3 Οκτωβρίου 2016

Apache Spot: σε αναζήτηση της κυβερνο – ασφάλειας

/ Πεμπτουσία

Image not found or type unknown

Μετά την ανακάλυψη της μεγαλύτερης -γνωστής- παραβίασης δεδομένων στην ιστορία, οι Cloudera και Intel ανακοίνωσαν την Τετάρτη ότι έχουν δωρίσει ένα νέο open source project στο Apache Software Foundation, με σκοπό να χρησιμοποιηθεί για big data analytics και μηχανική μάθηση για την ασφάλεια στον κυβερνοχώρο.

Αρχικά δημιουργήθηκε από την Intel και ξεκίνησε ως Open Network Insight (ONI) project το Φεβρουάριο. Ωστόσο, η προσπάθεια αυτή τώρα ονομάζεται Apache Spot και έχει γίνει δεκτή στο ASF Incubator.

«Η ιδέα είναι, ας δημιουργήσουμε ένα κοινό μοντέλο δεδομένων από το οποίο κάθε προγραμματιστής εφαρμογών μπορεί να επωφεληθεί φέρνοντας νέες δυνατότητες analytics για να αντιμετωπιστούν προβλήματα σχετικά με την ασφάλεια στον κυβερνοχώρο», είπε ο Mike Olson, συν-ιδρυτής της Cloudera και διευθύνων

σύμβουλος στρατηγικής, σε ένα ακροατήριο στο Strata+Hadoop World σόου στη Νέα Υόρκη. «Πρόκειται για μια μεγάλη υπόθεση και θα μπορούσε να έχει τεράστιο αντίκτυπο σε όλο τον κόσμο.»

Βασισμένο σε μια big data πλατφόρμα της Cloudera, το Spot χρησιμοποιεί το Apache Hadoop για άπειρη διαχείριση καταγραφής και κλίμακα αποθήκευσης δεδομένων, μαζί με το Apache Spark για μηχανική μάθηση και σχεδόν σε πραγματικό χρόνο ανίχνευση ανωμαλιών. Το λογισμικό μπορεί να αναλύσει δισεκατομμύρια γεγονότα με σκοπό τον εντοπισμό άγνωστων και εμπιστευτικών απειλών και την παροχή νέας ορατότητας δικτύου.

Ουσιαστικά, χρησιμοποιεί μηχανική μάθηση ως φίλτρο για το διαχωρισμό κακής κυκλοφορίας από την καλή και για να χαρακτηρίζει τη συμπεριφορά της κίνησης του δικτύου. Επίσης, χρησιμοποιεί μια διαδικασία, συμπεριλαμβανομένων των: εμπλουτισμός κειμένου, φιλτράρισμα θορύβου, whitelisting και heuristics για να παράγει μια λίστα από τα πιο πιθανές απειλές ασφάλειας.

Με την παροχή κοινών open data μοντέλων για το δίκτυο, το endpoint και τον χρήστη, το Spot κάνει ευκολότερη την ενσωμάτωση cross-application δεδομένων για καλύτερη ορατότητα των επιχειρήσεων και νέες analytic λειτουργίες. Αυτά τα open data μοντέλα δεδομένων καθιστούν ευκολότερο για τους οργανισμούς να μοιράζονται analytics καθώς και νέες απειλές που ανακαλύπτονται.

Άλλοι χρηματοδότες του project μέχρι στιγμής είναι οι eBay, Webroot, Jask, Cybraics, Cloudwick και Endgame.

«Η open source κοινότητα είναι το τέλειο περιβάλλον για το Apache Spot, ώστε να λάβει μια συλλογική προσέγγιση για να καταπολεμήσει το έγκλημα στον κυβερνοχώρο», δήλωσε ο Ρον Kasabian, αντιπρόεδρος και γενικός διευθυντής του Analytics and Artificial Intelligence Solutions Group της Intel. «Η συνδυασμένη εμπειρία των συνεργατών θα βοηθήσει περαιτέρω το open data όραμα του Apache Spot και θα θέσει βάσεις για συνεργασία απέναντι σε πιο δύσκολες και συνεχώς εξελισσόμενες προκλήσεις του κόσμου γύρω από το cybersecurity analytics.»

Πηγή: secnews.gr