

IBM Resilient Security Orchestration, Automation and Response on Cloud

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 Resilient Security Orchestration, Automation, and Response (SOAR) Platform on Cloud επιτρέπει σε οργανισμούς να ενορχηστρώνουν και να αυτοματοποιούν τα πρόσωπα, τις διαδικασίες και την τεχνολογία που σχετίζονται με την απόκριση σε περιστατικά.

Το IBM Resilient SOAR Platform on Cloud διασφαλίζει την αποτελεσματική διαχείριση της απόκρισης σε περιστατικά ασφάλειας και ζητήματα προστασίας δεδομένων προσωπικού χαρακτήρα, παρέχοντας έναν αυτοματοποιημένο, ταχύτερο και πιο ευέλικτο τρόπο για την αντιμετώπιση συμβάντων και περιστατικών. Το Resilient SOAR Platform on Cloud παρέχει την απαραίτητη υποδομή για την επιτυχή προστασία της ασφάλειας στον κυβερνοχώρο, επιτρέποντας στους οργανισμούς να κάνουν τα εξής:

- Δημιουργία σχεδίων αντιμετώπισης περιστατικών που βασίζονται στα πρότυπα και τις βέλτιστες πρακτικές του κλάδου.
- Εύκολη ενσωμάτωση εργαλείων ασφάλειας και πληροφορικής και ενορχήστρωση της απόκρισης σε συμβάντα και περιστατικά.
- Συνεργασία μεταξύ των χρηστών του οργανισμού, παρέχοντας στους διάφορους ενδιαφερόμενους τα εργαλεία που τους επιτρέπουν να αναλάβουν το δικό τους ρόλο και να προβούν στις απαραίτητες ενέργειες προκειμένου να συμβάλουν στην αποτελεσματική αντιμετώπιση ενός περιστατικού.

Το IBM Resilient SOAR Platform έχει σχεδιαστεί για οργανισμούς διαφορετικών μεγεθών και διαφορετικών βαθμών πολυπλοκότητας και μπορεί να αγοραστεί με διάφορες προαιρετικές πρόσθετες (add-on) υπηρεσίες. Ο Πελάτης δεν επιτρέπεται να χρησιμοποιεί λειτουργίες που δεν καθορίζονται ρητώς στην προσφορά ή στην πρόσθετη υπηρεσία που έχουν αγοράσει.

1.1 Προσφορές

Ο Πελάτης μπορεί να επιλέξει από τις ακόλουθες διαθέσιμες προσφορές:

1.1.1 IBM Resilient SOAR Platform on Cloud

Το IBM Resilient SOAR Platform on Cloud Orchestration παρέχει την απαραίτητη υποδομή για την προστασία της ασφάλειας στον κυβερνοχώρο. Οι Πελάτες μπορούν να δημιουργήσουν σχέδια αντιμετώπισης περιστατικών που βασίζονται στα πρότυπα και τις βέλτιστες πρακτικές του κλάδου, να ενσωματώσουν άλλα εργαλεία ασφάλειας και πληροφορικής και να ενορχηστρώσουν την απόκριση σε συμβάντα και περιστατικά. Η Υπηρεσία Cloud επιτρέπει τη συνεργασία μεταξύ των χρηστών του οργανισμού, όπου οι διάφοροι ενδιαφερόμενοι μπορούν να αναλάβουν το δικό τους ρόλο ώστε να συμβάλουν στην αντιμετώπιση ενός περιστατικού.

Οι ομάδες ασφάλειας μπορούν να συνεργαστούν στην αντιμετώπιση συμβάντων και περιστατικών ασφάλειας στον κυβερνοχώρο χρησιμοποιώντας τις ενσωματωμένες δυνατότητες διαχείρισης υποθέσεων της πλατφόρμας. Η λειτουργία Dynamic Playbooks επιτρέπει την άμεση προσαρμογή σε νέες απειλές και στις ομάδες ασφάλειας παρέχεται η δυνατότητα αναπροσαρμογής των διαδικασιών που ακολουθούν προκειμένου να βελτιώσουν την αποτελεσματικότητα της αντιμετώπισης των εν λόγω απειλών, προσαρμόζοντας σενάρια (playbooks), πεδία δεδομένων και τη διάταξη οθονών. Οι διαδικασίες για την απόκριση σε περιστατικά ασφάλειας μπορούν να βελτιωθούν περαιτέρω με τη διενέργεια προσομοιώσεων. Οι ενσωματωμένες και εγκαθιστώμενες δυνατότητες ενοποίησης επιτρέπουν τον εμπλουτισμό δεδομένων για την υποστήριξη της λήψης αποφάσεων και της ενορχήστρωση διορθωτικών ενεργειών από την ομάδα ασφάλειας, σύμφωνα με τη ποσότητα Ενεργειών ανά Μήνα που αντιστοιχεί στη συνδρομή που αγοράστηκε. Η δυνατότητα τροφοδότησης και ανάλυσης μηνυμάτων email επιτρέπει την εύκολη προώθηση δεδομένων από άλλα εργαλεία. Η πρόσβαση στην υπηρεσία μπορεί να ελέγχεται μέσω ταυτοποίησης SAML. Η διαφάνεια και η ανάλυση κινδύνων υποστηρίζονται από λειτουργίες ανάλυσης και αναφοράς δεδομένων. Η αγορά αυτής της προσφοράς αποτελεί απαραίτητη προϋπόθεση για όλες τις άλλες πρόσθετες υπηρεσίες που αναφέρονται παρακάτω.

1.2 Προαιρετικές Υπηρεσίες

1.2.1 IBM Resilient SOAR Platform Actions on Cloud

Το IBM Resilient SOAR Platform on Cloud Actions υποστηρίζει τις δυνατότητες ενορχήστρωσης της πλατφόρμας. Οι ενσωματωμένες και εγκαθιστώμενες δυνατότητες ενοποίησης με διάφορες τροφοδοσίες πληροφοριών για απειλές, επιτρέπουν τον αυτοματοποιημένο εμπλουτισμό δεδομένων για την υποστήριξη της λήψης αποφάσεων και της ενορχήστρωσης διορθωτικών ενεργειών από την ομάδα ασφάλειας.

1.2.2 IBM Resilient SOAR Platform on Cloud Privacy Add-On

Το IBM Resilient SOAR Platform on Cloud Privacy παρέχει στον Πελάτη τη δυνατότητα αποτίμησης και αντιμετώπισης παραβιάσεων δεδομένων προσωπικού χαρακτήρα. Τα σχέδια αντιμετώπισης περιστατικών που δημιουργούνται με χρήση αυτής της προσφοράς προσαρμόζονται ανάλογα με τα είδη δεδομένων, τις ποσότητες στοιχείων και τις ισχύουσες ρυθμιστικές δικαιοδοσίες. Οι Πελάτες έχουν επίσης πρόσβαση σε μια ενσωματωμένη γνωσιακή βάση δεδομένων με τις διατάξεις των διεθνών κανονισμών για τη γνωστοποίηση περιστατικών παραβίασης δεδομένων προσωπικού χαρακτήρα, η οποία συμβάλλει στην περαιτέρω αναπροσαρμογή των σχεδίων αντιμετώπισης περιστατικών.

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

Το IBM Resilient SOAR Platform on Cloud Teams παρέχει τη δυνατότητα διαχείρισης χρηστών και κατάτμησης δεδομένων μεταξύ διαφορετικών ομάδων. Η πρόσβαση σε ευαίσθητες πληροφορίες ελέγχεται με τη χρήση χώρων εργασίας και τον έλεγχο πρόσβασης βάσει ρόλων, έτσι ώστε οι πληροφορίες αυτές να είναι προσβάσιμες μόνο από άτομα που πρέπει να τις γνωρίζουν. Για την πιο απλή διαχείριση χρηστών και ομάδων μπορεί να χρησιμοποιηθεί το Active Directory για την ταυτοποίηση χρηστών. Επίσης παρέχεται η δυνατότητα ορισμού ξεχωριστών ομάδων που έχουν τον δικό τους Οργανισμό.

1.2.4 IBM Resilient SOAR Platform on Cloud MSSP Add-On

Το IBM Resilient SOAR Platform on Cloud MSSP παρέχει δυνατότητες διαχείρισης υποθέσεων, επεξεργασίας, προσαρμογής και σεναρίων για διαφορετικούς Οργανισμούς. Τα συμβάντα και τα περιστατικά διαφορετικών Οργανισμών μπορούν να προβληθούν σε μία ενιαία ουρά συμβάντων, επιτρέποντας έτσι σε αναλυτές παρόχων υπό διαχείριση υπηρεσιών ασφάλειας (managed security service providers - MSSP) να σχηματίσουν μια ολοκληρωμένη εικόνα των πελατών τους. Τα σενάρια (playbooks), τα οποία παραμετροποιούνται ανά οργανισμό, αποτελούν έναν εύχρηστο τρόπο διαχείρισης τυποποιημένων και προσαρμοσμένων διεργασιών.

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

Το IBM Resilient SOAR Platform on Cloud Non-Production είναι μια ξεχωριστή περίπτωση χρήσης του IBM Resilient SOAR Platform την οποία επιτρέπεται να χρησιμοποιεί ο Πελάτης μόνο για την εκτέλεση εσωτερικών μη παραγωγικών δραστηριοτήτων, συμπεριλαμβανομένων, ενδεικτικά και όχι περιοριστικά, δραστηριοτήτων διενέργειας δοκιμών, ρύθμισης απόδοσης, διάγνωσης σφαλμάτων, εσωτερικής συγκριτικής αξιολόγησης απόδοσης (benchmarking), δοκιμαστικής εφαρμογής (stating) και διασφάλισης ποιότητας ή/και για την ανάπτυξη εσωτερικά χρησιμοποιούμενων προσθηκών ή επεκτάσεων της Υπηρεσίας Cloud με τη χρήση δημοσιευμένων API (application programming interfaces).

1.3 Υπηρεσίες Επιτάχυνσης

Οι προσφορές υπηρεσιών IBM Security Expert Labs (SEL) for Resilient είναι εξ αποστάσεως παραδιδόμενες υπηρεσίες που παρέχουν χρόνο καθοδήγησης για θέματα αρχιτεκτονικής και υλοποίησης λύσεων Resilient από έναν ειδικό στα προϊόντα Resilient. Η προσφορά IBM Resilient Security, Orchestration and Response, είτε ως Υπηρεσία Cloud είτε ως τοπικά εγκαθιστώμενο λογισμικό, αποτελεί προαπαιτούμενο για οποιαδήποτε από αυτές τις Υπηρεσίες.

1.3.1 IBM SEL for Resilient Base Starter Service

Μια δέσμευση εξ αποστάσεως παροχής υπηρεσιών 5 ημερών κατά τη διάρκεια της οποίας η IBM:

- Θα βοηθήσει στον ορισμό της αρχιτεκτονικής του IBM Security Resilient.
- Θα εγκαταστήσει και θα παραμετροποιήσει το IBM Security Resilient (όπου απαιτείται).

- Θα εκπαιδεύσει τους αναλυτές και τους σχεδιαστές για την παραμετροποίηση και τη χρήση των υφιστάμενων σχεδίων αντιμετώπισης περιστατικών του Πελάτη με βάση τις κύριες απαιτήσεις του οργανισμού του Πελάτη.
- Θα παρέχει σενάρια ειδικά ρυθμισμένα για το IBM Security Resilient με βάση τις μοναδικές διεργασίες του οργανισμού του Πελάτη.
- Θα παρέχει οδηγίες για την παρακολούθηση καθορισμένων δεικτών KPI και μετρικών στοιχείων σύμφωνα με τις ανάγκες του οργανισμού του Πελάτη και τις βέλτιστες πρακτικές του κλάδου.
- Θα εντοπίσει ευκαιρίες ενοποίησης για την υποστήριξη, την αυτοματοποίηση και την εννοχή των διεργασιών.

1.3.2 IBM SEL for Resilient Premium Starter Service

Μια δέσμευση εξ αποστάσεως παροχής υπηρεσιών 3 ημερών κατά τη διάρκεια της οποίας η IBM:

- Θα βοηθήσει στον ορισμό της αρχιτεκτονικής του IBM Security Resilient.
- Θα εγκαταστήσει το IBM Security Resilient (όπου απαιτείται).
- Θα εκτελέσει την αρχική παραμετροποίηση του IBM Security Resilient στο περιβάλλον του Πελάτη.
- Θα εκπαιδεύσει τους αναλυτές και τους σχεδιαστές για την παραμετροποίηση και τη χρήση των υφιστάμενων σχεδίων αντιμετώπισης περιστατικών του Πελάτη με βάση τις κύριες απαιτήσεις του οργανισμού του Πελάτη.

1.3.3 IBM SEL for Resilient Additional Day

Επιπροσθέτως της υπηρεσίας Base Starter ή Premium Starter, η IBM θα αναλάβει στο πλαίσιο μιας δέσμευσης εξ αποστάσεως παροχής υπηρεσιών 1 ημέρας να εκτελέσει οποιαδήποτε προσυμφωνημένη δραστηριότητα για το IBM Security Resilient. Για παράδειγμα:

- Θα παρέχει περαιτέρω υποστήριξη για την εγκατάσταση ή την παραμετροποίηση του IBM Security Resilient ή επεκτάσεων (όπου απαιτείται).
- Θα παρέχει περαιτέρω εκπαίδευση ή υποστήριξη στους αναλυτές για να διασφαλίσει ότι το IBM Security Resilient είναι έτοιμο να χρησιμοποιηθεί ως η κύρια λύση SOAR του Πελάτη.
- Θα καθοδηγήσει τους σχεδιαστές για την παραμετροποίηση και τη χρήση των δικών τους σεναρίων (playbooks) που θα αντικατοπτρίζουν τις κύριες απαιτήσεις του οργανισμού του Πελάτη.
- Θα διεξαγάγει έναν γρήγορο έλεγχο του περιβάλλοντος IBM Security Resilient για να προτείνει πιθανές βελτιώσεις.

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 σε 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://www.ibm.com/dpa/dpl>.

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

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/>.

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:

- Εξουσιοδοτημένος Χρήστης (Authorized User) είναι ένας μοναδικός χρήστης που έχει εξουσιοδοτηθεί να αποκτά πρόσβαση στις Υπηρεσίες Cloud με οποιονδήποτε τρόπο, είτε άμεσα είτε έμμεσα (για παράδειγμα, μέσω ενός προγράμματος πολυπλεξίας (multiplexing), μιας συσκευής ή ενός εξυπηρετητή εφαρμογών (application server)) με οποιοδήποτε μέσο.
- Ταυτόχρονα Συνδεδεμένος Χρήστης (Concurrent User) είναι ένας χρήστης που αποκτά ταυτόχρονα πρόσβαση στην Υπηρεσία Cloud με οποιονδήποτε τρόπο, είτε άμεσα είτε έμμεσα (για παράδειγμα, μέσω ενός προγράμματος πολυπλεξίας (multiplexing), μιας συσκευής ή ενός εξυπηρετητή εφαρμογών (application server)), σε οποιαδήποτε χρονική στιγμή. Ένα πρόσωπο που αποκτά πρόσβαση στην Υπηρεσία Cloud περισσότερες από μία φορές ταυτόχρονα μετρά ως ένας μόνο Ταυτόχρονα Συνδεδεμένος Χρήστης.
- Δέσμευση (Engagement) είναι μια επαγγελματική ή εκπαιδευτική υπηρεσία που σχετίζεται με τις Υπηρεσίες Cloud.
- Στοιχείο (Item) είναι μια εμφάνιση ενός συγκεκριμένου αντικειμένου που βρίσκεται υπό διαχείριση ή επεξεργασία από την Υπηρεσία Cloud ή σχετίζεται με τη χρήση της Υπηρεσίας Cloud. Για το σκοπό αυτής της Υπηρεσίας Cloud, ένα στοιχείο είναι μια Ενέργεια. Μια Ενέργεια (Action) είναι ένα αίτημα ενορχήστρωσης ή αυτοματοποίησης που υποβάλλεται από την Υπηρεσία Cloud σε κάποιο άλλο πρόγραμμα λογισμικού.

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 Επαλήθευση

Ο Πελάτης i) θα τηρεί, και θα παρέχει κατόπιν σχετικού αιτήματος, αρχεία και δεδομένα που παράγονται από εργαλεία του συστήματος, στο βαθμό που είναι ευλόγως απαραίτητο ώστε να επαληθεύουν η IBM και ο ανεξάρτητος ελεγκτής της τη συμμόρφωση του Πελάτη με τις διατάξεις της Σύμβασης, και ii) θα παραγγέλλει και θα εξοφλεί άμεσα τα απαιτούμενα δικαιώματα έναντι των εκάστοτε ισχυουσών τιμών της IBM, καθώς και οποιεσδήποτε άλλες χρεώσεις και οφειλές που τυχόν προκύπτουν ως αποτέλεσμα της εν λόγω επαλήθευσης, όπως αυτές καθορίζονται από την IBM σε ένα τιμολόγιο. Οι εν λόγω υποχρεώσεις

επαλήθευσης συμμόρφωσης παραμένουν σε ισχύ κατά τη διάρκεια της περιόδου ισχύος της Υπηρεσίας Cloud και για δύο επιπλέον έτη μετά τη λήξη αυτής της περιόδου.

5.2 Απαιτούμενα Δικαιώματα για Πρόσθετες Υπηρεσίες

Ο Πελάτης πρέπει να προμηθευτεί τον ίδιο αριθμό και το ίδιο είδος δικαιωμάτων τόσο για την βασική Υπηρεσία Cloud όσο και για τις όποιες Πρόσθετες (Add-on) Υπηρεσίες Cloud.

5.3 Περιορισμοί Χρήσης

Κάθε Πελάτης δικαιούται να υποβάλλει έως εκατό χιλιάδες (100.000) αιτήματα ανάκτησης πληροφοριών Αντιμετώπισης Απειλών (Threat Service queries) ανά μήνα. Ο Πελάτης δημιουργεί ένα αίτημα ανάκτησης πληροφοριών Αντιμετώπισης Απειλών προσθέτοντας ένα τεχνούργημα σε ένα περιστατικό όταν έχει ενεργοποιηθεί η Υπηρεσία Αντιμετώπισης Απειλών. Στη συνέχεια, για κάθε περίοδο δύο (2) ημερών που το περιστατικό παραμένει ανοιχτό και ενεργό, θα υποβάλλεται αυτόματα ένα νέο αίτημα ανάκτησης πληροφοριών Αντιμετώπισης Απειλών.

Κάθε Πελάτης δικαιούται να δημιουργεί έως εκατό (100) email ειδοποίησης ανά ημέρα ανά Εξουσιοδοτημένο/Ταυτόχρονα Συνδεδεμένο Χρήστη. Τα email ειδοποίησης δημιουργούνται από την πλατφόρμα Resilient με βάση την ελεγχόμενη από τον Πελάτη παραμετροποίηση.

5.4 Πρόσθετες Πληροφορίες για την Επεξεργασία και την Προστασία των Δεδομένων

Για την αποφυγή οποιωνδήποτε αμφιβολιών, το IBM Resilient SOAR Platform on Cloud:

- Δεν κρυπτογραφεί το Περιεχόμενο που είναι αποθηκευμένο.
- Δεν έχει σχεδιαστεί για την επεξεργασία οποιωνδήποτε Ειδικών Κατηγοριών Δεδομένων Προσωπικού Χαρακτήρα.
- Δεν πρέπει να επιτρέπει την εισαγωγή δεδομένων προσωπικού χαρακτήρα στα πεδία ελεύθερου κειμένου, εφόσον αυτό δεν είναι απαραίτητο.

Αναλυτικές πληροφορίες σχετικά με την κρυπτογράφηση και τα είδη των Δεδομένων Προσωπικού Χαρακτήρα που υποβάλλονται σε επεξεργασία είναι διαθέσιμες στη διεύθυνση URL για το Φύλλο Δεδομένων που αναφέρεται στο Άρθρο 2 παραπάνω.

6. Υπερισχύοντες Όροι

6.1 Χρήση Δεδομένων

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. Ωστόσο, η IBM θα χρησιμοποιεί το Περιεχόμενο και άλλες πληροφορίες που προκύπτουν από το Περιεχόμενο (εκτός από Καίριες πληροφορίες) στο πλαίσιο της Υπηρεσίας Cloud για το σκοπό της βελτίωσης της Υπηρεσίας Cloud. Η IBM μπορεί επίσης να γνωστοποιεί αναγνωριστικά απειλών και άλλες πληροφορίες ασφαλείας που είναι ενσωματωμένες στο Περιεχόμενο για σκοπούς ανίχνευσης απειλών και προστασίας.

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.