Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Πληροφοριακά και Επικοινωνιακά Συστήματα

Μεταπτυχιακή Διατριβή

Ανίχνευση Εσωτερικών Απειλών με Χρήση Αλγορίθμων Τεχνητής Νοημοσύνης

Ιωάννης Πίτρης

Επιβλέπων Καθηγητής

Δρ. Σταύρος Σιαηλής

Ιανουάριος 2017

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών

Πληροφοριακά και Επικοινωνιακά Συστήματα

Μεταπτυχιακή Διατριβή

Ανίχνευση Εσωτερικών Απειλών με Χρήση Αλγορίθμων Τεχνητής Νοημοσύνης

Ιωάννης Πίτρης

Επιβλέπων Καθηγητής

Δρ. Σταύρος Σιαηλής

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στα Πληροφοριακά και Επικοινωνιακά Συστήματα από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Ιανουάριος 2017

ΛΕΥΚΗ ΣΕΛΙΔΑ

Περίληψη

Οι εσωτερικές απειλές αποτελούν ένα μεγάλο πρόβλημα για τους οργανισμούς. Οι αναφορές ασφάλειας από κορυφαίους οργανισμούς επισημαίνουν ότι παρόλα τα σύγχρονα και περιμετρικά σύστημα ασφαλείας που διαθέτουν, οι κυβερνοεγκληματίες κατάφεραν να διεισδύσουν και να αποσπάσουν πληροφορίες ύψιστης σημασίας από τους οργανισμούς αυτούς. Για αυτό το λόγο η ανίχνευση των εσωτερικών απειλών είναι υψίστης σημασίας. Όμως η ανίχνευση των εσωτερικών απειλών είναι ένα θέμα αρκετά δύσκολο και πολυπαραγωντικό. Μέχρι τώρα δεν έχει βρεθεί κάποια μέθοδος που να μπορεί να μας δώσει με ακρίβεια ή να προβλέψει συμπεριφορές που μπορεί να οδηγήσουν σε τέτοιου είδους ενέργειες που είναι καταστροφικές για τους οργανισμούς.

Η παρούσα μεταπτυχιακή διατριβή έχει ως κύριο στόχο την δημιουργία ενός συστήματος το οποίο θα εντοπίζει τις εσωτερικές απειλές σε ένα εταιρικό δίκτυο χωρίς να εξαρτάται από το λειτουργικό σύστημα και χωρίς ανθρώπινη παρέμβαση.

Για τον εντοπισμό των εσωτερικών απειλών υλοποιήθηκε η εφαρμογή ITDS, η οποία βασίζεται στους αλγορίθμους τεχνητής νοημοσύνης SOM και ESOINN. Η εφαρμογή προσαρμόστηκε κατάλληλα, ώστε να δοκιμαστεί στο σύνολο δεδομένων για εσωτερικές απειλές του CERT και η εκπαίδευση των αλγορίθμων SOM και ESOINN πραγματοποιήθηκε στο ίδιο δείγμα δεδομένων.

Τα αποτελέσματα δείχνουν ότι και οι δύο αλγόριθμοι εντοπίζουν με υψηλά ποσοστά ακρίβειας τις εσωτερικές απειλές που υπάρχουν στο συγκεκριμένο σύνολο δεδομένων. Συγκεκριμένα και οι δύο αλγόριθμοι είχαν 100% ανάκληση για την αναγνώριση των εσωτερικών απειλών του πρώτου σεναρίου του συνόλου δεδομένων.

Λέξεις κλειδιά: Εσωτερικές Απειλές, Τεχνητή Νοημοσύνη

Summary

Nowadays, insider threats comprise some of the greatest concerns for companies and corporations. According to security reports by leading organizations, cyber-criminals have managed to infiltrate and obtain information of utmost importance from these organizations, despite the available modern and perimeter security systems they have at their disposal. For this reason, the detection of insider threats is of great importance. However, detection of insider threats seems to be quite a difficult issue with different multifaceted components. There is no known method yet, which would provide us with accurate results or predict any harmful behaviors in order to prevent detrimental effects of malicious actions against these organizations.

The main objective of this thesis is to create a system that will identify insider threats in a corporate network irrespective of the operating system or human intervention.

Detection of insider threats it was carried out by the ITDS application which is based on artificial intelligence algorithms SOM and ESOINN. The application was made suitable to be tested in the insider threat dataset of CERT, while the training of SOM and ESOINN algorithms was held on the same sample data.

Our results prove that both algorithms can detect insider threats within this dataset while showing high accuracy rates. Specifically both algorithms showed 100% recall for the detection of insider threats in the first scenario of dataset.

Keywords: Insider threats, SOM, ESOINN, Artificial Intelligence

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον Υπεύθυνο Καθηγητή μου Δρ. Σταύρο Σιαηλή για την καθοδήγηση την οποία μου παρείχε, ώστε να επιτευχθεί η ολοκλήρωση και η παράδοση της παρούσας μεταπτυχιακής διατριβής. Την υπομονή και την επιμονή που είχε δείξει, ώστε να βρεθεί ένα θέμα αντάξιο των δυνατοτήτων και γνώσεων μου.

Ιδιαίτερες ευχαριστίες θέλω να απευθύνω στην Δρ. Μαρία Παπαδάκη για την καθοδήγηση και την πολύτιμη βοήθεια κατά τα πρώτα στάδια της έρευνάς μας.

Τέλος, θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες προς τα άτομα της οικογένειας μου για την θερμή τους συμπαράσταση καθ΄ όλη τη διάρκεια διεκπεραίωσης της παρούσας μεταπτυχιακής διατριβής.

Περιεχόμενα

Εικόνες

Πίνακες

Κεφάλαιο 1

Εισαγωγή

Στις μέρες μας οι εταιρίες αντιμετωπίζουν μεγάλο πρόβλημα στην διατήρησης της ασφάλεια των υποδομών πληροφορικής. Οι περισσότεροι οργανισμοί επενδύουν τεράστια ποσά για την ενίσχυση των επιπέδων ασφάλειας των υποδομών τους με σκοπό την αντιμετώπιση των εξωτερικών απειλών, όπως DDoS, Brute force attacks, Buffer Overflows κ.α., πράγμα το οποίο έχει επιτευχθεί σε αρκετά μεγάλο βαθμό. Από ότι έχει παρατηρηθεί τα τελευταία χρόνια οι περισσότερες σημαντικές παραβιάσεις δεδομένων σε μεγάλους οργανισμούς είναι δουλειά «εκ των έσω». Σύμφωνα με έρευνα που πραγματοποίησε η εταιρία Spotlight (Landers 2016) το 56% των ειδικών ασφαλείας που ερωτήθηκαν, δηλώνει ότι οι εσωτερικές απειλές έχουν γίνει περισσότερο συχνές τους τελευταίους 12 μήνες. Χαρακτηριστικό είναι ότι το 74% των οργανισμών νιώθει ευάλωτο στις εσωτερικές απειλές, ποσοστό που έχει αυξηθεί κατά 7 μονάδες από την έρευνα του προηγούμενου χρόνου της ίδιας εταιρίας.

Αρκετοί ερευνητές έχουν ερμηνεύσει τους όρους «εσωτερικός» και «εσωτερική απειλή». Εσωτερικός μπορεί να είναι κάποιος που είναι εξουσιοδοτημένος να χρησιμοποιεί υπολογιστές ή δίκτυα (Schultz 2002). Επίσης αναλογιζόμενοι την πρόσβαση σε βάσεις δεδομένων, εσωτερικός είναι ο χρήστης της βάσης δεδομένων που έχει προσωπική γνώση σε απόρρητα δεδομένα (Garfinkel et al. 2002). Στην έρευνα του RAND (Brackney & Anderson 2004) ορίζεται ως «εσωτερικός» ο οποιοσδήποτε έχει πρόσβαση, δικαιώματα ή γνώση των πληροφοριακών συστημάτων και υπηρεσιών. Ως εκ τούτου ορίζεται ως «κακόβουλος εσωτερικός» ο οποιοσδήποτε έχει κίνητρο να προκαλέσει ζημιά στην αποστολή του οργανισμού. Παρατηρούμε ότι οι διάφοροι ορισμοί της έννοιας εσωτερικός εξαρτώνται από την ερμηνεία και την έμφαση σε ένα ή περισσότερα από τα χαρακτηριστικά: πρόσβαση στο σύστημα, ικανότητα

αναπαράστασης του οργανισμού, γνώση και εμπιστοσύνη του οργανισμού (Hunker & Probst 2011).

Μία άλλη προσέγγιση των παραπάνω εννοιών γίνεται σε σχέση με τις πολιτικές ασφαλείας ενός οργανισμού (Bishop et al. 2008). Εσωτερικός ορίζεται ως ένα άτομο το οποίο έχει νόμιμα εξουσιοδοτηθεί με δικαιώματα να έχει πρόσβαση, να εκπροσωπεί ή να αποφασίζει σχετικά με ένα ή περισσότερα περιουσιακά στοιχεία της σύστασης του οργανισμού. Το σκεπτικό πίσω από αυτό τον ορισμό είναι ότι εστιάζει στα περιουσιακά στοιχεία του οργανισμού και όχι σε μία προσέγγιση που περιορίζεται στα διαπιστευτήρια του συστήματος, και ενώ στους ανθρώπους που αποτελούν απειλές μπορεί να μην τους παρέχεται πρόσβαση στα διαπιστευτήρια, μπορούν ακόμα να έχουν την δυνατότητα να αποφασίζουν, βασιζόμενοι στις πολιτικές του εκάστοτε οργανισμού και να τον εκπροσωπούν.

Λαμβάνοντας υπόψιν τον παραπάνω ορισμό για το τι είναι εσωτερικός, ορίζεται ως εσωτερική απειλή κάποιος νυν ή πρώην υπάλληλος, εργολάβος, ή άλλος επιχειρηματικός συνεργάτης, ο οποίος έχει ή είχε εξουσιοδοτημένη πρόσβαση στο δίκτυο, στο σύστημα ή στα δεδομένα ενός οργανισμού και εκ προθέσεως ξεπέρασε ή καταχράστηκε αυτή την πρόσβαση με τέτοιο τρόπο που επηρέασε αρνητικά την εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα των πληροφοριών ή των πληροφοριών συστημάτων του οργανισμού (Mundie et al. 2013).

Το τμήμα CERT του πανεπιστημίου Carnegie Mellon, το οποίο από το 2001 ασχολείται με την πρόβλεψη, τον εντοπισμό και τους τρόπους ανταπόκρισης στο πρόβλημα των εσωτερικών απειλών, αναγνωρίζει τρεις τύπους κακόβουλων εσωτερικών βάση των συγκεκριμένων χαρακτηριστικών τους και των εγκλημάτων τους: κλοπή πνευματικής ιδιοκτησίας, απάτη και δολιοφθορά των πληροφοριακών υποδομών του οργανισμού (Cappelli et al. 2012).

Στην κλοπή πνευματικής ιδιοκτησίας, ο εσωτερικός χρησιμοποιεί την πρόσβασή του στο πληροφοριακό σύστημα για να πάρει αποκλειστικές πληροφορίες του οργανισμού ώστε αφού φύγει να τις χρησιμοποιήσει για την δημιουργία της δικής του επιχείρησης, ως πλεονέκτημα σε μία νέα εργασία ή να τις δώσει σε μία ξένη κυβέρνηση ή οργανισμό. Τέτοιες πληροφορίες μπορεί να είναι πηγαίοι κώδικές, επιστημονικές φόρμουλες,

μηχανολογικά σχέδια ή προτάσεις. Η πλειοψηφία των επιθέσεων φαίνεται να είναι πιο πιθανή από το τεχνολογικό προσωπικό όπως επιστήμονες και μηχανικοί (Spooner et al. 2009). Οι εσωτερικοί συνήθως κλέβουν τις ίδιες πληροφορίες που έχουν πρόσβαση κατά τη διάρκεια τις κανονικής τους εργασίας στα κανονικά ωράρια εργασίας και γι' αυτό το λόγο μπορεί να είναι πολύ δύσκολο να γίνει διάκριση της παράνομης από της νόμιμης πρόσβασης.

Στην εσωτερική απάτη ένας κακόβουλος εσωτερικός χρησιμοποιεί τις γνώσεις του στην πληροφορική για τη μη εξουσιοδοτημένη μετατροπή, προσθήκη ή διαγραφή των δεδομένων του οργανισμού, όχι των προγραμμάτων ή των συστημάτων, για προσωπικό όφελος ή κλοπή πληροφοριών που οδηγούν σε ένα έγκλημα ταυτότητας (Weiland et al. 2012). Το έγκλημα ταυτότητας είναι η κατάχρηση των προσωπικών ή οικονομικών αναγνωριστικών, προκειμένου να αποκτηθεί κάτι αξίας και να διευκολυνθεί κάποια άλλη εγκληματική δραστηριότητα. Ανησυχητικό είναι ότι ο αριθμός των κρουσμάτων απάτης συνεχίζει να ανεβαίνει τα τελευταία χρόνια. Το ποσοστό των επιχειρήσεων που αναφέρει ότι έχει πέσει θύμα απάτης μέσα στα προηγούμενα χρόνια έχει ανέλθει στο 75%, το οποίο αυξήθηκε κατά 14% από πριν 3 χρόνια (Kroll 2015). Από τα ευρήματα της έρευνας διαπιστώθηκε ότι η μεγαλύτερη απειλή απάτης για τις εταιρίες προέρχεται εκ των έσω. Από το σύνολο των εταιριών που εξαπατήθηκαν, το 81% υπέστη απάτη από κάποιον εσωτερικό, ποσοστό που ήταν 72% σε προηγούμενη έρευνα. Ειδικότερα, το 36% των θυμάτων βίωσαν απάτη από τα χέρια των δικών τους ανωτέρων ή μεσαίων στελεχών, το 45% από έναν κατώτερο σε σχέση με αυτούς υπάλληλο και το 23% εξαπατήθηκαν από την συμπεριφορά ενός πράκτορα ή μεσάζοντα.

Η δολιοφθορά των πληροφοριακών υποδομών του οργανισμού συνήθως διαπράττεται από τεχνικό προσωπικό με προνομιακή πρόσβαση, όπως οι διαχειριστές συστήματος, οι διαχειριστές βάσεων δεδομένων και οι προγραμματιστές. Ένα παράδειγμα τέτοιας επίθεσης έγινε το 2012 όταν ένας αρχιτέκτονας συστήματος ειδοποιήθηκε για την απόλυσή του (αφού είχε μεταδώσει μη εξουσιοδοτημένο υλικό) (Miller 2016). Αφού χρησιμοποίησε απομακρυσμένη πρόσβαση για να διαγράψει δεδομένα και να επαναρυθμίσει τους διακομιστές, απενεργοποίησε τα συστήματα ψύξης των υπολογιστών. Ο οργανισμός θύμα, που υπέστη την ζημιά ήταν μια εταιρία ενέργειας, η οποία ανέφερε πάνω από 1 εκατομμύριο δολάρια ζημιά. Στην έρευνα των (Moore et al. 2008) διαπιστώθηκε ότι η δυσαρέσκεια του εργαζόμενου, η οποία οφειλόταν σε

κάποιες ανεκπλήρωτες προσδοκίες, ήταν ένα επαναλαμβανόμενο στοιχείο για να πραγματοποιηθεί η επίθεση στον οργανισμό. Επίσης στις περισσότερες περιπτώσεις, οι εσωτερικοί είχαν βιώσει ένα ή περισσότερα αγχωτικά γεγονότα, συμπεριλαμβανόμενων των κυρώσεων και άλλων αρνητικών γεγονότων που σχετίζονται με την εργασία. Ένα επιπλέον χαρακτηριστικό ήταν η έλλειψη φυσικού και ηλεκτρονικού ελέγχου πρόσβασης.

Αν και οι προσπάθειες πρόβλεψης, εντοπισμού και μετριασμού των εσωτερικών απειλών εστιάζονται στους παραπάνω τύπους επιθέσεων, οι οποίοι προέρχονται από πρόθεση, έχει αρχίσει να δίνεται μεγαλύτερη προσοχή και στις απειλές που προκύπτουν ακούσια. Η εταιρία Symantec στην έρευνα της για το 2015 αναφέρει ότι το ποσοστό των ταυτοτήτων που εκτέθηκαν στην δημοσιότητα χωρίς πρόσθεση ανέβηκε στο 48% από το 22% του έτους 2014 (Symantec 2016). Αυτή η μορφή επίθεσης προκύπτει από άτομα που έχουν νόμιμη πρόσβαση στο σύστημα λόγω αμέλειας ή ατυχήματος. Παραδείγματα τέτοιων ενεργειών είναι η απώλεια αποθηκευτικών συσκευών ή φορητών υπολογιστών.

Οι εσωτερικές απειλές θεωρούνται από τα πιο δύσκολα αντιμετωπίσιμα προβλήματα καθώς οι εσωτερικοί συχνά έχουν πληροφορίες και δυνατότητες οι οποίες είναι άγνωστες στους εξωτερικούς επιτιθέμενους. Συνεπώς μπορούν να προκαλέσουν σοβαρή ζημιά στις υποδομές ενός οργανισμού. Ο κύριος στόχος της παρούσας μεταπτυχιακής εργασίας είναι η αποτελεσματική και όσο το δυνατόν έγκαιρη ανίχνευση των εσωτερικών απειλών στο δίκτυο ενός οργανισμού ανεξαρτήτως του λειτουργικού συστήματος. Για το σκοπό αυτό, προτείνεται μια μεθοδολογία συγκέντρωσης και ανάλυσης δεδομένων με χρήση αλγορίθμων τεχνητής νοημοσύνης SOM (αυτό-οργανωμένοι χάρτες) και ESOINN (ενισχυμένα αυτό-οργανωμένα αυξητικά νευρωνικά δίκτυα). Για επαλήθευση της αποτελεσματικότητας της μεθοδολογίας γίνεται μια υλοποίηση σε Java με σκοπό την εξαγωγή συμπερασμάτων αποτελεσματικότητας και σύγκριση με άλλες μεθόδους.

Η παρούσα μεταπτυχιακή διατριβή χωρίζετε σε 7 κεφάλαια. Στο κεφάλαιο 2 επιχειρείται μια περιγραφή των σημαντικότερων ερευνών για την πρόληψη και τον εντοπισμό των εσωτερικών απειλών. Αναφέρουμε τις μεθόδους, που έχουν

χρησιμοποιήσει άλλοι ερευνητές για την επίλυσης του προβλήματος των εσωτερικών απειλών.

Το θεωρητικό υπόβαθρο των αλγορίθμων τεχνητής νοημοσύνης που χρησιμοποιήσαμε παρουσιάζεται στο κεφάλαιο 3. Ειδικότερα γίνεται αναφορά στους αλγορίθμους μη επιτηρούμενης μάθησης SOM, SOINN και ESOINN.

Στο κεφάλαιο 4 περιγράφεται το προτεινόμενο σύστημα το οποίο θα λειτουργεί ανεξαρτήτως λειτουργικού συστήματος. Επίσης περιγράφεται η εφαρμογή, η οποία υλοποιήθηκε για την ανίχνευση των εσωτερικών απειλών.

Η πειραματική διαδικασία αναλύεται στο κεφάλαιο 5. Παρουσιάζεται το σύνολο δεδομένων το οποίο επιλέχθηκε και θα τροφοδοτήσει την εφαρμογή. Στο κεφάλαιο 6 παρουσιάζονται τα αποτελέσματα της πειραματικής διαδικασίας καθώς και τα συμπεράσματα για την απόδοση των αλγορίθμων SOM και ESOINN

Τέλος, μια σύνοψη της δουλειάς που έχει γίνει στην παρούσα μεταπτυχιακή διατριβή καθώς και μελλοντικές επεκτάσεις της εφαρμογής παρουσιάζονται στο κεφάλαιο 7.

Κεφάλαιο 2
Βιβλιογραφική Ανασκόπηση

Σε αυτό το κεφάλαιο θα πραγματοποιηθεί μια ανασκόπηση των μεθόδων ανίχνευσης εσωτερικών απειλών. Το 2002 παρουσιάστηκε το εργαλείο ITPT για την πρόβλεψη των εσωτερικών απειλών, το οποίο στηρίζεται σε τρεις βασικές λειτουργίες (Magklaras & Furnell 2002). Η πρώτη λειτουργία έχει να κάνει με την παρακολούθηση των αρχείων και την θέση των καταλόγων στους οποίους τοποθετούνται. Αυτό στηρίζεται στο γεγονός ότι ορισμένοι τύποι κατάχρησης των ηλεκτρονικών υπολογιστών είναι συνδεμένοι με την τοποθέτηση κάποιον αρχείων σε ορισμένους καταλόγους. Η ανάλυση του περιεχομένου των αρχείων είναι η δεύτερη λειτουργία. Σκοπός της λειτουργίας είναι να ελεγχθούν ορισμένα μοτίβα απειλών, όπως οι υπογραφές των ιών μέσα στα αρχεία. Τελευταία λειτουργία είναι ο έλεγχος της ακεραιότητας των αρχείων, με σκοπό να εξεταστεί αν ένα αρχείο έχει εκτεθεί σε κίνδυνο, όπως τα αρχεία συστήματος. Στην συνέχεια δημιούργησαν μετρικές για την αξιολόγηση των πιθανών απειλών, οι οποίες μετρούν την συμπεριφορά των χρηστών, όπως το περιεχόμενο των αρχείων στους σταθμούς εργασίας τους και την γνώση τους για το σύστημα αρχείων. Η μελέτη είναι περισσότερο θεωρητική και δεν παρουσιάζονται αποτελέσματα για την αποδοτικότητα των μετρικών.

Ένα πλαίσιο για την ανίχνευση των εσωτερικών απειλών προτείνεται από τους (Nurse et al. 2014). Η ανίχνευση γίνεται με την μελέτη τεσσάρων θεματικών αξόνων. Στον πρώτο θεματικό άξονα μελετώνται οι λόγοι που μπορεί να ωθήσουν έναν υπάλληλο να επιτεθεί. Παραδείγματα τέτοιων λόγων μπορεί να είναι η απόλυση και ο υποβιβασμός θέσης. Στον δεύτερο άξονα εξετάζονται τα χαρακτηριστικά της προσωπικότητά του χρήστη όπως τα καθήκοντά του, οι γνώσεις του και το ιστορικό του σε παρόμοια περιστατικά. Στον τρίτο άξονα μελετιούνται τα χαρακτηριστικά πιθανών επιθέσεων. Ο τέταρτος άξονας είναι υπεύθυνος για την μελέτη των χαρακτηριστικών της επιχείρησης

ώστε να βρεθούν οι αδυναμίες του δικτύου της καθώς και οι πιθανοί στόχοι. Στο πλαίσιο αυτό δεν λαμβάνει υπόψιν του υλικό (hardware) του οργανισμού.

Στο επιστημονικό άρθρο (Bishop et al. 2010) προτείνεται μία διαβαθμισμένη έννοια της «εσωτερικότητας». Οι ερευνητές εισάγουν μία ιεράρχηση των διαφόρων επιπέδων των πολιτικών ασφαλείας σε ένα οργανισμό και υποστηρίζουν ότι αυτές οι διαχωρίσεις είναι χρήσιμες για τον εντοπισμό των εσωτερικών απειλών. Παρουσιάζεται το μοντέλο Attribute Based Group Access Control (ABGAC), το οποίο χωρίζει σε ομάδες τα υποκείμενα υπό εξέταση, αλλά και τους πόρους τους οποίους χρησιμοποιούν ανάλογα με τα χαρακτηριστικά που έχουν καθοριστεί. Τα χαρακτηριστικά τα οποία εξετάζουν περιλαμβάνουν το ρόλο εργασίας (όπως ο διαχειριστής συστήματος) και την πρόσβαση στον οργανισμό (όπως η πρόσβαση από τα μεσάνυχτα μέχρι τις 8:00 π.μ.). Για τον εντοπισμό των εσωτερικών απειλών καθορίζονται ομάδες με βάση τις δυνατότητες πρόσβασης και χρησιμοποιούνται για να αναγνωρίσουν τους χρήστες με υψηλό επίπεδο απειλής σε σχέση με τους πόρους υψηλού κινδύνου, χωρίς όμως να παρουσιάζονται αποτελέσματα για την απόδοση της μεθοδολογίας που προτείνεται.

Οι (Sinclair & Smith 2008) συζητούν την πρόληψη των επιθέσεων από εσωτερικούς χρησιμοποιώντας τον έλεγχο πρόσβασης. Συγκεκριμένα συζητούν τις δυσκολίες που υπάρχουν στην υλοποίηση μίας τεχνολογίας για τον έλεγχο πρόσβασης, η οποία και θα επιτρέπει στα μέλη ενός οργανισμού να ολοκληρώνουν τις εργασίες επιτυχημένα και αποτελεσματικά, αλλά και θα μπορεί να προβλέψει τις εσωτερικές απειλές που διαταράσσουν τις δραστηριότητες των μελών. Από την έρευνά τους σε οργανισμούς οικονομικών, υγείας και άλλων τομέων προκύπτει ποικιλία απόψεων για το αν οι τεχνικές όπως η πιστοποίηση και ο έλεγχος πρόσβασης βοηθούν ή εμποδίζουν τους χρήστες να ολοκληρώσουν τις εργασίες τους. Οι ερευνητές καταλήγουν στο συμπέρασμα ότι η πρόληψη συμπληρώνει και δεν αντικαθιστά τις προσπάθειες εντοπισμού των εσωτερικών απειλών, επειδή η καλύτερη πρόληψη μπορεί να περιορίσει το εύρος του προβλήματος το οποίο πρέπει να ανιχνευτεί.

Πολλές μελέτες για τον εντοπισμό των εσωτερικών απειλών προσπαθούν να δημιουργήσουν ένα μοντέλο με κανονική συμπεριφορά και μετά να εντοπίσουν της ανωμαλίες. Σε αυτή την κατηγορία ανήκουν οι τεχνικές εύρεσης των ανωμαλιών για εξωτερικές απειλές. Οι (Shavlik & Shavlik 2004) προτείνουν έναν αλγόριθμο μηχανικής

μάθησης τον οποίο χρησιμοποιεί ο (Littlestone 1988) για τη δημιουργία ενός συστήματος ανίχνευσης ανωμαλιών. Το σύστημα αυτό δημιουργεί στατιστικά προφίλ της κανονικής χρήσης για ένα υπολογιστή, ο οποίος έχει λειτουργικό σύστημα Windows. Αποκλίσεις από το κανονικό μοτίβο μπορεί να είναι δείκτες για εξωτερική απειλητική συμπεριφορά. Παραδείγματα χαρακτηριστικών είναι η δραστηριότητα του δικτύου, η πρόσβαση αρχείων και πολλά άλλα. Τα ποσοστά ανίχνευσης για σύνολο δεδομένων από 16 άτομα ήταν κοντά στο 95%.

Για να πραγματοποιηθεί μία επίθεση πρέπει να υπάρχουν τρεις παράγοντες: κίνητρο, ικανότητα και ευκαιρία (Kandias et al. 2010). Η «ευκαιρία» είναι αναμφισβήτητα ο πιο ευρέως χρησιμοποιημένος τύπος χαρακτηριστικού για την ανίχνευση των εσωτερικών απειλών (Gheyas & Abdallah 2016). Αναλόγως τις ευκαιρίες που έχει διαθέσιμες ένας εσωτερικός σε έναν οργανισμό μπορεί να επιχειρήσει μία επίθεση κατά του συστήματος. Για να καθορίσουν το επίπεδο αυτής της διαθέσιμης ευκαιρίας, οι περισσότερες μελέτες επικεντρώνονται σε δύο ευρείες κατηγορίες χαρακτηριστικών: ο ρόλος του εσωτερικού στο σύστημα και τα χαρακτηριστικά βάση δραστηριοτήτων.

Στο επιστημονικό άρθρο (Legg et al. 2013) προτείνεται ένα εννοιολογικό μοντέλο, το οποίο κάνει χρήση τεχνικών επίβλεψης και ψυχολογικών τεστ. Με βάση το επίπεδο πρόσβασης του χρήστη και τη χρήση ψυχολογικών τεστ πραγματοποιείται μία ταξινόμηση των χρηστών. Με την χρήση ψυχολογικών τεστ επιχειρείται να ανιχνευτεί αν ο χρήστης έχει υψηλά επίπεδα στρες, αν έχει την προδιάθεση για παράνομη ενέργεια καθώς και το γνωστικό του επίπεδο. Ο συνδυασμός των δεδομένων πραγματικού χρόνου που συλλέγονται με τα δεδομένα που προαναφέραμε δίνονται σαν είσοδο στο σύστημα διαχείρισης αποφάσεων για την εξαγωγή του επιπέδου επικινδυνότητας του κάθε χρήστη. Οι ερευνητές υποστηρίζουν ότι ο αλγόριθμος, ο οποίος θα χρησιμοποιηθεί στο σύστημα διαχείρισης αποφάσεων, πρέπει να είναι διαφορετικός για κάθε οργανισμό επειδή εξαρτάται από τα δεδομένα τα οποία θα χρησιμοποιήσει ο οργανισμός.

Οι (Alahmadi et al. 2014) προτείνουν την ανίχνευση εσωτερικών απειλών μέσω επίβλεψης της πλοήγησης του χρήστη στο διαδίκτυο. Το σύστημα που προτείνεται, συλλέγει το περιεχόμενο της κάθε ιστοσελίδας. Από το περιεχόμενο αφαιρούνται τα στοιχεία του πρωτοκόλλου HTML καθώς και λέξεις οι οποίες δεν έχουν νόημα, όπως τα

άρθρα και οι σύνδεσμοι, έτσι ώστε να μπορέσουν να εξαχθούν τα χαρακτηριστικά του κειμένου. Στην συνέχεια δημιουργείται το σύνολο δεδομένων και υπολογίζονται οι διαστάσεις του συνόλου, έτσι ώστε να μπορεί να εφαρμοστεί ο αλγόριθμος k-μέσων για την εξαγωγή των χαρακτηριστικών της προσωπικότητας του χρήστη. Ο συνδυασμός των χαρακτηριστικών της προσωπικότητας του χρήστη θα δώσει ως αποτέλεσμα, αν ο χρήστης είναι πιθανόν να αποτελέσει εσωτερική απειλή ή όχι.

Οι (Brdiczka et al. 2012) χρησιμοποιούν τη μάθηση γράφων και ψυχολογικού πλαισίου για την προσπάθεια ανίχνευσης των εσωτερικών απειλών. Αρχικά συλλέγουν δεδομένα από μέσα κοινωνικής δικτύωσης, ηλεκτρονικά μηνύματα, δικτυακή πλοήγηση κ.α. Από την επεξεργασία αυτών τον δεδομένων εξάγονται χαρακτηριστικά για την δημιουργία ψυχολογικού προφίλ. Οι ερευνητές υποστηρίζουν ότι η δημιουργία ψυχολογικού προφίλ βοηθάει στη συρρίκνωση του όγκου δεδομένων αλλά και στη μείωση των λανθασμένων ειδοποιήσεων. Για την εξαγωγή των τελικών αποτελεσμάτων χρησιμοποιείται ένα Μπεϋζιανό μοντέλο σύντηξης.

Στο άρθρο (Parveen et al. 2011) το πρόβλημα της ανίχνευσης των εσωτερικών απειλών μετατρέπεται σε ένα πρόβλημα εξόρυξης δεδομένων με συνεχή ροή (stream mining). Ως μεθοδολογία προτείνεται ο αλγόριθμος μη επιτηρούμενης μάθησης γράφων GRAD (Graph Based Anomaly Detection). Επίσης, διατυπώνονται οι δυσκολίες οι οποίες προκύπτουν από την χρήση αλγορίθμων επιτηρούμενης μάθησης για τον εντοπισμό των εσωτερικών απειλών, καθώς τα περισσότερα σύνολα δεδομένων για εσωτερικές απειλές έχουν μικρό ποσοστό απειλών και δημιουργείται μια ανισορροπία στα δεδομένα με αποτέλεσμα να μην αποδίδουν τόσο καλά. Πιο συγκεκριμένα, η κατηγοριοποίηση των δεδομένων στηρίζεται σε ένα σύνολο κατηγοριοποιητών αποτελούμενων από πολλαπλά μοντέλα GRAD. Ο προτεινόμενος αλγόριθμος εξετάστηκε στο σύνολο δεδομένων του εργαστηρίου του Λίνκολν, το οποίο είναι βασισμένο σε συστήματα UNIX. Η απόδοσή του μετρήθηκε σε όρους ολικά θετικά λάθη (FP) και αρνητικά λάθη (FN) και έδειξε ότι αυξάνοντας το σύνολο το κατηγοριοποιητών μειώνεται ο αριθμός των FP. Το πρόβλημα όμως είναι ότι ενώ αναγνωρίστηκαν όλες οι εσωτερικές απειλές ο αριθμός των θετικών λαθών παραμένει μεγάλος.

Ένα μεγάλο πρόβλημα για την επίλυση του προβλήματος ανίχνευσης των εσωτερικών απειλών είναι η έλλειψη δεδομένων για να αναλυθούν. Οι ερευνητές έχουν δύο πιθανές

επιλογές, είτε να χρησιμοποιήσουν πραγματικά δεδομένα, είτε συνθετικά δεδομένα. Ανησυχίες για την εμπιστευτικότητα και την ιδιωτικότητα δημιουργούν εμπόδια για την συλλογή και χρήση πραγματικών δεδομένων. Για αυτό το λόγω μερικές φορές είναι προτιμότερο να χρησιμοποιηθούν συνθετικά δεδομένα (Lindauer et al. 2013). Η δική μας έρευνα βασίζεται στην γεννήτρια συνθετικών δεδομένων που αναφέρεται στο επιστημονικό άρθρο (Glasser & Lindauer 2013). Πραγματοποιείται η παραγωγή δεδομένων για διάστημα άνω των 500 ημερών, τα οποία προσομοιώνουν την συλλογή αρχείων καταγραφής από αισθητήρες τοποθετημένους σε όλους τους σταθμούς εργασίας σε μία μεγάλη επιχείρηση ή κυβερνητικό οργανισμό. Διαπιστώνεται ότι η παραγωγή συνθετικών δεδομένων με ένα υψηλό επίπεδο του ανθρώπινου ρεαλισμού είναι πολύ πιο δύσκολο από ότι η παραγωγή συνθετικών δεδομένων απλά για τον έλεγχο της απόδοσης συστημάτων κατηγοριοποίησης.

Το πανεπιστήμιο Carnegie Mellon παρέχει σύνολα δεδομένων με διάφορα σενάρια εσωτερικών απειλών και βασίζεται στον παραπάνω τρόπο δημιουργίας δεδομένων. Από την έρευνά μας υπάρχουν λίγες εργασίες που χρησιμοποιούν αυτά τα σύνολα δεδομένων για να αξιολογήσουν την απόδοση ενός συστήματος εντοπισμού εσωτερικών απειλών. Μία προσέγγιση είναι η χρήση της έννοιας των δέντρων δραστηριότητας για τον καθορισμό όλων των συμπεριφορών ενός χρήστη ή στην περίπτωση των πολλαπλών χρηστών ο ρόλος τους στην επιχείρηση (Agrafiotis et al. 2014). Η έννοια αυτή επεκτείνεται στην γενικότερη ιδέα των δέντρων επίθεσης, τα οποία ενσωματώνουν όχι μόνο την ακολουθία των γεγονότων που θα έχουν ως αποτέλεσμα μία επίθεση, αλλά και την ακολουθία των γεγονότων που θα αποφέρουν σε έναν μη κακόβουλο σκοπό.

Μία άλλη προσέγγιση για την ανίχνευση των εσωτερικών απειλών γίνεται με τον συνδυασμό δύο τεχνικών σε πιθανολογικά μοντέλα κινδύνου βασιζόμενα σε Μπεϋζιανά δίκτυα (Schrag et al. 2014). Η πρώτη τεχνική είναι το μοντέλο Mc, το οποίο απευθύνεται στο ρίσκο που ένα άτομο P μπορεί να αποκαλύψει ιδιωτικές πληροφορίες μίας ομάδας χωρίς την κατάλληλη εξουσιοδότηση λαμβάνοντας υπόψιν τους σχετικούς τύπους συμβάντων, όπως η τεχνική της πιστοποίησης. Η δεύτερη τεχνική είναι το μοντέλο Ms, το οποίο απευθύνεται στον κίνδυνο που ένα άτομο μπορεί να αποτελέσει εσωτερική απειλή για μία ομάδα μέσω της πρόσβασής του πληροφοριακού συστήματος της ομάδας, όπως υπολογιστές, δίκτυα και σχετικών περιουσιακών στοιχείων.

Επιπλέον, έχει δημιουργηθεί ένα μοντέλο που βασίζεται στις ρυθμίσεις και τις εκτιμήσεις του συστήματος ανίχνευσης εσωτερικών απειλών μίας εταιρίας και προβλέπει την απόδοση του συστήματος (Roberts et al. 2016). Για να εφαρμοστεί ένα σενάριο εσωτερικής απειλής, στο μοντέλο χρησιμοποιούνται Μπεϋζιανά δίκτυα και γίνεται η αξιολόγηση της απόδοσής του σύμφωνα με τα μέτρα που λαμβάνονται από τους πίνακες σύγχυσης, όπως η ακρίβεια και η ανάκληση. Είναι κατασκευασμένο ώστε να παράγει ειδοποιήσεις για κάθε χρήστη ανά μήνα.

Το σύστημα ανίχνευση ανωμαλιών Corporate Insider Threat Detection (CITD) συνδυάζει τεχνικές δραστηριότητες και ενέργειες συμπεριφοράς για την αξιολόγηση της απειλής από τα άτομα (Legg et al. 2015). Από τα αρχεία καταγραφής δεδομένων ενός οργανισμού συγκεντρώνονται πληροφορίες για τις δραστηριότητες των χρηστών. Το σύστημα τροφοδοτείται με αυτές τις πληροφορίες και δημιουργεί ένα προφίλ σε δομή δέντρου για κάθε χρήστη και ρόλο.

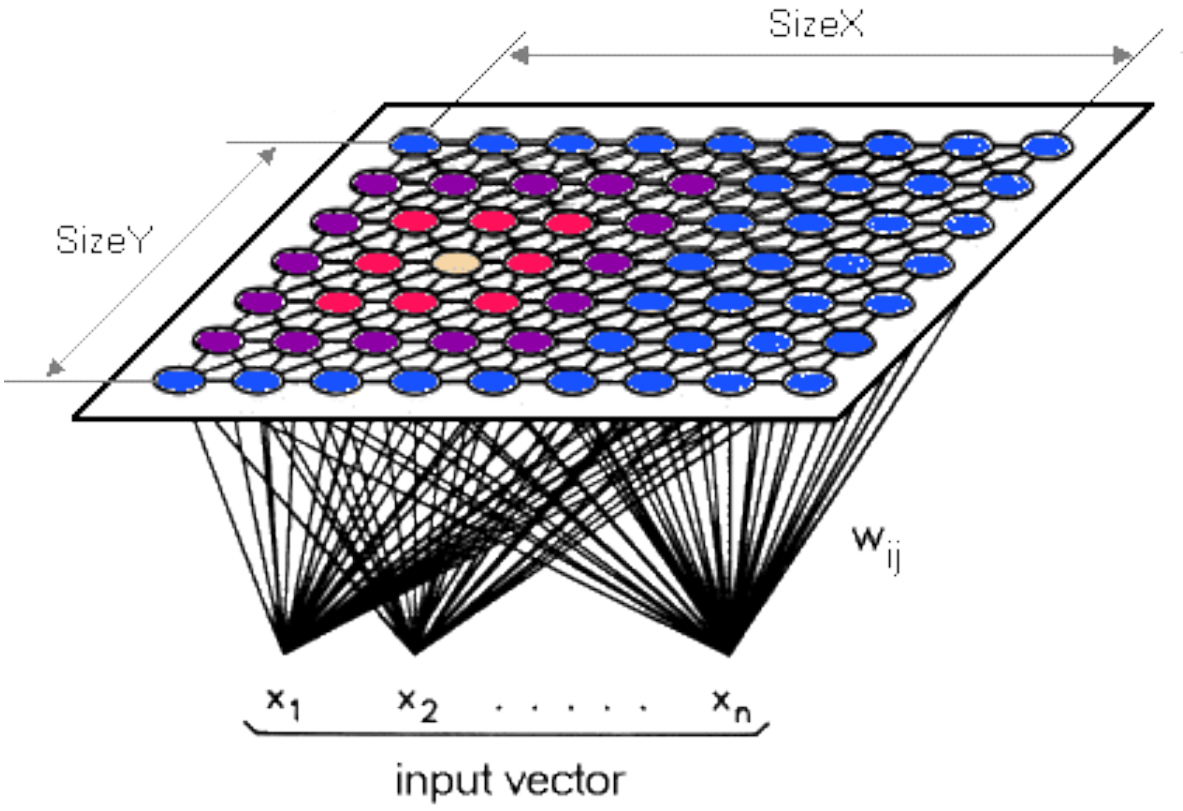
Κεφάλαιο 3
Μεθοδολογίες

Σε αυτό το κεφάλαιο αναλύονται οι μεθοδολογίες που χρησιμοποιήθηκαν για τον εντοπισμό των εσωτερικών απειλών. Παρουσιάζονται οι αλγόριθμοι μη επιτηρούμενης μάθησης χάρτες αυτό-οργάνωσης (Self-Organizing Maps ή SOMs) και αυτό-οργανωμένα αυξητικά νευρωνικά δίκτυα (Self-Organizing Incremental Neural Networks – SOINN). Στην δεύτερη μεθοδολογία επιλέγεται μία παραλλαγή της, ο enhanced-SOINN. Και οι δύο αλγόριθμοι ανήκουν στην κατηγορία των νευρωνικών δικτύων. Ένα τεχνητό νευρωνικό δίκτυο ορίζεται συνήθως ως ένα δίκτυο, το οποίο αποτελείται από ένα μεγάλο αριθμό απλών επεξεργαστών (νευρώνες), οι οποίοι είναι μαζικά διασυνδεμένοι, λειτουργούν παράλληλα και μαθαίνουν από την εμπειρία (παραδείγματα) (Specht 1991).

3.1 Αλγόριθμος SOM

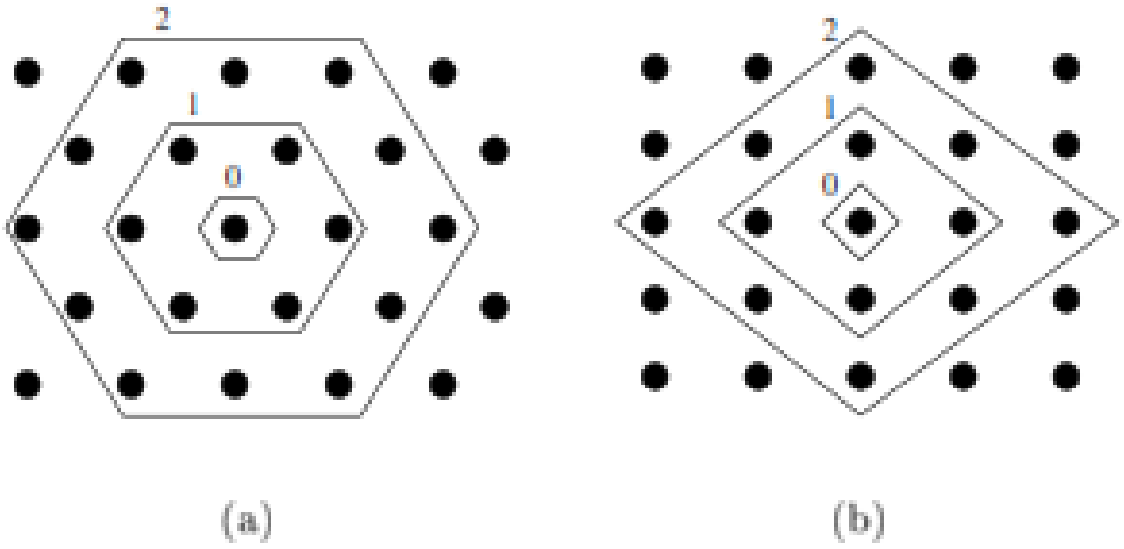
Οι χάρτες αυτό-οργάνωσης (Self-Organizing Maps ή SOMs) είναι μία ειδική κατηγορία νευρωνικού δικτύου. Επίσης είναι γνωστοί και ως χάρτες του Kohonen (Kohonen maps) επειδή αναπτύχθηκαν από τον καθηγητή Teuvo Kohonen το 1982 (Kohonen 1982). Όπως φανερώνει και το όνομα του αλγορίθμου SOM, μαθαίνει μόνος του, δηλαδή χωρίς την ανθρώπινη παρέμβαση και έτσι ανήκει στην κατηγορία των αλγορίθμων μάθησης χωρίς επίβλεψη. Ο βασικός στόχος του SOM είναι να μετατρέψει ένα εισερχόμενο μοτίβο της αυθαίρετης διάστασης σε ένα μη γραμμικό διακριτό χάρτη μικρότερης διάστασης, συνήθως μονοδιάστατο ή δυσδιάστατο, και να εκτελέσει αυτή την μετατροπή προσαρμοστικά με έναν διατεταγμένο τρόπο (Kubat 1999). Για αυτό το λόγο μπορεί να θεωρηθεί ως ένας τοπογραφικός διανυσματικός καταμεριστής (topographic vector quantizer), μία μη γραμμική μέθοδος αναπαράστασης ή ως μία

μέθοδος ομαδοποίησης. Ειδικότερα είναι ένας αλγόριθμος ομαδοποίησης που διατάσσει τις συστάδες.



Εικόνα 1. Νευρωνικό δίκτυο Kohonen

Το νευρωνικό δίκτυο των χαρτών του Kohonen αποτελείται από δύο επίπεδα, το επίπεδο εισόδου και το επίπεδο εξόδου (***Εικόνα 1***). Στο επίπεδο εξόδου, οι νευρώνες τοποθετούνται σε ένα πλέγμα (lattice), συνήθως δύο διαστάσεων. Πλέγματα μίας διάστασης ή περισσότερων από δυο διαστάσεων είναι πιθανά αλλά σπάνια. Το δισδιάστατο πλέγμα μπορεί να έχει ορθογώνια, εξαγωνική ή ακόμα και μη κανονική μορφή (***Εικόνα 2***). Η εξαγωνική μορφή είναι πιο αποτελεσματική όσον αφορά την οπτική παρουσίαση των δεδομένων. Οι νευρώνες ρυθμίζονται επιλεκτικά σε διάφορα μοτίβα δεδομένων εισόδου από το επίπεδο εισόδου. Ο SOM για να εκπαιδεύσει τους νευρώνες βασίζεται στην μέθοδο της ανταγωνιστικής μάθησης (competitive learning). Ενώ στην απλή ανταγωνιστική μάθηση προσαρμόζεται μόνο ο νευρώνας που ταιριάζει καλύτερα στα δεδομένα εισόδου, στον SOM προσαρμόζονται όλοι οι νευρώνες που ανήκουν στην τοπική γειτονιά του νευρώνα. Η γειτονιά καθορίζεται από την συνάρτηση γειτονιάς (Zhang 2010).



Εικόνα 2. Εξαγωνική (a) και ορθογώνια (b) τοπολογία

Οι νευρώνες ανταγωνίζονται μεταξύ τους για το ποιος θα ενεργοποιηθεί, χρησιμοποιώντας μία συνάρτηση ενεργοποίησης, η οποία συνήθως είναι η ευκλείδεια απόσταση μεταξύ του διανύσματος βαρών του νευρώνα και του διανύσματος εισόδου. Ο νευρώνας που κερδίζει τον ανταγωνισμό λέγεται νευρώνας νικητής. Σε κάθε διαδοχικό βήμα ο νευρώνας με την μικρότερη τιμή της συνάρτησης ενεργοποίησης επιλέγεται και αλλάζει το διάνυσμα βάρους του μαζί με τα διανύσματα βάρους των γειτονικών νευρώνων του, ώστε να προσεγγίζει όσο το δυνατόν καλύτερα τα δεδομένα. Όταν τελειώσει η εκπαίδευση του SOM, ο νικητήριος νευρώνας που θα συγκριθεί με ένα διάνυσμα δεδομένων λέγεται καλύτερη ομότιμη μονάδα (best-matching unit – BMU).

Αξίζει να σημειωθεί ότι οι νευρώνες τοποθετούνται στο δίκτυο με τέτοιο τρόπο ώστε να δημιουργείται ένα ουσιαστικό σύστημα συντεταγμένων για τα διάφορα χαρακτηριστικά των δεδομένων εισόδου (Kohonen 1990). Επομένως αν υποθέσουμε ότι ένα διάνυσμα εισόδου ενεργοποιεί κάποιων νευρώνα τότε παρόμοια διανύσματα εισόδου θα ενεργοποιούν τον ίδιο ή και γειτονικούς νευρώνες. Εν ολίγοις σε πρακτικό επίπεδο γειτονικοί νευρώνες στο πλέγμα έχουν παρόμοια βάρη (Vesanto et al. 1999). Κατά συνέπεια, ένας αυτό-οργανωμένος χάρτης χαρακτηρίζεται από το σχηματισμό ενός τοπογραφικού χάρτη των προτύπων εισόδου στον οποίο οι χωρικές θέσεις (όπως οι συντεταγμένες) των νευρώνων στο πλέγμα είναι ενδεικτικές των εγγενών στατιστικών χαρακτηριστικών τα οποία περιέχονται στα πρότυπα εισόδου.

Το πρώτο βήμα του αλγορίθμου για τον σχηματισμό του αυτό-οργανωμένου χάρτη είναι η αρχικοποίηση των διανυσμάτων βάρους στο πλέγμα. Η αρχικοποίηση μπορεί να γίνει δίνοντας μικρές τυχαίες τιμές από μία γεννήτρια τυχαίων αριθμών για να αποφύγουμε την εκ των προτέρων διάταξη των νευρώνων του χάρτη. Ένας εναλλακτικός τρόπος είναι να χρησιμοποιήσουμε την γεννήτρια τυχαίων αριθμών για την τυχαία επιλογή διανυσμάτων από το σύνολο των δεδομένων εισόδου. Όταν οι νευρώνες του χάρτη αρχικοποιηθούν, εκτελείται κατά επαναληπτικό τρόπο η εκπαίδευση του δικτύου. Οι διαδικασίες που είναι υπεύθυνες για την αυτό-οργάνωση του δικτύου είναι ο ανταγωνισμός, η συνεργασία και η προσαρμογή.

Στην διαδικασία του ανταγωνισμού σε κάθε επανάληψη του αλγορίθμου επιλέγεται τυχαία ένα διάνυσμα εισόδου από τον χώρο δεδομένων εισόδου. Έστω ότι ο χώρος των δεδομένων εισόδου έχει διάσταση m και ότι συμβολίζουμε το διάνυσμα εισόδου με

$$x = [x_1, x_2, \dots, x_m]^T$$

Έστω l το πλήθος των νευρώνων στο χάρτη. Για κάθε νευρώνα το διάνυσμα βάρους του έχει τον ίδιο αριθμό διάστασης με του χώρου εισόδου. Θεωρούμε ως διάνυσμα βάρους ενός νευρώνα j

$$w_j = [w_{j1}, w_{j2}, \dots, w_{jm}]^T \text{ , όπου j=1, 2,..., l}$$

Ο νευρώνας i με διάνυσμα βάρους w_j θεωρείται νικητής εφόσον το διάνυσμα βάρους του έχει ελάχιστη απόσταση από το διάνυσμα εισόδου x, δηλαδή

$$i = \arg\min_j \|x - w_j\| \text{ , } \quad \text{j = 1, 2,..., l}$$

Ως μέτρο απόστασης συνήθως χρησιμοποιείται η ευκλείδεια απόσταση. Ο νευρώνας νικητής ονομάζεται και καλύτερη ομότιμη μονάδα (best-matching unit – BMU).

Το επόμενο στάδιο είναι η διαδικασία της συνεργασίας. Στην διαδικασία της συνεργασίας ο νευρώνας νικητής γίνεται το κέντρο μίας τοπολογικής γειτονιάς από νευρώνες που συνεργάζονται. Από την νευρολογία γνωρίζουμε ότι ο νευρώνας που ενεργοποιείται έχει την τάση να διεγείρει περισσότερο τους άμεσα γειτονικούς του νευρώνες και λιγότερο αυτούς που βρίσκονται πιο μακριά. Για να επιτευχθεί αυτή η παρατήρηση πρέπει η συνάρτηση τοπολογικής γειτονιάς να είναι μία φθίνουσα συνάρτηση της πλευρικής απόστασης μεταξύ των νευρώνων. Επομένως η τοπολογική συνάρτηση γειτονιάς πρέπει να ικανοποιεί δύο προϋποθέσεις:

- Να αποκτά την μέγιστη τιμή της στον νευρώνα νικητή όταν η πλευρική απόσταση είναι μηδέν.

- Το πλάτος της να μειώνεται μονότονα όταν αυξάνεται η πλευρική απόσταση και να αποσβένει στο μηδέν όταν η πλευρική απόσταση τείνει στο άπειρο. Αυτή είναι και η απαραίτητη συνθήκη για να συγκλίνει ο αλγόριθμος.

Ένα παράδειγμα συνάρτησης γειτονιάς που ικανοποιεί τις παραπάνω προϋποθέσεις είναι Γκαουσσιανή συνάρτηση:

$$h_{ij}(x) = e^{\left(-\frac{\|r_i - r_j\|^2}{2\sigma^2}\right)}$$

Τα r_i και r_j συμβολίζουν τις θέσεις των νευρώνων i και j στο δισδιάστατο πλέγμα. Το σ είναι το «αποτελεσματικό πλάτος» (effective width) της τοπολογικής γειτονιάς, το οποίο μετρά τον βαθμό που οι διεγερμένοι νευρώνες στην γειτονιά του νευρώνα νικητή συμμετέχουν στην διαδικασία της μάθησης.

Ένα επιπλέον στοιχείο του αλγορίθμου είναι ότι το μέγεθος της συνάρτησης γειτονιάς του αλγορίθμου SOM μειώνεται σε σχέση με τον χρόνο. Έτσι για την παράμετρο σ πρέπει να επιλεγεί μία συνάρτηση που να φθίνει με τον χρόνο. Μία συνήθης επιλογή είναι η εκθετική μείωση που δίνεται από τον τύπο:

$$\sigma(n) = \sigma_0 e^{\left(-\frac{n}{\tau_1}\right)}$$

όπου σ_0 είναι η τιμή του αρχικού πλάτους της γειτονιάς, τ_1 είναι μία σταθερά χρόνου για όλη την διάρκεια εκπαίδευση του αλγορίθμου και n ο αριθμός της εκάστοτε επανάληψης. Με την προσθήκη του αριθμού της εκάστοτε επανάληψης n ως μία μορφή χρόνου ορίζεται η παρακάτω συνάρτηση γειτονιάς του αλγορίθμου SOM:

$$h_{ij}(n) = e^{\left(\frac{\|r_i - r_j\|^2}{2\sigma^2(n)}\right)}, \qquad n = 0,1,2, \ldots.$$

Η διαδικασία της προσαρμογής είναι ο μηχανισμός που επιτρέπει στους διεγερμένους νευρώνες να προσαρμόσουν τις τιμές των βαρών τους ώστε να ταιριάζουν καλύτερα στο διάνυσμα εισόδου. Ένας νευρώνας j σε χρόνο n, ο οποίος έχει διάνυσμα βάρους $w_j(n)$ αλλάζει τις τιμές του διανύσματος βάρους του $w_j(n+1)$ σε χρόνο n+1 με την σχέση:

$$w_j(n+1) = w_j(n) + \eta(n) h_{ij}(n)(x(n) - w_j(n))$$

η οποία εφαρμόζεται σε όλους τους νευρώνες που ανήκουν στην τοπολογική γειτονιά του νευρώνα νικητή i. Η παράμετρος η(n) είναι ο ρυθμός εκπαίδευσης του αλγορίθμου.

Αρχικά έχει μία μεγάλη τιμή αλλά κατά την διάρκεια της εκπαίδευσης μειώνεται. Οι τιμές του ρυθμού εκπαίδευσης κυμαίνονται από 0 έως 1. Η εφαρμογή της παραπάνω σχέσης έχει ως αποτέλεσμα την μετακίνηση του διανύσματος βάρους w_i του νευρώνα νικητή i προς το διάνυσμα εισόδου x. Μετά από πολλές επαναλήψεις της διαδικασίας εκπαίδευσης τα διανύσματα βαρών των νευρώνων τείνουν να ακολουθήσουν την κατανομή των δεδομένων εισόδου, εξαιτίας της ανανέωσης της γειτονιάς. Συνεπώς γειτονικοί νευρώνες τείνουν να έχουν παρόμοια διανύσματα βαρών δημιουργώντας μία τοπολογική διάταξη στο πλέγμα.

Συνοψίζοντας ο αλγόριθμος SOM έχει τα εξής βήματα:

- Αρχικοποίηση όλων των διανυσμάτων βάρους των νευρώνων του πλέγματος με τυχαίες τιμές.
- Τυχαία επιλογή ενός διανύσματος εισόδου x από τον χώρο εισόδου. Το x πρέπει να έχει την ίδια διάσταση με τα διανύσματα βάρους των νευρώνων.
- Εύρεση της καλύτερης ομότιμης μονάδας (BMU) i για το διάνυσμα εισόδου x σε χρονικό βήμα n βρίσκοντας την μικρότερη ευκλείδεια απόσταση μεταξύ των νευρώνων και του διανύσματος x.

$$i = \arg\min_j \left\| x(n) - w_j \right\|, \quad j = 1, 2, \ldots, l$$

- Προσαρμογή των διανυσμάτων βάρους όλων των νευρώνων που ανήκουν στην τοπολογική γειτονιά του νευρώνα νικητή i χρησιμοποιώντας την σχέση:

$$w_j(n+1) = w_j(n) + \eta(n) h_{ij}(n)(x(n) - w_j(n))$$

  Όπου η(n) είναι ο ρυθμός μάθησης και hij(n) είναι η συνάρτηση γειτονιάς του νευρώνα νικητή i.
- Επανάληψη των προηγούμενων βημάτων πλην του πρώτου μέχρι να μην παρατηρούνται αξιοσημείωτες αλλαγές στον χάρτη.

3.2 Αλγόριθμος SOINN

Ο αλγόριθμος SOINN (Furao & Hasegawa 2006) παρουσιάστηκε από τους Furao και Hasegawa το 2006. Βασίζεται στην γενική ιδέα των χαρτών αυτό-οργάνωσης και της αυξητικής μάθησης. Ο SOINN είναι ένας χάρτης αυτό-οργάνωσης ο οποίος δεν απαιτεί να γίνει κάποια υπόθεση για την τοπολογία ή την κατανομή των δεδομένων (Najjar & Hasegawa 2013). Για την εκπαίδευση του δικτύου των νευρώνων χρησιμοποιεί την τεχνική της αυξητικής μάθησης. Η αυξητική μάθηση απευθύνεται στην ικανότητα ενός

δικτύου το οποίο εκπαιδεύεται επαναλαμβανόμενα με την χρήση νέων δεδομένων να μην καταστρέφει τα παλιότερα μοτίβα προτύπων (Shen & Hasegawa 2010). Το θεμελιώδες ζήτημα για την αυξητική μάθηση είναι πως ένα σύστημα μάθησης μπορεί να προσαρμοστεί στις νέες πληροφορίες χωρίς να καταστραφούν ή να ξεχαστούν οι προηγούμενες πληροφορίες που έχει μάθει το σύστημα (Grossberg 1988).

Ο SOINN χωρίζει τα δεδομένα εισόδου σε συστάδες αυξάνοντας τους νευρώνες στο δίκτυο όταν αυτό είναι απαραίτητο. Οι νευρώνες ή αλλιώς κόμβοι, είναι συνδεμένοι με ακμές μεταξύ τους με σκοπό την διατήρηση της τοπολογίας του δικτύου. Επίσης κάθε κόμβος αποτελείται από ένα διάνυσμα βάρους το οποίο συμβολίζει ένα διάνυσμα αναφοράς. Εν κατακλείδι, τα πλεονεκτήματα του SOINN είναι ότι έχει μεγάλη αντοχή στο θόρυβο, είναι κατάλληλος για εργασίες που απαιτούν απευθείας εκπαίδευση καθώς και για τον χωρισμό των δεδομένων εισόδου σε συστάδες χωρίς να προκαθορίζεται ο αριθμός των συστάδων.

Αναλυτικότερο ο SOINN αποτελείται από ένα νευρωνικό δίκτυο δύο στρωμάτων. Το πρώτο στρώμα μαθαίνει την κατανομή πυκνότητας των δεδομένων εισόδου και αναπαριστά την κατανομή με κόμβους και ακμές. Έτσι δημιουργείται μια τοπολογική δομή των μοτίβων εισόδου. Στο δεύτερο στρώμα εντοπίζονται οι περιοχές χαμηλής πυκνότητας των δεδομένων εισόδου ώστε να γίνει ο διαχωρισμός των συστάδων. Και σε αυτό το στρώμα δημιουργείται μία τοπολογική δομή των μοτίβων εισόδου αλλά χρησιμοποιούνται λιγότεροι κόμβοι από ότι στο πρώτο στρώμα. Επιπλέον και στα δύο στρώματα εφαρμόζεται ο ίδιος αλγόριθμος μάθησης. Μετά το πέρας της εκπαίδευσης του δεύτερου στρώματος παρουσιάζεται ένα πρότυπο κόμβου για την κάθε συστάδα καθώς και το πλήθος των συστάδων. Στην συνέχεια αναλύουμε την διαδικασία μάθησης του αλγορίθμου SOINN (***Εικόνα 3***).

Το πρώτο βήμα του αλγορίθμου είναι η αρχικοποίηση ενός συνόλου κόμβων με την τυχαία επιλογή από τα δεδομένα εισόδου. Το σύνολο αυτό αποτελείται από δύο κόμβους. Αφού επιτευχθεί η αρχικοποίηση, για κάθε διάνυσμα εισόδου γίνεται η εύρεση του πλησιέστερου κόμβου, που ονομάζεται πρώτος νικητής και η εύρεση του δεύτερου πλησιέστερου κόμβου, δηλαδή του δεύτερου νικητή. Αν κριθεί ότι η κατανομή του διανύσματος εισόδου είναι άγνωστη τότε το πρώτο στρώμα του δικτύου ανανεώνει προσαρμοστικά το κατώτερο όριο ομοιότητας για κάθε κόμβο. Έστω i ο κόμβος που

ανανεώνεται το κατώτερο όριο ομοιότητας T_i. Αν ο κόμβος i έχει ένα σύνολο γειτονικών κόμβων N_i τότε η T_i υπολογίζεται από την μέγιστη απόσταση μεταξύ του κόμβου i και των γειτονικών του κόμβων από την σχέση:

$$T_i = \max_{j \in N_i} \|W_i - W_j\|$$

όπου W_i και W_j είναι τα διανύσματα βαρών του κόμβου i και του εκάστοτε γειτονικού κόμβου j.

Αν ο κόμβος i δεν έχει γειτονικούς κόμβους τότε ως κατώτερο όριο ομοιότητας ορίζεται η μικρότερη απόσταση μεταξύ του κόμβου i και των άλλων κόμβων στο δίκτυο. Αν θεωρήσουμε N το σύνολο όλων των κόμβων του δικτύου τότε ο παραπάνω τύπος γίνεται:

$$T_i = \min_{j \in N - \{i\}} \|W_i - W_j\|$$

Αν η απόσταση του διανύσματος εισόδου μεταξύ του πρώτου ή του δεύτερου νικητή είναι μεγαλύτερη από το κατώτερο όριο ομοιότητας του πρώτου ή του δεύτερου νικητή τότε εισάγεται ένας νέος κόμβος στο δίκτυο. Ο κόμβος αυτός αποτελεί τον πρώτο κόμβο της νέας κλάσης η οποία ονομάζεται ενδιάμεση-κλάση (between-class). Από την άλλη πλευρά αν το διάνυσμα εισόδου κριθεί ότι ανήκει στην ίδια συστάδα με τον πρώτο ή το δεύτερο νικητή και δεν υπάρχουν ακμές που ενώνουν τον πρώτο και τον δεύτερο νικητή, τότε ενώνεται με μία ακμή ο πρώτος με τον δεύτερο νικητή. Η «ηλικία» της ακμής παίρνει τιμή 0 και αυξάνονται κατά 1 οι ηλικίες όλων των ακμών που συνδέονται με τον πρώτο νικητή.

Ακολουθεί η ενημέρωση του διανύσματος βαρών του πρώτου νικητή και των γειτονικών κόμβων. Θεωρούμε ως i τον νικητή και M_i τον αριθμό των φορών που ο κόμβος i είναι νικητής. Η αλλαγή των βαρών του νικητή ΔW_i και των βαρών του γειτονικού κόμβου j που ανήκει στην γειτονιά N_i του νικητή i δίνονται από τις σχέσεις:

$$\Delta W_i = \frac{1}{M_i} \cdot (W_s - W_i)$$

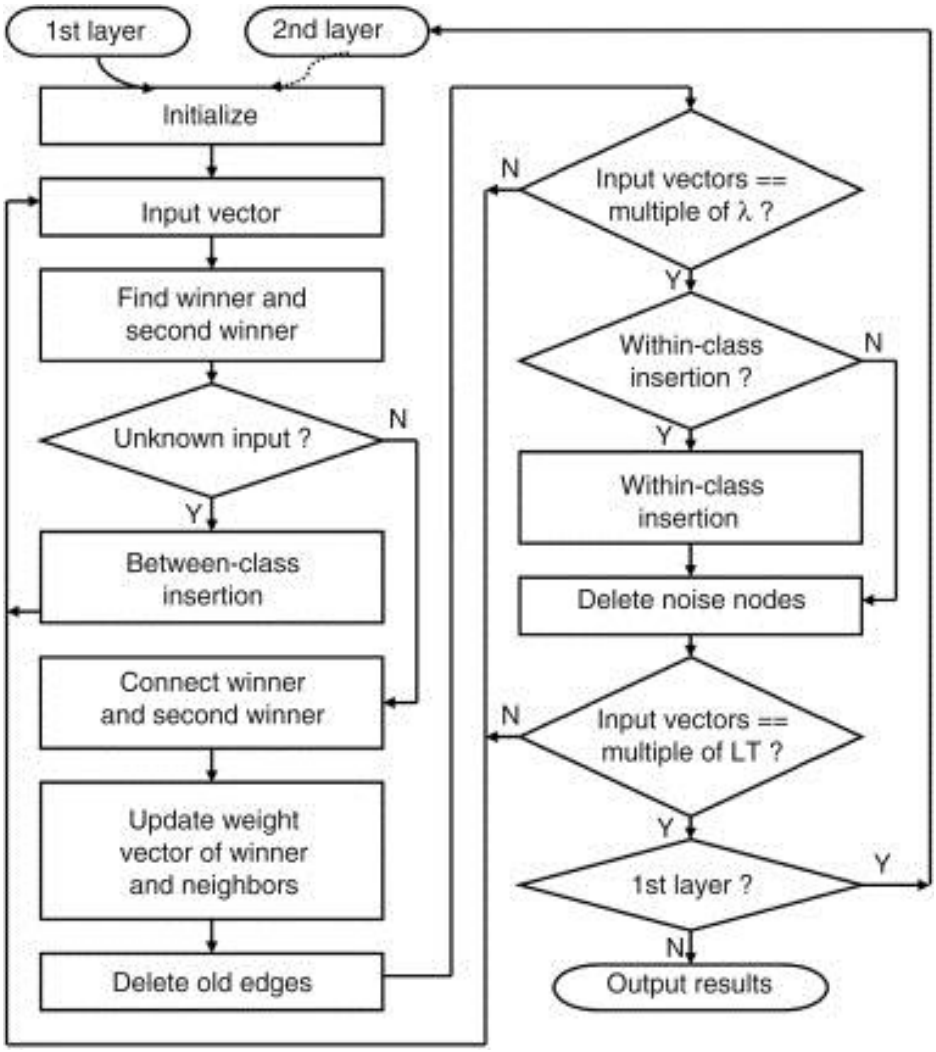
$$\Delta W_j = \frac{1}{100 M_i} \cdot (W_s - W_j),$$

όπου W_s είναι τα βάρη του διανύσματος εισόδου.

Ακολουθεί η διαγραφή όλων τον ακμών που έχουν ηλικία μεγαλύτερη από όριο της μέγιστης ηλικίας ακμής age_{max}. Έστω λ οι επαναλήψεις μάθησης. Αν το πλήθος των διανυσμάτων εισόδου δεν είναι ακέραιο πολλαπλάσιο του λ τότε ο αλγόριθμος επιστρέφει στο βήμα της εισαγωγής νέου διανύσματος εισόδου. Στην αντίθετη περίπτωση, δηλαδή όταν το πλήθος των διανυσμάτων εισόδου που δημιουργήθηκαν μέχρι τώρα είναι ακέραιο πολλαπλάσιο του λ, γίνεται η εισαγωγή νέου κόμβου στην θέση που το σφάλμα συσσώρευσης (accumulative error) είναι πολύ μεγάλο. Η εισαγωγή αυτή ονομάζεται εισαγωγή εντός-κλάσης (within-class) επειδή ο νέος κόμβος δημιουργείται μέσα στην υπάρχουσα κλάση. Αν η εισαγωγή κριθεί ότι δεν μειώνει το σφάλμα τότε ακυρώνεται.

Ο SOINN προχωρά στην διαδικασία διαγραφής των κόμβων οι οποίοι δημιουργήθηκαν από θόρυβο είτε η εισαγωγή του νέου κόμβου στην υπάρχουσα κλάση κριθεί επιτυχής είτε ακυρωθεί. Αν το πλήθος των διανυσμάτων εισόδου που δημιουργήθηκαν είναι ακέραιο πολλαπλάσιο του αριθμού των επαναλήψεων λ, τότε αφαιρούνται οι κόμβοι που έχουν μόνο ένα ή κανένα γείτονα.

Τα αποτελέσματα του πρώτου στρώματος χρησιμοποιούνται ως είσοδοι για το δεύτερο στρώμα. Αυτό γίνεται μετά από ένα χρονικό όριο εκπαίδευσης ή καλύτερα ένα όριο επαναλήψεων μάθησης LT, το οποίο έχει καθοριστεί για το πρώτο στρώμα. Ο ίδιος αλγόριθμος χρησιμοποιείται για την εκπαίδευση και του δεύτερου στρώματος. Στο δεύτερο στρώμα το κατώτερο όριο ομοιότητας είναι σταθερό σε αντίθεση με το κατώτερο όριο του πρώτου στρώματος που ανανεώνεται προσαρμοστικά. Υπολογίζεται χρησιμοποιώντας την απόσταση της εντός-κλάσης και της ενδιάμεσης-κλάσης (Furao & Hasegawa 2006).



Εικόνα 3. Διάγραμμα ροής SOINN

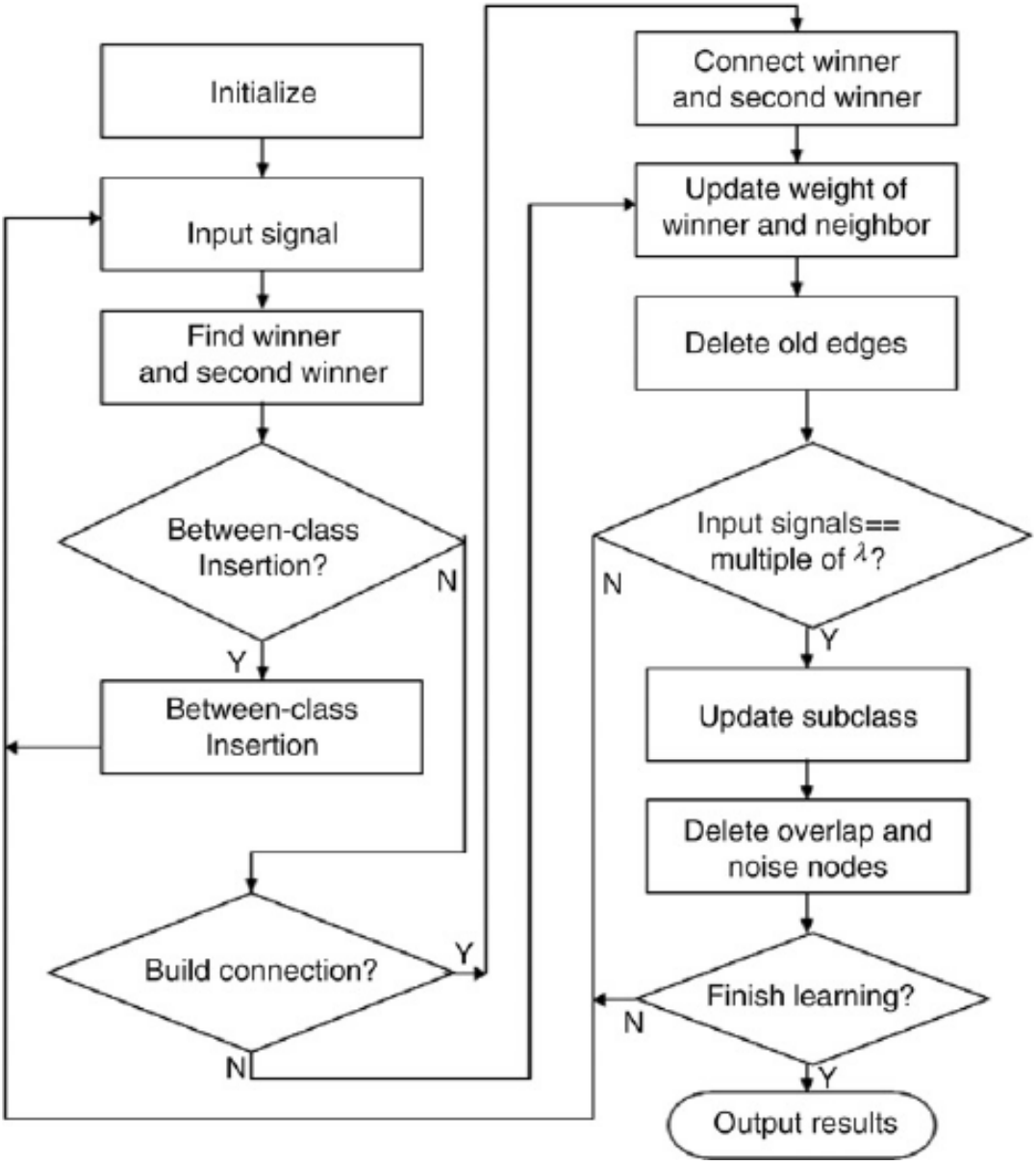
3.3 Αλγόριθμος ESOINN

Ο αλγόριθμος SOINN έχει τα παρακάτω μειονεκτήματα (Emil 2016):

- Το πρώτο και το δεύτερο στρώμα εκπαιδεύονται ξεχωριστά.
- Οι αλλαγές που προκύπτουν στα αποτελέσματα του πρώτου στρώματος κατά την εκπαίδευση, προκαλούν την επανεκπαίδευση του δεύτερου στρώματος. Συνεπώς το δεύτερο στρώμα είναι ακατάλληλο για την απευθείας αυξητική μάθηση.
- Όταν εμφανιστεί η εισαγωγή μίας εντός-κλάσης απαιτείται να καθοριστούν από τον χρήστη πολλές παράμετροι.
- Ο SOINN δεν μπορεί να διαχωρίσει ένα σύνολο με υψηλής συχνότητας επικαλυπτόμενες περιοχές.

Για να ξεπεραστούν τα παραπάνω μειονεκτήματα του SOINN αναπτύχθηκε ο αλγόριθμος ενισχυμένα αυτό-οργανωμένα αυξητικά νευρωνικά δίκτυα ESOINN (Furao et al. 2007). Ο ESOINN αποτελείται από ένα στρώμα και έτσι δεν χρειάζεται να καθοριστεί ο τρόπος με τον οποίο η εκπαίδευση του πρώτου στρώματος αλλάζει στην εκπαίδευση του δεύτερου. Με ένα στρώμα, ο ESOINN είναι σε θέση να ενσωματώσει τόσο την διαδικασία της κατανομής κατά μήκος ολόκληρης της επιφάνειας της κατηγοριοποίησης, όσο και τον διαχωρισμό των ομάδων χαμηλής πυκνότητας (Corchado et al. 2009). Αφαιρώντας το δεύτερο στρώμα και μία συνθήκη για την εισαγωγή ενός νέου κόμβου, ο αριθμός των απαιτούμενων παραμέτρων μειώνεται στις τέσσερεις συνολικά (Gori & Melacci 2010). Επιπλέον κάνει τον αλγόριθμο πιο κατάλληλο για εργασίες οι οποίες απαιτούν απευθείας ή δια βίου μάθηση.

Στην ***Εικόνα 4*** παρουσιάζεται το διάγραμμα ροής του ESOINN. Εκ πρώτης όψεως η μόνη διαφορά που φανερώνουν τα διαγράμματα ροής του ESOINN και SOINN (***Εικόνα 3***) είναι ο αριθμός των στρωμάτων του δικτύου τους. Για την εισαγωγή της ενδιάμεσης-κλάσης υιοθετείται το ίδιο σχέδιο όπως στον SOINN. Όμως για την δημιουργία μίας σύνδεσης μεταξύ των κόμβων προστίθεται μία συνθήκη που κρίνει αν χρειάζεται η σύνδεση αυτή. Μετά από λ αριθμό επαναλήψεων εκπαίδευσης ο ESOINN χωρίζει τους κόμβους σε διαφορετικές υποκλάσεις και διαγράφει τις ακμές που βρίσκονται σε επικαλυπτόμενες περιοχές. Επίσης αφαιρείται η διαδικασία της εισαγωγής εντός-κλάσης καθώς δεν υπάρχει δεύτερο στρώμα.



Εικόνα 4. Διάγραμμα ροής ESOINN

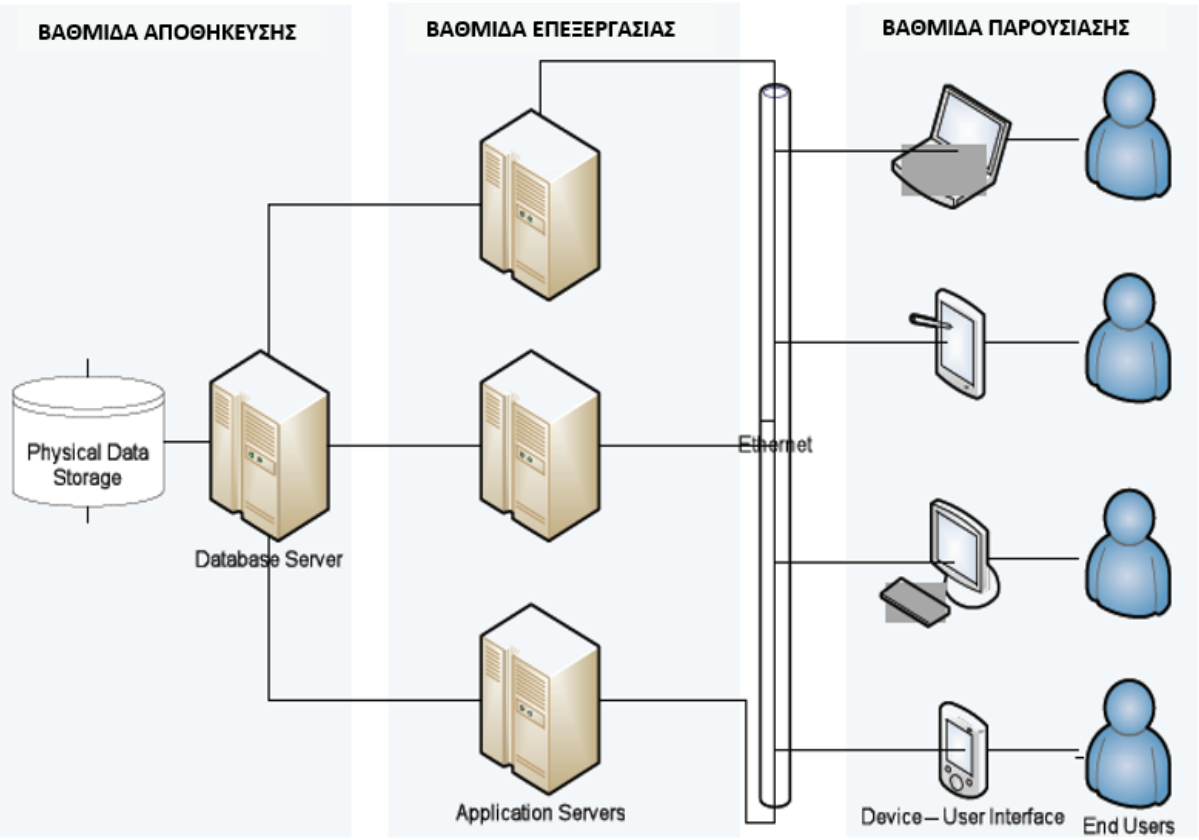
Κεφάλαιο 4
Περιγραφή Συστήματος

Σε αυτό το κεφάλαιο αναλύεται η αρχιτεκτονική τριών βαθμίδων που υπάρχει σε ένα τυπικό δίκτυο ενός οργανισμού. Επίσης προτείνεται ένα συστήματος επίβλεψης το οποίο θα δημιουργεί αρχεία καταγραφής τα οποία θα αποτυπώνουν τις δραστηριότητες των χρηστών των πληροφοριακών υποδομών του οργανισμού. Τα αρχεία καταγραφής συγκεντρώνονται σε μία βάση δεδομένων, κατάλληλα διαμορφωμένη, ακολουθώντας την μέθοδο της συγκεντρωτικής καταγραφής με σκοπό να τροφοδοτήσουν το σύστημα τεχνητής νοημοσύνης. Για το σύστημα τεχνητής νοημοσύνης έχουν επιλεχθεί οι αλγόριθμοι SOM και ESOINN που αναλύθηκαν στο προηγούμενο κεφάλαιο. Με βάση αυτούς τους αλγορίθμους και την μέθοδο της συγκεντρωτικής καταγραφής παρουσιάζεται η εφαρμογή που υλοποιήθηκε για την ανίχνευση των εσωτερικών απειλών σε ένα εταιρικό δίκτυο.

4.1 Αρχιτεκτονική Συστήματος

Ένα τυπικό εταιρικό δίκτυο είναι δομημένο στην αρχιτεκτονική τριών βαθμίδων (3-tier architecture): την βαθμίδα αποθήκευσης, την βαθμίδα επεξεργασίας και την βαθμίδα παρουσίασης (***Εικόνα 5***). Η Βαθμίδα Αποθήκευσης (Storage Tier) είναι υπεύθυνη για την διαχείριση των αιτήσεων ανάκτησης και αποθήκευσης των δεδομένων. Το σύστημα διαχείρισης βάσης δεδομένων (DBMS) είναι συνυφασμένο με το επίπεδο αποθήκευσης. Η βαθμίδα επεξεργασίας (processing tier), η οποία είναι η δεύτερη βαθμίδα, είναι ο ενδιάμεσος μεταξύ της πρώτης και της τρίτης βαθμίδας. Αυτό το επίπεδο λαμβάνει τις καταχωρήσεις του χρήστη από την βαθμίδα παρουσίασης, ελέγχει την εγκυρότητα των δεδομένων και εφαρμόζει τους κανόνες του οργανισμού. Επίσης επικοινωνεί με την βαθμίδα αποθήκευσης για να ανακτήσει επιπλέον δεδομένα ή να τα ελέγξει. Ο τελικός χρήστης (client) αλληλοεπιδρά με την βαθμίδα παρουσίασης η οποία αποτελεί την τρίτη βαθμίδα της αρχιτεκτονικής τριών βαθμίδων. Όλες οι λειτουργίες της εξαρτώνται

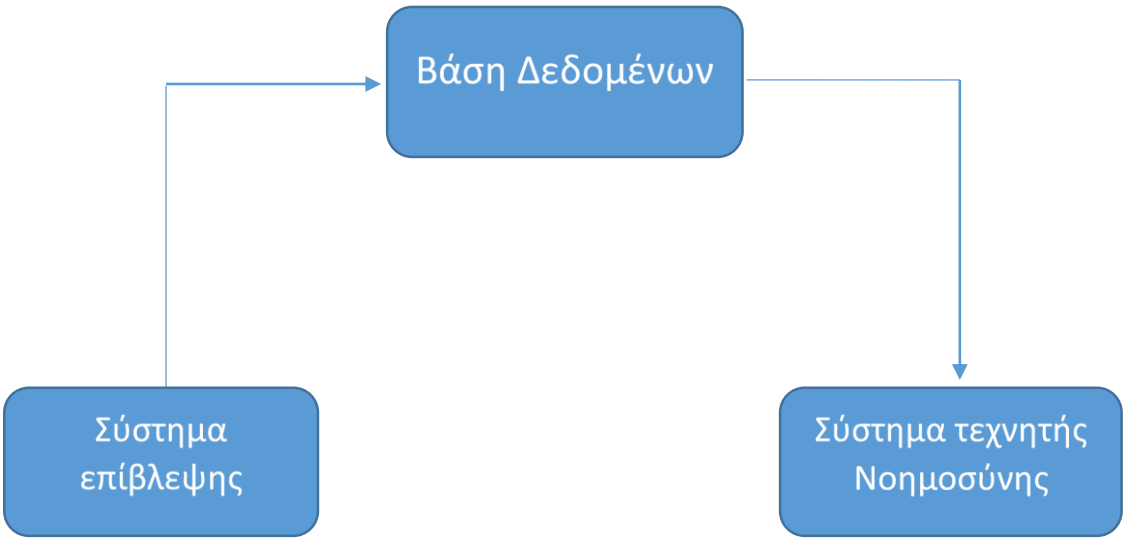
από τις συσκευές που μπορεί να χρησιμοποιηθεί πληκτρολόγιο ή ποντίκι, όπως επιτραπέζιους υπολογιστές και φορητούς υπολογιστές. Επίσης είναι υπεύθυνη για να δέχεται τις εισαγωγές του χρήστη, την παρουσίαση των δεδομένων και την καλή απόδοση της διασύνδεσης του χρήστη.



Εικόνα 5. Αρχιτεκτονική Τριών Βαθμίδων

Ένας από τους στόχους της παρούσας μεταπτυχιακής διατριβής αφορά την ανάπτυξη ενός συστήματος που θα εντοπίζει τις εσωτερικές απειλές σε ένα εταιρικό δίκτυο ανεξαρτήτως του λειτουργικού συστήματος. Σε όλα τα εταιρικά δίκτυα υπάρχουν συστήματα που καταγράφουν την κίνηση μέσα στο δίκτυο και την αποθηκεύουν σε αρχεία καταγραφής (log files). Επίσης πολλές εφαρμογές παράγουν αρχεία καταγραφής που φανερώνουν κάποιο είδος δραστηριότητας όπως η πρόσβαση σε ιστοσελίδες, το άνοιγμα κάποιου αρχείου καθώς και η είσοδος ή έξοδος από ένα τερματικό. Οι διάφοροι τύποι αρχείων καταγραφής είτε αυτά αφορούν πληροφορίες για το λειτουργικό του συστήματος ή για το δίκτυο ή για οτιδήποτε άλλο, έχουν ως κοινό χαρακτηριστικό την χρονολογική σειρά. Κάθε αρχείο καταγραφής περιέχει πληροφορίες σχετικά με το ποια ημερομηνία και τι ώρα έγινε μία ενέργεια.

Η εφαρμογή που αναπτύχθηκε στηρίζεται σε αρχεία καταγραφής της δραστηριότητας των χρηστών ενός εταιρικού δικτύου. Η δραστηριότητα των χρηστών αναλύεται για την εξαγωγή συμπερασμάτων σχετικά με το αν η συμπεριφορά του χρήστη είναι κακόβουλη ή όχι. Το σύστημα που προτείνουμε αποτελείται από τρία βασικά μέρη: το Σύστημα Επίβλεψης (Monitoring System), την Βάση Δεδομένων (Database) και το Σύστημα Τεχνητής Νοημοσύνης (Artificial Intelligent System) (***Εικόνα 6***). Παρότι ασχοληθήκαμε με την ανάπτυξη των τελευταίων δύο τμημάτων για λόγους πληρότητας παρουσιάζουμε μια μικρή περιγραφή και του συστήματος επίβλεψης καθότι έχει άμεση σχέση με την βάση δεδομένων.



Εικόνα 6. Βασικά μέρη συστήματος

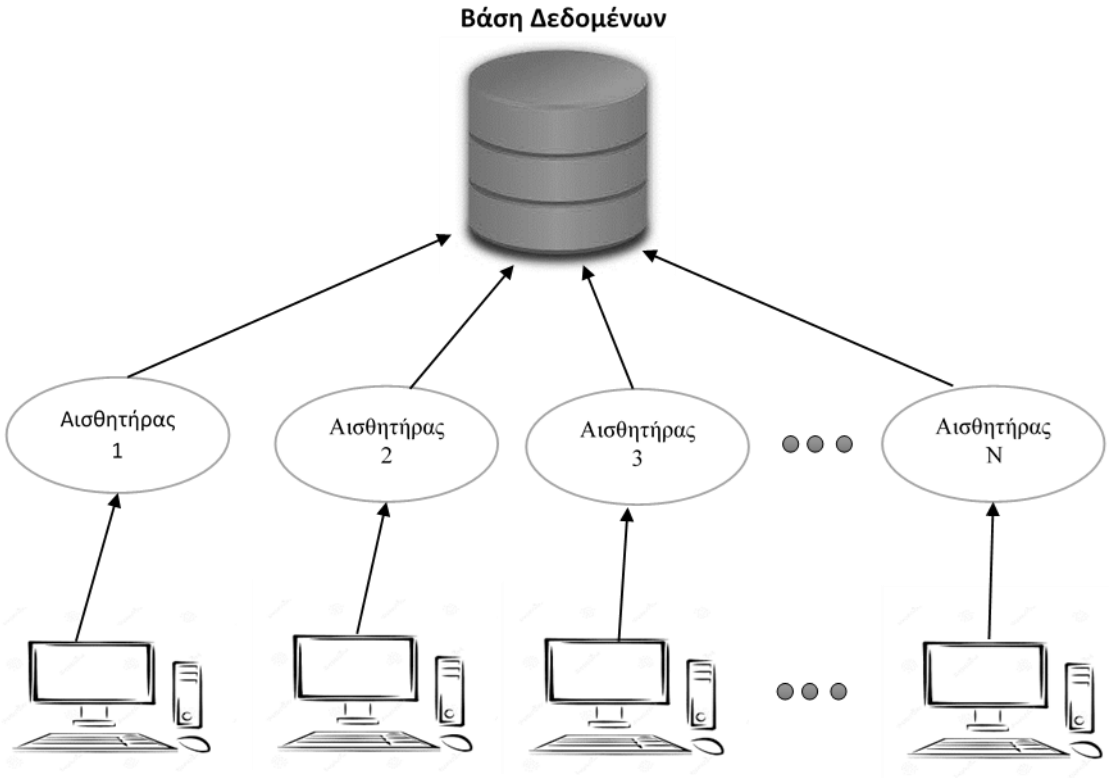
4.1.1 Σύστημα Επίβλεψης (Monitoring System)

Ένα σύστημα επίβλεψης μπορεί να χαρακτηριστεί ως ένα σύνολο από διαδικασίες που οδηγούν τις πληροφορίες, οι οποίες ρέουν μέσα σε ένα οργανισμό σε διαφορετικά επίπεδα διαχείρισης, προκειμένου να υποστηρίξουν την λήψη αποφάσεων και την μάθηση (MDF 2011). Το δικό μας σύστημα επίβλεψης θέλουμε να καταγράφει ενέργειες σχετικά με τις δραστηριότητες ενός χρήστη του πληροφοριακού συστήματος μίας εταιρίας.

Η παρακολούθηση των δραστηριοτήτων προσπαθεί να εντοπίσει σε μία ακολουθία δεδομένων πού ακριβώς έχει προκύψει μια ενδιαφέρουσα αλλαγή στην συμπεριφορά

(Fawcett & Provost 1999). Για την καταγραφή των δραστηριοτήτων κάθε χρήστη, προτείνουμε σε κάθε τερματικό της εταιρίας να υπάρχουν αισθητήρες οι οποίοι θα συγκεντρώνουν πληροφορίες σε σχέση με (***Εικόνα 7***):

- τις ώρες σύνδεσης και αποσύνδεσης από το σύστημα
- τις ώρες σύνδεσης και αποσύνδεσης συσκευών, όπως φορητούς σκληρούς δίσκους
- τα αρχεία που έχουν πρόσβαση οι χρήστες
- τις ιστοσελίδες που επισκέπτονται οι χρήστες
- τα μηνύματα ηλεκτρονικού ταχυδρομείου, όπως αποστολέας, παραλήπτης, μέγεθος επισυναπτόμενων αρχείων κτλ.



Εικόνα 7. Δομή Συστήματος Επίβλεψης

4.1.2 Βάση Δεδομένων

Τα αρχεία καταγραφής ως επί των πλείστων είναι διασκορπισμένα σε όλες τις εφαρμογές οι οποίες μπορεί να βρίσκονται σε διάφορα μέρη ενός δικτύου, όπως σε εξυπηρετητές και σταθμούς εργασίας. Σε ένα εταιρικό δίκτυο οι σταθμοί εργασίας αποτελούν την μεγαλύτερη πηγή αρχείων καταγραφής. Η πολυπλοκότητα της

ανάλυσης των αρχείων καταγραφής αυξάνει όταν υπάρχουν πολλές τοποθεσίες από τις οποίες πρέπει να συγκεντρωθούν δεδομένα. Αν υποθέσουμε ότι μία εταιρία έχει 100 σταθμούς εργασίας τότε η λήψη δεδομένων για ανάλυση, και από τους 100 υπολογιστές, θα υπερφορτώσει το δίκτυο. Επομένως, προκύπτει η ανάγκη να βρεθεί μία λύση ώστε τα δεδομένα να είναι ευκολότερα προσβάσιμα αλλά και να μην προκαλούν προβλήματα υπερφόρτωσης στο δίκτυο.

Η μεθοδολογία της συγκεντρωτικής καταγραφής (centralized logging) είναι η λύση για το παραπάνω πρόβλημα. Η συγκεντρωτική καταγραφή συγκεντρώνει τα αρχεία καταγραφής τα οποία είναι διασκορπισμένα στο δίκτυο και τα αποθηκεύει σε μία βάση δεδομένων. Συνεπώς, υπάρχει η δυνατότητα τα αρχεία να καταγράφονται σε ενιαίους πίνακες ανάλογα με την δραστηριότητα του χρήστη, οι οποίοι μπορούν να ταξινομηθούν κατά χρονολογική σειρά. Αυτή η συγκέντρωση σε πίνακες ανά δραστηριότητα μπορεί να χρησιμοποιηθεί για την περαιτέρω ανάλυση των δεδομένων μειώνοντας το κόστος αναζήτησης των αρχείων καταγραφής, όταν αυτά βρίσκονται αποκεντρωμένα σε διάφορα μέρη του δικτύου.

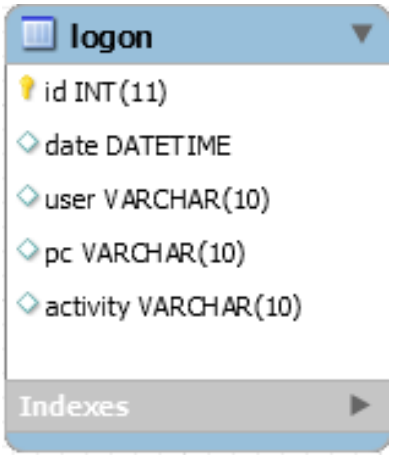
Στο προτεινόμενο σύστημα τα αρχεία καταγραφής συγκεντρώνονται στην βάση δεδομένων κατά δραστηριότητα χρήστη. Ειδικότερα, υπάρχουν οι παρακάτω πίνακες των οποίων τα δεδομένα είναι ταξινομημένα κατά χρονολογική σειρά:

- Logon: στον πίνακα Logon καταγράφονται οι δραστηριότητες σύνδεση και αποσύνδεση για κάθε χρήστη.
- Device: στον πίνακα Devices υπάρχουν πληροφορίες για το πότε συνδέθηκε μία συσκευή στο σύστημα για κάθε χρήστη.
- File: ο πίνακας File περιέχει πληροφορίες για τα αρχεία στα οποίο είχε πρόσβαση κάθε χρήστης.
- Http: σε αυτό τον πίνακα καταγράφονται οι ιστοσελίδες τις οποίες επισκέφτηκε κάθε χρήστης.
- Email: ο πίνακας Email έχει πληροφορίες για τα μηνύματα ηλεκτρονικού ταχυδρομείου τα οποία έστειλε ο κάθε χρήστης.

Κοινό στοιχείων όλων των παραπάνω πινάκων είναι ότι έχουν τις κοινές στήλες id, date, user και pc:

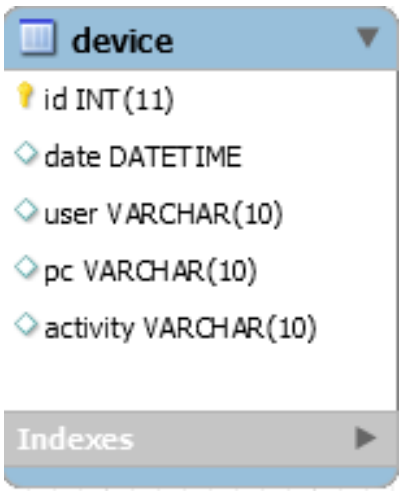
- id: είναι η στήλη η οποία περιέχει την «ταυτότητα» της συγκεκριμένης δραστηριότητας. Οι τιμές τις είναι ακέραιοι αριθμοί, ξεκινάνε από 1 και αυξάνονται κατά ένα όταν καταγράφεται καινούρια δραστηριότητα στον πίνακα.
- date: είναι η στήλη στην οποία καταγράφεται η ημερομηνία και η ώρα που έγινε μία δραστηριότητα. Οι τιμές τις είναι τύπου datetime.
- user: στην στήλη user καταχωρούνται οι χρήστες οι οποίο πραγματοποίησαν την συγκεκριμένη δραστηριότητα. Οι τιμές τις είναι τύπου varchar.
- pc: η στήλη pc περιέχει τον υπολογιστή στον οποίο έγινε η συγκεκριμένη δραστηριότητα του χρήστη. Οι τιμές τις είναι τύπου varchar.

Πιο αναλυτικά ο πίνακας Logon έχει την δομή που φαίνεται στην ***Εικόνα 8***. Η στήλη activity μπορεί να πάρει τις τιμές logon και logoff οι οποίες φανερώνουν αν ο χρήστης συνδέθηκε ή αποσυνδέθηκε από τον υπολογιστή αντίστοιχα. Οι τιμές της στήλης activity είναι τύπου varchar.



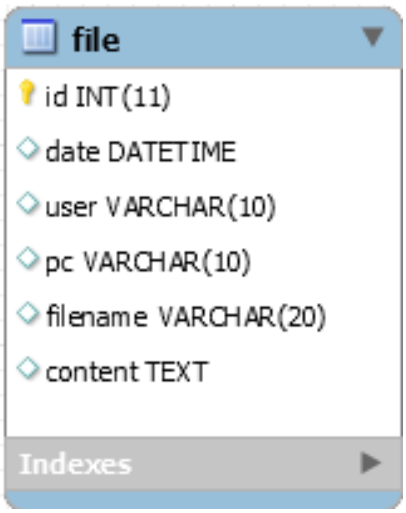
Εικόνα 8. Πίνακας Logon

Ο πίνακας Device αποτελείται από τις στήλες id, date, user, pc και activity (***Εικόνα 9***). Σε αντίθεση με τον πίνακα Logon, σε αυτόν το πίνακα η στήλη activity παίρνει τις τιμές connect ή disconnect ανάλογα με το αν ο χρήστης σύνδεσε ή αποσύνδεσε αφαιρούμενη συσκευή στον υπολογιστή. Οι τιμές της στήλης είναι τύπου varchar.



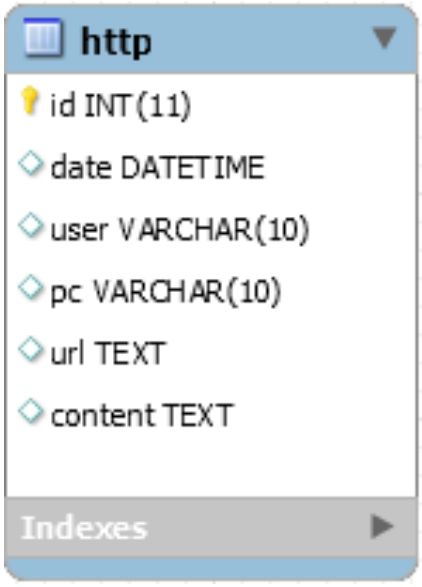
Εικόνα 9. Πίνακας Device

Ο πίνακας File αποτελείται από τις στήλες id, date, user, pc, filename και content (***Εικόνα 10***). Η στήλη filename έχει τα ονόματα των αρχείων των οποίων είχε πρόσβαση ο χρήστης καθώς και την προέκτασή τους. Είναι τύπου varchar. Η στήλη content μπορεί να περιέχει την επικεφαλίδα του αρχείου σε κωδικοποιημένη μορφή, όπως το δεκαεξαδικό σύστημα. Επίσης μπορούν να υπάρχουν λέξεις κλειδιά οι οποίες προϊδεάζουν για το περιεχόμενο του αρχείου. Για αυτό λόγο ο τύπος της στήλης είναι TEXT.



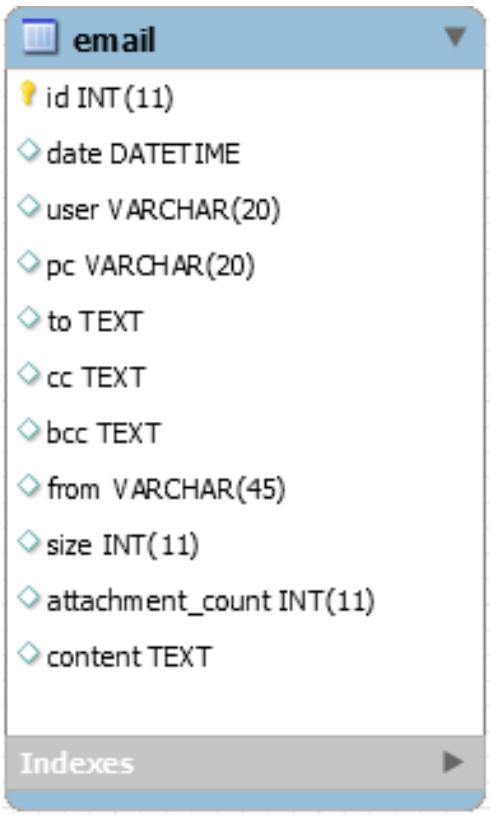
Εικόνα 10. Πίνακας File

Ο πίνακας Http περιέχει τις στήλες id, date, user, pc, url και content (***Εικόνα 11***). Η στήλη url παίρνει ως τιμές την διεύθυνση των ιστοσελίδων τις οποίες επισκέφτηκε ο χρήστης. Στην στήλη content καταχωρούνται οι λέξεις κλειδιά των περιεχομένων της ιστοσελίδας. Οι στήλες url και content είναι τύπου TEXT λόγω του μεγάλου μήκους χαρακτήρων που μπορούν να φτάσουν.



Εικόνα 11. Πίνακας Http

Στον πίνακα Email εκτός από τις κοινές στήλες τις οποίες αναφέραμε νωρίτερα υπάρχουν οι στήλες to, cc, bcc, from, size, attachment_count και content (***Εικόνα 12***). Η στήλη to δηλώνει τον παραλήπτη του ηλεκτρονικού μηνύματος και η στήλη from δηλώνει τον αποστολέα. Η στήλη from είναι τύπου varchar επειδή ο αποστολέας μπορεί να είναι μόνο ένας, ενώ η στήλη to είναι τύπου TEXT επειδή μπορεί να υπάρχουν πολλαπλοί παραλήπτες.



Εικόνα 12. Πίνακας Email

Οι στήλες cc και bcc περιέχουν επίσης παραλήπτες οι οποίοι μπορεί να είναι πολλαπλοί. Όταν οι παραλήπτες βρίσκονται στην στήλη cc τότε ενημερώνονται και για το ποιος άλλος έχει λάβει το ίδιο ηλεκτρονικό μήνυμα. Από την άλλη πλευρά όταν οι παραλήπτες είναι στην στήλη bcc, στο ηλεκτρονικό μήνυμα που λαμβάνουν, δεν υπάρχουν πληροφορίες για το ποιος άλλος το έχει λάβει. Η στήλη size έχει το μέγεθος του ηλεκτρονικού μηνύματος και η στήλη attachment_count το πλήθος των συνημμένων αρχείων. Τέλος στην στήλη content καταγράφονται λέξεις οι οποίες δηλώνουν το περιεχόμενο του μηνύματος.

4.2 Περιγραφή εφαρμογής

Βασιζόμενοι στο σύστημα το οποίο περιγράψαμε στο υποκεφάλαιο 4.1, αναπτύχθηκε η εφαρμογή Insider Threat Detection System (ITDS). Η εφαρμογή ITDS επικοινωνεί με την βάση δεδομένων στην οποία έχουν καταχωρηθεί οι δραστηριότητες των χρηστών ενός εταιρικού δικτύου. Αφού επιτευχθεί η σύνδεση της εφαρμογής με την βάση δεδομένων, επιλέγεται από τον χρήστη της εφαρμογής ένα χρονικό διάστημα ημερομηνιών από τις οποίες θέλει να λάβει δεδομένα. Τα δεδομένα που λαμβάνονται μπορεί να είναι, είτε για

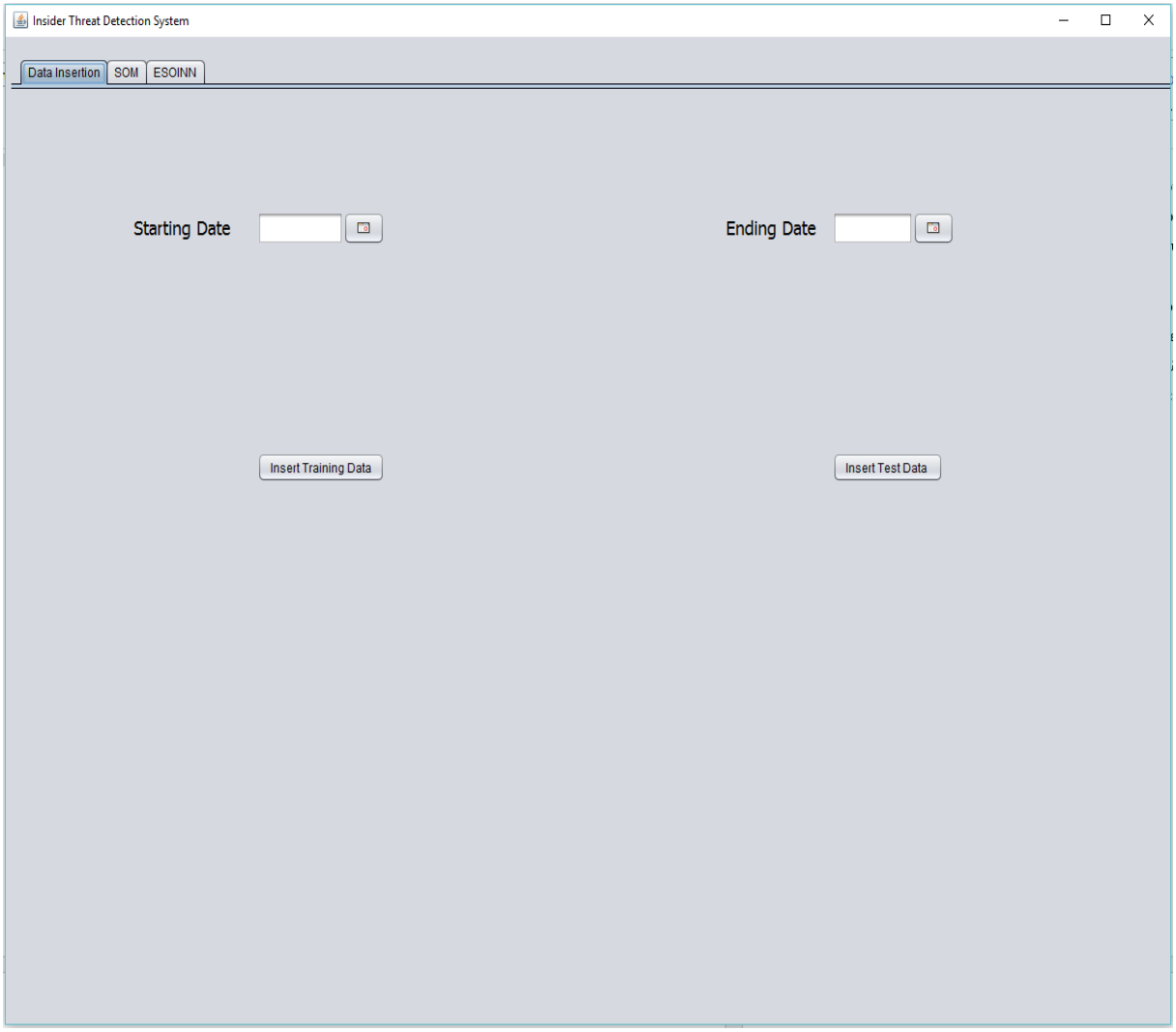
την εκπαίδευση, είτε για την δοκιμή των αλγορίθμων τεχνητής νοημοσύνης SOM και ESOINN.

Όταν ληφθούν τα δεδομένα εκπαίδευσης τροποποιούνται κατάλληλα ώστε να μπορέσουν να τροφοδοτήσουν τους αλγορίθμους SOM και ESOINN. Η διαδικασία αυτή λέγεται κανονικοποίηση (normalization) των δεδομένων. Κατά την διαδικασία της εκπαίδευσης η εφαρμογή παρέχει μετρικές για το νευρωνικό δίκτυο του αλγορίθμου SOM. Οι μετρικές αυτές αφορούν το πλήθος των δεδομένων τα οποία ταξινομήθηκαν σε κάθε κόμβο του δικτύου καθώς και την απόσταση του από τους γειτονικούς κόμβους. Έτσι ο χρήστης της εφαρμογής μπορεί να εκπαιδεύσει τους αλγορίθμους βασιζόμενος στις μετρήσεις αυτές. Για παράδειγμα μπορεί να δοκιμάσει διάφορες παραμέτρους ώστε όλοι οι κόμβοι του νευρωνικού δικτύου να μην είναι κενοί.

Μετά το πέρας κάθε εκπαιδευτικής διαδικασίας παρέχεται η δυνατότητα να παρουσιαστούν τα δεδομένα τα οποία έχουν ταξινομηθεί σε μία συστάδα. Αφού γίνει η επιθυμητή εκπαίδευση των αλγορίθμων η επόμενη διαδικασία είναι ο έλεγχος της απόδοσης των αλγορίθμων. Πριν γίνει αυτό πρέπει να έχουν επιλεγεί τα δεδομένα δοκιμής.

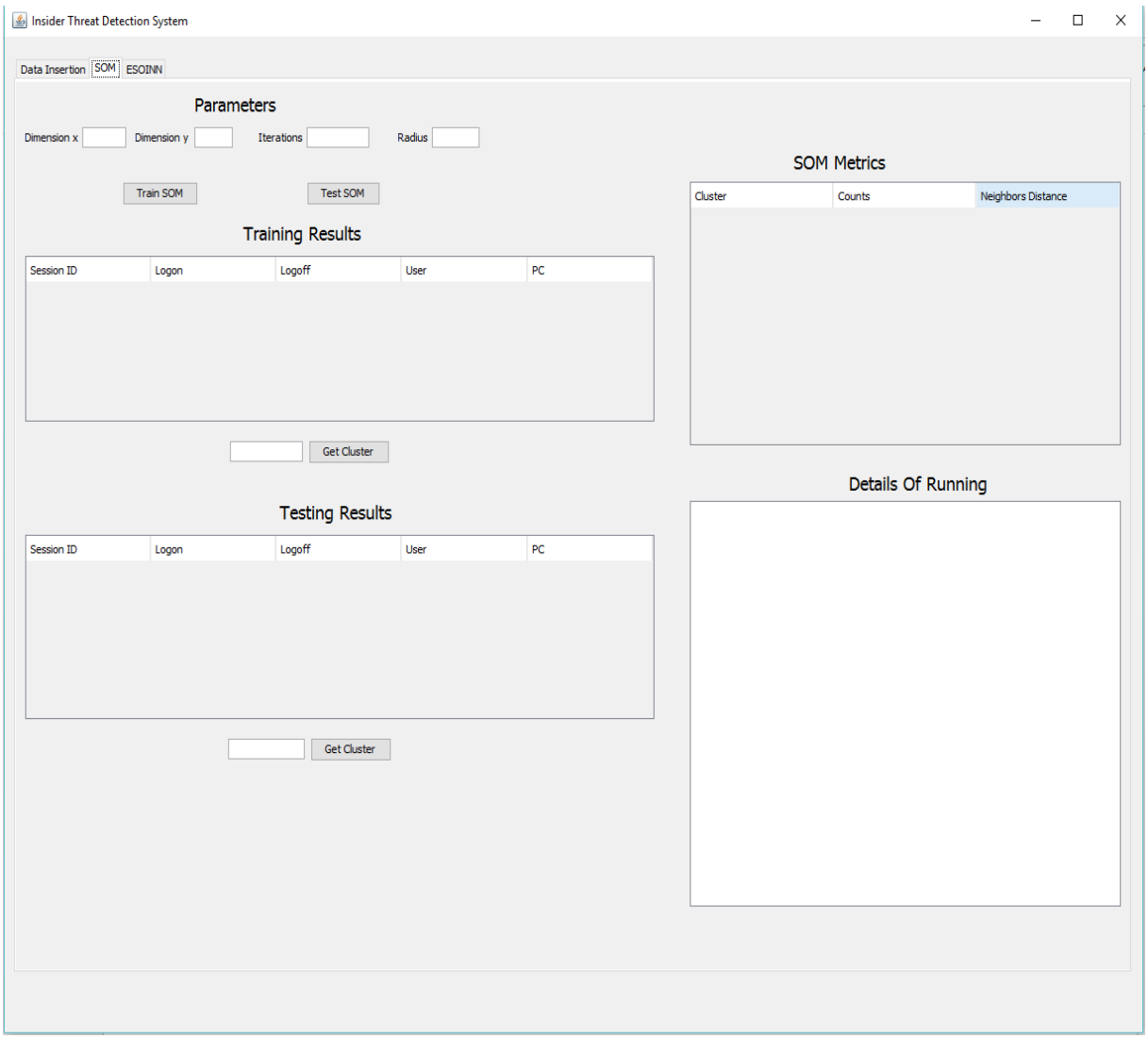
Στην διαδικασία της δοκιμής τα δεδομένα τροποποιούνται με την ίδια συνάρτηση κανονικοποίησης όπως και στην διαδικασία εκπαίδευσης. Κατά την διάρκεια της δοκιμής τα δεδομένα ταξινομούνται σε κόμβους οι οποίοι έχουν δημιουργηθεί στο βήμα της εκπαιδευτικής διαδικασίας. Και σε αυτή την διαδικασία παρέχεται η δυνατότητα να παρουσιαστούν τα δεδομένα δοκιμής τα οποία ανήκουν σε ένα κόμβο.

Πιο αναλυτικά η εφαρμογή ITDS αποτελείται από τρεις καρτέλες: την καρτέλα εισαγωγής δεδομένων (Data Insertion), την καρτέλα SOM και την καρτέλα ESOINN. Η καρτέλα Data Insertion είναι υπεύθυνη για την εισαγωγή δεδομένων (***Εικόνα 13***). Ο χρήστης μπορεί να εισάγει το χρονικό διάστημα των ημερομηνιών για το οποίο θέλει να πάρει δείγμα δεδομένων από την βάση. Τα κουμπιά Insert Training Data και Insert Test Data είναι για την εισαγωγή δεδομένων για την διαδικασία της εκπαίδευσης και του ελέγχου αντίστοιχα.



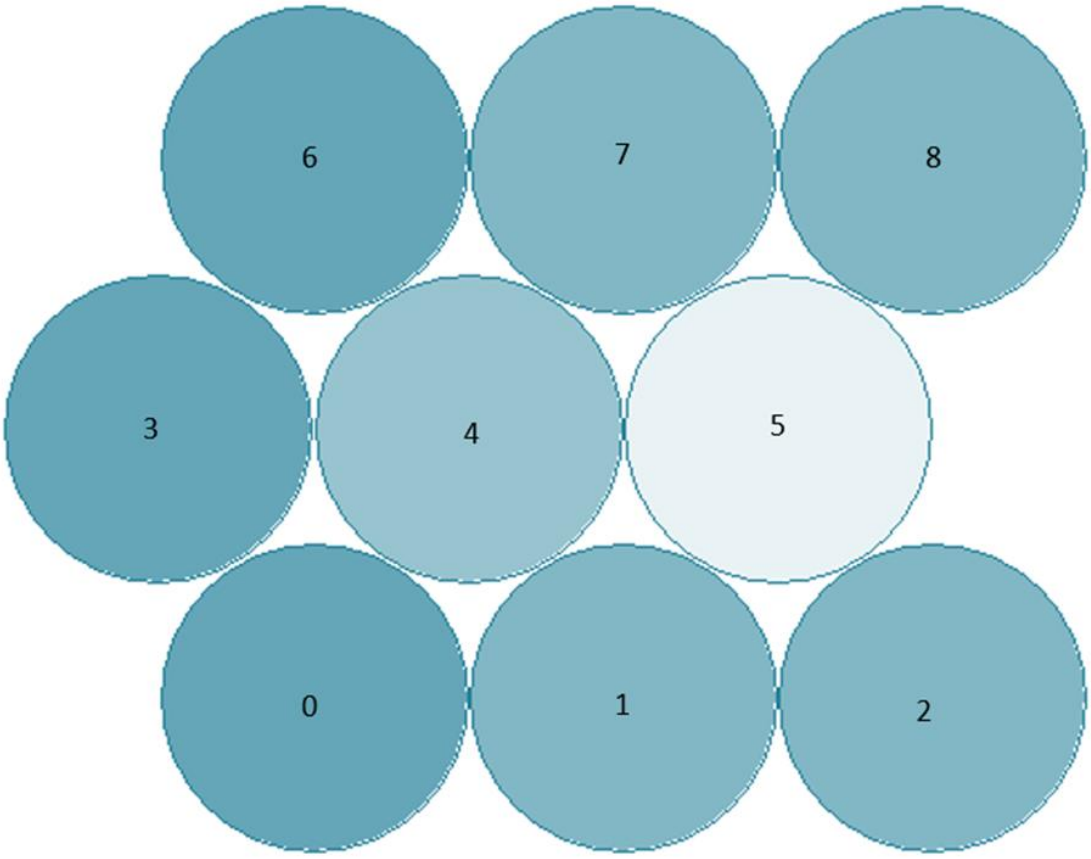
Εικόνα 13. Η καρτέλα Data Insertion της εφαρμογή ITDS

Η καρτέλα SOM φιλοξενεί όλες τις απαραίτητες λειτουργίες για την εκπαίδευση και την δοκιμή του αλγορίθμου SOM (***Εικόνα 14***). Στο τμήμα Parameters τα πεδία Dimension x και Dimension y καθορίζουν την διάσταση του πλέγματος του νευρωνικού δικτύου του αλγορίθμου SOM. Το πεδίο iteration αναφέρεται στον αριθμό των επαναλήψεων που θα εκτελεστεί ο SOM για το σύνολο των δεδομένων εκπαίδευσης. Στο πεδίο radius καθορίζεται η ακτίνα των γειτονικών κόμβων τους οποίος θα λάβει υπόψιν του ο κόμβος νικητής και θα ανανεώσει τις τιμές των βαρών του καθώς και των γειτονικών κόμβων ώστε να «μοιάσουν» στα δεδομένα εισόδου. Η εκπαίδευση και η δοκιμή του SOM στα δεδομένα εισόδου γίνεται με τα κουμπιά Train SOM και Test SOM.



Εικόνα 14. Η καρτέλα SOM της εφαρμογής ITDS

Στο τμήμα SOM Metrics παρουσιάζονται οι μετρήσεις για την διαδικασία εκπαίδευσης του αλγορίθμου SOM. Συγκεκριμένα απεικονίζεται για κάθε συστάδα το πλήθος των δεδομένων τα οποία έχουν ταξινομηθεί σε αυτό. Επίσης, μετριέται η απόσταση κάθε συστάδας από τις γειτονικές της βασιζόμενη στις θέσεις των νευρώνων στο δίκτυο, καθώς και στις διαστάσεις του πλέγματος οι οποίες δόθηκαν πριν την εκτέλεση της εκπαιδευτικής διαδικασίας. Για παράδειγμα σε ένα πλέγμα 3x3 η συστάδα 2 είναι στο κάτω μέρος και δεξιά (***Εικόνα 15***). Σημειώνουμε ότι οι συστάδες μετριούνται από το 0, άρα η συστάδα 2 είναι ο τρίτος κόμβος. Επομένως οι γειτονικοί κόμβοι είναι οι δύο κόμβοι που βρίσκονται αριστερά και πάνω, δηλαδή ο 1 και ο 5 αντίστοιχα.



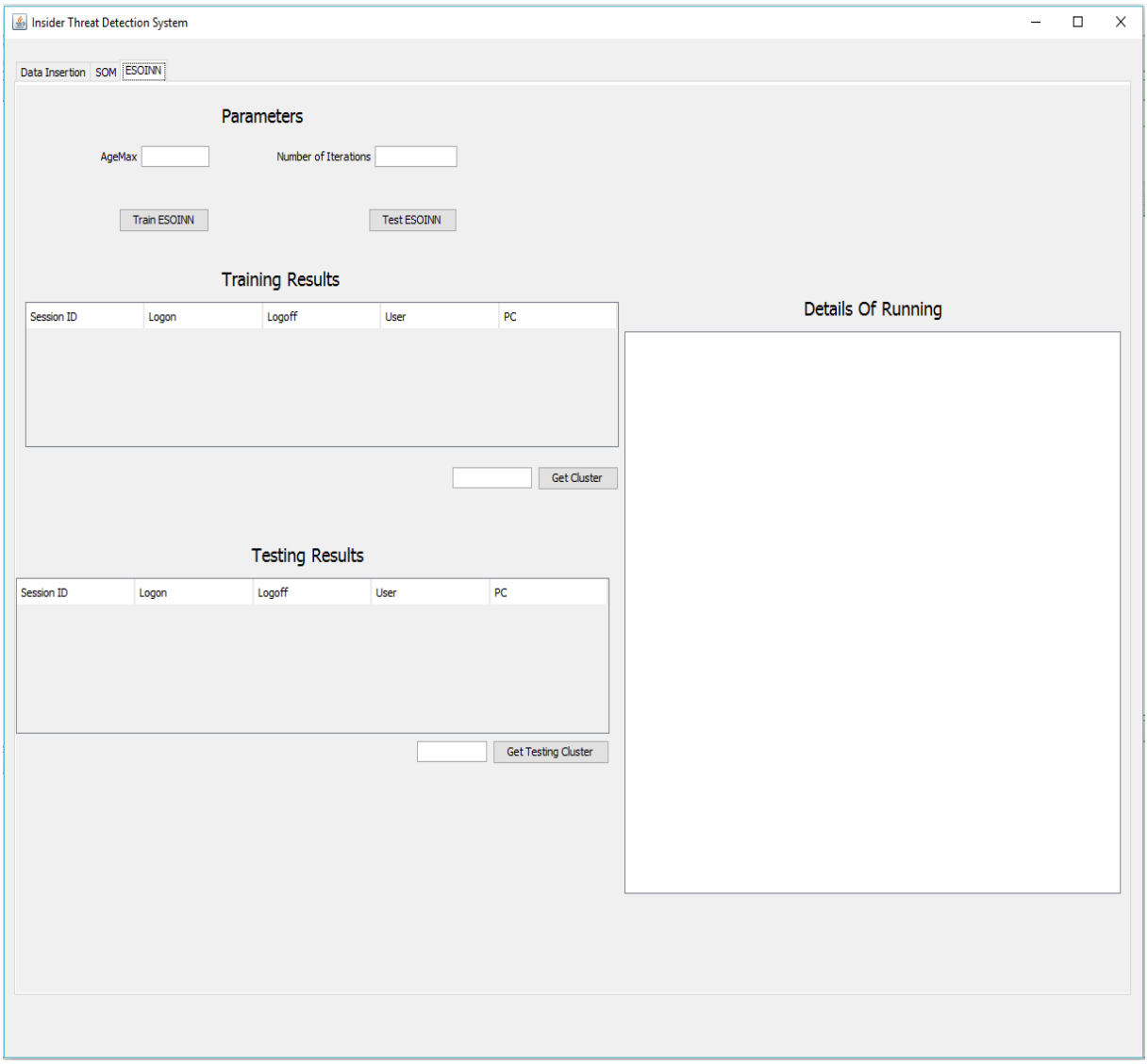
Εικόνα 15. Πλέγμα SOM διάστασης 3x3

Στο τμήμα Training Results απεικονίζονται με περισσότερη λεπτομέρεια οι συνεδρίες, οι οποίες ανήκουν σε μία συστάδα. Αναλυτικότερα ο χρήστης μπορεί να διαλέξει τον αριθμό της συστάδας και πατώντας το κουμπί Get Cluster, εμφανίζονται στον πίνακα οι συνεδρίες χρήστη οι οποίες έχουν ταξινομηθεί στην συστάδα αυτή μετά το πέρας της εκπαίδευσης. Κάθε γραμμή του πίνακα δείχνει τον αριθμό της συνεδρίας, την ημερομηνία και ώρα σύνδεσης και αποσύνδεσης του χρήστη, τον χρήστη της συνεδρίας, καθώς και τον υπολογιστή τον οποίο χρησιμοποιεί.

Το τμήμα Testing Results έχει ακριβώς τον ίδιο τρόπο λειτουργίας με το τμήμα Training Result, αλλά είναι υπεύθυνο για τα δεδομένα δοκιμής. Στον πίνακα του Testing Results παρουσιάζονται με λεπτομέρεια οι συνεδρίες χρήστη, οι οποίες ανήκουν στην συστάδα που επιλέχθηκε, αφού πρώτα έχει γίνει η διαδικασία δοκιμής του αλγορίθμου.

Τέλος, στο τμήμα Details Of Running παρουσιάζονται συγκεντρωτικά όλα τα αποτελέσματα για τις διαδικασίες εκπαίδευσης και δομικής του αλγορίθμου SOM. Συγκεκριμένα για κάθε διαδικασία παρουσιάζονται σε μορφή κειμένου ο αριθμός της συστάδας και οι αριθμοί των συνεδριών χρήστη που ανήκουν σε αυτή.

Η τελευταία καρτέλα ESOINN είναι υπεύθυνη για την χρήση του αλγορίθμου ESOINN στα δεδομένα εισόδου (***Εικόνα 16***). Στο τμήμα Parameters το πεδίο AgeMax αναφέρεται στον μέγιστο αριθμό των ακμών που μπορεί να φτάσει μία συστάδα του αλγορίθμου. Το πεδίο Number Of Iteration καθορίζει το σύνολο των επαναλήψεων που ένα διάνυσμα εισόδου θα εκπαιδευτεί στον ESOINN. Οι διαδικασίες της εκπαίδευση και της δοκιμής του ESOINN στα δεδομένα εισόδου γίνονται με τα κουμπιά Train ESOINN και Test ESOINN.



Εικόνα 16. Η καρτέλα ESOINN της εφαρμογής ITDS

Το τμήμα Training Results είναι υπεύθυνο για την απεικόνιση των αποτελεσμάτων μετά το πέρας της διαδικασίας εκπαίδευσης του αλγορίθμου. Ο χρήστης της εφαρμογής έχει τη δυνατότητα να επιλέξει τον αριθμό της συστάδας που επιθυμεί και να δει τις

συνεδρίες χρήστη οι οποίες είναι ταξινομημένες σε αυτή. Όταν επιλεγεί η συστάδα και πατηθεί το κουμπί Get Cluster τότε εμφανίζονται στον πίνακα οι συνεδρίες η οποίες ανήκουν στην συστάδα αυτή. Κάθε γραμμή του πίνακα δείχνει τον αριθμό της συνεδρίας, την ημερομηνία και ώρα σύνδεσης και αποσύνδεσης τους χρήστη, τον χρήστη της συνεδρίας καθώς και τον υπολογιστή τον οποίο χρησιμοποιεί.

Το τμήμα Testing Results είναι υπεύθυνο για την παρουσίαση των αποτελεσμάτων μετά το πέρας της διαδικασίας δοκιμής του ESOINN. Γράφοντας την συστάδα της οποίας τις συνεδρίες θέλουμε να δούμε και επιλέγοντας το κουμπί Get Cluster, παρουσιάζονται στον πίνακα οι συνεδρίες χρήστη που ανήκουν σε αυτή την συστάδα. Όπως και με τον πίνακα του τμήματος Training Results εμφανίζονται αναλυτικά οι λεπτομέρειες για κάθε συνεδρία.

Τέλος, στο τμήμα Details Of Running καταγράφονται όλα τα αποτελέσματα για τις διαδικασίες εκπαίδευσης και δοκιμής του αλγορίθμου ESOINN. Σε κάθε διαδικασία, είτε είναι της εκπαίδευσης, είτε της δοκιμής παρουσιάζονται για κάθε συστάδα οι συνεδρίες οι οποίες ανήκουν σε αυτή.

4.2.1 Αρχιτεκτονική Εφαρμογής

Η εφαρμογή ITDS υλοποιήθηκε με την χρήση του μοτίβου MVC (Model – View – Controller pattern).

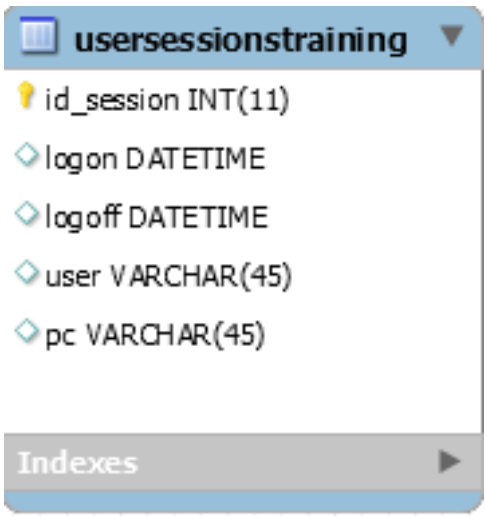
- Το μοντέλο (model) αντιπροσωπεύει μία δομή η οποία περιέχει δεδομένα. Μπορεί επίσης να έχει κάποια λογική να ενημερώνει τον ελεγκτή αν υπάρξει κάποια αλλαγή στα δεδομένα.
- Η παρουσίαση (view) είναι υπεύθυνη για την απεικόνιση των δεδομένων τα οποία περιέχει το μοντέλο.
- Ο ελεγκτής (controller) είναι ο ενδιάμεσος μεταξύ του μοντέλου και της παρουσίασης. Ελέγχει την ροή των δεδομένων που τροφοδοτούν το μοντέλο και ενημερώνει την παρουσίαση για τις ενδεχόμενες αλλαγές.

Στην εφαρμογή που υλοποιήσαμε μοντέλο είναι η βάση δεδομένων. Εκεί υπάρχουν όλες οι πληροφορίες για τις δραστηριότητες των χρηστών. Στην βάση δεδομένων εκτός από τους πίνακες logon, device, file, http και email προσθέσαμε και τους πίνακες

usersessionsTraining και usersessionsTesting. Οι πίνακες καταγράφουν ακριβώς τους ίδιους τύπους πληροφοριών, δηλαδή την σύνδεση και την αποσύνδεση ενός χρήστη σε έναν συγκεκριμένο υπολογιστή.

Θα μπορούσαμε να χρησιμοποιήσουμε έναν πίνακα για αυτές τις πληροφορίες αλλά θέλαμε να αποθηκεύονται ξεχωριστά οι συνεδρίες των χρηστών για την διαδικασία της εκπαίδευσης και του ελέγχου. Με την χρήση ενός πίνακα έπρεπε να πραγματοποιήσουμε την εκπαίδευση και των δύο αλγορίθμων πριν προχωρήσουμε στη διαδικασία του ελέγχου καθώς χάνονταν οι πληροφορίες για τις συνεδρίες χρήστη. Δημιουργώντας δύο πίνακες ανεξαρτητοποιήθηκαν οι διαδικασίες της εκπαίδευσης και του ελέγχου.

Αναλυτικότερα στον πίνακα usersessionsTraining αποθηκεύονται πληροφορίες σχετικά με την διάρκεια σύνδεσης ενός χρήστη σε έναν υπολογιστή για το δείγμα εκπαίδευσης. Αποτελείται από τις στήλες id_session, logon, logoff, user και pc (***Εικόνα 17***). Η στήλη id_session ξεκινάει από το 1 και αυξάνεται κατά ένα όταν εισαχθεί νέα συνεδρία χρήστη. Σημειώνουμε ότι ο αριθμός της συνεδρίας χρήστη ξεκινάει να μετράει από το χρονικό διάστημα, το οποίο έχει καθορίσει ο χρήστης της εφαρμογής για την επιλογή των δεδομένων εκπαίδευσης και όχι από το σύνολο των δεδομένων τα οποία είναι καταχωρημένα στην βάση δεδομένων.

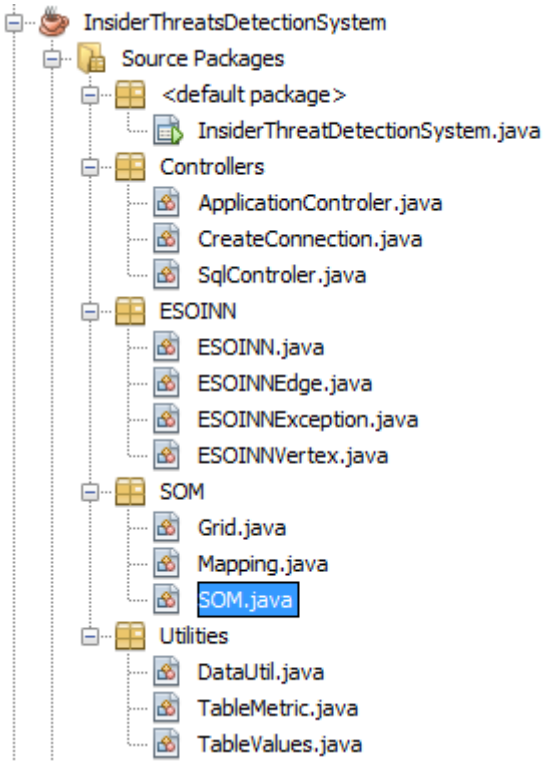


Εικόνα 17. Πίνακας usersessionsTraining

Ο βασικός ελεγκτής της εφαρμογής είναι η κλάση ApplicationControler. Η κλάση αυτή είναι υπεύθυνη για όλες τις λειτουργίες της εφαρμογής. Επικοινωνεί με την βάση

δεδομένων μέσω του SqlControler. Ο SqlControler χρησιμοποιεί την κλάση CreateConnection για να δημιουργήσει την σύνδεση με την βάση.

Η παρουσίαση είναι η κλάση InsiderThreatDetectionSystem. Στην κλάση αυτή υπάρχουν όλες οι λειτουργείες για να παρουσιαστούν τα δεδομένα στον χρήστη της εφαρμογής. Στην ***Εικόνα 18*** παρουσιάζονται όλες οι κλάσεις της εφαρμογής ITDS. Τα πακέτα ESOINN και SOM περιέχουν τις υλοποιήσεις των αλγορίθμων ESOINN και SOM αντίστοιχα.



Εικόνα 18. Διάρθρωση κλάσεων της εφαρμογής ITDS

Το πακέτο Utilities περιέχει όλες τις λειτουργίες οι οποίες, είτε βοηθάνε στην επεξεργασία των δεδομένων, είτε στην παρουσίαση τους. Αναλυτικότερα, η κλάση DataUtil παρέχει λειτουργίες για την επεξεργασία των δεδομένων πριν τροφοδοτήσουν τους αλγορίθμους. Μία από τις σημαντικότερες λειτουργίες που παρέχει είναι η κανονικοποίηση των δεδομένων.

Οι κλάσεις TableMetric και TableValues είναι βοηθητικές κλάσεις για την παρουσίαση των δεδομένων σε πίνακες. Συγκεκριμένα, η κλάση TableMetric δίνει τιμές στον πίνακα SOM Metrics ο οποίος βρίσκεται στην καρτέλα SOM. Η κλάση TableValues είναι

υπεύθυνη για τις αλλαγές των τιμών στους πίνακες Training Results και Testing Results, οι οποίοι βρίσκονται στις καρτέλες SOM και ESOINN.

Κεφάλαιο 5
Πειραματική Διαδικασία

Για να επικυρώσουμε την αποτελεσματικότητα του συστήματος που προτείναμε, αλλά και για να εξετάσουμε την απόδοση των αλγορίθμων SOM και ESOINN στην ανίχνευση των εσωτερικών απειλών, χρησιμοποιήθηκε το συνθετικό σύνολο δεδομένων εσωτερικών απειλών, το οποίο έχει δημιουργηθεί από το CERT (CERT Insider Threat Tools). Επίσης, στο κεφάλαιο αυτό αναλύουμε τις διαδικασίες που εφαρμόσαμε για την εξαγωγή χαρακτηριστικών από το σύνολο δεδομένων. Αυτά τα χαρακτηριστικά θα τροφοδοτήσουν τους αλγορίθμους SOM και ESOINN με σκοπό την εκπαίδευση και την δοκιμή τους.

Για την διεξαγωγή της πειραματικής διαδικασίας προσαρμόσαμε το σύστημά μας στο σύνολο δεδομένων του CERT. Στην βάση δεδομένων εισάγαμε τα αρχεία του συνόλου δεδομένων στους αντίστοιχους πίνακες. Ως βάση δεδομένων επιλέχθηκε η MySQL λόγω της δυνατότητας δωρεάν εγκατάστασής της. Η εκτέλεση της εφαρμογής ITDS που υλοποιήσαμε καθώς και η εγκατάσταση της MySQL έγινε σε μηχάνημα με λειτουργικό σύστημα Windows 10 64-bit. Τα βασικά τεχνικά χαρακτηριστικά του υπολογιστή ήταν τετραπύρηνος επεξεργαστής i5-3470 στα 3.20GHz και 8GB RAM.

5.1 Περιγραφή Δεδομένων

Τα σύνολα δεδομένων του CERT αποτελούνται από διάφορες εκδόσεις, η καθεμία με τα δικά της χαρακτηριστικά. Εμείς επιλέξαμε την έκδοση 4.2 η οποία περιέχει αρχεία δεδομένων που σχετίζονται με την καταγραφή της χρήσης αφαιρούμενων συσκευών, των συνδέσεων στους σταθμούς εργασίας, των ιστοσελίδων που επισκέφτηκαν οι εργαζόμενοι, των μηνυμάτων ηλεκτρονικού ταχυδρομείου καθώς και πληροφορίες με τα ψυχομετρικά αποτελέσματα των εργαζομένων. Επίσης, το σύνολο δεδομένων για

κάθε μήνα περιέχει αρχεία με όλους τους εργαζόμενους οι οποίοι εργάζονται στον οργανισμό μέσω του πρωτοκόλλου Lightweight Directory Access (LDAP).

Το σύνολο δεδομένων της έκδοσης 4.2 περιέχει τρία σενάρια εσωτερικής απειλής:

1. Ένας χρήστης ο οποίος δεν εργαζόταν σε ώρες εκτός ωραρίου εργασίας ή δεν χρησιμοποιούσε αφαιρούμενους δίσκους παλιότερα, αρχίζει να εισέρχεται στο πληροφοριακό σύστημα του οργανισμού και να χρησιμοποιεί αφαιρούμενους δίσκους για να ανεβάσει δεδομένα στο wikileaks.org.
2. Ένας υπάλληλος αρχίζει να ψάχνει σε ιστοσελίδες εύρεσης εργασίας και τελικά βρίσκει μία νέα θέση εργασίας σε ανταγωνίστρια εταιρία. Πριν φύγει από την τωρινή εταιρία, ο εργαζόμενος αρχίζει να χρησιμοποιεί μία φορητή συσκευή αποθήκευσης, με περισσότερη συχνότητα από ότι παλιότερα για να κλέψει δεδομένα και να τα χρησιμοποιήσει στην νέα του θέση.
3. Ένας διαχειριστής συστήματος γίνεται δυσαρεστημένος. Κατεβάζει έναν λογισμικό καταγραφής πληκτρολογήσεων (keylogger) και το εγκαθιστά στον υπολογιστή του προϊσταμένου του μέσω μίας φορητής συσκευής. Την επόμενη μέρα χρησιμοποιεί τις πληροφορίες που συλλέχθηκαν από το keylogger για να αποκτήσει πρόσβαση στον υπολογιστή του προϊσταμένου του. Αφού εισέλθει στο μηχάνημα στέλνει ένα μαζικό μήνυμα ηλεκτρονικού ταχυδρομείου στο προσωπικό του οργανισμού για να προκαλέσει πανικό.

Σε προηγούμενες εκδόσεις του συγκεκριμένου συνόλου δεδομένων, για παράδειγμα στην έκδοση 3.1 υπάρχει μόνο ένας χρήστης ο οποίος πραγματοποιεί το κάθε σενάριο. Στην έκδοση 4.2 υπάρχουν πολλαπλοί χρήστες που πραγματοποιούν το κάθε σενάριο. Αυτός ήταν και ο λόγος που επιλέξαμε την συγκεκριμένη έκδοση. Συγκεκριμένα ασχοληθήκαμε με τον εντοπισμό των εσωτερικών απειλών οι οποίες ικανοποιούν το σενάριο 1.

5.2 Εξαγωγή Χαρακτηριστικών

Μελετήσαμε τα δεδομένα για να εξάγουμε τα χαρακτηριστικά που πρέπει να επιλέξουμε ώστε να τροφοδοτήσουμε τους αλγορίθμους μας. Από τις πληροφορίες που υπάρχουν μέσα στο σύνολο δεδομένων του CERT για την συμπεριφορά των χρηστών,

επιλέξαμε ως συμπεριφορές οι οποίες υποδηλώνουν ενδείξεις εσωτερικής απειλής τα παρακάτω:

1. Χρήστες οι οποίοι συνδέονται στο πληροφοριακό σύστημα του οργανισμού σε ωράρια εκτός εργασίας και δεν έχουν προηγούμενη τέτοια συμπεριφορά.
2. Χρήστες οι οποίοι δεν έχουν προηγούμενο ιστορικό χρήσης αφαιρούμενων συσκευών.
3. Εργαζόμενοι οι οποίοι μεταφορτώνουν αρχεία σε ιστοσελίδες με υπηρεσίες διαμοιρασμού αρχείων.

Ο πρώτος παράγοντας που εξετάστηκε ήταν οι ώρες εκτός εργασίας. Δεν υπήρχαν πληροφορίες για το ποιες είναι αυτές οι ώρες. Για να καθορίσουμε τις ώρες εκτός εργασίας πραγματοποιήσαμε στατιστική ανάλυση για τους μήνες Ιούλιο έως και τον Αύγουστο. Σε αυτό το διάστημα 3 μηνών ξεχωρίσαμε τις ώρες σύνδεσης στο σύστημα από τις ώρες αποσύνδεσης για κάθε χρήστη. Εφαρμόσαμε μετρικές στατιστικής ανάλυσης, όπως επικρατούσα τιμή, μέση τιμή και τυπική απόκλιση.

Στο δείγμα που επιλέχθηκε υπήρχαν 88829 χρήστες οι οποίοι συνδέθηκαν στο πληροφοριακό σύστημα ενός οργανισμού και 72533 οι οποίοι αποσυνδεθήκαν (***Πίνακας 1***). Παρατηρήθηκε ότι η αναλογία σύνδεσης και αποσύνδεσης στο σύστημα δεν είναι ένα προς ένα. Συγκεκριμένα κάθε αποσύνδεση μπορεί να αντιστοιχίζεται και σε περισσότερες από μια συνδέσεις. Η διαφορά αυτή προκύπτει επειδή το κλείδωμα της οθόνης δεν καταγράφεται ως αποσύνδεση από το σύστημα, αλλά το ξεκλείδωμα της οθόνης καταγράφεται ως σύνδεση στο σύστημα.

Δραστηριότητα	Αριθμός χρηστών	Μέση Τιμή Ώρας	Τυπική Απόκλισης Ώρας
Σύνδεση στο σύστημα	88829	09:27:40	03:17:44
Αποσύνδεση από σύστημα	72533	16:50:06	03:32:45

Πίνακας 1. Αποτελέσματα μέσης τιμής και τυπικής απόκλισης ωρών σύνδεσης και αποσύνδεσης

Επίσης παρατηρήθηκε ότι η μέση τιμή σύνδεσης των χρηστών στο σύστημα ήταν γύρω στις 9:30 με απόκλιση περίπου 3 ωρών. Αντίστοιχα η μέση τιμή αποσύνδεσης από το σύστημα ήταν γύρω στις 17:00 με απόκλιση περίπου 3,5 ωρών. Και για την σύνδεση και

για την αποσύνδεση η απόκλιση ήταν αρκετά μεγάλη οπότε δεν μπορούσαμε να καταλήξουμε σε ένα σαφές συμπέρασμα. Συνεπώς προχωρήσαμε στην μέτρηση της επικρατούσας τιμής. Για να μπορέσουμε να έχουμε μία σχετικά καλή εικόνα του ωραρίου εργασίας μετρήσαμε τις δέκα επικρατέστερες ώρες σύνδεσης και αποσύνδεσης των χρηστών (***Πίνακας 2***, ***Πίνακας 3***).

Κατάταξη	Ώρα Σύνδεσης	Αριθμός Χρηστών
1	08:00:00	2372
2	08:01:00	1660
3	08:02:00	1610
4	07:45:00	1550
5	08:30:00	1311
6	08:03:00	1251
7	07:46:00	1157
8	07:47:00	1128
9	07:15:00	1036
10	07:48:00	993

Πίνακας 2. Οι δέκα επικρατέστερες ώρες σύνδεσης των χρηστών

Κατάταξη	Ώρα Αποσύνδεσης	Αριθμός Χρηστών
1	18:00:00	1195
2	17:00:00	1177
3	17:15:00	936
4	18:15:00	934
5	17:59:00	849
6	16:59:00	845
7	17:58:00	808
8	16:58:00	783

9	18:14:00	738
10	17:14:00	728

Πίνακας 3. Οι δέκα επικρατέστερες ώρες αποσύνδεσης των χρηστών

Παρατηρήσαμε ότι οι δέκα επικρατέστερες ώρες σύνδεσης στο σύστημα του οργανισμού ήταν μετά τις 7:00 και γύρω στις 8:00. Επίσης οι δέκα επικρατέστερες ώρες αποσύνδεσης ήταν μετά τις 17:00 και γύρω στις 18:00. Επίσης λάβαμε υπόψιν ότι το ωράριο εργασίας είναι μεγαλύτερο των 8 ωρών. Επιπλέον σε πολλούς οργανισμούς οι εργαζόμενοι έχουν την δυνατότητα να κάνουν διάλειμμα για μεσημεριανό γεύμα ή ακόμα και για κάποιο μικρό γεύμα όπως το δεκατιανό. Επομένως το ωράριο εργασίας μπορεί κάλλιστα να φτάσει και τις δέκα ώρες ή να τις ξεπεράσει.

Λαμβάνοντας υπόψιν τις παραπάνω στατιστικές μετρήσεις καθώς και το ωράριο εργασίας, καθορίσαμε ότι το μεγαλύτερο διάστημα που μπορεί να είναι συνδεμένος ένα χρήστης στο σύστημα είναι 11 ώρες και 13 λεπτά. Επίσης καταλήξαμε σε δύο πιθανές ώρες σύνδεσης και αποσύνδεσης στο σύστημα. Θεωρήσαμε ότι οι φυσιολογικές ώρες σύνδεσης στον υπολογιστή είναι, είτε μετά τις 7:00, είτε μετά τις 8:00. Οι φυσιολογικές ώρες αποσύνδεσης από το τερματικό του οργανισμού είναι, είτε πριν τις 18:00, είτε πριν τις 19:00. Οι ώρες αυτές συμφωνούν και με το ωράριο εργασίας του εξωτερικού.

Για να μπορέσουμε να καταγράψουμε τις δραστηριότητες του χρήστη όταν είναι συνδεμένος στο τερματικό του οργανισμού δημιουργήσαμε στη βάση δεδομένων τον πίνακα usersession, ο οποίος περιέχει πληροφορίες για το πότε ο χρήστης συνδέθηκε στο σύστημα και πότε αποσυνδέθηκε από αυτό. Η διαφορά του με τις πληροφορίες που υπάρχουν στο αρχείο καταγραφής σύνδεσης και αποσύνδεσης logon, είναι ότι ξεχωρίζει της ώρες ξεκλειδώματος οθόνης από τις πραγματικές ώρες εισόδου στο σύστημα. Στην εφαρμογή που υλοποιήσαμε χωρίσαμε τον πίνακα usersession στους πίνακες usersessionsTraining και usersessionTesting για πρακτικούς λόγους όπως προαναφέραμε.

Για να επιτύχουμε τον διαχωρισμό, σημαντικό ρόλο είχε το διάστημα εργασίας στο οποίο αναφερθήκαμε νωρίτερα, δηλαδή περισσότερο από 10 ώρες. Ειδικότερα, βρήκαμε τις ώρες σύνδεσης και αποσύνδεσης του κάθε χρήστη στο ίδιο υπολογιστή. Επίσης περιορίσαμε μέχρι 11 ώρες και 13 λεπτά το διάστημα σύνδεσης και

αποσύνδεσης. Ομαδοποιήσαμε αυτές τις ώρες κατά ημερομηνία και ώρα αποσύνδεσης για τον ίδιο χρήστη και το ίδιο μηχάνημα. Με αυτό τον τρόπο καταφέραμε κάθε αποσύνδεση να την αντιστοιχήσουμε σε πολλαπλές συνδέσεις.

Σαν αποτέλεσμα δημιουργήθηκαν οι λεγόμενες συνεδρίες χρήστη (user sessions). Το πρόβλημα όμως, όπως αναφέραμε ήταν ότι σε κάποιες συνεδρίες χρήστη είχαμε για την ίδια αποσύνδεση πολλαπλές συνδέσεις στον ίδιο υπολογιστή. Για να τις διαχωρίσουμε πήραμε για κάθε συνεδρία του ίδιου χρήστη στον ίδιο υπολογιστή και για την ίδια χρονική στιγμή αποσύνδεσης, την μικρότερη χρονική στιγμή σύνδεσης. Έτσι δημιουργήθηκε ο πίνακας usersession της βάσης δεδομένων ο οποίος δεν έχει πολλαπλές συνεδρίες εξαιτίας του ξεκλειδώματος οθόνης. Αυτό ήταν απαραίτητο για την πιο γρήγορη αναζήτηση των δραστηριοτήτων του χρήστη, όπως την εύρεση των ιστοσελίδων τις οποίες επισκέπτεται ή για την εύρεση του αριθμού των αφαιρούμενων συσκευών τις οποίες έχει συνδέσει στον υπολογιστή.

Ο πίνακας usersession αποτελεί τον βασικό πίνακα της μεθοδολογίας μας για την αναζήτηση οποιονδήποτε άλλων πληροφοριών σχετικά με κάποιον χρήστη, καθώς μας καθορίζει το χρονικό διάστημα αναζήτησης των δραστηριοτήτων του κατά την διάρκεια πρόσβασής του στις πληροφοριακές υποδομές ενός οργανισμού.

Έπειτα από την δημιουργία του πίνακα usersession ήταν αρκετά εύκολο να υπολογίσουμε για κάθε συνεδρία χρήστη, τον αριθμό σύνδεσης των αφαιρούμενων συσκευών και των ιστοσελίδων τις οποίες επισκέφτηκαν οι χρήστες του συστήματος. Αναλυτικότερα, για τον υπολογισμό του πλήθους χρήσης των αφαιρούμενων συσκευών ανά συνεδρία, ομαδοποιήσαμε τα δεδομένα του πίνακα devices κατά χρήστη και υπολογιστή. Επίσης από τις καταγραφές στον πίνακα devices επιλέξαμε μόνο τις συσκευές οι οποίες συνδέονται στο σύστημα και όχι αυτές που αποσυνδέονται.

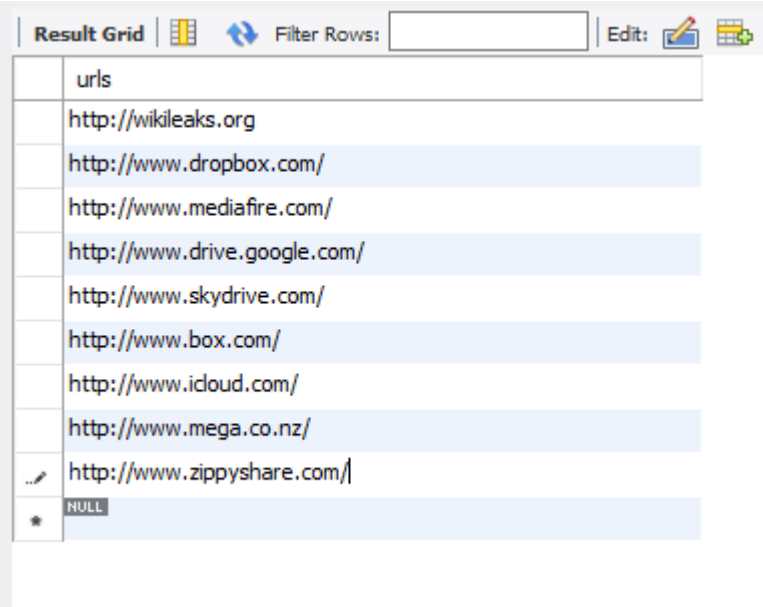
Στην συνέχεια, στον πίνακα devices καθορίσαμε ως χρονικό διάστημα αναζήτησης από την ημερομηνία και την ώρα σύνδεσης μέχρι την ημερομηνία και την ώρα αποσύνδεσης από το σύστημα, για κάθε συνεδρία χρήστη. Αυτές οι πληροφορίες υπάρχουν στον πίνακα usersession. Το αποτέλεσμα της παραπάνω διαδικασίας είναι το σύνολο των αφαιρούμενων συσκευών, τις οποίες χρησιμοποίησε κάθε χρήστης για τον ίδιο υπολογιστή στο χρονικό διάστημα κάθε συνεδρίας.

Γενικά κάθε άτομο έχει την συνήθεια, άλλοτε καλή και άλλοτε κακή, να «σερφάρει» στο διαδίκτυο. Χαρακτηριστικά παραδείγματα είναι τα μέσα κοινωνικής δικτύωσης (Facebook, Twitter) καθώς και ιστοσελίδες ενημέρωσης για θέματα πολιτικής, επικαιρότητας κτλ. Σε έναν οργανισμό υπάρχει κάποιο μικρό χρονικό διάστημα ελεύθερου χρόνου. Σε αυτόν τον περιορισμένο χρόνο υποθέσαμε ότι ένας εργαζόμενος επισκέπτεται κυρίως τις συνηθισμένες του ιστοσελίδες. Βασιζόμενοι στην παραπάνω υπόθεση, το επόμενο χαρακτηριστικό που υπολογίσαμε ήταν ο αριθμός των ιστοσελίδων τις οποίες επισκέφτηκαν οι χρήστες ανά συνεδρία.

Οι πληροφορίες για τις ιστοσελίδες τις οποίες επισκέφτηκαν οι χρήστης καταγράφονται στον πίνακα http της βάσης δεδομένων. Ομαδοποιήσαμε τα δεδομένα του πίνακα http κατά χρήστη και υπολογιστή, για να μπορέσουμε να τα συσχετίσουμε με τις συνεδρίες του πίνακα usersession. Επιπλέον καθορίσαμε ως χρονικό διάστημα αναζήτησης από την ημερομηνία και την ώρα σύνδεσης μέχρι την ημερομηνία και την ώρα αποσύνδεσης ανά συνεδρία χρήστη, χρησιμοποιώντας τις αντίστοιχες στήλες του πίνακα usersession.

Από την βάση δεδομένων ζητήσαμε το άθροισμα των γραμμών εφαρμόζοντας την παραπάνω διαδικασία. Σαν αποτέλεσμα, η βάση μας έδωσε το πλήθος των ιστοσελίδων τις οποίες επισκέφτηκε κάθε χρήστης στη διάρκεια μία συνεδρίας του στο πληροφοριακό σύστημα. Δεν ορίσαμε κάποιο κριτήριο για το ποιος θα πρέπει να είναι ο αριθμός των ιστοσελίδων ανά συνεδρία, ώστε να αποτελεί ανησυχητικό παράγοντα ή όχι. Το ίδιο έγινε και για τον αριθμό των αφαιρούμενων συσκευών. Θεωρήσαμε ότι με την κανονικοποίηση (normalization) των δεδομένων δεν θα χρειαστεί κάποιο κριτήριο.

Το τελευταίο χαρακτηριστικό το οποίο έπρεπε να εντοπίσουμε ήταν ποιοι χρήστες επισκέπτονταν ιστοσελίδες, οι οποίες προσφέρουν υπηρεσίες διαμοιρασμού αρχείων (EBizMBA 2016). Για το συγκεκριμένο σύνολο δεδομένων η μόνη ιστοσελίδα η οποία προσφέρει τέτοιες υπηρεσίες είναι η https://wikileaks.org/. Ο πίνακας badurls έχει δημιουργηθεί αποκλειστικά για αυτού του τύπου ιστοσελίδες. Επομένως, καταχωρήσαμε την συγκεκριμένη ιστοσελίδα στον πίνακα της βάσης δεδομένων μαζί με άλλες ιστοσελίδες διαμοιρασμού αρχείων (***Εικόνα 19***).



Εικόνα 19. Πίνακας badurls

Αρχικά ομαδοποιήσαμε τα δεδομένα του πίνακα http κατά χρήστη και υπολογιστή. Επίσης καθορίσαμε το χρονικό διάστημα κάθε αναζήτησης στην διάρκεια κάθε συνεδρίας, η οποία υπάρχει στον πίνακα usersession. Είναι ακριβώς η ίδια διαδικασία όπως πράξαμε και στην εύρεση των ιστοσελίδων τις οποίες επισκέφτηκαν οι χρήστες στην διάρκεια μίας συνεδρίας με μία μικρή διαφορά. Σε κάθε αναζήτηση για κάθε ιστοσελίδα του πίνακα http, η οποία ανήκει στην εκάστοτε συνεδρία, γίνεται σύγκριση με τις ιστοσελίδες τις οποίες περιέχει ο πίνακας badurls. Αν η ιστοσελίδα υπάρχει στον πίνακα badurls τότε αυξάνεται ο μετρητής των ιστοσελίδων με υπηρεσίες διαμοιρασμού αρχείων κατά ένα για τη συγκεκριμένη συνεδρία.

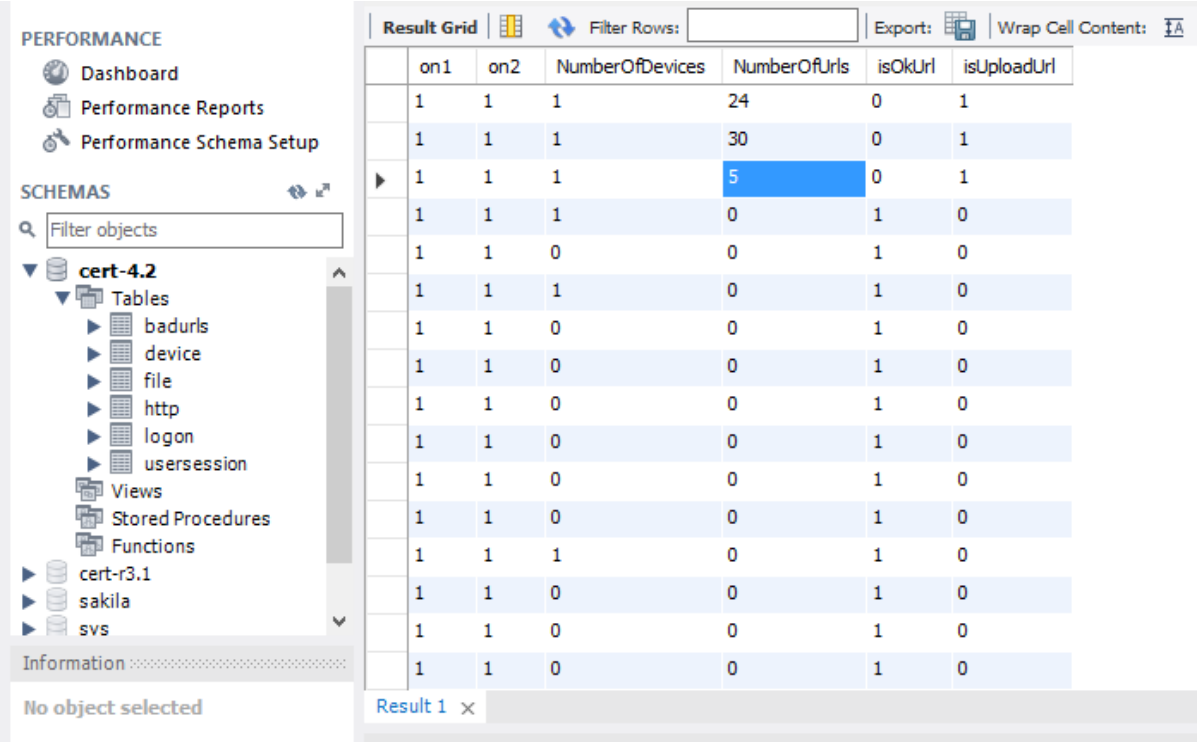
Όλα τα χαρακτηριστικά τα οποία αναλύθηκαν προηγουμένως τα συγκεντρώσαμε σε ένα μεγάλο ερώτημα προς την βάση δεδομένων. Το ερώτημα αντιστοιχίζει κάθε γραμμή του πίνακα usersession με τα αποτελέσματα των επιμέρους ερωτημάτων για κάθε συνεδρία. Συμπερασματικά προκύπτει ο πίνακας χαρακτηριστικών ο οποίος έχει τα ακόλουθα χαρακτηριστικά :

1. Σύνδεση στο σύστημα πριν τις 8:00 ή μετά τις 18:00 (on2). Όταν οι χρήστες εισέρχονται στο σύστημα πριν τις 8:00 ή μετά τις 18:00 θεωρείται μία ένδειξη κακόβουλης δραστηριότητας. Το χαρακτηριστικό παίρνει την τιμή 1 όταν ισχύει αλλιώς 0.
2. Σύνδεση στο σύστημα πριν τις 7:00 ή μετά τις 19:00 (on1). Όταν οι χρήστες του συστήματος συνδέονται πριν τις 7:00 ή μετά τις 19:00 θεωρείται ένας

ισχυρότερος παράγοντας κακόβουλης δραστηριότητας από ότι το χαρακτηριστικό on2. Ομοίως παίρνει την τιμή 1 αν ικανοποιείται αλλιώς 0.

3. Πλήθος συνδεμένων συσκευών (NumberOfDevices). Μετράει τον αριθμό των συσκευών τις οποίες έχει χρησιμοποιήσει ο χρήστης στο διάστημα μίας συνεδρίας.
4. Πλήθος ιστοσελίδων (NumberOfUrls). Μετράει το πλήθος των ιστοσελίδων τις οποίες επιστέφτηκε ο χρήστης κατά την διάρκεια μίας συνεδρίας.
5. «Καλές» ιστοσελίδες (isOkUrl). Δείχνει αν οι ιστοσελίδες τις οποίες επισκέφτηκε ο χρήστης σε μία συνεδρία δεν ανήκουν στις ιστοσελίδες του πίνακα badurls της βάσης δεδομένων. Η τιμή της είναι ίση με 1 αν ισχύει το παραπάνω κριτήριο αλλιώς 0.
6. Ιστοσελίδες διαμοιρασμού αρχείων (isUploadUrl). Δείχνει αν ο χρήστης κατά την διάρκεια μίας συνεδρίας επισκέφτηκε ιστοσελίδες διαμοιρασμού αρχείων. Η τιμή της είναι 1 αν ο χρήστης έχει επισκεφτεί τουλάχιστον μία ιστοσελίδα διαμοιρασμού αρχείων αλλιώς 0.

Στην ***Εικόνα 20*** παρουσιάζεται ένα παράδειγμα του πίνακα χαρακτηριστικών το οποίο θα χρησιμοποιηθεί για να την τροφοδοσία των αλγορίθμων SOM και ESOINN. Ο πίνακας χαρακτηριστικών έχει εξαχθεί από τα δεδομένα του χρονικού διαστήματος 07-07-2010 έως 15-07-2010 χρησιμοποιώντας το εργαλείου MySQL Workbench, το οποίο προσφέρει η βάση δεδομένων MySQL. Κάθε γραμμή του πίνακα αντιπροσωπεύει μία συνεδρία χρήστη. Κάθε στήλη του πίνακα αντιπροσωπεύει τα χαρακτηριστικά τα οποία αναλύσαμε παραπάνω. Σε όλες τις συνεδρίες οι χρήστες έχουν συνδεθεί στο σύστημα, είτε πριν τις 7:00, είτε μετά τις 19:00 (on1=1). Επίσης όλοι οι χρήστες έχουν συνδεθεί στον υπολογιστή, είτε πριν τις 8:00, είτε μετά τις 18:00 (on2=1).



on1	on2	NumberOfDevices	NumberOfUrls	isOkUrl	isUploadUrl
1	1	1	24	0	1
1	1	1	30	0	1
1	1	1	5	0	1
1	1	1	0	1	0
1	1	0	0	1	0
1	1	1	0	1	0
1	1	0	0	1	0
1	1	0	0	1	0
1	1	0	0	1	0
1	1	0	0	1	0
1	1	0	0	1	0
1	1	0	0	1	0
1	1	1	0	1	0
1	1	0	0	1	0
1	1	0	0	1	0
1	1	0	0	1	0

Εικόνα 20. Παράδειγμα Πίνακα Χαρακτηριστικών

Οι τρεις πρώτες γραμμές του πίνακα δείχνουν ότι και στις τρεις αυτές συνεδρίες ένας χρήστης επισκέφτηκε τουλάχιστον μία ιστοσελίδα η οποία παρέχει υπηρεσίες διαμοιρασμού αρχείων (isUploadUrl=1). Επίσης οι χρήστες έχουν χρησιμοποιήσει ακριβώς μία αφαιρούμενη συσκευή (NumOfDevices=1). Στην πρώτη συνεδρία κάποιος χρήστης έχει επισκεφτεί 24 ιστοσελίδες, στην δεύτερη συνεδρία 30 και στην τρίτη συνεδρία 5 ιστοσελίδες (τιμή του χαρακτηριστικού NumberOfUrls). Οι υπόλοιπες γραμμές του πίνακα περιέχουν συνεδρίες στις οποίες ο χρήστης δεν έχει επισκεφτεί ιστοσελίδες διαμοιρασμού αρχείων (isOkUrl=1).

5.3 Κανονικοποίηση Δεδομένων

Η τελευταία διαδικασία πριν την εισαγωγή των δεδομένων στους αλγορίθμους SOM και ESOINN είναι η κανονικοποίηση (normalization) των δεδομένων. Κανονικοποίηση με την μαθηματική έννοια, είναι ένας κοινός τύπος μετασχηματισμού των μεταβλητών ενός διανύσματος. Ο στόχος της κανονικοποίησης είναι να δώσει σε ένα σύνολο τιμών μία συγκεκριμένη ιδιότητα. Για παράδειγμα αν $\bar{x}$ είναι η μέση τιμή και s η τυπική απόκλιση των τιμών ενός διανύσματος τότε ο μετασχηματισμός:

$$x' = \frac{x - \bar{x}}{s},$$

δημιουργεί μία νέα μεταβλητή x', η οποία έχει μέση τιμή 0 και τυπική απόκλιση 1.

Αν πρόκειται να συνδυαστούν διαφορετικές μεταβλητές με κάποιο τρόπο, τότε ένας τέτοιος μετασχηματισμός είναι απαραίτητος για να αποφύγουμε να μην επικρατήσει στα αποτελέσματα των υπολογισμών μία μεταβλητή με μεγάλες τιμές, σε σχέση με τις τιμές των άλλων μεταβλητών. Για παράδειγμα, έστω ότι σε ένα σύνολο δεδομένων επιλέξουμε να συγκρίνουμε ανθρώπους με βάση τις μεταβλητές ηλικία και μισθός. Οι μεταβλητές ηλικία και μισθός έχουν μεγάλη διαφορά τιμών. Η ηλικία συνήθως είναι μικρότερη του 100, ενώ ο μισθός μπορεί να είναι μέχρι και χιλιάδες ευρώ. Αν αυτές οι διαφορές στο εύρος τιμών της ηλικίας και του μισθού δεν ληφθούν υπόψιν, τότε στην σύγκριση των ανθρώπων θα επικρατήσουν οι διαφορές των μισθών. Ειδικότερα, αν η ομοιότητα ή ανομοιότητα δύο ανθρώπων μετριέται χρησιμοποιώντας μέτρα ομοιότητας ή ανομοιότητας όπως η Ευκλείδεια απόσταση, τότε οι τιμές του μισθού θα επικρατήσουν των τιμών της ηλικίας.

Δεν υπάρχει ένας γενικός κανόνας για την κανονικοποίηση των συνόλων δεδομένων. Για αυτό το λόγο η επιλογή ενός συγκεκριμένου κανόνα κανονικοποίησης βρίσκεται στην διακριτική ευχέρεια του χρήστη (Visalakshi & Thangavel 2009). Υπάρχουν αρκετές μέθοδοι για την κανονικοποίηση των δεδομένων όπως κανονικοποίηση ελαχίστου-μεγίστου (min-max normalization) και η κανονικοποίηση με το Z-score (standardization). Η κανονικοποίηση min-max πραγματοποιεί μία γραμμική μετατροπή των αρχικών δεδομένων. Έστω min_x και max_x η ελάχιστη και η μέγιστη τιμή των τιμών ενός διανύσματος X αντίστοιχα. Η κανονικοποίηση min-max μετατρέπει τις τιμές του διανύσματος X στο εύρος (0,1) με τον τύπο:

$$x' = \frac{x - min_x}{max_x - min_x}$$

Η παράσταση $max_x - min_x$ ονομάζεται και εύρος τιμών του διανύσματος X.

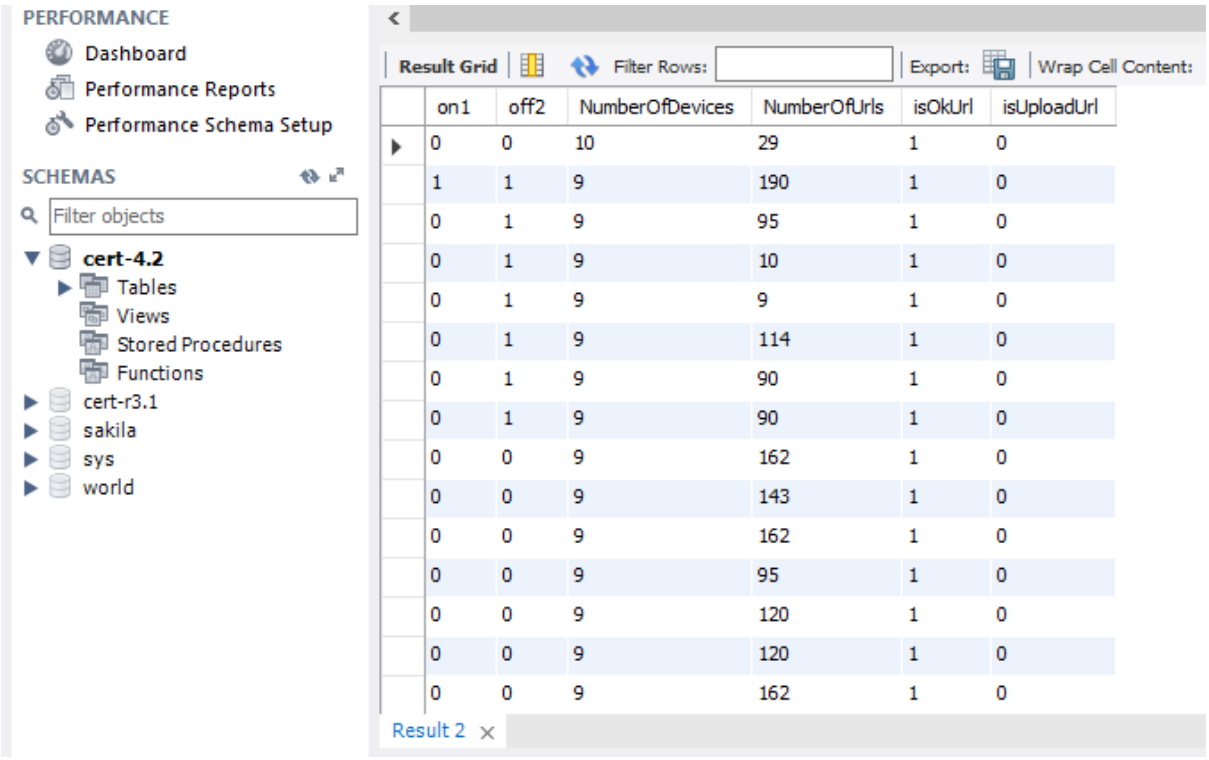
Στην κανονικοποίηση με το Z-score οι τιμές του διανύσματος X κανονικοποιούνται με βάση την μέση τιμή και την τυπική απόκλιση των τιμών του X. Συγκεκριμένα, οι τιμές μετατρέπονται με τέτοιο τρόπο ώστε η μέση τιμή να είναι 0 και η τυπική απόκλιση 1 με τον τύπο:

$$x' = \frac{x - \bar{x}}{s}$$

Η μεταβλητή $\bar{x}$ είναι η μέση τιμή και s η τυπική απόκλιση των τιμών του X.

Η κανονικοποίηση των δεδομένων είναι ζωτικής σημασίας επειδή ο αλγόριθμος SOM χρησιμοποιεί την ευκλείδεια απόσταση για να μετρήσει τις αποστάσεις μεταξύ των διανυσμάτων τα οποία συγκρίνει (Vesanto et al. 1999). Για να κανονικοποιήσουμε τα δεδομένα τα οποία προέκυψαν από τον πίνακα χαρακτηριστικών χρησιμοποιήσαμε την κανονικοποίηση με το Z-score. Ο λόγος που επιλέξαμε να κανονικοποιήσουμε τα δεδομένα ήταν οι μεγάλες διαφορές των τιμών των μεταβλητών NumberOfDevices και NumberOfUrls σε σύγκριση με τις υπόλοιπες τέσσερις μεταβλητές.

Όπως αναφέραμε στο υποκεφάλαιο 5.2 η μεταβλητή NumberOfDevices μετράει το πλήθος των αφαιρούμενων συσκευών οι οποίες συνδέθηκαν στον υπολογιστή στην διάρκεια μίας συνεδρίας. Η μεταβλητή NumberOfUrls μετράει το πλήθος των ιστοσελίδων τις οποίες επισκέφτηκε ο χρήστης στην διάρκεια μία συνεδρίας. Και στις δύο περιπτώσεις το πλήθος μπορεί να είναι αρκετά μεγάλο σε σχέση με τις τιμές των άλλων μεταβλητών ή ακόμα και μεταξύ τους.



on1	off2	NumberOfDevices	NumberOfUrls	isOkUrl	isUploadUrl
0	0	10	29	1	0
1	1	9	190	1	0
0	1	9	95	1	0
0	1	9	10	1	0
0	1	9	9	1	0
0	1	9	114	1	0
0	1	9	90	1	0
0	1	9	90	1	0
0	0	9	162	1	0
0	0	9	143	1	0
0	0	9	162	1	0
0	0	9	95	1	0
0	0	9	120	1	0
0	0	9	120	1	0
0	0	9	162	1	0

Εικόνα 21. Παράδειγμα πίνακα χαρακτηριστικών το οποίο δείχνει την μεγάλες διαφορές των τιμών των μεταβλητών**.**

Χαρακτηριστικό παράδειγμα είναι η ***Εικόνα 21***, στην οποία παρουσιάζονται δεδομένα για το χρονικό διάστημα από 07-07-2010 έως 15-07-2010. Σε όλες τις γραμμές του

πίνακα χαρακτηριστικών παρατηρούμε ότι το πλήθος των ιστοσελίδων και το πλήθος των αφαιρούμενων συσκευών διαφέρει αρκετά από όλα τα άλλα χαρακτηριστικά. Αυτό συμβαίνει επειδή τα υπόλοιπα χαρακτηριστικά είναι κατηγορικές μεταβλητές του τύπου ναι ή όχι, ενώ η μεταβλητές NumberOfDevices και NumberOfUrls είναι συνεχείς.

Επίσης στην γραμμή 2 παρατηρούμε ότι ο χρήστης έχει επισκεφτεί 190 ιστοσελίδες ενώ έχει συνδέσει αφαιρούμενη συσκευή μόλις εννέα φορές. Η διαφορά αυτή είναι τεράστια και σίγουρα θα επηρεάσει τον υπολογισμό της ευκλείδειας απόστασης. Συγκεκριμένα, ο αριθμός των ιστοσελίδων τις οποίες έχει επισκεφτεί ο χρήστης, θα γίνει ο κύριος παράγοντας για την σύγκριση της συγκεκριμένης συνεδρίας με άλλες συνεδρίες χρηστών. Βασιζόμενοι σε αυτή την παρατήρηση τα άλλα χαρακτηριστικά δεν θα μπορέσουν να συμβάλουν καθόλου στις συγκρίσεις.

Επομένως, πρέπει να φέρουμε τις τιμές όλων των μεταβλητών σε μία «ισορροπία» ώστε σε μία σύγκριση να μπορούν όλες να συμβάλλουν με το ίδιο τρόπο. Η κανονικοποίηση με το Z-score προσφέρει αυτή την δυνατότητα μετατρέποντας τις τιμές των δεδομένων με τέτοιο τρόπο, ώστε η μέση τιμής της κάθε μεταβλητής να είναι 0 και η τυπική απόκλιση 1.

5.4 Εκπαίδευση αλγορίθμων

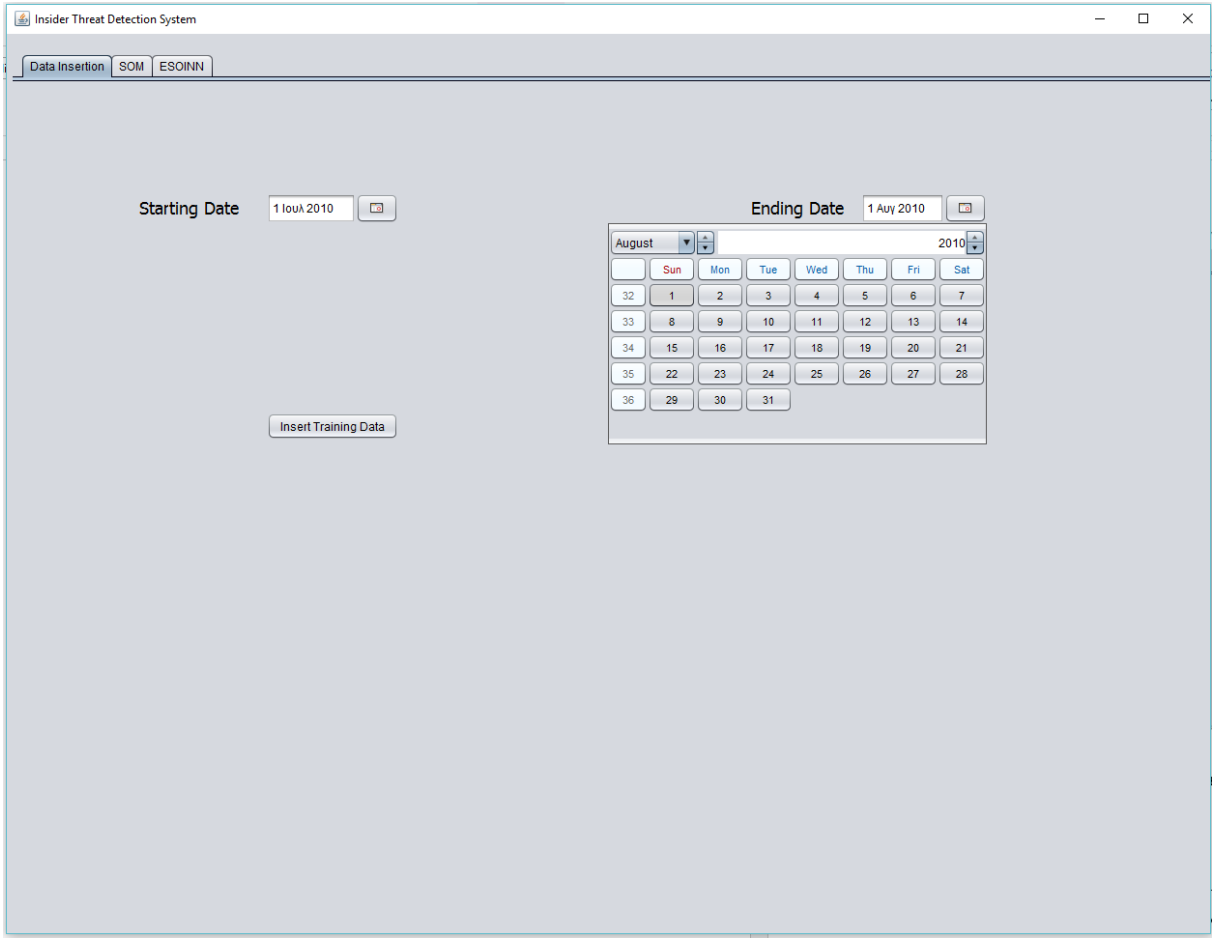
Για την εκπαίδευση του αλγόριθμου SOM επιλέχθηκε δισδιάστατο πλέγμα με εξαγωνική τοπολογία. Σε κάθε δοκιμή που πραγματοποιήθηκε εξετάστηκαν διάφορες διαστάσεις του πλέγματος. Σκοπός ήταν να βρούμε ποιες πρέπει να είναι οι διαστάσεις του πλέγματος ώστε όλοι οι κόμβοι να έχουν τιμές και να μην είναι κενοί. Αφού καθορίσαμε τις διαστάσεις του πλέγματος προχωρήσαμε στην επιλογή των υπόλοιπων παραμέτρων του αλγορίθμου.

Ο αλγόριθμος ESOINN δεν έχει πλέγμα όπως ο SOM. Για την δημιουργία του νευρωνικού του δικτύου χρησιμοποιεί γράφους. Έτσι γίνεται η αντικατάσταση ενός σταθερού πλέγματος ή πιο τεχνικά ενός πίνακα από νευρώνες, με ένα γράφο ο οποίος έχει την δυνατότητα να αυξάνεται και να μειώνεται. Αυτό είναι και το μεγαλύτερο πλεονέκτημα του ESOINN σε σχέση με τον SOM, ότι δηλαδή δεν χρειάζεται να

καθοριστούν οι διαστάσεις του νευρωνικού του δικτύου καθώς αυξάνεται όταν χρειάζεται.

5.4.1 Εκπαίδευση για δεδομένα ενός μήνα

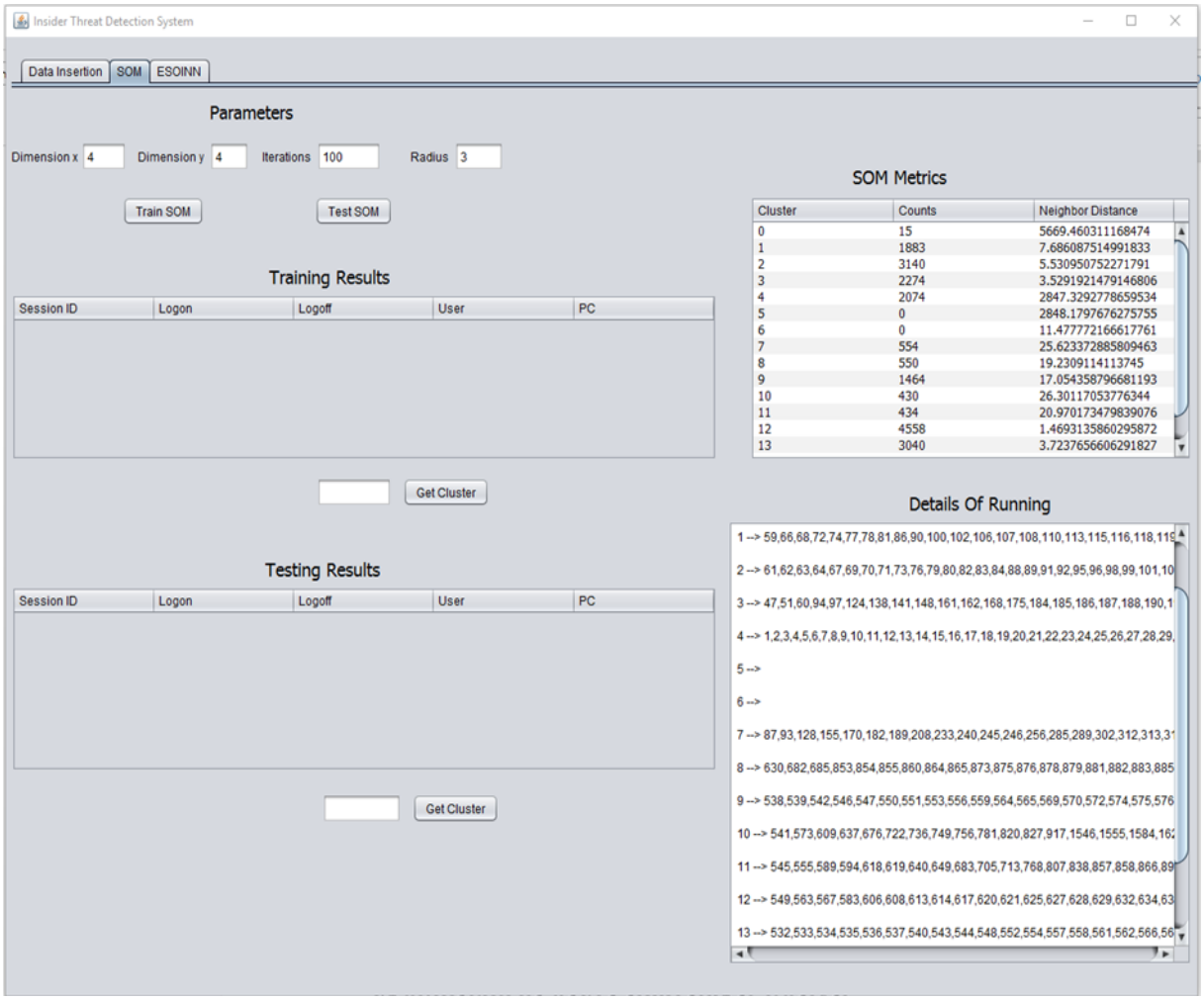
Επιλέξαμε για δείγμα εκπαίδευσης τα δεδομένα του μήνα Ιουλίου για το έτος 2010 (***Εικόνα 22***). Τα δεδομένα του μήνα Ιουλίου περιέχουν 15 συνεδρίες εσωτερικών απειλών. Κάναμε εισαγωγή των δεδομένων από την βάση για να προχωρήσουμε στην διαδικασία εκπαίδευσης των αλγορίθμων.



Εικόνα 22. Δεδομένα εκπαίδευσης μήνα Ιουλίου

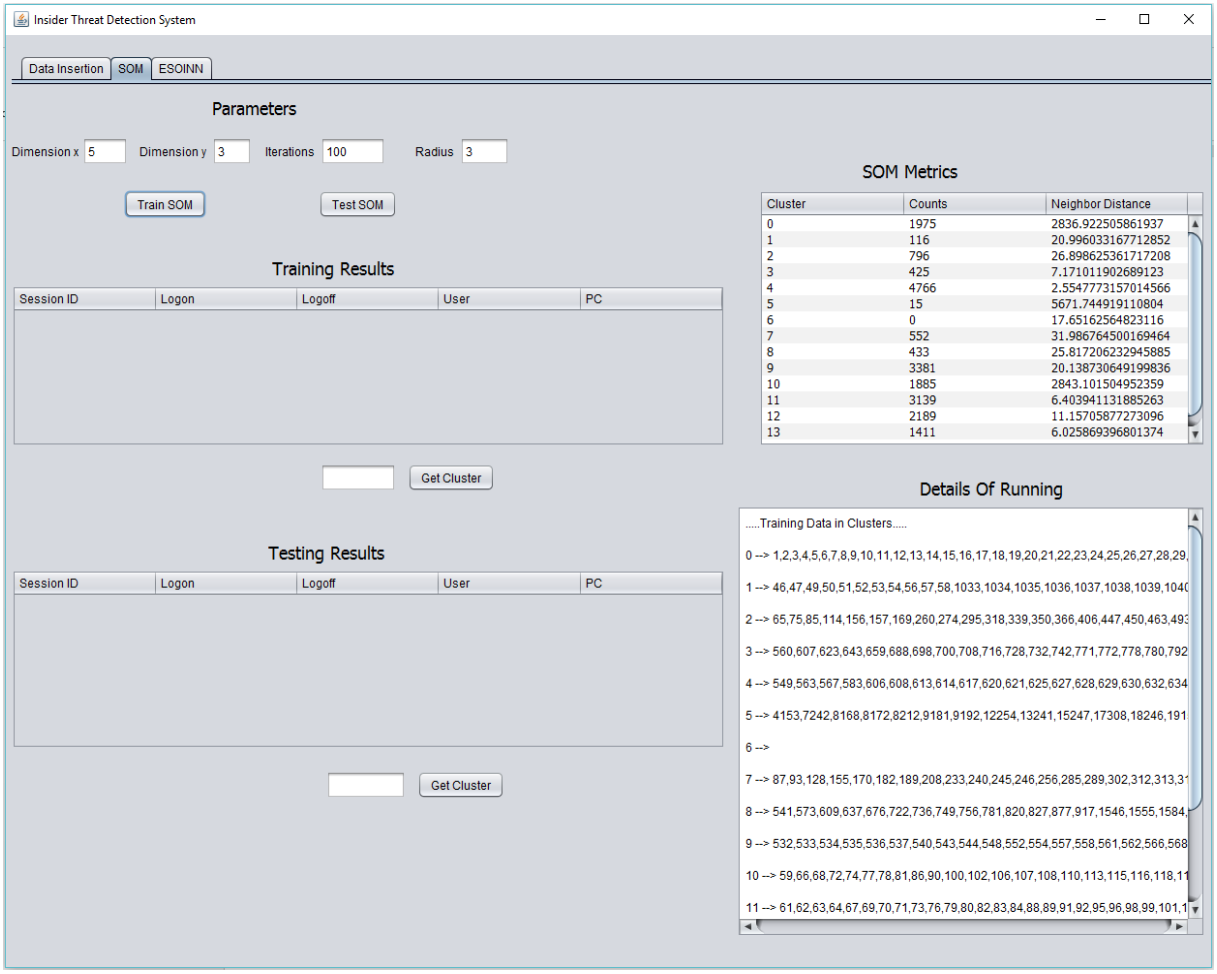
Ξεκινήσαμε την εκπαίδευση του αλγορίθμου SOM με την χρήση πλέγματος διάστασης 4x4 (***Εικόνα 23***). Επιλέξαμε ως 100 το σύνολο επαναλήψεων και ως 3 την ακτίνα γειτονιάς των νευρώνων στο πλέγμα. Στον πίνακα του τμήματος SOM Metrics φαίνεται ότι οι κόμβοι 5 και 6 είναι κενοί καθώς έχουν άθροισμα 0. Το ίδιο φαίνεται και στο τμήμα Details of Running καθώς δεν υπάρχει καμία συνεδρία η οποία να αντιστοιχίζεται στους κόμβους 5 και 6. Το ότι υπάρχουν κενοί κόμβοι υποδηλώνει, είτε ότι οι διστάσεις

του πλέγματος πρέπει να μειωθούν, ή ότι η ακτίνα γειτονίας πρέπει να προσαρμοστεί κατάλληλα. Στην συγκεκριμένη περίπτωση θεωρούμε ότι φταίνε οι διαστάσεις του πλέγματος γιατί οι κενοί κόμβοι είναι πάνω από ένας. Αλλαγές στην ακτίνα γειτονιάς επιφέρουν πολύ μικρές αλλαγές το πλέγμα.



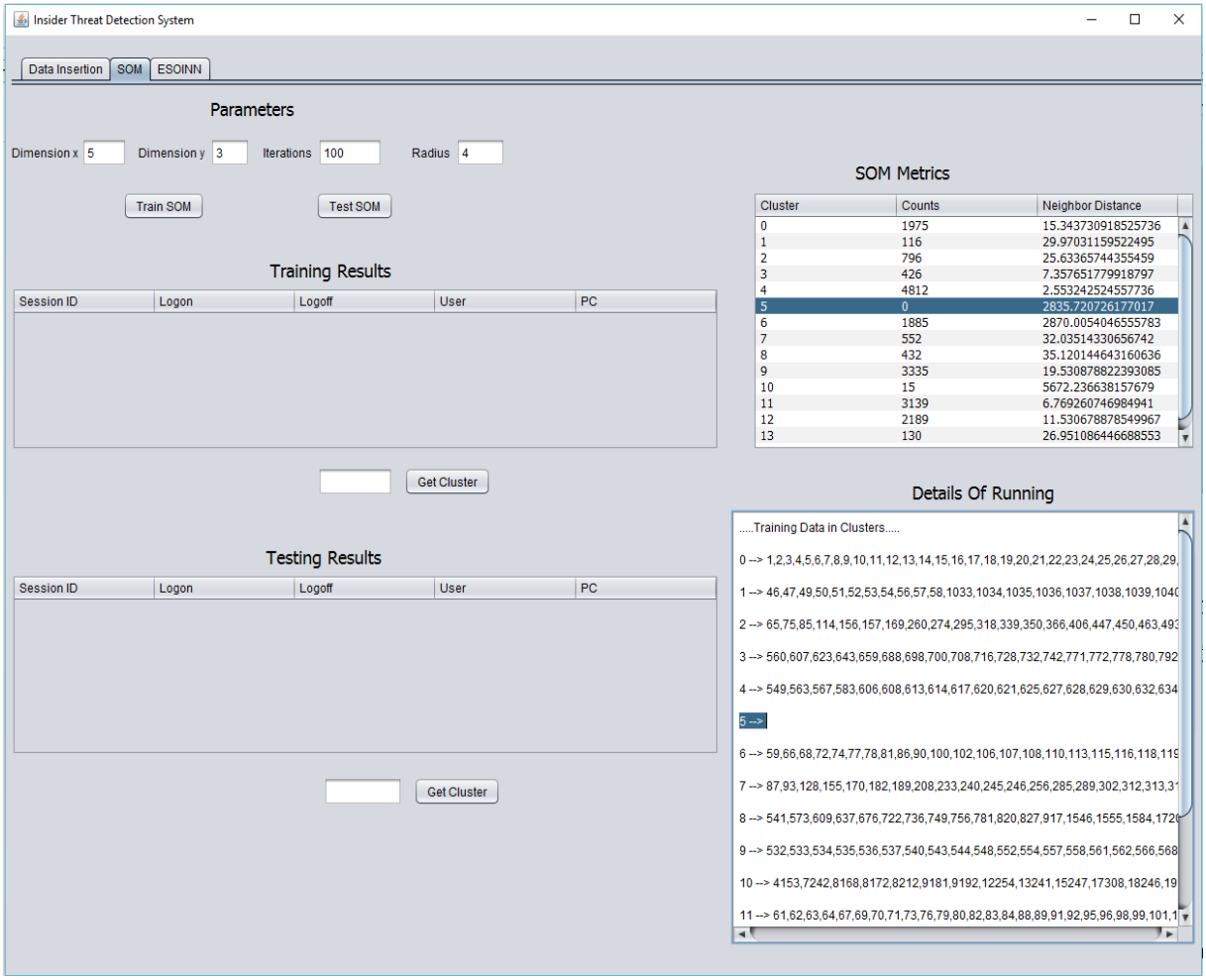
Εικόνα 23. Εκπαίδευση SOM μήνα Ιουλίου για πλέγμα 4x4 του SOM

Επιλέγουμε σαν νέες διαστάσεις του πλέγματος τις 5x3 (***Εικόνα 24***). Στην ουσία μειώνουμε τους νευρώνες κατά ένα. Αντί για 16 νευρώνες που είχαμε πριν τώρα έχουμε 15, διατηρούμε τον αριθμό των επαναλήψεων στις 100 και κρατάμε ίδια την ακτίνα γειτονιάς στο 3. Από τα αποτελέσματα της εκπαίδευσης του SOM παρατηρούμε ότι ο κόμβος 6 είναι κενός. Επειδή έχουμε μόνο ένα κόμβο κενό επιλέγουμε να εκπαιδεύσουμε τον αλγόριθμο με ίδια διάσταση πλέγματος αλλά αυξάνοντας την ακτίνα γειτονιάς στο 4.



Εικόνα 24. Εκπαίδευση SOM με δεδομένα του μήνα Ιουλίου σε πλέγμα 5x3 και ακτίνα γειτονιάς 3

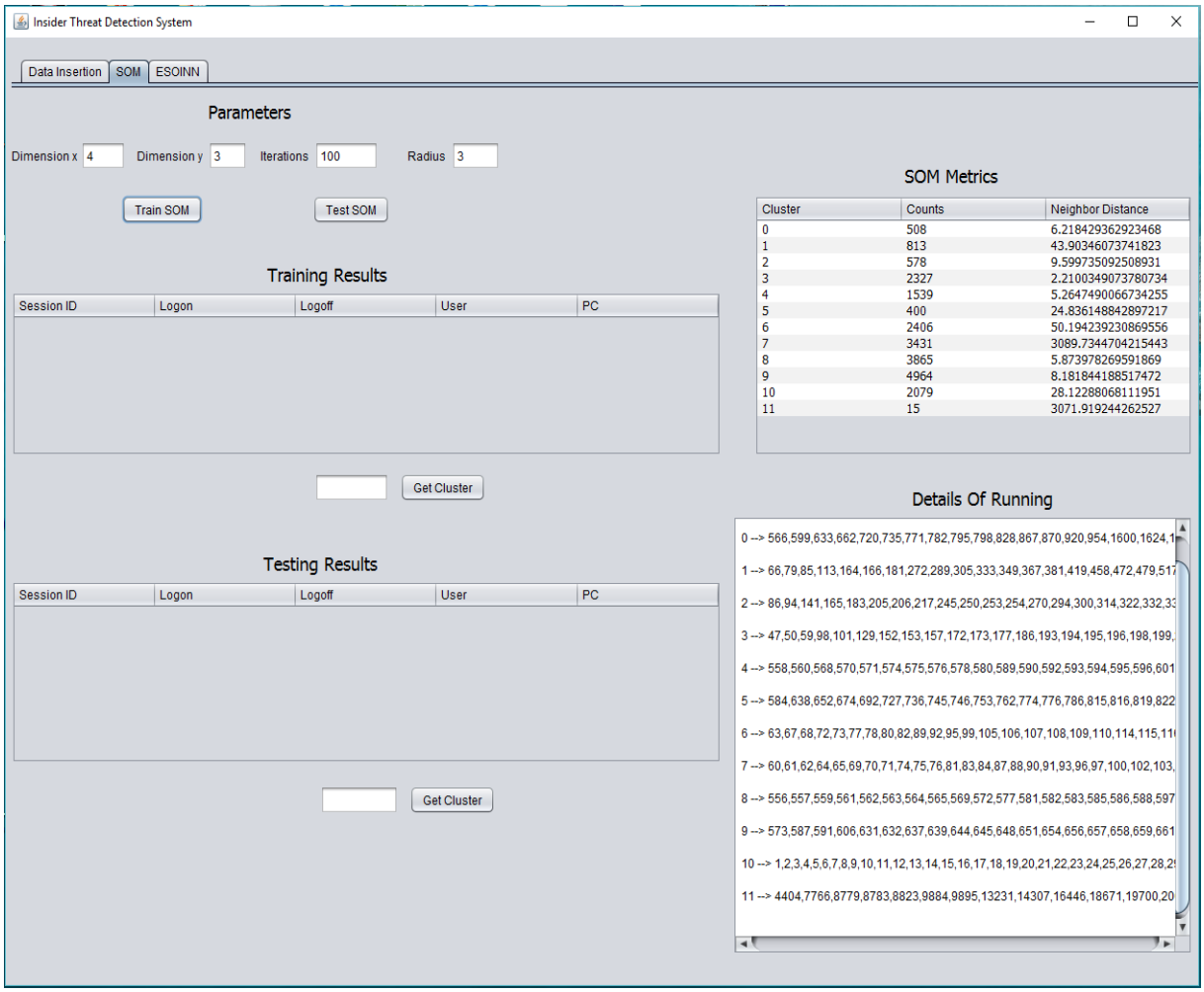
Η εκπαίδευση του SOM διατηρώντας τις ίδιες διαστάσεις στο πλέγμα και αυξάνοντας την ακτίνα γειτονιάς κατά ένα δεν βελτιώνει καθόλου την εκπαίδευση του (***Εικόνα 25***). Συγκεκριμένα παρατηρούμε ότι πάλι υπάρχει ένας κενός κόμβος αλλά αυτή την φορά είναι ο κόμβος 5. Είδαμε ότι με την μείωση των διαστάσεων από 4x4 σε 5x3 οι κόμβου που είναι κενοί μειώνονται από τους 2 στον 1.



Εικόνα 25. Εκπαίδευση SOM για τον μήνα Ιούλιο σε πλέγμα 5x3 και ακτίνα γειτονιάς 4

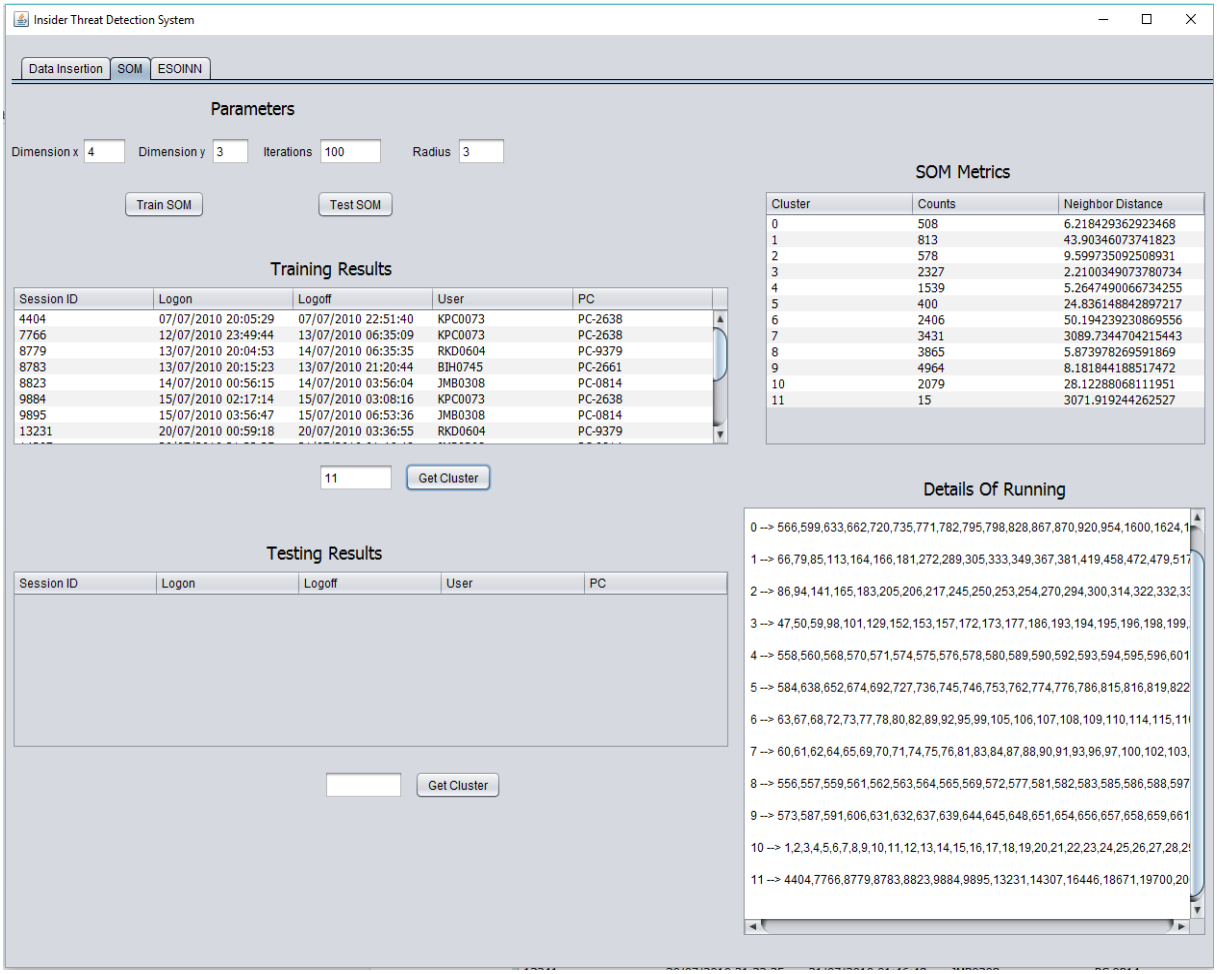
Επιλέγουμε ως νέα διάσταση του πλέγματος την 4x3 και έτσι οι κόμβοι στο πλέγμα γίνονται 12 (***Εικόνα 26***). Διατηρώντας τον ίδιο αριθμό επαναλήψεων και επιλέγοντας ακτίνα γειτονίας 3 εκπαιδεύουμε τον αλγόριθμο. Από τα αποτελέσματα στον πίνακα SOM Metrics, παρατηρούμε ότι δεν υπάρχει κανένας κόμβος ο οποίος να είναι κενός σε αντίθεση με τις προηγούμενες διαδικασίες εκπαίδευσης. Επίσης παρατηρούμε ότι οι κόμβοι 7 και 11 έχουν τη μεγαλύτερη απόσταση από τους γειτονικούς τους κόμβους (Neighbor Distance = 3089.73 και Neighbor Distance = 3071.92 αντίστοιχα).

Οι αποστάσεις αυτές δηλώνουν ότι οι κόμβοι 7 και 11 είναι αρκετά ανόμοιοι από τους υπόλοιπους γειτονικούς τους κόμβους και αποτελούν μια άλλη κατηγορία σε σχέση με τα υπόλοιπα δεδομένα. Επιπλέον, παρατηρούμε ότι το σύνολο των συνεδριών οι οποίες ταξινομήθηκαν στον κόμβο 11, συμπίπτει με τον αριθμό των εσωτερικών απειλών που υπάρχουν στον μήνα Ιούλιο (count = 15). Όλα αυτά τα στοιχεία μας οδηγούν στην εικασία ότι πιθανόν ο κόμβος 11 να είναι η συστάδα η οποία περιέχει και τις 15 συνεδρίες εσωτερικών απειλών που υπάρχουν στον μήνα Ιούλιο.

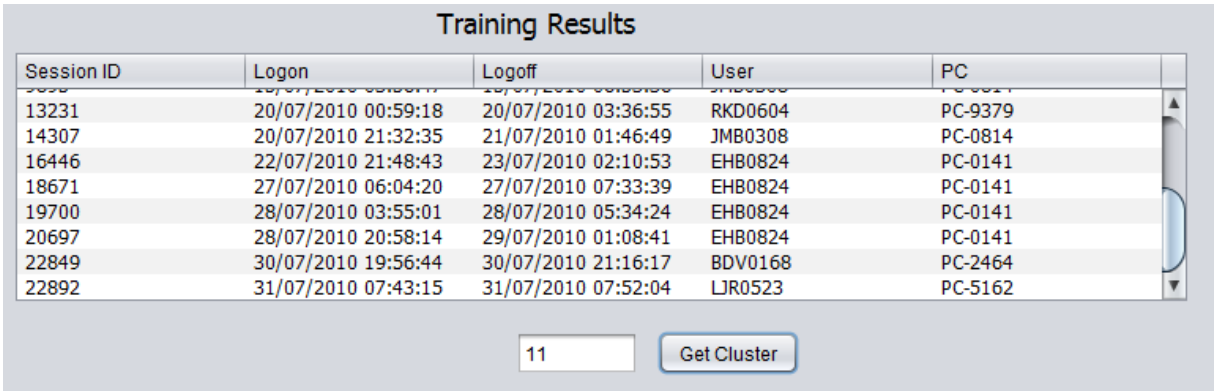


Εικόνα 26. Εκπαίδευση SOM για τον μήνα Ιούλιο με πλέγμα 4x3 και ακτίνα γειτονιάς 3

Για να επιβεβαιώσουμε την εικασία μας, ζητάμε από τη εφαρμογή να μας εμφανίσει τις συνεδρίες χρήστη οι οποίες ανήκουν στην συστάδα 11 (***Εικόνα 28***, ***Εικόνα 28***). Πράγματι, στον πίνακα Training Results όλες οι συνεδρίες είναι οι συνεδρίες με τις εσωτερικές απειλές του μήνα Ιουλίου. Άρα, για τον μήνα Ιούλιο και για δείγμα 15 εσωτερικών απειλών, ο αλγόριθμος SOM χρειάστηκε πλέγμα διαστάσεων 4x3 και ακτίνα γειτονιάς 3, ώστε να εκπαιδευτεί σωστά και να ταξινομήσει όλες τις απειλές στην ίδια συστάδα.



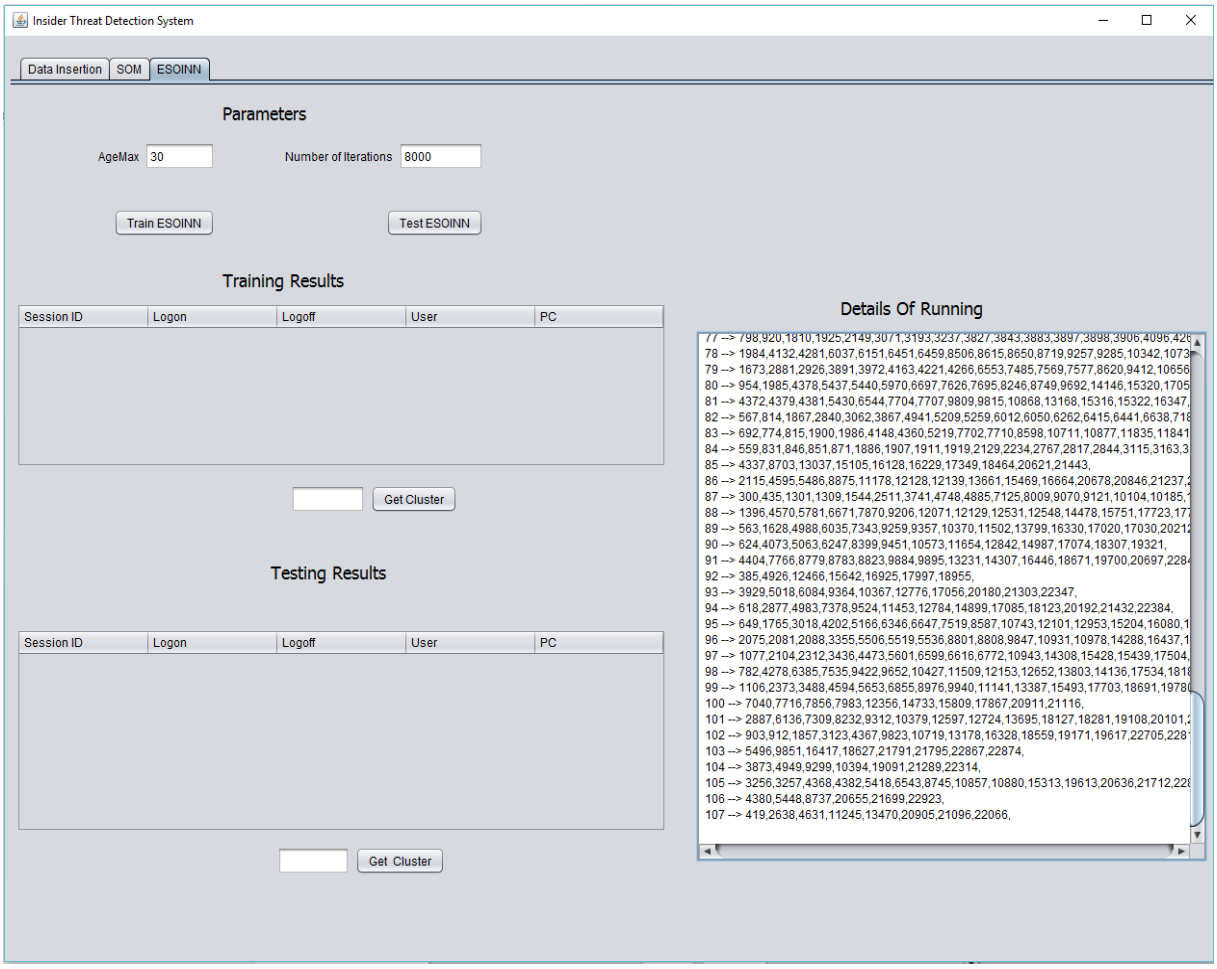
Εικόνα 27. Αποτελέσματα της συστάδας 11 για τον μήνα Ιούλιο με πλέγμα 4x3 και ακτίνα γειτονιάς 3 (τμήμα 1)



Εικόνα 28. Αποτελέσματα της συστάδας 11 για τον μήνα Ιούλιο με πλέγμα 4x3 και ακτίνα γειτονιάς 3 (τμήμα 2)

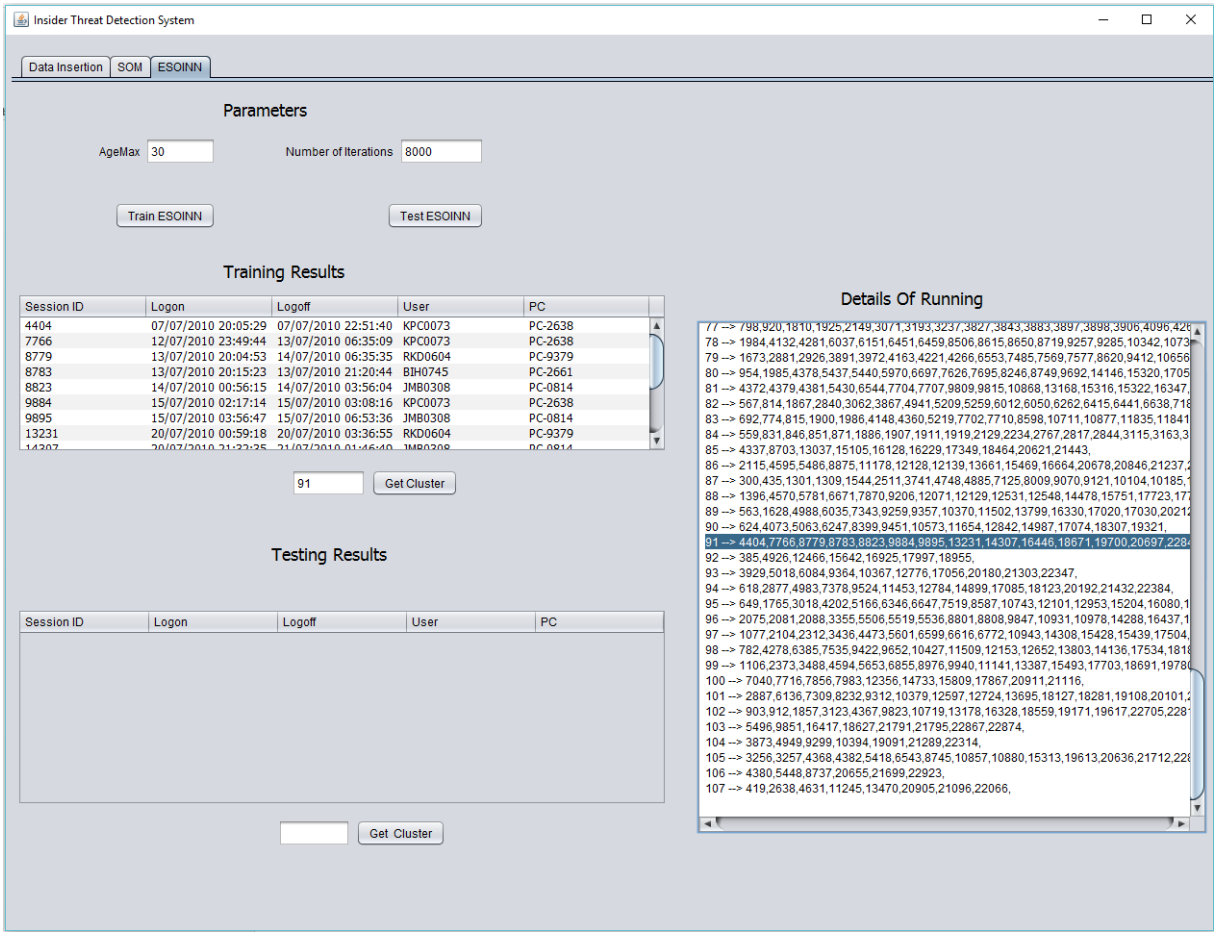
Μετά την επιτυχή εκπαίδευση του SOM προχωρήσαμε στην εκπαίδευση του αλγορίθμου ESOINN. Για την επιλογή του μέγιστου ορίου ακμών ανά συστάδα επιλέγουμε τον αριθμό 30. Επειδή στον μήνα Ιούλιο υπάρχουν 15 εσωτερικές απειλές, θεωρούμε ότι το όριο ακμών στο 30, φτάνει για να ταξινομηθούν οι απειλές σε μία συστάδα. Ξεκινάμε την εκπαίδευση του ESOINN με αριθμό επαναλήψεων ανά δείγμα

στις 8000 επαναλήψεις (***Εικόνα 29***). Οι συστάδες οι οποίες δημιουργεί ο ESOINN στο τέλος της εκπαιδευτικής διαδικασίας είναι 107 στο σύνολο.

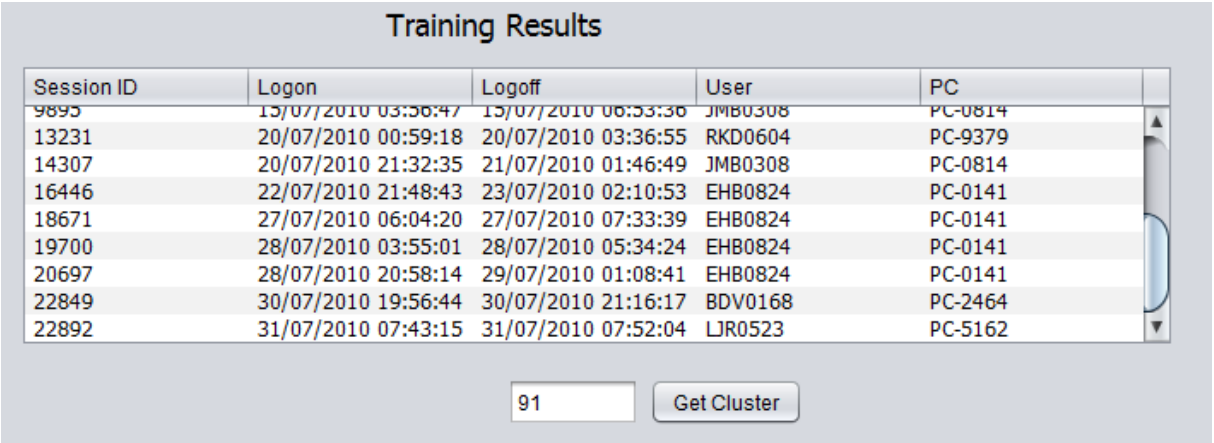


Εικόνα 29. Εκπαίδευση ESOINN για τον μήνα Ιούλιο με αριθμό επαναλήψεων στις 8000

Από τα αποτελέσματα στο τμήμα Details of Running παρατηρούμε ότι η συστάδα στην οποία ταξινομούνται και τα 15 δεδομένα εσωτερικής απειλής είναι η 91. Για την επιβεβαίωση των αποτελεσμάτων εμφανίζουμε τις συνεδρίες στον πίνακα Training Results. Από την ***Εικόνα 31*** και την ***Εικόνα 31*** παρατηρούμε ότι και οι 15 συνεδρίες εσωτερικής απειλής έχουν ταξινομηθεί στην συστάδα 91.



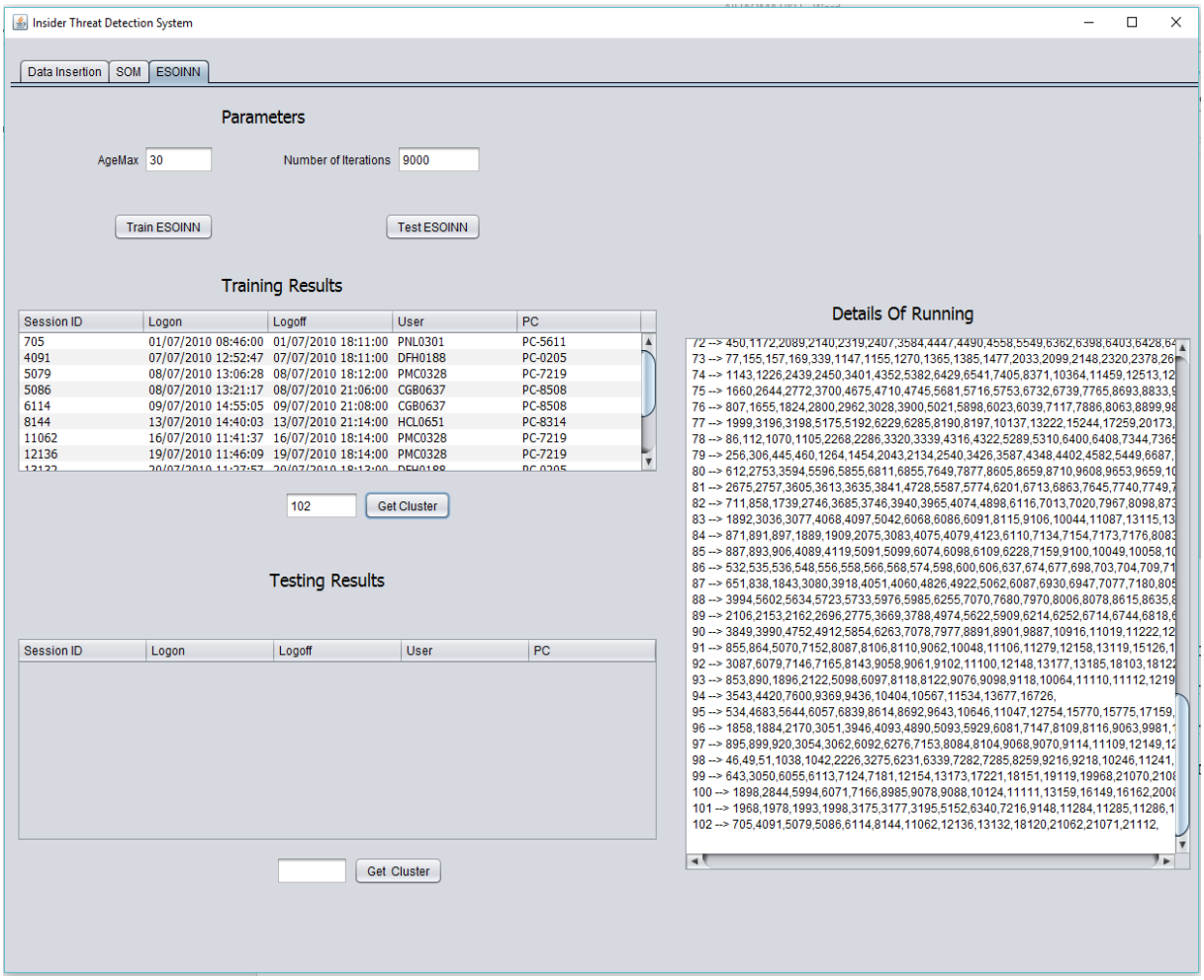
Εικόνα 30. Αποτελέσματα της συστάδας 91 κατά την εκπαίδευση του ESOINN τον μήνα Ιούλιο για 8000 επαναλήψεις (τμήμα 1)



Εικόνα 31. Αποτελέσματα της συστάδας 91 κατά την εκπαίδευση του ESOINN τον μήνα Ιούλιο για 8000 επαναλήψεις (τμήμα 2)

Αφού βρήκαμε τις κατάλληλες ρυθμίσεις για την εκπαίδευση του ESOINN, αυξήσαμε τον αριθμό των επαναλήψεων για να εξετάσουμε αν η σωστή κατηγοριοποίηση των εσωτερικών απειλών, εξαρτάται από το όριο των επαναλήψεων ή είναι θέμα κατάλληλων ρυθμίσεων. Αυξήσαμε τον αριθμό των επαναλήψεων στις 9000. Ο αριθμός

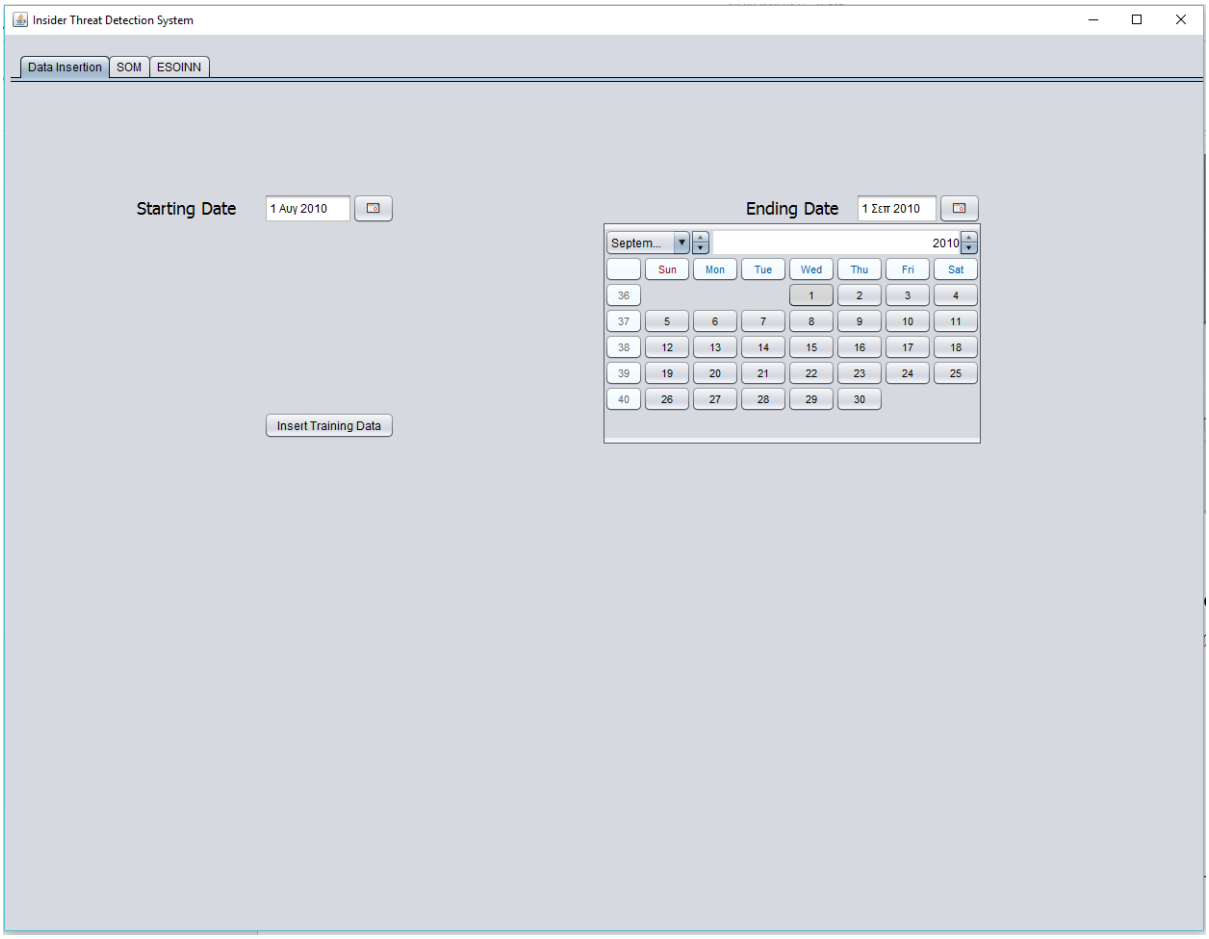
των παραγόμενων συστάδων μειώθηκε στις 102. Από τα αποτελέσματα επαληθέψαμε ότι οι εσωτερικές απειλές δεν ταξινομούνται σωστά (***Εικόνα 32***).



Εικόνα 32. Εκπαίδευση ESOINN για τον μήνα Ιούλιο με 9000 επαναλήψεις

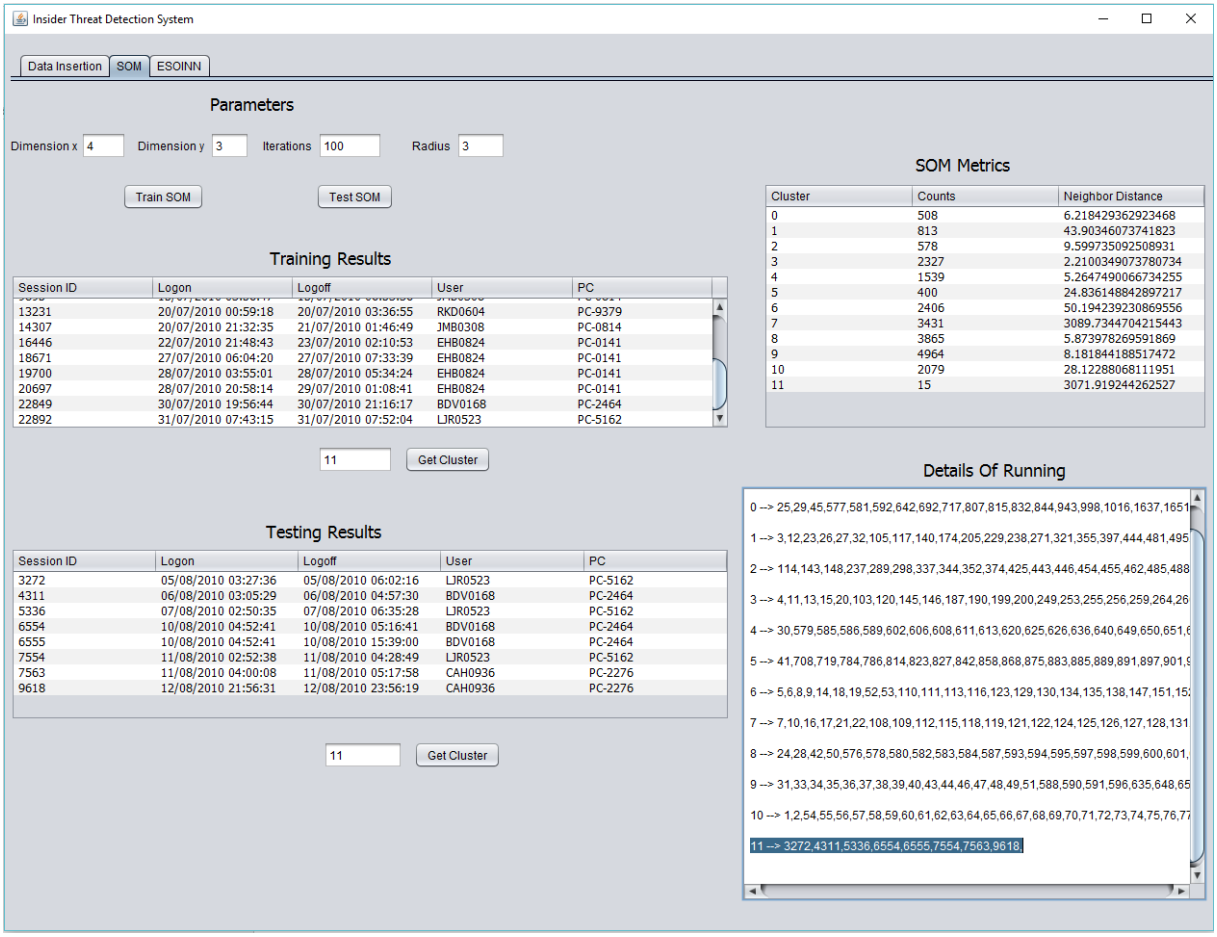
Αφού βρήκαμε τις κατάλληλες ρυθμίσεις για την εκπαίδευση των αλγορίθμων SOM και ESOINN προχωρήσαμε στην διαδικασία της δοκιμής. Η διαδικασία της δοκιμής πραγματοποιήθηκε ανά μήνα από τον Αύγουστο του 2010 μέχρι τον Οκτώβριο του 2010.

Πρώτα πήραμε από την βάση δεδομένων τις συνεδρίες του Αυγούστου (***Εικόνα 33***). Ο Αύγουστος περιέχει 7 συνεδρίες οι οποίες αποτελούν εσωτερική απειλή. Δοκιμάσαμε και τους δύο αλγορίθμους για να δούμε την απόδοσή τους στην ταξινόμηση νέων δεδομένων.



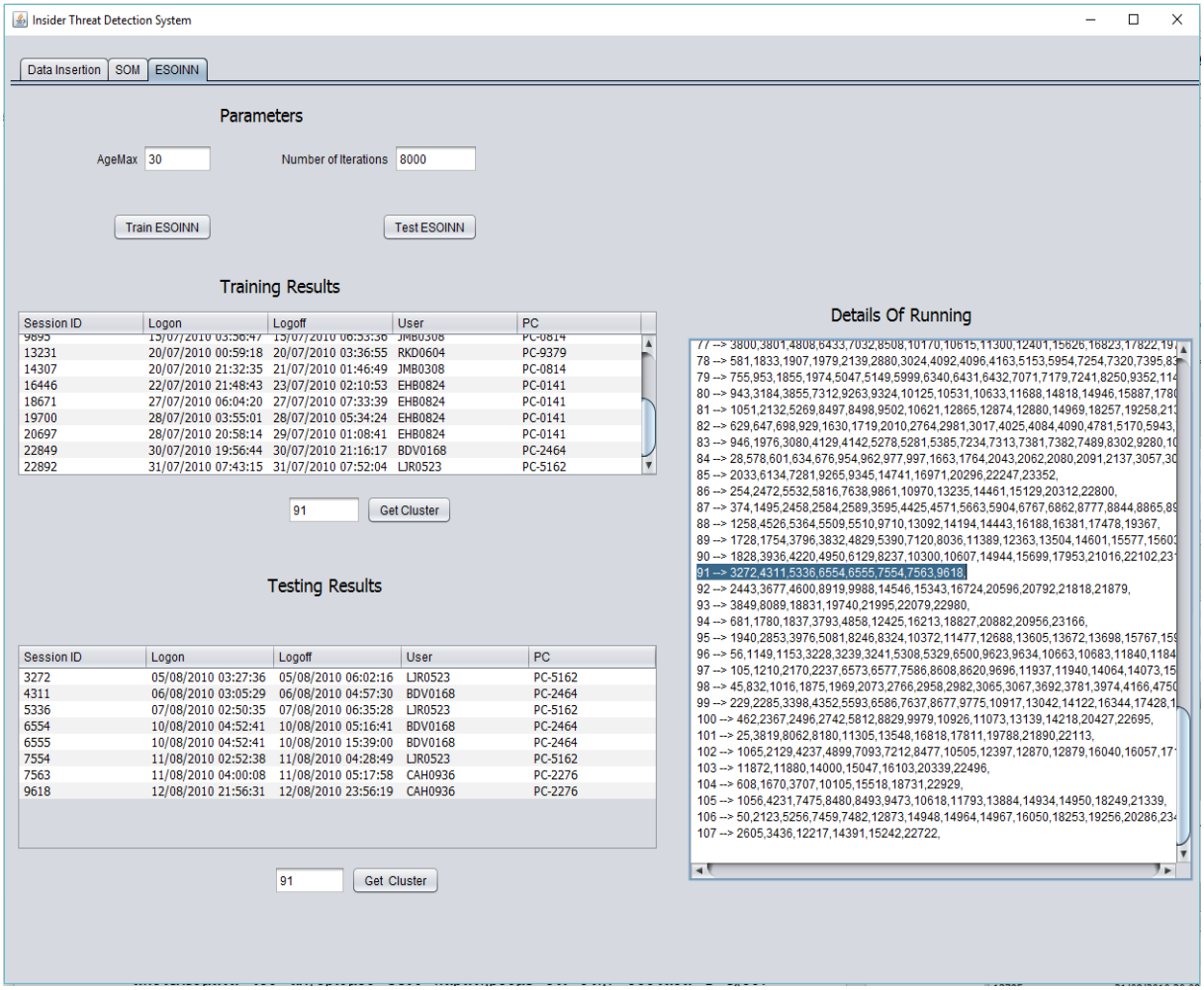
Εικόνα 33. Εισαγωγή δεδομένων Αυγούστου για την διαδικασία της δοκιμής

Στην καρτέλα SOM επιλέξαμε το κουμπί Test SOM, ώστε να αρχίσει η διαδικασία δοκιμής. Στο τμήμα Details of Running παρουσιάζονται οι συνεδρίες οι οποίες αντιστοιχούν σε κάθε συστάδα (***Εικόνα 34***). Στην συστάδα 11, η οποία κατά την διαδικασία της εκπαίδευσης ήταν η συστάδα των εσωτερικών απειλών, ταξινομήθηκαν οι συνεδρίες 3272, 4311, 5336, 6554, 6555, 7554, 7563 και 9618. Για να δούμε πιο αναλυτικά τις συνεδρίες, τις εμφανίζουμε στον πίνακα Test Results. Διαπιστώνουμε ότι ο αλγόριθμος αναγνώρισε 8 εσωτερικές απειλές. Η συνεδρία 6554 είναι υποσύνολο της συνεδρίας 6555 και για αυτό το λόγο οι δύο αυτές συνεδρίες μπορούν να θεωρηθούν σαν μια συνεδρία χρήστη. Επομένως ο αλγόριθμος SOM αναγνώρισε με επιτυχία και τις 7 εσωτερικές απειλές.



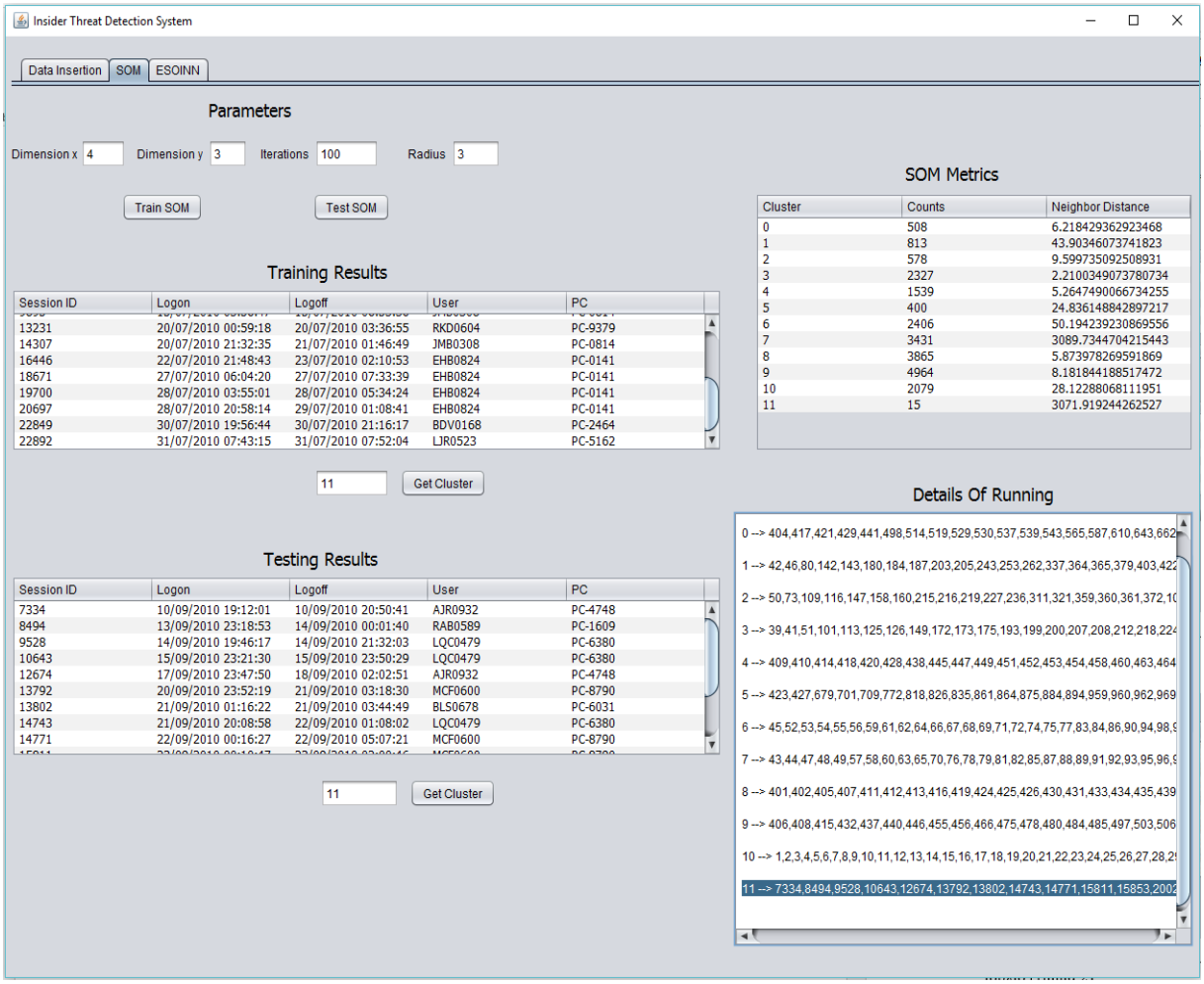
Εικόνα 34. Αποτελέσματα δοκιμής του SOM για τον Αύγουστο με δείγμα εκπαίδευσης από τον Ιούλιο

Δοκιμάζουμε τα ίδια δεδομένα και στον αλγόριθμο ESOINN (***Εικόνα 35***). Παρατηρούμε ότι και ο ESOINN ταξινομεί τις ίδιες συνεδρίες στην συστάδα 91, η οποία είναι η συστάδα των εσωτερικών απειλών. Στο πίνακα Testing Results φαίνονται με λεπτομέρεια οι συνεδρίες χρήστη, οι οποίες ανήκουν στην συστάδα 91.

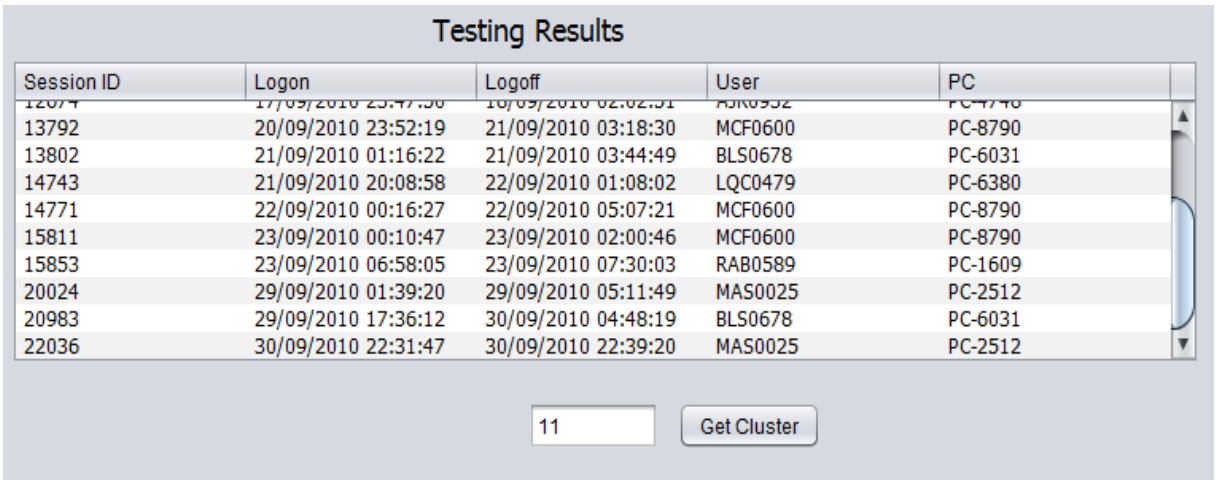


Εικόνα 35. Αποτελέσματα δοκιμής του ESOINN για τον Αύγουστο με δείγμα εκπαίδευσης από τον Ιούλιο

Η επόμενη δοκιμή των αλγορίθμων είναι για τον μήνα Σεπτέμβριο. Ο Σεπτέμβριος περιέχει 14 συνεδρίες χρήστη οι οποίες αποτελούν εσωτερικές απειλές. Από τα αποτελέσματα του αλγορίθμου SOM, παρατηρούμε ότι στην συστάδα 11 έχουν κατηγοριοποιηθεί και οι 14 συνεδρίες εσωτερικών απειλών, οι οποίες υπάρχουν στον μήνα Σεπτέμβριο. Στην ***Εικόνα 37*** και στην ***Εικόνα 37*** παρουσιάζονται με λεπτομέρεια οι συνεδρίες οι οποίες ανήκουν στον κόμβο 11.



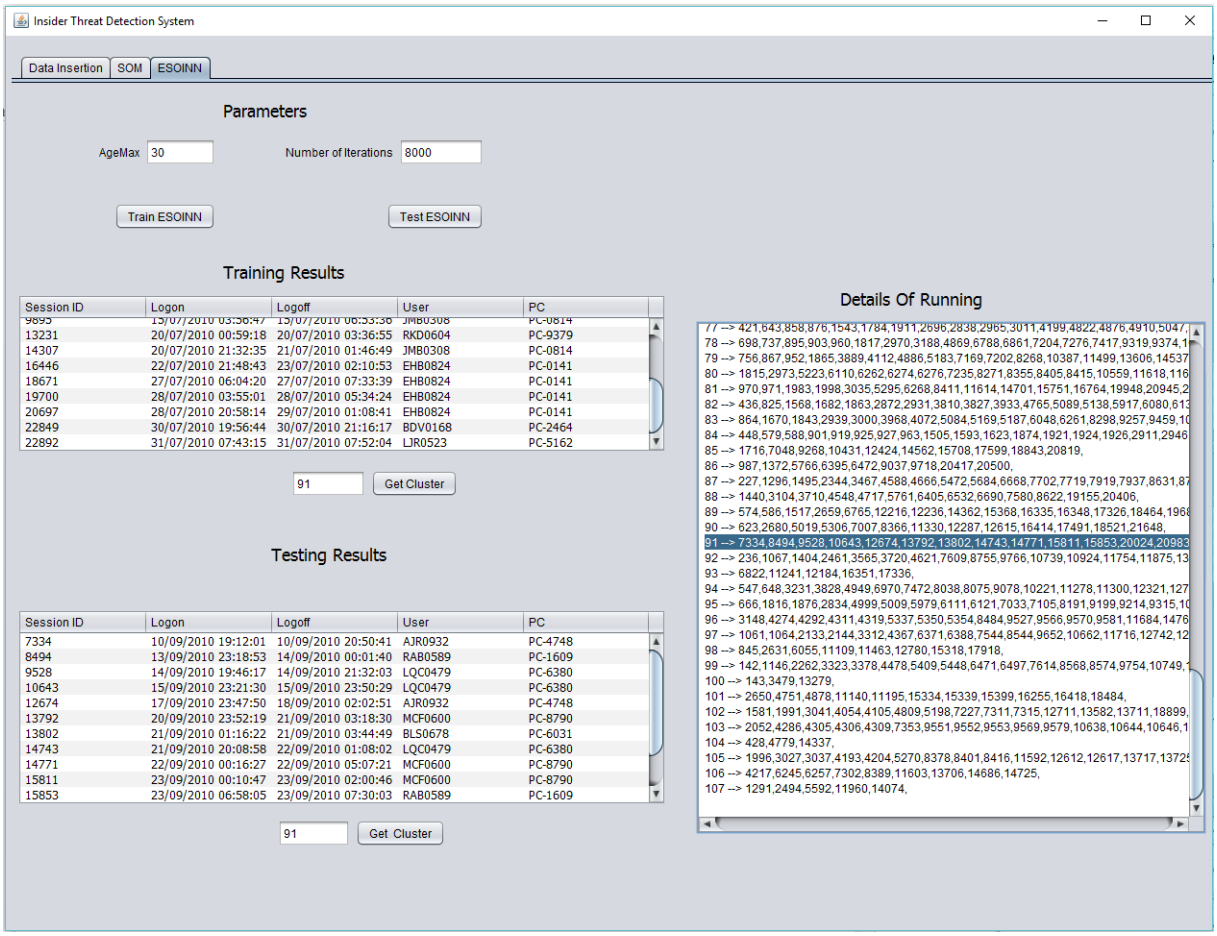
Εικόνα 36. Αποτελέσματα δοκιμής του SOM για τον Σεπτέμβριο με δείγμα εκπαίδευσης από τον Ιούλιο (τμήμα 1)



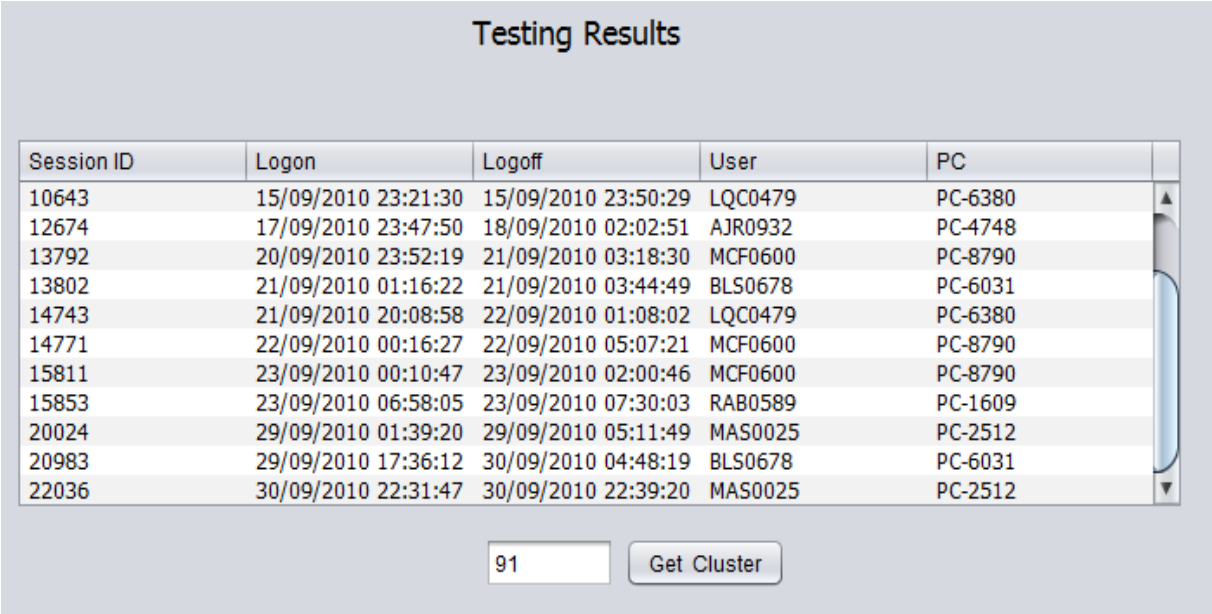
Εικόνα 37. Αποτελέσματα δοκιμής του SOM για τον Σεπτέμβριο με δείγμα εκπαίδευσης από τον Ιούλιο (τμήμα 2)

Προχωρήσαμε στην διαδικασία δοκιμής του αλγορίθμου ESOINN για τον μήνα Σεπτέμβριο. Από τις 14 συνεδρίες εσωτερικών απειλών του μήνα Σεπτεμβρίου, ο

ESOINN ταξινόμησε και τις 14 στον κόμβο 91 των εσωτερικών απειλών (***Εικόνα 39***, ***Εικόνα 39***).

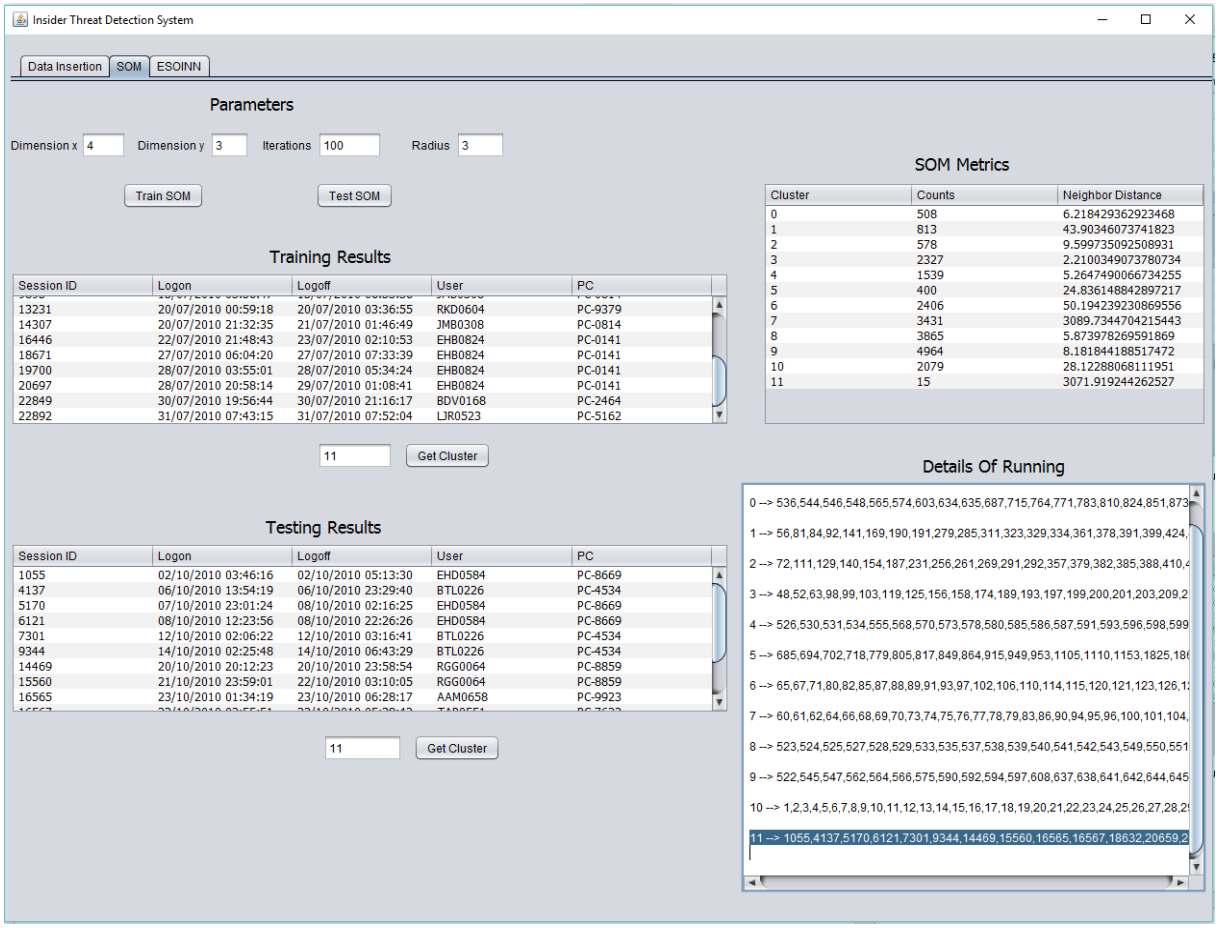


Εικόνα 38. Αποτελέσματα δοκιμής του ESOINN για τον Σεπτέμβριο με δείγμα εκπαίδευσης από τον Ιούλιο (τμήμα 1)

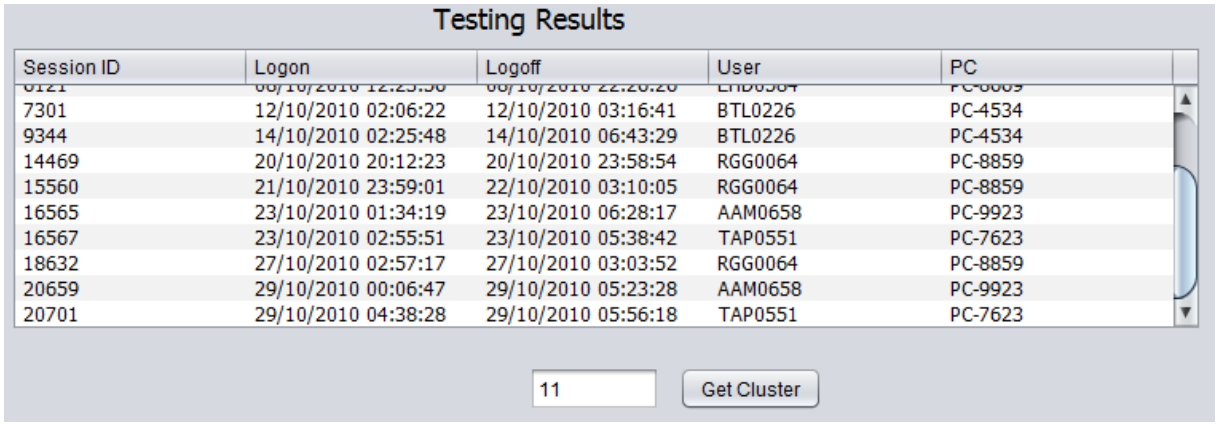


Εικόνα 39. Αποτελέσματα δοκιμής του ESOINN για τον Σεπτέμβριο με δείγμα εκπαίδευσης από τον Ιούλιο (τμήμα 2)

Τελευταίος μήνας για δοκιμή είναι ο Οκτώβριος. Ο μήνας αυτός περιέχει 13 συνεδρίες εσωτερικών απειλών. Ο αλγόριθμος SOM αναγνωρίζει και τις 13 συνεδρίες εσωτερικών απειλών που υπάρχουν (***Εικόνα 41***, ***Εικόνα 41***). Συγκεκριμένα οι συνεδρίες χρήστη 1055, 4137, 5170, 6121, 7301, 9344, 14469, 15560, 16565, 16567, 18632, 20659 και 20701 κατηγοριοποιούνται στον κόμβο 11.

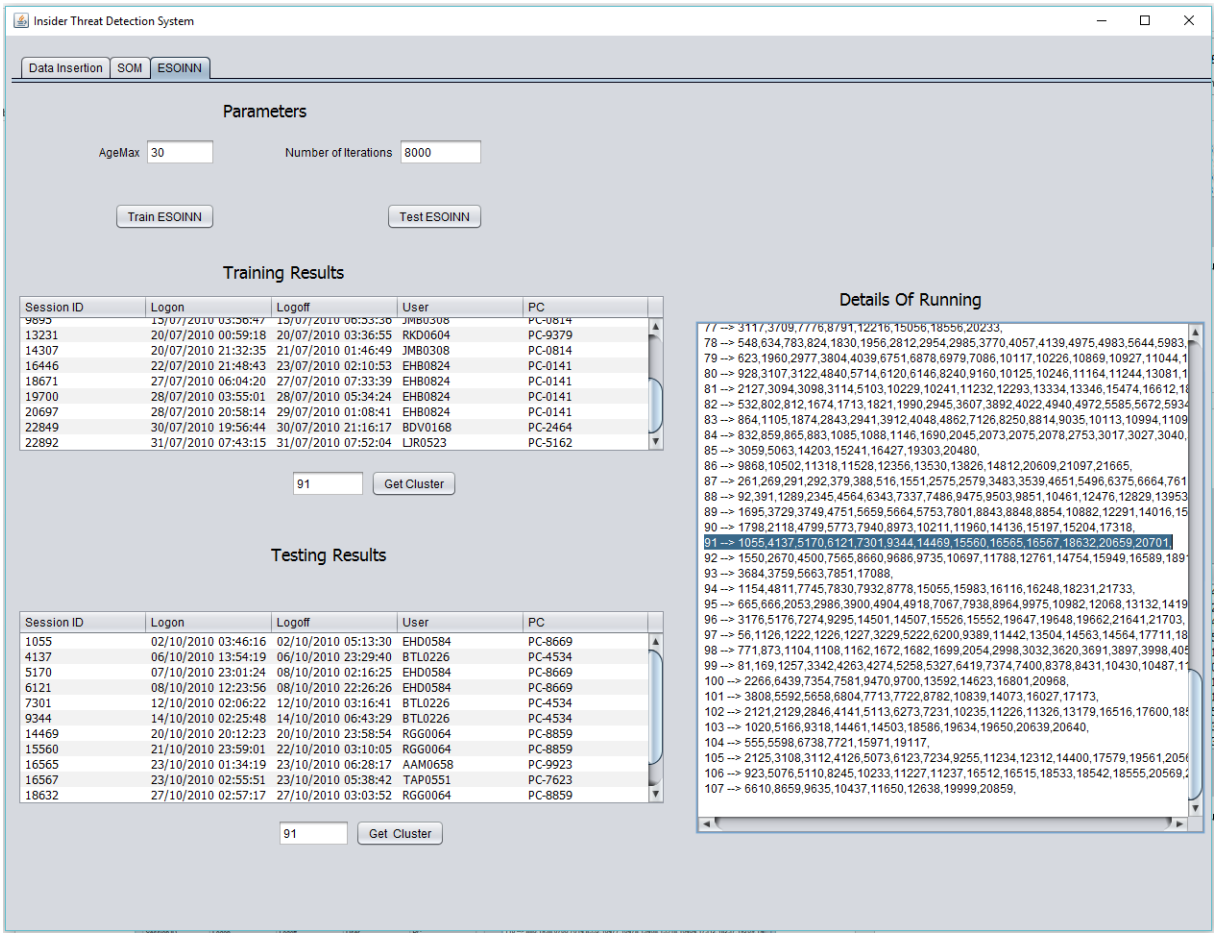


Εικόνα 40. Αποτελέσματα δοκιμής του SOM για τον Οκτώβριο με δείγμα εκπαίδευσης από τον Ιούλιο (τμήμα 1)

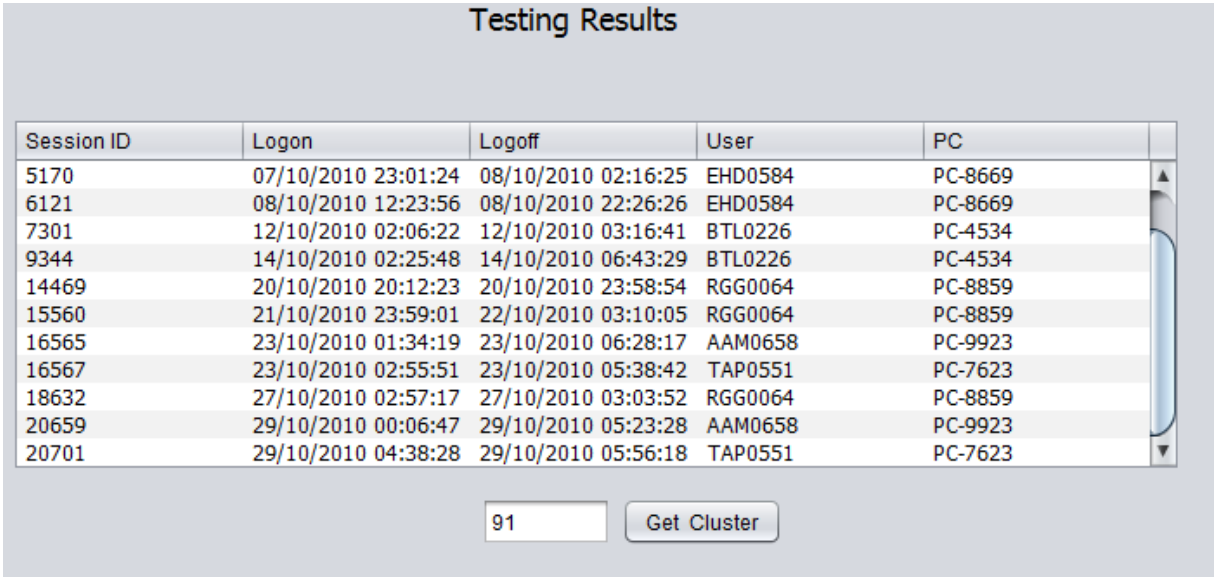


Εικόνα 41. Αποτελέσματα δοκιμής του SOM για τον Οκτώβριο με δείγμα εκπαίδευσης από τον Ιούλιο (τμήμα 2)

Ομοίως, ο αλγόριθμος ESOINN αναγνώρισε με επιτυχία όλες τις συνεδρίες εσωτερικών απειλών (***Εικόνα 43***, ***Εικόνα 43***). Όλες οι συνεδρίες ταξινομήθηκαν στη συστάδα 91.



Εικόνα 42. Αποτελέσματα δοκιμής του ESOINN για τον Οκτώβριο με δείγμα εκπαίδευσης από τον Ιούλιο (τμήμα 1)



Εικόνα 43. Αποτελέσματα δοκιμής του SOM για τον Οκτώβριο με δείγμα εκπαίδευσης από τον Ιούλιο (τμήμα 2)

Κεφάλαιο 6
Αποτελέσματα

Στην πειραματική διαδικασία εξετάσαμε την απόδοση των αλγορίθμων μη επιτηρούμενης μάθησης SOM και ESOINN. Διαμορφώσαμε την εφαρμογή που υλοποιήσαμε, ώστε να χρησιμοποιήσουμε τα συνθετικά σύνολα δεδομένων για εσωτερικές απειλές του CERT. Διαπιστώσαμε ότι η εκπαίδευση των αλγορίθμων SOM και ESOINN δεν είναι εύκολη υπόθεση. Χρειάστηκε να πραγματοποιήσουμε αρκετές δοκιμές αλλάζοντας τις παραμέτρους για να καταλήξουμε σε μία αποδοτική εκπαίδευση.

Αναλυτικότερα, πήραμε δείγμα δεδομένων από τον μήνα Ιούλιο το οποίο περιέχει 15 συνεδρίες εσωτερικών απειλών. Στον ***Πίνακας 4*** παρουσιάζονται κατά αύξουσα χρονολογική σειρά οι 15 συνεδρίες χρήστη, οι οποίες αποτελούν εσωτερικές απειλές για το σενάριο 1 του συνόλου δεδομένων που επιλέξαμε. Παρατηρούμε ότι οι ώρες που πραγματοποιούνται οι συνεδρίες εσωτερικών απειλών για τον Ιούλιο είναι μετά τις 19:00 και πριν τις 8:00.

Α/Α	ΣΥΝΔΕΣΗ	ΑΠΟΣΥΝΔΕΣΗ	ΧΡΗΣΤΗΣ	ΥΠΟΛΟΓΙΣΤΗΣ
1	07/07/2010 20:05:29	07/07/2010 22:51:40	KPC0073	PC-2638
2	12/07/2010 23:49:44	13/07/2010 06:35:09	KPC0073	PC-2638
3	13/07/2010 20:04:53	14/07/2010 06:35:35	RKD0604	PC-9379
4	13/07/2010 20:15:23	13/07/2010 21:20:44	BIH0745	PC-2661
5	14/07/2010 00:56:15	13/07/2010 03:56:04	JMB0308	PC-0814
6	15/07/2010 02:17:14	15/07/2010 03:08:16	KPC0073	PC-2638
7	15/07/2010 03:56:47	15/07/2010 06:53:36	JMB0308	PC-0814

8	20/07/2010 00:59:18	20/07/2010 03:36:55	RKD0604	PC-9379
9	20/07/2010 21:32:35	21/07/2010 01:46:49	JMB0308	PC-0814
10	22/07/2010 21:48:43	23/07/2010 02:10:53	EHB0824	PC-0141
11	27/07/2010 06:04:20	27/07/2010 07:33:39	EHB0824	PC-0141
12	28/07/2010 03:55:01	28/07/2010 05:34:24	EHB0824	PC-0141
13	28/07/2010 20:58:14	29/07/2010 01:08:41	EHB0824	PC-0141
14	30/07/2010 19:56:44	30/07/2010 21:16:17	BDV0168	PC-2464
15	31/07/2010 07:43:15	31/07/2010 07:52:04	LJR0523	PC-5162

Πίνακας 4. Συνεδρίες εσωτερικών απειλών για τον μήνα Ιούλιο

Για τον SOM, η πρώτη παράμετρος που έπρεπε να καθορίσουμε, ήταν η διάσταση του νευρωνικού του δικτύου. Δοκιμάσαμε τις διαστάσεις 4x4, 5x3 και 4x3. Καταλήξαμε στο συμπέρασμα ότι η διάσταση 4x3 του πλέγματος σε συνδυασμό με την τιμή 3 της ακτίνας γειτονιάς, είναι οι κατάλληλες παράμετροι για την εκπαίδευση του αλγορίθμου. Ο ***Πίνακας 5*** δείχνει την κατανομή των συνεδριών χρήστη στους κόμβους του νευρωνικού δικτύου του SOM. Οι δεκαπέντε εσωτερικές απειλές ταξινομήθηκαν στον κόμβο 11 του πλέγματος. Επίσης, παρατηρήθηκε μεγάλη απόσταση του κόμβου 11 από τους γειτονικούς του κόμβους (3071.92). Αυτή η απόσταση είναι η δεύτερη μεγαλύτερη κατά φθίνουσα σειρά απόσταση από τους γειτονικούς κόμβους του κάθε κόμβου. Μία τόσο μεγάλη διαφορά δηλώνει μια ανομοιογένεια του κόμβου 11 από τους γειτονικούς του.

Κόμβος Πλέγματος	Σύνολο Συνεδρίων	Απόσταση από γείτονες
0	508	6.218429362923468
1	813	43.90346073741823
2	578	9.599735092508931
3	2327	2.2100349073780734
4	1539	5.2647490066734255
5	400	24.836148842897217

6	2406	50.194239230869556
7	3431	3089.7344704215443
8	3865	5.873978269591869
9	4964	8.181844188517472
10	2079	28.12288068111951
11	15	3071.919244262527

Πίνακας 5. Δείχνει το σύνολο συνεδριών που ταξινομούνται σε κάθε κόμβο και τις αποστάσεις από τους γειτονικούς κόμβους

Συνεχίζοντας τη διαδικασία της εκπαίδευσης για το ίδιο δείγμα δεδομένων στον αλγόριθμο ESOINN, δοκιμάσαμε τις ρυθμίσεις με 9000 επαναλήψεις και 8000 επαναλήψεις κρατώντας την τιμή 30 του μέγιστου αριθμού ακμών. Οι συστάδες τις οποίες δημιούργησε ο ESOINN για 8000 επαναλήψεις, ήταν 107, ενώ για 9000 επαναλήψεις ήταν 102. Οι 8000 επαναλήψεις για κάθε διάνυσμα εισόδου κατηγοριοποίησαν τις συνεδρίες εσωτερικών απειλών σε μία συστάδα, η οποία ήταν η 91. Παρότι αυξήσαμε τον αριθμό των επαναλήψεων σε 9000, οι 15 εσωτερικές απειλές δεν ταξινομήθηκαν στον ίδιο κόμβο. Μπορεί η μείωση των συστάδων από 107 σε 102, να οδήγησε στην συγχώνευση της συστάδας των εσωτερικών απειλών με άλλες. Αποδείχτηκε λοιπόν ότι ο αριθμός των επαναλήψεων παίζει καθοριστικό ρόλο στην καλή εκπαίδευση του αλγορίθμου ESOINN.

Ένα επιπλέον συμπέρασμα που προκύπτει από την σύγκριση των αλγορίθμων, είναι ότι ο ESOINN χρησιμοποίησε σαφώς περισσότερους κόμβους από ότι ο SOM, για να ταξινομήσει τις εσωτερικές απειλές σε ένα κόμβο. Από την άλλη μεριά, ο SOM έχει περισσότερες παραμέτρους για να ρυθμιστούν. Επίσης, ο ESOINN δεν χρειάζεται να εκπαιδευτεί από την αρχή για καινούρια δεδομένα, καθώς έχει την ικανότητα να διατηρεί την προηγούμενη γνώση και να προσαρμόζεται κατάλληλα σε καινούρια δεδομένα.

Μετά την επιτυχή εκπαίδευση των αλγορίθμων προχωρήσαμε στην δοκιμή τους για τον εντοπισμό των εσωτερικών απειλών στους μήνες Αύγουστος, Σεπτέμβριος και Οκτώβριος. Η μέτρηση της απόδοσης των αλγορίθμων έγινε με την χρήση των μετρικών True Positive (TP), False Negative (FN) και Recall. Το TP αντιπροσωπεύει το σύνολο

των εσωτερικών απειλών που έχουν ταξινομηθεί σωστά. Το FN αντιπροσωπεύει το σύνολο των εσωτερικών απειλών οι οποίες κατηγοριοποιήθηκαν λάθος, δηλαδή δεν ταξινομήθηκαν στον κόμβο των εσωτερικών απειλών, ο οποίος δημιουργήθηκε στην διαδικασία εκπαίδευσης. Η ανάκληση (recall) μετριέται από τον τύπο:

$$recall = \frac{TP}{TP + FN}$$

Ο Αύγουστος έχει 7 συνεδρίες εσωτερικών απειλών. Όπως αναφέραμε και στην υποενότητα 5.4.1, οι αλγόριθμοι αναγνωρίζουν 8 εσωτερικές απειλές επειδή μία από αυτές τις συνεδρίες χρήστη είναι υποσύνολο μίας άλλης. Επομένως, μπορούμε να θεωρήσουμε ότι οι 8 συνεδρίες χρήστη στην ουσία είναι 7. Άρα οι δύο αλγόριθμοι ταξινόμησαν σωστά όλες τις συνεδρίες εσωτερικών απειλών. Ο ***Πίνακας 6*** δείχνει τα αποτελέσματα της ταξινόμησης των συνεδριών εσωτερικής απειλής. Παρατηρούμε ότι και οι δύο αλγόριθμοι έχουν 8 TP, κανένα FN και ανάκληση 1.

Αλγόριθμοι	True Positive	False Negative	Recall
SOM	8	0	1
ESOINN	8	0	1

Πίνακας 6. Μέτρα απόδοσης των αλγορίθμων SOM και ESOINN για τον Αύγουστο

Ο μήνας Σεπτέμβριος έχει 14 συνεδρίες εσωτερικών απειλών. Και οι δύο αλγόριθμοι ταξινομούν σωστά και τις 14 συνεδρίες χρήστη. Στον ***Πίνακας 7*** παρουσιάζονται τα μέτρα απόδοσης των αλγορίθμων SOM και ESOINN για τον Σεπτέμβριο. Παρατηρούμε ότι και οι δύο αλγόριθμοι έχουν 14 TP, κανένα FN και ανάκλαση 1.

Αλγόριθμοι	True Positive	False Negative	Recall
SOM	14	0	1
ESOINN	14	0	1

Πίνακας 7. Μέτρα απόδοσης των αλγορίθμων SOM και ESOINN για τον Σεπτέμβριο

Ο τελευταίος μήνας δοκιμών ήταν ο Οκτώβριος. Στον Οκτώβριο υπάρχουν 13 συνεδρίες εσωτερικών απειλών. Οι αλγόριθμοι SOM και ESOINN αναγνώρισαν με επιτυχία και τις 13 αυτές συνεδρίες. Συγκεκριμένα και οι δυο αλγόριθμοι είχαν 13 TP, κανένα FN και ανάκληση 1 (***Πίνακας 8***).

Αλγόριθμοι	True Positive	False Negative	Recall
SOM	13	0	1
ESOINN	13	0	1

Πίνακας 8. Μέτρα απόδοσης των αλγορίθμων SOM και ESOINN για τον Οκτώβριο

Επομένως, συνολικά για το διάστημα των τριών μηνών, οι αλγόριθμοι SOM και ESOINN ταξινόμησαν σωστά και τις 35 συνεδρίες εσωτερικών απειλών. Στον ***Πίνακας 9*** παρουσιάζονται τα μέτρα απόδοσης για το διάστημα των τριών μηνών δοκιμής των SOM και ESOINN. Διαπιστώνουμε συνολικά ότι η τιμή της ανάκλησης για το πρώτο σενάριο του συνόλου δεδομένων είναι 1, αποτέλεσμα εξαιρετικά καλό.

Αλγόριθμοι	True Positive	False Negative	Recall
SOM	35	0	1
ESOINN	35	0	1

Πίνακας 9. Μέτρα απόδοσης των αλγορίθμων SOM και ESOINN και για τους τρεις μήνες

Ψάξαμε στην βιβλιογραφία για έρευνες που έχουν χρησιμοποιήσει το σύνολο δεδομένων του CERT και συγκεκριμένα την έκδοση 4.2. Η πιο σχετική δουλειά με την δική μας είναι των (Roberts et al. 2016). Από τα έξι χαρακτηριστικά τα οποία προτείνουν για τον εντοπισμό των εσωτερικών απειλών του σεναρίου 1, συμφωνούμε σε 3. Συγκεκριμένα, από την πειραματική διαδικασία και μέσω της στατιστικής ανάλυσης συμφωνούμε στις δύο ρυθμίσεις που αφορούν το ωράριο εκτός εργασίας. Το τρίτο χαρακτηριστικό που συμφωνούμε είναι οι ιστοσελίδες διαμοιρασμού αρχείων.

Οι ερευνητές επέλεξαν ένα χρονικό διάστημα 3 μηνών για την εκπαίδευση των μοντέλων τους. Δημιούργησαν διάφορα μοντέλα επιλέγοντας κάποια από τα 6 χαρακτηριστικά από τα οποία πρότειναν. Ένα από τα μοντέλα τους, το οποίο έκανε χρήση όλων των χαρακτηριστικών είχε ανάκληση 70,6%. Η δική μας προσέγγιση έφερε ανάκληση 100% παρότι το χρονικό διάστημα το οποίο επιλέξαμε ήταν μικρότερο (ένας μήνας).

Κεφάλαιο 7

Επίλογος

Ο εντοπισμός των εσωτερικών απειλών είναι ένα πολύ σημαντικό πρόβλημα το οποίο απαιτεί μεγάλη προσοχή. Στην παρούσα μεταπτυχιακή διατριβή διατυπώσαμε την έννοιας της εσωτερικής απειλής και του εσωτερικού. Επίσης, αναφέραμε τις κατηγορίες των επιθέσεων οι οποίες προκύπτουν από πρόθεση. Ένας κακόβουλος υπάλληλος σε έναν οργανισμό γνωρίζει αρκετά καλά τις πληροφοριακές υποδομές του οργανισμού και μπορεί να προκαλέσει μεγαλύτερη ζημιά από έναν εξωτερικό. Για αυτό το λόγο υλοποιήθηκε ένα σύστημα εντοπισμού των εσωτερικών απειλών σε ένα εταιρικό δίκτυο.

Το σύστημα είναι δομημένο έτσι ώστε να εξυπηρετεί την εύκολη πρόσβαση στα δεδομένα καταγραφής. Από την ανάλυση των δεδομένων καταγραφής μπορούν να εξαχθούν σημαντικές πληροφορίες για τις δραστηριότητες των χρηστών του πληροφοριακού συστήματος ενός οργανισμού. Για την ανάλυση των δεδομένων αναπτύχθηκε η εφαρμογή ITDS, η οποία εφαρμόζει τους αλγορίθμους μη επιτηρούμενης μάθησης SOM και ESOINN.

Αξίζει να σημειωθεί ότι το σύστημα που αναπτύχθηκε καθώς και η εφαρμογή η οποία υλοποιήθηκε, δεν εξαρτάται από το λειτουργικό σύστημα. Για την εξέταση της απόδοσης των αλγορίθμων SOM και ESOINN, επιλέχθηκε το σύνολο δεδομένων του CERT. Επίσης πραγματοποιήθηκε η εκπαίδευση των αλγορίθμων για χρονικό διάστημα ενός μήνα και συγκεκριμένα του Ιουλίου.

Πραγματοποιήθηκαν οι δοκιμές των αλγορίθμων για συνολικό διάστημα 3 μηνών. Από τα αποτελέσματα προέκυψε ότι και οι δύο αλγόριθμοι αναγνωρίζουν τις εσωτερικές

απειλές εξίσου. Το ποσοστό επιτυχίας και των δύο αλγορίθμων ήταν 100% σε ένα σύνολο από 35 συνεδρίες εσωτερικών απειλών.

7.2 Μελλοντική Δουλεία

Η έκδοση 4.2 του συνόλου δεδομένων του CERT περιέχει και άλλα δύο σενάρια εσωτερικών απειλών. Κρίνεται αναγκαία η επέκταση της εφαρμογής και στον εντοπισμό των άλλων δύο σεναρίων. Επίσης, για την ενσωμάτωση αυτών των σεναρίων θα πρέπει να πραγματοποιηθεί επιπλέον ανάλυση των χαρακτηριστικών τα οποία θα πρέπει να λάβουμε υπόψιν δημιουργώντας μεγαλύτερη δυσκολία στους αλγορίθμους.

Κατά την πειραματική διαδικασία παρατηρήθηκε καθυστέρηση της εξαγωγής των χαρακτηριστικών από την βάση. Θα μελετήσουμε την βελτιστοποίηση της συγκεκριμένης αδυναμίας η οποία όμως δεν έχει σχέση με την απόδοση των αλγορίθμων, ώστε να δουλεύει πιο γρήγορα η εφαρμογή. Πιθανώς η χρήση πιο αποδοτικών indexes να βελτιώσει την ταχύτητα.

Επίσης διαπιστώθηκε ότι οι αλγόριθμοι έχουν την ίδια αποτελεσματικότητα στον εντοπισμό εσωτερικών απειλών. Θα δοκιμάσουμε να εκμεταλλευτούμε την δυνατότητα του ESOINN ως αυξητικός αλγόριθμος ώστε να εκπαιδευτεί για άλλο τύπο απειλής και να τον συγκρίνουμε με τον SOM, ο οποίος πρέπει να αρχίσει την διαδικασία της εκπαίδευσης από την αρχή.

Τέλος, σκοπεύουμε να διαμορφώσουμε την εφαρμογή ITDS με περισσότερα στατιστικά μέτρα για τους αλγορίθμους, καθώς και να ενσωματώσουμε γραφικές αναπαραστάσεις τους.

Παράρτημα Α

Απαντήσεις Συνόλου Δεδομένων

Στο κεφάλαιο αυτό παρουσιάζονται οι συνεδρίες εσωτερικών απειλών που υπάρχουν στο σύνολο δεδομένων εσωτερικών απειλών του CERT. Οι εσωτερικές απειλές ταξινομούνται ανά μήνα και χρονολογική σειρά σύνδεσης στο πληροφοριακό σύστημα ενός οργανισμού.

Α.1 Πίνακας Εσωτερικών Απειλών Ιουλίου 2010

Α/Α	ΣΥΝΔΕΣΗ	ΑΠΟΣΥΝΔΕΣΗ	ΧΡΗΣΤΗΣ	ΥΠΟΛΟΓΙΣΤΗΣ
1	07/07/2010 20:05:29	07/07/2010 22:51:40	KPC0073	PC-2638
2	12/07/2010 23:49:44	13/07/2010 06:35:09	KPC0073	PC-2638
3	13/07/2010 20:04:53	14/07/2010 06:35:35	RKD0604	PC-9379
4	13/07/2010 20:15:23	13/07/2010 21:20:44	BIH0745	PC-2661
5	14/07/2010 00:56:15	13/07/2010 03:56:04	JMB0308	PC-0814
6	15/07/2010 02:17:14	15/07/2010 03:08:16	KPC0073	PC-2638
7	15/07/2010 03:56:47	15/07/2010 06:53:36	JMB0308	PC-0814

8	20/07/2010 00:59:18	20/07/2010 03:36:55	RKD0604	PC-9379
9	20/07/2010 21:32:35	21/07/2010 01:46:49	JMB0308	PC-0814
10	22/07/2010 21:48:43	23/07/2010 02:10:53	EHB0824	PC-0141
11	27/07/2010 06:04:20	27/07/2010 07:33:39	EHB0824	PC-0141
12	28/07/2010 03:55:01	28/07/2010 05:34:24	EHB0824	PC-0141
13	28/07/2010 20:58:14	29/07/2010 01:08:41	EHB0824	PC-0141
14	30/07/2010 19:56:44	30/07/2010 21:16:17	BDV0168	PC-2464
15	31/07/2010 07:43:15	31/07/2010 07:52:04	LJR0523	PC-5162

Α.2 Πίνακας Εσωτερικών Απειλών Αυγούστου 2010

Α/Α	ΣΥΝΔΕΣΗ	ΑΠΟΣΥΝΔΕΣΗ	ΧΡΗΣΤΗΣ	ΥΠΟΛΟΓΙΣΤΗΣ
1	05/08/2010 03:27:36	05/08/2010 06:02:16	LJR0523	PC-5162
2	06/08/2010 03:05:29	06/08/2010 04:57:30	BDV0168	PC-2464
3	07/08/2010 02:50:35	07/08/2010 06:35:28	LJR0523	PC-5162
4	10/08/2010 04:52:41	10/08/2010 05:16:41	BDV0168	PC-2464
5	11/08/2010 02:52:38	11/08/2010 04:28:49	LJR0523	PC-5162
6	11/08/2010 04:00:08	11/08/2010 05:17:58	CAH0936	PC-2276
7	12/08/2010	12/08/2010	CAH0936	PC-2276

	21:56:31	23:56:19		

Α.3 Πίνακας Εσωτερικών Απειλών Σεπτεμβρίου 2010

Α/Α	ΣΥΝΔΕΣΗ	ΑΠΟΣΥΝΔΕΣΗ	ΧΡΗΣΤΗΣ	ΥΠΟΛΟΓΙΣΤΗΣ
1	10/09/2010 19:12:01	10/09/2010 20:50:41	AJR0932	PC-4748
2	13/09/2010 23:18:53	14/09/2010 00:01:40	RAB0589	PC-1609
3	14/09/2010 19:46:17	14/09/2010 21:32:03	LQC0479	PC-6380
4	15/09/2010 23:21:30	15/09/2010 23:50:29	LQC0479	PC-6380
5	17/09/2010 23:47:50	18/09/2010 02:02:51	AJR0932	PC-4748
6	20/09/2010 23:52:19	21/09/2010 03:18:30	MCF0600	PC-8790
7	21/09/2010 01:16:22	21/09/2010 03:44:49	BLS0678	PC-6031
8	21/09/2010 20:08:58	22/09/2010 01:08:02	LQC0479	PC-6380
9	22/09/2010 00:16:27	22/09/2010 05:07:21	MCF0600	PC-8790
10	23/09/2010 00:10:47	23/09/2010 02:00:46	MCF0600	PC-8790
11	23/09/2010 06:58:05	23/09/2010 07:30:03	RAB0589	PC-1609
12	29/09/2010 01:39:20	29/09/2010 05:11:49	MAS0025	PC-2512
13	29/09/2010 17:36:12	30/09/2010 04:48:19	BLS0678	PC-6031
14	30/09/2010 22:31:47	30/09/2010 22:39:20	MAS0025	PC-2512

Α.4 Πίνακας Εσωτερικών Απειλών Οκτωβρίου 2010

Α/Α	ΣΥΝΔΕΣΗ	ΑΠΟΣΥΝΔΕΣΗ	ΧΡΗΣΤΗΣ	ΥΠΟΛΟΓΙΣΤΗΣ
1	02/10/2010 03:46:16	02/10/2010 05:13:30	EHD0584	PC-8669
2	06/10/2010 22:25:52	06/10/2010 23:29:40	BTL0226	PC-4534
3	07/10/2010 23:01:24	08/10/2010 02:16:25	EHD0584	PC-8669
4	08/10/2010 20:03:33	08/10/2010 22:26:26	EHD0584	PC-8669
5	12/10/2010 02:06:22	12/10/2010 03:16:41	BTL0226	PC-4534
6	14/10/2010 02:25:48	14/10/2010 06:43:29	BTL0226	PC-4534
7	20/10/2010 20:12:23	20/10/2010 23:58:54	RGG0064	PC-8859
8	21/10/2010 23:59:01	22/10/2010 03:10:05	RGG0064	PC-8859
9	23/10/2010 01:34:19	23/10/2010 06:28:17	AAM0658	PC-9923
10	23/10/2010 02:55:51	23/10/2010 05:38:42	TAP0551	PC-7623
11	27/10/2010 02:57:17	27/10/2010 03:03:52	RGG0064	PC-8859
12	29/10/2010 00:06:47	29/10/2010 05:23:28	AAM0658	PC-9923
13	29/10/2010 04:38:28	29/10/2010 05:56:18	TAP0551	PC-7623

Α.5 Πίνακας Εσωτερικών Απειλών Νοεμβρίου 2010

Α/Α	ΣΥΝΔΕΣΗ	ΑΠΟΣΥΝΔΕΣΗ	ΧΡΗΣΤΗΣ	ΥΠΟΛΟΓΙΣΤΗΣ
1	09/11/2010	09/11/2010	GHL0460	PC-6255

	06:28:40	07:08:45		
2	19/11/2010 05:53:16	19/11/2010 06:59:41	HJB0742	PC-5635
3	24/11/2010 23:55:22	25/11/2010 04:51:16	HJB0742	PC-5635
4	25/11/2010 06:35:11	25/11/2010 06:51:18	FTM0406	PC-1786

Α.6 Πίνακας Εσωτερικών Απειλών Δεκεμβρίου 2010

Α/Α	ΣΥΝΔΕΣΗ	ΑΠΟΣΥΝΔΕΣΗ	ΧΡΗΣΤΗΣ	ΥΠΟΛΟΓΙΣΤΗΣ
1	02/12/2010 00:09:23	02/12/2010 00:35:19	FTM0406	PC-1786
2	13/12/2010 20:30:07	14/12/2010 06:42:27	MYD0978	PC-3401
3	15/12/2010 02:57:50	15/12/2010 06:35:56	MYD0978	PC-3401
4	18/12/2010 06:44:49	18/12/2010 07:02:34	MYD0978	PC-3401

Α.7 Πίνακας Εσωτερικών Απειλών Ιανουαρίου 2011

Α/Α	ΣΥΝΔΕΣΗ	ΑΠΟΣΥΝΔΕΣΗ	ΧΡΗΣΤΗΣ	ΥΠΟΛΟΓΙΣΤΗΣ
1	05/01/2011 21:53:29	05/01/2011 22:48:01	FMG0527	PC-4256
2	11/01/2011 23:33:58	12/01/2011 01:15:35	FMG0527	PC-4256
3	19/01/2011 20:25:05	20/01/2011 06:14:40	JRG0207	PC-8908
4	25/01/2011 17:12:18	26/01/2011 02:38:27	JRG0207	PC-8908

Α.8 Πίνακας Εσωτερικών Απειλών Φεβρουαρίου 2011

Α/Α	ΣΥΝΔΕΣΗ	ΑΠΟΣΥΝΔΕΣΗ	ΧΡΗΣΤΗΣ	ΥΠΟΛΟΓΙΣΤΗΣ
1	04/02/2011 07:08:00	04/02/2011 07:36:05	DCH0843	PC-8720
2	08/02/2011 05:55:53	08/02/2011 06:01:50	MAR0955	PC-6793
3	09/02/2011 02:40:01	09/02/2011 02:52:07	MAR0955	PC-6793
4	09/02/2011 03:00:27	09/02/2011 06:46:27	PPF0435	PC-1809
5	11/02/2011 06:02:36	11/02/2011 06:29:08	MAR0955	PC-6793
6	12/02/2011 07:11:50	12/02/2011 07:33:24	KLH0596	PC-0132
7	24/02/2011 19:49:41	24/02/2011 23:11:08	WDD0366	PC-0155

Α.9 Πίνακας Εσωτερικών Απειλών Μαρτίου 2011

Α/Α	ΣΥΝΔΕΣΗ	ΑΠΟΣΥΝΔΕΣΗ	ΧΡΗΣΤΗΣ	ΥΠΟΛΟΓΙΣΤΗΣ
1	02/03/2011 20:10:30	03/03/2011 01:01:02	WDD0366	PC-0155

Βιβλιογραφία

Agrafiotis, I. et al., 2014. Towards a user and role-based sequential behavioural analysis tool for insider threat detection. *Journal of Internet Services and Information Security (JISIS)*, 4(November), pp.127–137.

Alahmadi, B. a, Legg, P. a & Nurse, J.R.C., 2014. Using internet activity profiling for insider-threat detection.

Bishop, M. et al., 2010. A Risk Management Approach to the "Insider Threat." *Advances in Information Security*, 49, pp.115–137.

Bishop, M. et al., 2008. Countering insider threats. *Dagstuhl Seminar Proceedings 08*, pp.18–35. Available at: http://vesta.informatik.rwth-aachen.de/opus/volltexte/2008/1793/pdf/08302.SWM.1793.pdf.

Brackney, C.R. & Anderson, H.R., 2004. Understanding the Insider Threat. Proceedings of a March 2004 Workshop. Available at: http://www.dtic.mil/dtic/tr/fulltext/u2/a429854.pdf.

Brdiczka, O. et al., 2012. Proactive insider threat detection through graph learning and psychological context. *Proceedings - IEEE CS Security and Privacy Workshops, SPW 2012*, pp.142–149.

Cappelli, D.M., Moore, A.P. & Trzeciak, R.F., 2012. *The CERT Guide to Insider Threats*, Addison-Wesley.

CERT Insider Threat Tools, Insider Threat Tools | The CERT Division. Available at: https://www.cert.org/insider-threat/tools/index.cfm [Accessed December 27, 2016].

Corchado, J.M. et al., 2009. Model of experts for decision support in the diagnosis of leukemia patients. *Artificial Intelligence in Medicine*, 46(3), pp.179–200.

EBizMBA, 2016. Top 15 Most Popular File Sharing Websites | January 2017. Available at: http://www.ebizmba.com/articles/file-sharing-websites [Accessed January 8, 2017].

Emil, F., 2016. *New Approaches in Intelligent Image Analysis*, Available at:

http://link.springer.com/10.1007/978-3-319-32192-9.

Fawcett, T. & Provost, F., 1999. Activity monitoring: Noticing interesting changes in behavior. *Proceedings of the fifth ACM SIGKDD international conference on Knowledge discovery and data mining*, 1(212), pp.53–62. Available at: http://portal.acm.org/citation.cfm?id=312195.

Furao, S. & Hasegawa, O., 2006. An incremental network for on-line unsupervised classification and topology learning. *Neural Networks*, 19(1), pp.90–106.

Furao, S., Ogura, T. & Hasegawa, O., 2007. An enhanced self-organizing incremental neural network for online unsupervised learning. *Neural Networks*, 20(8), pp.893–903.

Garfinkel, R., Gopal, R. & Goes, P., 2002. Privacy Protection of Binary Confidential Data Against Deterministic, Stochastic, and Insider Threat. *Management Science*, 48(March 2015), pp.749–764.

Gheyas, I.A. & Abdallah, A.E., 2016. Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. *Big Data Analytics*, 1(1), p.6. Available at: http://dx.doi.org/10.1186/s41044-016-0006-0.

Glasser, J. & Lindauer, B., 2013. Bridging the Gap: A Pragmatic Approach to Generating Insider Threat Data. *2013 IEEE Security and Privacy Workshops*, pp.98–104. Available at: http://www.computer.org/csdl/proceedings/spw/2013/5017/00/5017a098-abs.html.

Gori, M. & Melacci, S., 2010. Artificial Neural Networks – ICANN 2010. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 6354(PART 3), pp.315–320. Available at: http://www.scopus.com/inward/record.url?eid=2-s2.0-78049385459&partnerID=tZOtx3y1.

Grossberg, S., 1988. Nonlinear neural networks: principles,\nmechanisms, and architectures. *Neural Networks*, 1, pp.17–61. Available at: http://www.sciencedirect.com/science/article/pii/0893608088900214.

Hunker, J. & Probst, C., 2011. Insiders and insider threats—an overview of definitions and mitigation techniques. *Journal of Wireless Mobile Networks, Ubiquitous …*, pp.4–27. Available at: http://isyou.info/jowua/papers/jowua-v2n1-1.pdf.

Kandias, M. et al., 2010. An Insider Threat Prediction Model. *Trust, Privacy and Security in Digital Business*, 6264, pp.26–37.

Kohonen, T., 1982. Self-organized formation of topologically correct feature maps. *Biological Cybernetics*, 43(1), pp.59–69. Available at: http://link.springer.com/10.1007/BF00337288.

Kohonen, T., 1990. The self-organizing map. *Proceedings of the IEEE*, 78(9), pp.1464–1480.

Kroll, 2015. GLOBAL FRAUD Vulnerabilities on the Rise. Available at: fraud.kroll.com.

Kubat, M., 1999. Neural networks: a comprehensive foundation by Simon Haykin, Macmillan, 1994, ISBN 0-02-352781-7. *The Knowledge Engineering Review*, 13(4), pp.409–412.

Landers, J.E., 2016. Insider Threat Spotlight Report.

Legg, P. et al., 2013. Towards a conceptual model and reasoning structure for insider threat detection. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 4(4), pp.20–37. Available at: http://www.scopus.com/inward/record.url?eid=2-s2.0-84890952452&partnerID=tZOtx3y1.

Legg, P.A. et al., 2015. Caught in the act of an insider attack: detection and assessment of insider threat. *2015 IEEE International Symposium on Technologies for Homeland Security (HST)*, (April), pp.1–6. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7446229.

Lindauer, B. et al., 2013. Generating Test Data for Insider Threat Detectors *. *Journal of Mobile Networks, Ubiquitous Computing and Dependable Applications*, 5(2), pp.80–94.

Littlestone, N., 1988. Learning Quickly When Irrelevant Attributes Abound: A New Linear-Threshold Algorithm. *Machine Learning*, 2(4), pp.285–318.

Magklaras, G.B. & Furnell, S.M., 2002. Insider threat prediction tool: Evaluating the probability of IT misuse. *Computers and Security*, 21(1), pp.62–73.

MDF, 2011. Design of a Monitoring System Design of a Monitoring System. , 1(15), pp.1–15.

Miller, S., 2016. Insider Threat Deep Dive on IT Sabotage: Updated Statistics (Part 1 of 2). Available at: https://insights.sei.cmu.edu/insider-threat/2016/09/insider-threat-deep-dive-on-it-sabotage-updated-statistics-part-1-of-2.html [Accessed January 9, 2017].

Moore, A.P., Cappelli, D.M. & Trzeciak, R.F., 2008. The " Big Picture " of Insider IT Sabotage Across U.S. Critical Infrastructures. *Cmu/Sei-2008-Tr-009*, (May), pp.1–46.

Mundie, D.A., Perl, S. & Huth, C.L., 2013. Toward an Ontology for Insider Threat Research:

Varieties of Insider Threat Definitions. *Workshop on Socio-Technical Aspects in Security and Trust, STAST*, pp.26–36.

Najjar, T. & Hasegawa, O., 2013. Self-organizing incremental neural network (SOINN) as a mechanism for motor babbling and sensory-motor learning in developmental robotics. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 7902 LNCS(PART 1), pp.321–330.

Nurse, J.R.C. et al., 2014. Understanding Insider Threat: A Framework for Characterising Attacks. *2014 IEEE Security and Privacy Workshops*, 8533 LNCS(4), pp.214–228. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6957307%5Cnhttp://www.scopus.com/inward/record.url?eid=2-s2.0-84890952452&partnerID=tZOtx3y1.

Parveen, P. et al., 2011. Insider Threat Detection Using Stream Mining and Graph Mining. *2011 IEEE Third Int'l Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third Int'l Conference on Social Computing*, pp.1102–1110.

Roberts, S.C. et al., 2016. A Model-Based Approach to Predicting the Performance of Insider Threat Detection Systems. *2016 IEEE Security and Privacy Workshops (SPW)*, pp.314–323. Available at: http://ieeexplore.ieee.org/document/7527784/.

Schrag, R.C. et al., 2014. Processing events in probabilistic risk assessment. *CEUR Workshop Proceedings*, 1304, pp.80–87.

Schultz, E.E., 2002. A framework for understanding and predicting insider attacks. *Computers and Security*, 21(6), pp.526–531.

Shavlik, J. & Shavlik, M., 2004. Selection, combination, and evaluation of effective software sensors for detecting abnormal computer usage. *Proceedings of the 2004 ACM SIGKDD international conference on Knowledge discovery and data mining - KDD '04*, p.276. Available at: http://portal.acm.org/citation.cfm?doid=1014052.1014084.

Shen, F. & Hasegawa, O., 2010. Self-organizing incremental neural network and its application. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 6354 LNCS(PART 3), pp.535–540.

Sinclair, S. & Smith, S.W., 2008. Preventative Directions For Insider Threat Mitigation Via Access Control. *Advances in Information Security*, 39, pp.165–193. Available at: http://www.scopus.com/inward/record.url?eid=2-s2.0-84875548700&partnerID=tZOtx3y1.

Specht, D.F., 1991. A general regression neural network. *Neural Networks, IEEE Transactions on*, 2(6), pp.568–576.

Spooner, D. et al., 2009. Spotlight On : Insider Theft of Intellectual Property inside the U . S . Involving Foreign Governments or Organizations. *Intellectual Property*, (June). Available at: http://resources.sei.cmu.edu/asset_files/TechnicalNote/2013_004_001_48680.pdf%5Cnhttp://resources.sei.cmu.edu/library/asset-view.cfm?assetid=48668.

Symantec, 2016. Internet Security Threat Report VOLUME 21, APRIL 2016. *Network Security*, 21. Available at: http://linkinghub.elsevier.com/retrieve/pii/S1353485805001947.

Vesanto, J. et al., 1999. Self-organizing map in Matlab : the SOM Toolbox. *Proceedings of the Matlab DSP Conference*, pp.35–40.

Visalakshi, N.K. & Thangavel, K., 2009. Impact of normalization in distributed K-means clustering. *International Journal of Soft Computing*, 4(4), pp.168–172.

Weiland, R.M. et al., 2012. Spotlight On : Insider Threat from Trusted Business Partners. , (Version 2: Updated and Revised), pp.1–18.

Zhang, X., 2010. Support Vector Machines. *Encyclopedia of Machine Learning*, pp.941–946.