα βασίζεται στον αριθμό συνεδριών που μετρήθηκαν κατά τη διάρκεια του συμβατικού μήνα.
- Ο χρόνος διακοπής λειτουργίας κάθε Υπηρεσίας Cloud ανά Εφαρμογή θα αθροίζεται χωριστά για το συμβατικό μήνα.

Ακολουθεί ένα παράδειγμα των υπολογισμών για ένα μήνα δραστηριοτήτων και την αντίστοιχη απόδοση ειδικών βαρών. Το παράδειγμα αυτό παρέχεται μόνο για διευκρινιστικούς σκοπούς:

Εφαρμογές Λιανικής	**Μερίδιο στο συνολικό αριθμό συνεδριών σε ένα δεδομένο συμβατικό μήνα**	**Συνολικός Χρόνος Διακοπής Λειτουργίας κατά τη διάρκεια του συμβατικού μήνα**	**Σταθμισμένος Χρόνος Διακοπής Λειτουργίας**
Εφαρμογή Λιανικής Α	40%	300 λεπτά	40% x 300 λεπτά = 120 λεπτά
Εφαρμογή Λιανικής Β	20%	250 λεπτά	20% x 250 λεπτά = 50 λεπτά
Εφαρμογή Λιανικής Γ	40%	150 λεπτά	40% x 150 λεπτά = 60 λεπτά
			Συνολικός σταθμισμένος Χρόνος Διακοπής Λειτουργίας = 230 λεπτά

Η Διαθεσιμότητα, η οποία εκφράζεται ως ποσοστό, υπολογίζεται ως εξής: ο συνολικός αριθμός λεπτών σε ένα συμβατικό μήνα, μείον το συνολικό σταθμισμένο αριθμό λεπτών Χρόνου Διακοπής Λειτουργίας κατά τη διάρκεια του συμβατικού μήνα, διαιρούμενος διά του συνολικού αριθμού λεπτών στο συμβατικό μήνα.

Οι υπολογισμοί με βάση το παραπάνω παραδείγματος είναι ως εξής:

Σύνολο λεπτών κατά τη διάρκεια ενός Συμβατικού Μήνα 30 ημερών = 43.200 λεπτά - 230 λεπτά Σταθμισμένου Χρόνου Διακοπής Λειτουργίας = 42.970 λεπτά Συνολική διάρκεια Συμβατικού Μήνα = 43.200 λεπτά	= 2% Πίστωση Διαθεσιμότητας για 99,4% διαθεσιμότητα κατά τη διάρκεια του συμβατικού μήνα

10. Τεχνική Υποστήριξη

Διατίθεται Τεχνική Υποστήριξη για τις Υπηρεσίες Cloud στον Πελάτη και τους Δικαιούμενους Συμμετέχοντές του ώστε να βοηθούνται στην εκ μέρους τους χρήση των Υπηρεσιών Cloud.

Περιλαμβάνεται Τυπική Υποστήριξη (Standard Support) στην συνδρομή για όλες τις προσφορές. Το Trusteer Rapport Mandatory Service, που αποτελεί πρόσθετη υπηρεσία (add-on) του Trusteer Rapport, έχει ως προαπαιτούμενο τη λήψη Υποστήριξης επιπέδου Premium για τη βασική συνδρομή του Trusteer Rapport.

Για κάθε Υπηρεσία Cloud διατίθεται μια συνδρομή Υποστήριξης επιπέδου Premium έναντι πρόσθετης χρέωσης, με την εξαίρεση των Υπηρεσιών Cloud για το IBM Trusteer Mobile SDK και το IBM Trusteer Rapport Mandatory Service. Για περισσότερες πληροφορίες, επικοινωνήστε με τον Εκπρόσωπο Πωλήσεων της IBM ή τον Εμπορικό Συνεργάτη της IBM που σας εξυπηρετεί.

Τυπική Υποστήριξη (Standard Support):

- Υποστήριξη από 8 π.μ. - 5 μ.μ., τοπική ώρα.
- Οι Πελάτες και οι Δικαιούμενοι Συμμετέχοντές τους μπορούν να υποβάλουν ηλεκτρονικά δελτία υποστήριξης (support tickets), όπως περιγράφεται στο Εγχειρίδιο Υποστήριξης του SaaS (Software as a Service [SaaS] Support Handbook).
- Οι Πελάτες μπορούν να αποκτούν πρόσβαση στην Πύλη Υποστήριξης Πελατών (Client Support Portal) για ειδοποιήσεις, έγγραφα, αναφορές περιπτώσεων και απαντήσεις σε συχνές ερωτήσεις στη διεύθυνση: http://www-01.ibm.com/software/security/trusteer/support/.
- Για επιλογές υποστήριξης και λεπτομέρειες, ανατρέξτε στο Εγχειρίδιο Υποστήριξης του SaaS (Software as a Service [SaaS] Support Handbook): http://www-01.ibm.com/software/support/handbook.html.

Υποστήριξη επιπέδου Premium (Premium Support):

- Υποστήριξη 24x7 για όλους τους βαθμούς κρισιμότητας.
- Οι Πελάτες μπορούν να επικοινωνήσουν με την υποστήριξη απευθείας μέσω τηλεφώνου ή με την υποβολή ενός αιτήματος επανάκλησης.
- Οι Πελάτες και οι Δικαιούμενοι Συμμετέχοντές τους μπορούν να υποβάλουν ηλεκτρονικά δελτία υποστήριξης (support tickets), όπως περιγράφεται στο Εγχειρίδιο Υποστήριξης του SaaS (Software as a Service [SaaS] Support Handbook).
- Οι Πελάτες μπορούν να αποκτούν πρόσβαση στην Πύλη Υποστήριξης Πελατών (Client Support Portal) για ειδοποιήσεις, έγγραφα, αναφορές περιπτώσεων και απαντήσεις σε συχνές ερωτήσεις στη διεύθυνση: http://www-01.ibm.com/software/security/trusteer/support/.
- Για επιλογές υποστήριξης και λεπτομέρειες, ανατρέξτε στο Εγχειρίδιο Υποστήριξης του SaaS (Software as a Service [SaaS] Support Handbook): http://www-01.ibm.com/software/support/handbook.html.

11. Δικαιώματα και Τιμολόγηση

11.1 Μετρικά Συστήματα Χρέωσης

Η Υπηρεσία Cloud καθίσταται διαθέσιμη βάσει του μετρικού συστήματος χρέωσης που καθορίζεται στο Έγγραφο Συναλλαγής:

α. Δικαιούμενος Συμμετέχων (Eligible Participant) είναι μια μονάδα μέτρησης βάσει της οποίας μπορεί να αποκτηθεί η Υπηρεσία Cloud. Κάθε φυσικό ή νομικό πρόσωπο που πληροί τις προϋποθέσεις για συμμετοχή σε οποιοδήποτε πρόγραμμα παράδοσης υπηρεσιών που βρίσκεται υπό τη διαχείριση ή παρακολούθηση της Υπηρεσίας Cloud θεωρείται Δικαιούμενος Συμμετέχων. Πρέπει να αποκτηθούν

επαρκή δικαιώματα για την κάλυψη όλων των Δικαιούμενων Συμμετεχόντων που βρίσκονται υπό τη διαχείριση ή παρακολούθηση της Υπηρεσίας Cloud κατά τη διάρκεια της περιόδου μέτρησης που καθορίζεται στο Έγγραφο Συναλλαγής του Πελάτη.

Κάθε πρόγραμμα παράδοσης υπηρεσιών που βρίσκεται υπό τη διαχείριση της Υπηρεσίας Cloud αναλύεται χωριστά και στη συνέχεια προστίθεται μαζί με τα άλλα προγράμματα. Τα φυσικά ή νομικά πρόσωπα που πληρούν τις προϋποθέσεις συμμετοχής σε περισσότερα από ένα προγράμματα παράδοσης υπηρεσιών πρέπει να αποκτήσουν χωριστά δικαιώματα χρήσης για τα προγράμματα αυτά.

Για τους σκοπούς του προσδιορισμού των απαιτούμενων δικαιωμάτων επί αυτών των Υπηρεσιών Cloud, Δικαιούμενος Συμμετέχων είναι ένας τελικός χρήστης του Πελάτη ο οποίος διαθέτει μοναδικά στοιχεία ταυτότητας για τη σύνδεση σε μια Επιχειρηματική Εφαρμογή ή Εφαρμογή Λιανικής του Πελάτη.

β. Συσκευή Πελάτη (Client Device) είναι μια μονάδα μέτρησης βάσει της οποίας μπορεί να αποκτηθεί η Υπηρεσία Cloud. Συσκευή Πελάτη είναι μια μεμονωμένη υπολογιστική συσκευή, ένας εξειδικευμένος αισθητήρας ή μια συσκευή τηλεμετρικής που ζητά να εκτελεστεί ή λαμβάνει για εκτέλεση ένα σύνολο εντολών, διαδικασιών ή εφαρμογών από ή παρέχει δεδομένα σε ένα άλλο υπολογιστικό σύστημα, το οποίο συνήθως αποκαλείται εξυπηρετητής (server), ή κατά άλλον τρόπο ελέγχεται από έναν εξυπηρετητή. Περισσότερες από μία Συσκευές Πελάτη μπορεί να έχουν κοινή πρόσβαση σε έναν κοινό εξυπηρετητή. Μια Συσκευή Πελάτη μπορεί να έχει κάποιες δυνατότητες επεξεργασίας ή μπορεί να προγραμματιστεί ώστε να επιτρέπει την εκτέλεση εργασιών από ένα χρήστη. Ο Πελάτης πρέπει να αποκτήσει δικαιώματα χρήσης για κάθε Συσκευή Πελάτη στην οποία εκτελούνται οι Υπηρεσίες Cloud της IBM, παρέχει δεδομένα στην Υπηρεσία Cloud, χρησιμοποιεί υπηρεσίες που παρέχονται από την Υπηρεσία Cloud ή κατά άλλον τρόπο αποκτά πρόσβαση στην Υπηρεσία Cloud κατά τη διάρκεια της περιόδου μέτρησης που καθορίζεται στο Έγγραφο Συναλλαγής του Πελάτη.

γ. Εφαρμογή (Application) είναι μια μονάδα μέτρησης βάσει της οποίας μπορεί να αποκτηθεί η Υπηρεσία Cloud. Εφαρμογή είναι ένα πρόγραμμα λογισμικού με μοναδικό όνομα. Πρέπει να αποκτηθούν επαρκή δικαιώματα για κάθε Εφαρμογή που καθίσταται διαθέσιμη για πρόσβαση και χρήση κατά τη διάρκεια της περιόδου μέτρησης που καθορίζεται στην Απόδειξη Δικαιώματος ή στο Έγγραφο Συναλλαγής του Πελάτη.

Για την Υπηρεσία Cloud, εφαρμογή είναι μία μεμονωμένη Επιχειρηματική Εφαρμογή ή Εφαρμογή Λιανικής του Πελάτη.

δ. Δέσμευση (Engagement) είναι μια μονάδα μέτρησης βάσει της οποίας μπορεί να αποκτηθούν οι υπηρεσίες. Μια Δέσμευση αποτελείται από επαγγελματικές ή/και εκπαιδευτικές υπηρεσίες που σχετίζονται με τις Υπηρεσίες Cloud. Πρέπει να αποκτηθούν επαρκή δικαιώματα χρήσης για την κάλυψη κάθε Δέσμευσης.

12. Συμμόρφωση και Έλεγχος

Η πρόσβαση στις Υπηρεσίες Cloud για το IBM Trusteer Fraud Protection υπόκειται σε ένα μέγιστο αριθμό Εφαρμογών, Δικαιούμενων Συμμετεχόντων ή/και Συσκευών Πελάτη, ο οποίος καθορίζεται στο Έγγραφο Συναλλαγής. Ο Πελάτης είναι υπεύθυνος να εξασφαλίζει ότι ο αριθμός Εφαρμογών, Δικαιούμενων Συμμετεχόντων ή/και Συσκευών Πελάτη του δεν υπερβαίνει τη μέγιστη ποσότητα που καθορίζεται στο Έγγραφο Συναλλαγής.

Ενδέχεται να διεξαχθεί έλεγχος από την IBM για την επαλήθευση της συμμόρφωσης με τη μέγιστη ποσότητα Εφαρμογών, Δικαιούμενων Συμμετεχόντων ή/και Συσκευών Πελάτη.

13. Περίοδος Ισχύος και Επιλογές Ανανέωσης

Η περίοδος ισχύος της Υπηρεσίας Cloud αρχίζει κατά την ημερομηνία που η IBM ειδοποιεί τον Πελάτη ότι έχει πρόσβαση στην Υπηρεσία Cloud, όπως τεκμηριώνεται στην Απόδειξη Δικαιώματος. Στην Απόδειξη Δικαιώματος θα καθορίζεται αν η Υπηρεσία Cloud ανανεώνεται αυτόματα, εξακολουθεί να παρέχεται βάσει συνεχόμενης χρήσης ή διακόπτεται στο τέλος της περιόδου ισχύος.

Σε περίπτωση αυτόματης ανανέωσης, εκτός εάν ο Πελάτης παράσχει έγγραφη ειδοποίηση τουλάχιστον 90 ημέρες πριν την ημερομηνία λήξης της περιόδου ισχύος, η Υπηρεσία Cloud θα ανανεώνεται αυτόματα για το χρονικό διάστημα που καθορίζεται στην Απόδειξη Δικαιώματος.

Σε περίπτωση συνεχόμενης χρήσης, η Υπηρεσία Cloud θα εξακολουθεί να είναι διαθέσιμη σε μηνιαία βάση έως ότου ο Πελάτης προβεί σε έγγραφη δήλωση καταγγελίας 90 ημερών. Η Υπηρεσία Cloud θα

εξακολουθεί να είναι διαθέσιμη μέχρι το τέλος του ημερολογιακού μήνα μετά την εν λόγω περίοδο 90 ημερών.

14. Πρόσθετοι Όροι

14.1 Λογισμικό Ενεργοποίησης

Αυτή η Υπηρεσία Cloud περιλαμβάνει λογισμικό ενεργοποίησης, το οποίο επιτρέπεται να χρησιμοποιείται μόνο σε συνάρτηση με τη χρήση της Υπηρεσίας Cloud από τον Πελάτη και μόνο κατά τη διάρκεια της περιόδου ισχύος της Υπηρεσίας Cloud.

14.2 Ετήσια Αύξηση Χρέωσης Συνδρομής για το IBM Trusteer

Η IBM διατηρεί το δικαίωμα να προβαίνει στην αναπροσαρμογή της χρέωσης συνδρομής για τις Υπηρεσίες Cloud. Η αναπροσαρμογή της χρέωσης συνδρομής θα περιλαμβάνεται στις τιμές που παρέχονται στην αντίστοιχη Προσφορά Τιμής για την περίοδο ισχύος της εν λόγω Προσφοράς Τιμής. Ενδέχεται να υπάρχουν πρόσθετες αναπροσαρμογές της χρέωσης συνδρομής, όχι συχνότερα από κάθε δώδεκα (12) μήνες κατά ένα ποσοστό που θα καθορίζεται από την IBM και δεν θα υπερβαίνει το 3%, σε περίπτωση παράτασης της περιόδου ισχύος της Υπηρεσίας Cloud λόγω ανανέωσης ή συνεχόμενης χρήσης. Οι αναπροσαρμογές της χρέωσης συνδρομής δεν συνεπάγεται καμία αλλαγή στα δικαιώματα του Πελάτη να χρησιμοποιεί την Υπηρεσία Cloud ή στο μετρικό σύστημα χρέωσης βάσει του οποίου αποκτά την Υπηρεσία Cloud. Οι Εμπορικοί Συνεργάτες της IBM είναι ανεξάρτητοι από την IBM και αποφασίζουν μονομερώς για τις δικές τους τιμές και τους δικούς τους όρους.

Σημαντικό: Η παρούσα Περιγραφή Υπηρεσιών συντάχθηκε στην αγγλική γλώσσα. Μπορείτε να βρείτε και να εκτυπώσετε αντίγραφο της παρούσας Περιγραφής Υπηρεσιών στην αγγλική από την εξής ιστοσελίδα:

http://www-03.ibm.com/software/sla/sladb.nsf/sla/saas

Η ελληνική μετάφραση παρέχεται μόνο για λόγους διευκόλυνσης. Σε περίπτωση ασυμφωνίας μεταξύ του αγγλικού κειμένου και της ελληνικής του μετάφρασης, το αγγλικό κείμενο υπερισχύει. Εάν για οποιονδήποτε λόγο δεν έχετε πρόσβαση στο αγγλικό κείμενο, παρακαλούμε όπως επικοινωνήσετε με τον τοπικό εκπρόσωπο της IBM προκειμένου να σας το αποστείλουμε άμεσα.