ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΠΜΣ:ΤΕΧΝΟΟΙΚΟΝΟΜΙΚΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Ανάπτυξη και ρύθμιση αισθητήρων συλλογής και επεξεργασίας πληροφοριών ασφαλείας, για τον εντοπισμό και αντιμετώπιση κυβερνοεπιθέσεων σε ετερόμορφη δικτυακή υποδομή

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΑΤΡΙΒΗ

Χρίστος Γ. Αναγνωστόπουλος

Συμβουλευτική επιτροπή:
Σωκράτης Κάτσικας(Επιβλέπων)
Κωνσταντίνος Λαμπρινουδάκης
Χρήστος Ξενάκης

ΑΘΗΝΑ, 2015

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ
ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΠΜΣ:ΤΕΧΝΟΟΙΚΟΝΟΜΙΚΗ ΔΙΟΙΚΗΣΗ ΚΑΙ ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Ανάπτυξη και ρύθμιση αισθητήρων συλλογής και επεξεργασίας πληροφοριών ασφαλείας, για τον εντοπισμό και αντιμετώπιση κυβερνοεπιθέσεων σε ετερόμορφη δικτυακή υποδομή

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΑΤΡΙΒΗ

Χρίστος Γ. Αναγνωστόπουλος

Συμβουλευτική επιτροπή: Σωκράτης Κάτσικας(Επιβλέπων)
Κωνσταντίνος Λαμπρινουδάκης
Χρήστος Ξενάκης

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή

.

.....	.....	.....
Σ. Κάτσικας	Κ. Λαμπρινουδάκης	Χ. Ξενάκης
Καθηγητής	Αναπληρωτής Καθηγητής	Αναπληρωτής Καθηγητής
Πανεπιστήμιο Πειραιά.	Πανεπιστήμιο Πειραιά.	Πανεπιστήμιο Πειραιά.

.....

Χρίστος Γ. Αναγνωστόπουλος

Περίληψη

Η διατήρηση της ασφάλειας των δικτύων υπολογιστών στα μοντέρνα εταιρικά περιβάλλοντα είναι υψίστης σημασίας. Ωστόσο, στη σύγχρονη εποχή, η απαίτηση για διαρκή διασύνδεση των υπολογιστικών συστημάτων, τα καθιστά ευάλωτα σε μια πληθώρα απειλών που αυξάνουν την πιθανότητα παραβίασης των βασικών αρχών ασφάλειας: της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των δεδομένων που αυτά περιέχουν και επεξεργάζονται.

Δυο από τους σημαντικότερους μηχανισμούς περιορισμούς της επικινδυνότητας σε ένα δίκτυο είναι α) τα Συστήματα Ανίχνευσης Εισβολών (IDS) που αναλύουν διαρκώς την κίνηση σε ένα δίκτυο και δράττουν ανάλογα, όταν αναγνωρίσουν μια αλληλουχία ενεργειών στο δίκτυο όμοια με αυτή μιας γνωστής επίθεσης και β) τα Συστήματα Αντιμετώπισης Εισβολών (IPS) τα οποία αυτόματα και σε πραγματικό χρόνο προβαίνουν σε όλες τις απαραίτητες ενέργειες που απαιτούνται για την αντιμετώπιση ενός αναγνωρισμένου περιστατικού ασφαλείας και την επαναφορά του δικτύου σε κανονικές συνθήκες. Ωστόσο, και οι δύο αυτές μέθοδοι παρουσιάζουν μια σειρά μειονεκτημάτων που τα καθιστούν μη βέλτιστη επιλογή. Η ανάγκη για την αντιμετώπιση πολύπλοκων επιθέσεων οδήγησε στη δημιουργία των Συστημάτων Πληροφοριών Ασφάλειας και Διαχείρισης Περιστατικών (Security Information and Event Management - SIEM), που συνδυάζουν πληροφορίες από πολλαπλούς μηχανισμούς ασφάλειας ενός δικτύου και προβαίνουν σε συνδυαστική ανάλυσή τους, αυξάνοντας έτσι την ακρίβεια των αποτελεσμάτων και μειώνοντας την πιθανότητα εξαγωγής λανθασμένων συμπερασμάτων.

Στόχος της εργασίας αυτής είναι η παροχή μια εις βάθος περιγραφής των αρχιτεκτονικών και των βασικών μελών από τα οποία αποτελείται ένα τυπικό εργαλείο SIEM, η ανάλυση του τρόπου λειτουργίας του και η παρουσίαση των πλεονεκτημάτων και των μειονεκτημάτων του, παρέχοντας μια επισκόπηση των πιο σημαντικών εξ αυτών. Μια από τις βασικότερες συνεισφορές αυτής της εργασίας, είναι και η παράθεση ενός εγχειριδίου για την εγκατάσταση και ορθή παραμετροποίηση του πιο γνωστού εργαλείου αυτής της κατηγορίας, του SIEM AlienVault OSSIM καθώς και του OSSEC, ενός IDS ανοιχτού κώδικα, του οποίου οι αισθητήρες συνεργάζονται με το OSSIM.

Abstract

The idea that network and systems security is essential in the modern enterprise environment is of utmost importance. However, the requirement for constant connectivity of computational systems in modern information systems makes them vulnerable to a series of threats that increase the probability of violating the core security principles: integrity, reliability, confidentiality and availability of the data they process.

Two of the most important mechanisms that limit the dangers in a network environment are a) the Intrusion Detection Systems, that constantly analyze the network traffic and when they identify a series of actions similar to a known attack, they act accordingly and b) the Intrusion Prevention Systems that take all necessary actions to deal with an identified security incident in real time in order to restore the network to its previous state. However, both of these methods present a series of limitations that deprive them of being an optimal solution. The need to cope with complex attacks led to the development of Security Information and Event Management Systems that combine and analyze information from multiple network security mechanisms and acting with increased accuracy and decreased chances of making false conclusions.

The goal of this master thesis is to provide a detailed description of the architecture and the basic components of a typical SIEM tool, an analysis of its functionality and presenting its advantages and disadvantages. Another important contribution of this thesis is a detailed documentation of the installation and initialization of a well-known tool under this category, the SIEM AlienVault OSSIM and OSSEC, an open source IDS whose sensors cooperate with OSSIM.

Ευχαριστίες

Η μεταπτυχιακή διατριβή αυτή περιλαμβάνει το σύνολο της ερευνητικής μου δραστηριότητας, η οποία εκπονήθηκε στο Πανεπιστήμιο Πειραιά. Αν και ως εργασία φέρει το όνομα ενός ατόμου, η τελική της μορφή οφείλεται και στη βοήθεια και την υποστήριξη συνεργατών, προς τους οποίους κρίνω σκόπιμο να απευθύνω τις ευχαριστίες μου.

Καταρχάς επιθυμώ να εκφράσω τις θερμές μου ευχαριστίες προς τους επιβλέποντες μου Καθηγητή κ. Σωκράτη Κάτσικα και τον κ. Σπυρίδων Παπαγεωργίου. Η συνεισφορά τους ήταν καθοριστική, δίνοντάς μου την ευκαιρία εκπόνησης του μεταπτυχιακού μου. Ιδιαίτερα, θα ήθελα να ευχαριστήσω τον Κωνσταντίνο Κόλια για την αμέριστη συμπαράσταση που προσέφερε σε όλα τα στάδια αυτής της προσπάθειας και την ουσιαστική συνεισφορά του στη διατριβή.

Τέλος, θα ήθελα να ευχαριστήσω τους γονείς μου , για την στήριξη τους όλα αυτά τα χρόνια.

Χρίστος Γ. Αναγνωστόπουλος,

Ιούνιος 2015

Πίνακας Περιεχομένων

Ευρετήριο Εικόνων

Κεφάλαιο 1 **Εισαγωγή**

Τα τελευταία χρόνια παρατηρείται μια ραγδαία αύξηση της συχνότητας και της πολυπλοκότητας των επιθέσεων που εκδηλώνονται ενάντια στα δίκτυα υπολογιστών. Ωστόσο λόγω της πολυεπίπεδης κρισιμότητας των υπηρεσιών που τα δίκτυα υπολογιστών προσφέρουν, σχεδόν άμεσα άρχισε να καταβάλλεται προσπάθεια για την αποτελεσματική προστασία και την αντιμετώπιση οποιασδήποτε μορφής απειλής προς αυτά.

Για την επίτευξη αυτού του σκοπού, έχουν αναπτυχθεί ποικίλοι μηχανισμοί οι οποίοι αντιμετωπίζουν το πρόβλημα της προστασίας δικτύων από διαφορετική σκοπιά ο καθένας. Τα τείχη πυρασφάλειας (firewall), πρωτόκολλα κρυπτογράφησης πληροφορίας όπως το IPSec, αλλά και αρχιτεκτονικές όπως τα honeypots συμβάλλουν στην διασφάλιση των δικτύων και την μείωση των ύποπτων ενεργειών από εξωτερικούς επιτιθέμενους ή εσωτερικούς κακόβουλους χρήστες.

Ένας από τους πιο σημαντικούς μηχανισμούς που εμπίπτει σε αυτή την κατηγορία είναι και τα Συστήματα Ανίχνευσης Εισβολών (Intrusion Detection Systems - IDS). Τέτοιου είδους συστήματα αναλύουν διαρκώς την κίνηση στο δίκτυο και αποστέλλουν τα κατάλληλα προειδοποιητικά σήματα στους διαχειριστές όταν εντοπιστεί μια αλληλουχία ενεργειών όμοια με μια αλληλουχία ενεργειών που έχει οριστεί ως «ταυτότητα» κάποιας γνωστής επίθεσης.

Η αξία τέτοιων εργαλείων είναι αδιαμφισβήτητη, ωστόσο τα μειονεκτήματα τους περιστρέφονται γύρω από (α) την πολυπλοκότητα στη ρύθμισή τους, (β) το γεγονός ότι οι ταυτότητες των επιθέσεων είναι δημόσια διαθέσιμες και ο επιτιθέμενος μπορεί εύκολα να διαφοροποιήσει και να αναπροσαρμόσει την στρατηγική του, (γ) την εκπαίδευση (και κατ' επέκταση τις ικανότητες) των επιτιθεμένων οι οποίες έχουν αυξηθεί δραματικά τα τελευταία χρόνια, (δ) το μέγεθος και την πολυπλοκότητα των υπό την εποπτεία δικτύων που αυξάνουν τα σημεία εισβολής, (ε) τις πιθανότητες αστοχίας μιας πρόβλεψης λόγω της φύσης των συστημάτων αυτών.

Κοινός παρονομαστής όλων των μεθόδων προστασίας που περιεγράφηκαν παραπάνω είναι ο παθητικός χαρακτήρας της προστασίας που αυτές παρέχουν. Έτσι, η πραγματική αξία τους ανάγεται στην έγκαιρη καταγραφή και αναφορά ενός περιστατικού. Από αυτό το σημείο και μετά ο διαχειριστής του δικτύου ή ο υπεύθυνος ασφάλειας είναι επιφορτισμένοι με το δύσκολο έργο της απόκρουσης της εισβολής. Για το λόγο αυτό αναπτύχθηκαν τα Συστήματα Αντιμετώπισης Εισβολών (Intrusion Prevention Systems - IPS) τα οποία αυτόματα και σε πραγματικό χρόνο προβαίνουν σε όλες τις απαραίτητες ενέργειες που απαιτούνται για την αντιμετώπιση ενός αναγνωρισμένου περιστατικού ασφαλείας και την επαναφορά του δικτύου σε κανονικές συνθήκες.

Γρήγορα όμως και αυτά τα συστήματα αποδείχθηκαν ανεπαρκή καθώς η πολυπλοκότητα των επιθέσεων αυξανόταν. Συνήθως, για την αντιμετώπιση πολύπλοκων επιθέσεων απαιτείται καθολική γνώση των συνθηκών που επικρατούν στο δίκτυο καθώς τέτοιου είδους επιθέσεις είναι συνδυαστικές. Αυτή η ανάγκη αποτέλεσε τον κινητήριο μοχλό για την δημιουργία των Συστημάτων Πληροφοριών Ασφάλειας και Διαχείρισης Περιστατικών (Security Information and Event Management - SIEM). Τα συστήματα αυτού του είδους συγκεντρώνουν πληροφορίες από πολλαπλούς μηχανισμούς ασφάλειας του δικτύου όπως IDPS και τείχη πυρασφάλειας και προβαίνουν σε συνδυαστική ανάλυση δεδομένων και ενδείξεων για την ανίχνευση κυβερνοπεριστατικών. Κα' αυτό τον τρόπο αυξάνεται σε μεγάλο βαθμό η ακρίβεια των αποτελεσμάτων και μειώνεται η πιθανότητα εξαγωγής λάθος συμπερασμάτων.

Ο στόχος αυτής της εργασίας είναι να παρέχει μια εις βάθος περιγραφή των αρχιτεκτονικών και των βασικών μελών από τα οποία αποτελείται ένα τυπικό εργαλείο SIEM, να αναλύσει τον τρόπο λειτουργίας, τα πλεονεκτήματα και τα μειονεκτήματα του. Ταυτόχρονα, επιχειρήθηκε μια επισκόπηση των πιο σημαντικών εξ αυτών. Μια από τις βασικότερες συνεισφορές αυτής της εργασίας, είναι και η παράθεση ενός εγχειριδίου για την εγκατάσταση και ορθή παραμετροποίηση του πιο γνωστού εργαλείου αυτής της κατηγορίας, του SIEM AlienVault OSSIM καθώς και του OSSEC ενός IDS ανοιχτού κώδικα, του οποίου οι αισθητήρες συνεργάζονται με το OSSIM.

Κεφάλαιο 2 **Συστήματα Ανίχνευσης Εισβολών**

Κάθε υπολογιστής βρίσκεται σε κίνδυνο μη εξουσιοδοτημένης πρόσβασης και ως επακόλουθο αυτού οι ευαίσθητες και προσωπικές πληροφορίες των χρηστών είναι πιθανώς εκτεθειμένες. Τα συστήματα ανίχνευσης εισβολών δημιουργήθηκαν με σκοπό τον εντοπισμό διαφορετικών τύπων επιθέσεων σε επίπεδο τόσο υπολογιστικού συστήματος όσο και δικτύων. Συστήματα αυτού του είδους παρατηρούν και αναλύουν συγκεκριμένα γεγονότα τα οποία λαμβάνουν χώρα και αναγνωρίζουν τα πιθανά προβλήματα ασφαλείας που προκύπτουν.

2.1 Ταξινόμηση

Τα IDS χωρίζονται σε 2 κύριες κατηγόριες: αυτά τα οποία διεξάγουν ανίχνευση στον ξενιστή (Host-based Intrusion Detection Systems - HIDS) και αυτά που διεξάγουν ανίχνευση στο δίκτυο καθολικά (Network-based Intrusion Detection Systems - NIDS). Εργαλεία τα οποία ανήκουν στην πρώτη κατηγορία, απαιτούν μικρά προγράμματα τα οποία καλούνται πράκτορες (agents) να εγκατασταθούν σε συστήματα ώστε να μπορεί να πραγματοποιείται μια διαρκής και άμεση αναγνώριση της κατάστασης αυτών των συστημάτων. Οι πράκτορες παρακολουθούν το λειτουργικό σύστημα και καταγράφουν τα δεδομένα σε ειδικά αρχεία, τις καταγραφές ασφαλείας (logs). Τυπικά παράγουν κάποιου είδους ειδοποίηση ή αναφορά σε περίπτωση εμφάνισης κάποιου προβλήματος.

Τα συστήματα που εμπίπτουν στην δεύτερη κατηγορία αποτελούνται από μια δικτυακή συσκευή η οποία παίζει το ρόλο αισθητήρα. Ένα τέτοιου είδους σύστημα τοποθετείται συνήθως στα όρια ενός δικτύου ώστε να μπορεί να παρακολουθεί όλη την κίνηση του δικτύου.

Τα σύγχρονα συστήματα ανίχνευσης εισβολών συνήθως συνδυάζουν χαρακτηριστικά από τις δυο αυτές αρχιτεκτονικές δημιουργώντας ένα υβριδικό τύπο συστήματος το οποίο είναι πιο αποτελεσματικό. Στη συνέχεια θα αναλυθούν τα χαρακτηριστικά κάθε μιας κατηγορίας με περισσότερη λεπτομέρεια.

2.1.1 Συστήματα Ανίχνευσης Εισβολών στον Ξενιστή

Ως συστήματα ανίχνευσης επιθέσεων στον ξενιστή χαρακτηρίζεται σε ένα σύστημα προστασίας στο οποίο η διαδικασία της ανίχνευσης εισβολών λαμβάνει χώρα αποκλειστικά εντός του συστήματος το οποίο προστατεύει. Τα δεδομένα συλλέγονται αποκλειστικά από αυτό το σύστημα και μόνο. Ένα ειδικό πρόγραμμα το οποίο καλείται ως «πράκτορας ξενιστή» παρακολουθεί τις δραστηριότητες που λαμβάνουν χώρα στο συγκεκριμένο σύστημα όπως τον έλεγχο ακεραιότητας, τις λειτουργίες των εφαρμογών, τις αλλαγές στα αρχεία, την δικτυακή κίνηση καθώς και τις

καταγραφές ασφαλείας του συστήματος. Παραδείγματος χάριν, με την χρήση κοινών εργαλείων κατακερματισμού (hashing), μπορεί να γίνει αντιληπτό αν έχει υπάρξει κάποια μη εξουσιοδοτημένη αλλαγή ή δραστηριότητα σε κάποιο κρίσιμο αρχείο συστήματος. Σε τέτοιες περιπτώσεις θα ανιχνευθεί άμεσα και θα ειδοποιηθεί ο χρήστης του συστήματος α) με κάποιο μήνυμα, β) με ανάλογη ειδοποίηση στο κεντρικό σύστημα διαχείρισης, γ) με το μπλοκάρισμα της συγκεκριμένης δραστηριότητας, ή δ) με συνδυασμό των παραπάνω. Η απόφαση για τον τρόπο αντίδρασης εξαρτάται από την εκάστοτε πολιτική ασφαλείας η οποία είναι εγκατεστημένη στο τοπικό σύστημα. Οι διαδικασίες που αυτά τα συστήματα διεξάγουν θεωρούνται ως παθητικά στοιχεία ανίχνευσης.

2.1.2 Συστήματα Ανίχνευσης Εισβολών στο Δίκτυο

Ένα σύστημα ανίχνευσης επιθέσεων στο δίκτυο, χρησιμοποιείται για την παρακολούθηση και ανάλυση της δικτυακής κίνησης έτσι ώστε να είναι σε θέση να το προστατεύσει από δικτυακές απειλές. Ένα NIDS προσπαθεί να ανιχνεύσει κακόβουλες δραστηριότητες όπως επιθέσεις άρνησης εξυπηρέτησης (DoS), ανίχνευση δικτυακών πορτών (port scanning) και παράνομη παρακολούθηση της κίνησης του δικτύου (sniffing). Ένα τυπικό σύστημα αυτής της κατηγορίας, ενσωματώνει ένα αριθμό αισθητήρων για την παρακολούθηση της δικτυακής κίνησης, έναν ή περισσότερους εξυπηρετητές για την διαχείριση και επεξεργασία των πληροφοριών καθώς και ένα ή περισσότερους εξυπηρετητές για προβολή αυτών των διαδικασιών και αποτελεσμάτων στους διαχειριστές του. Σκοπός του συστήματος είναι να αναλύει την κίνηση αυτή σε πραγματικό χρόνο (ή πολύ κοντά σε πραγματικό χρόνο) και να ανακαλύψει ομοιότητες με γνωστά μοτίβα επιθέσεων. Η ανάλυση των μοτίβων αυτών μπορεί να γίνεται είτε στους αισθητήρες, είτε σε εξυπηρετητές διαχείρισης και επεξεργασίας, είτε και στα δυο. Αυτές οι διαδικασίες θεωρούνται ως ενεργά στοιχεία ανίχνευσης.

2.1.3 Υβριδικά Συστήματα Εισβολών

Τα σημερινά Συστήματα Ανίχνευσης Εισβολών συνήθως συνδυάζουν τόσο τα χαρακτηριστικά των Συστημάτων Ανίχνευσης Εισβολών στον Ξενιστή όσο και αυτά των Συστημάτων Ανίχνευσης Εισβολών στο Δίκτυο για να δημιουργήσουν υβριδικά συστήματα. Τα συστήματα αυτού του είδους προσφέρουν μεγάλη ελαστικότητα και μπορούν να συνεισφέρουν στην αύξηση του επιπέδου ασφάλειας σε ένα σύστημα. Περιλαμβάνουν αισθητήρες σε διάφορες περιοχές του δικτύου ώστε να εντοπίζουν και να αναφέρουν επιθέσεις που συμβαίνουν σε ένα τμήμα ή σε όλο το δίκτυο.

2.2 Τεχνικές Ανίχνευσης Εισβολών

Υπάρχει ένα μεγάλο πλήθος από τεχνικές που χρησιμοποιούνται για να επιτευχθεί η αναγνώριση εισβολών. Οι δυο σημαντικότερες μέθοδοι για την ανίχνευση εισβολών στα σύγχρονα συστήματα είναι:

- Ανίχνευση ανωμαλιών (Anomaly Detection)
- Ανίχνευση κακής χρήσης (Misuse Detection)

2.2.1 Ανίχνευση Ανωμαλιών

Τα IDS που χρησιμοποιούν την τεχνική ανίχνευσης ανωμαλιών προσπαθούν να αναγνωρίσουν χαρακτηριστικά στην συμπεριφορά του συστήματος τα οποία εμφανίζονται μόνο όταν το σύστημα παρεκκλίνει από μια κατάσταση λειτουργίας που θεωρείται φυσιολογική. Τα IDS αυτά συγκεντρώνουν δεδομένα χρήσης για μια συγκεκριμένη περίοδο στην οποία το σύστημα βρίσκεται σε κανονικές συνθήκες. Η τεχνική αυτή είναι εξαιρετικά χρήσιμη για την ανίχνευση μη εξουσιοδοτημένης χρήσης του συστήματος, για την ανίχνευση εισβολής στα δίκτυα υπολογιστών καθώς και την αναγνώριση μη λογικών γεγονότων που με άλλους τρόπους θα ήταν δύσκολο να ανιχνευθούν. Αυτή η διαδικασία είναι γνωστή και ως ανίχνευση βάση συμπεριφοράς (behavior-based detection) επειδή σχετίζεται με αποκλίσεις στην συμπεριφορά των χρηστών ενός συστήματος. Συνήθως η ακρίβεια αυτής της φάσης αξιολογείται από εργαλεία όπως είναι τα σύνολα δεδομένων (datasets). Τέτοια είναι τα [1] και [2]. Το πλεονέκτημα των τεχνικών ανίχνευσης ανωμαλιών είναι ότι έχουν την δυνατότητα να ανιχνεύσουν νέες επιθέσεις ή παραλλαγές γνωστών απλά βασιζόμενες σε δεδομένα που έχουν συγκεντρωθεί σε μια προηγούμενη χρονική στιγμή. Ωστόσο, ένα από τα σημαντικότερα μειονεκτήματά της είναι οι εμφάνιση υψηλών ποσοστών σφαλμάτων κατά την αναγνώριση γνωστών επιθέσεων. Για περισσότερες λεπτομέρειες ο αναγνώστης παραπέμπεται στο [3], [4].

2.2.2 Ανίχνευση Κακής Χρήσης

Τα IDS αυτού του τύπου ανιχνεύουν μη λογικές συμπεριφορές με το να αναλύουν την κίνηση δεδομένων με βάση κανόνες που έχουν συντάξει ειδικοί στο χώρο. Η τεχνική αυτή είναι επίσης γνωστή και ως ανίχνευση βάσει υπογραφών (signature-based detection) επειδή στηρίζεται για την ανίχνευση των κακόβουλων ενεργειών σε συγκεκριμένες αλληλουχίες ενεργειών που συνιστούν τις υπογραφές επιθέσεων. Το πλεονέκτημα αυτών των τεχνικών είναι ότι επιτυγχάνουν υψηλούς ρυθμούς ανίχνευσης επιθέσεων με μικρό ποσοστό σφαλμάτων, όμως περιορίζεται στην ανίχνευση επιθέσεων που περιέχονται σε μια υπάρχουσα βάση υπογραφών. Προφανώς αυτή θα πρέπει να επικυρωποιείται διαρκώς για να περιλαμβάνει τις νεότερες επιθέσεις. Για περισσότερες λεπτομέρειες ο αναγνώστης παραπέμπεται στο [5].

Κεφάλαιο 3 Το Νεο Στάδιο Ανίχνευσης Εισβολών: SIEM

Η τεχνολογία SIEM είναι ένα σημαντικό στοιχείο για την στρατηγική ασφαλείας ενός οργανισμού, επειδή παρέχει μια ενοποιημένη εικόνα της κατάστασης της ασφάλειας του δικτύου από πολλαπλές και ετερογενείς μορφές παρακολούθησης. Έτσι μπορεί να χρησιμοποιηθεί για την ανίχνευση στοχευμένων και συνδυαστικών επιθέσεων στα αρχικά τους στάδια και να μειώσει τις επιπτώσεις τους στο δίκτυο. Τα εργαλεία SIEM προσφέρουν καταγραφή των ενεργειών που εκτελούν χρήστες και προγράμματα και εξάγουν αναφορές για την πιθανή ανίχνευση απειλών. Σήμερα πολλοί είναι οι οργανισμοί που επικεντρώνονται στην τυποποίηση τέτοιων εργαλείων, καθώς αναγνωρίζεται ότι αυτή η πρακτική βοηθάει στη βελτίωση της παρακολούθησης και της αντιμετώπισης των περιστατικών ασφαλείας.

3.1 Κίνητρα για την χρησιμοποίηση SIEM

Οι κυριότεροι λόγοι χρησιμοποίησης των SIEM είναι η αποδοτικότητα, η αποτελεσματικότητα καθώς και η συμμόρφωση με τα διεθνώς αποδεκτά πρότυπα ασφάλειας [6]. Αν κοιτάξουμε πιο αναλυτικά την σημερινή κατάσταση στον τομέα των δικτύων υπολογιστών θα παρατηρήσουμε μια ραγδαία αύξηση του μεγέθους και της πολυπλοκότητάς τους. Ως αποτέλεσμα, η ασφάλιση όλων αυτών των δικτυακών συσκευών απαιτεί την εγκατάσταση και λειτουργία εξειδικευμένων συσκευών και προγραμμάτων για την παρακολούθηση των δικτύων. Αυτό, όπως είναι λογικό, οδηγεί στην παραγωγή ενός τεράστιου αριθμού καταγραφών ασφαλείας (logs) καθημερινά, τα οποία πρέπει να παρακολουθούνται και να αναλύονται σε συνεχή βάση για όλες τις συσκευές και τα προγράμματα που παράγουν τέτοιου είδους καταγραφές. Σκοπός είναι η ανίχνευση κακόβουλων ενεργειών να είναι όσο το δυνατόν πιο άμεση, ώστε το αντίκτυπο της κακόβουλης ενέργειας να μετριαστεί ή ακόμα και να εκμηδενιστεί. Επίσης, η ομάδα παρακολούθησης της ασφάλειας των δικτύων θα πρέπει να έχει ανά πάσα στιγμή μια ολιστική εικόνα του τι συμβαίνει στα δίκτυα της, καθώς έχει αποδειχθεί στην πράξη ότι συσκευές μπορούν να παρακαμφθούν από κακόβουλους χρήστες με προχωρημένο γνωσιολογικό επίπεδο.

Συνοψίζοντας, γίνεται κατανοητό ότι δεν είναι εφικτή η επίτευξη ενός υψηλού επιπέδου ασφάλειας, αν οι συσκευές και τα προγράμματα ασφάλειας λειτουργούν ανεξάρτητα και η παρακολούθηση της κατάστασης του δικτύου γίνεται χειροκίνητα. Κρίνεται λοιπόν επιτακτική η ύπαρξη ενός αυτόνομου συστήματος το οποίο α) θα συγκεντρώνει τις καταγραφές ασφάλειας από όλες τις συσκευές που αλληλοεπιδρούν στο δίκτυο, β) θα εξάγει τις περιττές πληροφορίες, γ) θα

συνενώνει και θα εξάγει αποτελέσματα της κατάστασης του δικτύου σε πραγματικό χρόνο και δ) βάσει προκαθορισμένων ενεργειών θα μπορεί να αντιδράσει στην περίπτωση ανίχνευσης μιας κακόβουλης ενέργειας.

3.2 Τρόπος Λειτουργίας SIEM

Είναι βασικό να γίνει κατανοητός ο τρόπος λειτουργίας των SIEM ώστε να αποκομίσουμε μια γνώση σχετικά με το πως διαφοροποιείται από άλλες εφαρμογές και συσκευές ασφαλείας όπως τα συστήματα ανίχνευσης και αναχαίτησης εισβολών και τα τείχη πυρασφάλειας.

Παρόλο που στην αγορά σήμερα, υπάρχουν πολλές εναλλακτικές προτάσεις SIEM, στην πραγματικότητα τα συστήματα αυτού του είδους λειτουργούν με μια κοινή διαδικασία που μπορεί να διαχωριστεί σε 5 βασικά στάδια. Πιο συγκεκριμένα τα στάδια αυτά όπως περιγράφονται στο [7] είναι η α) Συλλογή (Collection), β) Ενοποίηση και Συσσωμάτωση (Consolidation and Aggregation), γ) Συσχέτιση (Correlation), δ) Επικοινωνία (Communication) και ε) Έλεγχος (Control). Απώτερος σκοπός των βημάτων αυτών είναι η ανάλυση των στοιχείων που λαμβάνονται από τις συσκευές του δικτύου και η εξαγωγή συμπερασμάτων σχετικών με το αν κακόβουλες ενέργειες λαμβάνουν χώρα στο υπό την εποπτεία δίκτυο.

3.2.1 Συλλογή

Τα SIEM λαμβάνουν ένα τεράστιο αριθμό καταγραφών ασφαλείας από διαφορετικά είδη δικτυακών συσκευών. Η μεταφορά τέτοιου τύπου δεδομένων θα πρέπει να γίνεται ασφαλώς, κάνοντας χρήση κρυπτογραφικών μεθόδων. Επιπλέον, θα πρέπει οι πηγές οι οποίες αποστέλλουν τις καταγραφές ασφαλείας να είναι αξιόπιστες ώστε να μη συντρέχει κίνδυνος λήψης παραποιημένων δεδομένων.

Ένα ακόμα ζήτημα που τίθεται είναι και η μορφή των δεδομένων που αποστέλλονται. Ο μεγαλύτερος αριθμός των σύγχρονων δικτυακών συσκευών ακολουθεί διεθνή πρότυπα όσον αφορά τη μορφή και τον τρόπο δομής των καταγραφών ασφαλείας (syslog, SNMP, OPSEC). Στην περίπτωση όμως που μία συσκευή του δικτύου δεν εναρμονίζεται με αυτά τα πρότυπα, γίνεται χρήση ενός προγράμματος που θα αναλάβει αυτή την εργασία. Αυτή είναι και μια από τις λειτουργίες των προγραμμάτων «πρακτόρων» καθώς απώτερος σκοπός τους είναι να συλλέξει τις καταγραφές ασφαλείας από ένα σύστημα και να τις αποστείλει στο SIEM σε μορφή που να είναι κατανοητή από το τελευταίο.

Υπάρχουν δύο τρόποι για την συλλογή των πληροφοριών: Η μέθοδος «λήψης» (pull), προϋποθέτει ότι το SIEM συνδέεται πάνω στην δικτυακή συσκευή και συλλέγει τις καταγραφές ασφαλείας. Αντίθετα η εναλλακτική μέθοδος η οποία χαρακτηρίζεται ως «αποστολή» (push) απαιτεί οι καταγραφές ασφαλείας να αποστέλλονται από την δικτυακή συσκευή προς το SIEM.

Η πρώτη μέθοδος προσδίδει στο SIEM μεγαλύτερο και καλύτερο έλεγχο, αλλά στον αντίποδα απαιτεί και περισσότερη υπολογιστική ισχύ. Σε τέτοιες περιπτώσεις το SIEM είναι υποχρεωμένο να δαπανήσει πόρους α) για να συνδέεται πάνω στην απομακρυσμένη συσκευή ανά τακτά χρονικά διαστήματα (ή να έχει μόνιμα μια σύνδεση ανοιχτή με την δικτυακή συσκευή), β) να ανιχνεύσει τις καταγραφές ασφαλείας, γ) να τις μεταφέρει σε αυτό και μετά δ) αν απαιτείται να τις μετατρέψει σε μια κατανοητή για αυτό μορφή.

Η δεύτερη μέθοδος είναι λιγότερο απαιτητική για το SIEM καθώς το μόνο που απαιτείται είναι ύπαρξη ενός προγράμματος (daemon) το οποίο θα εκτελείται διαρκώς «ακούγοντας» μια δικτυακή πόρτα (port). Όταν αυτή λάβει δεδομένα τότε το σύστημα τα επεξεργάζεται.

Μια ακόμα τεχνική που χρησιμοποιείται για την εξοικονόμηση πόρων, είναι το φιλτράρισμα των καταγραφών ασφαλείας τα οποία προορίζονται για περαιτέρω επεξεργασία. Καταγραφές ασφαλείας οι οποίες είναι μικρής σημασίας για την βιωσιμότητα και ασφάλεια του συστήματος και του δικτύου αποκλείονται. Με αυτόν τον τρόπο επιτυγχάνεται σημαντική εξοικονόμηση του εύρους (bandwidth) του δικτύου καθώς αποστέλλεται λιγότερος όγκος δεδομένων. Παράλληλα, εξοικονομείται τόσο αποθηκευτικός χώρος όσο και υπολογιστική ισχύς. Τέλος, μειώνεται και η πιθανότητα να πραγματοποιηθεί κατάρρευση του συστήματος από την μαζική αποστολή τεράστιου όγκου δεδομένων. Παράδειγμα τέτοιων περιπτώσεων είναι οι επιθέσεις άρνησης εξυπηρέτησης (Denial of Service Attacks - DoS).

Μια ακόμα σημαντική παράμετρος η οποία θα πρέπει να ληφθεί υπόψη είναι το είδος των καταγραφών ασφαλείας που δύναται να παραλειφθούν από την διαδικασία επεξεργασίας. Θα πρέπει πάντα να λαμβάνονται υπόψη οι νόμοι και οι ρυθμιστικοί κανονισμοί οι οποίοι πολλές φορές υποχρεώνουν την αποθήκευση συγκεκριμένων καταγραφών ασφαλείας για νομική χρήση ή ως αποδεικτικά στοιχεία σε περίπτωση που λάβει χώρα κάποιο περιστατικό που χρήζει περαιτέρω ανάλυσης.

3.2.2 Ενοποίηση και Συσσωμάτωση

Στο στάδιο αυτό οι καταγραφές ασφαλείας που έχουν συγκεντρωθεί κατά το προηγούμενο βήμα τροποποιούνται και μετατρέπονται σε καταγραφές ασφαλείας βάσει κάποιου κλειστού προτύπου. Παρόλα αυτά οι καταγραφές ασφαλείας αποθηκεύονται και στην αρχική τους μορφή (raw logs) για λόγους συμμόρφωσης με διεθνή πρότυπα διαχείρισης των πληροφοριών όπως το ISO-27001. Καθοριστικός παράγοντας στην συγκέντρωση των καταγραφών ασφαλείας είναι η σωστή χρονική συσχέτιση των καταγραφών που προέρχονται από διαφορετικές πηγές, οπότε κρίνεται αναγκαίος ο κοινός συγχρονισμός των πηγών που παράγουν τις καταγραφές ασφαλείας και αυτό μπορεί να επιτευχθεί με την χρήση του NTP (Network Time Protocol).

Μετά το στάδιο της κανονικοποίησης (normalization) έρχεται το στάδιο της συσσωμάτωσης (aggregation). Σε αυτό το στάδιο διαφορετικά γεγονότα (events) του ίδιου όμως τύπου συνδέονται μεταξύ τους με σκοπό να προσδώσουν μια πιο σχετική εικόνα του τι συμβαίνει. Είναι βασικό στο σημείο αυτό να διαχωρίσουμε τη διαδικασία της συσσωμάτωσης (aggregation) από αυτήν της συσχέτισης (correlation). Η βασική διαφορά είναι ότι κατά τη συσσωμάτωση συνδέονται ίδιου τύπου γεγονότα, όπως προαναφέρθηκε, ενώ κατά τη συσχέτιση συνδέονται μεταξύ τους διαφορετικού τύπου γεγονότα που προέρχονται από μια επίθεση.

3.2.3 Συσχέτιση

Στην φάση αυτή γεγονότα διαφορετικού τύπου συσχετίζονται μεταξύ τους με σκοπό την ανίχνευση της ύπαρξης μίας κακόβουλης ενέργειας. Τα περισσότερα SIEM συγκρίνουν τα συσχετιζόμενα γεγονότα με καταγραφές που βρίσκονται σε βάσεις δεδομένων που περιέχουν τις λεγόμενες υπογραφές διαφόρων επιθέσεων. Όπως αναφέρθηκε προηγουμένως ο τρόπος αυτός ανίχνευσης ονομάζεται και ανίχνευση με βάση υπογραφές. Μια δεύτερη τεχνική ανίχνευσης που δύναται να χρησιμοποιηθεί είναι η ανίχνευση βάσει συμπεριφοράς. Όπως προαναφέρθηκε, η μέθοδος αυτή βασίζεται στην ύπαρξη ενός μοντέλου που περιγράφει τα χαρακτηριστικά της «κανονικής» συμπεριφοράς για τις συσκευές και τους χρήστες του δικτύου. Στις περιπτώσεις που παρατηρηθούν αποκλίσεις από την «κανονική» αυτή συμπεριφορά, τότε το SIEM θα ενημερώσει τους χειριστές του για μια πιθανή ύπαρξη κάποιου κυβερνοπεριστατικού.

3.2.4 Επικοινωνία και Ειδοποίηση ή Αναφορά

Μια από τις κρισιμότερες διαδικασίες στον κύκλο λειτουργίας ενός εργαλείου SIEM είναι η διαδικασία με την οποία ενημερώνονται οι διαχειριστές των δικτύων για κάποιο περιστατικό, ώστε να παρθούν έγκαιρα οι αποφάσεις και να εκτελεστούν οι απαραίτητες διορθωτικές ενέργειες.

Οι κύριοι τρόποι με τους οποίους θα ενημερώσει ένα SIEM για τον εντοπισμό ύποπτης δραστηριότητας είναι τρεις: α) αποστολή μιας ειδοποίησης (alert) στους διαχειριστές μέσω κάποιων καναλιών επικοινωνίας όπως για παράδειγμα το email, β) αποστολή μιας αναφοράς στους χειριστές σε κάποια προκαθορισμένη χρονική στιγμή, και γ) ενημέρωση των διαχειριστών σε πραγματικό χρόνο μέσω μιας ιστοσελίδας. Υπάρχει και ένας ακόμα εναλλακτικός τρόπος δ) ο οποίος όμως εμφανίζεται μόνο στα πιο εξελιγμένα εκ των SIEM και είναι η αυτόματη άμεση αντίδραση (active - response). Σε αυτή τη μέθοδο το SIEM αντιδρά αυτόματα σε κάποιο περιστατικό σύμφωνα με κάποιες προκαθορισμένες διαδικασίες. Για παράδειγμα εάν ανιχνευθεί μια προσπάθεια παράνομης εισόδου σε ένα υπολογιστικό σύστημα, το SIEM μπορεί αυτόματα να μπλοκάρει την συγκεκριμένη ηλεκτρονική διεύθυνση και με αυτόν τον τρόπο να εμποδίσει την εξέλιξη της επίθεσης.

Όπως προαναφέρθηκε, πολλά σύγχρονα SIEM παράγουν αναφορές έτσι ώστε να ενημερώνουν για τυχόν περιστατικά τα οποία απαιτούν άμεση επίλυση. Οι αναφορές αυτές μπορούν να

προσδώσουν μια γρήγορη εικόνα της κατάστασης του δικτύου, καθώς και μέσω στατιστικών γραφημάτων να ενημερώσουν άτομα τα οποία δεν διαθέτουν τις απαραίτητες τεχνικές γνώσεις, όπως την ιεραρχία του οργανισμού.

3.2.5 Αποθήκευση

Μετά τη διαδικασία της ανάλυσης τα δεδομένα θα πρέπει να αποθηκευτούν σε βάσεις. Η αποθήκευση τέτοιου είδους πληροφορίας θα πρέπει να γίνεται τόσο στην επεξεργασμένη μορφή τους, για γρήγορη ανάκτηση τους σε περίπτωση που απαιτηθούν, όσο και στην αρχική τους μορφή (raw data). Η δεύτερη διαδικασία γίνεται ώστε να καλυφθεί η περίπτωση που θα πρέπει τα δεδομένα αυτά να χρησιμοποιηθούν σαν νομικό πειστήριο όσο και αν απαιτείται από κάποιο πιστοποιητικό συμμόρφωσής όπως ISO 27001 , PCI DSS 2.0/3.0.

3.3 Κρίσιμα Χαρακτηριστικά ενός SIEM

Δεκάδες εμπορικά προϊόντα SIEM έχουν κάνει την εμφάνισή τους τα τελευταία χρόνια. Αυτά προσπαθούν μέσω καινοτομιών να κερδίσουν την εμπιστοσύνη μεριδίου της αγοράς. Για την αντικειμενική αξιολόγηση των προϊόντων αυτών θα πρέπει να τεθούν κάποια χαρακτηριστικά τα οποία θα αποτελέσουν τη βάση σύγκρισης. Στην παρούσα εργασία λαμβάνουμε σαν άξονα σύγκρισης οκτώ βασικά χαρακτηριστικά όπως αυτά έχουν διατυπωθεί αρχικά στην εργασία [6]:

- Παρακολούθηση σε πραγματικό χρόνο (Real-time monitoring): Η διαδικασία ανάλυσης γεγονότων που λαμβάνει χώρα στα SIEM φανερώνει πιθανές συσχετίσεις ανάμεσα στα μηνύματα και καταγραφές ασφαλείας που παράγονται από τις συσκευές, τα συστήματα ή τις εφαρμογές, με βάση διαφορετικά χαρακτηριστικά όπως ο τύπος της πηγής, ο στόχος, τα πρωτόκολλα που χρησιμοποιούνται καθώς και τον τύπο των γεγονότων που λαμβάνουν χώρα. Τυπικά υπάρχει μια βιβλιοθήκη με προκαθορισμένους κανόνες συσχέτισης (correlation rules) και παρέχεται η δυνατότητα παραμετροποίησης των κανόνων. Κρίνεται αναγκαίο να υπάρχει ένα περιβάλλον απεικόνισης των γεγονότων και των περιστατικών αυτών σε πραγματικό χρόνο.

- Παρακολούθηση των δεδομένων και των χρηστών (Data and user monitoring): Αυτή η δυνατότητα καθορίζει το πλαίσιο στο οποίο επιτρέπεται να δρουν οι χρήστες και καθιστά δυνατή την πρόσβαση στα δεδομένα και τις δραστηριότητες αυτών. Μεταξύ άλλων, τέτοιες λειτουργίες ενσωματώνουν υποδομές ελέγχου πρόσβασης και ταυτοποίησης (IAM - Identity Access Management) έτσι ώστε να συγκεντρώνουν τις δραστηριότητες των χρηστών και να τις συσχετίζουν, να τις αναλύουν και να τις αναφέρουν. Η παρακολούθηση της δραστηριότητας χρηστών με υψηλά δικαιώματα καθώς και η ανάλυση ευαίσθητων δεδομένων είναι μια συνήθης προϋπόθεση.

- Παρακολούθηση των εφαρμογών (Application monitoring): Η ικανότητα ανάλυσης ροών προερχόμενων από διαφορετικού τύπου εφαρμογές που τρέχουν στο δίκτυο επιτρέπει την επίβλεψη της κατάστασης ασφαλείας στο επίπεδο εφαρμογών. Συνεργατική δράση των εφαρμογών καθώς και ένα πλαίσιο το οποίο θα επιτρέπει τον καθορισμό του τύπου περιστατικών που μέχρι τώρα δεν υποστηρίζονταν είναι σημαντικά χαρακτηριστικά για την ανίχνευση επιθέσεων που λαμβάνουν χώρα στα υψηλότερα επίπεδα.

- Ενημερωμένη βάση με απειλές (Threat Intelligence): Πληροφορίες σχετικά με τις πιο πρόσφατα εμφανιζόμενες απειλές μπορούν να αντληθούν από πολλές πηγές, συμπεριλαμβανομένων των ελεύθερα διαμοιραζόμενων λιστών ή των αναλύσεων που ειδικές ομάδες διεξάγουν. Οι πληροφορίες για τις απειλές μπορούν να ενσωματωθούν στο SIEM σε διάφορες μορφές όπως σε κανόνες συσχέτισης και έτσι μπορούν να αυξήσουν το ποσοστό ανίχνευσης των απειλών αυτών.

- Παρακολούθηση συμπεριφορών (Behavior profiling): Η διαδικασία δόμησης προφίλ που περιγράφουν την ομαλή συμπεριφορά του δικτύου, ξεκινάει αρχικά με το στάδιο εκμάθησης κατά το οποίο δομούνται τα προφίλ κανονικής λειτουργίας σε διάφορες κατηγορίες όπως δικτυακή κίνηση, δραστηριότητες χρηστών, πρόσβαση στους εξυπηρετητές κ.α. Το στάδιο παρακολούθησης λαμβάνει χώρα αμέσως μετά, ανιχνεύοντας αποκλίσεις από αυτά που υπαγορεύονται στο προφίλ και δημιουργώντας συναγερμούς. Η ανίχνευση των ανωμαλιών θεωρείται ως μια νέα δυνατότητα των SIEM η οποία βρίσκεται σε πειραματικό στάδιο και προς το παρόν συμπληρώνει την ανίχνευση με βάση τους κανόνες συσχέτισης.

- Ανάλυση των δεδομένων(Analytics): Η ανάλυση των συμβάντων ασφαλείας περιλαμβάνει την παράθεση δεδομένων σε σχεδιαγράμματα, αναφορές καθώς και τη δυνατότητα υποβολής ερωτημάτων, έτσι ώστε να διευκολύνεται η εξιχνίαση των δραστηριοτήτων που λαμβάνουν χώρα στο δίκτυο και να πραγματοποιείται γρήγορη ανίχνευση απειλών, ανίχνευση οποιασδήποτε παράνομης πρόσβασης καθώς και ανίχνευση μη ορθών χρήσεων των δικαιωμάτων πρόσβασης.

- Διαχείριση καταγραφών ασφαλείας και αναφορά (Log management and reporting): Εδώ περιλαμβάνονται λειτουργίες που υποστηρίζουν μια οικονομική αποθήκευση και ανάλυση ενός μεγάλου αριθμού πληροφοριών. Τέτοιες είναι η ταξινόμηση και αποθήκευση όλων των καταγραφών ασφαλείας και των συμβάντων από κάθε πηγή, καθώς και την δυνατότητα εύρεσης και αναφοράς των δεδομένων αυτών. Η μορφή της αναφοράς θα πρέπει να είναι προκαθορισμένες ή να δίδεται η ικανότητα κατασκευής φορμών από το χρήστη ή ακόμα και να επιτρέπεται χρήση φορμών από άλλα εμπορικά εργαλεία.

Πίνακας 1 Βαρύτητα στην αξιολόγηση των κρίσιμων χαρακτηριστικών

Κρίσιμα Χαρακτηριστικά	**Ολικό**	**Συμμόρφωση**	**Διαχείριση Απειλών**	**SIEM**
Παρακολούθηση σε Πραγματικό Χρόνο	12.5%	2.0%	18.0%	15.0%
Ενημερωμένη Βάση Απειλών	12.5%	2.0%	9.0%	10.0%
Παρακολούθηση Συμπεριφορών	12.5%	2.0%	10.0%	7.0%
Παρακολούθηση Δεδομένων και Χρηστών	12.5%	10.0%	10.0%	8.0%
Παρακολούθηση Εφαρμογών	12.5%	2.0%	10.0%	6.0%
Ανάλυση Δεδομένων	12.5%	2.0%	23.0%	8.0%
Διαχείριση Καταγραφών Ασφαλείας και Αναφορά	12.5%	55.0%	10.0%	26.0%
Ευκολία Εγκατάστασης και Συντήρησης	12.5%	25.0%	10.0%	20.0%

3.4 Γνωστά Προϊόντα

Η τεχνολογία των SIEM υποστηρίζει διαχείριση των απειλών και αντιμετώπιση των περιστατικών ασφαλείας. Κάτι τέτοιο επιτυγχάνεται μέσω της συλλογής και ανάλυσης των συμβάντων ασφαλείας από ένα μεγάλο πλήθος το οποίο συγκεντρώνονται από διάφορες πηγές στο δίκτυο, σε πραγματικό χρόνο. Οι κύριες δυνατότητες της τεχνολογίας των SIEM είναι το ευρύ φάσμα συλλογής συμβάντων και η δυνατότητα συσχέτισης και ανάλυσης δεδομένων από ετερογενείς πηγές. Τέτοιου είδους τεχνολογία εφαρμόζεται ώστε να επιτευχθεί:

- Ανίχνευση εσωτερικών και εξωτερικών απειλών
- Παρακολούθηση των δραστηριοτήτων των χρηστών με δικαιώματα
- Παρακολούθηση της πρόσβασης στους εξυπηρετητές και τις βάσεις δεδομένων

- Παρακολούθηση, συσχέτιση και ανάλυση των δραστηριοτήτων των χρηστών σε πολλαπλά συστήματα και εφαρμογές
- Παροχή αναφορών που βασίζονται πάνω σε πρότυπα συμμόρφωσης
- Παροχή πληροφοριών και τρόπων δράσης για την αντιμετώπιση των περιστατικών ασφαλείας

Γενικότερα, τα SIEM συγκεντρώνουν και αναλύουν τα συμβάντα από διάφορες συσκευές, συστήματα και εφαρμογές. Η κύρια πηγή δεδομένων είναι οι καταγραφές ασφαλείας. Η SIEM τεχνολογία μπορεί επιπλέον να επεξεργαστεί δεδομένα διαφορετικών μορφών. Τα δεδομένα κανονικοποιούνται έτσι ώστε τα συμβάντα από διάφορες πηγές να μπορούν να συσχετιστούν και να αναλυθούν για συγκεκριμένους σκοπούς όπως την παρακολούθηση των δικτυακών συμβάντων ασφαλείας και της δραστηριότητας των χρηστών για την ανίχνευση κακής χρήσης ή κάποιας παραβίασης.

3.4.1 AlienVault

Το λογισμικό διαχείρισης ασφαλείας της AlienVault προσφέρει δυνατότητες SIEM καθώς και ανίχνευση αδυναμιών πραγματοποιώντας α) ελέγχους ανίχνευσης ευπαθειών, β) ανίχνευση εισβολών τόσο σε δικτυακό επίπεδο όσο και σε επίπεδο υπολογιστή και γ) παρακολούθηση της ακεραιότητας των αρχείων. Η επί πληρωμή διανομή επεκτείνει τις δυνατότητες της ανοιχτής πλατφόρμας Open Source SIM (OSSIM) παρέχοντας δυνατότητες διαχείρισης των καταγραφών ασφαλείας, ενοποιημένη διαχείριση και αναφορά και διαμοιρασμό των εργασιών. Η AlienVault παρέχει το προϊόν της, σε τρεις εκδόσεις κάθε μια από τις οποίες απευθύνεται σε οργανισμούς διαφορετικής κλίμακας.

3.4.2 EiQ Networks

Η EiQ Networks' SecureVue παρέχει δυνατότητες Security Event Management (SEM), καθώς και Security Incident Management (SIM). Επιπρόσθετα, δίνει τη δυνατότητα για διαμόρφωση πολιτικών συμμόρφωσης με διάφορα πρότυπα, έλεγχο ακεραιότητας αρχείων, λειτουργίες παρακολούθησης της απόδοσης του συστήματος καθώς και δυνατότητες ανάλυσης της συμπεριφοράς του δικτύου. Η αρχιτεκτονική της SecureVue's περιλαμβάνει μια ιεραρχία από εξυπηρετητές καθώς και τους κατάλληλους αισθητήρες. Έτσι, μια μινιμαλιστική εγκατάσταση αποτελείται από έναν κεντρικό καθολικό εξυπηρετητή και ένα αισθητήρα. Ένας αισθητήρας είναι στην ουσία μια συσκευή στο δίκτυο η οποία χρησιμοποιείται για συλλογή δεδομένων. Επιπρόσθετα στρώματα από εξυπηρετητές και ειδικοί αισθητήρες μπορούν να προστεθούν ώστε να επεκτείνουν τη δομή. Τα διάφορα τμήματα του συγκεκριμένου προϊόντος είναι προγράμματα ή συσκευές. Οι αισθητήρες παρέχονται μόνο σε software μορφή. Η EiQ Networks επιπλέον παρέχει την SIEM τεχνολογία ειδικά παραμετροποιημένη για μικρού και μεσαίου μεγέθους εταιρίες. Ονομάζεται SecureVue NGS και διατίθεται σε μορφή λογισμικού αλλά και σε συσκευή.

3.4.3 EMC-RSA

Στην RSA, το τμήμα ασφάλειας του EMC σταδιακά αντικαθιστά το προϊόν enVision με το προϊόν RSA Security Analytics (SA), το οποίο είναι μια SIEM λύση που βασίζεται στην πλατφόρμα NetWitness. Το RSA SA παρέχει πλήρη καταγραφή εγγράφων ασφαλείας καθώς και πλήρη ανίχνευση πακέτων που διακινούνται στο δίκτυο, αλλά και βασική παρακολούθηση της κατάστασης του δικτύου και ανάλυση των δεδομένων.

Τα βασικά κομμάτια που δομούν το RSA SA είναι τα εξής:

- Κόμβοι οι οποίοι αποκωδικοποιούν και καταγράφουν την κίνηση του δικτύου
- Κόμβοι οι οποίοι συλλέγουν δεδομένα και αρχειοθετούν την πληροφορία αυτή σε πραγματικό χρόνο
- Κόμβοι οι οποίοι συγκεντρώνουν στοιχεία και δημιουργούν αναφορές βάσει στατιστικών αναλύσεων

3.4.4 HP-ArcSight

Το HP-ArcSight είναι μια οικογένεια προϊόντων ασφαλείας η οποία παρέχει τρεις εκδόσεις SIEM:

- Το Enterprise Security Manager για μεγάλης κλίμακας διαχείριση συμβάντων
- Το ArcSight Express για μικρού και μεσαίου μεγέθους οργανισμούς
- Το Logger για διαχείριση των καταγραφών ασφαλείας και δημιουργία αναφορών

Η δυνατότητα εγκατάστασης του Logger παράλληλα με το προϊόν ArcSight παρέχει επιπρόσθετες δυνατότητες για ανάλυση δεδομένων καθώς και συλλογή δεδομένων από το επίπεδο των εφαρμογών (application layer). Η HP χρησιμοποιεί το ArcSight για να ενοποιήσει την διαχείριση των συμβάντων με τις τεχνολογίες ασφάλειας και με αυτό τον τρόπο να παρέχει μια ολοκληρωμένη εικόνα των διαδικασιών και των συμβάντων ασφαλείας. Επιπλέον, το ArcSight μπορεί να συνδυάσει τις δυνατότητές του με άλλα προϊόντα όπως το Fortify, TippingPoint, and IT Performance Suite (Operations Manager and Network Node Manager). Το ArcSight επίσης μπορεί να διασυνδέεται με το HP EnterpriseView και παρέχει μια κεντρικοποιημένη εικόνα του IT τμήματος.

3.4.5 IBM-Q1 Labs

Η σειρά IBM-Q1 Labs' QRadar μπορεί να αποτελέσει μια ολοκληρωμένη λύση για μικρά εταιρικά περιβάλλοντα. Εναλλακτικά, μπορεί να αναπτυχθεί οριζοντίως ώστε να υποστηρίζει μεγαλύτερα περιβάλλοντα με εξειδικευμένη συλλογή συμβάντων, επεξεργασία και προβολή των περιστατικών ασφαλείας. Ένα ιδιαίτερο χαρακτηριστικό της τεχνολογίας αυτής είναι η συλλογή και

επεξεργασία δεδομένων από το πρωτόκολλο NetFlow που αποσκοπεί στην ανάλυση της συμπεριφοράς του δικτύου με βάση τις εφαρμογές που τρέχουν σε αυτό και στην ανάλυση της συμπεριφοράς των συμβάντων από κάθε πηγή που αλληλοεπιδρά με το SIEM. Το Q1 Labs προαιρετικά παρέχει το QRadar Risk Manager, το οποίο προσθέτει δυνατότητες παρακολούθησης των ρυθμίσεων του δικτύου και των firewalls καθώς και σε βάθος ανάλυση των συμβάντων ασφαλείας.

3.4.6 LogRhythm

Το LogRhythm μπορεί να χρησιμοποιηθεί ως μια συσκευή στο δίκτυο ή ως λογισμικό (συνήθως σε μικρότερες εγκαταστάσεις) για να παρέχει διαχείριση των καταγραφών και των συμβάντων ασφαλείας. Εναλλακτικά, μπορεί να εγκατασταθεί σαν σύνολο από εξειδικευμένες συσκευές για την καταγραφή περιστατικών, διαχείριση συμβάντων και κεντρικού ελέγχου. Η τεχνολογία αυτή περιλαμβάνει προαιρετικούς πράκτορες για τα κύρια λειτουργικά συστήματα οι οποίοι είναι υπεύθυνοι για τη διαδικασία του φιλτραρίσματος των καταγραφών ασφαλείας.

3.4.7 McAfee ESM

Η σειρά McAfee ESM (γνωστή και ως NitroView) συνδυάζει την συλλογή συμβάντων ασφαλείας και παρέχει διαδικασίες για την απεικόνιση αυτών σε πραγματικό χρόνο παρέχοντας ταυτόχρονα την δυνατότητα για DPI (Deep Packet Inspection), με σκοπό την επιθεώρηση του περιεχομένου των πακέτων που παράγονται από τις ενέργειες των χρηστών ή εφαρμογών.

3.4.8 NetIQ

Το NetIQ Sentinel αποτελείται από τρία κύρια μέρη: α) τον πυρήνα του συστήματος (Sentinel Server) , β) το Sentinel Log Manager καθώς και το Sentinel Agents. Ο Sentinel Server καθώς και το Sentinel Log Manager προσφέρονται και σε μορφή λογισμικού, αλλά και σαν εικονική συσκευή. Το NetIQ Sentinel συνεργάζεται και με άλλα προγράμματα της εταιρίας όπως το AppManager Identity Manager, Access Manager, Directory and Resource Administrator, και το Secure Configuration Manager.

3.4.9 Sensage

Το KEYW's Sensage είναι βελτιστοποιημένο για ανάλυση μεγάλου όγκου δεδομένων. Η τεχνολογία αυτή έχει αποδειχθεί κατάλληλη για περιπτώσεις όπου απαιτείται παρακολούθηση στο επίπεδο εφαρμογής για χρήστες και εφαρμογές.

3.4.10 SolarWinds

Το SolarWinds Log and Event Manager (LEM) λογισμικό παρέχεται σε μορφή εικονικής συσκευής. Το λογισμικό αυτό είναι κατάλληλο για μικρομεσαίες επιχειρήσεις και προσφέρει παρακολούθηση σε πραγματικό χρόνο καθώς και διαχείριση των καταγραφών ασφαλείας. Επιπλέον

προαιρετικά παρέχεται ένα επιπλέον στέλεχος το οποίο είναι κατάλληλο για παρακολούθηση των διεργασιών και των συμβάντων ασφαλείας στους τερματικούς σταθμούς.

3.4.11 Splunk

Το Splunk Enterprise παρέχει διαχείριση των καταγραφών ασφαλείας, επεξεργασία και στατιστική ανάλυση των δεδομένων τα οποία διευκολύνουν την συσχέτιση των δεδομένων ασφάλειας σε πραγματικό χρόνο. Το Splunk App for Enterprise Security παρέχει πίνακες απεικόνισης των πληροφοριών, αναζητήσεις, δημιουργία αναφορών καθώς και διαφορετικές μεθόδους ειδοποίησης αν κάποιο περιστατικό λάβει χώρα. Το Splunk είναι από τα πιο διαδεδομένα SIEM σε IT τμήματα και τμήματα υποστήριξης καθώς έχει σαν πρωταρχικό στόχο την διαθεσιμότητα των υπηρεσιών.

3.4.12 Symantec

Το Symantec Security Information Manager (SSIM) παρέχεται σε μορφή λογισμικού και παρέχει δυνατότητες διαχείρισης πληροφοριών ασφάλειας (Security Information Management – SIM) καθώς και διαχείρισης περιστατικών ασφαλείας (Security Events Management – SEM) και διαχείρισης καταγραφών ασφαλείας. Το SSIM συνεργάζεται και με τεχνολογίες όπως τα Security Endpoint Protection (SEP) καθώς και άλλα σχετικά εργαλεία. Η βάση δεδομένων των απειλών και των ευπαθειών ανανεώνεται μέσω του Symantec's DeepSight. Επιπλέον, το SIEM μπορεί να εγκατασταθεί και σε εικονικό περιβάλλον VMWare. Η Symantec σκοπεύει να ενσωματώσει όλα τις τα προϊόντα κάτω από μια ενιαία αρχιτεκτονική.

3.4.13 Tibco-LogLogic

Το LogLogic παρέχει δυνατότητες διαχείρισης των καταγραφών ασφαλείας καθώς και λειτουργίες για αναζητήσεις, ειδοποιήσεις και δημιουργία αναφορών για συμμόρφωση με την νομοθεσία. Το LogLogic επίσης διαθέτει το στέλεχος Security Event Manager appliance το οποίο είναι ένα SEM που παρέχει προστασία πραγματικού χρόνου. Παράλληλα, παρέχει και το Database Security Manager appliance που είναι ένα εργαλεία για παρακολούθηση των διεργασιών ενός συστήματος με τη βοήθεια πρακτόρων. Τέλος, παρέχεται και ένα εξειδικευμένο εργαλείο που βοηθάει τους οργανισμούς να κρίνουν αν το σύστημά τους συμμορφώνεται με τα διεθνή πρότυπα διαχείρισης των πληροφοριών.

Πίνακας 2 Αξιολόγηση κρίσιμων χαρακτηριστικών για δημοφιλή SIEM

Αξιολόγηση Προϊόντος	AlienVault	EiQ Networks	EMC-RSA	HP-ArcSight	IBM-Q1 Labs	LogRhythm	McAfee ESM	NetIQ	Sensage	SolarWinds	Splunk	Symantec	Tibco-LogLogic
Παρακολούθηση σε Πραγματικό Χρόνο	2.80	3.2	2.8	4.1	3.9	3.53	3.55	3.90	2.6	3.03	3.0	3.40	2.85
Ενημερωμένη Βάση Απειλών	3.30	3.0	4.0	4.0	4.0	3.00	4.00	1.00	3.5	1.00	3.5	4.7	1.0
Παρακολούθηση Συμπεριφορών	3.5	3.3	3.0	3.8	4.5	3.5	3.25	3.5	3.3	2.0	3.3	2.0	3.4
Παρακολούθηση Δεδομένων και Χρηστών	2.6	3.0	3.2	4.2	3.5	3.58	3.54	3.08	3.6	3.06	3.1	2.92	2.79
Παρακολούθηση Εφαρμογών	3.17	3.0	3.3	4.1	3.5	3.58	3.83	2.4	3.7	3.0	3.7	3.08	2.42
Ανάλυση Δεδομένων	3.28	2.9	3.5	3.7	3.9	3.0	3.7	2.69	3.7	2.25	3.7	3.0	2.87
Διαχείριση Καταγραφών Ασφαλείας και Αναφορά	3.04	3.3	2.9	3.8	3.5	3.62	3.68	3.31	3.5	3.29	3.4	3.48	4.0
Ευκολία Εγκατάστασης και Συντήρησης	3.53	3.2	2.5	3.3	4.0	4.0	3.5	3.8	2.3	5.0	2.9	3.0	3.85

Κεφάλαιο 4 **Εισαγωγή στη Λειτουργία του OSSIM**

4.1 Εισαγωγή

Σκοπός του κεφαλαίου είναι να παρέχει μια γρήγορη και περιεκτική εικόνα του εργαλείου AlienVault OSSIM, τα μέρη από τα οποία αποτελείται, τη μεθοδολογία εγκατάστασης , άλλα και τις επιλογές παραμετροποίησης. Τελικός στόχος είναι να καταστήσει τον αναγνώστη ικανό να αντιλαμβάνεται έγκαιρα τις δικτυακές επιθέσεις που μπορεί να λάβουν χώρα στα υπό την εποπτεία δίκτυα.

Το αρκτικόλεξο OSSIM προέρχεται από την συντομογραφία των λέξεων Open Source Security Information Management. Το εργαλείο αυτό υπάγεται στην κατηγορία εργαλείων διαχείρισης πληροφοριών ασφάλειας.

4.2 Κύρια Μέρη του OSSIM

Το OSSIM αποτελείται από πέντε (5) κύρια μέρη: (α) εξυπηρετητής, (β) πλαίσιο εργασίας, (γ) αισθητήρας, (δ) βάση δεδομένων, (ε) επιπρόσθετα στοιχεία. Καθένα από αυτά τα στοιχεία θα μελετηθεί με μεγαλύτερη λεπτομέρεια στη συνέχεια.

4.2.1 Εξυπηρέτης

Ο εξυπηρέτης είναι το βασικό στέλεχος του συστήματος. Εκεί, εκτελούνται όλες οι διεργασίες που απαιτούνται ώστε να εξαχθούν τα αποτελέσματα από την επεξεργασία των δεδομένων που του παρέχουμε. Οι κυριότερες διεργασίες οι οποίες πραγματοποιούνται στον εξυπηρέτη είναι:

- **Συσχέτιση Περιστατικών**: Είναι η διαδικασία κατά την οποία εξάγονται τα σημαντικότερα γεγονότα μέσα από ένα μεγάλο όγκο περιστατικών. Αυτό επιτυγχάνεται μέσω της παρακολούθησης, ανάλυσης και συσχέτισης των περιστατικών.

- **Αναγνώριση Κινδύνου**: Είναι η διαδικασία κατά την οποία γίνεται ανάλυση των κινδύνων βάσει της υποδομής και των λειτουργιών που διαθέτουμε και μετά από αυτό πραγματοποιείται κατάταξη των περιστατικών ανάλογα με την επικινδυνότητα τους.

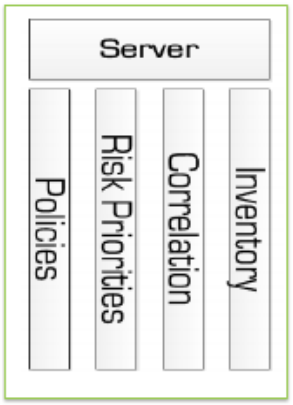
- **Διαχείριση Ευρετηρίου**: Είναι η διαδικασία κατά την οποία καταχωρούνται και αναλύονται οι συσκευές και υπηρεσίες οι οποίες υπάρχουν στην δικτυακή μας υποδομή.

- **Ειδοποιήσεις και Προγραμματισμός**: Είναι η διαδικασία κατά την οποία σε περίπτωση

ανίχνευσης κυβερνοπεριστατικού ενεργοποιείται κάποιος συναγερμός. Εδώ περιλαμβάνονται όλες οι διαδικασίες χειρισμού του σχεδιασμού για λειτουργίες που εκτελούνται περιοδικά (π.χ. vulnerability testing)

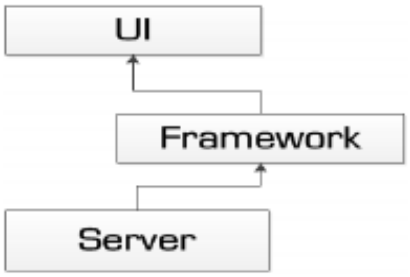
- **Διαχείριση Πολιτικών**: Είναι η διαδικασία κατά την οποία παρέχεται η δυνατότητα δημιουργίας και χειρισμού πολιτικών (φίλτρων) για την μείωση της πλεονάζουσας πληροφορίας.

- **Μηχανισμός Ενημέρωσης Απειλών** : Είναι μια διαδικασία κατά την οποία το σύστημα ανταλλάσσει δεδομένα με ένα δίκτυο ανταλλαγής ανώνυμων δεδομένων για κακόβουλες διευθύνσεις διαδικτύου. Η εταιρία AlienVault το ονομάζει αυτό το δίκτυο OTX (Open Threat Exchange).



Εικόνα 4-1 Κύριες Διεργασίες OSSIM Server

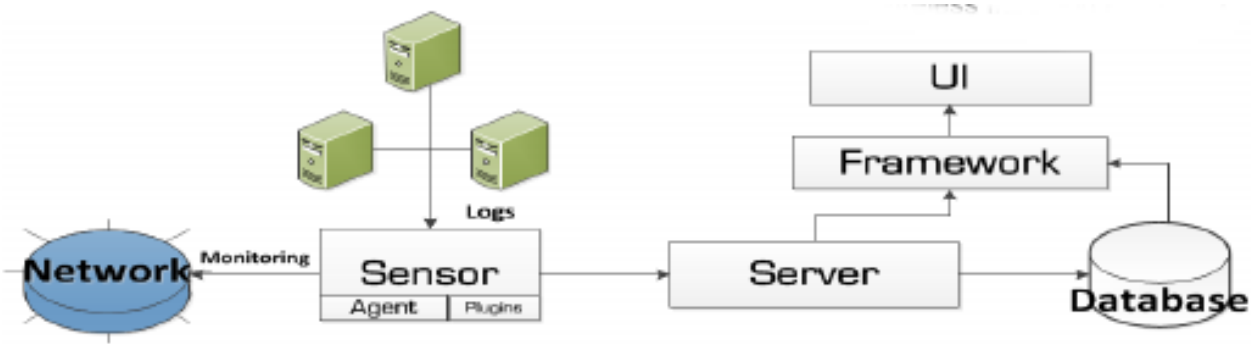
Το πλαίσιο εργασίας είναι το τμήμα το οποίο είναι επιφορτισμένο με την αρμοδιότητα να «μεταφράζει» τις εντολές που δίνονται από το γραφικό περιβάλλον σε εντολές που καταλαβαίνει ο εξυπηρέτης. Όπως γίνεται κατανοητό είναι ένα ενδιάμεσο επίπεδο μεταξύ του γραφικού περιβάλλοντος διαχείρισης και του εξυπηρέτη.



Εικόνα 4-2 Το πλαίσιο εργασίας OSSIM

4.2.2 Αισθητήρας

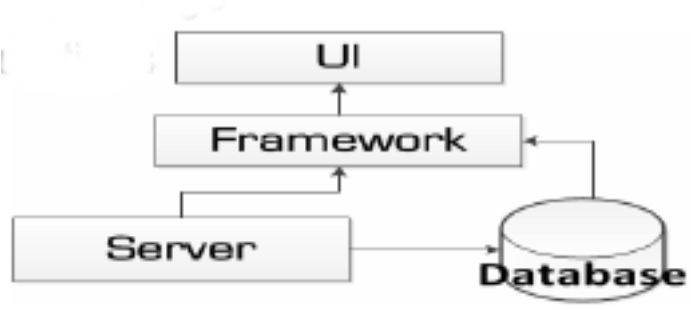
Ένας αισθητήρας είναι ένα κομμάτι του συστήματος το οποίο έχει ως αποστολή να συγκεντρώνει όλες τις καταγραφές ασφαλείας που έχουν συλλεχθεί είτε από τους ενσωματωμένους πράκτορες του είτε από εξωτερικούς πράκτορες και τους στέλνει στον εξυπηρέτη όπου και θα υποστούν περεταίρω επεξεργασία.



Εικόνα 4-3 Ο αισθητήρας OSSIM

4.2.3 Βάση Δεδομένων

Η βάση δεδομένων είναι το τμήμα του συστήματος το οποίο χρησιμοποιείται για την αποθήκευση όλων των παραμετροποιήσεων, των αγαθών, και των καταγραφών ασφαλείας. Σε αυτό το σημείο πρέπει να τονίζουμε ότι η βάση δεδομένων δεν αποθηκεύει καταγραφές ασφαλείας στην αρχική μορφή που αυτές παράγονται. Αυτό γίνεται ώστε να αυξηθεί η απόδοση του συστήματος ωστόσο για τις περιπτώσεις που αντίστοιχη λειτουργία απαιτείται, υπάρχει το κατάλληλο εργαλείο το οποίο διατίθεται μόνο στην επί πληρωμή έκδοση του AlienVault την USM.



Εικόνα 4-4 Η βάση δεδομένων OSSIM

4.3 Επιπρόσθετα Στοιχεία (DS Plug-ins)

Το OSSIM έχει την δυνατότητα να συγκεντρώνει καταγραφές ασφαλείας από πολλές γνωστές δικτυακές συσκευές, αλλά και από εφαρμογές οι οποίες διαθέτουν δυνατότητες καταγραφής ανάλογων πληροφοριών. Στην συνέχεια, επεξεργάζεται τις καταγραφές ασφαλείας αυτές και εξάγει τα απαραίτητα δεδομένα που εν συνεχεία τα χρησιμοποιήσει για την εξαγωγή των αποτελεσμάτων. Η επεξεργασία αυτή ονομάζεται κανονικοποίηση (normaliazation).

Για να επιτύχει κάτι τέτοιο ο αυτό ο αισθητήρας του OSSIM χρησιμοποιεί τα επονομαζόμενα Data Source Connectors (DS Connectors) ή OSSIM Collection Plug-ins ή εναλλακτικά τα DS Plug-ins.

Τα DS Plug-ins είναι απλά αρχεία ρυθμίσεων (configuration files) τα οποία περιέχουν όλες τις απαραίτητες οδηγίες που χρειάζεται ο αισθητήρας του OSSIM για να προχωρήσει σε κανονικοποίηση των εγγραφών ασφαλείας που λαμβάνει από μία συγκεκριμένη πηγή.

4.4 Εγκατάσταση OSSIM

Σε αυτή την ενότητα θα αναλύσουμε τα βήματα που απαιτούνται για να γίνει εγκατάσταση του OSSIM σε έναν φυσικό εξυπηρέτη. Το OSSIM στηρίζεται πάνω στην διανομή linux λειτουργικού Debian. Είναι ένα open-source project.

Το πρώτο βήμα είναι να κατεβάσουμε ένα ασφαλές αντίγραφο του OSSIM από το επίσημο website της εταιρίας AlienVault[1].

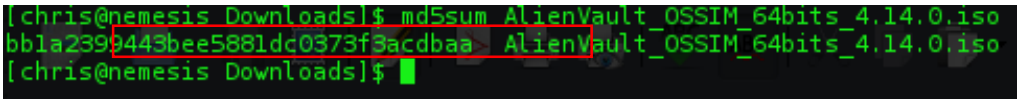
Από τον επίσημο δικτυακό τόπο υπάρχει η δυνατότητα για καταφόρτωση του αντίστοιχου αρχείου για το OSSIM. Το OSSIM παρέχεται ενοποιημένο με λειτουργικό σύστημα οπότε δεν χρειάζεται καμία προηγουμένως διαδικασία πριν αρχίσουμε την εγκατάσταση του. Το μόνο που απαιτείται είναι να πραγματοποιηθεί αντιγραφή του αντίστοιχου αρχείου σε ένα οπτικό μέσον (DVD).

Επειδή το OSSIM θα αλληλοεπιδρά με όλες τις συσκευές που είναι διασυνδεδεμένες στα δίκτυα που παρακολουθούμε θα είναι συνετό να γίνει έλεγχος πριν πραγματοποιηθεί εγκατάσταση του OSSIM σχετικά με το αν το αρχείο που καταφορτώθηκε δεν είναι παραποιημένο. Η διαδικασία αυτή μπορεί να πραγματοποιηθεί με τη χρήση της εντολής md5sum. Μέσω αυτής μπορεί να γίνει έλεγχος για το αν το αποτέλεσμα της μονόδρομης συνάρτησης κατακερματισμού (hash) είναι ίδια με αυτή που διατίθεται από τον αντίστοιχο ιστότοπο για επιβεβαίωση. Αν εναλλακτικά διατίθεται

[1] https://www.alienvault.com/open-threat-exchange/projects

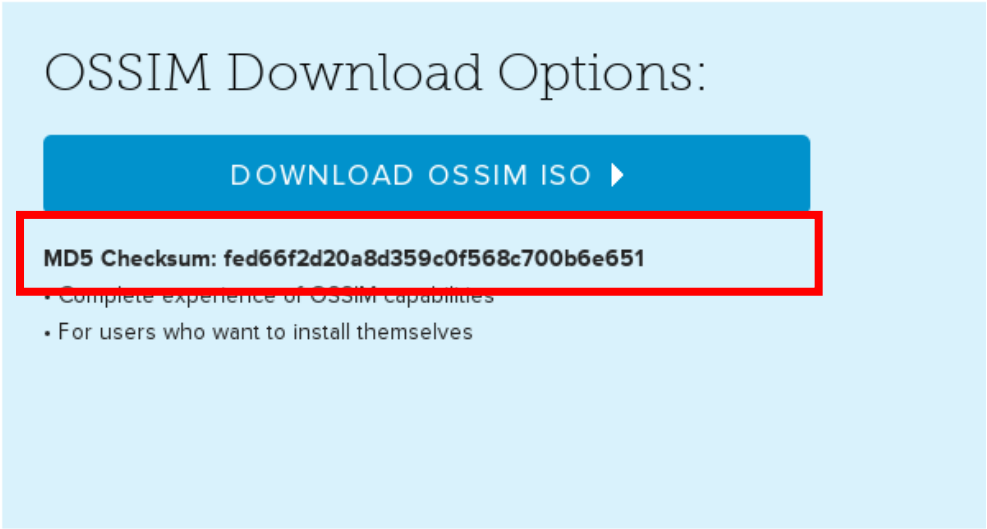
λειτουργικό σύστημα Windows μπορεί να γίνει χρήση ενός δωρεάν λογισμικού όπως το WinMD5free[2].

Η παραπάνω διαδικασία μπορεί να πραγματοποιηθεί σε ένα τερματικό Unix όπως παρουσιάζεται στην ακόλουθη εικόνα:



Εικόνα 4-5 Έλεγχος ακεραιότητας της εικόνας του OSSIM

Αντίθετα ο έλεγχος ακεραιότητας πραγματοποιείται ως εξής:



Εικόνα 4-6 MD5 Checksum για το OSSIM

Αφού ολοκληρωθεί επιτυχώς το παραπάνω βήμα, μπορεί να πραγματοποιηθεί η κύρια διαδικασία της εγκατάστασης του OSSIM.

Με την εκκίνηση του εξυπηρέτη θα πρέπει να γίνει τοποθέτηση του οπτικού μέσου που κατασκευάστηκε προηγουμένως. Μόλις εκκινήσει η ανάγνωση από το οπτικό μέσο θα πρέπει να επιλεχθεί η πρώτη εναλλακτική από το μενού "**Install Alienvault OSSIM x.xx (xx bit)**" όπου **xx** είναι η συγκεκριμένη έκδοση εγκατάστασης.

Η δεύτερη επιλογή "**Install Alienvault Sensor**" είναι χρήσιμη μόνο για τις περιπτώσεις που διατίθεται η επί πληρωμή έκδοση AlienVault USM όπου δύο ή περισσότεροι AlienVault Sensors ανταλλάσσουν δεδομένα μεταξύ τους. Στην open-source έκδοση (OSSIM) μας δίνεται η δυνατότητα να έχουμε μόνο έναν AlienVault Sensor.

Στην συνέχεια, παρέχεται η δυνατότητα επιλογής της γλώσσας, της χώρας στην οποία βρίσκεται ο εξυπηρέτης στον οποίο εγκαθίσταται το OSSIM καθώς και την διάταξη του πληκτρολογίου.

[2] http://www.winmd5.com/

Για να μην παρουσιαστούν τυχόν προβλήματα και ασυμβατότητες καλό θα είναι να γίνει επιλογή της Αγγλικής γλώσσας ως γλώσσα εγκατάστασης, γραφής και γραφικού περιβάλλοντος.

Εν συνεχεία θα πρέπει να γίνει καθορισμός της διεύθυνσης IP την οποία θα φέρει ο εξυπηρέτης. Τονίζεται ότι αυτή πρέπει να είναι στατική. Την IP αυτή θα χρησιμοποιηθεί μετά το τέλος της εγκατάστασης για να έχουμε πρόσβαση τόσο στο γραφικό περιβάλλον όσο και στο πλαίσιο εργασίας είτε μέσω τερματικού ή μέσω απομακρυσμένης πρόσβασης με ssh (Secure Shell).

Παράλληλα θα πρέπει να καθοριστούν η IP, η μάσκα υποδικτύου, η IP της πύλης (gateway) καθώς και αυτή του εξυπηρέτη DNS .

Η πύλη χρησιμοποιείται από μια δικτυακή συσκευή για να επικοινωνεί με άλλα δίκτυα τα οποία δεν ανήκουν στο broadcast domain της. Τις περισσότερες φορές είναι η IP της διεπαφής του δρομολογητή του ενδιάμεσου εξυπηρέτη (proxy server). Αν το δίκτυο είναι στεγανό (air-gap network) δεν θα υπάρχει IP για την πύλη.

Είναι επιθυμητό ο εξυπηρέτης στο οποίο θα εγκατασταθεί το OSSIM να έχει πρόσβαση στο διαδίκτυο, γιατί κάτι τέτοιο βοηθά στη διαδικασία της αναβάθμισης του εξυπηρέτη με ενημερώσεις ασφάλειας όσο και την ενημέρωση της βάσης δεδομένων με νέες υπογραφές επιθέσεων, κανόνες συσχέτισης επιθέσεων και επεκτάσεις (data source plug-ins). Για το λόγο αυτό, αν υπάρχει ανάμεσα στο διαδίκτυο και στον εξυπηρέτη μας κάποιο τοίχος ασφάλειας, θα πρέπει να το παραμετροποιήσουμε κατάλληλα ώστε να επιτρέπει την επικοινωνία αυτή.

Επόμενο βήμα είναι η εισαγωγή του κωδικού root (administrator password) του συστήματος. Στο σημείο αυτό, για την σωστή επιλογή οποιουδήποτε κωδικού που θα απαιτηθεί καλό θα να ήταν να ακολουθηθούν οι εξής αρχές: να γίνεται χρήση από κεφαλαία όσο και πεζά γράμματα αλφαβήτου, αριθμούς, και ειδικούς χαρακτήρες και συνετό είναι να μην χρησιμοποιούνται λέξεις που περιέχονται μέσα σε λεξικά. Επίσης θα πρέπει να έχει μήκος τουλάχιστον 8 χαρακτήρων ώστε να θεωρείται ασφαλής από επιθέσεις εξαντλητικών δοκιμών κωδικών (brute-force attacks).

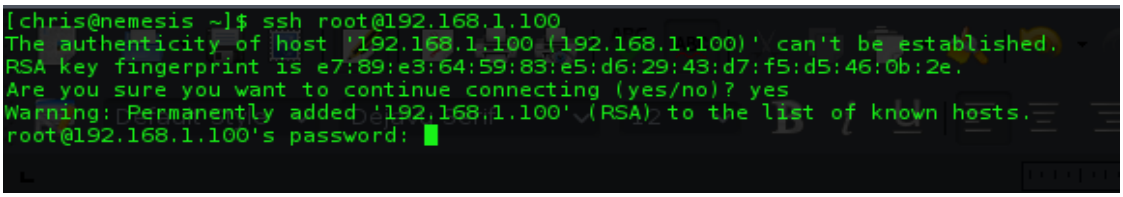
Με την ολοκλήρωση αυτής της διαδικασίας, το πρόγραμμα εγκατάστασης θα συνεχίσει την εγκατάσταση του συστήματος και των βασικών πακέτων που απαιτούνται από το OSSIM.

Εάν δεν παρουσιάσει κάποιο σφάλμα κατά τη διάρκεια της εγκατάστασης τότε θα παρέχεται η δυνατότητα για είσοδο στο διαχειριστικό περιβάλλον του OSSIM. Υπάρχουν πολλοί τρόποι για να πραγματοποιηθεί είσοδος:

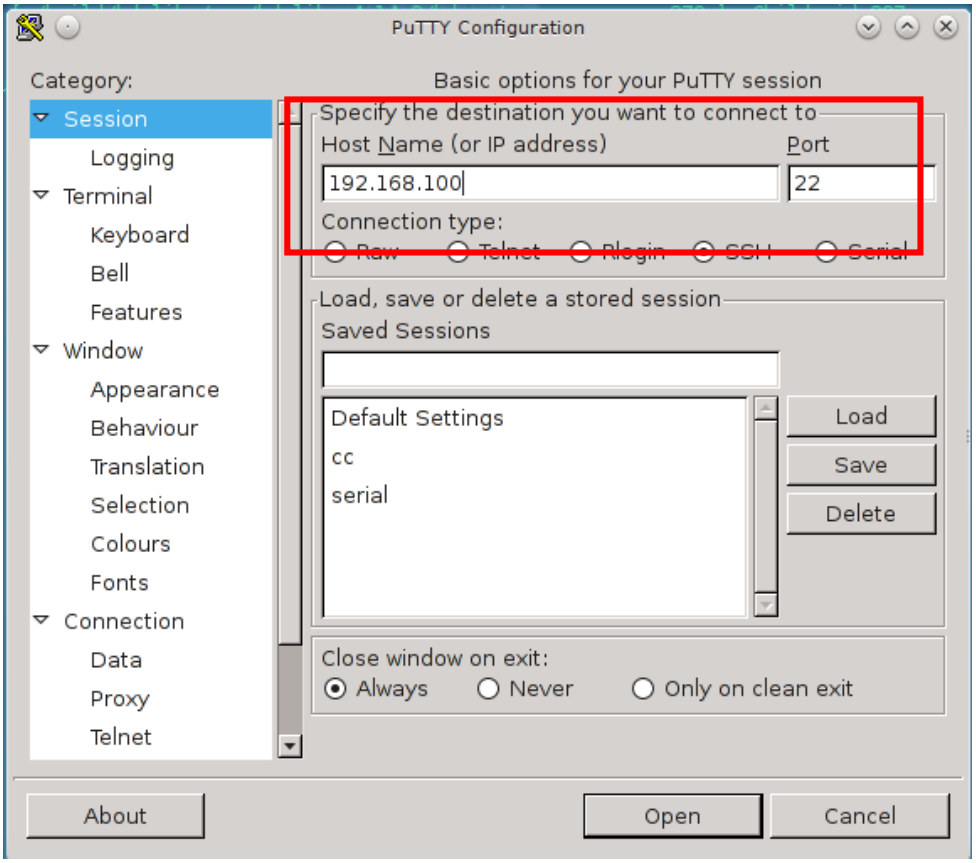
Ο πρώτος τρόπος είναι να χρησιμοποιηθεί το πλαίσιο εργασίας του OSSIM. Για κάτι τέτοιο απαιτείται φυσική πρόσβαση στο εξυπηρέτη και η διαχείριση πραγματοποιείται μέσω γραμμής εντολών.

Ο δεύτερος τρόπος είναι μέσω πρωτοκόλλου ssh, χρησιμοποιώντας το πρόγραμμα που προϋπάρχει σε λειτουργικά βασισμένα στο Unix ή (αν πρόκειται για λειτουργικά συστήματα Windows) μέσω ανάλογων προγραμμάτων όπως το Putty[3] .

Η διαδικασία σύνδεσης μέσω ssh φαίνεται στην Εικόνα 4-7. ενώ από Putty παρουσιάζεται στην Εικόνα 4-8. Τέλος η οθόνη για εισαγωγή στο σύστημα μέσω γραφικού περιβάλλοντος παρουσιάζεται στην Εικόνα 4-9.

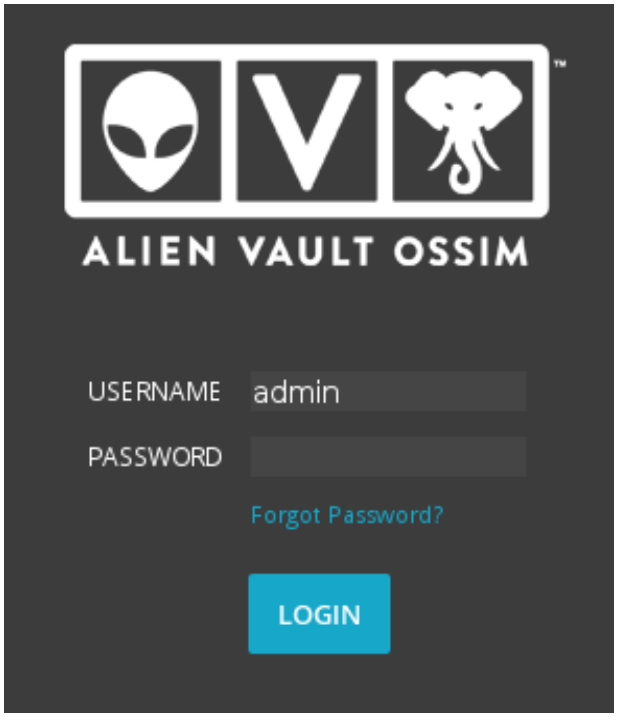


Εικόνα 4-7 Σύνδεση μέσω πρωτοκόλλου SSH



Εικόνα 4-8 Σύνδεση μέσω προγράμματος Putty

[3] http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html



Εικόνα 4-9 Σύνδεση μέσω διεπαφής Web

Την πρώτη φορά που θα πραγματοποιηθεί είσοδος στο OSSIM μέσω γραφικού περιβάλλοντος θα ζητηθεί να συμπληρωθεί μια φόρμα με τα στοιχεία του χρήστη. Μετά από αυτό το στάδιο, δίνεται η δυνατότητα να εισέλθουμε κανονικά στο γραφικό περιβάλλον της εφαρμογής χρησιμοποιώντας το όνομα χρήστη admin και τον επιλεγμένο κωδικό του διαχειριστή.

4.4.1 Καθορισμός δικτύων και αγαθών

Για την σωστή λειτουργία του OSSIM θα πρέπει να γίνει καθορισμός των δικτύων τα οποία θα παρακολουθεί (monitoring) το OSSIM καθώς και τα αγαθά (assets). Τα τελευταία περιλαμβάνουν δικτυακές συσκευές και εφαρμογές που βρίσκονται στα δίκτυα αυτά και στην ουσία είναι όλα εκείνα τα στοιχεία από τα οποία θα συγκεντρώνει καταγραφές ασφαλείας και δεδομένα το OSSIM και θα τα επεξεργάζεται. Οπότε για τη συγκεκριμένη φάση απαιτείται ιδιαίτερη προσοχή ώστε να γίνει ορθή και λεπτομερής εισαγωγή των στοιχείων αυτών ώστε να δοθεί στο OSSIM μια ολοκληρωμένη εικόνα του δικτύου για να είναι σε θέση να εξάγει σωστά αποτελέσματα.

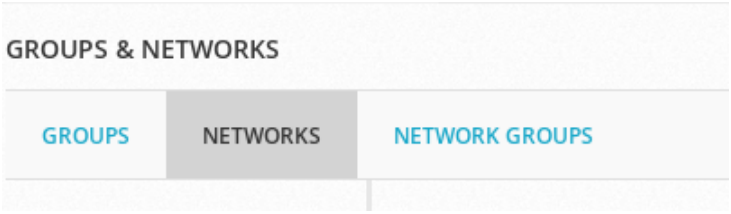
4.4.1.1 Ορισμός δικτύου

Για να εισάγουμε ένα από τα δίκτυα που θα παρακολουθούνται ακολουθείται η εξής διαδικασία:

1. Γίνεται επιλογή του "**Environment**" από το κύριο μενού.

2. Πραγματοποιείται επιλογή του "**Group & Networks**" απότο drop-down menu.

3. Γίνεται επιλογή της καρτέλας **"Networks"** όπως παρουσιάζεται στην Εικόνα 4-10.



Εικόνα 4-10 Μενού διαχείρισης δικτύων

4. Εκτελείται κλικ στο κουμπί **"Add Network"** που βρίσκεται στην δεξιά πλευρά της οθόνης. Και από το αναδυόμενο μενού γίνεται πάλι επιλογή του "**Add Network**" όπως φαίνεται στην Εικόνα 4-11.

Εικόνα 4-11 Εισαγωγή δικτύων

5. Από τη φόρμα που εμφανίζεται (παράδειγμα τέτοιας προβάλλεται στην Εικόνα 4-12) γίνεται εισαγωγή των στοιχείων που αφορούν το δίκτυο.

Εικόνα 4-12 Εισαγωγή στοιχείων δικτύου

Με μεγαλύτερη λεπτομέρεια τα σημαντικότερα πεδία που καλείται ο διαχειριστής του δικτύου να συμπληρώσει είναι τα εξής:

- **Name**: το όνομα του δικτύου.
- **CIDR:** (Classless Inter-Domain Routing): το εύρος διευθύνσεων του δικτύου (π.χ. 192.168.0.0/24).

- **Owner**: ο υπεύθυνος διαχείρισης του δικτύου.
- **Sensors**: τον sensor που θα παρακολουθεί το δίκτυο.
- **Asset Value**: την σπουδαιότητα που έχει το αγαθό αυτό σε κλίμακα από 1 έως 5. Όσο μεγαλύτερη η τιμή τόσο μεγαλύτερη είναι η σπουδαιότητα του συγκεκριμένου αγαθού.
- **External Asset**: αν το αγαθό είναι αναξιόπιστο ή ανήκει σε μη ασφαλές δίκτυο ή σε δίκτυο που δεν είναι δικής μας ευθύνης.
- **Threshold C** (Compromise Threshold Level): Η τιμή αυτή καθορίζει αν το OSSIM θα αποθηκεύει τις πληροφορίες για τα περιστατικά που λαμβάνουν χώρα στο συγκεκριμένο αγαθό.
- **Threshold A** (Attack Threshold Level): Η τιμή αυτή καθορίζει πάνω από ποιο επίπεδο το OSSIM θα αντιδράσει σε ένα περιστατικό που λαμβάνει χώρα στο συγκεκριμένο αγαθό.
- **Availability Monitoring**: Με την ενεργοποίηση αυτής της επιλογής επιτρέπουμε στο πρόγραμμα Nagios να επιβλέπει αν συγκεκριμένες υπηρεσίες που τρέχουν στο συγκεκριμένο αγαθό εκτελούνται.

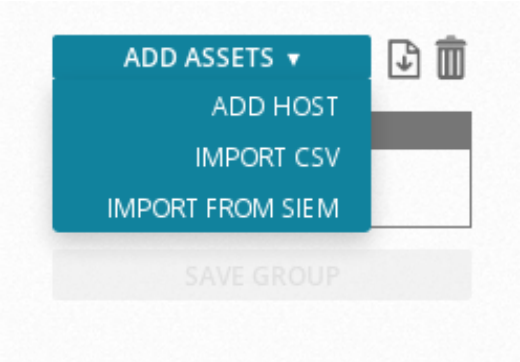
4.4.1.2 Ορισμός Αγαθών

Για να εισάγουμε ένα από τα αγαθά που θα βρίσκεται υπό την εποπτία του συστήματος ακολουθείται η εξής διαδικασία:

1. Γίνεται επιλογή του "**Environment"** από το κύριο μενού.

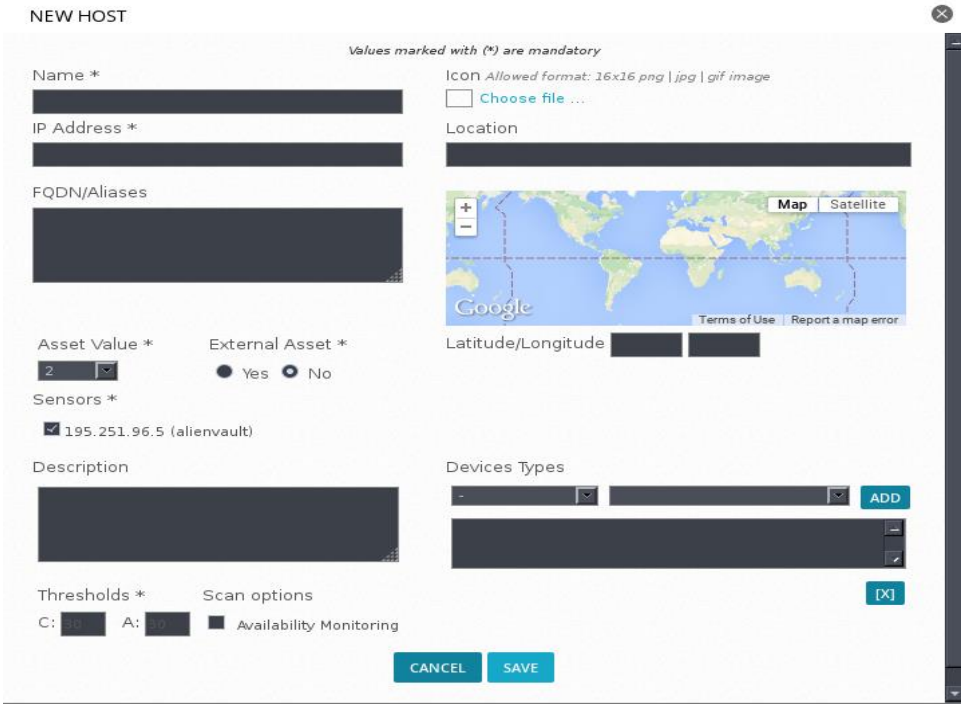
2. Γίνεται επιλογή του "**Assets**" από το drop-down menu.

3. Εκτελείται κλικ στο κουμπί "**Add Assets**" και από το αναδυόμενο μενού γίνεται επιλογή του "**Add host".**



Εικόνα 4-13 Εισαγωγή αγαθών

4. Πραγματοποιείται συμπλήρωση των απαραίτητων στοιχείων για το κάθε αγαθό.



Εικόνα 4-14 Εισαγωγή στοιχείων για κάθε αγαθό

Τα σημαντικότερα πεδία που καλείται ο διαχειριστής του δικτύου να συμπληρώσει είναι τα εξής:

- **Name**: το όνομα του αγαθού
- **IP Address**: την IP του αγαθού
- **FQDN/Aliases**: το πλήρες όνομα του αγαθού (π.χ ermis.domain.gr)
- **Asset Value**: την σπουδαιότητα που έχει για εμάς το αγαθού αυτό σε κλίμακα από 1 έως 5. Όσο μεγαλύτερη η τιμή τόσο μεγαλύτερη είναι η σπουδαιότητα του συγκεκριμένου αγαθού.
- **External Asset**: αν το αγαθό είναι αναξιόπιστο ή σε μη ασφαλές δίκτυο ή δίκτυο που δεν είναι δικής μας ευθύνης.
- **Threshold C** (Compromise Threshold Level): Η τιμή αυτή καθορίζει αν το OSSIM θα αποθηκεύει τις πληροφορίες για τα event που λαμβάνουν χώρα στο συγκεκριμένο αγαθό.
- **Threshold A** (Attack Threshold Level): Η τιμή αυτή καθορίζει πάνω από ποιο επίπεδο το OSSIM θα αντιδράσει σε ένα περιστατικό που λαμβάνει χώρα στο συγκεκριμένο αγαθό.
- **Availability Monitoring**: Με την ενεργοποίηση αυτής της επιλογής επιτρέπουμε στο πρόγραμμα Nagios να επιβλέπει αν συγκεκριμένες υπηρεσίες που τρέχουν στο συγκεκριμένο αγαθό είναι λειτουργικές.
- **DevicesType**: τι τύπος αγαθού είναι, δηλαδή τις υπηρεσίες που προσφέρει (π.χ DNS εξυπηρέτης)

4.4.2 Προσθήκη πράκτορα OSSEC στο OSSIM

Το OSSIM για την παρακολούθηση των εξυπηρετών του δικτύου του, συνεργάζεται με το ανοικτό λογισμικό OSSEC. Στην πραγματικότητα μαζί με τον εξυπηρέτη του OSSIM τρέχει παράλληλα και ένας εξυπηρέτης του OSSEC ο οποίος είναι υπεύθυνος για την συλλογή των καταγραφών ασφαλείας από τους πράκτορες OSSEC οι οποίοι τρέχουν στους εξυπηρέτες του δικτύου.

Για την διαχείριση των πρακτόρων OSSEC από το γραφικό περιβάλλον του OSSIM πρέπει να γίνει πλοήγηση στο "**Environment**" → "**Detection**" όπου παρουσιάζεται μια συνοπτική μορφή των πρακτόρων OSSEC που είναι εγκατεστημένοι στο σύστημα μας καθώς και πληροφορίες σχετικές με το αν είναι ενεργοί την δεδομένη χρονική στιγμή καθώς και την διεύθυνση IP τους.

Η προσθήκη ή η διαγραφή ενός πράκτορα OSSEC, μπορεί να πραγματοποιηθεί μέσω της καρτέλας "**Agents**".

Επιπλέον μας δίνει τις δυνατότητες στον OSSEC Agent για:

- Επανεκκίνηση.
- Έλεγχο ακεραιότητας.
- Έλεγχο rootkit.
- Εξαγωγή του κλειδιού αυθεντικοποίησης που απαιτείται για την αρχική επικοινωνία με τον OSSEC Server.
- Εξαγωγή ενός εκτελέσιμου αρχείου που θα εγκαταστήσει τον OSSEC Agent με κάποιες προκαθορισμένες ρυθμίσεις ώστε να είναι άμεσα λειτουργικός.

Για την προσθήκη ενός OSSEC Agent πρέπει να ακολουθηθεί η παρακάτω βηματική διαδικασία:

1. Εκτελείται κλικ στο κουμπί "**Add Agent**".
2. Συμπλήρωση του πεδίου "**Agent Name**", όπου μπορεί να καθοριστεί η ονομασία που θα έχει ο συγκεκριμένος πράκτορας και θα πρέπει να είναι ένα μοναδικό και χαρακτηριστικό όνομα.
3. Συμπλήρωση του πεδίου "**IP/CIDR**", με την διεύθυνση IP του συγκεκριμένου υπολογιστή ή στην περίπτωση που η διεύθυνση του υπολογιστή είναι δυναμική (δηλαδή έχει ληφθεί μέσω πρωτοκόλλου DHCP) τότε ορίζεται στο πεδίο αυτό το δίκτυο στο οποίο ανήκει ο συγκεκριμένος υπολογιστής (π.χ. 192.168.0.1/24).

4.4.3 Πολιτικές & Αντιδράσεις

Τα συστήματα SIEM είναι σχεδιασμένα να συγκεντρώνουν μεγάλο όγκο πληροφορίας από τις συσκευές που παρακολουθούν, κάτι το οποίο αναπόφευκτα οδηγεί σε κορεσμό πληροφορίας και εν τέλει καθιστά την παρακολούθηση του συστήματος μη διαχειρίσιμη.

Οι πολιτικές (policies) χρησιμοποιούνται στο OSSIM σαν φίλτρα στις καταγραφές ασφαλείας και έχουν ως στόχο να:

- κάνουν το SIEM ευκολότερα διαχειρίσιμο.

- μειώσουν την εμφάνιση άχρηστων πληροφοριών (noise).

- εξοικονομήσουν πόρους από το σύστημα αφού θα μειώσουν τον όγκο των δεδομένων που θα πρέπει να επεξεργαστούν.

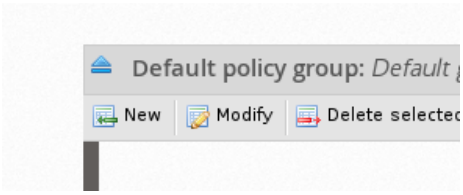
4.4.3.1 Κατασκευή πολιτικών

Μια πολιτική για να αναγνωρίσει την πληροφορία που θα διαχειριστεί στηρίζεται σε κάποιες παραμέτρους. Οι παράμετροι αυτοί ορίζονται με την παρακάτω διαδικασία.

1. Γίνεται πλοήγηση στο **Configuration → Threat Intelligence**.

2. Γίνεται επιλογή της καρτέλας **Policy**.

3. Εκτελείται κλικ στο κουμπί **New** όπως παρουσιάζεται στην Εικόνα 4-15.



Εικόνα 4-15 Δημιουργία νέας πολιτικής

4. Στο **Policy Conditions** πρέπει να συμπληρωθούν με τα πεδία **Source**, **Destination**, **Source Ports, Destination Ports** με τις κατάλληλες πληροφορίες.

5. Στην καρτέλα **Event Type** μπορεί να επιλεγεί ανάλογα με το επιθυμητό γεγονός (event) μια από τις εναλλακτικές **"Data Source Group"** (DS Group) ή "**Taxonomy**", όπως φαίνεται στην Εικόνα 4-16.

Εικόνα 4-16 Επιλογή τύπου συμβάντων για μια πολιτική

4.4.3.2 Κατασκευή αντιδράσεων

Αφού κατασκευαστεί επιτυχώς μια πολιτική μπορεί να πραγματοποιηθεί η σύνδεση της με μια αντίδραση (action). Μια αντίδραση για το OSSIM είναι μια αυτοματοποιημένη διαδικασία που εκτελείται όταν εκπληρώνονται οι προϋποθέσεις μιας πολιτικής.

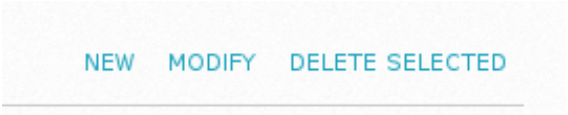
Για την κατασκευή μιας αντίδρασης:

1. Γίνεται πλοήγηση στο **Configuration → Threat Intelligence**.

2. Πραγματοποιείται επιλογή της καρτέλας **Action**, όπως φαίνεται στην Εικόνα 4-17.

Εικόνα 4-17 Μενού δημιουργίας νέας αντίδρασης

3. Εκτελείται κλικ στο κουμπί **New**.



Εικόνα 4-18 Δημιουργία νέας αντίδρασης

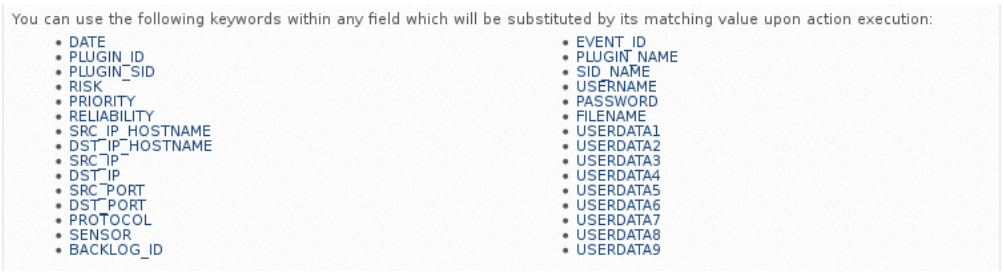
4. Στη συνέχεια συμπληρώνονται τα πεδία **Name** και **Description**, όπως παρουσιάζεται στην Εικόνα 4-19.

Εικόνα 4-19 Εισαγωγή στοιχείων κατά τον ορισμό νέας αντίδρασης

5. Στο πεδίο **Type** επιλέγεται το είδος της ενέργειας που θα πραγματοποιεί η συγκεκριμένη αντίδραση, όπως παρουσιάζεται στην Εικόνα 4-20.

Εικόνα 4-20 Εισαγωγή τύπου ενεργείας της αντίδρασης

Μια αντίδραση μπορεί να σημάνει συναγερμό, να στείλει ηλεκτρονική αλληλογραφία ή να εκτελέσει εντολές στο τερματικό. Στο OSSIM πάντα μια καθορισμένη αντίδραση πρέπει να συνδέεται με μια υπάρχουσα πολιτική. Το OSSIM μας δίνει την δυνατότητα να χρησιμοποιήσουμε μεταβλητές από το συμβάν και να τις περάσουμε ως ορίσματα, σε μια εντολή τερματικού ή στο email που θα σταλεί αυτόματα. Οι μεταβλητές που αφορούν το πεδίο **Name** παρουσιάζονται στην Εικόνα 4-21.



Εικόνα 4-21 Μεταβλητές που αναφέρονται στο πεδίο Name

4.4.4 Ενεργοποίηση/Απενεργοποίηση DS Plug-ins

4.4.4.1 Μέσω γραφικού περιβάλλοντος

Εκτελείται πλοήγηση στο **Configuration → Deployment.**

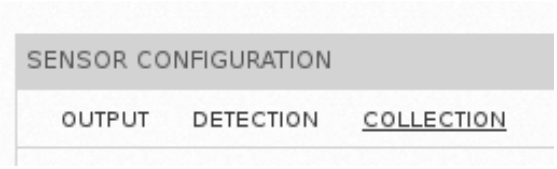
Γίνεται επιλογή της καρτέλας AlienVault Center .

Επιλέγουμε στο server τον οποίο θα διαχειριστούμε το κουμπί "**System Details**" το οποίο φέρει το σύμβολο .

Γίνεται επιλογή της καρτέλας **Sensor Configuration**.

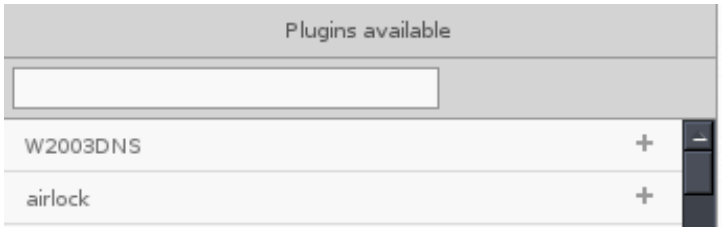
Εικόνα 4-22 Μενού επιλογής ρυθμίσεων του εξυπηρέτη OSSIM

Γίνεται επιλογή της καρτέλας **Collection** από τις εναλλακτικές που εμφανίζονται **Sensor Configuration**.

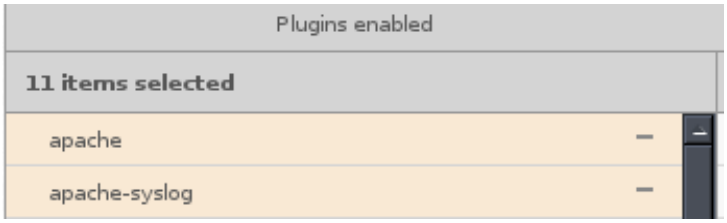


Εικόνα 4-23 Μενού ρυθμίσεων αισθητήρα OSSIM

Για την ενεργοποίηση ενός DS Plug-in εκτελείται κλικ στο κουμπί με το σύμβολο **+** από τα **Plugins Available** όπως παρουσιάζεται στην εικόνα 2.23. Αντίθετα, για την απενεργοποίηση εκτελείται κλικ στο κουμπί με το σύμβολο **-** από τα **Plugins Enabled**, όπως παρουσιάζεται στην Εικόνα 4-24.



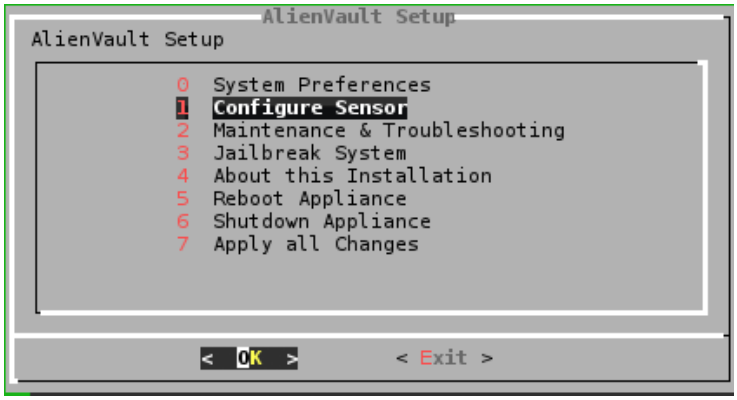
Εικόνα 4-24 Ενεργοποιήση επεκτάσεων



Εικόνα 4-25 Ενεργοποιημένες επεκτάσεις

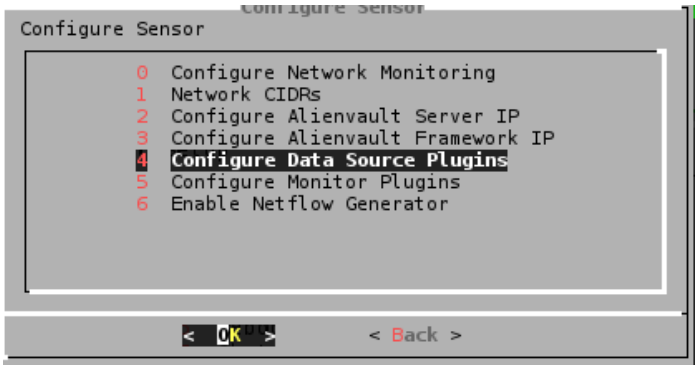
4.4.4.2 Μέσω τερματικού (διάλογοι)

1. Πραγματοποιείται σύνδεση στο τερματικό και γίνεται επιλογή του **Configure Sensor**.



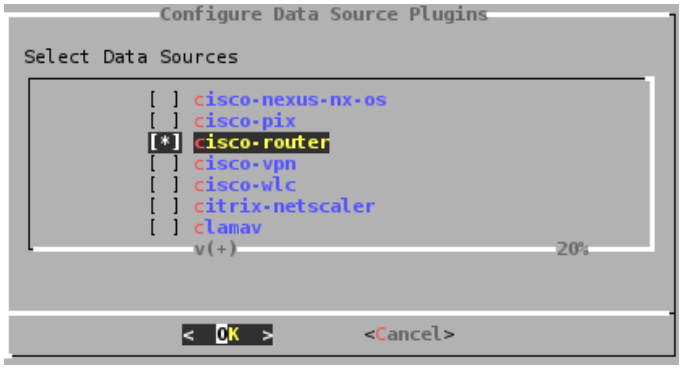
Εικόνα 4-26 Μενού τερματικού

2. Επιλέγεται το **Configure Data Source Plugins**.



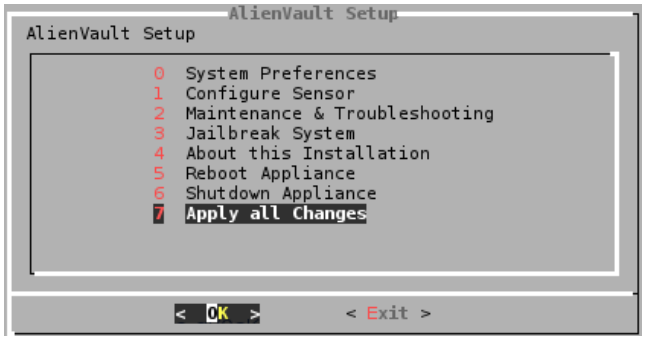
Εικόνα 4-27 Μενού ενεργοποίησης επεκτάσεων

3. Επιλέγονται τα DS Plug-ins προς ενεργοποιήση πατώντας το πλήκτρο διαστήματος. Αυτά τα οποία είναι ενεργοποιημένα εμφανίζονται με τη σήμανση **[*]** ενώ τα ανενεργά ως **[ ]**.



Εικόνα 4-28 Επιλογή επεκτάσεων για ενεργοποίηση

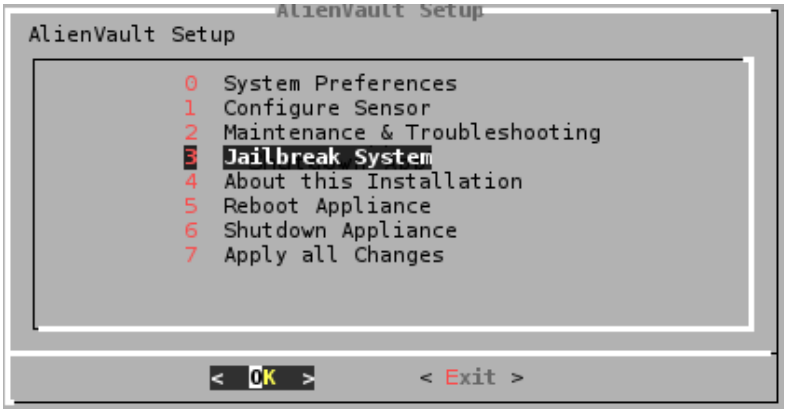
4. Αφού ολοκληρωθεί η εκτέλεση του συγκεκριμένου βήματος γίνεται μετάβαση στο αρχικό μενού και επιλογή του **Apply all Changes.** Τέλος εκτελείται κλικ στο κουμπί **OK** ώστε να επικυρωθούν οι αλλαγές που εμφανίζονται, όπως παρουσιάζεται στην Εικόνα 4-28.



Εικόνα 4-29 Εφαρμογή όλων των αλλαγών

4.4.4.3 Μέσω τερματικού (γραμμή εντολών)

1. Αρχικά επιλέγεται **Jailbreak System** για να αποκτήσουμε πρόσβαση στην γραμμή εντολών.



Εικόνα 4-30 Πρόσβαση στο τερματικό του εξυπηρέτη

2. Γίνεται πλοήγηση στον φάκελο **/etc/ossim/agent**.

3. Κάνοντας χρήση ενός επεξεργαστή κειμένου (π.χ. vim,nano) γίνεται επεξεργασία του αρχείου config.cfg. Πιο συγκεκριμένα στο σημείο **[plugins]**, προστίθεται το όνομα και η διαδρομή του αρχείου επέκτασης (plugin path) στο δίσκο. Με αυτό τον τρόπο η συγκεκριμένη επέκταση ενεργοποιείται. Εναλλακτικά, αν θέλουμε να απενεργοποιηθεί μια ήδη υπάρχουσα επέκταση, αφαιρείται η αντίστοιχη γραμμή από το αρχείο.

```
[plugins]
apache=/etc/ossim/agent/plugins/apache.cfg
apache-syslog=/etc/ossim/agent/plugins/apache-syslog.cfg
cisco-router=/etc/ossim/agent/plugins/cisco-router.cfg
nmap-monitor=/etc/ossim/agent/plugins/nmap-monitor.cfg
ntop-monitor=/etc/ossim/agent/plugins/ntop-monitor.cfg
ossec-single-line=/etc/ossim/agent/plugins/ossec-single-line.cfg
ossim-monitor=/etc/ossim/agent/plugins/ossim-monitor.cfg
pam_unix=/etc/ossim/agent/plugins/pam_unix.cfg
prads_eth0=/etc/ossim/agent/plugins/prads_eth0.cfg
remote_suricata=/etc/ossim/agent/plugins/remote_suricata.cfg
snort_syslog=/etc/ossim/agent/plugins/snort_syslog.cfg
ssh=/etc/ossim/agent/plugins/ssh.cfg
sudo=/etc/ossim/agent/plugins/sudo.cfg
suricata=/etc/ossim/agent/plugins/suricata.cfg
```

Εικόνα 4-31 Εμφάνιση ενεργοποιημένων επεκτάσεων

4. Για να εφαρμοστούν οι αλλαγές εκτελείται η ακόλουθη εντολή:

```
# service ossim-server restart && service ossim-agent restart
```

Εναλλακτικά εκτελείται η εντολή:

```
# alienvault-reconfig
```

4.4.5 Κατασκευή νέων επεκτάσεων (DS Plug-in)

Οι δύο κύριοι λόγοι οι οποίοι απαιτούν την κατασκευή μιας νέας επέκτασης: α) σε μια δικτυακή υποδομή υπάρχει συσκευή η οποία παράγει καταγραφές ασφαλείας οι οποίες έχουν δομή που δεν μπορεί να αναγνωρίσει το OSSIM, β) γιατί θέλουμε να προσθέσουμε μια εξωτερική πηγή η οποία στέλνει καταγραφές ασφαλείας και είναι επιθυμητό αυτά να βρίσκονται απομονωμένα από τις υπόλοιπες καταγραφές ασφαλείας. Το τελευταίο είναι μια καλή στρατηγική για την παραμετροποίηση μιας υπάρχουσας επέκτασης αν δεν επιθυμείται η διαγραφή της ή αν επιθυμείται η αλλαγή των όσων λάβει χώρα κατά την αναβάθμιση του συστήματος.

Στη συνέχεια θα δημιουργηθεί μια επέκταση για το IDPS Suricata η οποία θα δέχεται καταγραφές ασφαλείας από ένα IDPS Suricata εγκατεστημένο σε έναν άλλο εξυπηρέτη. Θα βασιστούμε στη δομή μιας ήδη υπάρχουσας επέκτασης.

1. Αρχικά γίνεται πλοήγηση στη διαδρομή **/etc/ossim/agent/plugins**.

2. Πραγματοποιείται αντιγραφή του snort_syslog.cfg με την εντολή:

```
#cp snort_syslog.cfg remote_suricata.cfg
```

Στο σημείο αυτό να τονιστεί ότι θα πρέπει να γίνει χρήση της επέκτασης του snort_syslog και όχι του ήδη υπάρχωντος suricata.cfg, γιατί οι καταγραφές ασφαλείας που θα λαμβάνονται είναι σε μορφή snort (fast.log) και όχι σε μορφή unified2.

3. Δημιουργείται ένας φάκελος στον οποίο θα αποθηκεύονται οι καταγραφές ασφαλείας από το εργαλείο Suricata που είναι εγκατεστημένο στον απομακρυσμένο εξ υπηρέτη και δημιουργείται μέσα σε αυτό ένα αρχείο στο οποίο θα αποθηκεύονται οι καταγραφές ασφαλείας.

```
# mkdir /var/log/suricata_remote
# touch /var/log/suricata_remote/fast.log
```

4. Γίνεται παραμετροποίηση του remote_suricata.cfg. Να σημειωθεί ότι το plugin_id πρέπει να είναι από 9000 έως 10000 για τα custom plugins. Ένα τέτοιο παράδειγμα είναι και το ακόλουθο:

```
[DEFAULT]
plugin_id=9001

[config]
type=detector
enable =yes

process=snort
start=no; launch plugin process when agent starts
stop=no; shutdown plugin process when agent stops
startup=/etc/init.d/%(process)s start
shutdown=/etc/init.d/%(process)s stop

source=log
location=/var/log/suricata_remote/fast.log

create_file=false

[translation]
PROTO255=139 # 139 is "OTHER" protocol in OSSIM language
```

5. Στο τέλος του αρχείο remote_suricata.cfg προστίθεται το regular expression μέσω του οποίου επιτυγχάνεται η κανονικοποίηση των καταγραφών ασφαλείας:

```
[022_snort-ossim-format-from-file]
event_type=event
regexp=^(\d+/\d+(?:/?\d\d)?-\d\d:\d\d:\d\d).*?\[(\d+):(\d+):\d+\]
<(\[reading from
afile\])>.*?{(\w+)}\s+([\d\.]+):?(\d+)?\s+..\s+([\d\.]+):?(\d+)?\s+\[(\d+):(
\d+)\]$
date={normalize_date($1)}
plugin_id={snort_id($2)}
plugin_sid={$3}
protocol={translate($5)}
src_ip={$6}
src_port={$7}
dst_ip={$8}
dst_port={$9}
snort_sid={$10}
snort_cid={$11}
```

```
[023_snort-ossim--format-from-pfsense]
event_type=event
regexp=^(?P<date>\w{3}\s+\d{1,2}\s\d\d:\d\d:\d\d)\s+(?P<hostname>[\d.]{7,15}
)\s(?P<sensor>\w+\[\d+\]):\s+\[(?P<pid>\d+):(?P<sid>\d+):\d\]\s*(?P<msg>.+)\
s*\[Classification:.+\]\s*\[Priority:.+\]\s*\{(?P<proto>.+)\}\s*(?P<src_ip>[
\d.]{7,15}):(?P<src_port>\d+)\s*-
>\s*(?P<dst_ip>[\d.]{7,15}):(?P<dst_port>\d+)$
date={normalize_date($date)}
plugin_id={snort_id($pid)}
plugin_sid={$sid}
protocol={$proto}
src_ip={$src_ip}
src_port={$src_port}
dst_ip={$dst_ip}
dst_port={$dst_port}
```

6. Το επόμενο βήμα είναι να εισαχθούν τα δεδομένα στη βάση. Με αυτά θα εκτελείται σύγκριση των κανονικοποιημένων δεδομένων ώστε να ανιχνεύεται αν κάποιο γνωστό περιστατικό λαμβάνει χώρα. Να σημειωθεί ότι ο κωδικός για την SQL database του OSSIM είναι βρίσκεται αποθηκευμένος στο αρχείο **/etc/ossim/server/config.xml**

Οι εντολές που θα χρησιμοποιηθούν στο παράδειγμα εκτελούν αντιγραφή των εγγραφών που υπάρχουν ήδη αλλά με διαφορετικό id.

```
CREATE TEMPORARY TABLE tmp SELECT * FROM plugin WHERE id = 1001;

UPDATE tmp SET id=9001 WHERE id = 1001;

INSERT INTO plugin SELECT * FROM tmp WHERE id = 9001;



DELETE FROM plugin WHERE id = "9001";
DELETE FROM plugin_sid where plugin_id = "9001";

INSERT IGNORE INTO plugin (id, type, name, description) VALUES (9001, 1,
'remote suricata', 'custom plugin for remote suricata');
```

Στην περίπτωση που είναι επιθυμητό να δημιουργηθεί μια επέκταση εξολοκλήρου από την αρχή, εκτός από το αρχείο θα πρέπει να εισαχθούν και τα ξεχωριστά περιστατικά τα οποία μπορεί να λάβουν χώρα. Αυτό μπορεί να επιτευχθεί με την εισαγωγή του στοιχείου **[translation]** μέσα στο αρχείο ρυθμίσεων, ώστε να συνδεθεί το περιστατικό με μία sid, όπως φαίνεται παρακάτω:

```
[translation]
HELO=1
MAIL=2
RCPT=3
DATA=4
QUIT=5
xxxx=6
_DEFAULT_=9999
```

Στο regular expression στο σημείο που περιγράφεται στην καταγραφή ασφάλειας το περιστατικό:

```
(?P<type>\w+)
```

Στο σημείο μου ορίζεται πως θα γίνει η κανονικοποίηση:

```
plugin_sid={translate($type)}
```

Στην SQL:

```
INSERT INTO plugin_sid (plugin_id, sid, category_id, class_id, name,
priority, reliability) VALUES (9001, 1, NULL, NULL, 'exchangews: HELO' ,3,
2);
```

4.4.6 Ενεργοποίηση Syslog

Στην ενότητα αυτή περιγράφεται δυνατότητα ενεργοποίησης αποστολής καταγραφών ασφαλείας από τους εξυπηρέτες που παρακολουθεί το OSSIM χωρίς την εγκατάσταση OSSEC πρακτόρων.

Αν στον εξυπηρέτη που παρακολουθείται υπάρχει πρόγραμμα που παράγει καταγραφές ασφαλείας και έχει την δυνατότητα να τους προσθέτει και ένα αναγνωριστικό τότε μπορεί απλά να προστεθεί στο αρχείο **/etc/rsyslog.conf** μια εγγραφή της μορφής:

```
local5.*@192.168.1.10 για αποστολή μέσω UDP
local5.*@@192.168.1.10 για αποστολή μέσω TCP
```

Στην περίπτωση που το λειτουργικό απαιτεί κατασκευή ξεχωριστού αρχείου ρυθμίσεων μπορεί να δημιουργηθεί ένα μέσα στον φάκελο **/etc/rsyslog.d** με όνομα αρχείου για παράδειγμα 60-to-ossim.conf και το οποίο να περιέχει εγγραφές της μορφής:

```
local5.*@192.168.1.10
```

Επιπροσθέτως, δίνεται η δυνατότητα να προωθηθεί ένα συγκεκριμένο αρχείο καταγραφής ασφαλείας και να αποστέλλεται αυτόματα οποιαδήποτε αλλαγή αφορά αυτό το αρχείο σε έναν απομακρυσμένο rsyslog εξυπηρέτη. Στην προκειμένη περίπτωση αυτός είναι το OSSIM. Για να επιτευχθεί αυτό θα πρέπει να εισαχθούν μέσα στο **/etc/rsyslog.conf** οι παρακάτω εγγραφές:

```
# send http.log to local5 -> alienvault

$ModLoadimfile
$InputFileName /var/log/suricata/http.log #τοόνομα του αρχείου
$InputFileTaghttplog
$InputFileStateFile http.log
$InputFileSeverity alert
$InputFileFacility local5
$InputRunFileMonitor
local6.*@<ip-remote-syslog-server>
```

Εάν διατίθεται μια συσκευή με λειτουργικό τύπου Cisco IOS ή παρόμοιο, τότε η δυνατότητα αποστολής καταγραφών ασφαλείας υποστηρίζεται εγγενώς. Για τέτοιου είδους συσκευές αρκεί να εκτελεστούν οι παρακάτω εντολές ώστε να ενεργοποιηθεί η δυνατότητα αυτή:

```
#configure terminal
#logging 192.168.1.10 (την ip του απομακρυσμένου syslog server)
#logging trap 3 (για level error και πάνω)
#logging facility local5
#end
```

Τέλος, θα πρέπει να ελεγχθούν οι ρυθμίσεις και από την μεριά του OSSIM ώστε να δέχεται καταγραφές ασφαλείας από απομακρυσμένους πελάτες.

Ελέγχονται οι ρυθμίσεις στο αρχείου **/etc/rsyslog.conf**

```
$ModLoadimudp
$UDPServerRun 514
```

και προσθέτουμε τις γραμμές αν θέλουμε να αποθηκεύονται τα logs που έρχονται με facility local5.* στον φάκελο /var/log/suricata_remote/fast.log

```
local5.*                        -/var/log/suricata_remote/fast.log
```

Τονίζεται ότι θα πρέπει να ενεργοποιήσουμε και τα απαραίτητα DS Plugins ώστε να μπορεί το OSSIM να κάνει normalization στα logs που δεχόμαστε.

Κεφάλαιο 5 **Εισαγωγή στη Λειτουργία του OSSEC**

5.1 Εισαγωγή

Σκοπός αυτού του κεφαλαίου είναι να παρέχει μια γρήγορη και περιεκτική εικόνα του εργαλείου OSSEC καθώς και τα βασικά μέρη από τα οποία αποτελείται. Ταυτόχρονα, επιχειρείται να αποδοθεί ένας οδηγός ορθής εγκατάστασης και ορθής παραμετροποίησης, ώστε ο ενδιαφερόμενος να είναι σε θέση να αντιληφθεί όσο πιο έγκαιρα γίνεται τις δικτυακές επιθέσεις που μπορεί να λάβουν χώρα στα υπό την εποπτεία δίκτυα. Για πιο λεπτομερείς περιγραφές ο αναγνώστης παρπέμπεται στο [8].

5.2 Τι είναι το OSSEC

Το OSSEC είναι ένα ανοιχτού κώδικα πρόγραμμα το οποίο έχει την δυνατότητα να λειτουργεί ως HIDS(Host-based Intrusion Detection System), SIM/SEM καθώς και παρακολούθηση καταγραφών ασφαλείας. Το αρκτικόλεξο OSSEC προέρχεται από την συντομογραφία των λέξεων Open Source Security. Με τον όρο HIDS εννοούμε προγράμματα ανίχνευσης εισβολών (IDS) τα οποία είναι κατανεμημένα σε όλες τις συσκευές που αλληλοεπιδρούν σε ένα δίκτυο (για περισσότερες λεπτομέρειες ο αναγνώστης παραπέμπεται στο Κεφάλαιο 2). Μπορεί να τρέχει σε διάφορες αρχιτεκτονικές επεξεργαστών και είναι γραμμένο για τα πιο δημοφιλή λειτουργικά συστήματα όπως Windows, Linux, BSD, AIX, Solaris, Mac OS X.

5.2.1 Δυνατότητες του OSSEC

Οι βασικότερες δυνατότητες του OSSEC είναι:

- **Ακεραιότητα στα σύστημα αρχείων** (File Integrity). Το OSSEC πραγματοποιεί σε συγκεκριμένα χρονικά διαστήματα παρακολούθηση για μη ηθελημένη τροποποίηση αρχείων και ρυθμίσεων του συστήματος.

- **Παρακολούθηση καταγραφών ασφαλείας** (Log Monitoring). Διαθέτει ειδικές διεργασίες (daemons) οι οποίες παρακολουθούν σε συνεχή βάση την προσθήκη καταγραφών ασφαλείας (logs) και ύστερα τις προωθούν για επεξεργασία στους OSSEC Servers.

- **Ανίχνευση Rootkits** . Διαθέτει διαδικασίες οι οποίες ανά συγκεκριμένα χρονικά διαστήματα ελέγχουν το σύστημα για την ύπαρξη κακόβουλων προγραμμάτων που επιτρέπουν την μη εξουσιοδοτημένη πρόσβαση στο σύστημα.

- **Άμεση αντίδραση σε περίπτωση ανίχνευσης περιστατικού** (Active-Response). Σε περίπτωση ανίχνευσης κακόβουλής ενέργειας το OSSEC μπορεί να αντιδράσει αυτόματα βάση προγραμματισμένων ενεργειών για να αποτρέψει την πιθανή εισβολή ή αν έχει ήδη επιτευχθεί, η μη

εξουσιοδοτημένη πρόσβαση, να την σταματήσει αποτρέποντας περεταίρω εξάπλωση του προβλήματος.

5.2.2 Αρχιτεκτονική του OSSEC

Το OSSEC λειτουργεί βασιζόμενο δενδροειδή διάταξη. Στην κορυφή της δομής αυτής βρίσκεται ο κεντρικός εξυπηρέτης του OSSEC ο οποίος επεξεργάζεται τα δεδομένα, διαχειρίζεται τις ρυθμίσεις λειτουργίας, ενώ ταυτόχρονα αναλύει και εξάγει τα αποτελέσματα.

Το OSSEC έχει την δυνατότητα να λειτουργήσει σε 4 κύριες μορφές:

5.2.2.1 Λειτουργία Εξυπηρετητή (Server Mode)

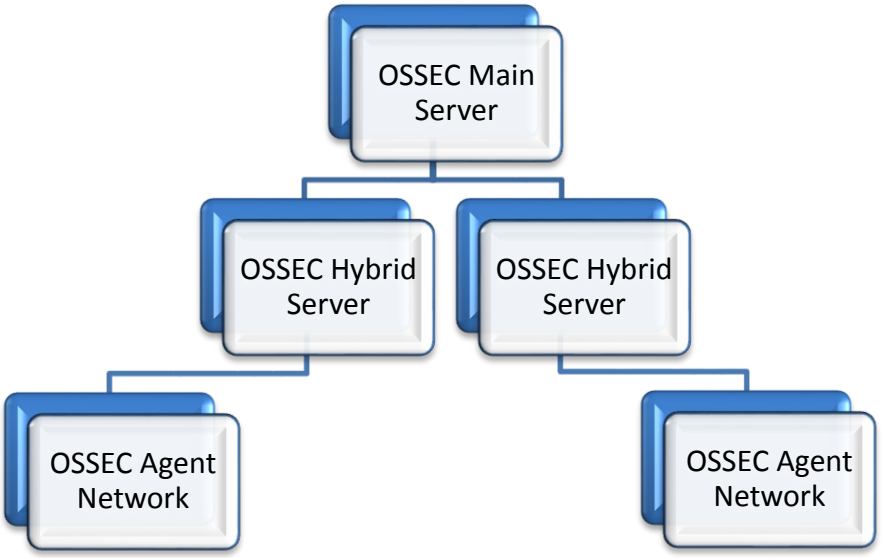
Αυτή η διάταξη λειτουργίας του OSSEC χρησιμοποιείται στην κορυφή της αρχιτεκτονικής της δομής παρακολούθησης. Σκοπός της είναι να συγκεντρώνει όλες τις καταγραφές ασφαλείας από τους πράκτορες που παρακολουθεί, να επεξεργάζεται τα αντίστοιχα δεδομένα, και να εξάγει αποτελέσματα. Επιπλέον διατηρεί αποθηκευμένα α) τα αποτελέσματα από τους ελέγχους ακεραιότητας του συστήματος αρχείων (file integrity checks) που έχουν πραγματοποιηθεί από τους πράκτορες, β) όλους του κανόνες ανίχνευσης επιθέσεων, γ) τα αρχεία ρυθμίσεων και δ) ότι άλλο απαιτείται για την παρακολούθηση του δικτύου και εξαγωγή αποτελεσμάτων.

5.2.2.2 Λειτουργία Πράκτορα (Agent Mode)

Είναι η δεύτερη κύρια διάταξη του OSSEC. Εγκαθίσταται στις συσκευές τις οποίες επιθυμούμε να παρακολουθούμε. Αυτή, έχει ως σκοπό να συγκεντρώνει και να προωθεί τις καταγραφές ασφαλείας του λειτουργικού, οι οποίες έχουν καθοριστεί μέσω του αρχείου ρυθμίσεων του OSSEC. Σε αυτή τη διάταξη, καταναλώνει σχεδόν μηδενικούς πόρους αφού δεν πραγματοποιεί καμία επεξεργασία. Επίσης είναι εγκατεστημένος σε ένα απομονωμένο περιβάλλον σε σχέση με το λειτουργικό (chroot jail) και για την λειτουργία του χρησιμοποιεί ξεχωριστό χρήστη(system user) με περιορισμένα δικαιώματα.

5.2.2.3 Υβριδική Λειτουργία (Hybrid Mode)

Η συγκεκριμένη διάταξη λειτουργίας είναι ένας συνδυασμός εξύπηρέτη και πράκτορα. Είναι σχετικά μια καινούργια μορφή που εμφανίστηκε στις τελευταίες εκδόσεις του OSSEC και σκοπεύει στο να απλοποιήσει τη διαχείριση για τις περιπτώσεις που υπάρχει ένας μεγάλος αριθμού από πράκτορες. Λειτουργεί σαν εξ υπηρέτης για τους πράκτορες που έχει σε χαμηλότερο επίπεδο από αυτόν. Αφού επεξεργαστεί τα δεδομένα, τότε προωθεί μόνο τις κρίσιμες καταγραφές ασφαλείας, με την λειτουργία του ως πράκτορας, στον εξυπηρέτη που βρίσκεται σε υψηλότερο επίπεδο στην αρχιτεκτονική. Μπορεί να τοποθετείται μεταξύ ενός μεγάλου εύρους δικτύου (bandwidth) και ενός με μικρό εύρος έτσι ώστε να επιτευχθεί μείωση του όγκου δεδομένων που θα στέλνονται μέσω του μικρού εύρους γραμμής.



Εικόνα 5-1 Σχεδιάγραμμα χρησιμοποίησης υβριδικού εξυπηρέτη OSSEC

5.2.2.4 Λειτουργία Χωρίς Πράκτορες (Agentless Mode)

Ο τελευταίος τύπος λειτουργίας του OSSEC αφορά συσκευές στις οποίες δεν μπορούμε να εγκαταστήσουμε ένα πράκτορα OSSEC. Με αυτή τη μορφή επιτρέπουμε στον εξυπηρέτη του OSSEC, χρησιμοποιώντας ένα ξεχωριστό χρήστη, να συνδέεται μέσω Secure Shell (ή μέσω κάποιου άλλου τρόπου) στην συσκευή που επιθυμούμε να παρακολουθήσουμε για να πραγματοποιεί έλεγχο ακεραιότητας αρχείων ή να εκτελεί κάποια εντολή στο σύστημα. Επίσης οι καταγραφές ασφαλείας των συσκευών αυτών μπορούν να στέλνονται μέσω Syslog πρωτοκόλλου στον OSSEC server.

5.3 Εγκατάσταση OSSEC

Στην ενότητα αυτή θα αναπτυχθεί η μεθοδολογία εγκατάστασης του OSSEC (εξυπηρέτη και πράκτορα) σε δημοφιλή λειτουργικά συστήματα. Είναι σκόπιμο να αναφέρουμε ότι OSSEC σε λειτουργία εξυπηρέτη, αλλά και σε υβριδικό τύπο λειτουργίας μπορεί να εγκατασταθεί μόνο σε λειτουργικά συστήματα βασισμένα στο Unix.

5.3.1 Για Windows Λειτουργικά Συστήματα

5.3.1.1 Χειροκίνητη Εγκατάσταση

Αρχικά πραγματοποιείται μεταφόρτωση του OSSEC από τον επίσημο διαδικτυακό χώρο[4] του με την χρήση ενός περιηγητή.

Θεωρείται καλή πρακτική ο έλεγχος για παραποίηση του εκτελέσιμου αρχείου εγκατάστασης. Για την επίτευξη αυτού συγκρίνεται το checksum πού παρέχεται από το διαδικτυακό τόπο του OSSEC με το αποτέλεσμα που παράγει ένα εργαλείο υπολογισμού μονόδρομων συναρτήσεων MD5. Ένα δωρεάν εργαλείο είναι το WinMD5Free[5] .

Κατά την διάρκεια εκτέλεσης του προγράμματος εγκατάστασης του OSSEC μπορεί να γίνει επιλογή για των καταγραφών ασφαλείας από τον Application Server IIS[6] καθώς και για το κατά πόσο θα εκτελείται έλεγχος ακεραιότητας των αρχείων του συστήματος (file integrity check).

Αφότου ολοκληρωθεί επιτυχώς η εγκατάσταση, εκκινείται ο πράκτορας. Για τη σωστή λειτουργία του απαιτεί η εισαγωγή δύο στοιχείων: α) η διεύθυνση IP του OSSEC Server που παρακολουθεί τον συγκεκριμένο πράκτορα β) το κλειδί αυθεντικοποίησης το οποίο υπάρχει η δυνατότητα να δημιουργηθεί και να εξαχθεί από τον OSSEC εξυπηρέτη. Το κλειδί αυτό χρησιμοποιείται σαν μέσο πιστοποίησης του OSSEC πράκτορα στον OSSEC εξυπηρέτη. Μετά απαιτείται η επανεκκίνηση του πράκτορα για χρησιμοποίηση των νέων ρυθμίσεων.

5.3.1.2 Μαζική εγκατάσταση μέσω MS Windows Active Directory

Για την αυτόματη εγκατάσταση πολλών OSSEC πρακτόρων απαιτείται η ύπαρξη ενός αυτοματοποιημένου τρόπου ταυτόχρονης εγκατάστασης αυτών των στοιχείων. Για την επίτευξη αυτού του σκοπού οι υπηρεσίες που παρέχονται από το MS Windows Active Directory κρίνονται απαραίτητες.

Αρχικά απαιτείται η μετατροπή του εκτελέσιμου αρχείου του OSSEC(ossec-agent-win32.exe) σε μορφή windows installer file (msi). Για την επίτευξη αυτού θα πρέπει να χρησιμοποιηθεί κάποιο πρόγραμμα που προσφέρει τέτοιες δυνατότητες. Για την αθόρυβη εγκατάσταση του OSSEC πράκτορα η παράμετρος (flag) που θα πρέπει να χρησιμοποιηθεί είναι η **/S**.

```
> ossec-agent-win32.exe /S
```

Μετά τη δημιουργία του Windows installer (msi) θα αναλυθεί η διαδικασία που ακολουθείται στο Active Directory για την αυτόματη εγκατάσταση του OSSEC σε όλους τους υπολογιστές ενός τομέα.

---

[4] http://www.ossec.net/?page_id=19

[5] http://www.winmd5.com

[6] Αν υπάρχει κάποιος εγκατεστημένος στην συσκευή που θα πραγματοποιήσουμε την εγκατάσταση

Πιο αναλυτικά τα βήματα για την επίτευξη αυτής της διαδικασίας είναι τα εξής:

1. Στο **Group Policy Management** γίνεται εκτέλεση κλικ στο δεξί κουμπί του ποντικιού πάνω στο **Group Policy Objects** και επιλέγεται η εναλλακτική **New** για να δημιουργηθεί έτσι μια καινούργια πολιτική (policy) και να εισαχθεί ένα χαρακτηριστικό όνομα για την πολιτική αυτή.

2. Επιλέγεται την πολιτική που μόλις δημιουργήθηκε και εκτελείται δεξί κλικ. Στο εμφανιζόμενο μενού επιλέγεται το **Edit**. Αφού ανοίξει το νέο παράθυρο επιλέγεται η εγγραφή που περιέχει το όνομα της νέας πολιτικής και εκτελείται πάλι δεξί κλικ. Σε αυτό το εμφανιζόμενο μενού γίνεται επιλογή του **Properties** και στην συνέχεια επιλέγεται η καρτέλα **Security** και στο group **Domain Computers.** Εκεί παραχωρείται η άδεια **Apply Group Policy** και διαγράφεται από τα group, αυτό που φέρει τον τίτλο **Authenticated Users** (εάν υπάρχει). Τέλος, κλείνουμε το παράθυρο **Properties**.

3. Γίνεται πλοήγηση στο **Computer Configuration -> Policies -> Software Settings -> Software Installation.**

4. Εκτελείται δεξί κλικ και επιλέγεται το **New -> Package**.

5. Εισάγεται το πρόγραμμα msi που προέκυψε από την προηγούμενη διαδικασία. Ελέγχεται η διαδρομή του προγράμματος αν είναι προσβάσιμη από το group **Domain Computers** και στο παράθυρο **Deploy Software** επιλέγεται το **Advanced**.

6. Γίνεται πλοήγηση στην καρτέλα **Deployment**. Ελέγχεται αν είναι επιλεγμένο το **Assigned** και εκτελείται κλικ στο **Advanced** και επιλέγεται το **Ignore language when deploy this package**. Ελέγχεται αν είναι επιλεγμένο το **Make this 32-bit X86 application available to Win64 Machines**.

7. Τέλος, επιλέγεται το **Domain** ή **Organization Unit (OU)** στο οποίο είναι επιθυμητό να ενεργοποιηθεί η πολιτική αυτή. Εκτελείται δεξί κλικ και επιλέγεται το **Link an Existing Policy** με την πολιτική που μόλις δημιουργήθηκε.

Σε αυτό το σημείο ολοκληρώνεται η διαδικασία αυτόματης εγκατάστασης του OSSEC Agent στους υπολογιστές του Domain.

Επόμενο βήμα στην διαδικασία είναι να εισαχθούν με αυτόματο τρόπο η διεύθυνση IP του OSSEC εξυπηρέτη και το κλειδί αυθεντικοποίησης που παρήχθη στον OSSEC Server.

Για την αυτόματη εξαγωγή όλων των κλειδιών στην πλευρά του OSSEC εξυπηρέτη εκτελείται στο τερματικό την εντολή:

```
# cat /var/ossec/etc/client.keys > master.keys
```

Αφότου μεταφερθεί το αρχείο με τα κλειδιά αυθεντικοποίησης σε ένα προσβάσιμο φάκελο από όλους τους υπολογιστές του τομέα, θα πρέπει να εκτελεστεί ένα αρχεία batch script ώστε αυτόματα να εισαχθεί η διεύθυνση IP του OSSEC εξυπηρέτη καθώς και το κλειδί αυθεντικοποίησης για τον συγκεκριμένο υπολογιστή. Η εκτέλεση αυτού του αρχείου μπορεί να γίνει με 2 τρόπους: α) ενσωματώνοντας το σαν μια σειρά εντολών η οποία θα εκτελείται στην τελική φάση της εγκατάστασης (post installation script) μέσω του msi builder (αν παρέχεται αυτή η δυνατότητα), β) με το να εκτελεστεί σαν script μέσω του Active Directory.

Στο παράδειγμα που παρουσιάζεται παρακάτω δημιουργείται ένα αρχείο το οποίο περιέχει το κλειδί αυθεντικοποίησης. Αυτό εντοπίζει στο αρχείο master.keys τον υπολογιστή στον οποίο εκτελείται (με κριτήριο την IP διεύθυνση). Έπειτα, εισάγει στο αρχείο ossec.conf την IP διεύθυνση του εξυπηρέτη OSSEC και εκκινεί την διεργασία του πράκτορα OSSEC έτσι ώστε να ληφθούν υπόψιν οι νέες ρυθμίσεις που πραγματοποιήθηκαν.

```
1.@echo off
2.set masterkeyfilepath=""
3.set clientkeyfilepath="c:\Program Files (x86)\ossec-agent\"
4.echo ^<ossec_config^> >> %clientkeyfilepath%ossec.conf
5.echo       ^<client^>   >> %clientkeyfilepath%ossec.conf
6.echo                ^<server-ip^>10.0.2.4^</server-
   ip^> >> %clientkeyfilepath%ossec.conf
7.echo       ^</client^> >> %clientkeyfilepath%ossec.conf
8.echo ^</ossec_config^> >> %clientkeyfilepath%ossec.conf
9.rem path Program Files (x86) ossec-agent
10.
11.rem set ip_address_string="IP Address"
12.set ip_address_string="IPv4 Address"
13.for /f "usebackq tokens=2 delims=:" %%f in (`ipconfig ^| findstr
   /c:%ip_address_string%`) do set myip=%%f
14.findstr %myip% %masterkeyfilepath%master.keys > %clientkeyfilepath%client
   .keys
15.net start OssecSvc
```

5.3.2 Για Linux/BSD (Unix-like) Λειτουργικά Συστήματα

5.3.2.1 Χειροκίνητη Εγκατάσταση

Αρχικά καταφορτώνεται το αρχείο εγκατάστασης του OSSEC από το επίσημο διαδικτυακό χώρο του εργαλείου με την εντολή:

```
# wget -U ossec http://www.ossec.net/files/ossec-hids-2.8.1.tar.gz
```

Καλή πρακτική είναι να γίνεται έλεγχος για παραποίηση του αρχείου αυτού. Για το σκοπό αυτό θα πρέπει να καταφορτωθεί και το checksum του προγράμματος εγκατάστασης του OSSEC με την εντολή:

```
# wget -U ossec http://www.ossec.net/files/ossec-hids-2.8.1-checksum.txt
```

Για να εμφανιστεί η τιμή του checksum εκτελείται η εντολή :

```
# cat ossec-hids-2.8.1-checksum.txt
```

Η παραπάνω τιμή θα πρέπει να συγκριθεί και να ταιριάζει με το αποτέλεσμα ενός εκ των εντολών:

```
# md5sum ossec-hids-2.8.1.tar.gz
# sha1sum ossec-hids-2.8.1.tar.gz
```

Επόμενο βήμα είναι η εγκατάσταση των βασικών εργαλείων που απαιτούνται για τη μετατροπή του πηγαίου κώδικα σε εκτελέσιμο αρχείο (compile).

Για διανομές όπως το Ubuntu αρκεί να εκτελεστεί η ακόλουθη εντολή:

```
# apt-get install build-essential
```

Αν απαιτείται η υποστήριξη των mysql ή postgres database εκτελείται η εντολή:

Για διανομές βασισμένες στο Ubuntu, εκτελείται η ακόλουθη εντολή:

```
# apt-get install mysql-dev postgres-dev
```

Αντίθετα για διανομές βασισμένες στο Redhat, εκτελείται η ακόλουθη εντολή:

```
# yum install mysql-devel postgres-devel
```

Επόμενο βήμα είναι η αποσυμπίεση του αρχείου του OSSEC:

```
# tar -xvzf ossec-hids-2.8.1.tar.gz
```

Γίνεται μετάβαση στο φάκελο που μόλις δημιουργήθηκε με την εντολή:

```
# cd ossec-hids-2.8.1
```

Στη συνέχει εκτελείται το script εγκατάστασης με την εντολή:

```
#./install.sh
```

Σε αυτό το σημείο θα πρέπει να τονιστεί ότι υπάρχει και η δυνατότητα εγκατάστασης του προγράμματος από τα διαδικτυακά αποθετήρια (repositories) των δημοφιλών λειτουργικών συστημάτων μέσω των διαχειριστών πακέτων (package managers).

Για τις Debian διανομές θα πρέπει να εκτελεστούν οι παρακάτω εντολές:

```
# wget -O - http://ossec.alienvault.com/repos/apt/conf/ossec-key.gpg.key|
apt-key add -
# echo "deb http://ossec.alienvault.com/repos/apt/debian wheezy main" >>
/etc/apt/sources.list
(αλλαγή του wheezy στην Debian διανομή που έχουμε)
# apt-get update
# apt-get install ossec-hids  (ή ossec-hids-agent)
```

Για τις Redhat διανομές θα πρέπει να εκτελεστούν οι παρακάτω εντολές:

```
# wget -q -O - https://www.atomicorp.com/installers/atomic | sh
# yum install ossec-hids ossec-hids-server (ή ossec-hids-client για agent
εγκατάσταση)
```

1. Γίνεται επιλογή της γλώσσας εγκατάστασης του OSSEC. Για μεγαλύτερη συμβατότητα καλή πολιτική είναι να επιλεχθούν τα Αγγλικά.

2. Επιλέγουμε τον τύπο (server,hybrid,agent,local) λειτουργίας του OSSEC στη συγκεκριμένη συσκευή γράφοντας το ολογράφως (πχ agent).

3. Γίνεται επιλογή της διαδρομή στο σύστημα αρχείων στην οποία θα εγκατασταθεί το OSSEC (πχ **/var/ossec/**).Προεπιλεγμένο είναι το **/var/ossec**.

4. Γίνεται εισαγωγή της διεύθυνσης IP του OSSEC εξυπηρέτη με την οποία θα επικοινωνεί ο συγκεκριμένος πράκτορας.

5. Γίνεται επιλογή για το αν στον συγκεκριμένο agent θα εκτελείται έλεγχος ακεραιότητας, ανίχνευσης rootkit και αν θέλουμε να έχουμε ενεργοποιημένη την άμεση αντίδραση (active response) σε περίπτωση που λάβει χώρα κάποιο περιστατικό.

Μετά την ολοκλήρωση των παραπάνω βημάτων θα αρχίσει αυτόματα η εγκατάσταση του OSSEC στο σύστημα.

Όταν ολοκληρωθεί επιτυχώς η εγκατάσταση θα εμφανιστούν στην οθόνη πληροφορίες για το πως εκκινείται και τερματίζεται το πρόγραμμα του OSSEC καθώς και σε ποια διαδρομή βρίσκεται το αρχείο ρυθμίσεων του OSSEC.

Το επόμενο βήμα είναι η εισαγωγή του authentication key, ώστε να δοθεί η δυνατότητα επικοινωνίας του πράκτορα με τον εξυπηρέτη.

5.4 Εγκατάσταση Εξυπηρέτη OSSEC

Στην ενότητα αυτή θα περιγραφούν τα βήματα εγκατάστασης ενός εξυπηρέτη OSSEC σε ένα λειτουργικό σύστημα τύπου Unix.

1. Αρχικά γίνεται επιλογή της γλώσσας. Για μεγαλύτερη συμβατότητα καλή πολιτική είναι να επιλεχθούν τα Αγγλικά.

2. Γίνεται επιλογή για τον τύπο εγκατάστασης. Στην συγκεκριμένη περίπτωση είναι **server**.

3. Γίνεται επιλογή της διαδρομή εγκατάστασης . Προεπιλεγμένη είναι το **/var/ossec**.

4. Πραγματοποιείται επιλογή για την ενεργοποίηση ειδοποιήσεων μέσω ηλεκτρονικού ταχυδρομείου.

5. Γίνεται επιλογή για την εκτέλεση του ελέγχου ακεραιότητας στα αρχεία και ελέγχου για rootkits.

6. Γίνεται επιλογή για ενεργοποίηση της άμεσης αντίδραση σε περίπτωση που ανιχνευθεί κάποια κακόβουλη δραστηριότητα (active response).

7. Επιλέγεται αν θα παρέχεται η δυνατότητα στο OSSEC να εισάγει στο τοίχος πυρασφάλειας καταγραφές με κακόβουλες IP και πάνω από ποιο επίπεδο θα τις θεωρεί επικίνδυνες (προεπιλογή 6).

8. Στην συνέχεια γίνεται επιλογή για ενεργοποίηση ή μη του μηχανισμού IP white listing. Ο μηχανισμός αυτός παρέχει τη δυνατότητα σε κάποιές IP να μην αποκόπτονται ακόμα και αν ανιχνευθούν σαν πηγή κακόβουλων ενεργειών. Αυτές είναι τις περισσότερες φορές οι IP διευθύνσεις των εξυπηρετών μας.

9. Γίνεται επιλογή για ενεργοποίηση η μη του ο remote syslog server στην πόρτα 514 (UDP).

Αφότου ολοκληρώσουμε τα παραπάνω βήματα ο εξυπηρέτης OSSEC είναι έτοιμος για χρήση.

5.5 Απεγκατάσταση Εξυπηρέτη/Πράκτορα

5.5.1 Λειτουργικά Συστήματα Τύπου Unix

Για την απεγκατάσταση ενός πράκτορα OSSEC από λειτουργικά συστήματα τύπου Unix, θα πρέπει να χρησιμοποιηθεί το κατάλληλου script. Αυτό αναιρεί τις αλλαγές που έχει πραγματοποιήσει στο λειτουργικό η εγκατάσταση και η λειτουργία του OSSEC προγράμματος. Το script είναι το ακόλουθο:

```
sudo rm -f /etc/init.d/ossec /etc/rc0.d/K20ossec /etc/rc1.d/K20ossec\
/etc/rc2.d/S20ossec /etc/rc3.d/S20ossec /etc/rc4.d/S20ossec\
/etc/rc5.d/S20ossec /etc/rc6.d/K20ossec;
sudo rm -rf /var/ossec;
sudo /usr/sbin/deluser ossec;
sudo /usr/sbin/deluser ossecm;
sudo /usr/sbin/deluser ossecr;
sudo /usr/sbin/deluser ossecd;
sudo /usr/sbin/delgroup ossec;
sudo /usr/sbin/delgroup ossecd;
```

5.5.2 Windows Λειτουργικά

Για την απεγκατάσταση ενός πράκτορα OSSEC από λειτουργικά συστήματα Windows απαιτείται μόνο η εκτέλεση του αντίστοιχου προγράμματος που υπάρχει στο φάκελο εγκατάστασης του OSSEC.

5.6 Προσθήκη Πράκτορα

5.6.1 Χειροκίνητος τρόπος

Για την εκκίνηση της επικοινωνίας μεταξύ ενός εξυπηρέτη OSSEC και ενός πράκτορα OSSEC θα πρέπει αρχικά στον πράκτορα να εισαχθεί ένα κλειδί αυθεντικοποίησης. Για την επίτευξη αυτού θα πρέπει να παράγουμε ένα μοναδικό κλειδί μέσω του OSSEC server.

Η διαδικασία για την παραγωγή αυτού του κλειδιού είναι η ακόλουθη:

1. Στην πλευρά του εξυπηρέτη γίνεται πλοήγηση στην διεύθυνση **/var/ossec/bin** και εκτελείαι το αρχείο **manage_agents**. Γίνεται επιλογή του **Add an agent (A)** και εισάγονται οι απαραίτητες πληροφορίες για τον πράκτορα που θέλουμε να προσθέσουμε.

2. Για να εξαχθεί το κλειδί για έναν συγκεκριμένο πράκτορα, γίνεται ξανά εκτέλεση του αρχείου **manage_agents** και επιλέγεται το **Extract key for an agent (E)** για τον πράκτορα που επιθυμούμε να εκτελεστεί η διαδικασία.

3. Αντίστοιχα στον πράκτορα γίνεται πλοήγηση στην διεύθυνση **/var/ossec/bin** και εκτελείται το αρχείο **manage_agents**. Επιλέγεται το **Import key from server (I)** και εκτελείται επικόλληση του κλειδιού.

4. Απαιτείται επανεκκίνηση του OSSEC εξυπηρέτη και πράκτορα για την εφαρμογή των αλλαγών.

```
#service ossec restart
```

5. Για να γίνει επιβεβαίωση του κατά πόσο η προηγούμενη διαδικασία ήταν επιτυχημένη εκτελείται η παρακάτω εντολή

```
#/var/ossec/bin/list_agents
```

5.6.2 Αυτόματη λήψη κλειδιού

Είναι μία διαδικασία με την οποία οι πράκτορες λαμβάνουν το κλειδί αυτόματα από τον εξυπηρέτη μέσω OpenSSL. Να σημειωθεί ότι αυτή η διαδικασία αφορά μόνο πράκτορες που είναι εγκατεστημένοι σε λειτουργικά τύπου Unix.

Για να επιτευχθεί αυτό θα πρέπει πριν την εγκατάσταση του server και των agents να έχει εγκατασταθεί η υποστήριξη του πρωτοκόλλου SSL στα λειτουργικά συστήματα.

Αυτό γίνεται εφικτό μέσω της εντολής:

```
# apt-get install libssl-dev
```

Επόμενο βήμα στην διαδικασία αυτή είναι να παραχθεί στον εξυπηρέτη ένα πιστοποιητικό ασφάλειας. Αυτό επιτυγχάνεται με τις παρακάτω εντολές:

```
# openssl genrsa -out /var/ossec/etc/sslmanager.key 2048
# openssl req -new -x509 -key /var/ossec/etc/sslmanager.key -out
/var/ossec/etc/sslmanager.cert -days 365
```

Το script **ossec-authd** από προεπιλογή εντοπίζει το κλειδί και το πιστοποιητικό στην διεύθυνση **/var/ossec/etc/** με τα ονόματα **sslmanager.key** και **sslmanager.cert** αντίστοιχα. Σε αντίθετη περίπτωση πρέπει να οριστεί ο φάκελος που περιέχει τα πιστοποιητικά αυτά με την χρήση των παραμέτρων -x και -k όταν τρέχουμε το πρόγραμμα **ossec-authd**.

Για να την εκκίνηση του daemon από στον server εκτελούμε την εντολή:

```
# /var/ossec/bin/agent-authd -p 1515 > /dev/null 2>&1
```

Το πρόγραμμα **agent-authd** από προεπιλογή τρέχει στην πόρτα 1515.

Σε καθένα από τους πράκτορες πρέπει να εκτελεστεί η εντολή:

```
# /var/ossec/bin/agent-auth -m <ip-server> -p 1515
```

Από προεπιλογή εισάγεται σαν όνομα το όνομα(hostname) του υπολογιστή που εκτελείται το πρόγραμμα. Σε αντίθετη περίπτωση θα πρέπει να οριστεί το όνομα με την παράμετρο -A.

5.6.3 Λειτουργία Agentless

Ο τρόπος λειτουργίας του OSSEC ο οποίος δεν βασίζεται σε πράκτορες, όπως προαναφέρθηκε στην αρχή του κεφαλαίου δίνει την δυνατότητα να εκτελούνται διάφορες διεργασίες (όπως π.χ. έλεγχος ακεραιότητας αρχείων συστήματος), σε συσκευές που δεν παρέχεται η δυνατότητα εγκατάστασης ενός πράκτορα. Τέτοιες συσκευές είναι οι δρομολογητές (routers) ή switches.

Τα βήματα παραμετροποίησης για την εκκίνηση του τρόπου λειτουργίας χωρίς πράκτορες είναι τα ακόλουθα:

1. Αρχικά απαιτείται η εγκατάσταση του προγράμματος **expect**:

```
# apt-get install expect
```

2. Για την ενεργοποίηση της λειτουργίας εκτελείται:

```
#/var/ossec/bin/ossec-control enable agentless
```

3. Επόμενο βήμα είναι να γίνει προσθήκη συσκευών. Αυτό πραγματοποιείται με την χρήση της εντολής:

```
#/var/ossec/agentless/register_host.sh add <username>@<ip> <pass>
```

όπου **<username>** το όνομα χρήστη, ο οποίος θα έχει δικαίωμα εκτέλεσης διεργασιών στην απομακρυσμένη συσκευή, **<ip>** η διεύθυνση της απομακρυσμένης συσκευής και **<pass>** ο κωδικός αυθεντικοποίησης του χρήστη που ορίστηκε στην αρχή.

4. Τροποποιείται το κύριο αρχείο ρυθμίσεων (**ossec.conf**) ανάλογα με τις λειτουργίες που επιθυμούμε να ελέγχονται μέσα στην συσκευή. Για παράδειγμα, αν είναι επιθυμητό να εκτελεστεί έλεγχος ακεραιότητας των αρχείων στους φακέλους **/etc**, **/boot**, **/bin**, **/sbin** ανά μια ώρα, θα πρέπει να προστεθεί μέσα στο **ossec.conf** ο παρακάτω κώδικας:

```
<agentless>
      <type>ssh_integrity_check_linux</type>
      <frequency>3600</frequency>
      <host>use_sudo chris@172.16.0.11</host>
      <state>periodic_diff</state>
      <arguments>"/etc /boot /bin /sbin"</arguments>
</agentless>
```

Στο παραπάνω παράδειγμα να ξεκαθαριστεί ότι το πεδίο που ορίζεται από την ετικέτα <type> περιέχει έτοιμα shell scripts που βρίσκονται στον φάκελο **/var/ossec/agentless/**. Σε αυτή το φάκελο μπορούν να προστεθούν και shell scripts τα οποία έχουν γραφτεί από εμάς.

Για την διαγραφή ενός εξυπηρέτη ο οποίος βρίσκεται σε λειτουργία χωρίς πράκτορες απλά διαγράφουμε την συγκεκριμένη εγγραφή από το κρυφό αρχείο **/var/ossec/agentless/.passlist**

Εάν είναι επιθυμητό να μην εισάγεται κωδικός για την εκτέλεση των διεργασιών παρέχεται η δυνατότητα να αποθηκευτεί το δημόσιο κλειδί του εξυπηρέτη OSSEC μέσα στην απομακρυσμένη συσκευή.

Τα βήματα για την υλοποίηση κάτι τέτοιου είναι τα εξής:

1. Δημιουργείται το κλειδί στον εξυπηρέτη OSSEC

```
# sudo -u ossec ssh-keygen
```

2. Γίνεται μετάβαση στον φάκελο **/var/ossec/.ssh** και αντιγράφουμε το δημόσιο κλειδί που δημιουργήθηκε στην απομακρυσμένη συσκευή

```
#cd /var/ossec/.ssh/
#cat id_rsa.pub | ssh chris@172.16.0.11 ' cat >>
/home/chris/.ssh/authorized_keys'

Ή

ssh-copy-id chris@172.16.0.11
```

3. Γίνεται εισαγωγή των παραμέτρων διασύνδεσης της απομακρυσμένης συσκευής στον εξυπηρέτη OSSEC χωρίς την χρήση του κωδικού

```
#/var/ossec/agentless/register_host.sh add chris@172.16.0.11 NOPASS
```

Στην περίπτωση που δεν υπάρχει ήδη το αρχείο **authorized_keys** μπορούμε να το δημιουργήσουμε ένα με τις εντολές

```
#mkdir -p /home/<user>/.ssh
#touch authorized_keys
```

5.7 Αυτόματη Απομακρυσμένη Μεταφορά Αρχείου Ρυθμίσεων

Όπως έχει αναφερθεί το κύριο αρχείο ρυθμίσεων του OSSEC είναι το **ossec.conf** το οποίο βρίσκεται στον φάκελο **/var/ossec/etc**. Η χειροκίνητη τροποποίησή του σε εκτεταμένες δικτυακές υποδομές είναι μια επίπονη διαδικασία. Για τον λόγο αυτό διατίθεται ένα επιπρόσθετο αρχείο ρυθμίσεων το οποίο λειτουργεί συμπληρωματικά στο **ossec.conf**.

Για την επίτευξη αυτού αρχικά θα πρέπει να εντοπιστεί το αρχείο **agent.conf** στο φάκελο **/var/ossec/etc/shared**. Σε αυτό θα πρέπει να τοποθετηθούν ένα σύνολο από επιπρόσθετες ρυθμίσεις. Έχουμε την δυνατότητα να προσδιορίσουμε ποιες ρυθμίσεις θα μεταφερθούν στους υπολογιστές με κριτήριο α) το λειτουργικό που έχουν εγκατεστημένο, β) το όνομα του υπολογιστή (hostname) ή γ) σε ποια κατηγορία υπολογιστών αυτοί ανήκουν (π.χ webservers). Ένα παράδειγμα τέτοιων ρυθμίσεων φαίνεται παρακάτω:

```
<agent_config name="agent1">
  <localfile>
    <location>/var/log/my.log</location>
    <log_format>syslog</log_format>
```

```
  </localfile>
</agent_config>

<agent_config os="Linux">
  <localfile>
    <location>/var/log/my.log2</location>
    <log_format>syslog</log_format>
  </localfile>
</agent_config>

<agent_config os="Windows">
  <localfile>
    <location>C:\myapp\my.log</location>
    <log_format>syslog</log_format>
  </localfile>
</agent_config>
```

Ο πράκτορας ανά προκαθορισμένα χρονικά διαστήματα ελέγχει το checksum του αρχείου **agent.conf** και αν διαπιστώσει αλλαγή το κατεβάζει τοπικά. Τα αρχεία ρυθμίσεων **ossec.conf** και **agent.conf** τρέχουν παράλληλα στον πράκτορα. Για να λάβουν χώρα οι αλλαγές στο **agent.conf** θα πρέπει να γίνει επανεκκίνηση του πράκτορα OSSEC.

Η επανεκκίνηση του πράκτορα μπορεί να επιτευχθεί με τρείς τρόπους: α) χειροκίνητα μέσω τερματικού, β) απομακρυσμένα με το πρόγραμμα **agent_control** που βρίσκεται στον φάκελο **/var/ossec/bin/**, γ) με την βοήθεια της λειτουργίας του **active_response**, όπου όταν ανιχνεύσει αλλαγή στο συγκεκριμένο αρχείο θα προκαλέσει επανεκκίνηση του agent. Το τελευταίο μπορεί να επιτευχθεί με τον παρακάτω τρόπο για τα λειτουργικά συστήματα βασισμένα στο Unix:

1. Δημιουργείται ένας κανόνας στο αρχείο **local_rules.xml** που βρίσκεται στον φάκελο **/var/ossec/rules/** στον εξυπηρέτη OSSEC.

```
<rule id="710001" level="1">
  <if_group>syscheck</if_group>
  <match>/var/ossec/etc/shared/agent.conf</match>
  <description>agent.conf was modified</description>
</rule>
```

2. Ενσωματώνονται οι παρακάτω ρυθμίσεις στο αρχείο **ossec.conf** του συστήματος το οποίο παίζει το ρόλο του πράκτορα.

```
<command>
  <name>restart-ossec</name>
```

```
  <executable>restart-ossec.sh</executable>
  <expect></expect>
</command>
<active-response>
  <command>restart-ossec</command>
  <location>local</location>
  <rules_id>710001</rules_id>
</active-response>
```

Το αρχείο **agent.conf** θα πρέπει να έχει δικαιώματα ανάγνωσης από τον χρήστη **ossec**. Αυτό αποσκοπεί στο να μπορούν οι πράκτορες του OSSEC να διαβάσουν απομακρυσμένα το αρχείο αυτό. Μπορούμε να ελέγξουμε για λάθη στο **agent.conf** με το πρόγραμμα **/var/ossec/bin/verify-agent-conf**.

5.8 Hybrid Service bug

Η έκδοση του OSSEC 2.8.1 φέρει ένα σφάλμα στο αρχείο που αφορά την ταυτόχρονη εκκίνηση, επανεκκίνηση και τερματισμό των υπηρεσιών του υβριδικού εξυπηρέτη OSSEC (server/agent). Αυτό επηρεάζει την εντολή:

```
#service ossec {start/restart/stop/status}
```

κατά τέτοιο τρόπο ώστε να εκκινεί μόνο τον πράκτορα OSSEC και όχι τον εξυπηρέτη που τρέχει παράλληλα στο σύστημα. Για να τη λύση του προβλήματος αυτού απαιτείται η τροποποίηση του αρχείου εκκίνησης. Πιο συγκεκριμένα η διαδικασία που θα πρέπει να ακολουθηθεί είναι η επόμενη:

1. Σε έναν επεξεργαστή κειμένου (vim, nano) επεξεργάζεται το αρχείο **/etc/init.d/ossec**
2. Προστίθεται μέσα στις συναρτήσεις start, stop, status η γραμμή:

```
/var/ossec/bin/ossec-control {start, stop,status}
```

Με άλλα λόγια οι συναρτήσεις αυτές θα έχουν την ακόλουθη μορφή:

```
start(){
       ${DIRECTORY}/bin/ossec-control start
       /var/ossec/bin/ossec-control start
}

stop() {
       ${DIRECTORY}/bin/ossec-control stop
       /var/ossec/bin/ossec-control     stop
 }
```

```
status() {
       ${DIRECTORY}/bin/ossec-control status
       /var/ossec/bin/ossec-control      status
 }
```

Βιβλιογραφία

[1] M. Tavallaee, E. Bagheri, W. Lu and A.-A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *Proceedings of the Second IEEE Symposium on Computational Intelligence for Security and Defence Applications 2009*, 2009.

[2] C. Kolias, Kambourakis, Georgios, Stavrou, Angelos and Gritzalis, Stefanos, "Intrusion Detection in 802.11 Networks: Empirical Evaluation of Threats and a Public Dataset," *Communications Surveys & Tutorials,* 2015.

[3] P. Garcia-Teodoro, Diaz-Verdejo, J and Macia-Fernandez, Gabriel , "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Computers \& Security,* vol. 28, no. 1, pp. 18-28, 2009.

[4] A. Lazarevic, L. Ertoz, V. Kumar, A. Ozgur and J. Srivastava, "A Comparative Study of Anomaly Detection Schemes in Network Intrusion Detection.," in *SIAM*, 2003.

[5] M. Roesch, "Snort: Lightweight Intrusion Detection for Networks," *LISA,* vol. 99, no. 1, 1999.

[6] M. Nicolett and K. M. Kavanagh, "Critical capabilities for security information and event management technology," Gartner, 2011.

[7] H. Karlzén, *An Analysis of Security Information and Event Management Systems-The Use or SIEMs for Log Collection, Management and Analysis,* 2009.

[8] J. Rossi, "OSSEC Documentation," [Online]. Available: http://www.ossec.net/?page_id=11. [Accessed Jun 2015].