Περιγραφή QRADAR

To IBM® QRadar® SIEM είναι μια πλατφόρμα που ενοποιεί τα γεγονότα καταγραφής και τα δεδομένα της ροής του δικτύου από συσκευές, τελικά σημεία και τις εφαρμογές που διανέμονται σε όλο το δίκτυο.

Έχει την δυνατότητα να ομαλοποιεί και να συσχετίζει ανεπεξέργαστα δεδομένα για τον εντοπισμό παραβάσεων της ασφάλειας. Η πλατφόρμα χρησιμοποιεί μια προηγμένη μηχανή Sense Analytics για να καταγράφει τις τιμές της φυσιολογικής συμπεριφοράς, να επιτρέπει την ανίχνευση ανωμαλιών, και να παρέχει τη δυνατότητα να αποκαλύπτει προηγμένες απειλές, και να αφαιρεί τα faulse positives.

Στις τελευταίες του εκδόσεις το λογισμικό αυτό έχει ενσωματωμένο το IBM X-Force® Threat Intelligence, που παρέχει μια λίστα με τις δυνητικά κακόβουλες διευθύνσεις IP, συμπεριλαμβανομένων malware hosts, πηγές spam και άλλες απειλές.

Προκειμένου να υπάρξει αξιοποίηση των παρεχόμενων αναφορών της πλατφόρμας Qradar για περιστατικά που αφορούν την ασφάλεια των Πληροφοριακών Συστημάτων της Βουλής, είναι επιθυμητό όποτε αυτό κριθεί απαραίτητο από την Υπηρεσία, να παρασχεθούν από τον ανάδοχο συμβουλευτικές υπηρεσίες αλλά κυρίως υπηρεσίες αντιμετώπισης των περιστατικών ασφαλείας που ανιχνεύονται από την εν λόγω πλατφόρμα. και συνίστανται κυρίως σε επιβεβλημένη έκτακτη αλλαγή στοιχείων ασφάλειας του πληροφοριακού συστήματος, ή και τροποποίηση απαιτήσεων που παρέχονται από το πληροφοριακό σύστημα.

Ο ανάδοχος θα πρέπει να είναι πιστοποιημένος κατά ISO/IEC 27001:2013 και επίσης να διαθέτει τεχνικό που να είναι πιστοποιημένος για παροχή υπηρεσιών υποστήριξης του προϊόντος QRadar Security v7.x.x

Οι άδειες που έχει στην κατοχή της η Βουλή και οι οποίες χρειάζονται ανανέωση είναι στον επισυναπτόμενο πίνακα.