Πανεπιστήμιο Πειραιώς

Τμήμα Ψηφιακών Συστημάτων

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Τεχνοοικονομική Διοίκηση & Ασφάλεια Ψηφιακών Συστημάτων»

SECART

Ανάπτυξη Λογισμικού Συσχέτισης Συμβάντων Ασφαλείας και Λήψης Μέτρων Προστασίας

Φοιτητής	Καλοφύρης Αθανάσιος
Καθηγητής	Κωνσταντίνος Λαμπρινουδάκης
Ημερομηνία	16/11/2013

Περίληψη

Η κολοσσιαία ανάπτυξη του διαδικτύου, δημιούργησε ευκαιρίες ανάπτυξης επιχειρήσεων και οργανισμών και παρέσυρε αυτές σε μεγάλες επενδύσεις στα πληροφοριακά συστήματα. Σήμερα, δισεκατομμύρια [1] και πλέον χρήστες αλληλεπιδρούν με αυτά και μια μερίδα αυτών έχει κακόβουλο σκοπό. Τα καταγεγραμμένα συμβάντα ασφαλείας είναι τόσα πολλά [2] που μόνο με αυτοματοποιημένους τρόπους ανάλυσης και επεξεργασίας μπορούν πλέον να μελετηθούν και να υπάρξουν έγκαιρες και άμεσες αντιδράσεις. Η κατοχή λογισμικού που θα μπορεί αυτοματοποιημένα να λαμβάνει αυτά τα συμβάντα ασφαλείας, να αντιλαμβάνεται επιθέσεις και να λαμβάνει αποφάσεις για την ασφάλεια των πληροφοριακών συστημάτων αποτελεί πλέον επιτακτική ανάγκη.

Η εκπόνηση της παρούσας διπλωματικής εργασίας γίνεται στο πλαίσιο του προγράμματος μεταπτυχιακών σπουδών «Τεχνοοικονομική Διοίκηση & Ασφάλεια Ψηφιακών Συστημάτων». Σκοπός της εργασίας είναι η ανάπτυξη μιας τεχνικής λύσης υπό τη μορφή εφαρμογής ιστού που θα επεξεργάζεται συμβάντα ασφαλείας από γνωστές εφαρμογές και προϊόντα ασφαλείας , θα τα συσχετίζει βάση ορισμένων κανόνων, θα τα παρουσιάζει στον χειριστή της κατηγοριοποιημένα βάση κρισιμότητας και θα εκτελεί αν απαιτείται αυτοματοποιημένες ενέργειες απομόνωσης ή απαγόρευσης της δικτυακής οντότητας στην οποία οφείλεται η επίθεση.

Εισαγωγικά επιχειρείται μια επισκόπηση στις τεχνολογίες διαχείρισης συμβάντων ασφαλείας καθώς και στις τεχνολογίες έλεγχου δικτυακής πρόσβασης, που αποτέλεσαν και την ιδέα για την ανάπτυξης της παρούσας "Υβριδικής" λύσης. Παρουσιάζονται επίσης τα εμπορικότερα "προϊόντα" αντίστοιχων τεχνολογιών και γίνεται σύγκριση των χαρακτηριστικών τους.

Στο δεύτερο κεφάλαιο προδιαγράφονται οι απαιτήσεις της εφαρμογής και περιγράφεται η αρχιτεκτονικής της. Η εφαρμογή είναι τριεπίπεδη και γραμμένη στην αντικειμενοστραφή γλώσσα λογισμικού Java. Το πρώτο επίπεδο της εφαρμογής έχει αναπτυχθεί με την τεχνολογία

ιστού JSF και αφορά στην παρουσίαση των αποτελεσμάτων. Το δεύτερο επίπεδο περιέχει τη λογική της εφαρμογής. Εκεί η εφαρμογή ρωτά τους υπάρχοντες μηχανισμούς ασφαλείας για κρίσιμα συμβάντα. Αν υπάρχουν τα συλλέγει, τα ταξινομεί και τα τοποθετεί στη Βάση Δεδομένων της που αποτελεί και το τρίτο επίπεδο της. Αν τα συμβάντα συσχετίζονται και αθροιστικά η κρισιμότητα τους ξεπερνά το προκαθορισμένο κατώφλι, τότε η οντότητα που προκαλεί το συμβάν απομονώνεται δικτυακά.

Στα επόμενα κεφάλαια περιγράφονται με λεπτομέρειες τα δομικά στοιχεία του λογισμικού και τα συμπεράσματα της εργασίας παρουσιάζονται στην ενότητα 4.4 . Ακολουθεί η σχετική βιβλιογραφία και τα σχετικά με την εργασία παραρτήματα.

Λέξεις Κλειδιά: Κυβερνοχώρος, έλεγχος πρόσβασης, συμβάντα ασφαλείας, συσχετισμός συμβάντων ασφαλείας, ασφάλεια δικτύων και συστημάτων, εξόρυξη δεδομένων.

Περιεχόμενα

Ευρετήριο εικόνων

Ευρετήριο πινάκων

Πίνακας Ακρωνυμίων και Συντομογραφιών

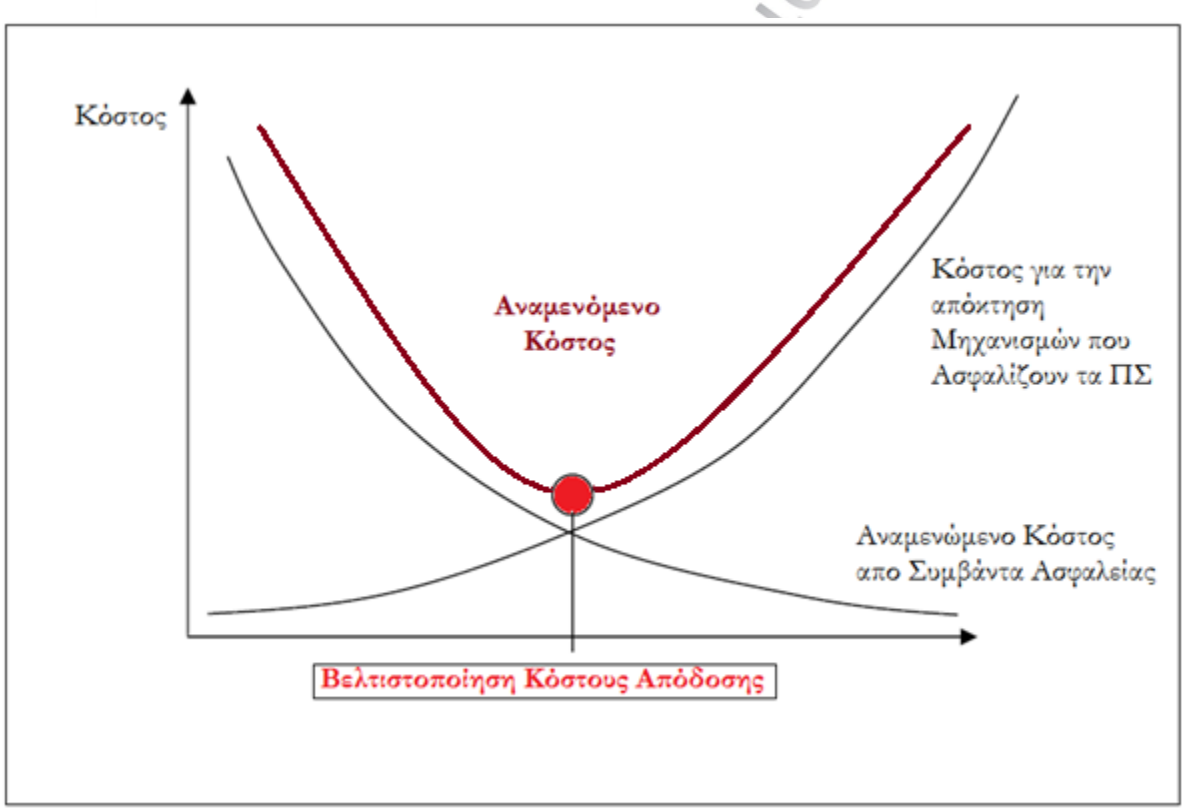
ΕΛΛΗΝΙΚΗ	
Λ.Σ.	Λειτουργικό Σύστημα
ΟΠΣ.	Ολοκληρωμένο Πληροφοριακό Σύστημα
Η.Υ.	Ηλεκτρονικός Υπολογιστής
Ο.Π.Σ.	Ολοκληρωμένο Πληροφοριακό Σύστημα
Τ.Π.Ε	Τεχνολογίες Πληροφορικής και Επικοινωνιών
ΥΑΣ	Υπεύθυνος Ασφαλείας Συστήματος
Β.Δ.	Βάση Δεδομένων
ΑΓΓΛΙΚΗ	
ACL	Access control list
AD	Active Directory
API	Application Programming Interface
AV	Antivirus
CAA	Clean Access Agent
CAM	Content Addressable Memory
CAM	Clean Access Manager
CAS	Clean Access Server
CGI	Common Gateway Interface
CIDR	Classless Inter-Domain Routing
CSS	Cascading Style Sheets
CVE	Common Vulnerabilities and Exposures
DBMS	Database Management System
DDOS	Distributed Denial of Service
DHCP	Dynamic Host Configuration Protocol
DLP	Data Loss Prevention
DNS	Domain Name System
DOS	Denial of Service
EJB	Enterprise Java Beans
FIM	File Integrity Monitoring
FTP	File Transfer Protocol
GPO	Group Policy Object
HIDS	Host Intrusion Detection System

HTTPS	Hypertext Transfer Protocol Secure
IAM	Identity and Access Management
IDS	Intrusion Detection System
IDE	Integrated Development Environment
IP	Internet Protocol
Java EE	Java Enterprise Edition
JSF	Java Server Faces
MVC	Model–view–controller
NAC	Network Access Control / Network Admission Control
SIEM	Security Information and Event Management
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSO	Single Sign On
SYSLOG	System Log
UML	Unified Modeling Language
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
WSUS	Windows Server Update Services

Πίνακας 1: Ακρωνύμια και Συντομογραφίες

1 Εισαγωγή

"Όνειρο θερινής νυκτός" αποτελεί η διαβεβαίωση, από κάποιον οργανισμό ή επιχείρηση, της ολοκληρωτικής ασφάλειας των Πληροφοριακών Συστημάτων του, ειδικά όταν αυτά συνδέονται άμεσα με το διαδίκτυο. Και αυτό γιατί η εξασφάλιση της ακεραιότητας , της εμπιστευτικότητας και της διαθεσιμότητας εξαρτάται από πληθώρα παραμέτρων, πολλές από τις οποίες για την εφαρμογή τους απαιτούν μεγάλο κόστος[1], πράγμα που τις καθιστά ασύμφορες στην εφαρμογή τους [3]. Στο παρακάτω σχήμα φαίνεται καθαρά ότι το κόστος για την απόκτηση επιπλέον μηχανισμών ασφάλισης ΟΠΣ μεγαλώνει ασύμφορα με την απόκτηση



Εικόνα 1: Η συνάρτηση Κόστους Ασφάλειας [3]

και εφαρμογή κατάλληλων μηχανισμών.

Συνηθισμένοι μηχανισμοί ασφαλείας ΟΠΣ αποτελούν σήμερα τα τείχη προστασίας [4], τα συστήματα ανίχνευσης και αποτροπής εισβολέων [5], οι σουίτες προστασίας από κακόβουλο

[1] Αφορά στο οικονομικό κόστος, ανεξάρτητα από την αιτία που το προκάλεσαι.

λογισμικό [6], το λογισμικό που διαχειρίζεται τις επιδιορθώσεις ασφαλείας (patches) άλλων λογισμικών [7] και οι μηχανισμοί που συλλέγουν συμβάντα (security logs) [8] ασφαλείας από τους εξυπηρετητές των ΟΠΣ.

Η εφαρμογή των παραπάνω μηχανισμών, στα πλαίσια της εφαρμογής ενός Συστήματος Διαχείρισης για την Ασφάλεια των Πληροφοριών, (π.χ. EN ISO 27001:05) [9], αδιαμφισβήτητα ενισχύει την ασφάλεια, αλλά συνήθως, στον "πραγματικό κόσμο" προκύπτουν δυσκολίες από την διαχείριση των ίδιων των μηχανισμών. Οι συνηθέστεροι λόγοι για αυτό είναι η πληθώρα τους και η δυσκολία στο να βρεθούν άνθρωποι με ειδικές γνώσεις που θα μπορέσουν να τα διαχειριστούν σωστά. Συνήθως οι διαχειριστές ΠΣ οργανισμών και επιχειρήσεων ασχολούνται με την λειτουργία και την συντήρηση αυτών, εστιάζοντας μόνο επιφανειακά σε συμβάντα ασφαλείας που δεν δείχνουν κρίσιμα με την πρώτη ματιά. Δεν πρέπει να ξεχνάμε και τον παράγοντα ωράριο εργασίας, το προσωπικό που έχει την τεχνογνωσία για την ορθή αναγνώριση και αντιμετώπιση εξελιγμένων επιθέσεων, συνήθως απουσιάζει.

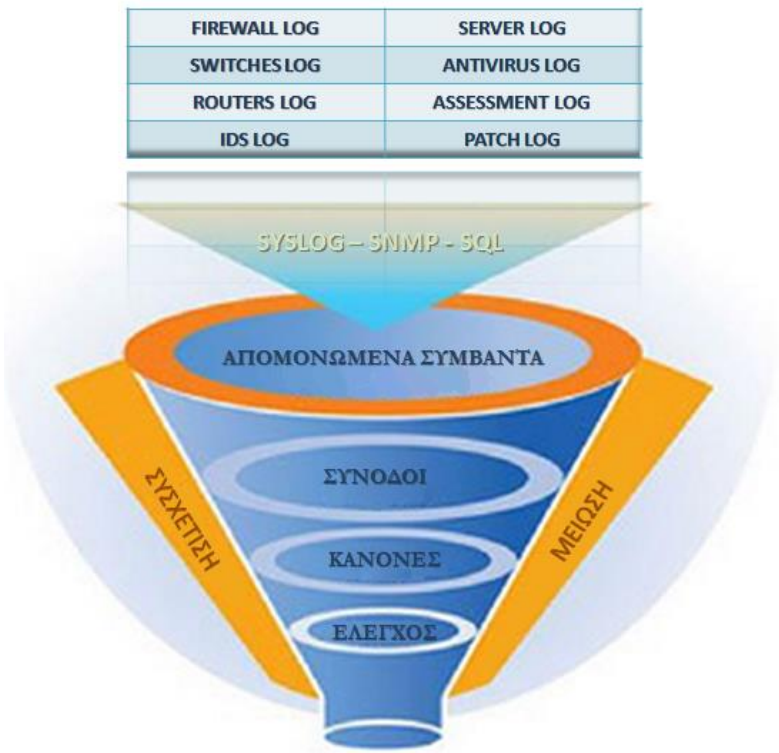
Φαίνεται λοιπόν καθαρά η ανάγκη για την ανάπτυξη νέων προϊόντων ασφαλείας που θα μπορούν να προσαρμόζονται εύκολα στις υπάρχουσες δικτυακές υποδομές, θα μπορούν να συνεργάζονται με τους υπάρχοντες μηχανισμούς ασφαλείας, να συσχετίζουν τα συμβάντα που συγκέντρωσαν (πχ Firewall , Antivirus, Patch Server) και αντιμετωπίζουν όσα εκτιμούνται ως κρίσιμα. Και όλα τα παραπάνω αυτοματοποιημένα σε χρονικό πλαίσιο 24x7.

Ανάγκη για Συνεχόμενη Παρακολούθηση Συμβάντων Ασφαλείας

Ακόμη και σήμερα, ελάχιστες εταιρείες ή οργανισμοί παρακολουθούν σε χρόνο 24x7 τα συμβάντα ασφαλείας που παράγουν οι μηχανισμοί ασφαλείας των ΟΠΣ τους. Οι ποιο συνηθισμένοι μηχανισμοί και διατάξεις ασφαλείας είναι:

- ACL σε Routers
- Security controls σε Switches
- Firewalls
- HIDS,NIDS,HIPS,NIPS
- VPN Aggregators

- Antivirus
- Vulnerability Assessment Tools
- Patch Management Applications
- Content scanning applications,
- Server/WorkStation Security Events



Εικόνα 2: Πηγές Συμβάντων Ασφαλείας

Κάθε συσκευή ή εφαρμογή από τις διατάξεις ασφαλείας μπορεί να παραγάγει σε ημερήσια βάση εκατοντάδες γραμμές από συμβάντα. Από τη μία πλευρά, η έρευνα για συγκεκριμένα συμβάντα συνήθως καθίσταται δύσκολη και χρονοβόρα. η απόκριση από την άλλη πρέπει να είναι άμεση και σχεδόν σε πραγματικό χρόνο.

Συσχετισμός Συμβάντων Ασφαλείας

Ορισμός

Ορίζουμε σαν συσχετισμό συμβάντων ασφαλείας την διεργασία που γίνεται στα συμβάντα ασφαλείας που προέρχονται από όλες τις διατάξεις ασφαλείας του ΟΠΣ και που έχει ως σκοπό

την εξακρίβωση πιθανών συσχετίσεων και μοτίβων που αποτελούν ένδειξη κακόβουλης επίθεσης σε αυτά [10]. Ως εναλλακτικό ορισμό θα μπορούσαμε να ισχυριστούμε την διαδικασία που εφαρμόζεται στα συμβάντα ασφαλείας και που έχει σκοπό μέσα από την ομαδοποίησή τους να μειώσει την ποσότητά τους αλλά να αυξήσει την ποιότητά τους[11].

Αναλυτικότερα, τα συσχετιζόμενα συμβάντα ομαδοποιούνται ως συνδυασμένα συμβάντα, τα οποία είναι σαφώς περιορισμένα σε σχέση με τον όγκο των αρχικών. Γίνεται χρήση των μεταδιδομένων τους (χρόνος, τοποθεσία, είδος, συσκευή από την οποία προσήλθαν,) Επιπρόσθετα αποδίδεται σε αυτά μια τιμή προτεραιότητας και ανάλογος της κρισιμότητας και της επεξεργασίας που επιδέχονται λαμβάνεται ή όχι κάποια αυτοματοποιημένη ενέργεια για ειδοποίηση ή άμεση προστασία.

Συστατικά

Τα κύρια συστατικά του συσχετισμού συμβάντων ασφαλείας είναι: Φιλτράρισμα, Συγχώνεψη, Απόκρυψη και Επεξεργασία για εύρεση συσχετισμών [12]. Αναλυτικότερα:

Το **Φιλτράρισμα** αφορά στη απόρριψη συμβάντων που κρίνονται άσχετα με την ενέργεια κάποιας κακόβουλης επίθεσης. Τέτοια συμβάντα είναι συνήθως συμβάντα που αφορούν στην διαθεσιμότητα. Για παράδειγμα ένα συμβάν που αναφέρει περιοδικά ότι το κύριο τροφοδοτικό μιας δικτυακής συσκευής έπαψε να λειτουργεί.

Η **Συγχώνεψη** αφορά στην διαγραφή των διπλότυπων. Για παράδειγμα το ίδιο γεγονός στέλνεται ξανά και ξανά από την πηγή προέλευσης μέχρι να λυθεί το πρόβλημα.

Η **Απόκρυψη** συνίσταται στη παράβλεψη των συμβάντων που δημιουργούνται από κάποια γνωστή αιτία, όπως για παράδειγμα κάποιος έλεγχος ευπαθειών από τον ΥΑΣ ή κάποιος προβληματικός δρομολογητής.

Η **Επεξεργασία** αφορά στην ανάλυση των συμβάντων βάση κάποιας λογικής (κανόνων ή μοντέλου) για εύρεση εξαρτήσεων.

Απαραίτητη προϋπόθεση για σωστή συσχέτιση συμβάντων αποτελεί η ύπαρξη ακριβούς εξυπηρετητή χρόνου (NTP Server)[13].

Κατηγορίες - Μεθοδολογίες

Υπάρχουν τρεις μεθοδολογίες για την συσχέτιση συμβάντων [14]:

- Συσχέτιση **Βασισμένη σε Μοντέλα** (Model Based). Αφορά στη δημιουργία πολύπλοκων συσχετισμών, με απλές κινήσεις από πλευράς χρήστη. Η ανάπτυξη ενός τέτοιου συστήματος είναι δύσκολή αλλά δίνει το πλεονέκτημα της ευελιξίας.

- Συσχέτιση **Βασισμένη σε Κανόνες** (Rule Based) Δίνει την δυνατότητα προσθήκης λογικής και ευφυΐας στο σύστημα σχετικά με την διεύρυνση των συμβάντων χωρίς την ανάγκη προγραμματιστικής γνώσης.

- Συσχέτιση **Βασισμένη σε Πολιτικές** (Policy Based). Μοιάζει σαν την μεθοδολογία που βασίζεται σε κανόνες, αλλά προσεγγίζει το θέμα ποιο γενικά. Παράδειγμα αν σε κάποιο υποδίκτυο το τοίχος προστασίας καταγράφει πακέτα αναζήτησης συγκεκριμένων ευάλωτων υπηρεσιών από πολλές εσωτερικές διευθύνσεις, τότε αποφαίνεται ότι υπάρχει γενικευμένη μόλυνση στο δίκτυο.

Γενικά μπορούμε να ισχυριστούμε ότι υπάρχουν δύο κατηγορίες συσχετισμού συμβάντων ασφαλείας [15]: Βασισμένη σε κανόνες (ruled based) ή σε στατιστικές μεθόδους και αλγορίθμους (statistical/algorithmic).

- Οι **κανόνες** αποτελούν προϋπάρχουσα γνώση και ταύτιση σε κανόνα καθορίζει με ακρίβεια το τύπο του συμβάντος που εξελίχθηκε. Μπορεί να είναι πραγματικού χρόνου (Real Time Rule Based Correlation) αν κρατούν πληροφορίες στην μνήμη ενός συστήματος η να αποθηκεύουν αυτές τις πληροφορίες σε μια Βάση Δεδομένων(Database rule-based correlation).

- Οι **στατιστικές μέθοδοι** δεν βασίζονται σε προϋπάρχουσα γνώση αλλά σε γνώση που αποκτάται από «κανονικές» δραστηριότητες στο δίκτυο. Ένα συμβάν ασφαλείας θα διαφέρει από τις συνηθισμένες δραστηριότητες, που έχουν γνωστά πρότυπα (pattern). Αναζητούν για αποκλείσεις από δικτυακά μοτίβα που θεωρούνται ως κανονικά. Οι αποκλίσεις μπορούν να εντοπισθούν σε πραγματικό χρόνο ή με ιστορικότητα από αποθηκευμένα δεδομένα.

Η διαχείριση των συσχετισμένων αρχείων καταγραφής ασφαλείας (SIM) έχει καθιερωθεί πλέον ως όρος στη ασφάλεια ψηφιακών συστημάτων [16] και οι τεχνολογίες που υιοθετούν τις παραπάνω μεθοδολογίες εφαρμόζονται σήμερα σε εργαλεία λογισμικού γνωστά ως SIEM [17].

Ανάγκη για Έλεγχο πριν την Πρόσβαση στο Εσωτερικό Δίκτυο

Ας υποθέσουμε ένα σενάριο: Είμαστε υπεύθυνοι ασφαλείας σε κάποιο εταιρικό δίκτυο. Κάποιος Η/Υ συνδέεται σε αυτό. Τι θα συμβεί αν είναι μολυσμένος, τι θα πρέπει να κάνουμε αν είναι "άγνωστος", αν δεν ανήκει σε ένα σύνολο Η/Υ που έχουμε εφαρμόσει ένα σύνολο από συγκεκριμένες πολιτικές ασφαλείας; Διακρίνεται λοιπόν η ανάγκη για την δημιουργία ενός μηχανισμού ασφαλείας που θα εξασφαλίζει ότι αν κάποιος Η/Υ συνδεθεί σε κάποιο εταιρικό δίκτυο, δεν θα πρέπει να έχει πρόσβαση σε καμία υπηρεσία εκτός και αν συμμορφώνεται με τις πολιτικές ασφαλείας του οργανισμού, το επίπεδο ενημερώσεων ασφαλείας του Λειτουργικού Συστήματος και το επίπεδο προστασίας από κακόβουλο λογισμικό.

Συστήματα Ελέγχου της Πρόσβασης στο Εσωτερικό Δίκτυο

Ορισμός

Ο έλεγχος πρόσβασης στο δίκτυο (Network Access Control ή Network Admission Control) αποτελεί μια μέθοδο ενίσχυσης της ασφάλειας ενός δικτύου, περιορίζοντας την διαθεσιμότητα των πόρων του δικτύου στα τερματικά των χρηστών, σε σχέση με την καθορισμένη πολιτική ασφαλείας [17].

Ο έλεγχος πρόσβασης στο δίκτυο (Network Access Control) αποτελεί μια σύγχρονη λύση στο πεδίο της ασφάλειας Η/Υ και Δικτύων και αποσκοπεί στην ενοποίηση τεχνολογιών ασφαλείας τερματικών (όπως το λογισμικό προστασίας από κακόβουλο λογισμικό, το λογισμικό ανίχνευσης εισβολέων και τα αποτελέσματα από ελέγχους τρωτότητας κ.α) με τεχνολογίες αυθεντικοποίησης και τεχνολογίες επιβολής πολιτικής ασφαλείας δικτύου [17].

Ιστορικό

Οι τεχνολογίες NAC είναι σχετικά νέες. Στις αρχές του 2003 έγινε η πρώτη μαζική υιοθέτηση τους από τη Cisco και τη Microsoft (δες "Strategic Road Map for Network Access Control") με βασική φιλοσοφία τον έλεγχο των ρυθμίσεων ασφαλείας στους τερματικούς κόμβους του εκάστοτε δικτύου. Ποιο συγκεκριμένα γινόταν έλεγχος στα τερματικά για πιθανή απουσία κάποιων διορθώσεων ασφαλείας του λειτουργικού συστήματος καθώς και για την ύπαρξη των

ποιό σύγχρονων ενημερώσεων στο λογισμικό προστασίας από κακόβουλες απειλές (antivirus). Αυτή η προσέγγιση διήρκησε έως το 2006.

Γύρω στο 2007, τα NAC διαβαίνουν την δεύτερη φάση της ανάπτυξης τους. Η νέα προσέγγιση βασίστηκε στην χρήση γνωστών μηχανισμών αυθεντικοποίησης και τη δημιουργία ενός υποδικτύου για «επισκέπτες» (Guest VLAN) για τις δικτυακές οντότητες που χαρακτηρίζονται ως μη διαχειρίσιμες.

Το 2011 η τεχνολογία των NAC μπαίνει στην τρίτη φάση της, που συνδυάζει τις δύο προηγούμενες. Η διαφορά είναι ότι για τις μη διαχειρίσιμες συσκευές δημιουργείται μια «ζώνη περιορισμένης πρόσβασης» σε αυστηρά ελεγχόμενες υπηρεσίες.

Συστατικά

Στα βασικά συστατικά που χαρακτηρίζουν κάθε NAC σύστημα θα πρέπει να περιέχεται η δυνατότητά του να ανακαλύπτει νέες δικτυακές οντότητες (π.χ. Η/Υ) και η δυνατότητα του να ελέγχει αν η συγκεκριμένη οντότητα συμμορφώνεται με την πολιτική ασφαλείας του οργανισμού. Αν δεν συμμορφώνεται το σύστημα NAC θα πρέπει να μπορεί να περιορίσει την πρόσβαση της οντότητας στο δίκτυο. Γενικά, τα συστατικά που ενδέχεται να περιλαμβάνουν λύσεις NAC είναι[18]:

- **Ανίχνευση για Δικτυακές Οντότητες:** Άμεση ανίχνευση με την εισαγωγή τους στο δίκτυο.
- **Αυθεντικοποίηση:** Με ενσωματωμένο μηχανισμό, ανεξάρτητα από άλλους μηχανισμούς αυθεντικοποίησης.
- **Διερεύνηση του επίπεδου ασφαλείας:** Ελέγχει αν η νέα οντότητα συμμορφώνεται ή όχι με την πολιτική ασφαλείας του οργανισμού. Συνήθως γίνεται έλεγχος του Λ.Σ και του επιπέδου ενημέρωσης αυτού και έλεγχος ύπαρξης προστασίας από κακόβουλο λογισμικό.
- **Απομόνωση:** Τοποθετεί την οντότητα που δεν πληροί τις απαιτήσεις τις πολιτικής ασφαλείας σε προστατευμένη περιοχή του δικτύου.
- **Αποκατάσταση:** Στην προστατευμένη περιοχή του δικτύου η οντότητα παραμένει έως ότου αναγνωριστεί και αρμονιστεί με την αντίστοιχη πολιτική δικτύου. Αυτό μπορεί να γίνει αυτοματοποιημένα ή όχι.

- **Εξουσιοδότηση:** Ταυτοποιεί την δικτυακή οντότητα ή και τον χρήστη. Ανάλογα με το αποτέλεσμα την επαλήθευση τοποθετεί την οντότητα σε κατάλληλο υποδίκτυο με ορισμένες προσβάσεις στα ΟΠΣ του οργανισμού.
- **Προστασία:** Οι δικτυακές οντότητες παρακολουθούνται συνεχώς για πιθανή ύποπτη από πλευράς ασφαλείας δραστηριότητα. Αν βρεθεί κάποια (όπως για παράδειγμα μόλυνση από κάποιο δικτυακό σκουλήκι) τότε λαμβάνονται και ανάλογα μέτρα προστασίας (π.χ. απομόνωση).

Εικόνα 3: Συστατικά Στοιχεία Συστήματος NAC

Κατηγορίες - Μεθοδολογίες

Τα NAC ανάλογα με την μεθοδολογία που χρησιμοποιούν για να προστατέψουν το δίκτυο μπορούν να κατηγοριοποιηθούν σε δύο μεγάλες κατηγορίες:

- Εκείνα που χρησιμοποιούν κάποιο ενδιάμεσο λογισμικό ασφαλείας τύπου πράκτορα (agent-based) για την επίτευξη των λειτουργιών τους και
- εκείνα που δεν χρησιμοποιούν ενδιάμεσο λογισμικό ασφαλείας τύπου πράκτορα (agent-less) για την επίτευξη των λειτουργιών τους. Βέβαια υπάρχουν και μικτές λύσεις [19].

Αναλυτικότερα:

Χωρίς χρήση ενδιάμεσου λογισμικού ασφαλείας τύπου πράκτορα:

- **Τεχνικές Ανίχνευσης Βασισμένες στο Δίκτυο**: Με πληροφορίες που προκύπτουν από τις υπάρχουσες διατάξεις ασφαλείας, καθώς και με συνεχείς δικτυακούς ελέγχους τρωτότητας με εργαλεία όπως το nessus vulnerability scanner [20], και το msba [21] εξάγονται συμπεράσματα για την κατάσταση από πλευράς ασφαλείας των δικτυακών οντοτήτων. Δεν απαιτείται κάποια ειδική παραμετροποίηση στην οντότητα που ανιχνεύεται. Απαιτείται απενεργοποίηση του τοίχους προστασίας για να γίνει έλεγχος από τις διατάξεις του NAC.
- **Τεχνικές Ανίχνευσης Βασισμένες σε Μικρό-εφαρμογή Ιστού (Applet/ActivX):** Η νέα δικτυακή οντότητα αναγκάζεται με κατάλληλη τεχνική να "κατεβάσει" κάποια μικροεφαρμογή (όπως Java Applet ή ActiveX Control) από εσωτερική τοποθεσία ιστού που έχει φτιαχτεί επί τούτου. Η εφαρμογή τρέχει στο σύστημα, το ελέγχει ως προς την πολιτική ασφαλείας του οργανισμού και αναλόγως αποτελέσματος επιτρέπει ή όχι την πρόσβαση.

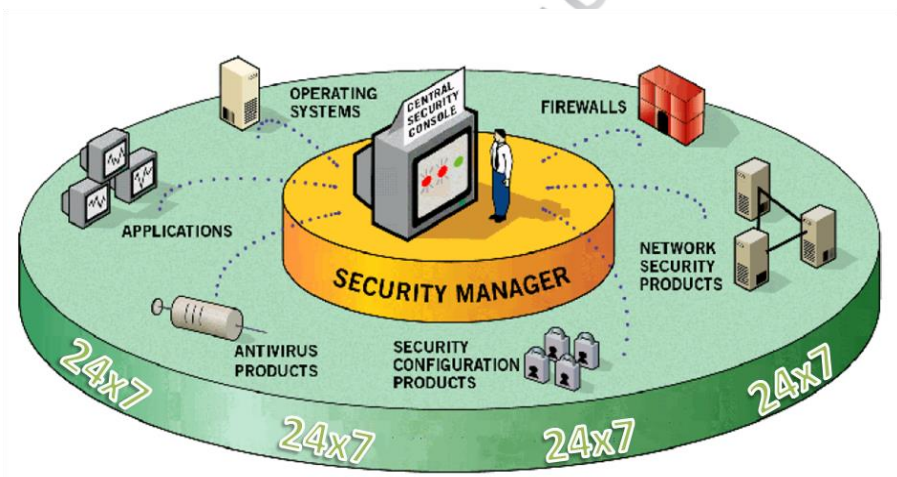
Με χρήση ενδιάμεσου λογισμικού ασφαλείας τύπου πράκτορα:

- **Τεχνικές χρήσης "*Thin Agent*":** Είναι λογισμικό που προεγκαθίσταται στις δικτυακές οντότητες από τον αντίστοιχο NAC σύστημα, απασχολεί ελάχιστους πόρους στο σύστημα που εγκαθίσταται και επικοινωνεί συνεχώς με κατάλληλο εξυπηρετητή της υποδομής NAC.
- **Τεχνικές χρήσης "*Thick Agent*":** Είναι λογισμικό που προεγκαθίσταται στις δικτυακές οντότητες από τον αντίστοιχο NAC σύστημα, απασχολεί αρκετούς πόρους στο σύστημα που εγκαθίσταται. Συνήθως το ίδιο παρέχει δυνατότητες απομόνωσης (για παράδειγμα όπως ένα HIDS). Επικοινωνεί συνεχώς με κατάλληλο εξυπηρετητή της υποδομής NAC.

2 SIEM

Διαχείριση Συμβάντων Ασφαλείας

Η διαχείριση των συμβάντων ασφαλείας ως έννοια είναι σχετικά νέα. Χρησιμοποιήθηκε για πρώτη φορά από μια μικρή εταιρεία με την ονομασία " E-Security" το 1999 [22]. Έκτοτε και ως σήμερα έχει αναπτυχτεί σε μεγάλο βαθμό και συνέχεια αναπτύσσεται. Για να γίνει εφικτή πρέπει όλα τα αρχεία καταγραφής να συγκεντρωθούν σε μια κοινή βάση. Στην εικόνα 3 φαίνεται ότι όλα τα αρχεία καταγραφής συγκεντρώνονται σε κάποια κεντρική βάση δεδομένων για να υποστούν την επεξεργασία που περιγράψαμε στην παράγραφο 1.2 και να παρουσιάσουν το επιθυμητό αποτέλεσμα.



Εικόνα 4: Οπτική αναπαράσταση της Διαχείρισης Συμβάντων Ασφαλείας

Ανάλογα με την υλοποίηση, για την συγκέντρωση των επιθυμητών δεδομένων χρησιμοποιούνται συνήθως διαδεδομένα πρωτόκολλα συλλογής πληροφοριών όπως τα: *Syslog, SNMP* και επερωτήσεις *SQL* . Τα συμβάντα ασφαλείας συγκεντρώνονται σε βάση δεδομένων που παρέχει τα κάτωθι πλεονεκτήματα:

- Υπάρχει μόνο μια κεντρική διεπαφή για την πρόσβαση σε όλα τα αρχεία καταγραφής.
- Παρέχεται η δυνατότητα προστασίας των συμβάντων λόγω κεντρικοποίησης
- Μπορεί να γίνει συμπίεση
- Μπορούν να εφαρμοστούν εύκολα τεχνικές εξόρυξης δεδομένων

- Τα συμβάντα κατηγοριοποιούνται βάση κρισιμότητας
- Γίνεται δυνατή η συσχέτιση των συμβάντων μεταξύ διαφορετικών συστημάτων
- Η διατήρηση των συμβάντων σε δύο μέρη ταυτόχρονα αποκλείει την περίπτωση ηθελημένης ή αθέλητης διαγραφής αυτών από το σύστημα που τα παρήγαγε.

Κατά την επεξεργασία των συγκεντρωμένων συμβάντων θεωρείται απαραίτητη η προσθήκη παραμέτρων από τρίτες πηγές που μπορούν να επαυξήσουν τις δυνατότητες εντοπισμού πραγματικά κρίσιμων συμβάντων. Τέτοιοι παράμετροι μπορούν να είναι η αξία του πόρου που δέχεται την επίθεση για τον οργανισμό ή τα αποτελέσματα από έναν πρόσφατο έλεγχο ασφαλείας (vulnerability scanning)[15].

Μια ιδέα για τον τρόπο λειτουργίας του συστήματος εντοπισμού συμβάντος: Για παράδειγμα αν μια επίθεση δεν ανιχνευτεί από το IDS αλλά υπάρχουν από άλλα συστήματα ενδείξεις όπως εγκατάσταση λογισμικού σε κάποιον εξυπηρετητή και άνοιγμα μιας πόρτας για έναρξη επικοινωνίας, τότε το σύστημα συσχετισμού συμβάντων θα πρέπει να είναι σε θέση καταδείξει την επίθεση.

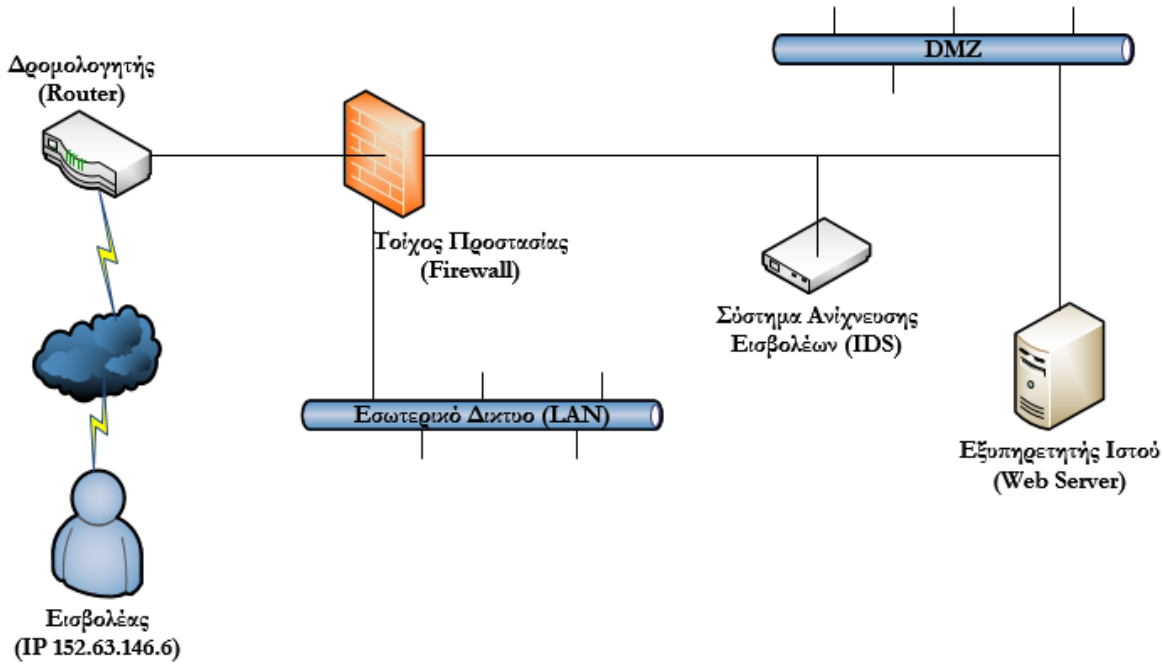
Δεν θα πρέπει το σύστημα να υπερφορτώνεται με κανόνες που δεν βασίζονται σε καλή γνώση της τοπολογίας και των υπηρεσιών που υπάρχουν στο δίκτυο. Η υπερφόρτωση γενικών κανόνων οδηγεί συχνά σε λάθους συναγερμούς (false positives). Επιπρόσθετα η υπερφόρτωση κανόνων απαιτεί τη δέσμευση πολλών υπολογιστικών πόρων. Λύση στα παραπάνω προβλήματα είναι μια μηχανή συσχετισμού συμβάντων με δυνατότητες βελτιστοποίησης ανάλογα με το περιβάλλον που χρησιμοποιείται.

Τέλος θα πρέπει να διευκρινιστεί ότι τα SIEM ως εργαλεία για να αποδώσου σωστά απαιτούν και το προσωπικό που τα χρησιμοποιεί να έχει τις αντίστοιχες δεξιότητες. Οι αναλυτές συμβάντων ασφαλείας (security analyst) εφαρμόζουν τις απαιτήσεις του επιχειρησιακού περιβάλλοντος στις ρυθμίσεις του SIEM. Εύκολα όμως, μπορεί ο όγκος των συμβάντων ασφαλείας να ξεπεράσει τις δυνατότητες ανάλυσης του αναλυτή. Αυτή η περίπτωση συμβαίνει στο σενάριο που γίνεται αλόγιστη συλλογή συμβάντων από τις διατάξεις ασφαλείας του οργανισμού, που καταλήγει σε αλόγιστη συγκέντρωση μη αξιοποιήσιμης πληροφορίας. Έτσι ο ρόλος του αναλυτή απαιτεί γνώση των επιχειρησιακών διαδικασιών, των πολιτικών ασφαλείας του οργανισμού και των τεχνολογιών και εφαρμογών που χρησιμοποιούνται από τα ΟΠΣ στα

πλαίσια του οργανισμού. Με αυτές τις γνώσεις ο αναλυτής θα μπορέσει να απομονώσει σε χρόνο αποδεκτό τα χρήσιμα δεδομένα από τον θόρυβο.

Σενάριο Χρήσης SIEM

Για να γίνει ευκολότερη η κατανόηση του τρόπου λειτουργίας των SIEM παραθέτουμε το εξής σενάριο: Στο δίκτυο της εικόνας 5, θα γίνει μια απόπειρα εισβολής από τον επιτιθέμενο χάκερ στον εξυπηρετητή ιστού. Τα συμβάντα που θα δημιουργηθούν, αν εξεταστούν ανεξάρτητα δεν θα είναι ικανά να παρουσιάσουν το εύρος και το αποτέλεσμα της επίθεσης. Αν όμως συσχετιστούν με κάποιον μηχανισμό SIEM θα καταδείξουν άμεσα τις λεπτομέρειες της επίθεσης.



Εικόνα 5: Συσχετισμός Συμβάντων με SIEM σε Απλό Δίκτυο

Στο τυπικό δίκτυο της εικόνας 5, έχουμε ενεργοποιήσει την καταγραφή συμβάντων στις συσκευές του δρομολογητή, του τοίχους προστασίας, του συστήματος ανίχνευσης εισβολέων και τέλος του εξυπηρετητή ιστού. Όλα τα παραπάνω συμβάντα αποστέλλονται προς ανάλυση στο SIEM.

Διατάξεις Ασφαλείας - Μέτρα Ασφαλείας

Οι διατάξεις και τα μέτρα ασφαλείας που έχουν ληφθεί, ανάλογα με την συσκευή, είναι:

- **Δρομολογητής:** Υπάρχουν λίστες ελέγχου πρόσβασης (ACLs) που παρέχουν την πρώτη γραμμή άμυνας του δικτύου. Η παρούσα λίστα επιτρέπει μόνο υπηρεσίες ιστού, οπότε οποιαδήποτε άλλη αναζήτηση υπηρεσίας από το Διαδίκτυο, θα απορριφτεί και θα καταγραφεί στα συμβάντα καταγραφής του (log file) του. Στην περίπτωσή μας είναι τύπου Cisco.
- **Τοίχος προστασίας:** Δίνει την δυνατότητα ελέγχου σε επίπεδο εφαρμογής των δικτυακών πακέτων που περνάνε μέσα από αυτό. Επιπλέον μας δίνει τη δυνατότητα αναλυτικής καταγραφής συμβάντων ασφαλείας. Στην περίπτωσή μας είναι τύπου Linux/sguil
- **Σύστημα ανίχνευσης εισβολέων:** Μπορεί να ανιχνεύσει ύποπτη δικτυακή συμπεριφορά, βασισμένη σε γνωστά μοτίβα και πρότυπα επιθέσεων ή σε στατιστική ανάλυση του δικτύου. Σε αυτή την περίπτωση δημιουργεί προειδοποιητικά μηνύματα (Alerts) και τα αποθηκεύει στη Β.Δ του. Συνήθως όμως παράγει πολλούς λανθασμένους συναγερμούς (false positives) και σε αυτό το σημείο η συσχέτιση συμβάντων θα φανεί απαραίτητη. Στην περίπτωσή μας είναι τύπου Linux/snort
- **Εξυπηρετητής ιστού**: Παρέχει υπηρεσίες ιστού, προσβάσιμες από το διαδίκτυο. Βρίσκεται σε διακριτό λογικά χώρο του δικτύου, που αποκαλείται αποστρατικοποιημένη ζώνη (DMZ). Συνήθως αποτελεί στόχο κακόβουλων επιθέσεων. Πολλές φορές ο στόχος της επίθεσης είναι η περαιτέρω διείσδυση στο εσωτερικό δίκτυο. Είναι σημαντικό να ενεργοποιηθεί η καταγραφή συμβάντων κατά την διάρκεια όλων των συνόδων και να αποστέλλονται αυτά στο SIEM σύστημα. Στην περίπτωσή μας είναι τύπου Linux/Apache

Ευπάθειες Εξυπηρετητή Ιστού

Στο παρόν σενάριο ο επιτιθέμενος θα αναζητήσει για τρεις γνωστές ευπάθειες, τις:

- *CVE-1999-0067: CGI phf:* Επιτρέπει απομακρυσμένη εκτέλεση εντολών μέσα από μεταχαρακτήρες[23].
- *CVE-1999-0172: FormMail CGI:* Μέσου αυτού επιτρέπει την απομακρυσμένη εκτέλεση εντολών στον εξυπηρετητή ιστού[24].

- *CVE-1999-0936 BNB survey.cgi:* Το συγκεκριμένο CGI επιτρέπει την εκτέλεση απομακρυσμένων εντολών στον εξυπηρετητή ιστού μέσα από μεταχαρακτήρες[25].

Καταγραφή των συμβάντων από κάθε συσκευή

Δρομολογητής:

```
...
May 31 09:27:44 router.company.com 1410875: May 31 09:27:43: %SEC-6-IPACCESSLOGP: list from-internet
denied       tcp       152.63.146.6(1459)       ->       xxx.yyy.zzz.1(80),       1       packet

May 31 09:27:50 router.company.com 1410880: May 31 09:27:50: %SEC-6-IPACCESSLOGP: list from-internet
denied       tcp       152.63.146.6(1673)       ->       xxx.yyy.zzz.2(80),       1       packet

May 31 09:27:54 router.company.com 1410883: May 31 09:27:53: %SEC-6-IPACCESSLOGP: list from-internet
denied      tcp      152.63.146.6(1750)      ->      xxx.yyy.zzz.3      (80),      1       packet

May 31 09:27:57 router.company.com 1410885: May 31 09:27:56: %SEC-6-IPACCESSLOGP: list from-internet
denied       tcp       152.63.146.6(1722)       ->       xxx.yyy.zzz.5(80),       1       packet

May 31 09:27:58 router.company.com 1410886: May 31 09:27:57: %SEC-6-IPACCESSLOGP: list from-internet
denied       tcp       152.63.146.6(1930)       ->       xxx.yyy.zzz.6(80),       1       packet

May 31 09:28:01 router.company.com 1410888: May 31 09:28:00: %SEC-6-IPACCESSLOGP: list from-internet
denied       tcp       152.63.146.6(1976)       ->       xxx.yyy.zzz.7(80),       1       packet

May 31 09:28:05 router.company.com 1410891: May 31 09:28:04: %SEC-6-IPACCESSLOGP: list from-internet
denied       tcp       152.63.146.6(2167)       ->       xxx.yyy.zzz.8(80),       1       packet
.
.                                        <data                                        pruned>
.
```

Πίνακας 2: Καταγραφή Συμβάντων από Δρομολογητή

Παρατηρούμε ότι από την Δνση: *152.63.146.6* στις 31 Μαϊ 0927 γίνεται απόπειρα σύνδεσης στο δίκτυο *xxx.yyy.zzz.0/24*. Ο δρομολογητής έχει καταγράψει μόνο τις αρνήσεις πρόσβασης, μιας και είναι ρυθμισμένος να επιτρέπει την πρόσβαση στον εξυπηρετητή με Δνση: *xxx.yyy.zzz.4* . Εν συντομία θα λέγαμε ότι από τα συμβάντα καταγραφής ο χρήστης με IP Δνση: *152.63.146.6* ψάχνει σε όλο το δίκτυο κλάσης C για εξυπηρετητές ιστού (πόρτα 80). Μόνο με αυτά τα συμβάντα καταγραφής δεν γνωρίζουμε τι έχει συμβεί περαιτέρω. Περιληπτικά οι πληροφορίες που αντλούνται από τα παραπάνω αρχεία καταγραφής φαίνονται στον πίνακα 3.

Συσκευή	Δρομολογητής
Ποιός:	152.63.146.6
Τι:	Αναζήτηση για εξυπηρετητές ιστού στο δίκτυο xxx.yyy.zzz.0/24. Πιθανή εύρεση του xxx.yyy.zzz.4

Πότε:	31 Μάι στις 0927 με 0928
Που:	Στο DMZ δίκτυο του οργανισμού
Γιατί	Πιθανώς για αναγνώριση

Πίνακας 3: Αποτελέσματα επεξεργασίας αρχείων καταγραφής Δρομολογητή

Τοίχος προστασίας:

```
...

Jun 1 06:08:50 firewall.company.com http-gw[29142]: log host=nodnsquery/152.63.146.6 protocol=http
cmd=get              dest=xxx.yyy.zzz.4              path=/cgi-bin/phf              ID=29142174970

Jun 1 06:08:54 firewall.company.com http-gw[29142]: log host=nodnsquery/152.63.146.6 protocol=http
cmd=get            dest=xxx.yyy.zzz.4            path=/cgi-bin/formmail            ID=29142174971

Jun 1 06:08:58 firewall.company.com http-gw[29142]: log host=nodnsquery/152.63.146.6 protocol=http
cmd=get dest=xxx.yyy.zzz.4 path=/cgi-bin/survey.cgi ID=29142174972

...
```

Πίνακας 4: Καταγραφή Συμβάντων από το Τοίχος Προστασίας

Παρατηρούμε ότι από την Δνση: *152.63.146.6* στις 1 Ιουν 0608 επιτράπηκαν συνδέσεις προς τον εξυπηρετητή του οργανισμού. Ποιό συγκεκριμένα φαίνεται από την URL των αρχείων καταγραφής ότι ζητήθηκαν τα παρακάτω CGI: *phf,formmail,* και *survey.cgi* . Δεν γνωρίζουμε αν οι απόπειρες πρόσβασης είναι πετυχημένες και ποιό το αποτέλεσμά τους (για παράδειγμα, αν δεν έχουμε υπόψη μας τις συγκεκριμένες ευπάθειες, θεωρούμε τις συνδέσεις νόμιμες). Γνωρίζουμε μόνο ότι επιτράπηκαν. Περιληπτικά οι πληροφορίες που αντλούνται από τα παραπάνω αρχεία καταγραφής φαίνονται στον πίνακα 5.

Συσκευή	Τοίχος Προστασίας
Ποιός:	152.63.146.6
Τι:	Τρεις http συνδέσεις στον εξυπηρετητή ιστού με Δνση IP xxx.yyy.zzz.4 .Απόπειρα πρόσβασης στα CGI: *phf,formmail,* και *survey. Δεν γνωρίζουμε αν τελικά ήταν πετυχημένη η πρόσβαση. Επίσης Δεν υπάρχουν άλλα στοιχεία πρόσβασης από αυτή τη Δνση*
Πότε:	1 Ιουν 0608 - 0609

Που:	Στο DMZ δίκτυο του οργανισμού
Γιατί	Αρχικά Άγνωστο. Μετά από έρευνα γίνεται κατανοητό ότι πρόκειται για κακόβουλη ενέργεια μιας και αφορά στην εκμετάλλευση ευπαθειών, που τελικά επιτρέπουν την απομακρυσμένη εκτέλεση εντολών.

Πίνακας 5: Αποτελέσματα επεξεργασίας αρχείων καταγραφής Τοίχους Προστασίας

Σύστημα ανίχνευσης εισβολέων:

```
...
[**] [1:886:3] WEB-CGI phf access [**]
[Classification: Attempted Information Leak] [Priority: 2]
06/01-06:08:50.764332 152.63.146.6:3308 -> xxx.yyy.zzz.4:80
TCP TTL:52 TOS:0x0 ID:61884 IpLen:20 DgmLen:280 DF
***AP*** Seq: 0x591AF831 Ack: 0x92D23FAF Win: 0x16D0 TcpLen: 32
TCP Options (3) => NOP NOP TS: 59902357 300726
[Xref => http://www.securityfocus.com/bid/629]
[Xref => http://www.whitehats.com/info/IDS128]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0067]

[**] [1:884:2] WEB-CGI formmail access [**]
[Classification: Attempted Information Leak] [Priority: 2]
06/01-06:08:54.411065 152.63.146.6:3309 -> xxx.yyy.zzz.4:80
TCP TTL:52 TOS:0x0 ID:15383 IpLen:20 DgmLen:285 DF
***AP*** Seq: 0x85C51FDB Ack: 0xC0D4B803 Win: 0x16D0 TcpLen: 32
TCP Options (3) => NOP NOP TS: 59974615 372988
[Xref => http://www.securityfocus.com/bid/1187]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0172]
[Xref => http://www.whitehats.com/info/IDS226]

[**] [1:871:2] WEB-CGI survey.cgi access [**]
[Classification: Attempted Information Leak] [Priority: 2]
06/01-06:08:58.609416 152.63.146.6:3310 -> xxx.yyy.zzz.4:80
TCP TTL:52 TOS:0x0 ID:32890 IpLen:20 DgmLen:295 DF
***AP*** Seq: 0x8B55C63C Ack: 0xC624745D Win: 0x16D0 TcpLen: 32
TCP Options (3) => NOP NOP TS: 59983434 381809
[Xref => http://www.securityfocus.com/bid/1817]
[Xref => http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-1999-0936]

...
```

Πίνακας 6: Καταγραφή Συμβάντων από το σύστημα ανίχνευσης εισβολέων

Παρατηρούμε ότι από την Δνση: *152.63.146.6* στις 1 Ιουν 0608, καταγράφηκαν προειδοποιήσεις σχετικές με CGI ευπάθειες που μπορούν να χρησιμοποιηθούν για απομακρυσμένη εκτέλεση εντολών. Οι προειδοποιήσεις ενεργοποιήθηκαν εξαιτίας των κανόνων του πίνακα 7.

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-CGI phf access";flags: A+;
uricontent:"/phf"; nocase; reference:bugtraq,629; reference:arachnids,128; reference:cve,CVE-1999-
0067; classtype:attempted-recon; sid:886; rev:3;)

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-CGI formmail access";flags: A+;
uricontent:"/formmail"; nocase; reference:bugtraq,1187; reference:cve,CVE-1999-0172;
reference:arachnids,226; classtype:attempted-recon; sid:884; rev:2;)

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-CGI survey.cgi access";flags: A+;
uricontent:"/survey.cgi"; nocase; reference:bugtraq,1817; reference:cve,CVE-1999-0936;
classtype:attempted-recon; sid:871; rev:2;)
```

Πίνακας 7: Κανόνες που ενεργοποιήθηκαν στο σύστημα ανίχνευσης εισβολέων

Συνήθως τέτοιες προειδοποιήσεις είναι εσφαλμένες, ειδικά αν δεν ξέρουμε τι άλλο έχει συμβεί στο δίκτυο. Ωστόσο μπορούμε να καταλάβουμε ότι πρόκειται για κακόβουλη ενέργεια μιας και η πιθανότητα να ζητηθούν τρία CGI σενάρια, που τυχαίνει να είναι ευάλωτα, από μια Δνση και την ίδια σχεδόν στιγμή είναι πολύ μικρή. Παρόλα αυτά όμως δεν γνωρίζουμε αν οι απόπειρες ήταν πετυχημένες ή αποτυχημένες. . Περιληπτικά οι πληροφορίες που αντλούνται από τα παραπάνω αρχεία καταγραφής φαίνονται στον πίνακα 8.

Συσκευή	Σύστημα ανίχνευσης εισβολέων
Ποιός:	152.63.146.6
Τι:	Τρεις http συνδέσεις στον εξυπηρετητή ιστού με Δνση IP xxx.yyy.zzz.4 .Απόπειρα πρόσβασης στα CGI: *phf,formmail,* και *survey. Δεν γνωρίζουμε αν τελικά ήταν πετυχημένη η πρόσβαση. Επίσης Δεν υπάρχουν άλλα στοιχεία πρόσβασης από αυτή τη Δνση*
Πότε:	1 Ιουν 0608 - 0609
Που:	Στο DMZ δίκτυο του οργανισμού
Γιατί	Αν τα παραπάνω CGI σενάρια είναι ενεργοποιημένα στον εξυπηρετητή ιστού, θα επιτρέψουν στον επιτιθέμενο την εκτέλεση εντολών από απόσταση.

Πίνακας 8: Αποτελέσματα επεξεργασίας αρχείων καταγραφής από το σύστημα ανίχνευσης εισβολέων

Εξυπηρετητής ιστού:

access_log

```
152.63.146.6 - - [01/Jun/2002:06:08:50 -0400] "GET /cgi-bin/phf HTTP/1.0" 404 304 "-"
"Lynx/2.8.5dev.2 libwww-FM/2.14 SSL-MM/1.4.1 OpenSSL/0.9.6a"

152.63.146.6 - - [01/Jun/2002:06:08:54 -0400] "GET /cgi-bin/formmail HTTP/1.0" 404 309 "-"
"Lynx/2.8.5dev.2 libwww-FM/2.58 SSL-MM/1.4.1 OpenSSL/0.9.6a"

152.63.146.6 - - [01/Jun/2002:06:08:58 -0400] "GET /cgi-bin/survey.cgi HTTP/1.0" 404 311 "-"
"Lynx/2.8.5dev.2 libwww-FM/2.14 SSL-MM/1.4.1 OpenSSL/0.9.6a"
```

error_log

```
[Sat Jun 1 06:08:50 2002] [error] [client 152.63.146.6] script not found or unable to stat:
/var/www/cgi-bin/phf

[Sat Jun 1 06:08:54 2002] [error] [client 152.63.146.6] script not found or unable to stat:
/var/www/cgi-bin/formmail

[Sat Jun 1 06:08:58 2002] [error] [client 152.63.146.6] script not found or unable to stat:
/var/www/cgi-bin/survey.cgi
```

Πίνακας 9: Καταγραφή Συμβάντων από τον Εξυπηρετητή ιστού

Παρατηρούμε ότι από την Δνση: *152.63.146.6* στις 1 Ιουν 0608, καταγράφηκαν οι εξής κινήσεις: έγιναν προσπάθειες πρόσβασης συγκεκριμένων CGI σεναρίων: *phf,formmail,* και *survey.cgi* (όπως φαίνεται στο access_log) αλλά απέτυχαν μιας και τα συγκεκριμένα CGI δεν ήταν ενεργοποιημένα στον εξυπηρετητή (error_log). Δεν υπάρχει άλλη πληροφορία σχετικά με την εν' λόγω Δνση. Περιληπτικά οι πληροφορίες που αντλούνται από τα παραπάνω αρχεία καταγραφής φαίνονται στον πίνακα 10.

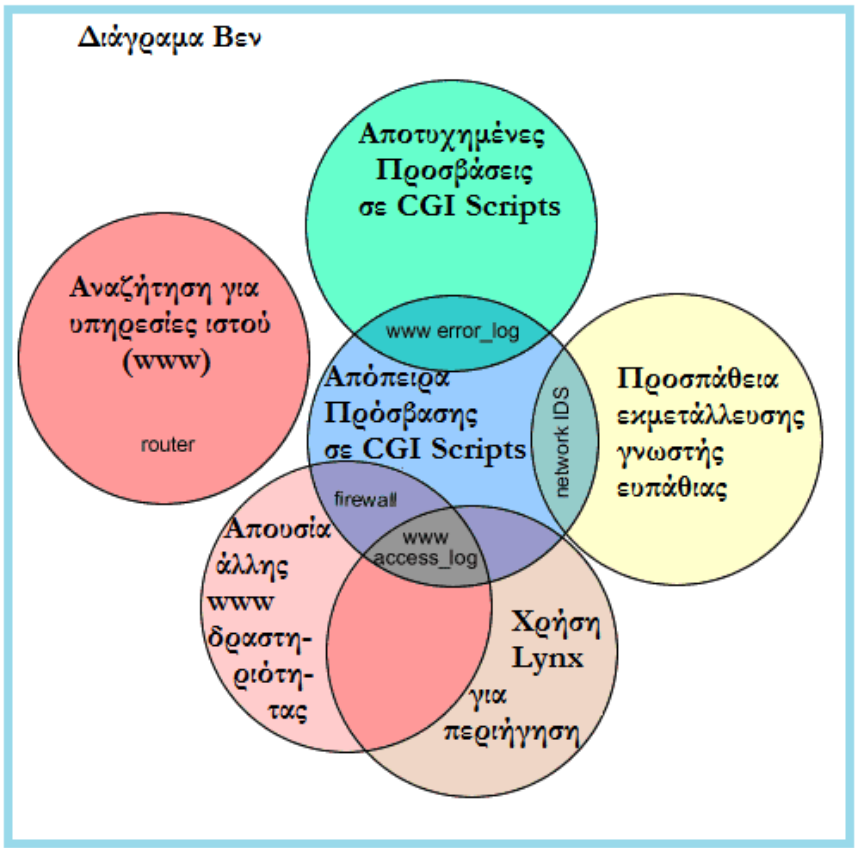
Συσκευή	Εξυπηρετητής ιστού
Ποιός:	152.63.146.6. Πιθανώς με Unix/Linux Η/Υ και κάνοντας χρήση του λογισμικού Lynx v2.8.5dev.2
Τι:	Τρεις http συνδέσεις στον εξυπηρετητή ιστού με Δνση IP xxx.yyy.zzz.4 .Απόπειρα πρόσβασης στα CGI: *phf,formmail,* και *survey. Τα εν λόγω CGI δεν προσπελάθηκαν μιας και δεν βρέθηκαν στον εξυπηρετητή. Δεν υπάρχει άλλη δραστηριότητα από αυτή την Δνση*
Πότε:	1 Ιουν 0608 - 0609
Που:	Στο DMZ δίκτυο του οργανισμού
Γιατί	Μάλλον η απόπειρα επίθεσης έληξε "άδοξα" για τον επιτιθέμενο.

Πίνακας 10: Αποτελέσματα επεξεργασίας αρχείων καταγραφής από τον Εξυπηρετητή ιστού

Συσχετισμός των συμβάντων από το SIEM

Με τη βοήθεια SIEM συστημάτων συμβάντα όπως τα παραπάνω μπορεί να συσχετιστούν και να επιτευχτεί έτσι μια λογική αναπαράσταση της "συνεισφοράς" που έχει κάθε διάταξη ασφαλείας του οργανισμού στην συνολική μας εικόνα για την αντίληψη του συμβάντος. Για παράδειγμα

στην εικόνα 6, γίνεται φανερό ότι η απουσία έστω και μιας συσκευής από τις διατάξεις ασφαλείας που χρησιμοποιήθηκαν θα μείωνε αισθητά την ικανότητα αντίληψης του συμβάντος. Δηλαδή αν απουσίαζαν τα αρχεία καταγραφής του εξυπηρετητή ιστού, δεν θα ξέραμε αν πέτυχε ή όχι η προσπάθεια. Αν απουσίαζαν τα αρχεία καταγραφής του δρομολογητή, δεν θα ήμασταν σε θέση να γνωρίζουμε ότι έγινε διερεύνηση σε όλο το υποδίκτυο της DMZ του οργανισμού κ.ο.κ. Τον ρόλο του αναλυτή συμβάντων ασφαλείας, διευκολύνουν τα SIEM, κάνοντας όλες τις απαραίτητες συσχετίσεις και δίνοντας έτσι το κατάλληλο περιθώριο αντίδρασης.



Εικόνα 6: Διάγραμμα Venn - Συσχέτιση Συμβάντων

Σύγκριση SIEM Προϊόντων Αγοράς

Για την σύγκριση των προϊόντων SIEM χρησιμοποιήσαμε την έρευνα της gartner με τίτλο "Critical Capabilities for Security Information and Event Management"[26] των Mark Nicolett, Kelly M. Kavanagh που διεξάχθηκε το 2012, την έρευνα που διεξήχθη από το

ηλεκτρονικό περιοδικό "InformationWeek Security" με τίτλο " IT Pro Ranking: SIEM " [27] καθώς και την έρευνα του ηλεκτρονικού περιοδικού " Dr. Dobb's Journal" [28]

Αποτελέσματα έρευνας όπως παρουσιάστηκαν από "Gartner"

Στην έρευνα της gartner συγκρίνονται τα προϊόντα του κάτωθι πίνακα 11 :

Α/Α	Εταιρεία - Προϊόν SIEM	URL
1	eIQnetworks	http://www.eiqnetworks.com/
2	HP (ArcSight)	http://www8.hp.com/us/en/software-solutions/software.html?compURI=1340477#.UYDD_7VkN-p
3	IBM (QRadar)	http://www-03.ibm.com/software/products/us/en/qradar-siem/
4	LogLogic	http://www.tibco.com/products/event-processing/log-management/default.jsp
5	LogRhythm	http://logrhythm.com/siem-2.0/security-information-event-management/siem-with-logrhythm.aspx
6	McAfee (NitroSecurity)	http://www.mcafee.com/us/products/siem/index.aspx
7	NetIQ (Novell)	https://www.netiq.com/products/sentinel/
8	RSA (EMC)	http://www.emc.com/security/rsa-envision.htm
9	Sensage	http://www.sensage.com/content/advanced-siem-and-log-management
10	SolarWinds	http://www.solarwinds.com/siem-security-information-event-management-software.aspx
11	Splunk	http://www.splunk.com/view/it-security/SP-CAAAAKD
12	Symantec	http://www.ndm.net/siem/main/symantec-siem

Πίνακας 11: Λίστα με προϊόντα SIEM και URL βάση Garner

Στη συνέχεια παρατίθεται ο πίνακας 12 με τις λειτουργικότητες που ελέχθησαν:

Α/Α	Λειτουργία	Παρατηρήσεις
1	Παρακολούθηση σε πραγματικό χρόνο (Real-time monitoring)	Τα συμβάντα μεταφέρονται από τις ετερογενείς πηγές τους (συσκευές, συστήματα, εφαρμογές) σε πραγματικό σχεδόν χρόνο, σε μια κεντρική Β.Δ. Εκεί κανονικοποιούνται και συσχετίζονται βάση μιας βιβλιοθήκης προκαθορισμένων κανόνων. Τα βασικά χαρακτηριστικά συσχέτισης είναι: τύπος συμβάντος, προέλευση, προορισμός και χρόνος. Τέλος γίνεται παρουσίαση των αποτελεσμάτων σε γραφικό περιβάλλον.
2	Πληροφορίες για απειλές (Threat intelligence)	Οι πληροφορίες για πιθανές απειλές μπορεί να προέρχονται από λίστες ανοικτής κοινότητας (π.χ. η Emerging Threats [29]), από τα ερευνητικά τμήματα της εταιρείας και από τη λογική των κανόνων που εισάγονται.
3	Προφίλ κανονικής λειτουργίας (Behavior profiling)	Παρέχονται δυνατότητες εκμάθησης της συνήθους δραστηριότητας του δικτύου και των συμβάντων που δημιουργούνται. Μετά την δημιουργία του προφίλ, αποκλίσεις από την κανονική δραστηριότητα καταγράφονται ως ύποπτες.
4	Παρακολούθηση χρηστών και δεδομένων (Data and user and monitoring)	Γίνεται με αλληλεπίδραση με τις υπάρχουσες τεχνολογίες διαχείριση ταυτοτήτων και δεδομένων όπως η υπηρεσία καταλόγου (directory service), τα συστήματα διαχείρισης Β.Δ (DBMS), συστήματα αποτροπής απώλειας δεδομένων (DLP), κ.λ.π
5	Παρακολούθηση εφαρμογών (Application monitoring)	Βασίζεται στην ικανότητα να αναλύει τις εξόδους εφαρμογών, εμπορικών και μη (in house developed), με κατάλληλες διεπαφές (API), επαυξάνοντας έτσι την δυνατότητα εντοπισμού απειλών στο επίπεδο των εφαρμογών.
6	Αναλυτικές Παρουσιάσεις (Analytics - compliance reporting)	Συνήθως παρουσιάζουν τα αποτελέσματα των συσχετίσεων σε καλοσχεδιασμένες και φιλικές στον χρήστη προβολές, με δυνατότητες αναζήτησης και εξαγωγής γραφικών αναφορών.
7	Διαχείριση συμβάντων (Log management)	Υποστηρίζουν αποδοτική αποθήκευση και ανάλυση μεγάλου όγκου πληροφοριών, καθώς και δυνατότητα αναζήτησης δεδομένων.
8	Απλότητα στην εγκατάσταση και τη χρήση (Deployment and	Χρησιμοποιούν γραφικά βοηθήματα και οδηγούς εγκατάστασης και χρήσης. Παρέχουν επιπρόσθετα τυποποιημένους τρόπους για τροποποίηση ρυθμίσεων για άμεση προσαρμογή στις ανάγκες του

	support simplicity)	οργανισμού.

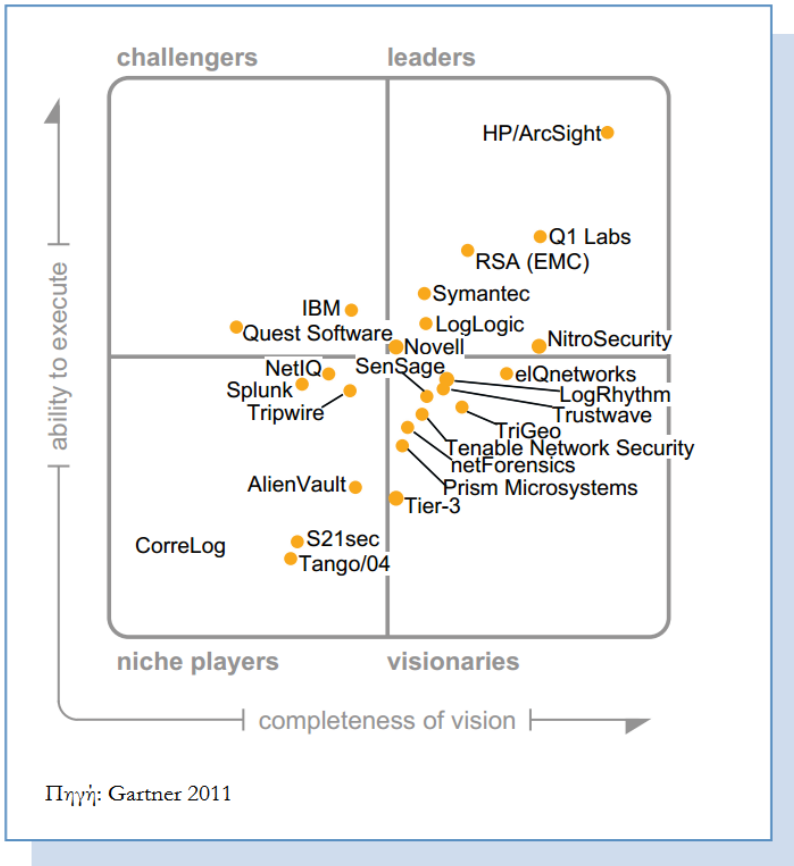
Πίνακας 12: Εξεταζόμενες Λειτουργικότητες των SIEM (Πηγή: Gartner_May 2012)

Στον επόμενο πίνακα 13 προβάλλονται τα αποτελέσματα όπως αυτά παρουσιάζονται στην έρευνα της gartner [26].

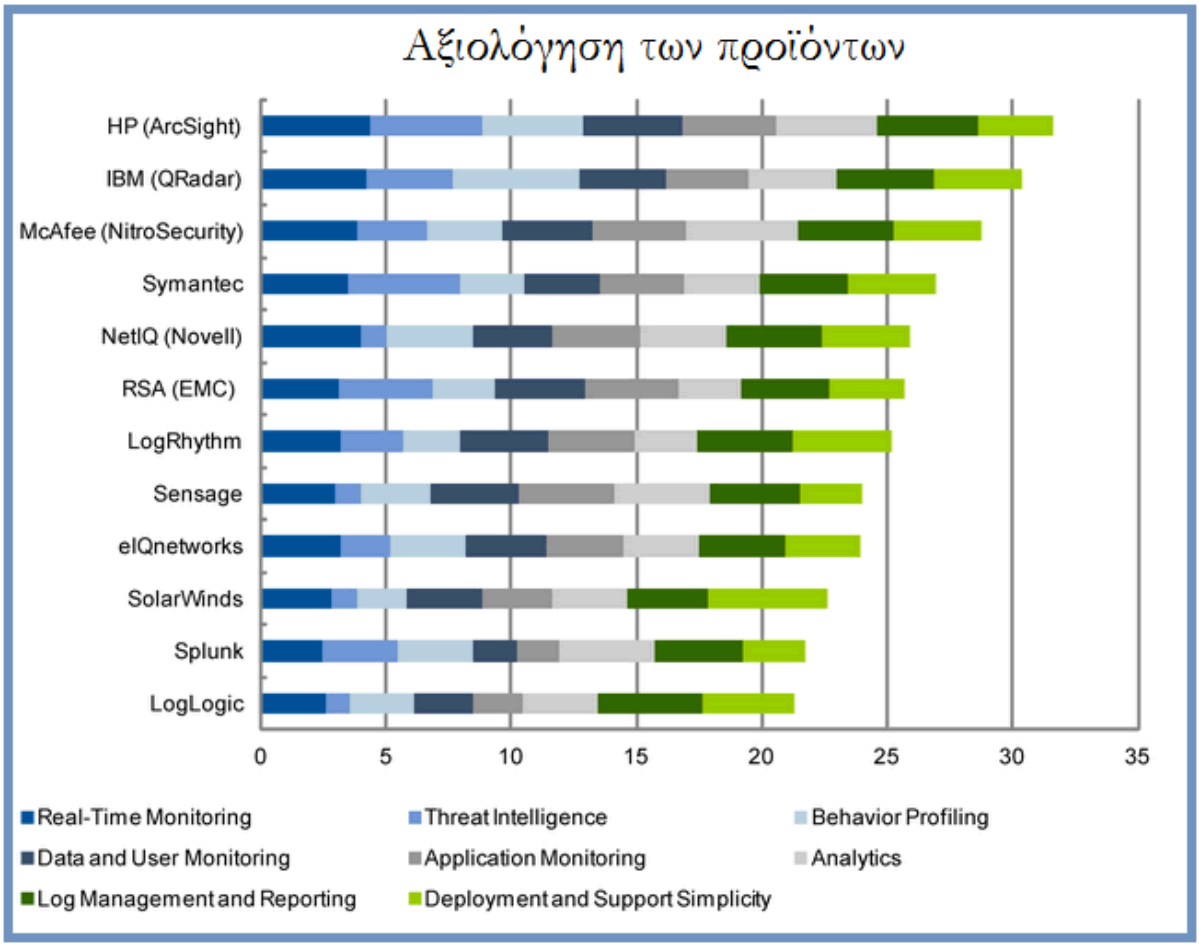
Product Rating	elQnetworks	HP (ArcSight)	IBM (QRadar)	LogLogic	LogRhythm	McAfee (NitroSecurity)	NetIQ (Novell)	RSA (EMC)	Sensage	SolarWinds	Splunk	Symantec
Real-Time Monitoring	3.2	4.4	4.2	2.6	3.2	3.9	4.0	3.1	3.0	2.9	2.5	3.5
Threat Intelligence	2.0	4.5	3.5	1.0	2.5	2.8	1.0	3.7	1.0	1.0	3.0	4.5
Behavior Profiling	3.0	4.0	5.0	2.5	2.3	3.0	3.5	2.5	2.8	2.0	3.0	2.5
Data and User Monitoring	3.2	4.0	3.5	2.4	3.5	3.6	3.1	3.6	3.5	3.0	1.7	3.0
Application Monitoring	3.1	3.8	3.3	2.0	3.5	3.7	3.5	3.8	3.8	2.8	1.8	3.3
Analytics	3.0	4.0	3.5	3.0	2.5	4.5	3.5	2.5	3.8	3.0	3.8	3.0
Log Management and Reporting	3.4	4.0	3.9	4.2	3.8	3.8	3.8	3.5	3.6	3.3	3.5	3.5
Deployment and Support Simplicity	3.0	3.0	3.5	3.7	4.0	3.5	3.5	3.0	2.5	4.8	2.5	3.5

Πίνακας 13: Αξιολόγηση προιόντων SIEM (Πηγή: Gartner_May 2012)

Στην εικόνα 7 προβάλει η τελική αξιολόγηση των προϊόντων βάση της έρευνας της gartner [26].



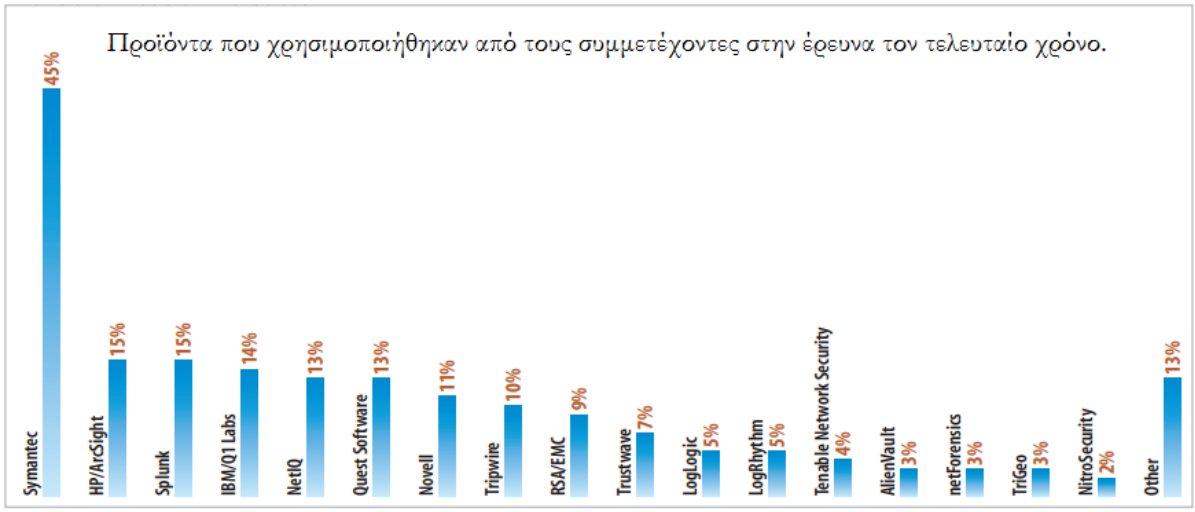
Εικόνα 7: Αξιολόγηση προϊόντων SIEM



Εικόνα 8: Αξιολόγηση Προϊόντων SIEM (Πηγή: Gartner - May 2012)

Αποτελέσματα έρευνας όπως παρουσιάστηκαν από "InformationWeek.com "

Στην εικόνα 8 απεικονίζονται τα προϊόντα που χρησιμοποιήθηκαν από τους συμμετέχοντες στην έρευνα κατά τον τελευταίο χρόνο.



Εικόνα 9: Προϊόντα SIEM (Πηγή: informationweek.com)

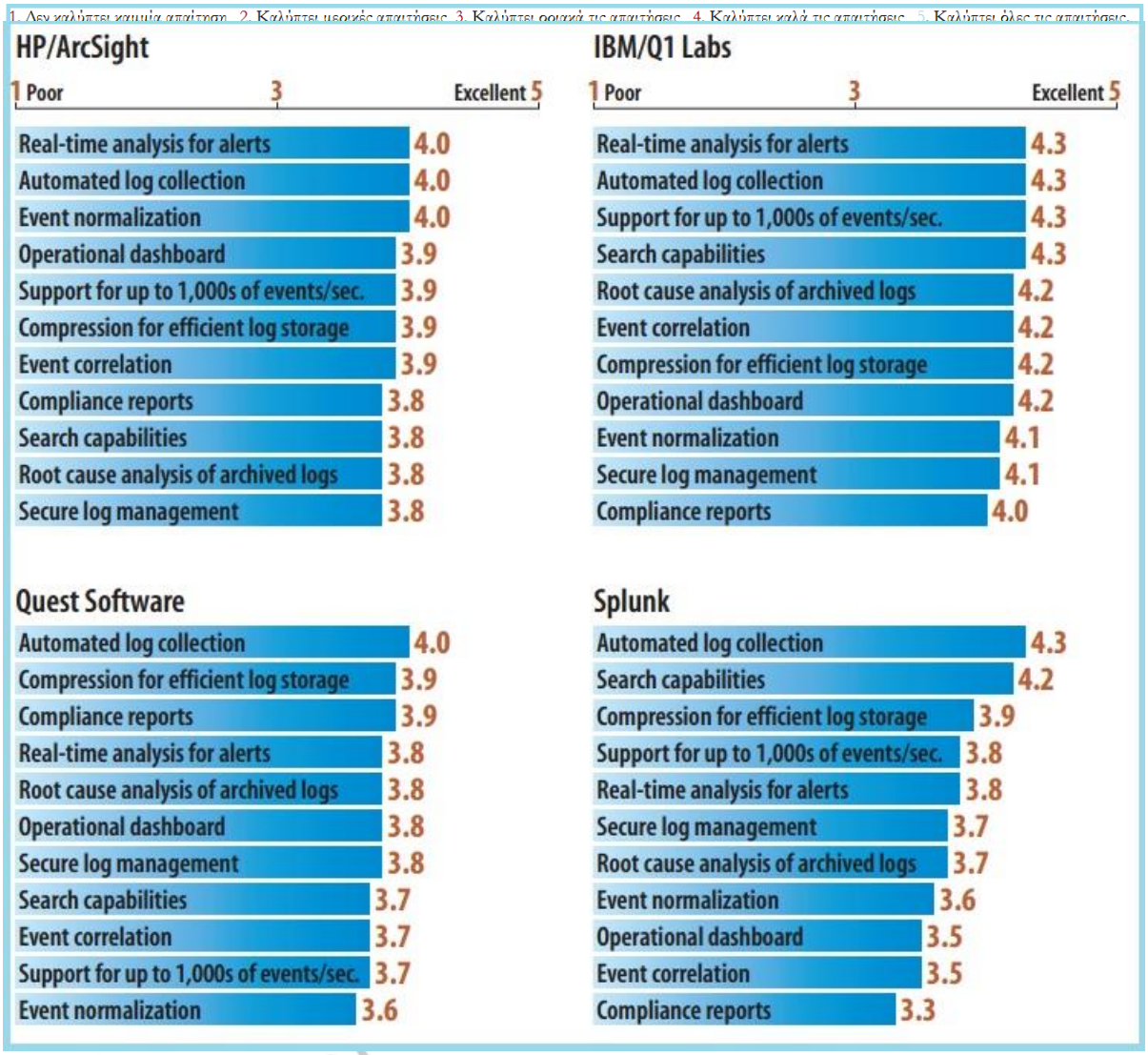
Στη συνέχεια παρατίθεται ο πίνακας 14 με τις λειτουργικότητες που ελέχθησαν από το " informationweek.com "

Α/Α	Λειτουργία	Παρατηρήσεις
1	Παρακολούθηση σε πραγματικό χρόνο (Real-time analysis for alerts)	Τα συμβάντα μεταφέρονται από τις ετερογενείς πηγές τους (συσκευές, συστήματα, εφαρμογές) σε πραγματικό σχεδόν χρόνο, σε μια κεντρική Β.Δ.
2	Αυτόματη συλλογή συμβάντων (Automated log collection)	Ο βαθμός παραμετροποίησης για την συλλογή συμβάντων διαφέρει ως προς τον αυτοματισμό.
3	Κανονικοποίηση συμβάντων (Event normalization)	Τα συμβάντα που έχουν συλλεχθεί κανονικοποιούνται και συσχετίζονται βάση μιας βιβλιοθήκης προκαθορισμένων κανόνων. Τα βασικά χαρακτηριστικά συσχέτισης είναι: τύπος συμβάντος, προέλευση, προορισμός και χρόνος.
4	Παρουσίαση - προβολή αποτελεσμάτων συσχέτισης (Operational dashboard)	Δυνατότητα παρουσίασης των αποτελεσμάτων συσχέτισης σε γραφικό περιβάλλον.
5	Ρυθμός επεξεργασίας Συμβάντων (Support for up to 1,000s of	Το προϊόν θα πρέπει να είναι σε θέση να διαχειριστεί μεγάλο όγκο Συμβάντων σε μικρό χρόνο (συμβάντα αν δευτερόλεπτο)

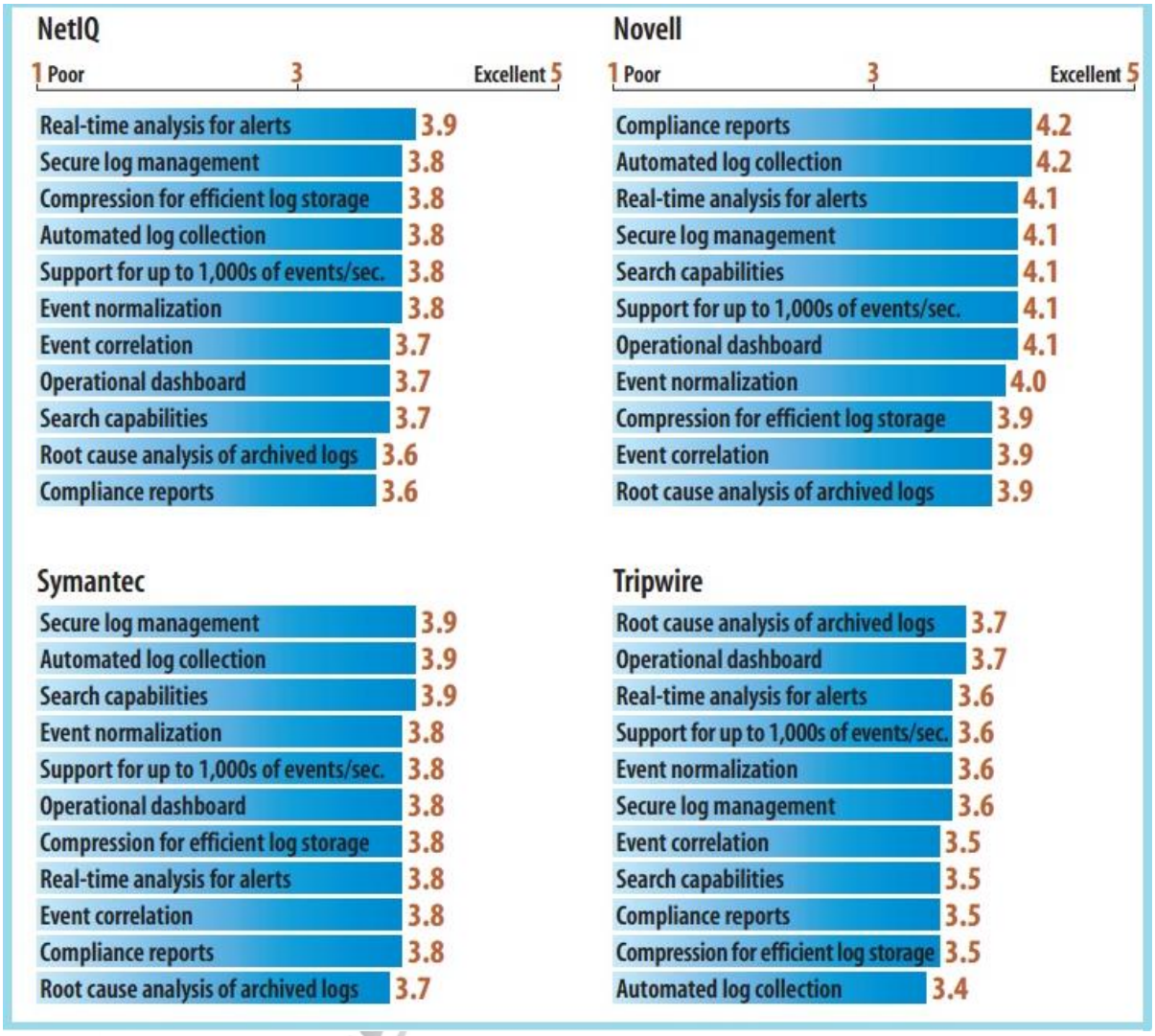
	events/sec.)	
6	Βέλτιστη χρήση αποθηκευτικού χώρου (Compression for efficient log storage)	Γίνεται χρήση τεχνικών συμπίεσης για την εξοικονόμηση αποθηκευτικού χώρου.
7	Συσχέτιση Συμβάντων (Event correlation)	Οι τεχνικές συσχέτισης που χρησιμοποιούνται αποτελούν έναν από τους ποιό κρίσιμους παράγοντες αξιολόγησης ενός SIEM
8	Αναφορές Συμμόρφωσης (Compliance reports)	Παρέχουν την δυνατότητα αυτοματοποιημένης δημιουργίας αναφορών συμμόρφωσης με τις πολιτικές ασφαλείας του οργανισμού
9	Δυνατότητα σύνθετης αναζήτησης συμβάντων (Search capabilities)	Η δυνατότητα σύνθετης αναζήτησης συμβάντων παρέχει στον αναλυτή ασφαλείας το κατάλληλο εργαλείο για περαιτέρω διερεύνηση περιστατικών ασφαλείας που το SIEM τα χαρακτήρισε ως ύποπτα.
10	Ανάλυση των αρχικών αιτιών προβλημάτων από τα αρχεία καταγραφής (Root cause analysis of archived logs)	Δίνουν την δυνατότητα: • Καθορισμού του τι συνέβη. • Προσδιορισμού του γιατί συνέβη. • Λήψης μέτρων που θα μειώσουν την πιθανότητα επανάληψης του συμβάντος
10	Ασφάλεια κατά τη διαχείριση των συμβάντων (Secure log management)	Γίνεται χρήση τεχνικών όπως η κρυπτογράφηση και ο έλεγχος πρόσβασης για την ασφαλή διαχείριση όλων των αποθηκευμένων συμβάντων.

Πίνακας 14: Εξεταζόμενες Λειτουργικότητες των SIEM (Πηγή: informationweek.com)

καθώς και τα αποτελέσματα της έρευνας, σχετικά με τις δυνατοτήτων τους (εικόνες 9 και 10).



Εικόνα 10: Αξιολόγηση Προϊόντων SIEM (Α) (Πηγή: informationweek.com)



Εικόνα 11:Αξιολόγηση Προϊόντων SIEM (Β) (Πηγή: informationweek.com)

Αποτελέσματα έρευνας όπως παρουσιάστηκαν από το "Dr. Dobb's Journal"

	ArcSight ESM	Network Intelligence enVision	High Tower Software Security Event Manager	Q1 Labs QRadar	Symantec Security Information Manager 9500	LogLogic ST 3000 and LX 2000	SenSage Enterprise Security Analytics	OpenService Security Threat Manager 3.5
REAL-TIME FEATURES								
User interface (20%)	4.5	3.5	4	3.5	3.5	3	3	2
Event correlation (15%)	5	4	3	4	3.5	1	3	2
CORE FEATURES								
Device support (10%)	5	4	3	3	3	2	4	4
Data management (5%)	4	4	3	3	2	4	3	3
Device provisioning (5%)	4	3	5	3	2	4	2	2
Transport capabilities (5%)	5	3	3	3	3	3.5	3	2
PRICING (25%)	3	4	4.5	4	3	4	2	3
REPORTING (15%)	4	3	2	3	3	3.5	4	3
TOTAL SCORE (100%)	4.15	3.65	3.53	3.50	3.08	3.05	2.95	2.65
A≥4.3, B≥3.5, C≥2.5, D≥1.5, F<1.5 A-C GRADES INCLUDE + OR - IN THEIR RANGES. TOTAL SCORES AND WEIGHTED SCORES ARE BASED ON A SCALE OF 0-5.	B+	B-	B-	B-	C+	C+	C	C-

TRANSPORT CAPABILITIES rates how well the product moves data from point A to point B.
DATA MANAGEMENT reflects how well we could manage data once it's in the product; are there DBA-like UI tools or is everything manual?

Εικόνα 12: Αξιολόγηση Προϊόντων SIEM (Πηγή: www.drdobbs.com)

Από τρεις έρευνες γίνεται φανερό ότι τα τρία καλύτερα προϊόντα SIEM της αγοράς όπως αυτή διαμορφώνεται το 2012, είναι:

1. HP ArcSight [30]

2. IBM Q1labs [31]

3. Novel NetIQ [32]

3 NAC

Αντιμετώπιση Συμβάντων Ασφαλείας με Συστήματα Έλεγχου Πρόσβασης

Τα συστήματα ελέγχου πρόσβασης (NAC) εντάσσονται σε μια νέα και αναδυόμενη κατηγορία προϊόντων ασφαλείας και εξαιτίας αυτής της "ανωριμότητας" παρατηρούνται αποκλίσεις τόσο στα χαρακτηριστικά τους όσο και στις τεχνικές που χρησιμοποιούν για την υλοποίηση των λειτουργιών τους [17]. Η αντιμετώπιση των συμβάντων ασφαλείας, όσον αφορά στα συστήματα ελέγχου πρόσβασης μπορεί να υλοποιηθεί με::

- Περιορισμό της εξάπλωσης γνωστών δικτυακών μολύνσεων
- Επιβολή πολιτικής ασφαλείας δικτύου
- Διαχείριση ταυτοτήτων και πρόσβασης

Αναλυτικότερα ο Περιορισμό της εξάπλωσης γνωστών δικτυακών μολύνσεων επιτυγχάνεται μέσω της απομόνωσης της μολυσμένης δικτυακής οντότητας με σκοπό πάντοτε την μη εξάπλωση της μόλυνσης και την προστασία εκείνων των τερματικών που δεν έχουν την κατάλληλη προστασία για αυτή (π.χ. ενημερωμένο λογισμικό). Μερικά προϊόντα NAC δίνουν επιπρόσθετα και τη δυνατότητα εξάλειψης της απειλής, με αποκατάσταση του προβλήματος.

Η επιβολή πολιτικής ασφαλείας δικτύου, δίνει την δυνατότητα στους υπευθύνους ασφαλείας του δικτύου να καθορίσουν πολιτικές της μορφής: ποιοί τύποι Η/Υ, ποιοί χρήστες και σε ποιά υποδίκτυο επιτρέπεται να έχουν πρόσβαση; Αυτές οι πολιτικές εφαρμόζονται στις αντίστοιχες δικτυακές συσκευές (π.χ. Δρομολογητές, μεταγωγής κ.α.)

Τέλος η διαχείριση ταυτοτήτων και πρόσβασης αφορά στην εφαρμογή πολιτικών πρόσβασης βάση επικυρωμένων ταυτοτήτων χρηστών.

Σενάριο Χρήσης Cisco NAC

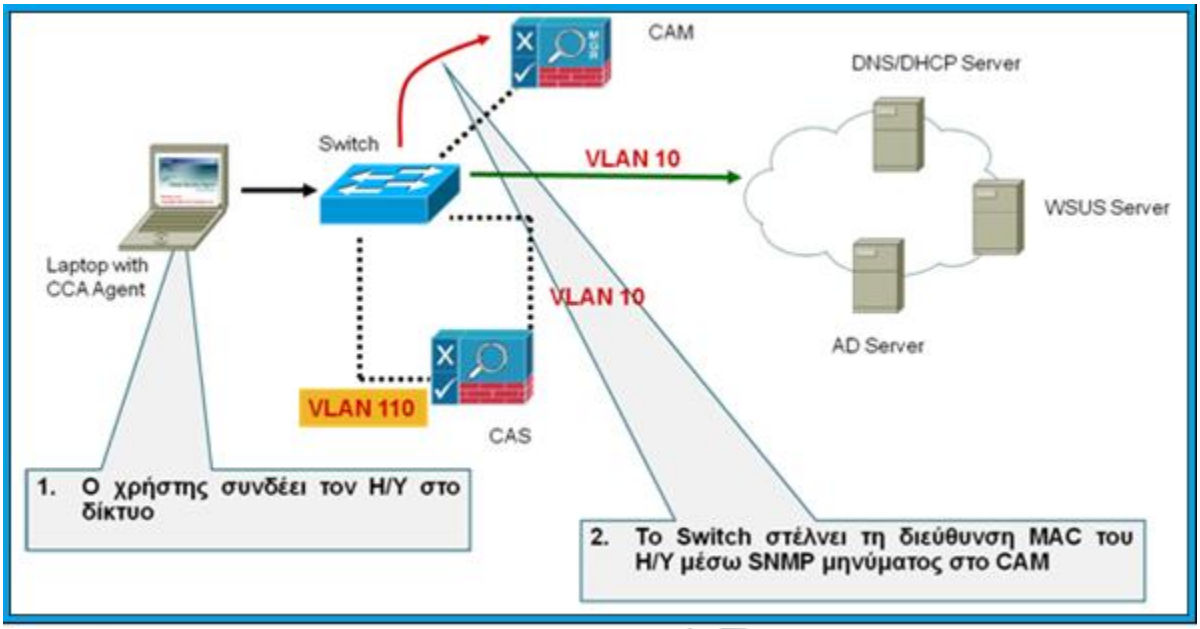
Για να αντιληφτούμε τον τρόπο λειτουργίας ενός μηχανισμού NAC θα μελετήσουμε ένα σενάριο χρήσης που περιγράφει την εισόδου ενός κινητού χρήστη με φορητό Η/Υ στο δίκτυο

μια επιχείρησης. Το σενάριο χρήσης υλοποιείται με το προϊόν της CISCO [33] "Cisco Network Admission Control (NAC)"[34]. Για την υλοποίηση του σεναρίου χρησιμοποιήθηκαν:

- Φορητός Η/Υ (Laptop) με λειτουργικό σύστημα Windows και CCA agent
- Μεταγωγέας (Switch) τύπου Cisco
- Εξυπηρετητής WSUS
- Εξυπηρετητής AV
- Εξυπηρετητής AD
- Εξυπηρετητής DNS/DHCP
- Εξυπηρετητής CAM
- Εξυπηρετητής CAS
- VLAN 110: Χρησιμοποιείται ως προσωρινό υποδίκτυο για έλεγχο και επιδιόρθωση του Η/Υ
- VLAN 10: Είναι το υποδίκτυο εργασίας του χειριστή του Η/Υ.

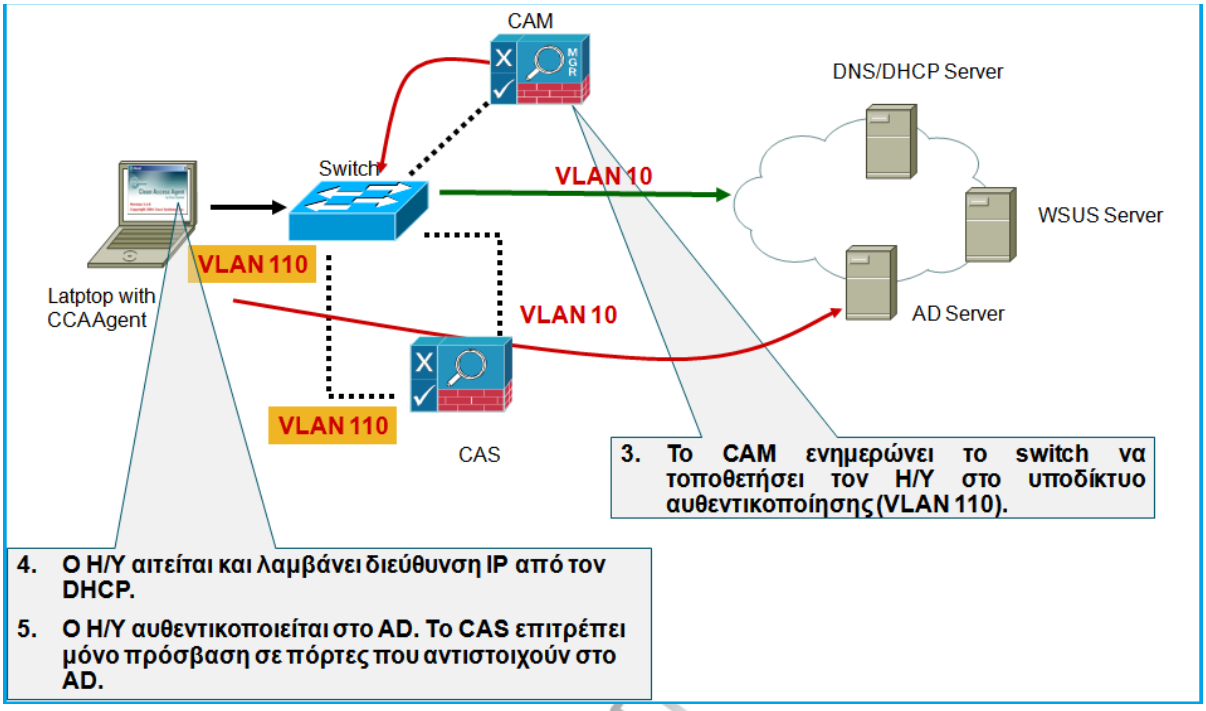
Τα βήματα που ακολουθούνται για την είσοδο του φορητού Η/Υ στο υποδίκτυο εργασίας (VLAN 10) παριστάνονται γραφικά στις παρακάτω εικόνες:

1. *Ο χρήστης συνδέει τον Η/Υ στο δίκτυο*
2. *Το Switch στέλνει τη διεύθυνση MAC του Η/Υ μέσω SNMP μηνύματος στο CAM (εικόνα 13)*



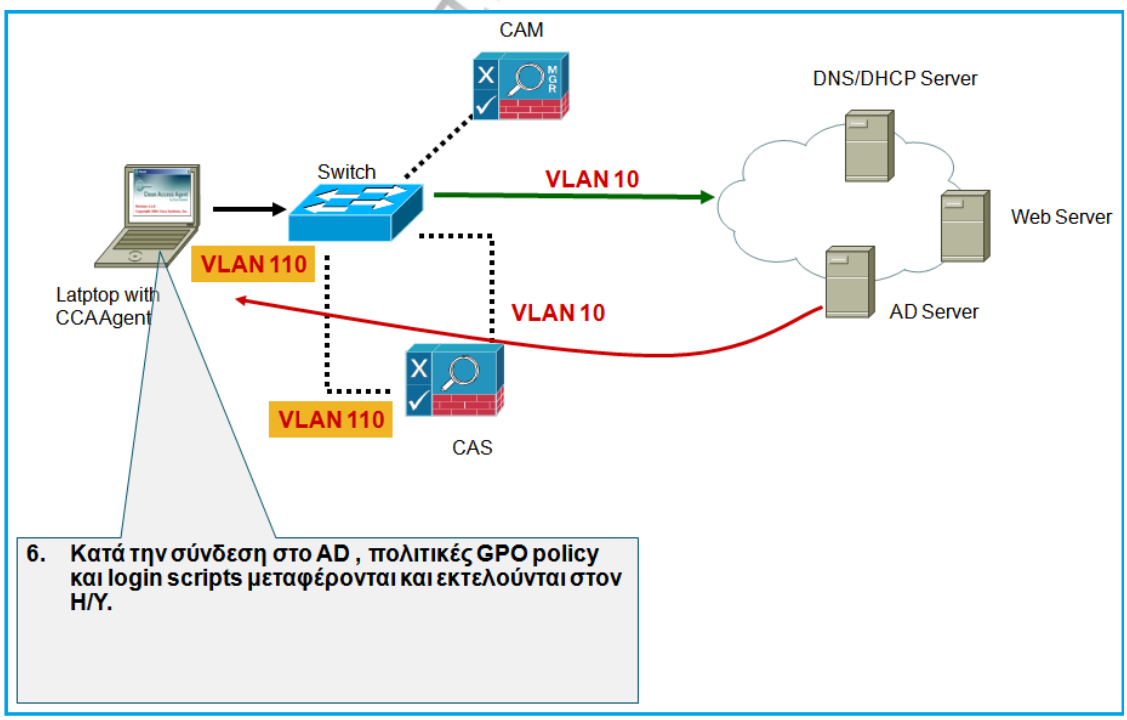
Εικόνα 13: Λειτουργία Cisco NAC (Βήμα 1ο)

3. *Το CAM ενημερώνει το switch να τοποθετήσει τον Η/Υ στο υποδίκτυο αυθεντικοποίησης (VLAN 110).*
4. *Ο Η/Υ αιτείται και λαμβάνει διεύθυνση IP από τον DHCP.*
5. *Ο Η/Υ αυθεντικοποιείται στο AD. Το CAS επιτρέπει μόνο πρόσβαση σε πόρτες που αντιστοιχούν στο AD (εικόνα 14) .*



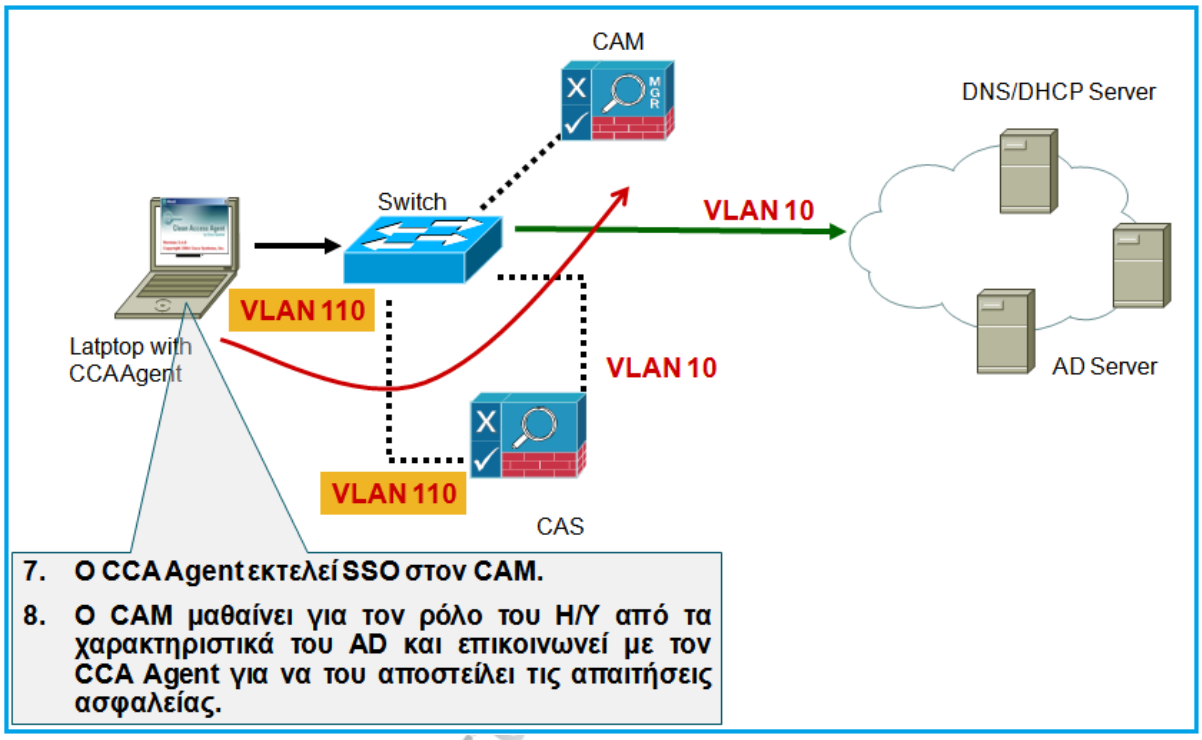
Εικόνα 14: Λειτουργία Cisco NAC (Βήμα 2ο)

6. *Κατά την σύνδεση στο AD , πολιτικές GPO policy και login scripts μεταφέρονται και εκτελούνται στον Η/Υ(εικόνα 15).*



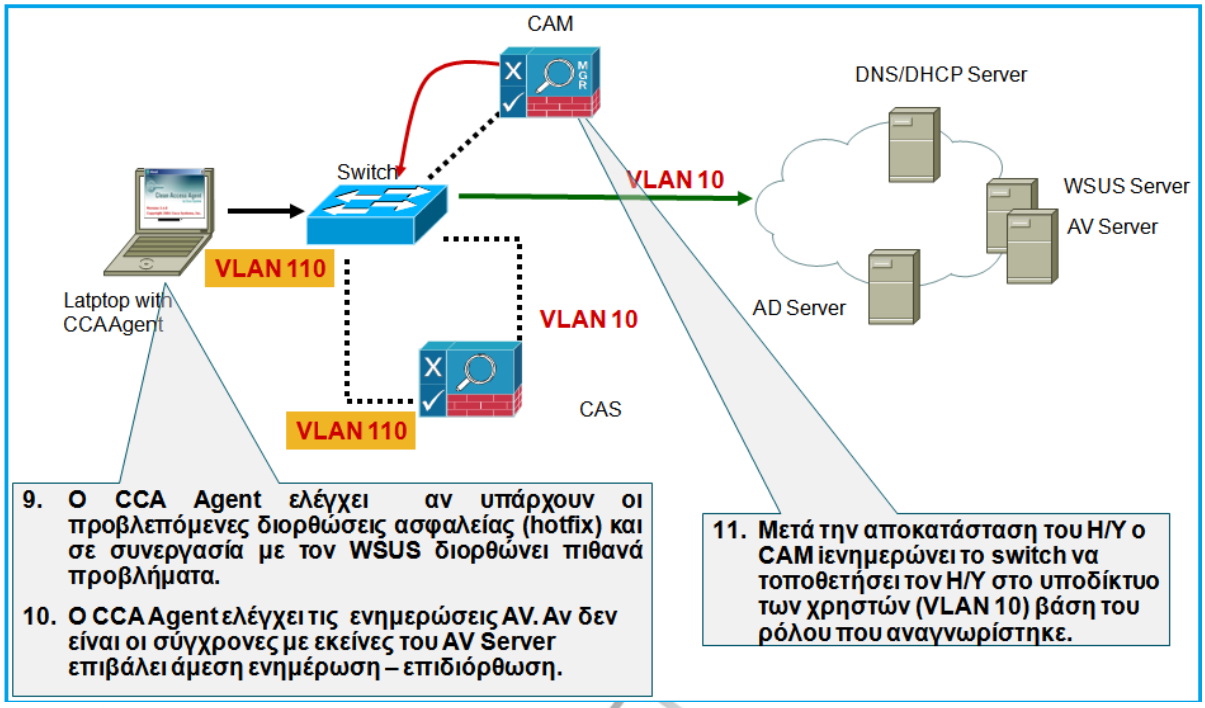
Εικόνα 15: Λειτουργία Cisco NAC (Βήμα 3ο)

7. *Ο CCA Agent εκτελεί SSO στον CAM.*
8. *Ο CAM μαθαίνει για τον ρόλο του Η/Υ από τα χαρακτηριστικά του AD και επικοινωνεί με τον CCA Agent για να του αποστείλει τις απαιτήσεις ασφαλείας (εικόνα 16).*

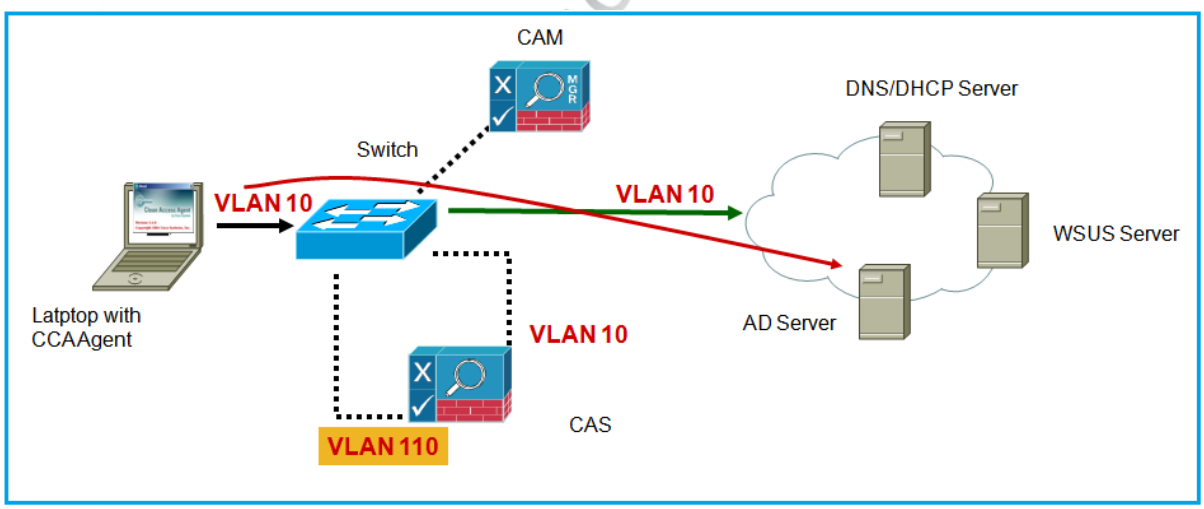


Εικόνα 16: Λειτουργία Cisco NAC (Βήμα 4ο)

9. *Ο CCA Agent ελέγχει αν υπάρχουν οι προβλεπόμενες διορθώσεις ασφαλείας (hotfix) και σε συνεργασία με τον WSUS διορθώνει πιθανά προβλήματα.*
10. *Ο CCA Agent ελέγχει τις ενημερώσεις AV. Αν δεν είναι οι σύγχρονες με εκείνες του AV Server επιβάλει άμεση ενημέρωση – επιδιόρθωση (εικόνα 17).*
11. *Μετά την αποκατάσταση του Η/Υ ο CAM ιενημερώνει το switch να τοποθετήσει τον Η/Υ στο υποδίκτυο των χρηστών (VLAN 10) βάση του ρόλου που αναγνωρίστηκε (εικόνα 18).*



Εικόνα 17: Λειτουργία Cisco NAC (Βήμα 5ο)



Εικόνα 18: Λειτουργία Cisco NAC (Βήμα 6ο)

Σύγκριση NAC Προϊόντων Αγοράς

Για την σύγκριση των προϊόντων SIEM χρησιμοποιήσαμε την έρευνα της gartner με τίτλο "Magic Quadrant for Network Access Control" που εκδόθηκε την 8 Δεκεμβρίου 2011 [35],

την έρευνα της Info-Tech Research Group με τίτλο " Vendor Landscape: Network Access Control" που εκδόθηκε την 18 Απριλίου 2012 [36] και την έρευνα του ηλεκτρονικού περιοδικού Network World με τίτλο " NAC access control: A multi-dimensional puzzle " που εκδόθηκε την 21 Ιουνίου 2010 [37].

Αποτελέσματα έρευνας όπως παρουσιάστηκαν από "Gartner"

Στην έρευνα της gartner συγκρίνονται τα προϊόντα του κάτωθι πίνακα 15 :

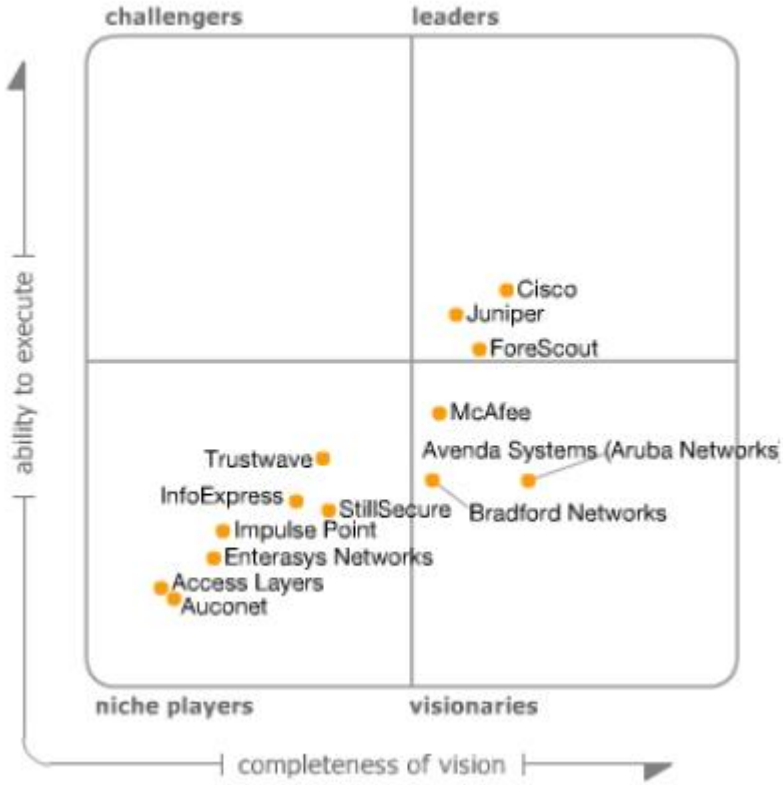
Α/Α	Εταιρεία - Προϊόν SIEM	URL
1	Access Layers	http://www.accesslayers.com/
2	Auconet	http://www.auconet.com/en/auconet-network-solutions/auconet-nac-management/
3	Avenda Systems	http://www.arubanetworks.com/products/clearpass/
4	Bradford Networks	http://www.bradfordnetworks.com/network_access_control
5	Cisco	http://www.cisco.com/en/US/netsol/ns466/index.html
6	Enterasys	http://www.enterasys.com/company/literature/nac-ds.pdf
7	ForeScout	http://www.forescout.com/solutions/network-access-control/
8	Impulse Point	http://www.impulse.com/
9	InfoExpress	http://www.infoexpress.com/
10	Juniper	http://www.juniper.net/us/en/products-services/security/uac/
11	McAfee	http://www.intel.cn/content/dam/www/public/us/en/documents/product-briefs/consumerization-network-access-control-brief.pdf
12	StillSecure	http://www.stillsecure.com/
13	Trustwave	https://www.trustwave.com/network-access-control/

Πίνακας 15: Λίστα με προϊόντα NAC και URL βάση Garner

Η έρευνα της Gartner αφορά στον έλεγχο των λειτουργικοτήτων που φαίνονται στον πίνακα 16

Α/Α	Λειτουργία	Παρατηρήσεις
1	Πολιτική (Policy)	Η λύση NAC πρέπει να περιλαμβάνει ένα αποκλειστικό server για διαχείριση των ρυθμίσεων ασφαλείας βάση της πολιτικής ασφαλείας. Θα πρέπει να υπάρχει κατάλληλη γραφική διεπαφή που να επιτρέπει την εύκολη ρύθμιση των παραπάνω (για παράδειγμα, να επιτρέψει ή να βάλει σε καραντίνα δικτυακούς πόρους. Η διαχείριση της πολιτικής και οι λειτουργίες που εξάγουν αναφορές αποτελούν τους βασικούς τομείς όπου καινοτομούν οι κατασκευαστές συστημάτων NAC.
2	Σημεία Αναφοράς (Baseline)	Με τη δημιουργία σημείων αναφοράς καθορίζεται η κατάσταση ασφαλείας ενός τερματικού, που επιχειρεί να συνδεθεί σε ένα δίκτυο, έτσι ώστε να μπορεί να ληφθεί απόφαση σχετικά με το επίπεδο πρόσβασης που θα επιτρέπεται. Περιλαμβάνουν τη δυνατότητα αξιολόγησης της συμμόρφωσης με τις υπάρχουσες πολιτικές (για παράδειγμα, σύγχρονες ενημερώσεις και ενημερωμένες υπογραφές antivirus) καθώς και τη δυνατότητα να ανιχνεύει κακόβουλο λογισμικό στα τερματικά που επιδιώκουν τη σύνδεση στο δίκτυο. Διάφορες τεχνολογίες μπορούν να χρησιμοποιηθούν για τη δημιουργία σημείων αναφοράς, με agent ή χωρίς (όπως σαρώσεις εκτίμησης τρωτότητας).
3	Έλεγχος Πρόσβασης (Access control)	Μια λύση NAC πρέπει να περιλαμβάνει τη δυνατότητα να μπλοκάρει, να απομονώνει ή να παρέχει πλήρη πρόσβαση σε ένα τερματικό δικτύου. Η λύση πρέπει να είναι αρκετά ευέλικτη ώστε να επιβάλει τον έλεγχο της πρόσβασης ανεξαρτήτου προμηθευτών υποδομής δικτύου, και πρέπει να είναι σε θέση να επιβάλει την πρόσβαση σε ενσύρματα,ασύρματα τοπικά δίκτυα, VPN πύλες. Επιβολή πρέπει να επιτευχθεί μέσω της υποδομής του δικτύου (για παράδειγμα, 802.1X, VLANs, ACL) ή μέσω της NAC λύσης (για παράδειγμα, reset session με [ARP] spoofing κτλ).

Πίνακας 16: Λειτουργικότητες NAC Προϊόντων



Εικόνα 19: Αξιολόγηση προϊόντων NAC (Gartner 2012)

Αποτελέσματα έρευνας όπως παρουσιάστηκαν από " Info-Tech Research Group "

Στην έρευνα της Info-Tech Research Group συγκρίνονται τα προϊόντα του κάτωθι πίνακα 16 :

Α/Α	Εταιρεία - Προϊόν NAC	URL
1	Bradford.	http://www.bradfordnetworks.com/network_access_control
2	Cisco.	http://www.cisco.com/en/US/netsol/ns466/index.html
3	Enterasys.	http://www.enterasys.com/company/literature/nac-ds.pdf
4	ForeScout.	http://www.forescout.com/solutions/network-access-control/
5	Juniper.	http://www.juniper.net/us/en/products-services/security/uac/
6	McAfee.	http://www.intel.cn/content/dam/www/public/us/en/documents/product-

		briefs/consumerization-network-access-control-brief.pdf
7	StillSecure.	http://www.stillsecure.com/
8	Trustwave.	https://www.trustwave.com/network-access-control/

Πίνακας 17: Προϊόντα NAC προς σύγκριση από Info-Tech Research Group (2012)

Αποτελέσματα έρευνας όπως παρουσιάστηκαν από " Network World "

Στην έρευνα της Nerwork World συγκρίνονται τα προϊόντα του κάτωθι πίνακα 17 :

Α/Α	Εταιρεία - Προϊόν NAC	URL
1	Alcatel-Lucent	http://enterprise.alcatel-lucent.com/?solution=Security&page=SafeNetworkAccess
2	Avenda Systems	http://www.arubanetworks.com/products/clearpass/
3	Bradford.	http://www.bradfordnetworks.com/network_access_control
4	Cisco.	http://www.cisco.com/en/US/netsol/ns466/index.html
5	Enterasys.	http://www.enterasys.com/company/literature/nac-ds.pdf
6	ForeScout.	http://www.forescout.com/solutions/network-access-control/
7	Juniper	http://www.juniper.net/us/en/products-services/security/uac/
8	McAfee.	http://www.intel.cn/content/dam/www/public/us/en/documents/product-briefs/consumerization-network-access-control-brief.pdf
9	Trustwave.	https://www.trustwave.com/network-access-control/

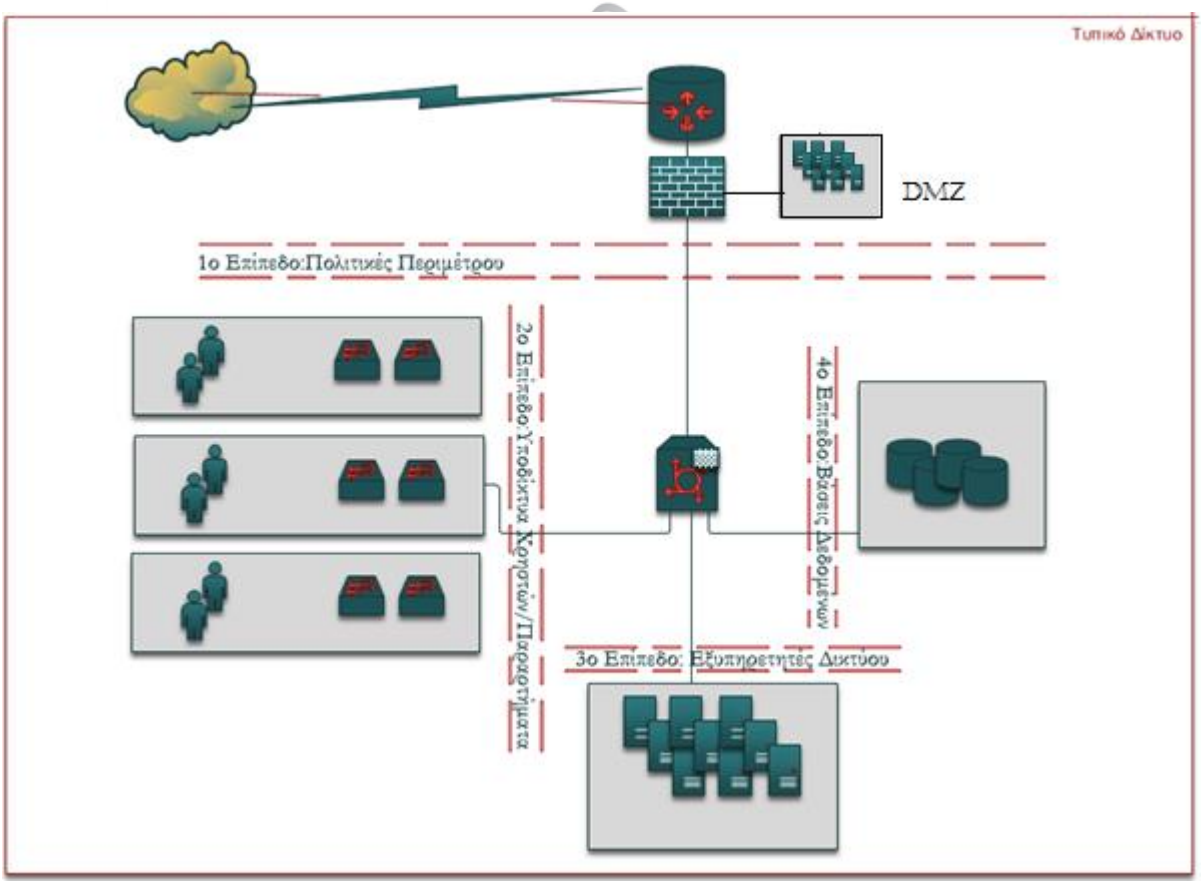
Πίνακας 18: Προϊόντα NAC προς σύγκριση από Network World (2012)

4 Ανάπτυξη Εφαρμογής SECART

Στο παρόν κεφάλαιο περιγράφεται η ανάπτυξη μιας τεχνικής λύσης υπό τη μορφή εφαρμογής ιστού που θα επεξεργάζεται συμβάντα ασφαλείας από γνωστές εφαρμογές και προϊόντα ασφαλείας , θα τα συσχετίζει βάση ορισμένων κανόνων, θα τα παρουσιάζει στον χειριστή της κατηγοριοποιημένα βάση κρισιμότητας και θα εκτελεί αν απαιτείται αυτοματοποιημένες ενέργειες απομόνωσης ή απαγόρευσης της δικτυακής οντότητας στην οποία οφείλεται η επίθεση.

Περιγραφή Δικτυακού Περιβάλλοντος

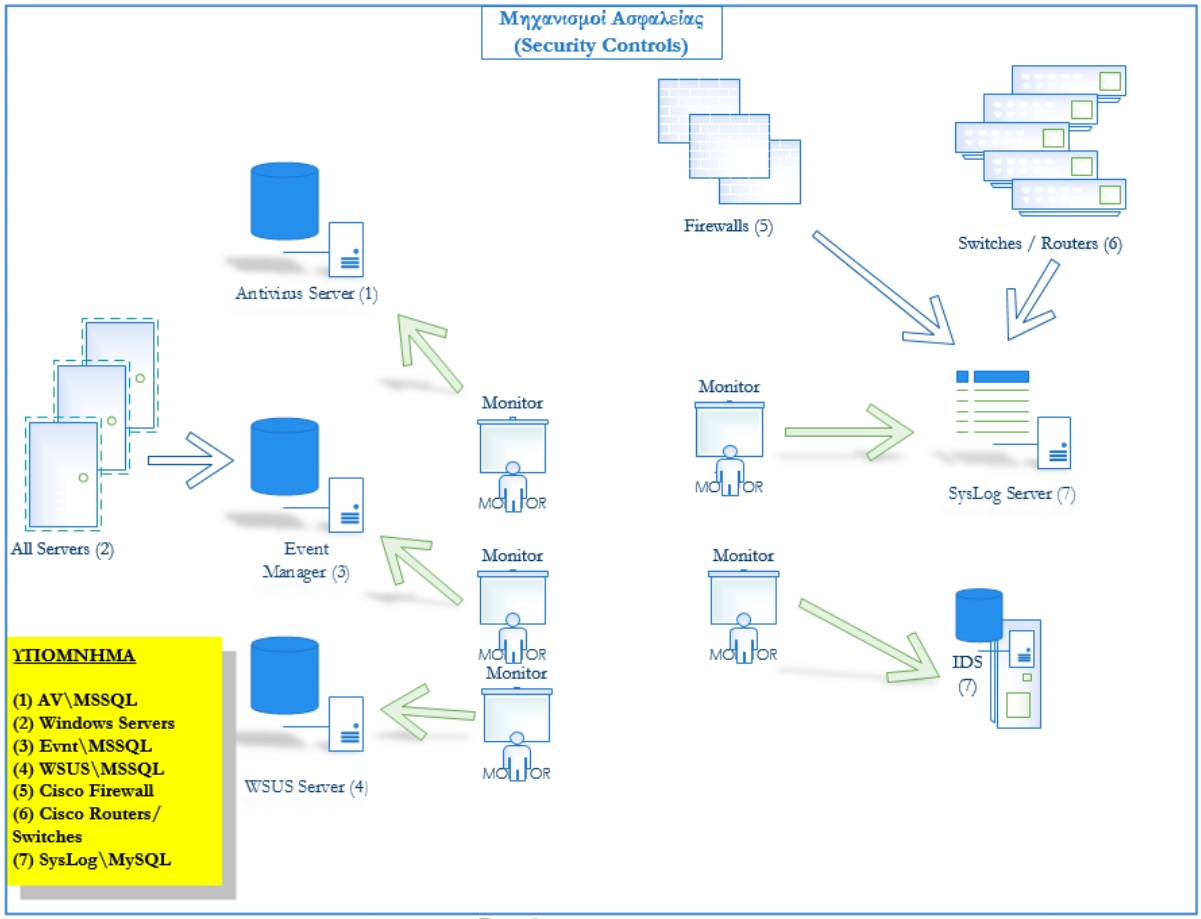
Η εφαρμογή που αναπτύχθηκε, μπορεί να εφαρμοστεί σε οποιοδήποτε Δικτυακό περιβάλλον. Στη περίπτωση μας εφαρμόζεται στο τυπικό δικτυακό περιβάλλον αναφοράς που απεικονίζεται στην εικόνα 20.



Εικόνα 20: Τυπικό δικτυακό περιβάλλον αναφοράς

Σε κάθε σύγχρονο δικτυακό περιβάλλον εφαρμόζεται μια λογική διαμερισματοποίησης, που απομονώνει τους πόρους και τις υπηρεσίες του με τρόπο συμβατό στην εκάστοτε πολιτική ασφαλείας. Η διαμερισματοποίση μας οδηγεί αναγκαστικά στη δημιουργία πολυεπίπεδων δικτύων. Τα πολυεπίπεδα δίκτυα διευκολύνουν στην εφαρμογή πολιτικών ασφαλείας και στη υλοποίηση αξιόπιστων μηχανισμών έλεγχου της δικτυακής κίνησης. Στην εικόνα 20, το δίκτυο που παρουσιάζεται, εκτός της DMZ, παρουσιάζει 4 επίπεδα. Στο επίπεδο 0, εφαρμόζονται οι πολιτικές της DMZ. Στο 1ο επίπεδο, που υλοποιεί την περίμετρο του δικτύου, εφαρμόζονται οι πολιτικές περιμέτρου: τι δικτυακή κίνηση επιτρέπεται, πως θα εξασφαλιστεί αυτή, πότε επιτρέπεται και γιατί επιτρέπεται. Στο 2ο επίπεδο, εφαρμόζονται πολιτικές σχετικές με τα υποδίκτυα των χρηστών. Ανάλογα με το παράρτημα που ανήκει ο χρήστης συνήθως τοποθετείται σε αντίστοιχο υποδίκτυο και εφαρμόζονται ανάλογες πολιτικές δικτύου. Στο 3ο επίπεδο, συνήθως εντοπίζουμε, τη φάρμα με τους εξυπηρετητές του εσωτερικού δικτύου. Στο 4ο επίπεδο συναντάμε τις Βάσεις Δεδομένων του οργανισμού, που αποθηκεύουν την ποιό κρίσιμη πληροφορία του οργανισμού και η ασφάλεια της χρήζει ιδιαίτερης προσοχής.

Στην εικόνα 21 παρουσιάζονται οι μηχανισμοί ασφαλείς που είναι εγκατεστημένοι στο προς εξέταση δίκτυο και ο τρόπος που γίνεται η συλλογή των αρχείων καταγραφής συμβάντων ασφαλείας.



Εικόνα 21: Μηχανισμοί ασφαλείας και καταγραφή αρχείων συμβάντων ασφαλείας (χωρίς συγκεντρωτική διαχείριση)

Αναλυτικότερα, όπως φαίνεται και στην εικόνα 21, τα συμβάντα ασφαλείας από το Firewall, Router, Switch(es) καταγράφονται σε SysLog-ng Server [38]. Ο SysLog-ng χρησιμοποιεί σύστημα διαχείρισης σχεσιακής ΒΔ MySQL [39]. Το ίδιο σύστημα χρησιμοποιεί και το IDS του οργανισμού για να αποθηκεύσει τα δικά του καταγεγραμμένα συμβάντα ασφαλείας. Τα συμβάντα ασφαλείας από τον μηχανισμό προστασίας από κακόβουλο λογισμικό, τα συμβάντα ασφαλείας από Εξυπηρετητές του οργανισμού, καθώς και πληροφορίες από τον εξυπηρετητή ενημερώσεων ασφαλείας της microsft (wsus) [40] καταγράφονται σε σύστημα διαχείρισης σχεσιακής ΒΔ MSSQL [41]. '

Η αποκέντρωση των συμβάντων ασφαλείας σε πολλές ΒΔ, δημιουργεί δυσχέρειες στην συγκέντρωση τους και στη συσχέτιση τους. Η Λύση στο παραπάνω πρόβλημα επιτυγχάνεται με τρεις τρόπους:

α. Με εμπορικά SIEM, μεγάλων δυνατοτήτων αλλά και μεγάλου κόστους

β. SIEM ανοικτού κώδικα, που καλύπτουν αρκετά αλλά όχι όλα τα αρχεία συμβάντων ασφαλείας από κατασκευαστές λογισμικού

γ. Ανάπτυξη εφαρμογών (In house Development) που καλύπτουν ακριβώς τις ανάγκες του οργανισμού, απαιτούν όμως χρόνο να αναπτυχθούν και προσωπικό για να συντηρηθούν.

Ανάλυση Απαιτήσεων

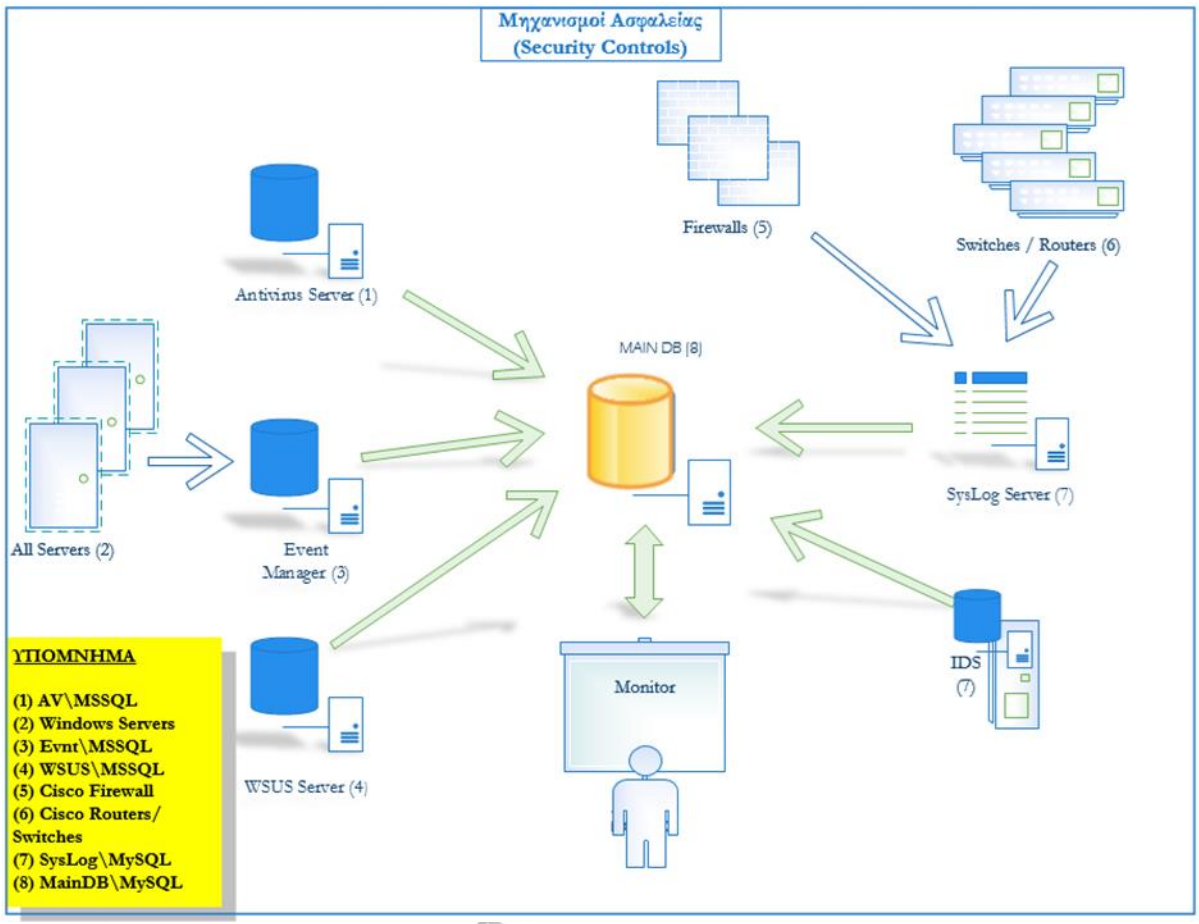
Στον πίνακα που ακολουθεί φαίνεται η ανάλυση των απαιτήσεων της εφαρμογής σε Λειτουργικές και Μη Λειτουργικές.

Λειτουργικές Απαιτήσεις (ΛΑ)	Μη-Λειτουργικές Απαιτήσεις (ΜΛΑ)
Να συλλέγει συμβάντα ασφαλείας από οποιοδήποτε σύστημα διαχείρισης σχεσιακής Βάσης Δεδομένων (cross database dialect)	Να είναι ανεπτυγμένη σε αντικειμενοστραφή γλώσσα προγραμματισμού
Να επιλέγει συγκεκριμένα συμβάντα (event filtering) για παρουσίαση.	Να είναι εφαρμογή ιστού (web application)
Μετά την αρχική ενημέρωση, να μπορεί να επιτελεί αυξητικά (incremental updates) επερωτήματα, μόνο για τα νέα συμβάντα ασφαλείας.	Να χρησιμοποιεί γνωστά και ανοικτά πλαίσια (frameworks)
Να δίνει την δυνατότητα στον διαχειριστή της εφαρμογής να ορίζει την συχνότητα χρονοπρογραμματισμού (update scheduling) των ενημερώσεων.	Να δίνει τη δυνατότητα εύκολης αναβάθμισης
Να αποθηκεύει τα συλλεχθέντα συμβάντα σε κεντρικό σύστημα διαχείρισης σχεσιακής Βάσης Δεδομένων(event aggregation)	Να μπορεί να τρέξει σε εξυπηρετητή μικρών υπολογιστικών απαιτήσεων
Να δίνει τη δυνατότητα συσχετισμού των	Να παρουσιάζει τα αποτελέσματα της

συλλεχθέντων συμβάντων ασφαλείας (event correlation)	συλλογής και συσχέτισης των συμβάντων με δυναμικά γραφικά και πίνακες.
Ο συσχετισμός να γίνεται βάση χαρακτηριστικών όπως ο χρόνος εμφανίσεως και η διάρκεια, ο τύπος ή η κρισιμότητα του συμβάντος.	
Να δίνει τη δυνατότητα δημιουργίας νέων κανόνων συσχέτισης συμβάντων.	
Για τα συσχετισμένα συμβάντα να υπολογίζει το μέτρο κρισιμότητας	
Για συσχετισμένα συμβάντα που ξεπερνούν ένα προκαθορισμένο κατώφλι (critical threshold) κρισιμότητας να λαμβάνει συγκεκριμένες αυτοματοποιημένες ενέργειες.	
Να δίνει τη δυνατότητα ενημέρωσης στον διαχειριστή της εφαρμογής για το ιστορικό αυτοματοποιημένων ενεργειών.	

Πίνακας 19: Λειτουργικές και μη λειτουργικές απαιτήσεις

Από την ανάλυση απαιτήσεων της εφαρμογής γίνεται σαφές ότι η εικόνα 21, που απεικονίζει πολλαπλούς μηχανισμούς ασφαλείας να καταγράφουν τα συμβάντα τους σε ξεχωριστές ΒΔ και το προσωπικό που είναι υπεύθυνο για την δικτυακή ασφάλεια του οργανισμού να πρέπει να συσχετίσει τα συμβάντα με μη αυτοματοποιημένους τρόπους , μετεξελίσσεται στην εικόνα 22.



Εικόνα 22: Μηχανισμοί ασφαλείας και καταγραφή αρχείων συμβάντων ασφαλείας (με συγκεντρωτική διαχείριση)

Στην νέα πλέον κατάσταση (εικόνα 22) το προσωπικό που είναι υπεύθυνο για την δικτυακή ασφάλεια του οργανισμού αρκεί να παρακολουθεί την κύρια ΒΔ και να δημιουργεί κανόνες συσχέτισης για την αυτοματοποιημένη και έγκαιρη εύρεση συμβάντων ασφαλείας που έχουν καταγραφεί σε έναν ή περισσότερους μηχανισμούς ασφαλείας.

Αρχιτεκτονική

3.1.1 Γενικά – Πλαίσια - Βιβλιοθήκες

Η εφαρμογή έχει αναπτυχθεί σε γλώσσα προγραμματισμού java enterprise edition (EE 6.0) [42]. Για την ανάπτυξή της χρησιμοποιήθηκαν τα παρακάτω πλαίσια (frameworks):

- JavaServer(TM) Faces technology [43]

- Spring Framework [44]
- Hibernate Framework [45]

Και οι παρακάτω βιβλιοθήκες:

- MSSQL JDBC Driver (sqljdbc4) [46]
- mySQL JDBC Driver (mySQL-java-connector) [47]
- css parser (cssparser) [48]
- xml parser (dom4j) [49]
- Logger (log4j) [50]
- Scheduler (quartz) [51]

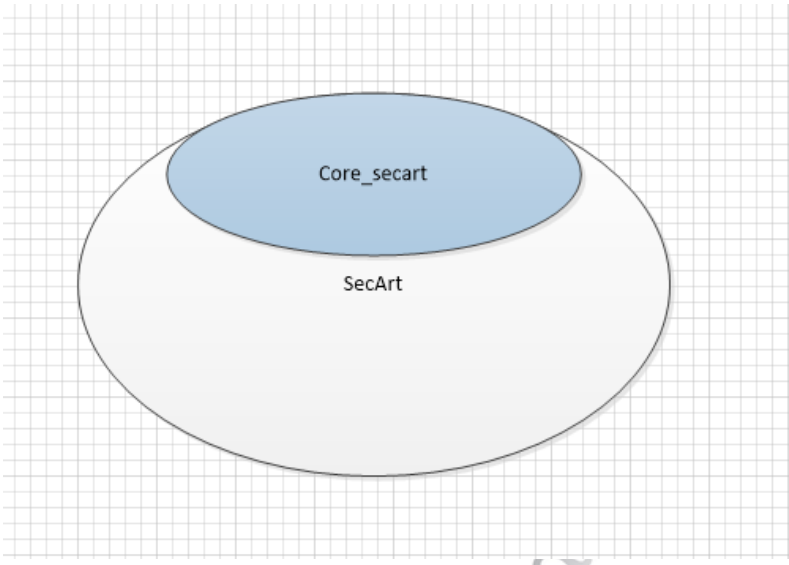
Ο εξυπηρετητής εφαρμογών ιστού (application server) που χρησιμοποιήθηκε είναι ο Apache Tomcat 7.0.27.0 [52]

Το IDE που χρησιμοποιήθηκε για την ανάπτυξη της εφαρμογής είναι το NetBeans 7.2 [53]

Η Εφαρμογή έχει αναπτυχθεί με βάση την αρχιτεκτονική εφαρμογής ιστού τριών επιπέδων (3 tier web application) [54] και συγκεκριμένα κάνοντας χρήση του μοντέλου Model–view–controller (MVC) [55]

3.1.2 Κύρια Συστατικά της Εφαρμογής

Η εφαρμογή SecArt περιέχει δύο βασικά συστατικά που αποτελούν από μόνα τους και ανεξάρτητα project (εικόνα 23). Αυτά είναι:



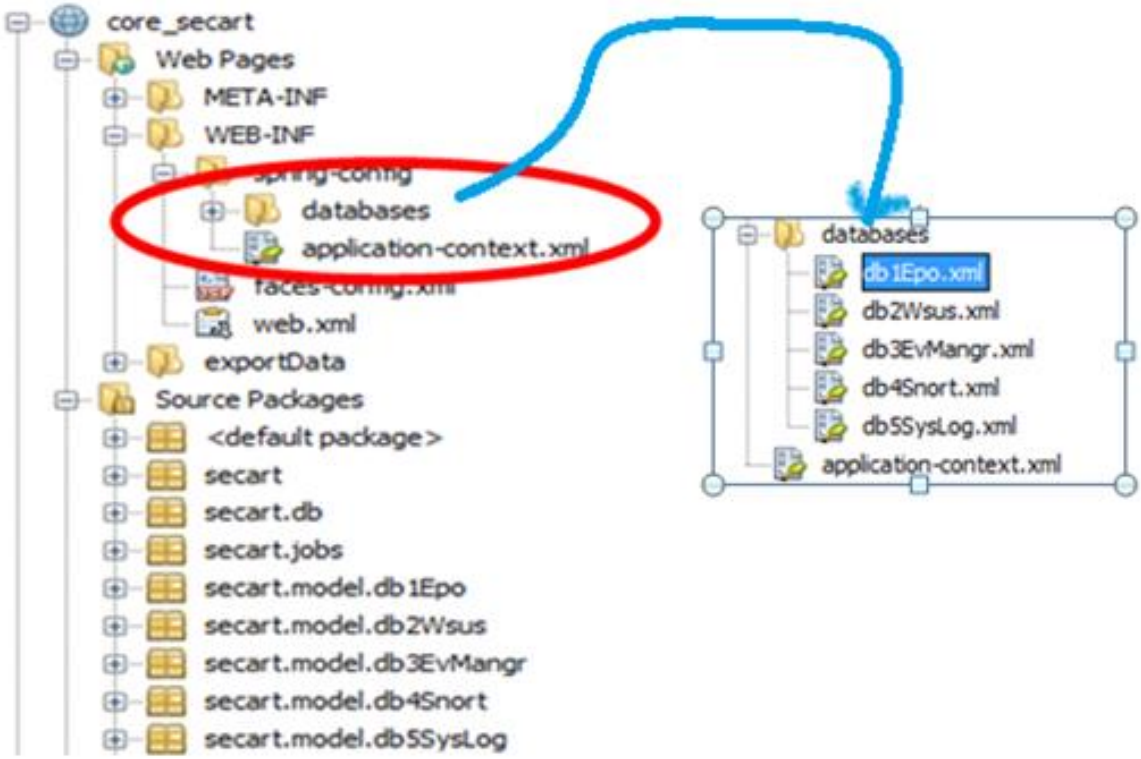
Εικόνα 23: Βασικά συστατικά της Εφαρμογής

Το πρώτο συστατικό φέρει το όνομα **Core_secart** και αποτελεί τον «πυρήνα» της εφαρμογής. Είναι υπεύθυνο για την σύνδεση με γνωστές σχεσιακές ΒΔ (π.χ MSSQL, Oracle, MySQL κτλ), την ανάγνωση από αυτές των επιλεγμένων συμβάντων ασφαλείας και την εγγραφή αυτών στην κύρια ΒΔ που στην περίπτωσή μας είναι η «maindb». Έχει επιλεχθεί για την «maindb» το σύστημα διαχείρισης σχεσιακής ΒΔ MySQL. Είναι ανεπτυγμένο ως Java EE project με χρήση του Spring, Quartz και Hibernate.

Το δεύτερο συστατικό φέρει το όνομα **Secart** και αποτελεί το μέρος της εφαρμογής που σχετίζεται με την λογική των συσχετίσεων, την λήψη αυτόματων ενεργειών και την παρουσίαση των αποτελεσμάτων μέσα ιστοσελίδες. Κάνει αποκλειστική χρήση της «maidb» και είναι ανεπτυγμένο ως Java EE project με χρήση των JSF, CSS, EJB, Hibernate.

3.1.2.1 Ανάλυση Core_secart

Η δομή του Core_secart φαίνεται στην εικόνα 24.



Εικόνα 24: Η δομή του Core_secart

Διακρίνουμε τον φάκελο databases, ως υποφάκελο του Spring-config. Εκεί δημιουργούμε τα **dbxyyy.xml** αρχεία που αποτελούν τις δηλώσεις των bean [56] του Spring και αφορούν στη προσθήκη νέων βάσεων δεδομένων και το αρχείο **application-context.xml** που αφορά στην «maindb» καθώς και στον χρονοπρογραμματισμό των της συχνότητας επικοινωνίας με τις ΒΔ που έχουν προδιαγραφεί στα αρχεία της μορφής dbxyyy.xml. Αναλυτικότερα:

- Η Δομή των dbxyyy.xml αρχεών φαίνεται στο παρακάτω, db1Epo.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<beans xmlns="http://www.springframework.org/schema/beans"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.springframework.org/schema/beans
            http://www.springframework.org/schema/beans/spring-beans-3.1.xsd">
    <!—Δηλώνουμε το Sprng bean MonitoredDatabaseImpl -->
<bean id="epoid" class="secart.MonitoredDatabaseImpl">
    <!—Την ιδιότητα displayName την χρησιμοποιούμε κυρίως για λόγους καταγραφής (loggin) -
->
    <property name="displayName" value="DB1_epo"/>
    <!—Υλοποιείται το dataFetcher αντικείμενο της κλάσης-->
    <property name="dataFetcher">
      <bean class="secart.model.db1Epo.Db1EpoDataFetcher"/>
    </property>
    <!—Αυτό το πεδίο αναπαριστά την maindb, είναι σε όλα τα αρχεία ίδιο-->
    <property name="targetDbTransactions" ref="mainDbTransactions"/>
```

```
    <!-- Αυτό το πεδίο περιέχει όλες τις ρυθμίσεις για την σύνδεση με την εκάστοτε βάση.-->
    <property name="sourceDbTransactions">
      <bean class="secart.db.DbTransactions">
        <property name="sessionFactory">
          <bean class="org.springframework.orm.hibernate3.LocalSessionFactoryBean">
            <property name="dataSource">
              <bean class="org.apache.commons.dbcp.BasicDataSource" destroy-method="close">
                <property name="driverClassName"
                          value="com.microsoft.sqlserver.jdbc.SQLServerDriver"/>
                <property name="url"
value="jdbc:sqlserver://localhost:1433;databaseName=epo;"/>
                <property name="username" value="test"/>
                <property name="password" value="xxxxxxxx"/>
              </bean>
            </property>
            <property name="hibernateProperties">
              <props>
                <prop key="hibernate.dialect">org.hibernate.dialect.SQLServerDialect</prop>
                <prop key="hibernate.show_sql">true</prop>
                <!--na min kanei validate to schema me tin klasi-->
                <!--<prop key="hibernate.hbm2ddl.auto">validate</prop>-->
              </props>
            </property>
      <!—Σε αυτό το πεδίο βάζουμε την λίστα με τις αντιστοιχίσεις (mapping) του hibernate για
την ΒΔ-->
            <property name="mappingLocations">
              <list>
                <value>classpath:/secart/model/db1Epo/visitepo.hbm.xml</value>
                <value>classpath:/secart/model/db1Epo/visiteporogue.hbm.xml</value>
              </list>
            </property>
          </bean>
        </property>
      </bean>
    </property>
  </bean>
</beans>
```

Πίνακας 20: Δομή των Bean Configuration Files του Spring

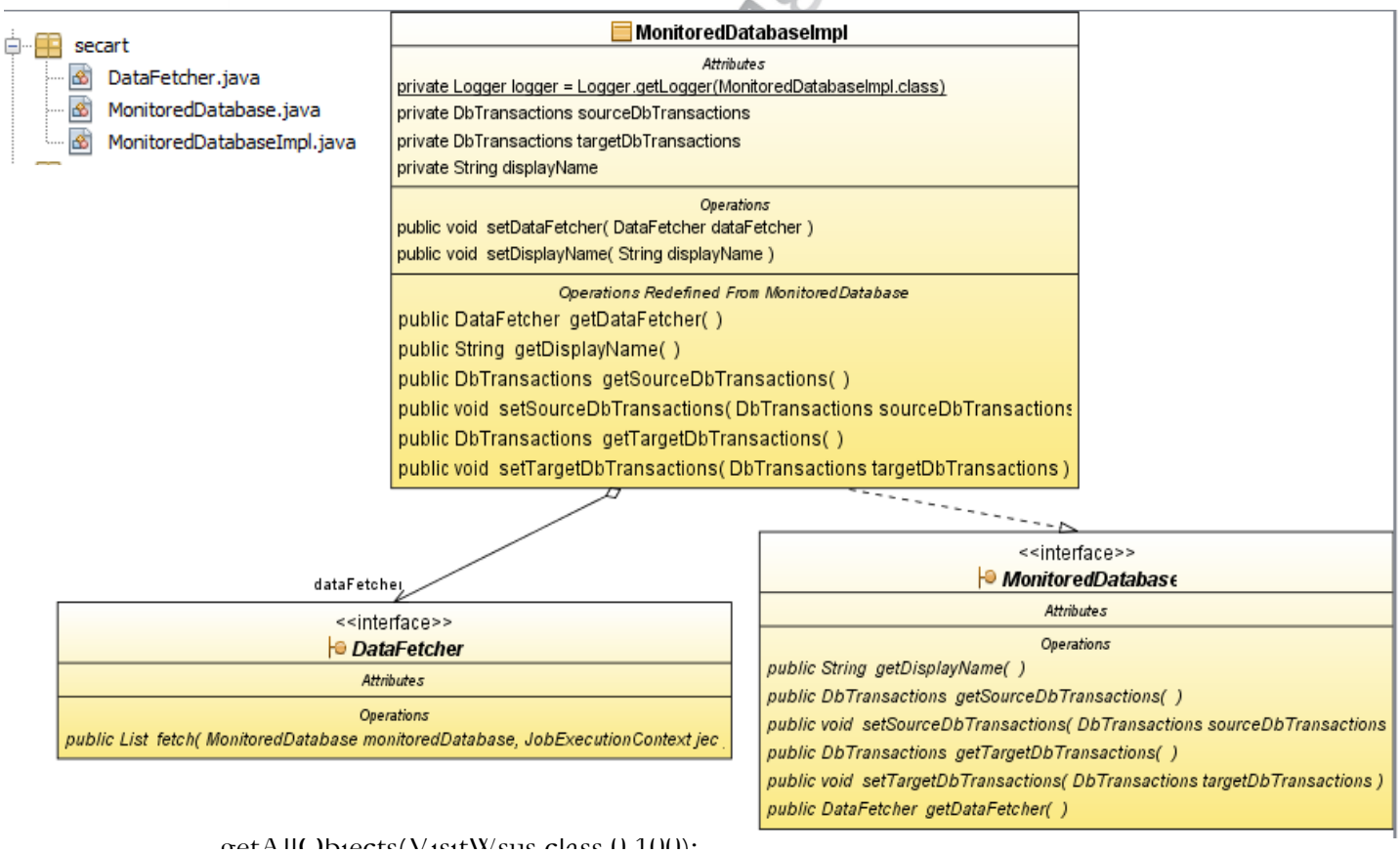
- Η Δομή του application-context.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<beans xmlns="http://www.springframework.org/schema/beans"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:context="http://www.springframework.org/schema/context"
    xsi:schemaLocation="http://www.springframework.org/schema/beans
    http://www.springframework.org/schema/beans/spring-beans-3.1.xsd
    http://www.springframework.org/schema/context
    http://www.springframework.org/schema/context/spring-context- 3.1.xsd">

<bean class="org.springframework.scheduling.quartz.SchedulerFactoryBean">
    <property name="triggers">
      <list><ref bean="everyXminutesJob"/> </list>
    </property>
    <property name="schedulerContextAsMap">
```

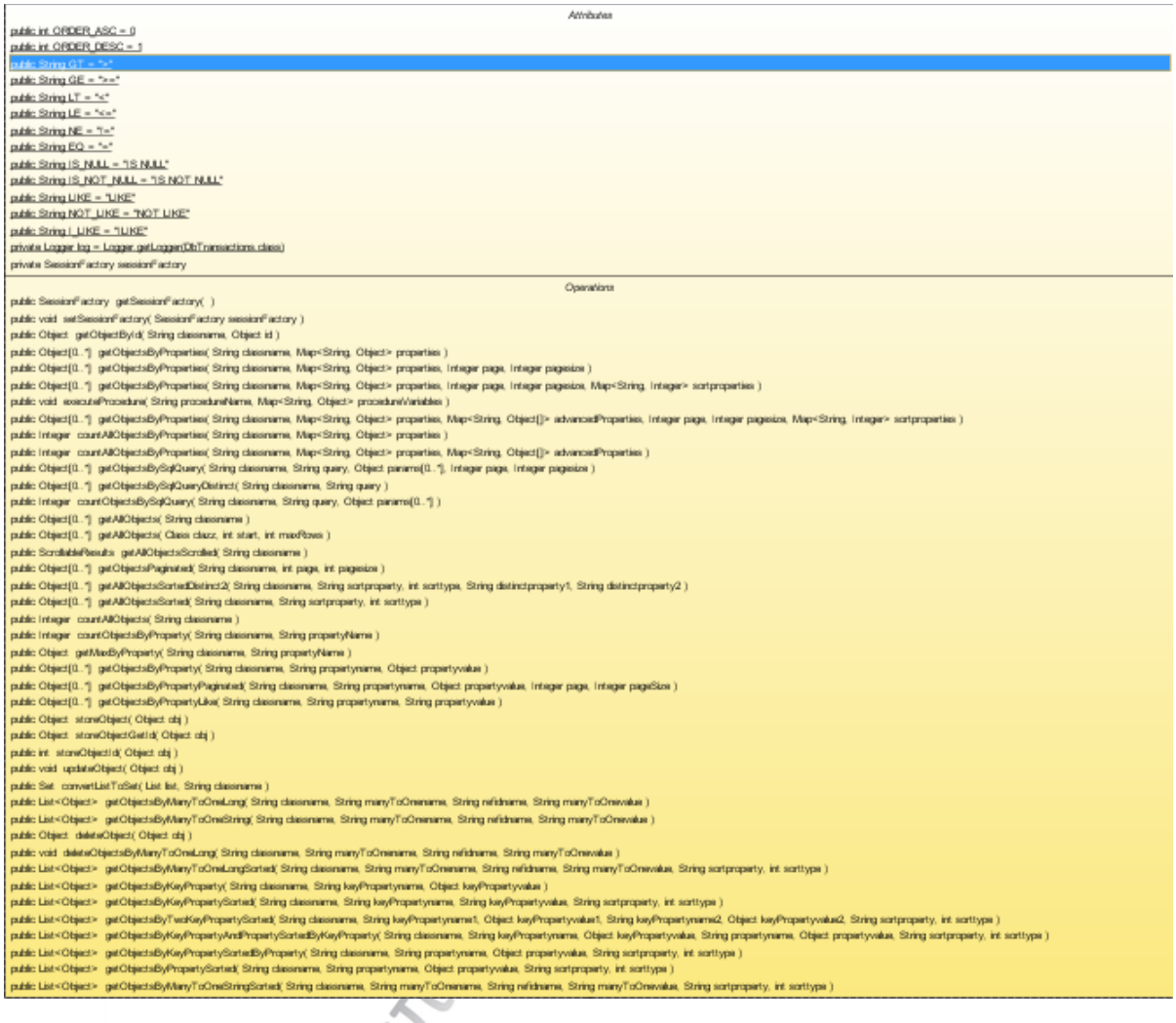
```
        <map>    <entry key="databases"> </entry>
          <entry key="mainDbTransactions" value-ref="mainDbTransactions"/>
        </map>
      </property>
      <property name="applicationContextSchedulerContextKey">
        <value>applicationContext</value>
      </property>
    </bean>
    <!—Εδώ ρυθμίζεται το ο χρόνος ενεργοποίησης της Προγραμματισμένης Διεργασίας-->
    <bean id="everyXminutesJob" class="org.springframework.scheduling.quartz.SimpleTriggerBean">
      <property name="jobDetail" ref="job"/>
      <property name="repeatInterval" value="240000"/>
    </bean>
    <!—Εδώ αναπαριστάται η εργασία που τρέχει περιοδικά.-->
    <bean name="job" class="org.springframework.scheduling.quartz.JobDetailBean">
      <property name="jobClass" value="secart.jobs.ProcessDatabasesJob"/>
      <property name="jobDataAsMap">
        <map>  </map>
      </property>
    </bean>
    <!—Εδώ παρέχονται οι μέθοδοι για ανάκτηση και αποθήκευση της maindb από τις ΒΔ τις επιλογής μας-->
    <bean id="mainDbTransactions" class="secart.db.DbTransactions">
      <property name="sessionFactory">
        <bean class="org.springframework.orm.hibernate3.LocalSessionFactoryBean">
          <property name="dataSource" ref="targetDataSource"/>
          <property name="hibernateProperties">
            <props>
              <prop key="hibernate.dialect">org.hibernate.dialect.MySQLDialect</prop>
              <prop key="hibernate.show_sql">true</prop>
              <prop key="hibernate.hbm2ddl.auto">update</prop>
            </props>
          </property>
          <property name="mappingLocations">
            <list>
              <value>classpath:/secart/model/db1Epo/visitepo.hbm.xml</value>
              <value>classpath:/secart/model/db1Epo/visiteporogue.hbm.xml</value>
              <value>classpath:/secart/model/db2Wsus/visitWsus.hbm.xml</value>
              <value>classpath:/secart/model/db3EvMangr/visitEvMangr.hbm.xml</value>
              <value>classpath:/secart/model/db4Snort/visitSnort.hbm.xml</value>
              <value>classpath:/secart/model/db5SysLog/visitSysLog.hbm.xml</value>
            </list>
          </property>
        </bean>
      </property>
    </bean>
    <!—Εδώ παρέχονται τα στοιχεία για σύνδεση στην maidb-->
    <bean id="targetDataSource" class="org.apache.commons.dbcp.BasicDataSource" destroy-method="close">
      <property name="driverClassName"  value="com.mysql.jdbc.Driver"/>
      <property name="url" value="jdbc:mysql://localhost:3306/maindb"/>
      <property name="username" value="root"/>
      <property name="password" value="XXXXXXXXXX"/>
    </bean>

    <context:component-scan base-package="secart"/>
    <context:annotation-config/>
</beans>
```

Πίνακας 21: Δομή του Spring application-context.xml

- *Package Secart:* Όπως φαίνεται και στην εικόνα 25, το πακέτο Secart, περιέχει:
  - Το interface [57] *DataFetcher.java* καλείται από τον scheduler κάθε φορά που απαιτείται να κληθούν τα νέα συμβάντα από τις ΒΔ. Ποιο συγκεκριμένα καλείται η μέθοδος *fetch*. Απαιτεί συγκεκριμένη υλοποίηση για κάθε ΒΔ.
  - Το interface *MonitoredDatabase.java* καλείται από την κλάση *MonitoredDatabaseImpl.java*
  - Η κλάση *MonitoredDatabaseImpl.java* αναπαριστά την ΒΔ από την από την οποία θα ζητήσουμε τα συμβάντα ασφαλείας. Είναι γενική και παρόμοια για κάθε μια και προσφέρει πεδία τα οποία είναι συγκεκριμένα για κάθε βάση. Το κυριότερο πεδίο είναι το αντικείμενο *DataFetcher* το οποίο περιέχει και τη λογική της κάθε ΒΔ. Η ρύθμιση της κάθε ΒΔ γίνεται από τα spring xml αρχεί ***dbxyyy.xml*** .

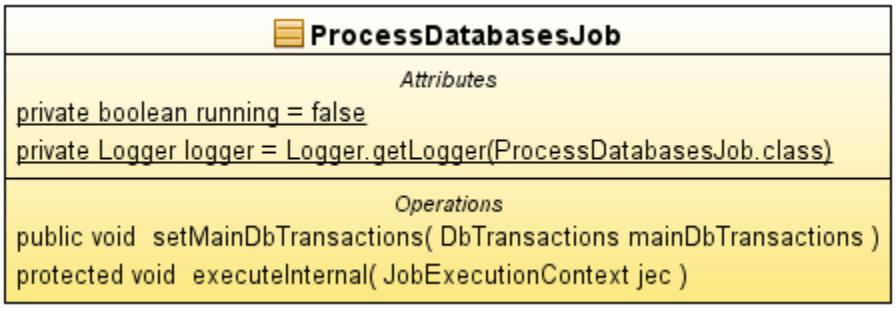


Εικόνα 25: Package Secart Class Diagram



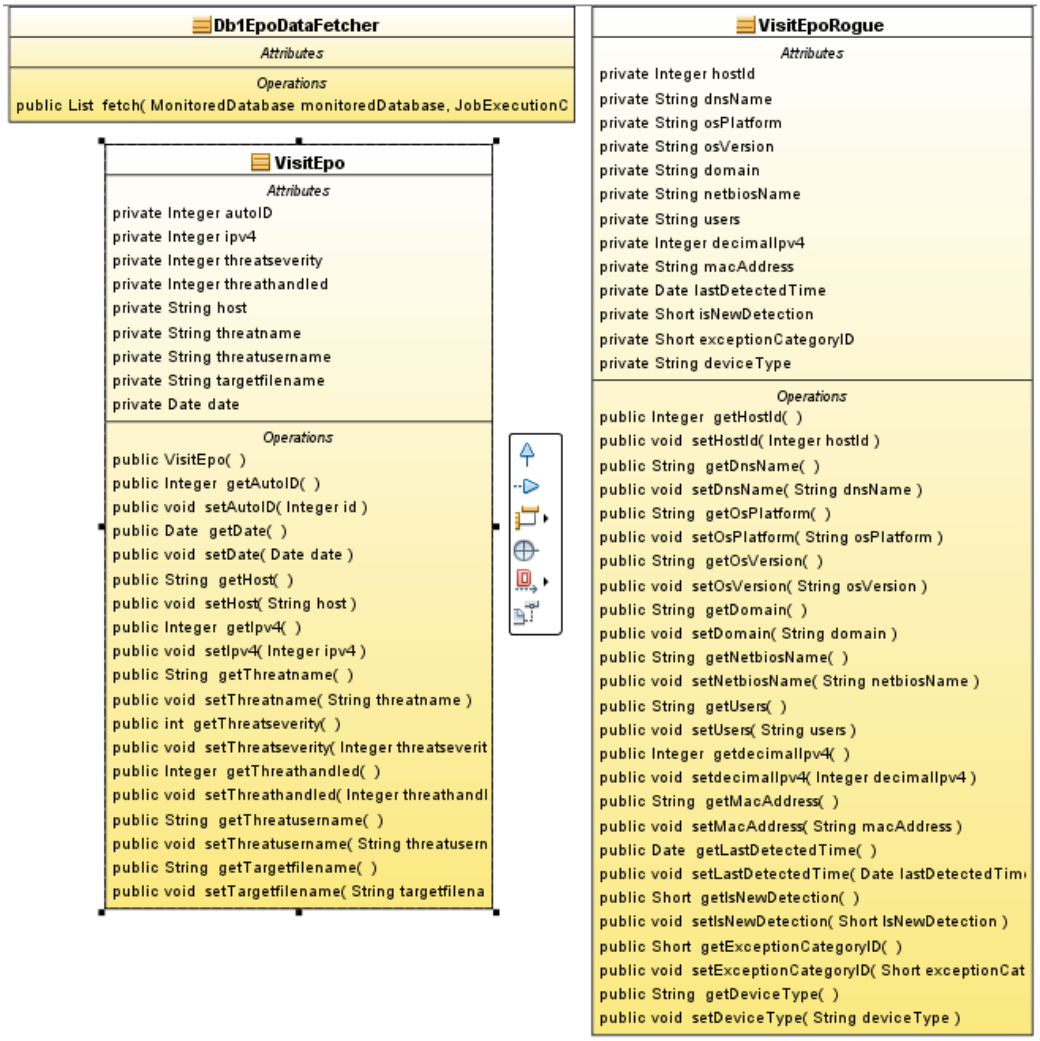
Εικόνα 26: Class DbTransactions.java

- *Package secart.job: Περιέχει την κλάση class ProcessDatabasesJob.java (εικόνα 27) Αυτή η κλάση αναπαριστά την διεργασία που θα τρέχει περιοδικά και θα ψάχνει σε όλες τις Β_Δ να φέρει νέα συμβάντα ασφαλείας.*
    - *Υλοποιεί την μέθοδο executeInternal η οποία καλείται από το Quartz.*
    - *Βρίσκει όλα τα αντικείμενα τύπου MonitoredDatabase που έχουν δηλωθεί και εκτελεί την getDataFetcher().fetch().*
    - *Ότι αποτελέσματα επιστρέφει από την dataFetcher, τα αποθηκεύει στην maindb.*



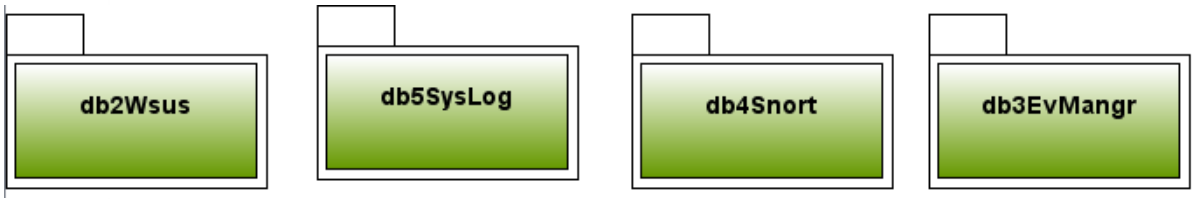
Εικόνα 27: Class ProcessDatabasesJob.java

- *Package secart.job (εικόνα 28)*: Περιέχει τις κλάσεις:
  - *Db1EpoDataFetcher.java* – Υλοποιεί την DataFetcher για την ΒΔ db1Epo. Φέρνει κάθε φορά που καλείται τις νέες εγγραφές (νέα συμβάντα ασφαλείας)
  - *VisitEpo.java* και *VisitEpoRogue* – τα Beans για την αποθήκευση και χρήση των εγγραφών που κλήθηκαν.



Εικόνα 28: Package secart.job

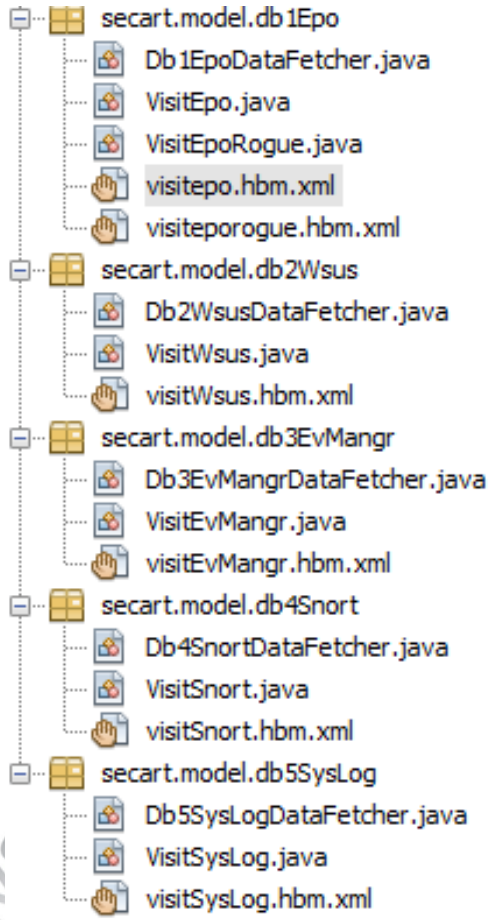
- *Packages Secart.model.db2Wsus, Secart.model.db5SysLog, Secart.model.db4Snort, Secart.model.db3EvMangr* (εικόνα 29): Ισχύει ότι ακριβώς και στην περίπτωση του Package secart.job.



Εικόνα 29: Packages db2Wsus, db5SysLog, db4Snort, db3EvMangr

- Hibernate mapping: Για κάθε μοντέλο που δημιουργούμε για να επικοινωνήσει με μια από τις υποψήφιες ΒΔ συλλογής συμβάντων θα πρέπει να δημιουργήσουμε και το

αντίστοιχο .hbm.xml αρχείο, που είναι απαραίτητο στο Hibernate για την αντιστοίχιση (mapping) μεταξύ της ΒΔ πηγής και της ΒΔ προορισμού. Στην εικόνα 30 φαίνονται όλα τα μοντέλα με τα αρχεία .hbm και στην εικόνα 31 φαίνεται το περιεχόμενο ενός τέτοιου αρχείου.



Εικόνα 30: Μοντελα και αντιστοιχίες

```
<?xml version="1.0"?>
<!DOCTYPE hibernate-mapping PUBLIC "-//Hibernate/Hibernate Mapping
DTD 3.0//EN"
"http://hibernate.sourceforge.net/hibernate-mapping-3.0.dtd">
<!—Αντιστοιχούμε στήλες από τον πίνακα της ΒΔ που θέλουμε να διαβάσουμε με τις
αντίστοιχες ιδιότητες των αντικειμένων που δημιουργούμε-->
<hibernate-mapping>
   <class name="secart.model.db1Epo.VisitEpo" table="EPOEvents">
      <id name="autoID" type="int" column="AutoID"></id>
      <property name="date" column="DetectedUTC"></property>
      <property name="host" column="TARGETHOSTNAME"
type="java.lang.String"></property>
      <property name="ipv4" column="AnalyzerIPV4"></property>
```

```
      <property name="threatname" column="THREATNAME"></property>
      <property name="threatseverity"
column="THREATSEVERITY"></property>
      <property name="threathandled"
column="THREATHANDLED"></property>
      <property name="threatusername"
column="TARGETUSERNAME"></property>
      <property name="targetfilename"
column="TARGETFILENAME"></property>
   </class>
</hibernate-mapping>
```

Πίνακας 22: Υπόδειγμα hbm.xml αρχείου για αντιστοίχιση πινάκων – αντικειμένων από το Hibernate

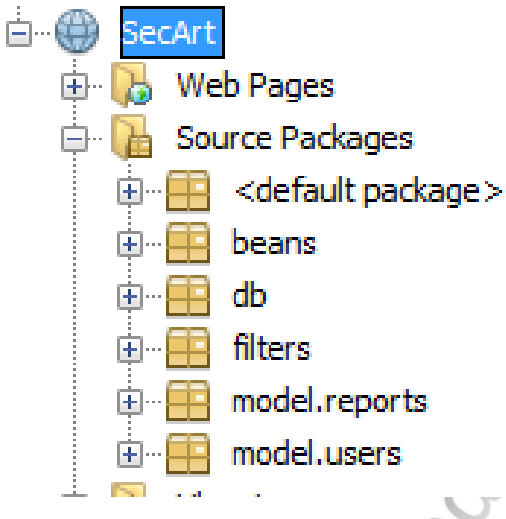
3.1.2.2 Ανάλυση SecArt

Η εφαρμογή SecArt, αποτελεί το γραφικό μέρος της εφαρμογής και αφορά σε όλες τις ενέργειες που γίνονται από την στιγμή που τα συμβάντα ασφαλείας έχουν αποθηκευτεί στην maindb και ύστερα.

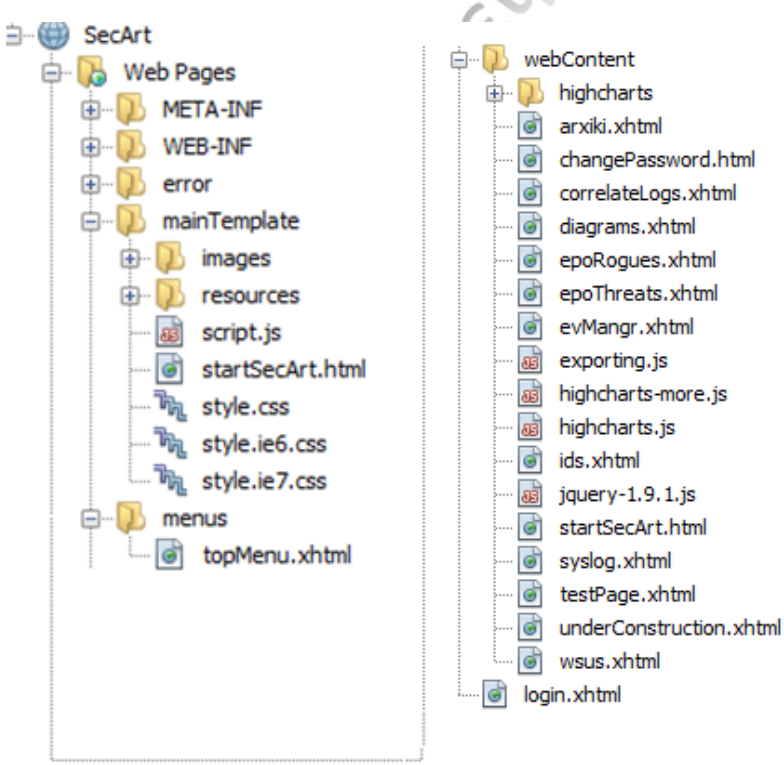
Χαρακτηριστικά της εφαρμογής:

- Είναι εφαρμογή ιστού που βασίζεται στην τεχνολογία JSF της Java.
- Χρησιμοποιούνται τα Rich Faces (AJAX) [58] για άμεση αλληλεπίδραση με τον χρήστη
- Περιέχει ενσωματωμένο API για χρήση πλήθους από charts που διατίθενται ελεύθερα ως charting library [59]
- Παρουσιάζει γραφικά στατιστικά για την κατάσταση του δικτύου, αναλύοντας τα συμβάντα που έχουν αποθηκευτεί στην maindb.
- Συσχετίζει συμβάντα βάση απλών sql κανόνων που εύκολα μπορεί να προστεθούν στην κλάση CorrelatedThreats.java
- Απομονώνει δικτυακά συμβάντα, αν μετά από συσχέτιση η κρισιμότητα τους περνά συγκεκριμένο κατώφλι κρισιμότητας (critical threshold).
- Κρατά αρχείο καταγραφής για αυτοματοποιημένες ενέργειες απομόνωσης (περισσότερες πληροφορίες στο Παράρτημα Γ: Οδηγίες Χρήσης)

Η δομή του SecArt φαίνεται στην εικόνα

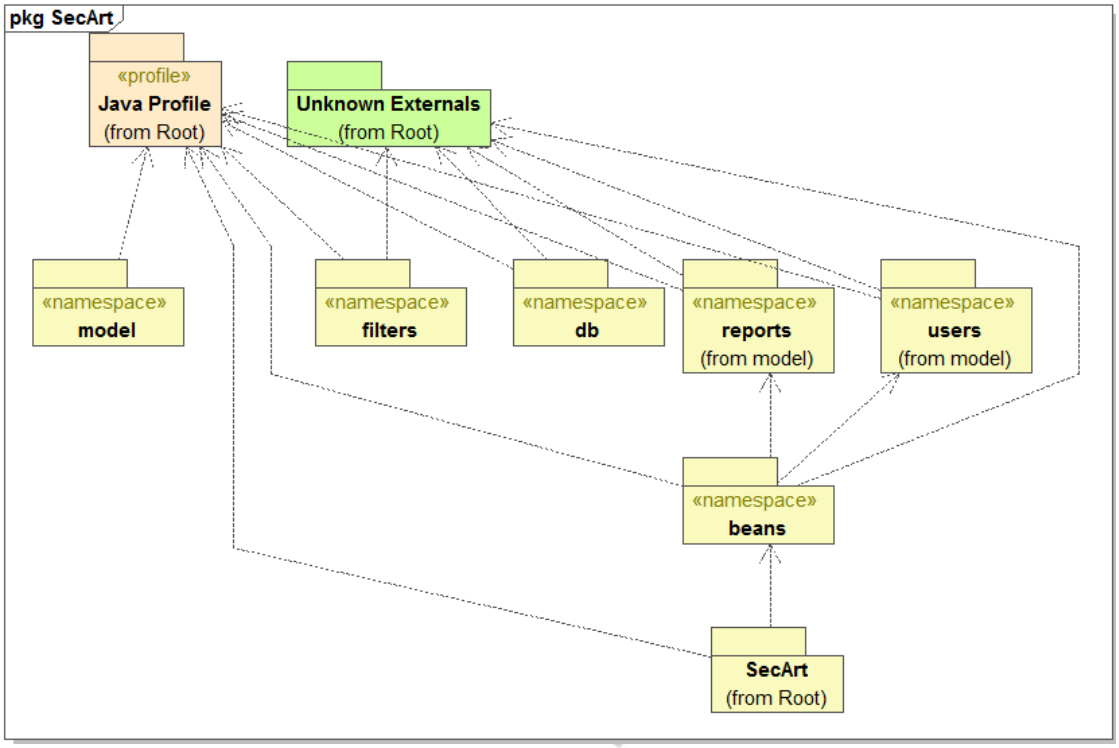


Εικόνα 31: Δομή SecArt



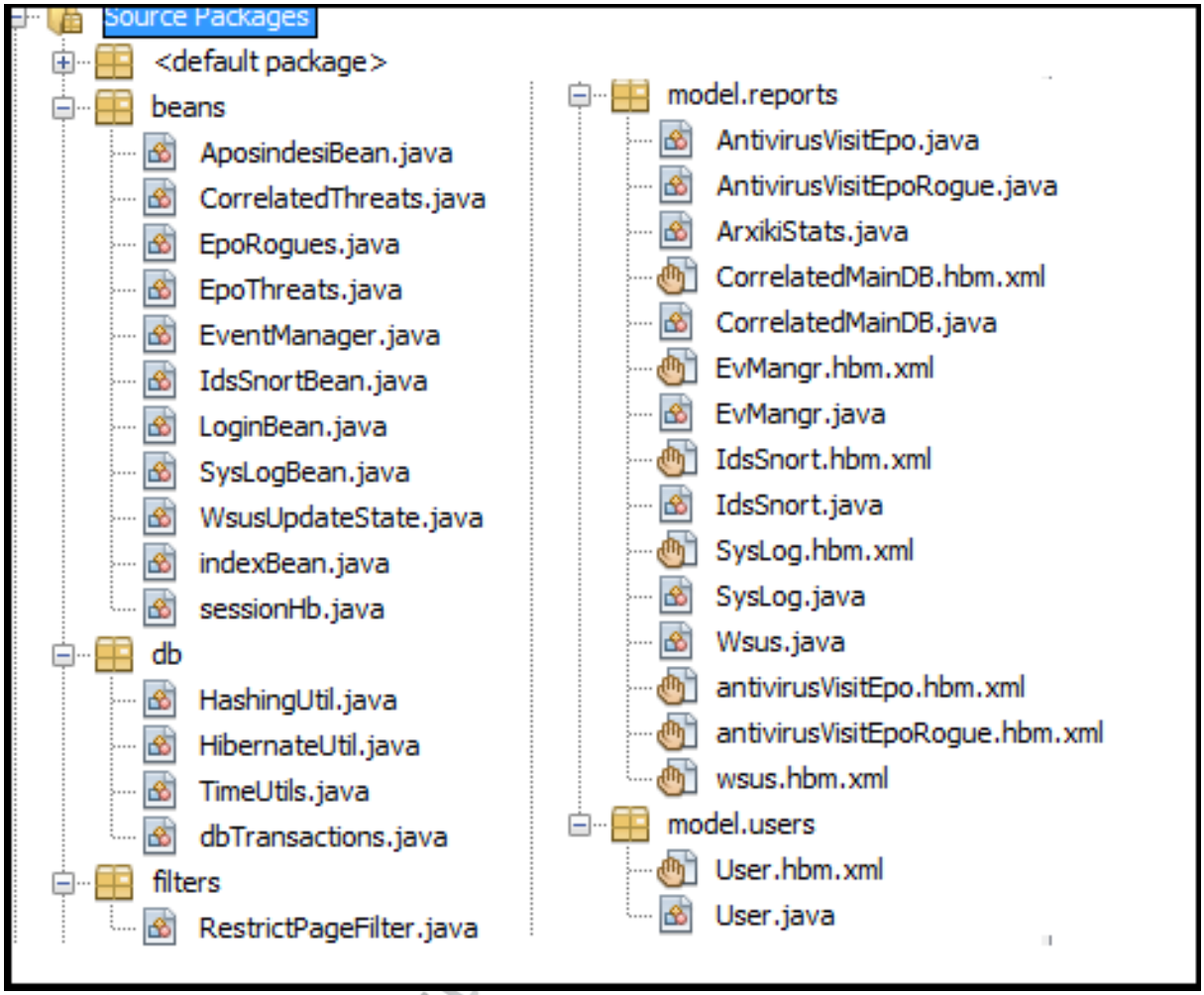
Εικόνα 32: Απεικόνιση των ιστοσελίδων που περιέχει το SecArt

Στην εικόνα 32 φαίνονται οι ιστοσελίδες που έχουν αναπτυχτεί, ενώ στην εικόνα 33 φαίνονται τα πακέτα και οι εξαρτήσεις αυτών.

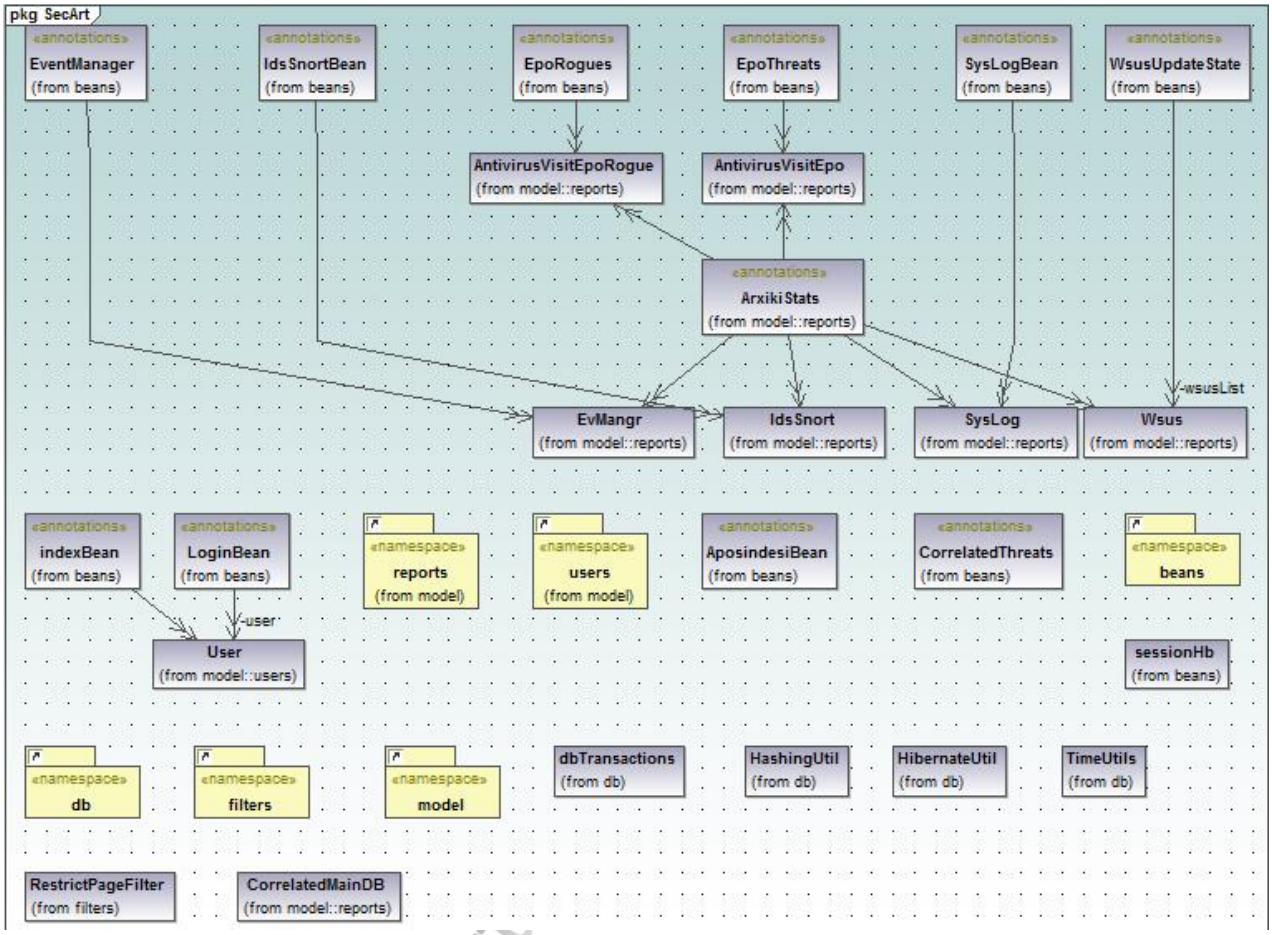


Εικόνα 33: Εξαρτήσεις Πακέτων (SecArt)

Στην εικόνα 34 φαίνονται τα πακέτα με τις κλάσεις και τα απαραίτητα hbm.xml αρχεία. αναλυτικότερα τα πακέτα και τα υποπακέτα της εφαρμογής με τις εξαρτήσεις αυτών.



Εικόνα 34:Πακέτα και κλάσεις (Secart)



Εικόνα 35: Περιεχόμενα πακέτων με εξαρτήσεις (SecArt)

3.2 Συμπεράσματα από την ανάπτυξη και λειτουργίας της εφαρμογής

Τα συμπεράσματα που προέκυψαν μετά την ανάπτυξη και λειτουργία της εφαρμογής, συνοψίζονται στα παρακάτω:

- Πριν την ανάπτυξη απαιτείται να έχει γίνει ανάλυση απαιτήσεων, με την βοήθεια των διαχειριστών και των υπευθύνων ασφαλείας των ΠΣ
- Μικρό κόστος ανάπτυξης: εφαρμογή αναπτύχθηκε με λογισμικό ανοικτού κώδικα.
- Για την ανάπτυξη της εφαρμογής απαιτείται από τον οργανισμό να έχει τουλάχιστον έναν προγραμματιστή.
- Η συντήρηση της εφαρμογής είναι σχετικά εύκολή, παρόλα αυτά είναι συνήθως χρονοβόρα.
- Η εφαρμογή δεν απαιτεί ισχυρούς υπολογιστικούς πόρους από πλευράς χρήστη

- Όλη η λογική της εφαρμογής μπορεί να υλοποιηθεί με sql ερωτήματα στην κύρια ΒΔ τύπου MySQL.
- Η εφαρμογή συνδυάζει χαρακτηριστικά από τόσο από SIEM όσο και από NAC Συστήματα. Στον Πίνακα που ακολουθεί φαίνεται τι καλύπτει σε αυτό το στάδιο της ανάπτυξης, χωρίς αυτό να σημαίνει ότι δεν μπορεί να βελτιωθεί σε επόμενες εκδόσεις της.

A/A	Λειτουργία	NAC	SIEM	SECART
1	Παρακολούθηση σε πραγματικό χρόνο (Real-time monitoring)	ΝΑΙ	ΝΑΙ	ΝΑΙ
2	Πληροφορίες για απειλές (Threat intelligence)	ΟΧΙ	ΝΑΙ	ΟΧΙ
3	Προφίλ κανονικής λειτουργίας (Behavior profiling)	ΟΧΙ	ΝΑΙ	ΟΧΙ
4	Παρακολούθηση χρηστών και δεδομένων (Data and user and monitoring)	ΟΧΙ	ΝΑΙ	ΟΧΙ
5	Παρακολούθηση εφαρμογών (Application monitoring)	ΝΑΙ	ΝΑΙ	ΟΧΙ
6	Αναλυτικές Παρουσιάσεις (Analytics - compliance reporting)	ΝΑΙ	ΝΑΙ	ΝΑΙ
7	Διαχείριση συμβάντων	ΝΑΙ	ΝΑΙ	ΝΑΙ

	(Log management)			
8	Απλότητα στην εγκατάσταση και τη χρήση (Deployment and support simplicity)	ΟΧΙ	ΟΧΙ	ΝΑΙ
9	Πολιτική (Policy)	ΝΑΙ	ΟΧΙ	ΝΑΙ
10	Έλεγχος Πρόσβασης (Access control)	ΝΑΙ	ΟΧΙ	ΝΑΙ

Πίνακας 23: Σύγκριση SIEM/NAC με εφαρμογή SECART

Βιβλιογραφία

[1] http://www.internetworldstats.com/stats.htm Feb 17, 2013.
[2] http://www.symantec.com/threatreport/ Feb 18, 2013.
[3] A Structured Approach to Computer Security
[4] Guidelines on Firewalls and Firewall Policy
[5] Guide to Intrusion Detection .pdf
[6] Guide to Malware Incident .pdf
[7] Creating a Patch and Vulnerability Management Program .pdf
[8] Guide to Computer Security Log Management.pdf
[9] http://www.iso.org/iso/ Mar 12, 2013.
[10] SECURITY EVENT CORRELATION AND MANAGEMENT SANS
[11] limmer2008survey.πδφ
[12] http://en.wikipedia.org/wiki/Event_correlation
[13] Event Correlation And SIEM Vendor Approaches.pdf
[14] essential ingredients for efective event corelation.pdf
[15] http://www.packetsource.com/article/enterprise-security/39999/event-correlation-in-security
[16] http://en.wikipedia.org/wiki/Security_information_management
[17] http://en.wikipedia.org/wiki/Network_Access_Control
[18] ByPassing_NAC.pdf
[19] nac-wp.pdf
[20] http://www.tenable.com/products/nessus
[21] http://www.microsoft.com/en-us/download/details.aspx?id=7558
[22] http://en.wikipedia.org/wiki/Security_event_manager
[23] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0067
[24] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0172
[25] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0936
[26] http://www.gartner.com/technology/reprints.do?id=1-1AMSMRL&ct=120523&st=sb&elq=f23b4882acf74ee2ad7b1cbed775ebdd
[27] http://www.informationweek.com/security/management/it-rates-ibms-q1-labs-top-siem-performer/240002862
[28] http://www.drdobbs.com/security/review-security-information-management-p/192700836?pgno=1
[29] http://www.emergingthreats.net/login/
[30] http://www8.hp.com/us/en/software-solutions/software.html?compURI=1214365#.UYvGv7VkN-o
[31] http://q1labs.com/
[32] https://www.netiq.com/products/sentinel/
[33] http://www.cisco.com/
[34] http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5707/ps8418/ps6128/prod_presentation0900aecd805456b4.pdf
[35] 50-57-171-168.static.cloud-ips.com/wp-content/media/2011-Gartner-Magic-Quadrant-NAC.pdf
[36] http://www.infotech.com/research/ss/it-vendor-landscape-network-access-control

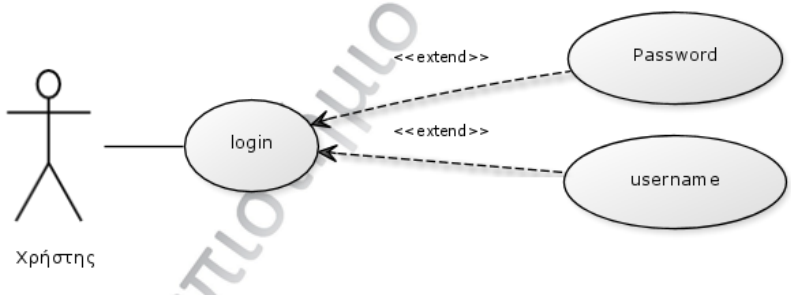
[37] http://www.networkworld.com/reviews/2010/062110-network-access-control-test-access.html
[38] https://wiki.archlinux.org/index.php/syslog-ng
[39] http://www.mysql.com/
[40] http://technet.microsoft.com/en-us/windowsserver/bb332157.aspx
[41] https://www.microsoft.com/en-us/sqlserver/default.aspx
[42] http://www.oracle.com/technetwork/java/javaee/overview/index.html
[43] https://javaserverfaces.java.net/
[44] http://spring.io/
[45] http://www.hibernate.org/
[46] http://msdn.microsoft.com/en-us/sqlserver/aa937724.aspx
[47] http://dev.mysql.com/downloads/connector/j/
[48] http://grepcode.com/snapshot/repo1.maven.org/maven2/net.sourceforge.cssparser/cssparser/0.9.5
[49] http://dom4j.sourceforge.net/dom4j-1.6.1/
[50] http://logging.apache.org/log4j/1.2/apidocs/org/apache/log4j/Logger.html
[51] http://quartz-scheduler.org/
[52] http://tomcat.apache.org/
[53] https://netbeans.org/
[54] http://www.techopedia.com/definition/24649/three-tier-architecture
[55] http://en.wikipedia.org/wiki/Model%E2%80%93view%E2%80%93controller
[56] http://docs.spring.io/spring/docs/3.0.0.M3/reference/html/ch04s04.html
[57] http://docs.oracle.com/javase/tutorial/java/concepts/interface.html
[58] http://www.jboss.org/richfaces/
[59] http://www.highcharts.com/

Παράρτημα Α: UML Διαγράμματα

Για αναφορά στην πλήρη τεκμηρίωση της εφαρμογής με UML διαγράμματα, επικοινωνήστε στο kalofiris@gmail.com

Διάγραμμα περιπτώσεων χρήσης (use case diagram)

Παρουσιάζουμε ενδεικτικά με διαγράμματα περιπτώσεων χρήσεως τις βασικές λειτουργίες της εφαρμογής SecArt. Η πρώτη βασική λειτουργία που αφορά στην είσοδο του χρήστη στο σύστημα (εικόνα 36), γίνεται μέσα από φόρμα εισόδου ονόματος χρήστη και κωδικού πρόσβασης. Αν η αυθεντικοποίηση είναι επιτυχής, ο χρήστης μεταβαίνει στην κύρια σελίδα της εφαρμογής.

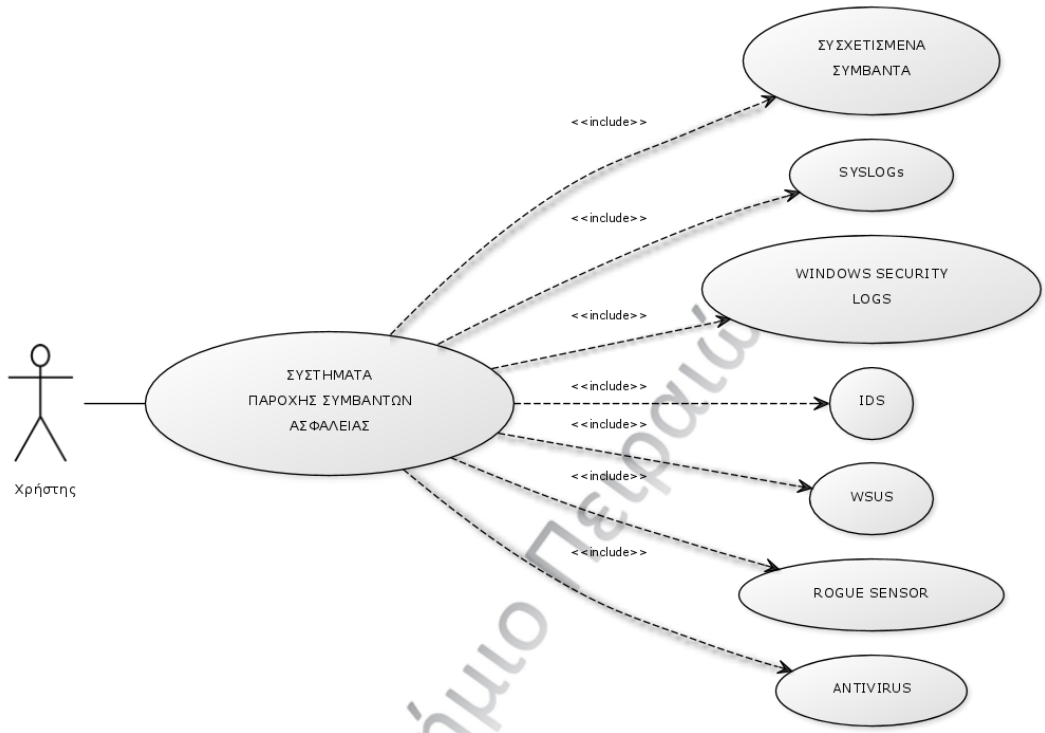


Εικόνα 36: Διάγραμμα Περίπτωσης Χρήσης (Είσοδος)

Στην κύρια σελίδα της εφαρμογής, ανάλογα με το μενού επιλογών που διατίθεται, μπορεί να επιλέξει την παρουσίαση στατιστικών από τα συλλεχθέντα συστήματα παροχής συμβάντων ασφαλείας ή μπορεί να επιλέξει άλλες ενέργειες, όπως αντιμετώπιση περιστατικών ή άλλες διαχειριστικές ενέργειες (π.χ. αναζήτηση βάση mac address ή ip address). Αναλυτικότερα στην εικόνα 37 φαίνονται οι επιλογές που διατίθενται στον χρήστη και αποτελούν την πρόσβαση του:

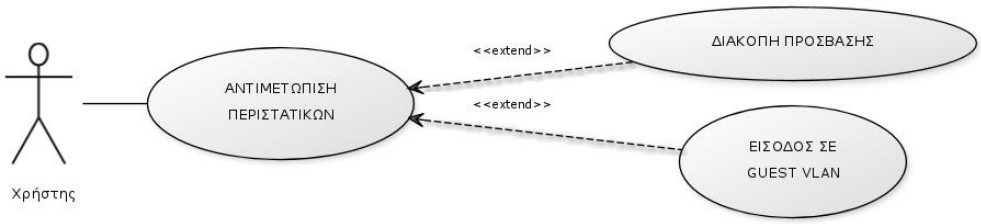
- Στα συλλεχθέντα συμβάντα από το antivirus (McAfee Virus Scan)
- Στα συλλεχθέντα συμβάντα από τον Rogue Sensor (McAfee Rogue Sensor)
- Στα συλλεχθέντα συμβάντα από IDS (Snort)
- Στα συλλεχθέντα συμβάντα από Event Manager (GFI)
- Στα συλλεχθέντα συμβάντα από τον SysLog Server (SysLog-ng)

- Στα δεδομένα από τον εξυπηρετητή ενημερώσεων του δικτύου (WSUS)
- Και τέλος στα συσχετισμένα συμβάντα.



Εικόνα 37: Διάγραμμα Περίπτωσης Χρήσης (Επιλογή Συστήματος Παροχής Συμβάντων Ασφαλείας)

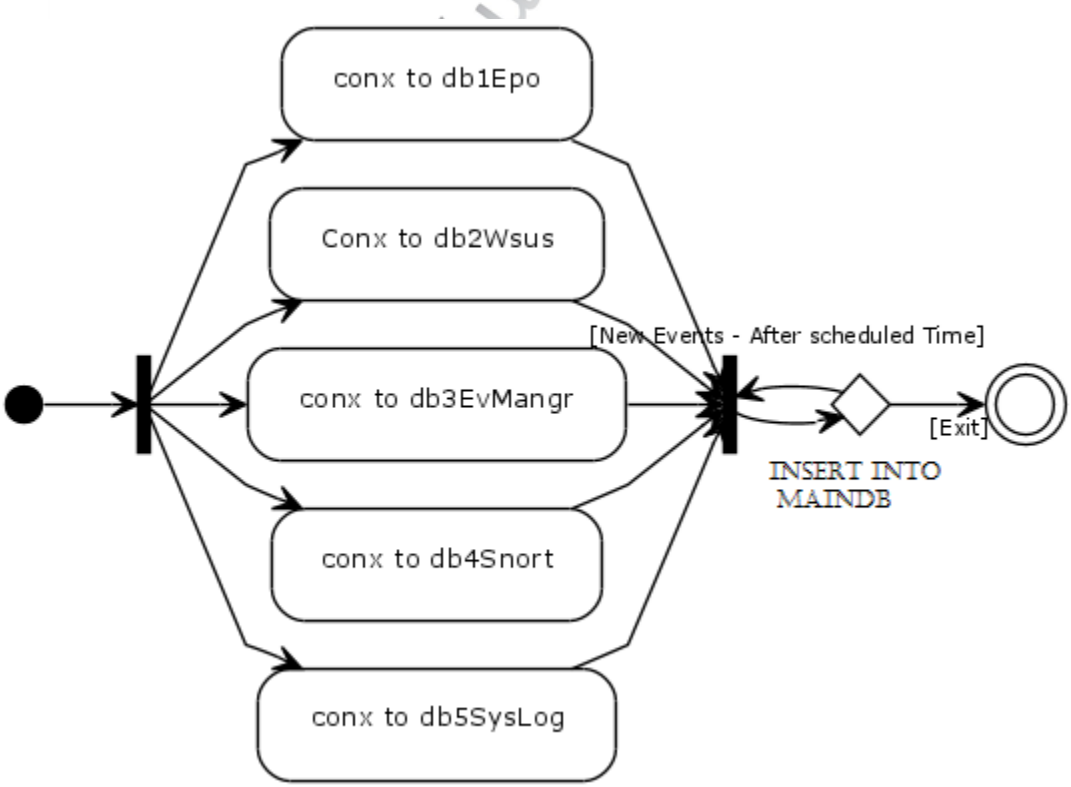
Επιπροσθέτως ο χρήστης μπορεί να ενεργήσει, σε συμβάντα που έχουν συσχετιστεί και είναι κρίσιμα με διακοπή πρόσβασης ή είσοδος του συστήματος σε guest VLan (Εικόνα 38)



Εικόνα 38: Διάγραμμα Περίπτωσης Χρήσης (Αντιμετώπιση Περιστατικών)

Διάγραμμα δραστηριοτήτων (activity diagram)

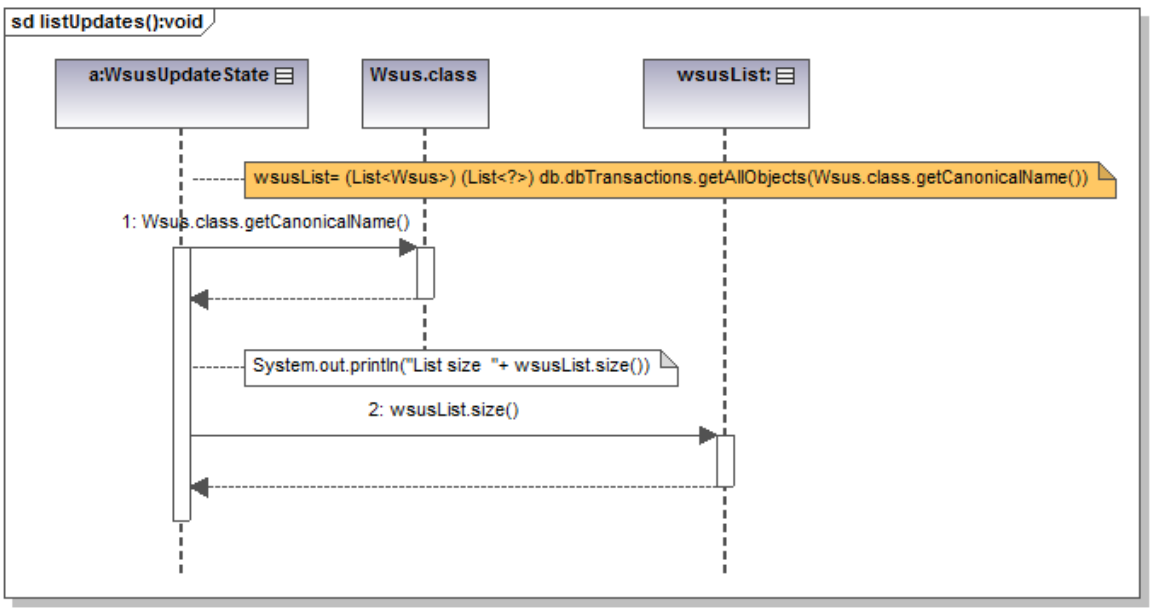
Στο διάγραμμα της εικόνας 39 φαίνεται ο τρόπος λειτουργίας του Core_secart. Αναλυτικότερα το λογισμικό συνδέεται αυτόματα με τις Βάσεις Δεδομένων των συστημάτων παροχής συμβάντων ασφαλείας μέσω του Hibernate και ρωτά για νέα συμβάντα σε χρόνο που ρυθμίζεται μέσα από τον Quartz Scheduler. Τα επιστρεφόμενα αποτελέσματα επιστρέφονται στην MainDB.



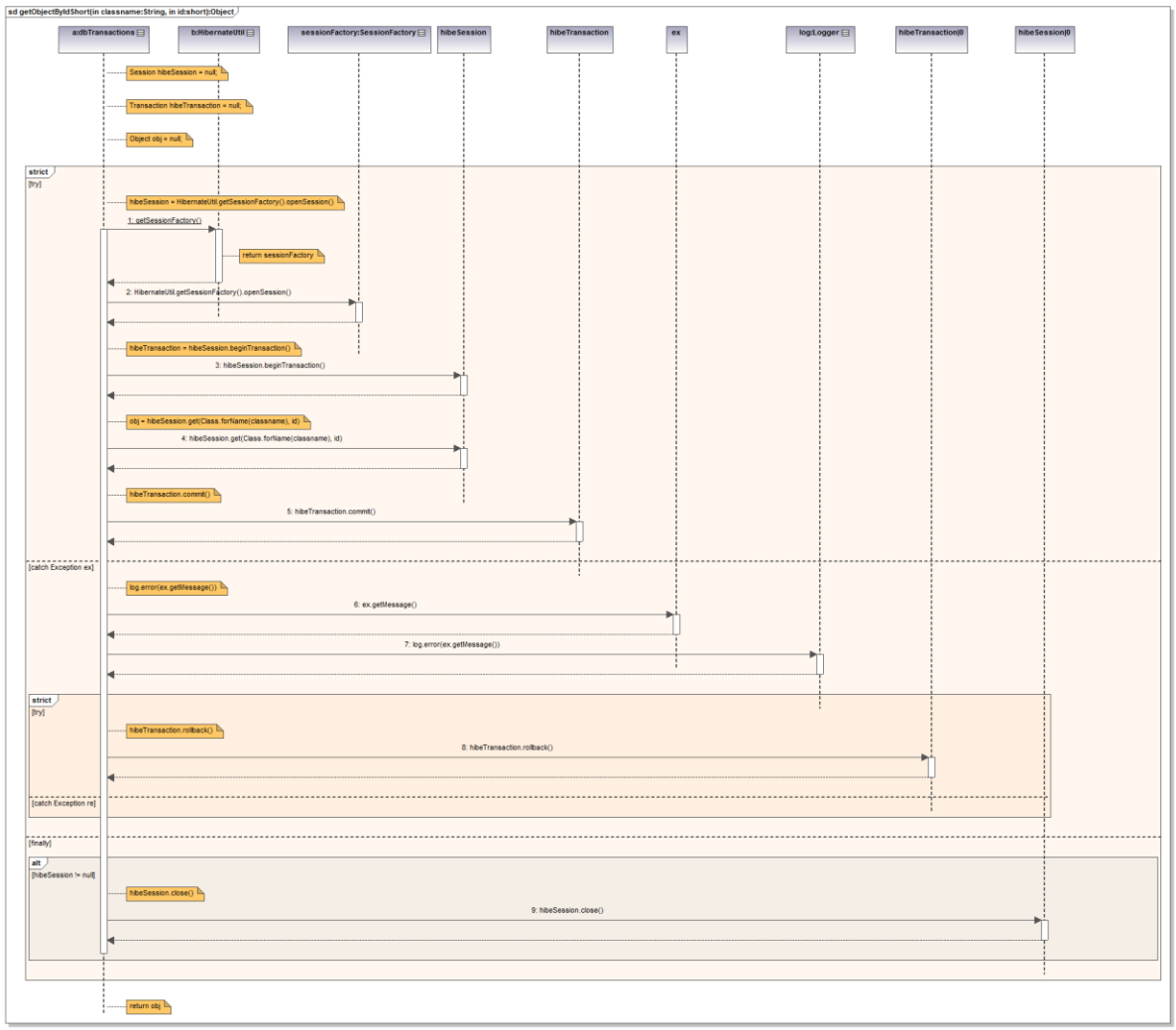
Εικόνα 39: Διάγραμμα δραστηριοτήτων Core_secart

Διάγραμμα ακολουθίας (sequence diagram)

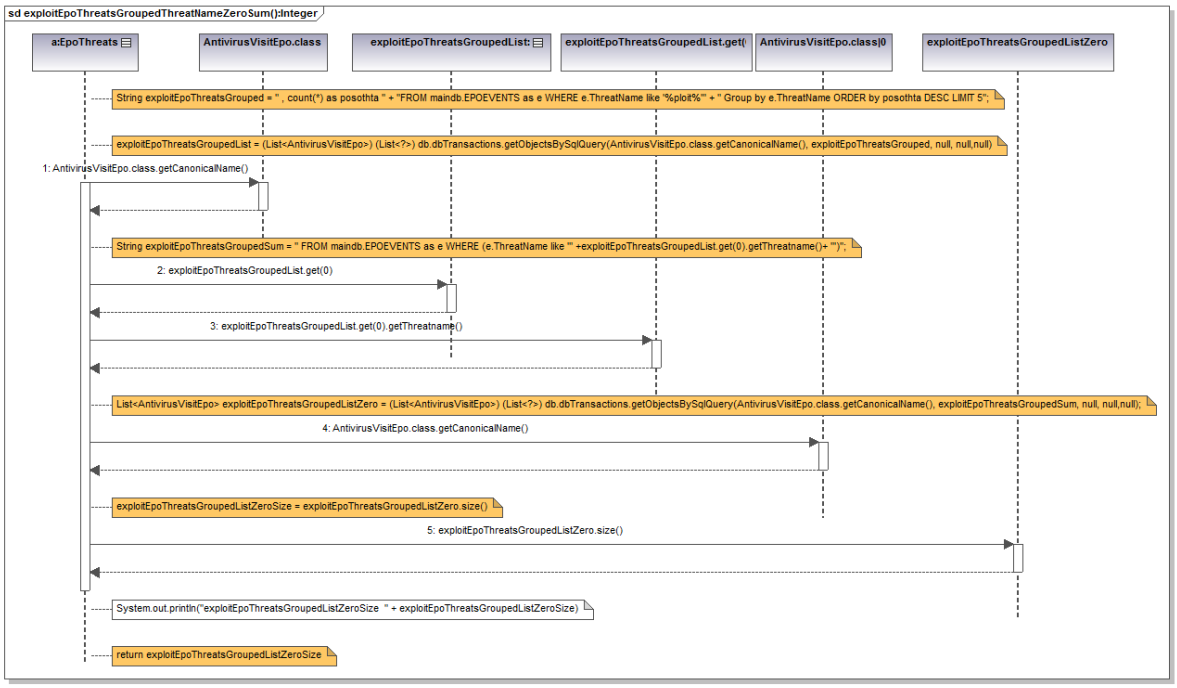
Στις εικόνες 40, 41 και 42 παρουσιάζονται ενδεικτικά διαγράμματα ακολουθίας.



Εικόνα 40: Διάγραμμα ακολουθίας - listUpdates



Εικόνα 41: Διάγραμμα ακολουθίας - getObjectById



Εικόνα 42: Διάγραμμα ακολουθίας - exploitEpoThreatsGroupedtThreatNameZeroSum

Παράρτημα Β: Πηγαίος Κώδικας (source code)

Η πρόσβαση στον πηγαίο κώδικα είναι διαθέσιμη κατόπιν επικοινωνίας στο ipirotis@yahoo.com

.

Παράρτημα Γ: Οδηγίες Χρήσης

Καλώντας την εφαρμογή μέσα από οποιονδήποτε φυλλομετρητή ιστού παρουσιάζετε η ιστοσελίδα της εικόνας 43.

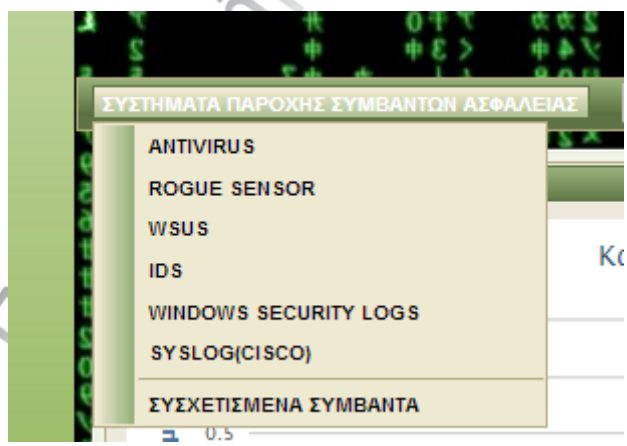
Εικόνα 43: Σελίδα σύνδεσης

Αφού πιστοποιηθούμε η εφαρμογή μας παρουσιάζει στην αρχική της σελίδα (εικόνα 44) μια γενική κατάσταση του επιπέδου ασφαλείας του δικτύου. Αναλυτικότερα παρουσιάζονται:

- Ο αριθμός συμβάντων ανά βάση δεδομένων (σε βάθος επτά ημερών)
- Αν έχουν αντιμετωπιστεί ή όχι αναγνωρισθέντα περιστατικά ασφαλείας
- Μια γενική κατηγοριοποίηση των συμβάντων ασφαλείας, ανά μηχανισμό ασφαλείας.

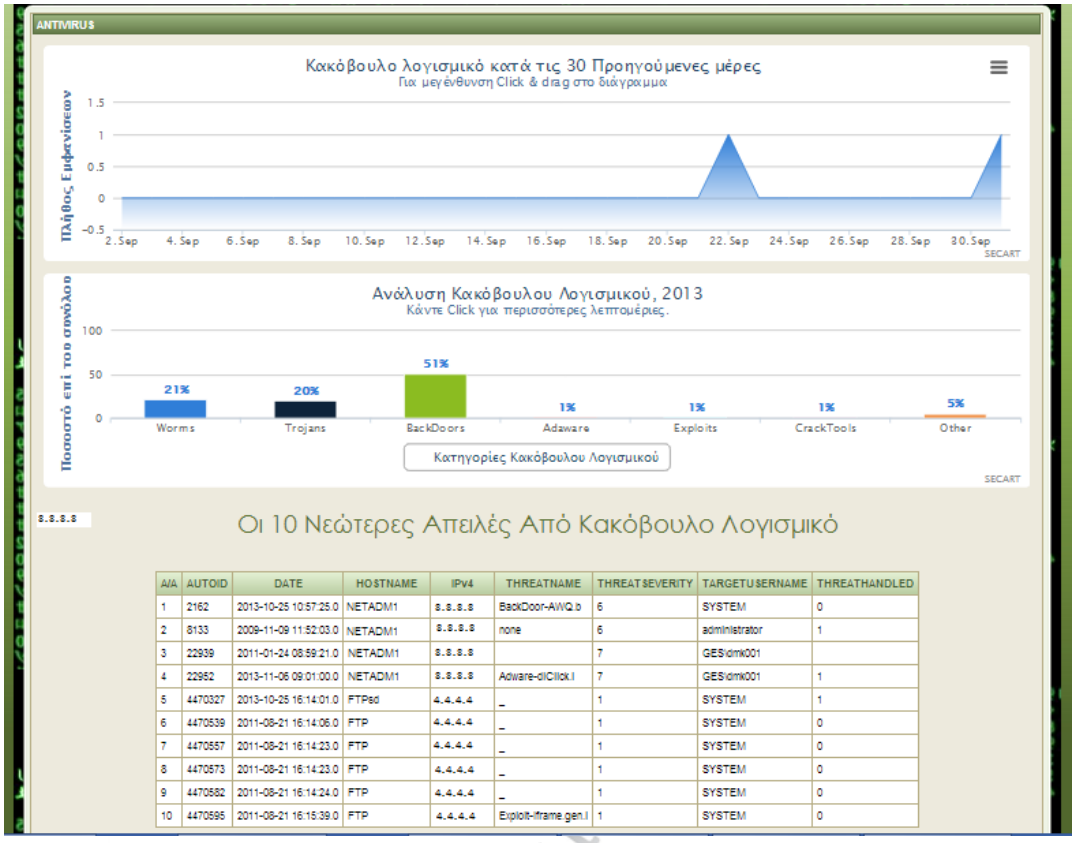
Εικόνα 44: Αρχική Σελίδα

Φέρνοντας τον δείκτη πάνω συστήματα παροχής Συμβάντων Ασφαλείας, εμφανίζονται οι επιλογές τις εικόνας 45.



Εικόνα 45: Μενού επιλογών για τα συστήματα παροχής Συμβάντων Ασφαλείας

Η πρώτη επιλογή «ANTIVIRUS» μας φέρνει σε επαφή με πληροφορίες που αφορούν στην κατάσταση του δικτύου από πλευράς κακόβουλου λογισμικού (εικόνα 46). Να τονίζουμε ότι τα γραφήματα είναι δυναμικά και επιπροσθέτως με την επιλογή τους παρουσιάζουν επιπρόσθετες πληροφορίες.



A/A	AUTOID	DATE	HOSTNAME	IPv4	THREATNAME	THREATSEVERITY	TARGETUSERNAME	THREATHANDLED
1	2162	2013-10-25 10:57:25.0	NETADM1	8.8.8.8	BackDoor-AWQ.b	6	SYSTEM	0
2	8133	2009-11-09 11:52:03.0	NETADM1	8.8.8.8	none	6	administrator	1
3	22939	2011-01-24 08:59:21.0	NETADM1	8.8.8.8		7	GES\dmk001	
4	22952	2013-11-06 09:01:00.0	NETADM1	8.8.8.8	Adware-clClick.l	7	GES\dmk001	1
5	4470327	2013-10-25 16:14:01.0	FTPsd	4.4.4.4	_	1	SYSTEM	1
6	4470539	2011-08-21 16:14:06.0	FTP	4.4.4.4	_	1	SYSTEM	0
7	4470557	2011-08-21 16:14:23.0	FTP	4.4.4.4	_	1	SYSTEM	0
8	4470573	2011-08-21 16:14:23.0	FTP	4.4.4.4	_	1	SYSTEM	0
9	4470582	2011-08-21 16:14:24.0	FTP	4.4.4.4	_	1	SYSTEM	0
10	4470595	2011-08-21 16:15:39.0	FTP	4.4.4.4	Exploit-iframe gen.l	1	SYSTEM	0

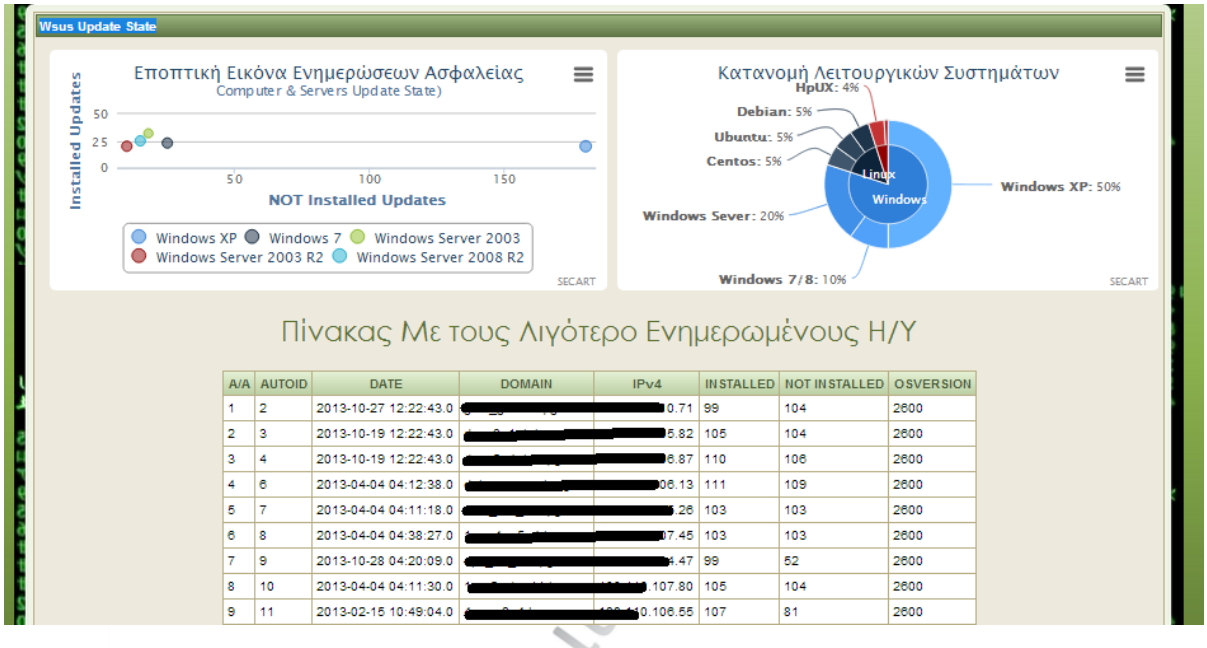
Εικόνα 46: Σελίδα με συμβάντα ασφαλείας από το Antivirus

Η δευτερη επιλογή «ROGUES» παρουσιάζει Πόρους Δικτύου που δεν συμμορφόνονται με τις πολιτικές δικτύου, δηλαδή ύπαρξη ενημερωμένου αντιικου λογισμικού και windows updates.

A/A	AUTOID	DATE	DOMAIN	HOSTNAME	IPv4	MAC	OSVERSION	OSPLATFORM	DEVICETYPE
1	6	2013-10-19 10:57:25.0	[redacted]	[redacted]	[redacted]	[redacted]	XP	Windows	computer
2	7	2013-10-19 12:12:00.0	[redacted]	[redacted]	[redacted]	[redacted]	XP	Windows	computer
3	9	2013-10-19 12:12:29.0	[redacted]	[redacted]	[redacted]	[redacted]	XP	Windows	computer
4	10	2013-01-09 09:30:33.0	[redacted]	[redacted]	[redacted]	[redacted]	XP	Windows	computer
5	11	2013-01-09 09:38:18.0	[redacted]	[redacted]	[redacted]	[redacted]	XP	Windows	computer
6	12	2013-01-09 09:36:50.0	[redacted]	[redacted]	[redacted]	[redacted]	XP	Windows	computer
7	14	2013-01-09 09:40:49.0	[redacted]	[redacted]	[redacted]	[redacted]	XP	Windows	computer
8	16	2013-01-09 09:40:03.0	[redacted]	[redacted]	[redacted]	[redacted]	XP	Windows	computer
9	21	2013-01-04 12:37:27.0	[redacted]	[redacted]	[redacted]	[redacted]	XP	Windows	computer

Εικόνα 47: Σελίδα με Rogues πόρους στο δίκτυο

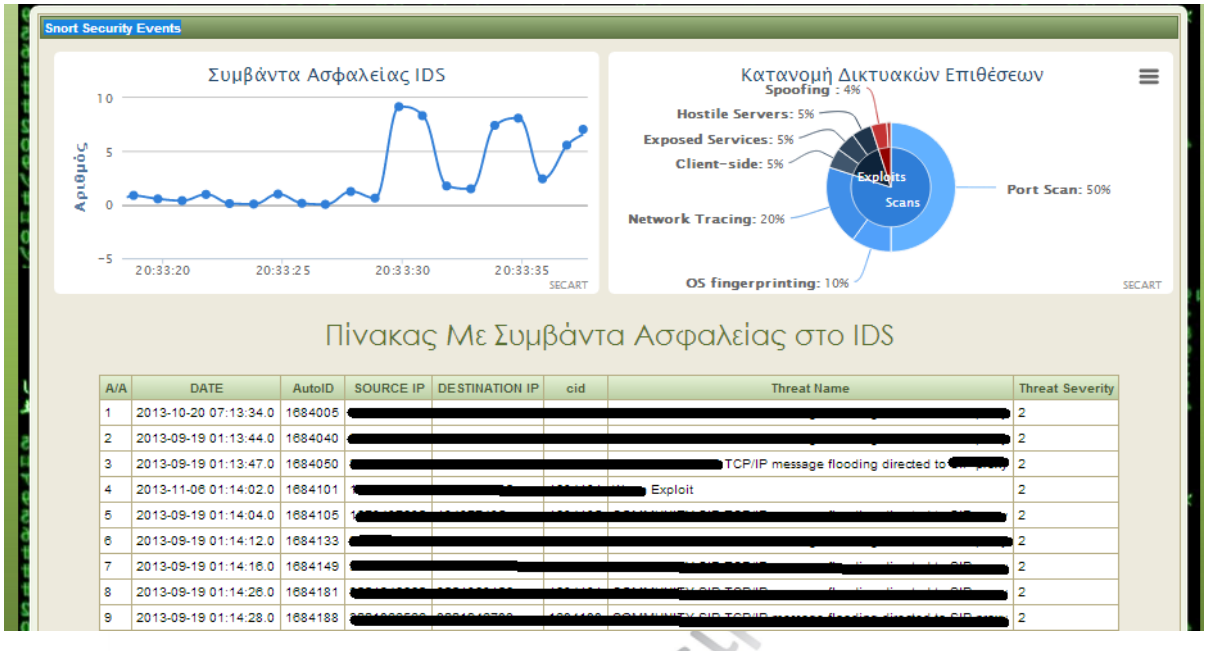
Η τρίτη επιλογή «WINDOWS UPDATE STATE» παρουσιάζει συνοπτικά την κατάσταση, των Η/Υ και Servers του Δικτύου, από πλευράς ενημερώσεων ασφαλείας.



A/A	AUTOID	DATE	DOMAIN	IPv4	INSTALLED	NOT INSTALLED	OSVERSION
1	2	2013-10-27 12:22:43.0	[redacted]	[redacted]0.71	99	104	2600
2	3	2013-10-19 12:22:43.0	[redacted]	[redacted]5.82	105	104	2600
3	4	2013-10-19 12:22:43.0	[redacted]	[redacted]6.87	110	106	2600
4	6	2013-04-04 04:12:38.0	[redacted]	[redacted]06.13	111	109	2600
5	7	2013-04-04 04:11:18.0	[redacted]	[redacted].26	103	103	2600
6	8	2013-04-04 04:38:27.0	[redacted]	[redacted]07.45	103	103	2600
7	9	2013-10-28 04:20:09.0	[redacted]	[redacted]4.47	99	52	2600
8	10	2013-04-04 04:11:30.0	[redacted]	[redacted].107.80	105	104	2600
9	11	2013-02-15 10:49:04.0	[redacted]	[redacted]0.106.55	107	81	2600

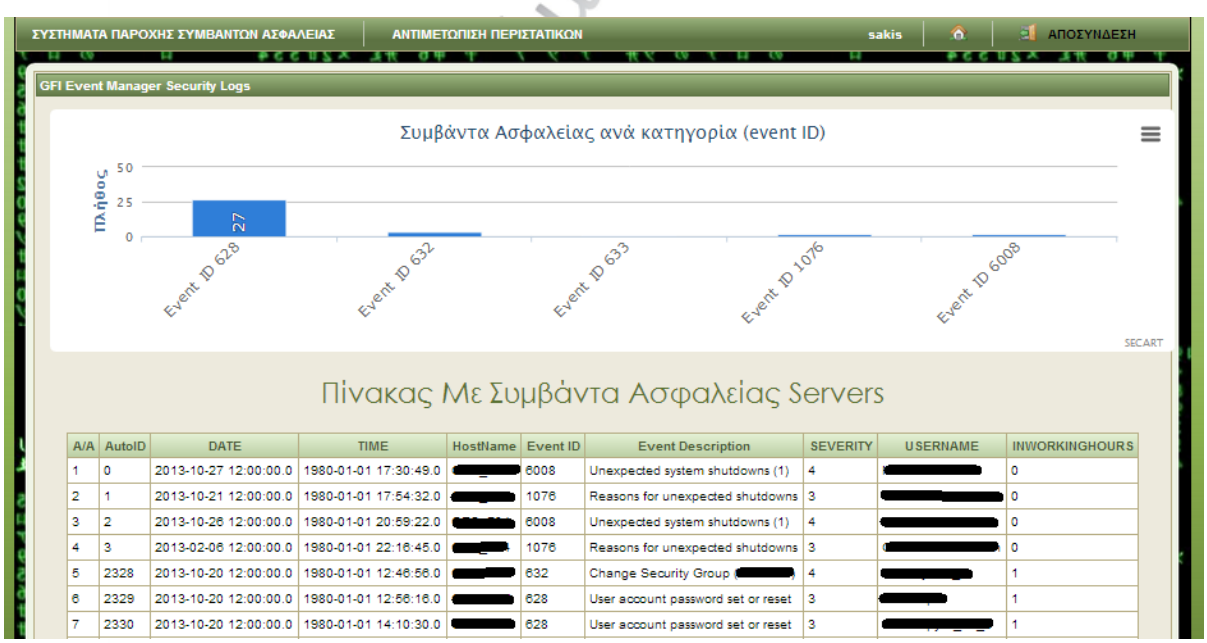
Εικόνα 48: Σελίδα με εποπτική εικόνα ενημερώσεων ασφαλείας

Η τέταρτη επιλογή «SNORT SECURITY EVENTS» παρουσιάζει τη Σελίδα με τα συμβάντα ασφαλείας του IDS.



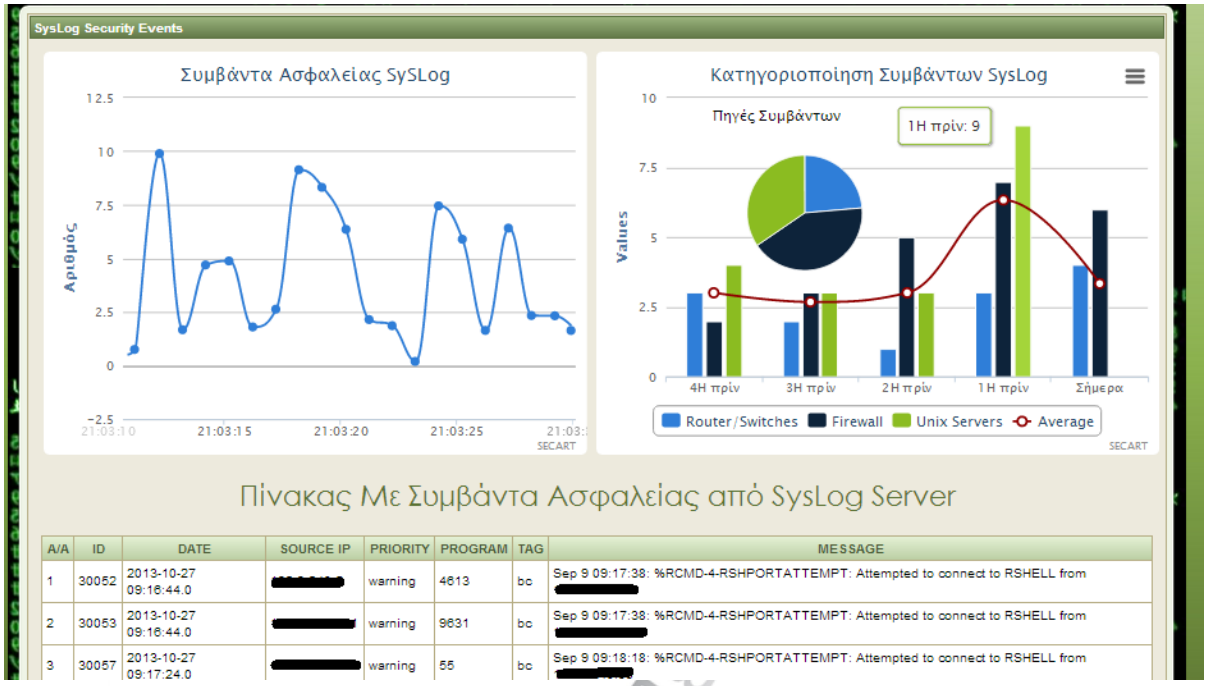
Εικόνα 49: Σελίδα με συμβάντα ασφαλείας απο IDS

Η Πέμπτη επιλογή με τίτλο «GFI EVENT MANAGER SECURITY LOGS» αφορά στην παρουσίαση επιλεγμένων συμβάντων ασφαλείας από τους WINDOWS Εξυπηρετητές δικτύου.



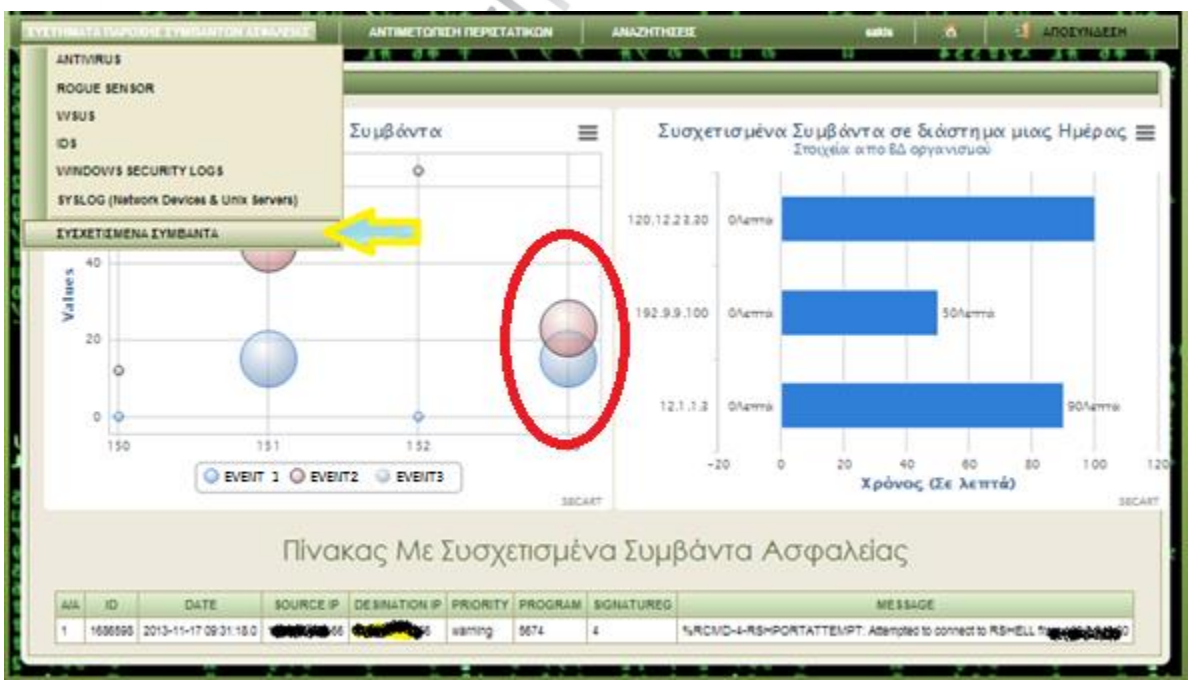
Εικόνα 50: Σελίδα με συμβάντα ασφαλείας εξυπηρετητών δικτύου.

Η έκτη επιλογή «SYSLOG SECURITY EVENTS» παρουσιάζει τα συμβάντα ασφαλείας από τους syslog servers του δικτύου, τα οποία περιέχουν συμβάντα απο unix servers, switches, routers και firewalls.

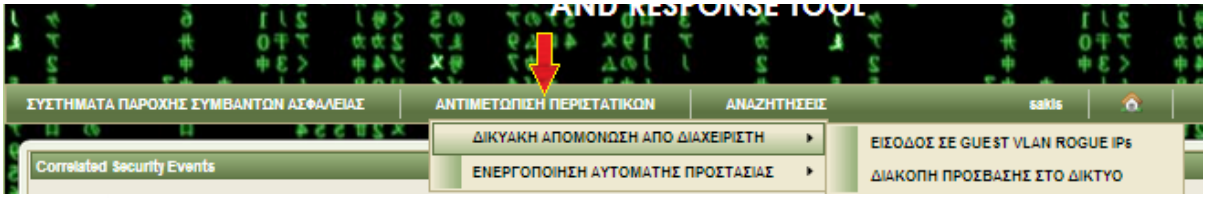


Εικόνα 51: Σελίδα με συμβάντα ασφαλείας απο syslog Server

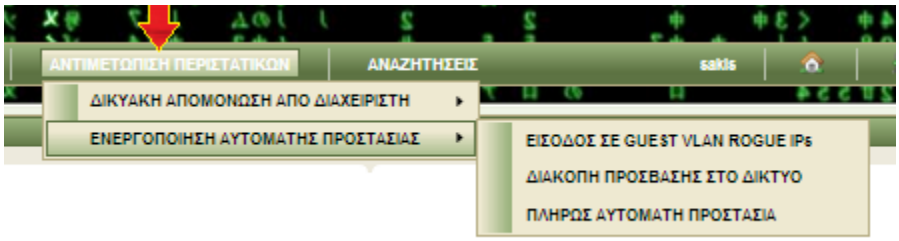
Τέλος η επόμενη επιλογή μας δείχνει τα συσχετισμένα συμβάντα βάση της λογικής συσχετίσεων που περιέχεται στο αρχείο CorrelatedMainDB.java



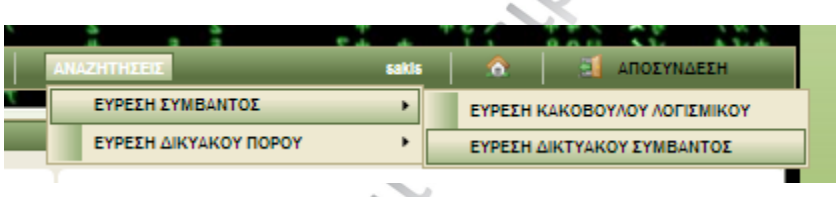
Εικόνα 52: Σελίδα με συσχετισμένα συμβάντα



Εικόνα 53: Αντιμετώπιση Περιστατικών – Μη Αυτόματη



Εικόνα 54: Αντιμετώπιση Περιστατικών – Αυτόματη



Εικόνα 55: Αναζήτηση Πόρου ή Συβάντος Ασφαλείας

Παράρτημα Δ: Εργαλεία Που Χρησιμοποιήθηκαν

- IDE: NetBeans 7.2
- JAVA EE - HIBERNATE – SPRING – QUARTZ – JSP
- MSSQL JDBC CONNECTOR
- MYSQL JDBC CONNECTOR
- MCAFEE EPO DATABASE
- GFI EVENT MANAGER DATABASE
- SYSLOG-ng SERVER & MYSQL
- SMORBY
- WSUS DATABASE