IBM QRadar Advisor with Watson

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

Η υπηρεσία IBM QRadar Advisor with Watson επεκτείνει τις λειτουργίες γνωσιακής ανάλυσης του QRadar Security Platform, βοηθώντας τους Πελάτες και τους αναλυτές ασφάλειας στη 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 ανταπόκριση σε περιστατικά και τη λήψη 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.

1.1 Προσφορές

Ο Πελάτης μπορεί να επιλέξει από τις ακόλουθες διαθέσιμες προσφορές.

1.1.1 IBM QRadar Advisor with Watson

Προϋπόθεση για τη χρήση του IBM QRadar Advisor with Watson είναι ότι ο Πελάτης έχει ένα ενεργό περιβάλλον IBM QRadar, είτε τοπικά στις εγκαταστάσεις του Πελάτη είτε στο cloud, και έχει εγκαταστήσει το λογισμικό ενεργοποίησης της Υπηρεσίας Cloud στο εν λόγω περιβάλλον ώστε να είναι δυνατή η πρόσβαση του Πελάτη στις λειτουργίες του. Όταν η Υπηρεσία Cloud διαθέτει δικαιώματα για Συμβάντα ανά Δευτερόλεπτο, περιέχει ένα όριο για τον αριθμό αιτημάτων αναζήτησης πληροφοριών για παραβιάσεις ασφάλειας που ο Πελάτης μπορεί να υποβάλει στην ΥπηρεσίαCloud, το οποίο είναι 1,5 αιτήσεις την ημέρα ανά 100 Συμβάντα ανά Δευτερόλεπτο (στρογγυλοποιημένη στο πλησιέστερο ερώτημα) για τα οποία ο Πελάτης διαθέτει τα απαιτούμενα δικαιώματα. Όταν η Υπηρεσία Cloud διαθέτει δικαιώματα για Υπό Διαχείριση Εικονικό Εξυπηρετητή (MVS), περιέχει ένα 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 100 MVS για τα οποία ο Πελάτης διαθέτει τα απαιτούμενα δικαιώματα. Τα αιτήματα αναζήτησης πληροφοριών που υποβάλλονται καθ' υπέρβαση αυτού του ορίου θα τίθενται σε χαμηλότερη προτεραιότητα και ενδέχεται να μην υφίστανται επεξεργασία από την Υπηρεσία Cloud για το υπόλοιπο της εν λόγω ημέρας.

1.1.2 IBM QRadar Advisor with Watson – Enterprise

Το IBM QRadar Advisor with Watson – Enterprise είναι η πλέον κατάλληλη λύση για μεγάλα Κέντρα Επιχειρησιακών Λειτουργιών Ασφάλειας (Security Operations Center - "Κέντρο SOC") που υπερβαίνουν γενικά τις διακόσιες πενήντα χιλιάδες Συμβάντα ανά Δευτερόλεπτο. Ο Πελάτης πρέπει να εγκαταστήσει το λογισμικό ενεργοποίησης της Υπηρεσίας Cloud στο περιβάλλον IBM QRadar του, το οποίο πρέπει να αποκτηθεί χωριστά, προκειμένου να έχει πρόσβαση στις λειτουργίες της Υπηρεσίας Cloud. Το IBM QRadar Advisor with Watson – Enterprise καθίσταται διαθέσιμο βάσει ενός μετρικού συστήματος χρέωσης ανά Περίπτωση Χρήσης, το οποίο είναι ανεξάρτητο από την κλίμακα του περιβάλλοντος IBM QRadar του Πελάτη. Ο Πελάτης υπόκειται στον περιορισμό των 25 ερωτημάτων στην ουρά σε οποιαδήποτε δεδομένη στιγμή.

1.1.3 IBM QRadar Advisor with Watson – Starter Pack

Το πακέτο IBM QRadar Advisor with Watson – Starter Pack απευθύνεται σε χρήστες που χρησιμοποιούν για πρώτη φορά το QRadar Advisor with Watson. Αυτή η Υπηρεσία Cloud διαθέτει όλες τις λειτουργίες του QRadar Advisor with Watson, όπως περιγράφονται στο Άρθρο 1.1.1 παραπάνω, αλλά διατίθεται μόνο κατά την πρώτη αγορά του QRadar Advisor with Watson από τον Πελάτη και δεν ανανεώνεται.

1.2 Προαιρετικές Υπηρεσίες

1.2.1 IBM QRadar Advisor with Watson – Test Environment

Το IBM QRadar Advisor with Watson – Test Environment προορίζεται για Πελάτες που θέλουν να χρησιμοποιούν την Υπηρεσία Cloud στο εσωτερικό περιβάλλον διενέργειας δοκιμών τους και μπορεί να χρησιμοποιηθεί μόνο για τη διενέργεια δοκιμών εκτός περιβάλλοντος παραγωγής. Το IBM QRadar Advisor with Watson – Test Environment πρέπει να συνδυαστεί με μια συνδρομή για την Υπηρεσία Cloud για το περιβάλλον παραγωγής.

1.3 Υπηρεσίες Επιτάχυνσης

1.3.1 IBM QRadar Advisor with Watson Advanced Services

Για αυτή την εξ αποστάσεως παραδιδόμενη συνδρομητική υπηρεσία, η IBM θα παρέχει στον Πελάτη οποιαδήποτε από τις ακόλουθες συμβουλευτικές υπηρεσίες έως και για πέντε (5) ημέρες στη διάρκεια ενός (1) έτους:

- Διεργασία αξιολόγησης Κέντρου SOC Πελάτη (συμπεριλαμβανομένης της διεργασίας διερεύνησης περιστατικών ή/και απόκρισης σε περιστατικά)
- Επαναξιολόγηση απόκρισης συνόλων αναφοράς
- Προσαρμογή αυτόματης ανάλυσης για σοβαρές παραβιάσεις
- Ανάπτυξη σεναρίων χρήσης
- Παροχή συστάσεων για τις αλλαγές στις διεργασίες του Κέντρου SOC που σχετίζονται με το QRadar Advisor with Watson
- Καθοδήγηση για την αποτελεσματικότερη κατανόηση και ενσωμάτωση των δεδομένων από το QRadar Advisor with Watson στις υπάρχουσες διεργασίες του Πελάτη
- Μεταφορά γνώσεων για ζητήματα που σχετίζονται με το QRadar Advisor with Watson

ΣΗΜΕΙΩΣΗ: Οι ακόλουθες δραστηριότητες μπορούν να ενσωματωθούν σε αυτή την υπηρεσία με βάση την κατάσταση της υλοποίησης του QRadar του Πελάτη:

- Εκτέλεση ενός γενικού ελέγχου υγείας της υλοποίησης του QRadar του Πελάτη
- Πραγματοποίηση πρόσθετων ρυθμίσεων στην υπάρχουσα υλοποίηση του QRadar
- Παροχή βοήθειας για την προσθήκη πρόσθετων πηγών δεδομένων καταγραφής στην υλοποίηση του QRadar του Πελάτη

1.3.2 IBM QRadar Advisor with Watson Basic Setup Service

Πρόκειται για μια εξ αποστάσεως παραδιδόμενη υπηρεσία προετοιμασίας διάρκειας σαράντα (40) ωρών που λήγει ενενήντα (90) ημέρες μετά την αγορά, εκτός αν αναφέρεται διαφορετικά, ανεξάρτητα από το αν θα έχουν χρησιμοποιηθεί όλες οι ώρες. Οι υπηρεσίες περιλαμβάνουν έναν καθορισμένο IBM Engagement Manager ο οποίος θα προγραμματίσει τη διεξαγωγή οποιωνδήποτε εναρκτήριων τηλεδιασκέψεων.

Η IBM θα προβεί στην εκτέλεση μερικών από ή όλων των ακόλουθων εργασιών:

- Διεργασία αξιολόγησης Κέντρου SOC Πελάτη (συμπεριλαμβανομένης της διεργασίας διερεύνησης περιστατικών ή/και απόκρισης σε περιστατικά)
- Υλοποίηση του QRadar Advisor with Watson στο περιβάλλον του Πελάτη:
    - Εγκατάσταση του QRadar Advisor with Watson
    - Αντιστοίχιση ενοποιημένων ιδιοτήτων στο QRadar Advisor with Watson
    - Υλοποίηση απόκρισης συνόλων αναφοράς
    - Προσαρμογή αυτόματης ανάλυσης για σοβαρές παραβιάσεις
    - Καθοδήγηση σεναρίων χρήσης

- Παροχή συστάσεων για τις αλλαγές στις διεργασίες του Κέντρου SOC που σχετίζονται με το QRadar Advisor with Watson

1.3.3 IBM QRadar Advisor with Watson Quick Setup Service

Αυτή η υπηρεσία ρύθμισης έχει σχεδιαστεί για Πελάτες με λιγότερα από 5.000 συμβάντα ανά δευτερόλεπτο (EPS).

Για αυτή την εξ αποστάσεως παραδιδόμενη υπηρεσία, η IBM θα παρέχει στον Πελάτη οποιαδήποτε από τις ακόλουθες συμβουλευτικές υπηρεσίες (ή συνδυασμό αυτών) έως και για 16 ώρες στη διάρκεια μια περιόδου 90 ημερών:

- Εγκατάσταση QRadar Advisor with Watson.
- Διαχείριση δικαιωμάτων για το QRadar Advisor with Watson.
- Παραμετροποίηση του QRadar Advisor with Watson, η οποία μπορεί να περιλαμβάνει:
  - Παραμετροποίηση ασφαλούς εξυπηρετητή μεσολάβησης.
  - Υποβολή στοιχείων ταυτότητας X-Force Exchange.
  - Δημιουργία εξουσιοδοτημένων διακριτικών υπηρεσίας.
  - Παραμετροποίηση πολιτικών διατήρησης για την αποθήκευση αποτελεσμάτων ανάλυσης.
  - Αντιστοίχιση προσαρμοσμένων ιδιοτήτων συμβάντων.
  - Εξαγωγή συνόλων αναφοράς.
  - Αντιστοίχιση πληροφοριών για απειλές.
  - Παραμετροποίηση προσδιορισμού πόρων.
  - Βελτιστοποίηση χρήσης.
- Αυτόματη διερεύνηση επιθέσεων και αποτελεσμάτων (επίδειξη τουλάχιστον μίας περίπτωσης χρήσης).
- Εξερεύνηση τεκμηριωμένων πληροφοριών με το γράφημα σχέσης.

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=0B439290AB5011E6BE74C84817AAB206

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:

- Συμβάντα ανά Δευτερόλεπτο (Events per Second (EPS)) 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. Για το σκοπό αυτής της Υπηρεσίας Cloud, τα μετρούμενα Συμβάντα ανά Δευτερόλεπτα είναι εκείνα τα συμβάντα που συλλέγονται και υφίστανται επεξεργασία από το περιβάλλον IBM QRadar του Πελάτη.
- Περίπτωση Χρήσης (Instance) είναι κάθε πρόσβαση σε μια συγκεκριμένη παραμετροποίηση των Υπηρεσιών Cloud.
- Δέσμευση (Engagement) είναι μια επαγγελματική ή εκπαιδευτική υπηρεσία που σχετίζεται με τις Υπηρεσίες Cloud.
- Ένας Διαχειριζόμενος Εικονικός Εξυπηρετητής (Managed Virtual Server) αποτελείται από μονάδες επεξεργασίας, μνήμη και δυνατότητες εισόδου/εξόδου και εκτελεί ζητούμενες διαδικασίες, εντολές ή εφαρμογές των οποίων η διαχείριση γίνεται από τις Υπηρεσίες 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

Η Υπηρεσία Cloud περιέχει το ακόλουθο Λογισμικό Ενεργοποίησης:

- IBM QRadar with Watson App (https://exchange.xforce.ibmcloud.com/hub)

5.2 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.

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. 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.