

IBM QRadar 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

1.1 Προσφορές

Ο Πελάτης μπορεί να επιλέξει από τις ακόλουθες διαθέσιμες προσφορές.

1.1.1 IBM QRadar on Cloud

Η προσφορά IBM QRadar on Cloud παρέχει μια προηγμένη λύση συλλογής πληροφοριών ασφάλειας από το IBM Cloud η οποία βασίζεται στο προϊόν IBM Security QRadar SIEM. Επιτρέπει στον Πελάτη να συλλέγει, να συσχετίζει και να αποθηκεύει συμβάντα που παράγονται τόσο από το περιβάλλον cloud όσο και από το περιβάλλον πληροφορικής της επιχείρησής του και να εκτελεί εργασίες διαχείρισης ασφάλειας και απειλών όπως θα έκανε με ένα προϊόν QRadar SIEM που έχει εγκατασταθεί στο περιβάλλον της επιχείρησής του. Στο πλαίσιο αυτής της προσφοράς, η IBM παρέχει επίσης υπηρεσίες παρακολούθησης υποδομής καθημερινά όλο το 24ωρο (24x7) και εφαρμόζει τις τελευταίες εκδόσεις λογισμικού και τις κρίσιμες επιδιορθώσεις όποτε αυτές καθίστανται διαθέσιμες.

Αυτή η Υπηρεσία Cloud περιλαμβάνει ενεργό χώρο αποθήκευσης με δυνατότητα αναζήτησης πληροφοριών για ενενήντα (90) ημέρες και διατίθεται σε ποσότητα 100 Συμβάντων ανά Δευτερόλεπτο (Events per Second - "EPS").

1.2 Προαιρετικές Υπηρεσίες

1.2.1 IBM QRadar on Cloud Temporary Upgrade

Μια αναβάθμιση υπηρεσιών που παρέχει πρόσθετη δυναμικότητα 1.000 EPS για τη συλλογή και επεξεργασία καταγεγραμμένων συμβάντων, αλλά μόνο προσωρινά για έναν συγκεκριμένο αριθμό μηνών. Ο Πελάτης μπορεί να αγοράσει περισσότερες από μία μονάδες αυτής της αναβάθμισης, έως το μέγιστο επίπεδο EPS που υποστηρίζεται από αυτή την προσφορά. Ο σκοπός αυτής της αναβάθμισης είναι να παρέχει σε έναν Πελάτη που χρειάζεται επιπλέον κάλυψη σε περιόδους αιχμής κατά τη διάρκεια του έτους τη δυνατότητα να ανταποκρίνεται στις αυξημένες απαιτήσεις αυτές με μια προσωρινή αναβάθμιση δυναμικότητας. Στο τέλος της περιόδου ισχύος, η εν λόγω προσωρινή αυξημένη δυναμικότητα θα αφαιρεθεί από το περιβάλλον του Πελάτη.

1.2.2 IBM QRadar on Cloud Data Capacity

Η αναβάθμιση χωρητικότητας δεδομένων (Data Capacity Upgrade) προσθέτει πρόσθετο χώρο αποθήκευσης και παρατείνει την περίοδο ανάλυσης. Η αναβάθμιση χωρητικότητας παρέχει στον Πελάτη ένα (1) πλήρες έτος αποθήκευσης δεδομένων συμβάντων για κάθε αγορά αναβάθμισης 100 EPS.

1.2.3 IBM QRadar on Cloud Flows Add-On

Ενοποιείται με το IBM QRadar SIEM και επεξεργαστές ροών για την παροχή ορατότητας δικτύου Επιπέδου (Layer) 3 και την ανάλυση ροών βοηθώντας τον Πελάτη στην ανίχνευση, στον εντοπισμό και στην ανταπόκριση σε δραστηριότητες στο δίκτυο του Πελάτη.

Αυτή η Υπηρεσία Cloud περιλαμβάνει ενεργό χώρο αποθήκευσης με δυνατότητα αναζήτησης πληροφοριών για ενενήντα (90) ημέρες και διατίθεται σε ποσότητα 10.000 Ροών ανά Λεπτό (Flows per Minute - "FPM").

1.2.4 IBM QRadar on Cloud Vulnerability Management Add-On

Επιτρέπει την προληπτική ανίχνευση και ανακάλυψη τρωτών σημείων στην ασφάλεια συσκευών και εφαρμογών δικτύου, προσθέτει αντίστοιχες πληροφορίες και υποστηρίζει την ιεράρχηση δραστηριοτήτων επιδιόρθωσης και μετριασμού των επιπτώσεων.

1.2.5 IBM QRadar on Cloud Log Archival

Παρέχει στον Πελάτη τη δυνατότητα αρχειοθέτησης δεδομένων συμβάντων από την Υπηρεσία Cloud κατά τη διάρκεια της περιόδου συνδρομής. Η IBM θα συνεργάζεται με τον Πελάτη για την εγγραφή των καθορισμένων συμβάντων στον χώρο αποθήκευσης αντικειμένων για σκοπούς αρχειοθέτησης. Κατόπιν αιτήματος του Πελάτη, η IBM θα επαναφέρει αρχειοθετημένα δεδομένα συμβάντων μιας περιόδου μέγιστης διάρκειας τριάντα (30) ημερών στην περίπτωση χρήσης της Υπηρεσίας Cloud του Πελάτη εντός τριών (3) εργάσιμων ημερών από την ημερομηνία υποβολής του εν λόγω αιτήματος. Τα εν λόγω δεδομένα θα παραμείνουν διαθέσιμα στον Πελάτη για 48 ώρες προτού επιστραφούν στο χώρο αποθήκευσης αρχειοθετημένων αντικειμένων. Ο Πελάτης μπορεί να υποβάλει έως δύο αιτήματα ανά τρίμηνη περίοδο. Η αναβάθμιση χωρητικότητας παρέχει στον Πελάτη ένα (1) πλήρες έτος αποθήκευσης δεδομένων για κάθε αγορά αναβάθμισης 100 EPS.

1.2.6 IBM QRadar on Cloud Flows Add-On Data Capacity

Η αναβάθμιση χωρητικότητας δεδομένων (Data Capacity Upgrade) προσθέτει πρόσθετο χώρο αποθήκευσης και παρατείνει την περίοδο ανάλυσης παρέχοντας στον Πελάτη μέχρι ένα (1) πλήρες έτος αποθήκευσης δεδομένων ροής για κάθε αναβάθμιση 10.000 FPM που αγοράζει.

1.2.7 IBM QRadar on Cloud Flows Add-On Log Archival

Αυτή η προσφορά παρέχει στον Πελάτη τη δυνατότητα αρχειοθέτησης δεδομένων ροών από την Υπηρεσία Cloud κατά τη διάρκεια της περιόδου συνδρομής. Η IBM θα συνεργάζεται με τον Πελάτη για την εγγραφή των καθορισμένων εγγραφών ροής στον χώρο αποθήκευσης αντικειμένων για σκοπούς αρχειοθέτησης. Κατόπιν αιτήματος του Πελάτη, η IBM θα επαναφέρει τα αρχειοθετημένα δεδομένα ροών μιας περιόδου μέγιστης διάρκειας τριάντα (30) ημερών στην περίπτωση χρήσης της Υπηρεσίας Cloud του Πελάτη εντός τριών (3) εργάσιμων ημερών από την ημερομηνία υποβολής του εν λόγω αιτήματος. Τα εν λόγω δεδομένα θα παραμείνουν διαθέσιμα στον Πελάτη για 48 ώρες προτού επιστραφούν στο χώρο αποθήκευσης αρχειοθετημένων αντικειμένων. Ο Πελάτης μπορεί να υποβάλει έως δύο αιτήματα ανά τρίμηνη περίοδο. Η αναβάθμιση χωρητικότητας παρέχει στον Πελάτη ένα (1) πλήρες έτος αποθήκευσης δεδομένων για κάθε αγορά αναβάθμισης 10.000 FPM.

1.2.8 IBM QRadar on Cloud for Non-Production Environment

Η προσφορά IBM QRadar on Cloud for Non-Production Environment παρέχει μια αποκλειστική περίπτωση χρήσης διενέργειας δοκιμών της υπηρεσίας Cloud. Επιτρέπει στον Πελάτη να συλλέγει, να συσχετίζει και να αποθηκεύει συμβάντα που παράγονται τόσο από το περιβάλλον cloud όσο και από το τοπικό περιβάλλον πληροφορικής του Πελάτη και να εκτελεί εργασίες διαχείρισης ασφάλειας και απειλών, όπως θα έκανε με ένα προϊόν QRadar SIEM που θα ήταν εγκατεστημένο στο τοπικό περιβάλλον του οργανισμού του σε ένα αποκλειστικό περιβάλλον διενέργειας δοκιμών. Στο πλαίσιο αυτής της προσφοράς, η IBM παρέχει επίσης υπηρεσίες παρακολούθησης υποδομής καθημερινά όλο το 24ωρο (24x7) και εφαρμόζει τις τελευταίες εκδόσεις λογισμικού και τις κρίσιμες επιδιορθώσεις όποτε αυτές καθίστανται διαθέσιμες. Ο Πελάτης μπορεί να χρησιμοποιήσει αυτή την Υπηρεσία Cloud μόνο για σκοπούς διενέργειας δοκιμών και όχι για σκοπούς παραγωγής.

Αυτή η Υπηρεσία Cloud περιλαμβάνει ενεργό χώρο αποθήκευσης με δυνατότητα αναζήτησης πληροφοριών για ενενήντα (90) ημέρες.

1.3 Υπηρεσίες Επιτάχυνσης

1.3.1 IBM QRadar on Cloud Optimization Service

Για αυτή την εξ αποστάσεως παραδιδόμενη υπηρεσία συνδρομής, η IBM θα διεξαγάγει μια σύσκεψη ανασκόπησης με τον Πελάτη κατά την οποία θα αξιολογηθεί η τρέχουσα κατάσταση υγείας της περίπτωσης χρήσης της Υπηρεσίας Cloud του Πελάτη και θα παραδώσει τα αποτελέσματα της εν λόγω αξιολόγησης στον Πελάτη μέσω μιας αναφοράς Κατάστασης Υγείας (Health Status) του QRadar on Cloud, στην οποία θα επισημανθούν τα όποια σημεία που χρήζουν βελτίωσης.

Επιπροσθέτως, η IBM θα παρέχει, κατόπιν αιτήματος του Πελάτη, οποιεσδήποτε από τις ακόλουθες συμβουλευτικές υπηρεσίες στον Πελάτη για οκτώ (8) το πολύ ημέρες κατά τη διάρκεια μιας περιόδου 1 έτους:

- Παροχή βοήθειας στην προσθήκη πρόσθετων πηγών δεδομένων καταγραφής στην Υπηρεσία Cloud,
- Παραμετροποίηση πρόσθετων αναζητήσεων, αναφορών και χειριστηρίων (dashboards),
- Πραγματοποίηση πρόσθετων ρυθμίσεων στην υπάρχουσα υλοποίηση του QRadar, και

- Μεταφορά τεχνογνωσίας για σχετικά θέματα του QRadar.

1.3.2 Υπηρεσίες Προετοιμασίας

Οι ακόλουθες υπηρεσίες προετοιμασίας (setup) παρέχονται εξ αποστάσεως και μπορούν να παραγγελθούν χωριστά. Κάθε παραγγελθείσα υπηρεσία θα λήγει ενενήντα (90) ημέρες από την ημερομηνία αγοράς της, εκτός εάν άλλως ορίζεται, ανεξάρτητα από το εάν έχουν χρησιμοποιηθεί όλες οι ώρες (ανάλογα με την περίπτωση). Οι υπηρεσίες περιλαμβάνουν έναν καθορισμένο IBM Engagement Manager ο οποίος θα προγραμματίσει τη διεξαγωγή οποιωνδήποτε εναρκτήριων τηλεδιασκέψεων.

a. IBM QRadar on Cloud Deployment Services

Αυτή η υπηρεσία παρέχει επαγγελματικές υπηρεσίες διάρκειας έως σαράντα (40) ωρών κατά τις οποίες η IBM θα εκτελέσει ορισμένες ή όλες τις ακόλουθες δραστηριότητες:

Η IBM θα διεξαγάγει μια ανασκόπηση αρχιτεκτονικής SIEM διάρκειας δεκαέξι (16) ωρών για τον ορισμό των απαιτήσεων δημιουργίας αναφορών του Πελάτη και θα παραδώσει τα ευρήματά της στον Πελάτη σε μια αναφορά αρχιτεκτονικής της λύσης που θα διευκολύνει τον ορισμό και τη συγκέντρωση των απαιτήσεων του Πελάτη.

Στην αναφορά αυτή θα περιλαμβάνονται τα εξής στοιχεία:

- Οι καθορισμένες από τον Πελάτη απαιτήσεις δημιουργίας αναφορών προκειμένου να ανταποκρίνεται ο Πελάτης στις απαιτήσεις συμμόρφωσης, ελέγχου και συγκέντρωσης πληροφοριών ασφάλειας.
- Οι απαιτήσεις συγκέντρωσης πληροφοριών ασφάλειας, τα σενάρια χρήσης και οι εφαρμογές (apps) με την υλοποίηση των οποίων μπορεί να βοηθήσει η IBM (έως δέκα (10) σενάρια χρήσης και έως δύο (2) εφαρμογές).
- Πληροφορίες γενικού επιπέδου για τις πηγές δεδομένων καταγραφής και ροών του Πελάτη που θα είναι απαραίτητες για την υποστήριξη των σεναρίων χρήσης.
- Ζητήματα σχετικά με τη δικτυακή υποδομή, όπως π.χ. τα τείχη προστασίας (firewalls) και οι θύρες (ports).

Με βάση την αναφορά αρχιτεκτονικής της λύσης, η IBM θα εκτελέσει τις ακόλουθες εργασίες εφόσον επαρκεί ο υπολειπόμενος χρόνος:

- Παραμετροποίηση της συλλογής συμβάντων για τρεις (3) το πολύ περιπτώσεις χρήσης δέκα (10) το πολύ ειδών πηγών δεδομένων καταγραφής στην Υπηρεσία Cloud. Η δραστηριότητα αυτή θα περιλαμβάνει τη μεταφορά τεχνογνωσίας στα αρμόδια μέλη του προσωπικού του Πελάτη ώστε να μπορούν να προσθέσουν επιπλέον πηγές δεδομένων καταγραφής αν είναι απαραίτητο. Μόνο οι πηγές δεδομένων καταγραφής που υποστηρίζονται από τα πρότυπα QRadar Device Support Modules (DSMs) θα περιλαμβάνονται ως τμήμα αυτής της υπηρεσίας.
- Αρχική ρύθμιση, η οποία περιλαμβάνει α) την ενεργοποίηση τυποποιημένων κανόνων, αποθηκευμένων αναζητήσεων, γραφημάτων και αναφορών αθροιστικών χρονοσειρών, β) τον εντοπισμό και αφαίρεση πηγών "θορύβου" και γ) την παραμετροποίηση της εκτός σύνδεσης αποθήκευσης μέσω NFS, CIFS ή iSCSI.
- Υλοποίηση των δέκα (10) σεναρίων χρήσης και των δύο (2) εφαρμογών από το IBM QRadar App Exchange, όπως τεκμηριώνεται στο έγγραφο αρχιτεκτονικής της λύσης.

b. IBM QRadar on Cloud Custom Parser Service

Αυτή η υπηρεσία προβλέπει την ανάπτυξη ενός (1) προσαρμοσμένου συντακτικού αναλυτή/uDSM για την υποστήριξη μη τυπικών ειδών πηγών δεδομένων καταγραφής που θα αποστέλλονται στην Υπηρεσία Cloud και περιλαμβάνει τις ακόλουθες εργασίες:

- Δημιουργία ενός προσαρμοσμένου συντακτικού αναλυτή (parser) για ένα (1) μη τυπικό είδος πηγής δεδομένων καταγραφής (η εργασία αυτή θα εκτελεστεί εξ αποστάσεως),
- Δημιουργία, παραμετροποίηση και συσχέτιση ενός uDSM,
- Θέση σε εφαρμογή και δοκιμή του προσαρμοσμένου uDSM, και
- Συντακτική ανάλυση (parsing) έως είκοσι πέντε ειδών μηνυμάτων για την πηγή δεδομένων καταγραφής.

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>.

<https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=FB0F42F0750011E6865BC3F213DB63F7>

3. Επίπεδα Παροχής Υπηρεσιών και Τεχνική Υποστήριξη

3.1 Σύμβαση Επιπέδου Παροχής Υπηρεσιών

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	Πίστωση (% 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. Χρέώσεις

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.
- Συμβάντα ανά Δευτερόλεπτο (Events per Second) είναι το πλήθος των εμφανίσεων ανά δευτερόλεπτο ενός συγκεκριμένου συμβάντος που βρίσκεται υπό την επεξεργασία των Υπηρεσιών Cloud ή σχετίζεται με τη χρήση των Υπηρεσιών Cloud.
- Ροές ανά Δευτερόλεπτο (Flows per Minute) είναι το πλήθος των ροών ανά δευτερόλεπτο τις οποίες διαχειρίζονται ή επεξεργάζονται οι Υπηρεσίες Cloud. Ροή (Flow) είναι μια καταγεγραμμένη

επικοινωνία μεταξύ δύο υπολογιστικών συστημάτων. Τα πακέτα που περιέχουν την ίδια διεύθυνση IP προέλευσης, διεύθυνση IP προορισμού, θύρα προέλευσης, θύρα προορισμού και πρωτόκολλο συνδυάζονται σε μία εγγραφή Ροής.

- Περιουσιακό Στοιχείο (Asset) είναι ένας υλικός πόρος ή ένα αντικείμενο αξίας με μοναδικά στοιχεία ταυτότητας στο οποίο έχουν πρόσβαση οι Υπηρεσίες Cloud ή το οποίο βρίσκεται υπό τη διαχείριση των Υπηρεσιών Cloud.

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 Λογισμικό Ενεργοποίησης

Το λογισμικό ενεργοποίησης παρέχεται στον Πελάτη βάσει των παρακάτω όρων:

Λογισμικό Ενεργοποίησης	Ισχύοντες Όροι Άδειας Χρήσης (αν υπάρχουν)
Data Gateway	Ο Πελάτης επιτρέπεται να εγκαταστήσει και να χρησιμοποιεί έως δέκα (10) αντίγραφα του Data Gateway.

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.