IBM Trusteer Pinpoint Detect

Στην παρούσα Περιγραφή Υπηρεσιών παρέχεται μια περιγραφή της Υπηρεσίας Cloud. Στα αντίστοιχα έγγραφα παραγγελίας παρέχονται πληροφορίες τιμολόγησης και πρόσθετες λεπτομέρειες σχετικά με την παραγγελία του Πελάτη.

1. Υπηρεσία Cloud

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. 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 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. Το IBM Trusteer Pinpoint Detect και το IBM Trusteer Pinpoint Verify χρησιμοποιούνται στο πλαίσιο σύνδεσης στο TMA.

β. Web Script ή/και APIs:

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

Μια συνεδρία Pinpoint μετράται από την αρχή έως το τέλος μιας αλληλεπίδρασης χρήστη. Η συνεδρία ξεκινά μετά την υποβολή των στοιχείων ταυτότητας ή την εναλλακτική επαλήθευση των στοιχείων ταυτότητας στη σελίδα σύνδεσης του πελάτη. Η συνεδρία λήγει όταν λάβει χώρα ένα από τα ακόλουθα συμβάντα:

- Επαναφορά της συνεδρίας με τον κανονικό τρόπο αποσύνδεσης από την εφαρμογή
- Κλείσιμο του προγράμματος πλοήγησης ή της καρτέλας
- Διαγραφή των cookies
- Λήξη συνεδρίας

1.1 Προσφορές

Ο Πελάτης μπορεί να επιλέξει από τις ακόλουθες διαθέσιμες προσφορές.

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

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 μια 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 μια Εφαρμογή Λιανικής.

Αυτή η Υπηρεσία Cloud περιλαμβάνει την παροχή υποστήριξης επιπέδου Standard (όπως ορίζεται στο άρθρο "Τεχνική Υποστήριξη" παρακάτω). Για τη λήψη υποστήριξης επιπέδου Premium, ο Πελάτης πρέπει να αγοράσει την υπηρεσία Pinpoint Standard Premium Support.

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.

Η υπηρεσία μπορεί να αγοραστεί σε πακέτα των 100 Δικαιούμενων Συμμετεχόντων ή σε πακέτα των 100 Συνδέσεων. Σε περίπτωση που ο Πελάτης επιλέξει την αγορά της υπηρεσίας βάσει Συνδέσεων ("by Connections"), ισχύει μια χρέωση Πρόσθετης Εφαρμογής (Additional Application) από την πρώτη εφαρμογή.

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

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 μια 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 (deployment) και προετοιμασίας (set-up), προσαρμοσμένες πολιτικές ασφάλειας, υπηρεσίες διερεύνησης κ.ο.κ. Η υπηρεσία περιλαμβάνει υπηρεσίες υλοποίησης διάρκειας έως 200 ωρών ανά εφαρμογή και υπηρεσίες ανάλυσης ασφάλειας διάρκειας 200 ωρών ανά εφαρμογή μετά την ολοκλήρωση της προετοιμασίας (set-up). Οι εν λόγω υπηρεσίες παρέχονται από προσωπικού υποστήριξης που εξυπηρετεί παράλληλα και άλλους Πελάτες. Οι διαρκείς υπηρεσίες περιλαμβάνουν 20 ώρες συντήρησης υλοποίησης ετησίως ανά εφαρμογή και 100 ώρες έρευνας ασφάλειας ετησίως ανά εφαρμογή. Οποιεσδήποτε πρόσθετες εργασίες υπόκεινται σε μια πρόσθετη χρέωση.

Το Pinpoint Detect μπορεί να καταναλώσει συναλλαγές τόσο από κανάλια φορητών συσκευών και όσο και από διαδικτυακά κανάλια. Σε περίπτωση που περιλαμβάνονται συναλλαγές μέσω φορητών συσκευών, η υπηρεσία Pinpoint παρέχεται βάσει Συνδέσεων ("by Connections"). 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.

Οι υπηρεσίες IBM Trusteer Pinpoint Detect Premium for Retail και IBM Trusteer Pinpoint Detect Premium for Business μπορούν να αγοραστούν σε πακέτα των 100 Δικαιούμενων Συμμετεχόντων ή σε πακέτα των 100 Συνδέσεων. Σε περίπτωση που ο Πελάτης επιλέξει την αγορά της υπηρεσίας βάσει Συνδέσεων ("by Connections"), ισχύει μια χρέωση Πρόσθετης Εφαρμογής (Additional Application) από την πρώτη εφαρμογή.

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.

1.1.3 IBM Trusteer Pinpoint Detect for Connections

Αυτή η Υπηρεσία Cloud παρέχει προστασία και στοχεύει στον εντοπισμό προσπαθειών οικειοποίησης λογαριασμών (account takeover) και στην παράδοση βαθμολογικών στοιχείων αξιολόγησης κινδύνου/εμπιστοσύνης των προγραμμάτων πλοήγησης ή/και των φορητών συσκευών (μέσω του εγγενούς προγράμματος πλοήγησης της φορητής εφαρμογής Πελάτη) που έχουν πρόσβαση σε μια Επιχειρηματική Εφαρμογή ή Εφαρμογή Λιανικής. Η λύση χρησιμοποιεί διάφορους δείκτες κινδύνου αναλύοντας τη συσκευή, τη σύνδεση και τη συμπεριφορά του τελικού χρήστη και συγκρίνοντάς τα με το ιστορικό του χρήστη για την αναγνώριση της ύποπτης χρήσης.

Η Υπηρεσία Cloud μπορεί να καταναλώσει συνδέσεις τόσο από κανάλια φορητών συσκευών όσο και από διαδικτυακά κανάλια. Το IBM Trusteer Pinpoint Detect περιλαμβάνει δικαίωμα χρήσης του IBM Trusteer Mobile SDK, εάν χρειάζεται.

Η Υπηρεσία Cloud είναι διαθέσιμη για αγορά σε πακέτα των 100 Συνδέσεων ανά έτος.

1.2 Προαιρετικές Υπηρεσίες

Για τις Υπηρεσίες Cloud σε αυτό το άρθρο, απαιτείται δικαίωμα χρήσης του IBM Trusteer Pinpoint Detect Premium, του IBM Trusteer Pinpoint Detect Standard ή του IBM Trusteer Pinpoint for Connections.

1.2.1 IBM Trusteer Pinpoint Detect Standard Application

Η Εφαρμογή Πελάτη παραπέμπει σε μια Διαδικτυακή Εφαρμογή ή/και μια Εφαρμογή για Φορητές Συσκευές. Μια Διαδικτυακή Εφαρμογή ομαδοποιεί όλες τις λειτουργίες που προσφέρονται στους Δικαιούμενους Συμμετέχοντες του Πελάτη μέσω διαφόρων ιστοσελίδων από μια οθόνη σύνδεσης ή ταυτοποίησης και παρακολουθούνται ως ενιαία Εφαρμογή στην κονσόλα Trusteer (Trusteer Management Application). Μια Εφαρμογή για Φορητές Συσκευές ομαδοποιεί όλες τις λειτουργίες που προσφέρονται στους Δικαιούμενους Συμμετέχοντες του Πελάτη μέσω ενός προγράμματος λογισμικού που μπορεί να μεταφορτωθεί (downloaded) από ένα κατάστημα εφαρμογών, από μια οθόνη σύνδεσης ή ταυτοποίησης και παρακολουθούνται ως ενιαία Εφαρμογή στην κονσόλα Trusteer (Trusteer Management Application).

Για την ενοποίηση του IBM Trusteer Pinpoint απαιτείται δικαίωμα χρήσης της Εφαρμογής IBM Trusteer Pinpoint για κάθε Εφαρμογή.

- Για την υλοποίηση του IBM Trusteer Pinpoint Detect Standard απαιτείται η απόκτηση δικαιώματος χρήσης του IBM Trusteer Pinpoint Detect Standard Application για κάθε Εφαρμογή.

1.2.2 IBM Trusteer Pinpoint Detect Premium Application

Η Εφαρμογή Πελάτη παραπέμπει σε μια Διαδικτυακή Εφαρμογή ή/και μια Εφαρμογή για Φορητές Συσκευές. Μια Διαδικτυακή Εφαρμογή ομαδοποιεί όλες τις λειτουργίες που προσφέρονται στους Δικαιούμενους Συμμετέχοντες του Πελάτη μέσω διαφόρων ιστοσελίδων από μια οθόνη σύνδεσης ή ταυτοποίησης και παρακολουθούνται ως ενιαία Εφαρμογή στην κονσόλα Trusteer (Trusteer Management Application). Μια Εφαρμογή για Φορητές Συσκευές ομαδοποιεί όλες τις λειτουργίες που προσφέρονται στους Δικαιούμενους Συμμετέχοντες του Πελάτη μέσω ενός προγράμματος λογισμικού που μπορεί να

μεταφορτωθεί (downloaded) από ένα κατάστημα εφαρμογών, από μια οθόνη σύνδεσης ή ταυτοποίησης και παρακολουθούνται ως ενιαία Εφαρμογή στην κονσόλα Trusteer (Trusteer Management Application).

Η υπηρεσία περιλαμβάνει υπηρεσίες υλοποίησης διάρκειας έως 200 ωρών ανά εφαρμογή και υπηρεσίες ανάλυσης ασφάλειας διάρκειας 200 ωρών ανά εφαρμογή μετά την ολοκλήρωση της προετοιμασίας (setup). Οι εν λόγω υπηρεσίες παρέχονται από προσωπικού υποστήριξης που εξυπηρετεί παράλληλα και άλλους Πελάτες. Οι διαρκείς υπηρεσίες περιλαμβάνουν 20 ώρες συντήρησης υλοποίησης ετησίως ανά εφαρμογή και 100 ώρες έρευνας ασφάλειας ετησίως ανά εφαρμογή.

- Για την υλοποίηση του IBM Trusteer Pinpoint Premium απαιτείται η απόκτηση δικαιώματος χρήσης του IBM Trusteer Pinpoint Detect Premium Application για κάθε Εφαρμογή.

1.2.3 IBM Trusteer New Account Fraud for Retail ή/και IBM Trusteer New Account Fraud for Business

Αυτή η υπηρεσία, η οποία καθίσταται διαθέσιμη σε συνδρομητές του Pinpoint, έχει σχεδιαστεί για τον εντοπισμό ανωμαλιών, την επισήμανση ύποπτων δραστηριοτήτων και την αποστολή προειδοποιητικών σημάτων στα αρχικά στάδια της διαδικασίας δημιουργίας νέου λογαριασμού. Η υπηρεσία παρακολουθεί νέους λογαριασμούς προκειμένου να εντοπίζει δραστηριότητες που σχετίζονται με απατηλές πράξεις μέσω τεχνικών δημιουργίας προφίλ λογαριασμών (account profiling) για τροποποιημένους και νέους λογαριασμούς, προειδοποιώντας τον Πελάτη σε πρώιμο στάδιο, μέσω των αναφορών χρήσης που διατίθενται στο TMA, ότι ένας νέος λογαριασμός ενδέχεται να χρησιμοποιείται για παράνομες οικονομικές συναλλαγές ή απατηλές πράξεις.

Το IBM Trusteer New Account Fraud for Retail και το IBM Trusteer New Account Fraud for Business διατίθενται σε πακέτα των 10 Κλήσεων API.

1.2.4 IBM Trusteer Digital Content Pack for Retail ή/και IBM Trusteer Digital Content Pack for Business

Το IBM Trusteer Digital Content Pack επιτρέπει σε αναλυτές ασφάλειας την ενσωμάτωση νέων μοντέλων καταπολέμησης απάτης, ενώ υποστηρίζει πλήρως τη δημιουργία και τροποποίηση μοντέλων ειδικού σκοπού για την άμεση αντιμετώπιση νέων απειλών. Αποτελείται από ένα ευρύ φάσμα κανόνων, εμπεριστατωμένων γνώσεων και πολιτικών που μπορούν να αγοραστούν ως πρόσθετο και δομικό τμήμα της λύσης. Το Digital Content Pack συμβάλλει στην περαιτέρω ενοποίηση των δυνατοτήτων πρόληψης ψηφιακής απάτης της Trusteer και των καναλιών ηλεκτρονικών πληρωμών IBM Safer Payments. Αξιοποιώντας τους ενσωματωμένους κανόνες και τη συγκεκριμένη επιχειρησιακή του λογική, το Digital Content Pack επιτρέπει σε τράπεζες και άλλους χρηματοπιστωτικούς οργανισμούς την περαιτέρω ενίσχυση των υπαρχόντων μηχανισμών εντοπισμού και πρόληψης απάτης τους.

Το IBM Trusteer Digital Content Pack for Retail διατίθεται σε πακέτα των 100 Δικαιούμενων Συμμετεχόντων. Το IBM Trusteer Digital Content Pack for Business διατίθεται σε πακέτα των 10 Δικαιούμενων Συμμετεχόντων.

Απαιτούνται συμβουλευτικές υπηρεσίες για την ενοποίηση του Digital Content Pack με το Pinpoint Detect και το IBM Safer Payments, καθώς και για τις υπηρεσίες υποστήριξης που απαιτούν ιδιαίτερη προσοχή. Οι συμβουλευτικές υπηρεσίες αποκτώνται χωριστά βάσει μιας χωριστής Περιγραφής Έργου.

1.2.5 IBM Trusteer Pinpoint Malware Detection

Σε περίπτωση που εντοπιστεί επιβλαβής κώδικας από τις Υπηρεσίες Cloud IBM Trusteer Pinpoint Malware 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 II 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 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).

1.2.6 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 αλληλεπιδράσεις 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:

Οι Εκδόσεις Standard για Επιχειρηματική Χρήση (for Business) ή/και για Λιανική Χρήση (for Retail) είναι άμεσα υλοποιήσιμες λύσεις που παρέχουν 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.

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

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

1.2.8 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 II, το οποίο πρέπει να 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. Για τους σκοπούς της παρούσας Περιγραφής Υπηρεσιών, ο "Κάτοχος Λογαριασμού" είναι 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 κάλυψη της οποίας ο Πελάτης έχει προμηθευτεί συνδρομή για την Υπηρεσία Cloud. Το "Λογισμικό Πελάτη για Κάτοχο Λογαριασμού" είναι το λογισμικό ενεργοποίησης πελάτη IBM Trusteer Rapport ή οποιοδήποτε άλλο λογισμικό ενεργοποίησης πελάτη που παρέχεται με ορισμένες Υπηρεσίες Cloud για εγκατάσταση στη συσκευή του τελικού χρήστη.

1.2.9 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 Retail ή το IBM Trusteer Pinpoint Malware Detection Advanced Edition II for Retail, προϋπόθεση για την υλοποίηση οποιασδήποτε πρόσθετης Εφαρμογής Λιανικής επιπλέον της πρώτης Εφαρμογής είναι η απόκτηση δικαιώματος χρήσης του IBM Trusteer Pinpoint Malware Detection Additional Applications for Retail.
- 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 οποιασδήποτε πρόσθετης Επιχειρηματικής Εφαρμογή επιπλέον της πρώτης Εφαρμογής είναι η απόκτηση δικαιώματος χρήσης του IBM Trusteer Pinpoint Malware Detection Additional Applications for Business.

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

- Το IBM Trusteer Rapport for Mitigation for Retail 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.
- Το IBM Trusteer Rapport for Mitigation for Business στοχεύει στη διερεύνηση, αντιμετώπιση, αποτροπή και αφαίρεση μολύνσεων από επιβλαβή κώδικα από μολυσμένες συσκευές (PC/MAC) Δικαιούμενων Συμμετεχόντων του Πελάτη που αποκτούν πρόσβαση στην Επιχειρηματική Εφαρμογή 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 Επιχειρηματική Εφαρμογή του Πελάτη. Ο Πελάτης επιτρέπεται να χρησιμοποιεί αυτή την Υπηρεσία Cloud μόνο σε συνάρτηση με Δικαιούμενους Συμμετέχοντες που αποκτούν πρόσβαση στην Επιχειρηματική 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 for Mitigation for Business 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 Επιχειρηματική Εφαρμογή 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.

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

- Για το IBM Trusteer Pinpoint Detect Standard for Retail, προϋπόθεση για την υλοποίηση οποιασδήποτε πρόσθετης Εφαρμογής 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 Detect Standard for Business, προϋπόθεση για την υλοποίηση οποιασδήποτε πρόσθετης Επιχειρηματικής Εφαρμογής επιπλέον της πρώτης Εφαρμογής είναι η απόκτηση δικαιώματος χρήσης του IBM Trusteer Pinpoint Detect Standard Additional Applications for Business.

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

Η υπηρεσία περιλαμβάνει υπηρεσίες υλοποίησης διάρκειας έως 200 ωρών ανά εφαρμογή και υπηρεσίες ανάλυσης ασφάλειας διάρκειας 200 ωρών ανά εφαρμογή μετά την ολοκλήρωση της προετοιμασίας (setup). Οι εν λόγω υπηρεσίες παρέχονται από προσωπικού υποστήριξης που εξυπηρετεί παράλληλα και άλλους Πελάτες. Οι διαρκείς υπηρεσίες περιλαμβάνουν 20 ώρες συντήρησης υλοποίησης ετησίως ανά εφαρμογή και 100 ώρες έρευνας ασφάλειας ετησίως ανά εφαρμογή.

- Για το IBM Trusteer Pinpoint Premium for Retail, προϋπόθεση για την υλοποίηση οποιασδήποτε πρόσθετης Εφαρμογής Λιανικής επιπλέον της πρώτης Εφαρμογής είναι η απόκτηση δικαιώματος χρήσης του IBM Trusteer Pinpoint Detect Premium Additional Applications for Retail.
- Για το IBM Trusteer Pinpoint Premium for Business, προϋπόθεση για την υλοποίηση οποιασδήποτε πρόσθετης Επιχειρηματικής Εφαρμογής επιπλέον της πρώτης Εφαρμογής είναι η απόκτηση δικαιώματος χρήσης του IBM Trusteer Pinpoint Detect Premium Additional Applications for Business.

1.2.13 IBM Trusteer Pinpoint Detect Standard for Retail Premium Support ή/και IBM Trusteer Pinpoint Detect Standard for Business Premium Support

Οι Πελάτες που αγοράζουν την Υπηρεσία Cloud Pinpoint Detect Standard μπορούν να αγοράσουν την υπηρεσία Premium Support. Το εύρος των υπηρεσιών Premium Support περιγράφεται στο παρακάτω άρθρο 4.

1.2.14 IBM Trusteer Mobile Carrier Intelligence for Pinpoint Detect

Ο Πελάτης πρέπει να διαθέτει μια ισχύουσα συνδρομή για το IBM Trusteer Pinpoint Detect πριν προμηθευτεί μια συνδρομή για αυτή την Υπηρεσία Cloud.

Αυτή η Υπηρεσία Cloud βελτιώνει το IBM Trusteer Pinpoint Detect παρέχοντας πρόσθετες πληροφορίες και δεδομένα για τους αριθμούς κινητού τηλεφώνου που παρέχονται σε οποιαδήποτε από αυτές τις Υπηρεσίες Cloud, βοηθώντας έτσι στον προσδιορισμό των κινδύνων απάτης για μια δεδομένη συνεδρία. Ο Πελάτης μπορεί να υποβάλει αιτήσεις πληροφοριών (queries) στην Υπηρεσία Cloud προκειμένου να ενημερωθεί για τα χαρακτηριστικά ενός δεδομένου αριθμού κινητού τηλεφώνου, όπως π.χ. πληροφορίες για τον πάροχο υπηρεσιών κινητής τηλεφωνίας που αντιστοιχεί στον αριθμό.

Τα δεδομένα που παρέχονται από αυτή την Υπηρεσία Cloud για αριθμούς κινητού τηλεφώνου ("Πληροφορίες Κινητής Τηλεφωνίας") επιτρέπεται να χρησιμοποιούνται μόνο για εσωτερικούς σκοπούς του οργανισμού του Πελάτη και να διατηρούνται για μια χρονική περίοδο που δεν υπερβαίνει τις τριάντα (30) ημέρες. Ο Πελάτης πρέπει να υποβάλει μια νέα αίτηση πληροφοριών στην Υπηρεσία Cloud για τον ίδιο αριθμό κινητού τηλεφώνου μετά την εν λόγω χρονική περίοδο προκειμένου να αποκτήσει Πληροφορίες Κινητής Τηλεφωνίας για το συγκεκριμένο αριθμό και δεν του επιτρέπεται να χρησιμοποιήσει απλώς τις Πληροφορίες Κινητής Τηλεφωνίας που ελήφθησαν μετά την υποβολή μιας παλιότερης αίτησης πληροφοριών. Ο Πελάτης δεν επιτρέπεται να προβεί στην αποθήκευση, παρά μόνο στο βαθμό που επιτρέπεται ανωτέρω, ή επαναχρησιμοποίηση Πληροφοριών Κινητής Τηλεφωνίας, ή χρησιμοποιήσει Πληροφορίες Κινητής Τηλεφωνίας, εν όλω ή εν μέρει, σε συνάρτηση με οποιαδήποτε δραστηριότητα

εξόρυξης δεδομένων (data mining) και δεν επιτρέπεται η αρχειοθέτηση οποιωνδήποτε Πληροφοριών Κινητής Τηλεφωνίας.

1.3 Υπηρεσίες Επιτάχυνσης

1.3.1 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.

1.3.2 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 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.

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

2. Φύλλα Δεδομένων για την Επεξεργασία και Προστασία Δεδομένων

Η Πρόσθετη Πράξη για την Επεξεργασία Δεδομένων (Data Processing Addendum - Πρόσθετη Πράξη DPA) της IBM, που διατίθεται στην ιστοσελίδα http://ibm.com/dpa, και το(-α) Φύλλο(-α) Δεδομένων για την Επεξεργασία και Προστασία Δεδομένων (τα οποία αναφέρονται ως φύλλο(-α) δεδομένων ή Παράρτημα(-τα) DPA), που διατίθενται στις ιστοσελίδες που παραπέμπουν οι παρακάτω διασυνδέσεις, παρέχουν πρόσθετες πληροφορίες για την προστασία δεδομένων στις Υπηρεσίες Cloud και τις επιλογές που παρέχουν οι Υπηρεσίες Cloud για τα είδη Περιεχομένου που μπορεί να υφίστανται επεξεργασία, τις δραστηριότητες επεξεργασίας και τις λειτουργίες προστασίας δεδομένων καθώς και τη διατήρηση και επιστροφή Περιεχομένου. Η Πρόσθετη Πράξη DPA διέπει τα δεδομένα προσωπικού χαρακτήρα που περιλαμβάνονται στο Περιεχόμενο, εάν και στο βαθμό που ισχύουν i) ο Ευρωπαϊκός Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) (ΕΕ/2016/679) ή ii) άλλοι νόμοι περί προστασίας δεδομένων που προσδιορίζονται στην ιστοσελίδα http://ibm.com/dpa/dpl.

Διευκρινίζεται ότι τα Φύλλα Δεδομένων αναγράφουν γενικά όλες τις τοποθεσίες στις οποίες η IBM (συμπεριλαμβανομένων οποιωνδήποτε τρίτων υπεργολάβων που εκτελούν επεξεργασία) φιλοξενεί και επεξεργάζεται Δεδομένα Προσωπικού Χαρακτήρα, ανεξάρτητα από το κέντρο πληροφοριακών συστημάτων από το οποίο υλοποιούνται οι υπηρεσίες. Για μια λίστα των τοποθεσιών φιλοξενίας και επεξεργασίας για το συγκεκριμένο κέντρο πληροφοριακών συστημάτων από το οποίο υλοποιούνται οι υπηρεσίες, ανατρέξτε παρακάτω στο Άρθρο 5.2 (Πρόσθετες Πληροφορίες για τις Τοποθεσίες Επεξεργασίας).

IBM Trusteer Pinpoint Criminal Detect

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

IBM Trusteer Pinpoint Detect

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

IBM Trusteer Pinpoint Malware Detection

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

IBM Trusteer Mobile SDK

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

3. Επίπεδα Παροχής Υπηρεσιών και Τεχνική Υποστήριξη

3.1 Σύμβαση Επιπέδου Παροχής Υπηρεσιών (SLA)

Η IBM παρέχει στον Πελάτη την ακόλουθη σύμβαση επιπέδου παροχής υπηρεσιών (SLA). Η IBM θα παρέχει την υψηλότερη ισχύουσα αποζημίωση με βάση τη σωρευτική διαθεσιμότητα της Υπηρεσίας Cloud, όπως αναφέρεται στον παρακάτω πίνακα. Το ποσοστό διαθεσιμότητας υπολογίζεται ως ο συνολικός αριθμός λεπτών σε ένα συμβατικό μήνα, μείον το συνολικό αριθμό λεπτών του Χρόνου Διακοπής της Υπηρεσίας κατά τη διάρκεια του συμβατικού μήνα, διαιρούμενος διά του συνολικού αριθμού λεπτών στο συμβατικό μήνα. Ο ορισμός του Χρόνου Διακοπής Υπηρεσίας, η διαδικασία για την έγερση αξιώσεων πίστωσης και ο τρόπος επικοινωνίας με την IBM για ζητήματα διαθεσιμότητας υπηρεσιών αναφέρονται στον Οδηγό Υποστήριξης Υπηρεσιών Cloud (Cloud Service Support Guide) της IBM που διατίθεται στην ιστοσελίδα https://www.ibm.com/software/support/saas_support_overview.html.

Διαθεσιμότητα	Credit (% της μηνιαίας χρέωσης συνδρομής*)
Χαμηλότερη από 99,9%	2%
Χαμηλότερη από 99,0%	5%
Χαμηλότερη από 95,0%	10%

* Η χρέωση συνδρομής είναι η συμβατικά προβλεπόμενη τιμή για το μήνα που αποτελεί το αντικείμενο της αξίωσης.

3.2 Τεχνική Υποστήριξη

Για πληροφορίες σχετικά με την τεχνική υποστήριξη που παρέχεται για την Υπηρεσία Cloud, συμπεριλαμβανομένων στοιχείων επικοινωνίας για τη λήψη υποστήριξης, των βαθμών κρισιμότητας, των χρόνων απόκρισης και άλλων πληροφοριών και διαδικασιών υποστήριξης, επιλέξτε την Υπηρεσία Cloud στον οδηγό υποστήριξης της IBM (IBM support guide) στην ιστοσελίδα https://www.ibm.com/support/home/pages/support-guide/.

Υποστήριξη επιπέδου Premium (Premium Support):

Μια συνδρομή Υποστήριξης Επιπέδου Premium διατίθεται για την Υπηρεσία Cloud έναντι πρόσθετης χρέωσης και περιλαμβάνει:

- 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 υποθέσεων και απαντήσεις σε συχνές ερωτήσεις στη διεύθυνση: http://www.ibm.com/software/security/trusteer/support/.

4. Χρεώσεις

4.1 Μετρικά Συστήματα Χρέωσης

Τα μετρικά συστήματα χρέωσης για την Υπηρεσία Cloud καθορίζονται στο Έγγραφο Συναλλαγής.

Χρησιμοποιούνται τα ακόλουθα μετρικά συστήματα χρέωσης για αυτή την Υπηρεσία Cloud:

- Δέσμευση (Engagement) είναι μια επαγγελματική ή εκπαιδευτική υπηρεσία που σχετίζεται με τις Υπηρεσίες Cloud.
- Δικαιούμενος Συμμετέχων (Eligible Participant) είναι ένα φυσικό ή νομικό πρόσωπο που πληροί τις προϋποθέσεις για συμμετοχή σε οποιοδήποτε πρόγραμμα παράδοσης υπηρεσιών που βρίσκεται υπό τη διαχείριση ή παρακολούθηση των Υπηρεσιών Cloud.
- Εφαρμογή (Application) είναι ένα πρόγραμμα λογισμικού με μοναδικό όνομα που αναπτύχθηκε ή καθίσταται διαθέσιμη για την πρόσβαση στις Υπηρεσίες Cloud ή για χρήση από τις Υπηρεσίες Cloud.
- Κλήση API (API Call) είναι η ενεργοποίηση των Υπηρεσιών Cloud μέσω μιας διεπαφής προγραμματισμού.
- Σύνδεση (Connection) είναι μια διασύνδεση ή συσχέτιση μιας βάσης δεδομένων, μιας εφαρμογής, ενός εξυπηρετητή (server) ή οποιουδήποτε άλλου τύπου συσκευής που καθίσταται ή έχει καταστεί διαθέσιμη στην Υπηρεσία Cloud.

4.2 Χρεώσεις για Εξ Αποστάσεως Υπηρεσίες

Μια εξ αποστάσεως παραδιδόμενη υπηρεσία θα λήξει 90 ημέρες από την ημερομηνία αγοράς της, ανεξάρτητα από το εάν η εξ αποστάσεως παραδιδόμενη υπηρεσία έχει χρησιμοποιηθεί.

5. Πρόσθετοι Όροι

Για τις Συμβάσεις Υπηρεσιών Cloud (ή ισοδύναμες βασικές συμβάσεις cloud) που συνάφθηκαν πριν την 1η Ιανουαρίου 2019, ισχύουν οι όροι που αναφέρονται στον ιστότοπο https://www.ibm.com/acs.

5.1 Σύμβαση EULA και Βάση για την Επεξεργασία Δεδομένων των Υποκειμένων των Δεδομένων

Για τις Υπηρεσίες Cloud IBM Trusteer Rapport (συμπεριλαμβανομένων του Rapport Remediation και του Rapport for Mitigation όταν υλοποιείται σε συνδυασμό με τις Υπηρεσίες Cloud Pinpoint): Εκτός εάν άλλως συμφωνηθεί και σύμφωνα με τη βάση για την επεξεργασία δεδομένων που έχει ορίσει ανεξάρτητα ο Πελάτης, ο Πελάτης εξουσιοδοτεί την IBM να παρέχει στους τελικούς χρήστες τη Σύμβαση Άδειας Χρήσης Τελικού Χρήστη (End User License Agreement - "Σύμβαση EULA") που διατίθεται στην ιστοσελίδα https://trusteer.secure.force.com/PKB/articles/en_US/FAQ/RAPPORT-DATA-PRIVACY-NOTICE-AND-END-USER-LICENSE-AGREEMENT-EULA, προκειμένου να παρέχει στην IBM τη δυνατότητα να συλλέγει και να επεξεργάζεται τις πληροφορίες που είναι απαραίτητες για την παροχή των Υπηρεσιών Cloud.

Για τις Υπηρεσίες Cloud IBM Trusteer Rapport, ο Πελάτης εξουσιοδοτεί την IBM, ως εκτελούντα την επεξεργασία δεδομένων για την Επιχείρηση-Χορηγό, να χρησιμοποιεί το Πρόγραμμα για τη συλλογή επιβλαβούς κώδικα και τεχνουργημάτων επιβλαβούς κώδικα (δηλαδή, αρχείων που σχετίζονται με κακόβουλες δραστηριότητες ή με τη γενική δυσλειτουργία του Προγράμματος). Η IBM δεν χρησιμοποιεί το Πρόγραμμα με σκοπό την ανάκτηση πληροφοριών από αρχεία που περιέχουν πληροφορίες προσωπικού χαρακτήρα του τελικού χρήστη. Όμως, τα αρχεία που συλλέγονται ενδέχεται να περιέχουν δεδομένα προσωπικού χαρακτήρα του τελικού χρήστη που έχουν συγκεντρωθεί από επιβλαβή κώδικα χωρίς την έγκρισή του. Η IBM θα προβαίνει 1) στην άμεση διαγραφή αρχείων που δεν σχετίζονται με την εν λόγω ανάλυση, και 2) στη διατήρηση σχετικών αρχείων μόνο για τη διάρκεια της ανάλυσης και σε καμία περίπτωση για χρονικό διάστημα που υπερβαίνει τους τρεις μήνες.

5.2 Πρόσθετες Πληροφορίες για τις Τοποθεσίες Επεξεργασίας

Όλες οι εργασίες φιλοξενίας και επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα, συμπεριλαμβανομένων οποιωνδήποτε τρίτων υπεργολάβων που εκτελούν επεξεργασία και προσδιορίζονται στο Φύλλο Δεδομένων, θα πραγματοποιούνται στις τοποθεσίες που ορίζονται παρακάτω:

Για όλες τις υπηρεσίες που παρέχονται μέσω του κέντρου πληροφοριακών συστημάτων στη Γερμανία, η IBM θα περιορίζει τη φιλοξενία και την επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα στη χώρα του συμβαλλόμενου νομικού προσώπου IBM και στις ακόλουθες χώρες: Γερμανία, Ισραήλ, Ιρλανδία και Ολλανδία.

Για όλες τις υπηρεσίες που παρέχονται μέσω του κέντρου πληροφοριακών συστημάτων στην Ιαπωνία, η IBM θα περιορίζει τη φιλοξενία και την επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα στη χώρα του συμβαλλόμενου νομικού προσώπου IBM και στις ακόλουθες χώρες: Ιαπωνία, Ισραήλ και Ιρλανδία.

Για όλες τις υπηρεσίες που παρέχονται μέσω του κέντρου πληροφοριακών συστημάτων στις Η.Π.Α., η IBM θα περιορίζει τη φιλοξενία και την επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα στη χώρα του συμβαλλόμενου νομικού προσώπου IBM και στις ακόλουθες χώρες: Η.Π.Α., Ισραήλ, Ιρλανδία, Σιγκαπούρη και Αυστραλία.

Εκτός των τοποθεσιών που αναφέρθηκαν παραπάνω, για όλες τις υπηρεσίες που παρέχονται μέσω των κέντρων πληροφοριακών συστημάτων στη Γερμανία, την Ιαπωνία και τις Η.Π.Α., (1) τα δεδομένα υποστήριξης μπορεί να φιλοξενούνται και να υποβάλλονται σε επεξεργασία στη Γερμανία και τη Γαλλία από την Salesforce.Com ως τρίτο υπεργολάβο της IBM που εκτελεί επεξεργασία, και (2) για τους πελάτες που επιλέγουν να αποστέλλουν δεδομένα σε παρόχους υπηρεσιών Mobile Carrier Intelligence, τα Δεδομένα Προσωπικού Χαρακτήρα μπορεί να φιλοξενούνται και να υποβάλλονται σε επεξεργασία στις χώρες των αντίστοιχων υπεργολάβων που εκτελούν επεξεργασία σύμφωνα με το Φύλλο Δεδομένων. Παρά τα όσα προβλέπονται περί του αντιθέτου στο Φύλλο Δεδομένων, οι οριζόμενοι στη διάταξη (2) της παραπάνω πρότασης τρίτοι υπεργολάβοι που εκτελούν επεξεργασία μπορεί να μην συμμορφώνονται με το πρότυπο ISO 27001 ή SOC2.

Επιπλέον, ενδέχεται να παρέχονται υπηρεσίες υποστήριξης και συντήρησης των λογαριασμών IBM Trusteer όποτε είναι απαραίτητο, ανάλογα με τη διαθεσιμότητα του απαιτούμενου προσωπικού της IBM, την τοποθεσία του Πελάτη και το κέντρο πληροφοριακών συστημάτων όπου φιλοξενούνται τα δεδομένα.

5.3 Δεδομένα Κατόχου Λογαριασμού

Διευκρινίζεται ότι, αν υπάρχουν περισσότεροι από ένας πελάτες της IBM που συνδέονται με το Λογισμικό Πελάτη για Κάτοχο Λογαριασμού (οι εν λόγω πελάτες της IBM αναφέρονται ως "Συνδεδεμένοι Πελάτες") και οι υπηρεσίες βάσει της παρούσας Περιγραφής Υπηρεσιών παρέχονται από την IBM στους εν λόγω Συνδεδεμένους Πελάτες μέσω κέντρων πληροφοριακών συστημάτων σε διαφορετικές περιοχές, τα δεδομένα του Κατόχου Λογαριασμού μπορεί να υποβάλλονται σε επεξεργασία σε κάποιες ή όλες τις τοποθεσίες που σχετίζονται με τα αντίστοιχα κέντρα πληροφοριακών συστημάτων, όπως ορίζεται στο Άρθρο 5.2.

5.4 Ολοκληρωμένες Λύσεις

Διευκρινίζεται ότι οι διάφορες προσφορές υπό την εμπορική επωνυμία Trusteer μπορούν να αποτελέσουν μια ολοκληρωμένη λύση. Ως εκ τούτου, αν ο Πελάτης διακόψει τη χρήση οποιασδήποτε από αυτές τις Υπηρεσίες Cloud, η IBM μπορεί να διατηρήσει τα δεδομένα του Πελάτη με σκοπό την παροχή στον Πελάτη των υπόλοιπων Υπηρεσιών Cloud βάσει της παρούσας Περιγραφής Υπηρεσιών καθώς και άλλων υπηρεσιών Trusteer βάσει των Περιγραφών Υπηρεσιών που ισχύουν για τις εν λόγω υπηρεσίες Trusteer.

5.5 Λογισμικό Ενεργοποίησης

Η Υπηρεσία Cloud περιέχει το ακόλουθο Λογισμικό Ενεργοποίησης:

- IBM Rapport Agents

5.6 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).

5.7 Δεδομένα που συλλέγονται κατά την υλοποίηση

Η υλοποίηση της Υπηρεσίας Cloud ενδέχεται να συνεπάγεται την παροχή ορισμένων δεδομένων στην IBM από τον Πελάτη. Τα εν λόγω δεδομένα δεν πρέπει να περιλαμβάνουν πληροφορίες που μπορούν να προσδιορίσουν ή να αντιστοιχιστούν με συγκεκριμένα άτομα. Οι οδηγίες σχετικά με τα δεδομένα που παρέχονται στην IBM κατά την ανάπτυξη περιλαμβάνονται στις Οδηγίες Υλοποίησης Trusteer που παρέχονται στον Πελάτη.

6. Υπερισχύοντες Όροι

6.1 Χρήση Δεδομένων

Η ακόλουθη διάταξη υπερισχύει των όσων προβλέπονται περί του αντιθέτου στο άρθρο Προστασία Περιεχομένου και Δεδομένων στους βασικούς όρους για Υπηρεσίες Cloud που έχουν υπογράψει τα συμβαλλόμενα μέρη: Η IBM δεν θα χρησιμοποιεί και δεν θα αποκαλύπτει τα αποτελέσματα που προκύπτουν από τη χρήση της Υπηρεσίας Cloud από τον Πελάτη τα οποία θα είναι μοναδικά για το Περιεχόμενο του Πελάτη (Εμπεριστατωμένες Γνώσεις) ή από τα οποία μπορεί να προκύψει κατά άλλον τρόπο η ταυτότητα του Πελάτη. Όμως, η IBM θα κάνει χρήση Περιεχομένου και άλλων πληροφοριών που προκύπτουν από Περιεχόμενο στο πλαίσιο της Υπηρεσίας Cloud υπό την προϋπόθεση ότι έχουν αφαιρεθεί πληροφορίες από τις οποίες μπορεί να προκύψει η ταυτότητα συγκεκριμένων προσώπων, με τέτοιον τρόπο ώστε να μην είναι πλέον δυνατή η συσχέτιση δεδομένων προσωπικού χαρακτήρα με ένα συγκεκριμένο πρόσωπο χωρίς τη χρήση πρόσθετων πληροφοριών. Η IBM θα χρησιμοποιεί τέτοια δεδομένα μόνο για ερευνητικούς σκοπούς, για τη διενέργεια δοκιμών και για την ανάπτυξη προσφορών.

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.