

IBM QRadar Advisor with Watson

Στην παρούσα Περιγραφή Υπηρεσιών περιγράφονται οι υπηρεσίες που παρέχονται από την IBM στον Πελάτη. Με τον όρο "Πελάτης" νοούνται η εταιρεία, οι εξουσιοδοτημένοι χρήστες της ή 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

1.1 IBM QRadar Advisor with Watson Service

Η υπηρεσία IBM QRadar Advisor with Watson επεκτείνει τις λειτουργίες γνωσιακής ανάλυσης του QRadar Security Platform, βοηθώντας τους πελάτες και τους αναλυτές ασφάλειας στη γρήγορη διερεύνηση και αντιμετώπιση απειλών. Αξιοποιεί τη γνωσιακή βάση του Watson for Cyber Security, προσθέτοντας μη δομημένα δεδομένα (όπως π.χ. πληροφορίες από ιστοτόπους ασφάλειας, ιστολόγια (blogs) και ερευνητικές μελέτες) και συσχετίζοντάς τα με τοπικά περιστατικά ασφάλειας. Με αυτό τον τρόπο μπορεί να συμβάλει σημαντικά στον εντοπισμό κρυφών απειλών και στην αυτόματη παροχή πληροφοριών για την άμεση αντιμετώπιση ανταπόκριση σε περιστατικά και τη λήψη καλύτερων αποφάσεων. Το QRadar Advisor with Watson παρέχει σε έναν αναλυτή ασφάλειας τη δυνατότητα αποστολής ενός περιστατικού παραβίασης ασφάλειας στο Watson για την εκτέλεση μιας διαδικασίας εντοπισμού απειλών, χρησιμοποιώντας τη γνωσιακή του βάση με εκατοντάδες χιλιάδες μη δομημένων και δομημένων πηγών δεδομένων και συσχετίζοντας τις πληροφορίες αυτές με στοιχεία απειλών που σχετίζονται με την αρχική παραβίαση ασφάλειας, όπως π.χ. κακόβουλα αρχεία, ύποπτες διευθύνσεις IP, ψευδή στοιχεία και η σχέση μεταξύ των στοιχείων αυτών. Η διαδικασία μπορεί να είναι ιδιαίτερα χρήσιμη για να διαπιστωθεί εάν μια παραβίαση ασφάλειας σχετίζεται με κάποια γνωστή εκστρατεία κακόβουλου λογισμικού. Στην περίπτωση αυτή, η Watson παρέχει όλες τις απαιτούμενες πληροφορίες για το εν λόγω κακόβουλο λογισμικό, τα τρωτά σημεία που εκμεταλλεύεται και την εμβέλεια της απειλής (συμπεριλαμβανομένων των άλλων τελικών σημείων που ενδέχεται να έχουν επηρεαστεί), μαζί με άλλες καίριες πληροφορίες.

Προϋπόθεση για τη χρήση της Υπηρεσίας Cloud είναι ότι ο Πελάτης έχει ένα ενεργό περιβάλλον IBM Security QRadar και έχει εγκαταστήσει τον κώδικα ενεργοποίησης της Υπηρεσίας Cloud στο εν λόγω περιβάλλον ώστε να είναι δυνατή η πρόσβαση του Πελάτη στις λειτουργίες του. Η Υπηρεσία Cloud περιέχει ένα 'εύκαμπτο όριο' για τον αριθμό αιτημάτων αναζήτησης πληροφοριών για παραβιάσεις ασφάλειας που ο Πελάτης μπορεί να υποβάλει στην Υπηρεσία Cloud, το οποίο είναι δεκαπέντε (15) αιτήσεις την ημέρα ανά 1000 Συμβάντα ανά Δευτερόλεπτο για τα οποία ο Πελάτης διαθέτει τα απαιτούμενα δικαιώματα. Τα αιτήματα αναζήτησης πληροφοριών που υποβάλλονται κατ' υπέρβαση αυτού του ορίου θα υφίστανται επεξεργασία από την Υπηρεσία Cloud, αλλά με χαμηλότερη προτεραιότητα και με μικρότερη ταχύτητα επιστροφής αποτελεσμάτων.

1.2 IBM QRadar Advisor with Watson Trial

Το IBM QRadar Advisor with Watson Trial ("Υπηρεσία Cloud Δοκιμαστικής Χρήσης") παρέχει τις λειτουργίες του IBM QRadar Advisor with Watson για δοκιμαστική χρήση. Η πρόσβαση του Πελάτη στην Υπηρεσία Cloud Δοκιμαστικής Χρήσης θα είναι για μια χρονική περίοδο που καθορίζεται σε ένα Έγγραφο Συναλλαγής ή σε κάποιο άλλο έγγραφο και στο τέλος της εν λόγω περιόδου δοκιμαστικής χρήσης η πρόσβαση του Πελάτη θα διακοπεί. Ο Πελάτης έχει το δικαίωμα να αποστέλλει μόνο 5 το πολύ αιτήματα αναζήτησης πληροφοριών για παραβιάσεις ασφάλειας ανά ημέρα κατά τη διάρκεια της περιόδου δοκιμαστικής χρήσης. Η Υπηρεσία Cloud Δοκιμαστικής Χρήσης παρέχεται χωρίς εγγύηση και 'ως έχει' και ο Πελάτης επιτρέπεται να τη χρησιμοποιήσει μόνο για μη παραγωγικούς σκοπούς και για τη διενέργεια δοκιμών. Οι χρόνοι απόκρισης σε αιτήματα αναζήτησης πληροφοριών μπορεί να διαφέρουν κατά τη διάρκεια της περιόδου δοκιμαστικής χρήσης ανάλογα με τον όγκο των εκτελούμενων ροών δεδομένων.

2. Περιγραφή Ασφάλειας

Αυτή η Υπηρεσία Cloud συμμορφώνεται με τις βασικές αρχές προστασίας και ασφάλειας δεδομένων της IBM, οι οποίες καθίστανται διαθέσιμες στην ιστοσελίδα <http://www-03.ibm.com/software/sla/sladb.nsf/sla/dsp> και με οποιουδήποτε 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 επιλεγμένου 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. Ο Πελάτης αποδέχεται ότι η IBM δεν έχει γνώση των ειδών δεδομένων που περιλαμβάνονται στο περιεχόμενο και δεν μπορεί να προβεί σε μια αποτίμηση της καταλληλότητας των Υπηρεσιών Cloud ή των μέτρων προστασίας που έχουν εφαρμοστεί.

Η Υπηρεσία Cloud θα παρέχει στον Πελάτη τη δυνατότητα εισαγωγής και διαχείρισης μόνο του ακόλουθου περιεχομένου, που ορισμένα τμήματά του μπορεί να θεωρούνται πληροφορίες προσωπικού χαρακτήρα (personal information - "PI") σύμφωνα με τους ισχύοντες νόμους περί προστασίας δεδομένων προσωπικού χαρακτήρα:

- Διευθύνσεις IP προορισμού/προέλευσης
- Διευθύνσεις URL
- Τομείς (domains)
- Τιμές κατακερματισμού (hashes) αρχείων

2.1 Λειτουργίες Ασφάλειας και Υποχρεώσεις

Η Υπηρεσία Cloud παρέχει τις ακόλουθες λειτουργίες ασφάλειας:

Η Υπηρεσία Cloud κρυπτογραφεί περιεχόμενο κατά τη μετάδοση δεδομένων μεταξύ του δικτύου της IBM και του περιβάλλοντος IBM Security QRadar του Πελάτη. Η Υπηρεσία Cloud δεν κρυπτογραφεί περιεχόμενο όταν βρίσκεται σε κατάσταση αναμονής για τη μετάδοση δεδομένων.

Η Υπηρεσία Cloud δεν διατηρεί ούτε αποθηκεύει μόνιμα τα δεδομένα που εισάγονται μετά την εκτέλεση της λειτουργίας που ζητήθηκε για τα εν λόγω δεδομένα.

3. Τεχνική Υποστήριξη

Παρέχεται τεχνική υποστήριξη για την Υπηρεσία Cloud μέσω email, online φόρουμ και ενός συστήματος online αναφοράς προβλημάτων, όπως περιγράφεται παρακάτω. Η τεχνική υποστήριξη παρέχεται μαζί με την Υπηρεσία Cloud και δεν διατίθεται ως χωριστή προσφορά.

Κρισιμότητα	Ορισμός Κρισιμότητας	Στόχοι σχετικά με τους Χρόνους Απόκρισης	Κάλυψη Χρόνων Απόκρισης
1	Κρίσιμες επιπτώσεις στη λειτουργία της επιχείρησης/διακοπή παροχής υπηρεσιών: Δεν μπορούν να χρησιμοποιηθούν κρίσιμες λειτουργίες της επιχείρησης ή δεν λειτουργεί κάποια κρίσιμη σημασίας διεπαφή (interface). Οι περιπτώσεις αυτές αφορούν συνήθως το περιβάλλον παραγωγής και έχουν κρίσιμες επιπτώσεις στη γενική λειτουργία της επιχείρησης εξαιτίας της αδυναμίας πρόσβασης σε υπηρεσίες. Στις περιπτώσεις αυτές απαιτείται η άμεση παροχή μιας λύσης.	Εντός 1 ώρας	24x7
2	Σημαντικές επιπτώσεις στη λειτουργία της επιχείρησης: Η δυνατότητα χρήσης ενός στοιχείου ή μιας λειτουργίας της υπηρεσίας περιορίζεται σοβαρά ή υπάρχει κίνδυνος ο Πελάτης να μη μπορεί να ανταποκριθεί σε επιχειρηματικές προθεσμίες.	Εντός 2 εργάσιμων ωρών	Εργάσιμες ώρες (Δευτέρα έως Παρασκευή)
3	Περιορισμένες επιπτώσεις στη λειτουργία της επιχείρησης: Δηλώνει ότι η υπηρεσία ή η λειτουργία μπορεί να χρησιμοποιηθεί και δεν υπάρχουν κρίσιμες επιπτώσεις στη γενική λειτουργία της επιχείρησης.	Εντός 4 εργάσιμων ωρών	Εργάσιμες ώρες (Δευτέρα έως Παρασκευή)

Κρισιμότητα	Ορισμός Κρισιμότητας	Στόχοι σχετικά με τους Χρόνους Απόκρισης	Κάλυψη Χρόνων Απόκρισης
4	Ελάχιστες επιπτώσεις στη λειτουργία της επιχείρησης: Μια ερώτηση ή ένα αίτημα μη τεχνικού χαρακτήρα.	Εντός 1 εργάσιμης ημέρας	Εργάσιμες ώρες (Δευτέρα έως Παρασκευή)

Για Πελάτες που έχουν συμμετάσχει στη δοκιμή της έκδοσης beta της Υπηρεσίας Cloud και εξακολουθούν να χρησιμοποιούν την έκδοση 7.2.7 του QRadar Platform, ενδέχεται να μην είναι δυνατή η επίλυση ορισμένων ζητημάτων τεχνικής υποστήριξης. Οι λόγω Πελάτες θα πρέπει να αναβαθμίσουν το προϊόν στην έκδοση 7.2.8 και να εγκαταστήσουν την τελευταία επιδιόρθωση (patch) προκειμένου να λάβουν πλήρη τεχνική υποστήριξη.

4. Δικαιώματα και Τιμολόγηση

4.1 Μετρικά Συστήματα Χρέωσης

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

- α. **100 Συμβάντα ανά Δευτερόλεπτο (100 Events Per Second)** – μια μονάδα μέτρησης βάσει της οποίας μπορεί να αποκτηθεί η Υπηρεσία Cloud. Ένα Συμβάν (Event) είναι μια εμφάνιση ενός συγκεκριμένου συμβάντος που βρίσκεται υπό την επεξεργασία της Υπηρεσίας Cloud. Πρέπει να αποκτηθούν επαρκή δικαιώματα για την κάλυψη του αριθμού Συμβάντων ανά δευτερόλεπτο, στρογγυλοποιημένων στην επόμενη εκατοντάδα, που προκύπτουν κατά τη διάρκεια της περιόδου μέτρησης που καθορίζεται σε μια Απόδειξη Δικαιώματος (Proof of Entitlement - "PoE") ή ένα Έγγραφο Συναλλαγής.

5. 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.

6. Λογισμικό Ενεργοποίησης

Για την Υπηρεσία Cloud απαιτείται η χρήση λογισμικού ενεργοποίησης, το οποίο μεταφορτώνεται από τον Πελάτη στα συστήματά του προκειμένου να καθίσταται δυνατή η χρήση της Υπηρεσίας Cloud. Ο Πελάτης επιτρέπεται να χρησιμοποιεί το λογισμικό ενεργοποίησης μόνο σε συνάρτηση με την εκ μέρους του χρήση της Υπηρεσίας Cloud. Το λογισμικό ενεργοποίησης παρέχεται "ΩΣ EXEI".

Το λογισμικό ενεργοποίησης για την Υπηρεσία Cloud καθίσταται διαθέσιμο για μεταφόρτωση από τον Πελάτη από το IBM Security App Exchange στη διεύθυνση <https://exchange.xforce.ibmcloud.com/hub>.

7. Πρόσθετοι Όροι

7.1 Γενικές Διατάξεις

Ο Πελάτης συμφωνεί ότι η IBM μπορεί να αναφέρει τον Πελάτη δημοσίως ως συνδρομητή των Υπηρεσιών Cloud σε διαφημίσεις και σε δημοσιεύσεις στον τύπο.

7.2 Λογισμικό Ενεργοποίησης

Για την Υπηρεσία Cloud απαιτείται η χρήση λογισμικού ενεργοποίησης, το οποίο μεταφορτώνεται από τον Πελάτη στα συστήματά του προκειμένου να καθίσταται δυνατή η χρήση της Υπηρεσίας Cloud. Ο Πελάτης επιτρέπεται να χρησιμοποιεί το λογισμικό ενεργοποίησης μόνο σε συνάρτηση με την εκ μέρους του χρήση της Υπηρεσίας Cloud. Το λογισμικό ενεργοποίησης παρέχεται "ΩΣ EXEI".

Το λογισμικό ενεργοποίησης για την Υπηρεσία Cloud καθίσταται διαθέσιμο για μεταφόρτωση από τον Πελάτη από το IBM Security App Exchange στη διεύθυνση <https://exchange.xforce.ibmcloud.com/hub>.

7.3 Νόμιμη Χρήση της Υπηρεσίας Cloud

Η Υπηρεσία Cloud έχει σχεδιαστεί για να βοηθά τον Πελάτη να ενισχύει την ασφάλεια του περιβάλλοντός του και των δεδομένων του. Η χρήση της Υπηρεσίας Cloud μπορεί να διέπεται από διάφορους νόμους ή κανονισμούς, συμπεριλαμβανομένων εκείνων που αφορούν στην ιδιωτικότητα, στην προστασία δεδομένων, στην απασχόληση και στην ηλεκτρονική επικοινωνία και αποθήκευση. 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. Ο Πελάτης δηλώνει ότι θα αποκτήσει ή έχει ήδη αποκτήσει τις απαιτούμενες συναινέσεις, άδειες ή δικαιώματα χρήσης προκειμένου να καθίσταται δυνατή η νόμιμη χρήση της Υπηρεσίας Cloud.

7.4 Λήξη της Υπηρεσίας Cloud

Πριν τη λήξη ή τη διακοπή της Υπηρεσίας Cloud, ο Πελάτης μπορεί να κάνει χρήση οποιασδήποτε από τις παρεχόμενες λειτουργίες δημιουργίας αναφορών ή εξαγωγής της Υπηρεσίας Cloud για την εξαγωγή δεδομένων.

7.5 Δεδομένα 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 ή οποιουδήποτε μεμονωμένου προσώπου, με εξαίρεση την περίπτωση που περιγράφεται στο στοιχείο (δ) παρακάτω. Επιπροσθέτως, ο Πελάτης συμφωνεί με το παρόν ότι η IBM μπορεί 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, και
- δ. κοινοποίηση πληροφοριών τρίτων με αποδεδειγμένη παραβατική δραστηριότητα

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.