
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

# «ΣΥΣΤΗΜΑΤΑ ΕΝΤΟΠΙΣΜΟΥ (SIEM) : ΕΦΑΡΜΟΓΗ ΣΤΟ ΔΙΚΤΥΑΚΟ ΠΕΡΙΒΑΛΛΟΝ ΤΟΥ ΤΜΗΜΑΤΟΣ ΜΠΗΣ»

**Του φοιτητή**
**Νικολόπουλου Δημήτριου**
**Αρ. Μητρώου: 175070**

**Επιβλέπων**
**Ηλιούδης Χρήστος**
**Καθηγητής**

**Ημερομηνία 30/05/2025**

Συστήματα εντοπισμού (SIEMs) :Εφαρμογή στο δικτυακό περιβάλλον του τμήματος ΜΠΗΣ

Κωδικός Π.Ε. 24168

Νικολόπουλος Δημήτριος

Ηλιούδης Χρήστος

Ημερομηνία ανάληψης Π.Ε. 27/03/2024

Ημερομηνία περάτωσης Π.Ε. 30/05/2025

*Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως διπλωματική εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.*

*«Σε όλους όσους είναι πάντα δίπλα μου»*

# Πρόλογος

Η παρούσα πτυχιακή εργασία εστιάζει στην σταδιακή μελέτη και ενσωμάτωση τεχνολογιών ασφαλείας, με στόχο την καλύτερη ορατότητα και πιο αποτελεσματική αντιμετώπιση απειλών και κινδύνων, στα συστήματα ασφαλείας του ιδρύματος μας. Το θέμα επιλέχθηκε με βάση το ενδιαφέρον μου ,σε θεωρητικό και πρακτικό επίπεδο, στον συνδυασμό δύο τομέων που διδάχτηκα κατά την περίοδο φοίτησης μου, αυτοί των δικτύων και της ασφάλειας πληροφοριακών συστημάτων. Αποτελεί πρόκληση καθώς είναι η πρώτη απόπειρα εφαρμογής όλων των θεωρητικών και πρακτικών γνώσεων που έλαβα και μελετώ, σε μια μεγαλύτερη και πολύ πιο απαιτητική κλίμακα, δηλαδή αυτή του δικτύου και των συστημάτων ασφαλείας του ιδρύματος μας.

# Περίληψη

Η προστασία δεδομένων και υπηρεσιών που χρησιμοποιούνται καθημερινά, αποτελεί ένα από τα σημαντικότερα ζητήματα τόσο σε επίπεδο χρήστη, όσο και σε επίπεδο διαχείρισης. Στόχος είναι η ανακάλυψη των σωστών εργαλείων ασφαλείας ώστε να υπάρξει μια ξεκάθαρη εικόνα στο που οφείλονται και πως μπορούν να καταπολεμηθούν σωστά και άμεσα απειλές και κίνδυνοι που παραμονεύουν. Τα συστήματα SIEM αποτελούν μια ολοκληρωμένη λύση ασφαλείας για τον εντοπισμό και την αποτροπή επιθέσεων. Τέτοιου είδους συστήματα κρίνετε αναγκαίο να ενσωματωθούν σε οργανισμούς όπως το τμήμα μας. Το τμήμα μας παρέχει μια μεγάλη ποσότητα δεδομένων και υπηρεσιών, κατά τα οποία περιλαμβάνονται και ευαίσθητες πληροφορίες που πρέπει να προστατεύονται. Επίσης, οι υπηρεσίες και τα δεδομένα δεν σημαίνει πως προστατεύονται μόνο από εξωτερικούς παράγοντες, αλλά και από εσωτερικούς οι οποίοι θα πρέπει να συμμορφώνονται με βάση τους κανόνες ασφαλείας που έχουν τεθεί. Στόχος αυτής της πτυχιακής εργασίας είναι η ανάλυση των χαρακτηριστικών των τεχνολογιών SIEM, συγκριτική ανάλυση τεχνολογιών SIEM καθώς και ενσωμάτωση και πειραματισμός τους με το δίκτυο και τα συστήματα ασφαλείας του τμήματος.

System Information and Event Management Systems :

Application in the network environment of Department of Information and Electronics Engineering

Dimitrios Nikolopoulos

## Abstract

Nowadays, the use of network services and data exchange are a part of our everyday life. Organisations, such as our university, provide a wide variety of different services for students and professors such as VPN services, databases and other applications that contributes to training and education. Additionally, our university store a huge amount of personal data, that refers to students and professors, about grades, thesis and other sensitive data. Safety measures have been taken, but the continuous development of new and more effective network attacks, create the need for stronger security measures. SIEM systems are a complete security solution that provide data analysis and prevention against different types of attacks and network anomalies. They also provide information about network and security vulnerabilities which are very important for the network's management team. Concluding, in this thesis we are going to analyse what is a SIEM technology, how we use it, how can we benefit from it, compare different SIEM technologies, install and experiment with the university's network and it's security systems.

# Ευχαριστίες

Θα ήθελα να ευχαριστήσω μέσα από την καρδιά μου όλους όσους πίστεψαν και συνέβαλαν στην προσπάθεια, την πορεία και την υλοποίηση της πτυχιακής μου εργασίας. Πιο συγκεκριμένα θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου Καθηγητή κ. Ηλιούδη Χρήστο ο οποίος μου εμπιστεύτηκε ένα τόσο απαιτητικό αλλά ταυτόχρονα τόσο σημαντικό θέμα για ανάπτυξη και πειραματισμό. Επίσης θα ήθελα να επισημάνω την πολύτιμη βοήθειά του σε θέματα παρατηρήσεων, διορθώσεων και βελτίωσης της εργασίας. Επιπλέον οφείλω να ευχαριστήσω και την Καθηγητή κ. Σιδηρόπουλο Αντώνιο ο οποίος βοήθησε πάρα πολύ σε θέματα που αφορούσαν τεχνικά και πρακτικά θέματα της πτυχιακής εργασίας. Τέλος θα ήθελα να ευχαριστήσω μέσα από την καρδιά μου την οικογένεια και τους φίλους που με στήριξαν καθ' όλη την διάρκεια της πτυχιακής μου εργασίας.

# Περιεχόμενα

# Κατάλογος Εικόνων

# Κεφάλαιο 1ο: Εισαγωγή

## 1.1 Αντικείμενο Πτυχιακής

Το τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων παρέχει μια μεγάλη πληθώρα υπηρεσιών και παροχών τόσο σε φοιτητές όσο και στο εκπαιδευτικό του προσωπικό. Όμως, καθοριστικό ρόλο για να επιτευχθεί η σωστή χρήση και η αποφυγή παραβίασης των συστημάτων και των υπηρεσιών του τμήματος παίζουν οι κανόνες και τα συστήματα ασφαλείας που έχουν ληφθεί για αυτό τον σκοπό. Ωστόσο, αυτό δεν καθιστά τα συστήματα και γενικότερα όλα τα μέτρα ασφαλείας τα οποία έχουν υλοποιηθεί "άτρωτα" σε οποιαδήποτε απειλή. Ειδικότερα στην εποχή μας όπου οι κυβερνοαπειλές και οι κυβερνοεπιθέσεις ολοένα και εξελίσσονται. Στόχος μας λοιπόν είναι η αναβάθμιση του συστήματος ασφαλείας του τμήματος με σκοπό την πιο αποτελεσματική και άμεση ανταπόκριση σε κινδύνους και σε κακόβουλη χρήση των υπηρεσιών του τμήματος.

Ένα πολύ σημαντικό και καινοτόμο εργαλείο που μπορεί να συμβάλλει σημαντικά στην αναβάθμιση, καλύτερη κατανόηση και ανταπόκριση απέναντι σε ευπάθειες και κινδύνους που μπορεί να προκληθούν είναι οι τεχνολογίες SIEM (Security Information and Event Management). Οι τεχνολογίες SIEM έχουν ως στόχο την συλλογή και ανάλυση δεδομένων καταγραφής από σχεδόν όλα τα σημεία ενός δικτύου. Αυτό σημαίνει πως εκτός από δικτυακές συσκευές και πληροφοριακά συστήματα, μπορεί να διεισδύσει και σε εφαρμογές καθώς και σε άλλα εργαλεία ασφάλειας, όπως ένα τείχος ασφαλείας ώστε να μπορέσει να εντοπίσει κινδύνους και ευπάθειες που δεν έγιναν αντιληπτές. Πέρα από την σημαντική ικανότητα των τεχνολογιών SIEM να μπορούν να εντοπίσουν κινδύνους και ευπάθειες, παρέχουν και την δυνατότητα αποτροπής επιθέσεων σε πραγματικό χρόνο. Είναι ένα πολύ σημαντικό χαρακτηριστικό που προσφέρουν καθώς μπορούν να αποτρέψουν κινδύνους που δεν γίνονται αντιληπτοί εύκολα και βοηθούν με αυτό τον τρόπο σημαντικά την ομάδα διαχείρισης δικτύου.

Συνοπτικά, μπορούμε να καταλάβουμε πως η ενσωμάτωση μιας τεχνολογίας σε έναν οργανισμό όπως το τμήμα μας, μπορεί να συνεισφέρει σημαντικά στην κατανόηση των ευπαθειών που δεν είχαν γίνει αντιληπτές, στην θέσπιση νέων κανόνων ασφαλείας τόσο για εξωτερικούς όσο και για εσωτερικούς παράγοντες, συμμόρφωση με τους νέους κανόνες καθώς και άμεση και αποτελεσματική ανταπόκριση απέναντι σε κρίσιμα περιστατικά ασφαλείας.

Ωστόσο, αυτό που πρέπει να αναφερθεί είναι πως τα στάδια από την επιλογή έως και την πλήρη ενσωμάτωση μιας τεχνολογίας SIEM δεν αποτελεί μια εύκολη και γρήγορη διαδικασία. Επίσης δεν πρέπει να αποτελεί και μια βιαστική διαδικασία. Γι αυτό θα πρέπει να γίνει μια σωστή μελέτη διαφόρων τεχνολογιών SIEM, μια σωστή ανάλυση των θετικών και αρνητικών τους χαρακτηριστικών, ένας σωστός καταμερισμός των πόρων που είναι να χρησιμοποιηθούν ώστε να μην εκμεταλλευτούμε περισσότερους πόρους από όσους χρειάζεται και τελικά η επιλογή που θα κάνουμε να ανταποκρίνεται όσο πιο αποδοτικά γίνετε απέναντι στους κανόνες και τους στόχους που θέλουμε να πετύχουμε.

## 1.2 Ανάλυση Στόχων

Η ενσωμάτωση μιας SIEM τεχνολογίας σε έναν οργανισμό, όπως το τμήμα μας, αποτελεί μια σημαντική και αναγκαία λύση ασφαλείας. Οι δυνατότητες που παρέχουν οι τεχνολογίες SIEM συμβάλλουν σημαντικά στην κατανόηση λειτουργίας των συστημάτων ασφαλείας και του δικτύου καθώς και συνεισφέρουν πλήρως και αποδοτικά στην αντιμετώπιση περιστατικών ασφαλείας.

Σημαντικό όμως, πέρα από την ανάλυση των δυνατοτήτων και των διάφορων θετικών χαρακτηριστικών που μπορούμε να αποκτήσουμε από αυτές, είναι να αναφερθούμε στους στόχους που θέλουμε να πετύχουμε με την εγκατάσταση μιας τέτοιας τεχνολογίας.

Αρχικά θα πρέπει να αναφέρουμε πως η ασφάλεια των πληροφοριακών συστημάτων και υπηρεσιών που παρέχει το τμήμα μας τόσο σε φοιτητές όσο και στο εκπαιδευτικό προσωπικό δεν αφορά μόνο τις απειλές και τις επιθέσεις που μπορεί να δεχθεί, αλλά αφορά και την κακόβουλη και καταχρηστική συμπεριφορά που μπορεί να δεχθεί από τους ίδιους τους χρήστες του. Για παράδειγμα μια υπηρεσία που παρέχεται από το τμήμα μας, είναι η δωρεάν πρόσβαση στον VPN Server της σχολής. Στόχος αυτής της υπηρεσίας είναι η απομακρυσμένη πρόσβαση και χρήση διαφόρων πόρων που παρέχονται σε κάθε χρήστη όπως η προσωπική βάση δεδομένων καθώς και άλλες υπηρεσίες όπως η δυνατότητα πρόσβασης σε επιστημονικά άρθρα που απαιτούν πληρωμή. Πέραν όλων αυτών των υπηρεσιών που επιτυγχάνονται με την χρήση του, κάποιος χρήστης μπορεί να χρησιμοποιήσει την υπηρεσία VPN με καταχρηστικό τρόπο. Το VPN δίνοντας την δυνατότητα απόκρυψης της πραγματικής μας διεύθυνσης δικτύου καθώς και την δυνατότητα ανώνυμης περιήγησης μπορεί να οδηγήσει κάποιον χρήστη στο να επισκεφτεί απαγορευμένο περιεχόμενο καθώς και να κατεβάσει αρχεία τα οποία μπορούν να διωχθουν ποινικά βάσει των πνευματικών τους δικαιωμάτων, όπως η λήψη κάποιας μη αυθεντικής έκδοσης ενός λογισμικού. Αυτό δεν θα φέρει σε κίνδυνο μόνο τον χρήστη, αλλά όλο το σύστημα ασφαλείας της σχολής διότι όλες οι ενέργειες που γίνονται στον VPN Server αφορούν τοπικά συστήματα του τμήματος. Επίσης αυτό μπορεί να φέρει σε πολύ δύσκολη θέση το τμήμα μας διότι μπορεί πολύ εύκολα να δυσφημιστεί η ασφάλεια των πληροφοριακών συστημάτων και πληροφοριών που παρέχει καθώς και να διωχθούν ποινικά οι αρμόδιοι που υποστηρίζουν αυτά τα συστήματα ασφαλείας.

Επίσης, οι κίνδυνοι και οι απειλές εξελίσσονται με πολύ γρήγορους ρυθμούς και γίνονται αντιληπτοί ολοένα και δυσκολότερα από τις διάφορες λύσεις ασφαλείας. Για παράδειγμα, υπάρχουν διάφορες απειλές και κίνδυνοι που μπορούν να προσπεράσουν το τείχος ασφαλείας. Σε ένα τέτοιο παράδειγμα δεν είναι μόνο το γεγονός ότι η επίθεση προσπέρασε το τείχος ασφαλείας, αλλά το γεγονός ότι δεν έγινε αντιληπτή, δεν γνωρίζουμε τον τύπο της επίθεσης και σίγουρα θα υπάρξουν σημαντικές συνέπειες σε ευαίσθητα δεδομένα και πληροφοριακά συστήματα. Επιπροσθέτως, σε περιπτώσεις που η ομάδα διαχείρισης του δικτύου δεν έχει την απαραίτητη γνώση για τον εντοπισμό και την αποτροπή της επίθεσης, δυστυχώς δεν θα έχει πολλές επιλογές ώστε να αποφύγει τυχόν ζημιές που μπορεί να προκληθούν.

Γι αυτούς τους λόγους, οι στόχοι που πρέπει να πραγματοποιηθούν αφορούν αρχικά την σωστή και δίκαιη θέσπιση και εφαρμογή κανόνων. Είναι πολύ σημαντικό, οι εσωτερικοί και εξωτερικοί παράγοντες που αλληλεπιδρούν με το δίκτυο καθώς και τις υπηρεσίες που παρέχει το τμήμα, να χρησιμοποιούνται με σωστό και ηθικό τρόπο απέναντι στο τμήμα και την ομάδα διαχείρισης δικτύου για την αποφυγή διώξεων και δυσφήμισης του τμήματος. Ακόμα ένας σημαντικός στόχος είναι η κατανόηση, η μελέτη, η αναγνώριση και τελικά η ανταπόκριση ευπαθειών και κινδύνων που εξελίσσονται στο δίκτυο. Θα πρέπει να είμαστε σε θέση να μπορούμε να ανταπεξέλθουμε στα περισσότερα περιστατικά που θα τύχει να εξελιχθούν.

## 1.3 Επιτεύγματα

Με την εκπόνηση της παρούσας πτυχιακής εργασίας επιτεύχθηκαν σημαντικά αποτελέσματα, τόσο σε θεωρητικό όσο και σε πρακτικό επίπεδο, με σκοπό την κατανόηση των τεχνολογιών SIEM καθώς και τον τρόπο με τον οποίο διαχειρίζονται περιστατικά ασφαλείας.

Πιο συγκεκριμένα, σε θεωρητικό επίπεδο πραγματοποιείται μια λεπτομερής ανάλυση σχετικά με τον ορισμό, τα θετικά και αρνητικά χαρακτηριστικά, τα οφέλη του SIEM καθώς και συγκριτική ανάλυση με προγενέστερες τεχνολογίες ασφαλείας όπως τα IDS. Επίσης γίνεται αναφορά στην σημαντικότητα

των πόρων, του εκπαιδευτικού υπόβαθρου και των στόχων που θέλουμε να πετύχουμε με την ενσωμάτωση μιας τέτοιας τεχνολογίας σε ένα γενικότερο επίπεδο.

Εν συνεχεία ακολουθεί μια αναλυτική περιγραφή και σύγκριση τεχνολογιών SIEM. Πραγματοποιείται μια λεπτομερής αξιολόγηση ανάμεσα στις τεχνολογίες OSSEC, OSSIM, SNORT και Wazuh βασισμένη στα τεχνικά χαρακτηριστικά και τις λειτουργικές τους ικανότητες.

Το πιο σημαντικό κομμάτι της πτυχιακής εργασία είναι το πρακτικό κομμάτι της, καθώς δημιουργήθηκε ένα πειραματικό περιβάλλον προσομοίωσης και διαχείρισης επιθέσεων. Σε αυτό το σημείο καταφέραμε να καταγράψουμε περιστατικά ασφαλείας, να δημιουργήσουμε ειδοποιήσεις και να παρατηρήσουμε σε πραγματικό χρόνο την εξέλιξη ενός κινδύνου.

Τέλος όλα τα παραπάνω επιτεύγματα βοήθησαν πλήρως στην κατανόηση, την εξοικείωση και την εκπαίδευση, έστω και σε ένα πρώτο στάδιο, σε τεχνολογίες SIEM. Με την βοήθεια τους μπορούμε να θέσουμε ως στόχο την πλήρη ενσωμάτωση και αλληλεπίδραση της τεχνολογίας SIEM με το περιβάλλον διαχείρισης και συστημάτων ασφαλείας του ΜΠΗΣ.

## 1.4 Διάρθρωση της πτυχιακής εργασίας

Η παρούσα πτυχιακή εργασία διαρθρώνεται σε τεσσερα κεφάλαια κατά τα οποία καλύπτονται τόσο σε θεωρητικό επίπεδο τεχνολογίες SIEM, όσο και σε πρακτικό επίπεδο με την εφαρμογή πειραματικού περιβάλλοντος για τις ανάγκες προβολής αποτελεσμάτων. Πιο αναλυτικά:

- Κεφάλαιο 1 : Εισαγωγη : Στο πρώτο κεφάλαιο της πτυχιακής εργασίας πραγματοποιείται η παρουσίαση του θέματος της πτυχιακής εργασίας, των στόχων και την αναγκαιότητα που προκύπτει κατά την ενσωμάτωση τεχνολογιών SIEM σε δίκτυα. Επίσης, πραγματοποιείται μια αναφορά σχετικά με τις υπηρεσίες και την τρέχουσα κατάσταση ασφαλείας και υπηρεσιών που παρέχει το τμήμα καθώς και το πόσο σημαντική είναι η ενσωμάτωση μιας τέτοιας τεχνολογίας απέναντι σε κακόβουλες ενέργειες εντός του οργανισμού.
- Κεφάλαιο 2 : Τεχνολογίες SIEM : Το δεύτερο κεφάλαιο μας αναφέρει τον ορισμό των SIEM τεχνολογιών. Γίνετε λεπτομερής αναφορά των θετικών και αρνητικών τους χαρακτηριστικών, πως μπορούν να ωφελήσουν καθώς και με τι προκλήσεις μπορεί να έρθουμε αντιμέτωποι. Επίσης γίνεται αντίστοιχη αναφορά στις τεχνολογίες IDS και σύγκριση τους με τις τεχνολογίες SIEM. Τέλος πραγματοποιείται μια ανάλυση χαρακτηριστικών και σύγκριση ανάμεσα στις τεχνολογίες OSSEC, OSSIM, SNORT και Wazuh. Τέλος, εφόσον γίνει μια αξιολόγηση των χαρακτηριστικών που θέλουμε να ενσωματωθούν με την προσθήκη μιας τεχνολογίας SIEM, πραγματοποιείται και η επιλογή της αντίστοιχης τεχνολογίας για περαιτέρω πειραματισμό.
- Κεφάλαιο 3 : Ενσωμάτωση και πειραματισμός με το Wazuh : Στο τρίτο κεφάλαιο επικεντρωνόμαστε πλέον στο πρακτικό κομμάτι της πτυχιακής εργασίας. Βάση της τελικής μας επιλογής, δηλαδή της τεχνολογίας Wazuh, πραγματοποιείται η ανάλυση και η παρουσίαση της διαδικασίας εγκατάστασης του Wazuh, του Wazuh Agent καθώς και όλων των απαραίτητων εργαλείων που χρησιμοποιήθηκαν για την δημιουργία ενός περιβάλλοντος προσομοίωσης επιθέσεων. Επίσης γίνεται μια πιο λεπτομερής περιγραφή ορισμένων εργαλείων που χρησιμοποιήθηκαν καθώς και δοκιμές προσομοίωσης επίθεσης για την αξιολόγηση της αποτελεσματικότητας του.
- Κεφάλαιο 4 : Συμπεράσματα και προτάσεις βελτίωσης : Το τέταρτο και τελευταίο κεφάλαιο περιλαμβάνει τα συμπεράσματα και τα αποτελέσματα που προέκυψαν από την μελέτη και την εφαρμογή των τεχνολογιών SIEM. Επιπροσθέτως παρουσιάζονται σημαντικά επιτεύγματα της εργασίας, οφέλη που μπορούν να ενισχύσουν τα μέτρα προστασία και ασφάλειας του

τμήματος, καθώς και προτάσεις για μελλοντική αξιοποίηση, επέκταση και συνύπαρξη της τεχνολογίας με άλλα εργαλεία ασφάλειας και υλοποίηση σε μεγαλύτερη κλίμακα.

## 1.5 Συμπεράσματα

Με την ανάλυση του πρώτου κεφαλαίου πραγματοποιείται η ανάδειξη των ζητημάτων ασφαλείας που έρχονται αντιμέτωπα τα πληροφοριακά συστήματα και δίκτυα, ειδικότερα σε περιβάλλοντα όπως το τμήμα ΜΠΗΣ. Είναι σαφές πως ένας οργανισμός όπως το τμήμα ΜΠΗΣ, παρέχει ικανά και αξιόπιστα συστήματα ασφαλείας, ωστόσο η συνεχής εξέλιξη και η πολυπλοκότητα που αποκτούν οι κυβερνοεπιθέσεις καθημερινά, απαιτούν πιο ισχυρές λύσεις ασφαλείας.

Οι τεχνολογίες SIEM αποτελούν μια ισχυρή και αξιόπιστη λύση ασφαλείας, καθώς παρέχουν από την φύση τους την δυνατότητα ανίχνευσης, καταγραφής και αποτροπής επιθέσεων σε πραγματικό χρόνο, ενισχύοντας σημαντικά την ανταπόκριση των συστημάτων ασφαλείας απέναντι σε κινδύνους. Πέρα από την αναφορά κινδύνων που προέρχονται από παράγοντες εκτός δικτύου του τμήματος, αναφορά γίνεται και για παράγοντες εντός δικτύου για την έμφαση στην δημιουργία κανόνων με σκοπό την συμμόρφωση των χρηστών απέναντι στις υπηρεσίες που τους παρέχονται.

Οι στόχοι που θέσαμε παίζουν πολύ σημαντικό ρόλο για την προσέγγιση του πλαισίου ασφαλείας που θέλουμε να δημιουργήσουμε. Μέσω της ανάλυσης τεχνολογιών, τεχνικών χαρακτηριστικών, ενσωμάτωση και πειραματισμό, παρακολούθηση κακόβουλων δραστηριοτήτων και λήψη των κατάλληλων μέτρων πρόληψης, δημιουργείται ένα υπόβαθρο στο οποίο οικοδομείται η παρούσα πτυχιακή εργασία.

Τέλος, το πρώτο κεφάλαιο λειτουργεί ως αφετηρία για την μελέτη και καταγραφή των τεχνολογιών SIEM σε θεωρητικό επίπεδο και συνεχίζει με την εφαρμογή πειραμάτων για την τελική αξιολόγηση των επιδόσεων τους.

# Κεφάλαιο 2ο: Τεχνολογίες SIEM

## 2.1 Εισαγωγή

Σε έναν οργανισμό με μεγάλο αριθμό υπολογιστικών συστημάτων όπου η χρήση του διαδικτύου αποτελεί ζωτική σημασία για την παροχή υπηρεσιών, τόσο εντός του οργανισμού όσο και εκτός αυτού, είναι πολύ σημαντικό να υπάρχουν τα κατάλληλα εργαλεία για την άμεση ανάλυση και ανταπόκριση σε περιπτώσεις κυβερνοεπιθέσεων. Ένα τέτοιο εργαλείο που συνδέεται απόλυτα με τα χαρακτηριστικά που αναφέραμε είναι το SIEM.

## 2.2 Ορισμός SIEM

Το SIEM (**Security Information and Event Management**) είναι ένα λογισμικό το οποίο χρησιμοποιείται για τον εντοπισμό, την ανάλυση και την απόκριση σε διάφορες απειλές που μπορεί να προκληθούν σε έναν οργανισμό προτού αυτές οι απειλές προλάβουν να προκαλέσουν οποιαδήποτε ζημιά σε αυτόν. Το βασικό χαρακτηριστικό του SIEM είναι ο συνδυασμός των τεχνολογιών SIM και SEM.

### 2.2.1 Ορισμός και χαρακτηριστικά τεχνολογιών SIM και SEM

Το SIM (Security Information Management) είναι ένα σύστημα που χρησιμοποιείται για την συλλογή, αποθήκευση και ανάλυση δεδομένων ασφαλείας από οποιοδήποτε σημείο κατά μήκος του δικτύου. Στόχος του SIM, μέσω των διαδικασιών που εκτελεί, είναι η διαμόρφωση μιας πλήρης εικόνας για την κατάσταση ασφαλείας που επικρατεί σε έναν οργανισμό. [1]

Το SEM (Security Event Management) είναι ένα σύστημα που χρησιμοποιείται για την συλλογή και ανάλυση συμβάντων ασφαλείας που εξελίσσονται καθώς και την αποστολή ειδοποιήσεων στην ομάδα διαχείρισης του δικτύου για την άμεση λήψη μέτρων προστασίας. Με αυτό τον τρόπο, το SEM μπορεί να συμβάλλει τόσο στην άμεση εξουδετέρωση ενός κινδύνου που εξελίσσεται στο δίκτυο, όσο και στην ανακάλυψη ευπαθειών που υπάρχουν στα μέτρα προστασίας που έχει καθορίσει η ομάδα διαχείρισης. [1]

Η συνύπαρξη των δύο αυτών τεχνολογιών είναι απαραίτητη και από τις δύο μεριές. Επειδή το SEM παρέχει την δυνατότητα αποστολής ειδοποιήσεων, ενω το SIM όχι, δεν σημαίνει πως το SIM είναι αχρείαστο. Αντίθετα και οι δύο αυτές τεχνολογίες είναι εξίσου σημαντικές και απαραίτητες για την σύνθεση και την λειτουργία του SIEM. Συνοπτικά [1]:

- Το SIM χρησιμοποιείται για την συλλογή, αρχειοθέτηση και αναφορά περιστατικών ασφαλείας
- Το SEM χρησιμοποιείται για την συλλογή και συσχέτιση δεδομένων ασφαλείας καθώς και αναφορά σε πραγματικό χρόνο σε περιπτώσεις εντοπισμού ανωμαλιών στα δεδομένα ή εντοπισμού απειλής που εξελίσσεται.

### 2.2.2 Βασικά Οφέλη Τεχνολογιών SIEM

Το βασικότερο όφελος που προσφέρουν οι τεχνολογίες SIEM κατά την ενσωμάτωση τους σε έναν οργανισμό είναι η δημιουργία μιας πιο σφαιρικής και πιο ξεκάθαρης εικόνας των συμβάντων ασφαλείας που εξελίσσονται στο δίκτυο. Η συγκέντρωση δεδομένων καταγραφής από πολλά

διαφορετικά συστήματα του δικτύου ,που μπορεί να αφορούν πληροφοριακά συστήματα μέχρι λειτουργικά συστήματα και εφαρμογές, και η ανάλυση όλων αυτών των δεδομένων, αποτελούν τα βασικά χαρακτηριστικά ώστε το σύστημα SIEM να είναι σε θέση να εντοπίσει και να αποτρέψει τυχόν ευπάθειες ή επιθέσεις που εξελίσσονται ανάμεσα τους. Λόγο της φύσης του SIEM, να μπορεί να διεισδύει σε όλους τους σταθμούς ενός δικτύου, δίνετε η δυνατότητα αναγνώρισης νέων ευπαθειών και επιθέσεων που μέχρι πρότινος δεν μπορούσαν να εντοπιστούν από άλλα εργαλεία ασφάλειας. Αυτό επιτυγχάνεται λόγο του πεδίου ορατότητας που αποκτά, το οποίο εκτείνεται σε όλα τα μέρη του οργανισμού. Επιπροσθέτως, ένα από τα βασικότερα οφέλη που προσφέρουν οι περισσότερες τεχνολογίες SIEM είναι η δυνατότητα αποτροπής επιθέσεων σε πραγματικό χρόνο. Το χαρακτηριστικό αυτό αποτελεί υψηλης σημασίας καθώς είναι πολύ σημαντικό να υπάρχει συνεχής ενημέρωση για την εξέλιξη των δεδομένων του δικτύου και να υπάρξει άμεση ανταπόκριση σε περιπτώσεις επιθέσεων.

### 2.2.3 Πλεονεκτήματα τεχνολογιών SIEM

Μπορούμε να καταλάβουμε πως η ενσωμάτωση μιας SIEM τεχνολογίας σε έναν οργανισμό μπορεί να ωφελήσει σε μεγάλο βαθμό την ασφάλεια των πληροφοριακών συστημάτων και δεδομένων που εξελίσσονται μέσα στο δίκτυο. Για να μπορέσουμε να αιτιολογήσουμε όλα τα οφέλη που μπορούμε να αντλήσουμε από αυτή, θα πρέπει να γίνει μια λεπτομερή αναφορά στα πλεονεκτήματα της [2]:

- **Βελτιωμένη ανίχνευση περιστατικών ασφάλειας** : Οι τεχνολογίες SIEM ανιχνεύουν περιστατικά ασφαλείας με την μέθοδο συλλογής και ανάλυσης μεγάλου όγκου δεδομένων που εξελίσσονται σε πραγματικό χρόνο σε κάθε γωνία του δικτύου. Μέσω της ανάλυσης αυτών των δεδομένων, το SIEM είναι σε θέση να μπορεί να εντοπίσει μέχρι και μοτίβα ή τυχόν ανωμαλίες που μπορεί να υποδηλώνουν κάποια ενδεχόμενη απειλή. Έτσι μπορούμε να πούμε πως το SIEM δεν λειτουργεί μόνο με παραδοσιακές μεθόδους αλλά βελτιώνει ορατότητα των συστημάτων ασφαλείας και παρέχει μια πιο ολοκληρωμένη και καθαρή εικόνα στους διαχειριστές του δικτύου.
- **Αποτελεσματική αντιμετώπιση περιστατικών** : Οι τεχνολογίες SIEM παρέχουν την δυνατότητα αντιμετώπισης επιθέσεων σε πραγματικό χρόνο. Αυτό επιτυγχάνεται κατα τον εντοπισμό ενός περιστατικού ασφαλείας, όπου το SIEM με την δυνατότητα δημιουργίας ειδοποιήσεων επιτρέπει στο προσωπικό ασφαλείας να αντιδράσει την σωστή στιγμή στο σωστό σημείο. Με αυτόν τον τρόπο επιταχύνεται η διαδικασία εξάλειψης και αντιμετώπισης περιστατικών ελαχιστοποιόντας έτσι την πιθανότητα επιπτώσεων σε ενδεχόμενη παραβίαση ασφαλείας.
- **Ενισχυμένη διαχείριση στην συμμόρφωση με τους κανόνες ασφαλείας** : Τα συστήματα SIEM παρέχουν τα κατάλληλα εργαλεία και δυνατότητες για την παρακολούθηση, την αναφορά και την συμμόρφωση με βάση τα πρότυπα και τους κανόνες ασφαλείας που έχουμε θέσει. Με αυτόν τον τρόπο συμβάλλουν στον εντοπισμό κενών ασφαλείας του οργανισμού τεκμηριώνοντας πάντα με βάση την αναφορά περιστατικών και τελικά δημιουργούν αναφορές για την λήψη μέτρων συμμόρφωσης. Έτσι διασφαλίζουν ότι ο οργανισμός για τον οποίο έχουν ενσωματωθεί έχει μια ισχυρή στάση ασφαλείας ανάλογη με τους κανονισμούς που έχουν τεθεί.
- **Κεντρική διαχείριση δεδομένων ασφαλείας** : Όλα τα δεδομένα ασφαλείας που συλλέγονται από τις διάφορες πηγές του δικτύου μεταφέρονται σε ένα κεντρικό σύστημα. Με αυτόν τον τρόπο δεν χρειάζεται να γίνεται η ανάλυση και η διαχείριση του συμβάντος στο σημείο που επικρατεί. Έτσι εξαλείφεται η χειροκίνητη συλλογή και ανάλυση για κάθε σύστημα ξεχωριστά, πράγμα που εξοικονομεί χρόνο και προσπάθεια. Επίσης με την συγκέντρωση των δεδομένων σε ένα κεντρικό σημείο του δικτύου επιτυγχάνεται ευκολότερη διατήρηση των

δεδομένων και συγκέντρωση log καθώς και πιο άμεση και αποτελεσματική ανάλυση περιστατικών ασφαλείας.

- **Μειωμένο κόστος διαχείρισης ασφάλειας**: Οι τεχνολογίες SIEM μπορούν να συμβάλλουν στην εξοικονόμηση κόστους διαχείρισης ασφάλειας με πολλούς τρόπους:
    - Με την συλλογή και η ανάλυση δεδομένων από την στιγμή που γίνονται σε ένα κεντρικό σημείο του δικτύου, αυτοματοποιούν τις χειροκίνητες εργασίες που θα συναίβεναν σε άλλες περιπτώσεις.
    - Η παρακολούθηση σε πραγματικό χρόνο και η δυνατότητα ταχείας αντιμετώπισης περιστατικών συμβάλλουν στην αποφυγή πιθανών οικονομικών επιπτώσεων, παραβιάσεις προσωπικών δεδομένων αλλά και δεδομένων ασφαλείας ή ακόμα και διακοπή λειτουργίας κάποιου συστήματος. Έτσι ελαχιστοποιείται η πιθανότητα οικονομικής ζημίας ή δυσφήμηση.

### 2.2.4 Προκλήσεις κατά την χρήση τεχνολογιών SIEM

Παρόλα τα θετικά χαρακτηριστικά και οφέλη που προσφέρουν οι SIEM τεχνολογίες, πολλές φορές συνοδεύονται με χαρακτηριστικά που μπορεί να δυσκολέψουν κατά την διαδικασία ενσωμάτωσης είτε σε μελλοντικό χρόνο. Γι αυτό είναι απαραίτητη η αναφορά των αρνητικών αυτών χαρακτηριστικών [3]:

- **Πολυπλοκότητα διαμόρφωσης** : Θα πρέπει να κατανοήσουμε πως μια τεχνολογία SIEM δεν αποτελεί μια διαδικασία απλής εγκατάστασης και άμεσης εφαρμογής των δυνατοτήτων και λειτουργιών που παρέχει. Όσες περισσότερες είναι οι ανάγκες που θέλουμε να εξυπηρετήσουμε, τόσο πιο σύνθετη και επίπονη γίνεται η διαδικασία διαμόρφωσης του συστήματος. Ο καθορισμός των σημείων που θα αποτελέσουν πηγές για τα δεδομένα που θέλουμε να συλλέξουμε , η θέσπιση των κανόνων ασφαλείας και η ρύθμιση των ειδοποιήσεων που θέλουμε να λαμβάνουμε απαιτούν σχολαστική προσοχή και μεγάλη λεπτομέρεια. Πρέπει όσο γίνεται δυνατό να αποφευχθούν λάθη όπως ψευδή θετικά στοιχεία ή διαφυγή απειλών. Για αυτό τον λόγο θα πρέπει να γίνει μια σοβαρή επένδυση χρόνου και συνεχής μελέτη πάνω σε τέτοιου είδους τεχνολογίες για να διασφαλίσουμε τελικά ότι το σύστημα SIEM που έχουμε ενσωματώσει είναι σωστά και λεπτομερός ρυθμισμένο.
- **Εμπόδια ενσωμάτωσης** : Πριν από την ενσωμάτωση μιας SIEM τεχνολογίας θα πρέπει να υπάρξει μια σωστή αποτίμηση των δυνατοτήτων και των πόρων που διαθέτουν τα σύστημα και οι εφαρμογές που ανήκουν στο δίκτυό μας. Μια πιθανή έλλειψη συμβατότητας ενός σημείου μέσα στο δίκτυο μπορεί να αποδειχθεί μοιραία καθώς το SIEM δεν θα μπορεί να είναι σε θέση να δώσει μια ολοκληρωμένη εικόνα για το τι συμβαίνει σε αυτό το σημείο. Γι αυτό τον λόγο ένα πολύ σημαντικό στάδιο που θα πρέπει να εξετάσουμε είναι το κατά πόσο μπορεί να βασιστεί η τεχνολογία SIEM που θα επιλέξουμε με βάση τις υποδομές που παρέχονται.
- **Περιορισμοί πόρων** : Για την ενσωμάτωση μιας SIEM τεχνολογίας, απαιτείται η χρήση πολλών πόρων. Πιο συγκεκριμένα :
    - Χρόνος
    - Χρήμα
    - Εξειδικευμένο Προσωπικό

Αυτό αποτελεί πρόκληση για εμάς διότι δεν έχουμε μεγάλο και εξειδικευμένο προσωπικό καθώς και δεν έχουμε οικονομικές ανέσεις ίδιες όπως μιας μεγάλης επιχείρησης. Θα πρέπει να γίνει μια σωστή κατανομή απέναντι στις ανάγκες που θέλουμε να εξυπηρετήσουμε με βάση τους τομείς

που μας αφορούν περισσότερο έχοντας πάντα στο νου μας τους περιορισμούς που μπορούμε να συναντήσουμε απέναντι στους πόρους που διαθέτουμε.

- **Κρυφά κόστοι** : Με την πάροδο των χρόνων και με την ενσωμάτωση ολοένα και περισσότερων υπηρεσιών και συστημάτων στο δίκτυό μας, μπορεί να εμφανιστεί ένας όγκος δεδομένων που υπερβαίνει τις αρχικές μας προσδοκίες. Έτσι αναπτύσσοντας τις υπηρεσίες και τα συστήματα που χρησιμοποιούμε, μπορεί να πιαστούμε απροετοίμαστοι απέναντι σε νέα μεγέθη δεδομένων. Ως αποτέλεσμα ο οργανισμός μπορεί να επιβαρυνθεί τόσο στον τομέα του προϋπολογισμού, όσο και στο γεγονός διατάραξης κατά την διαδικασία υλοποίησης ενεργειών που εκτελεί το SIEM που έχουμε ενσωματώσει.
- **Προκλήσεις κατα την εισαγωγή δεδομένων** : Όλα τα σημεία και οι εφαρμογές που βρίσκονται στο δίκτυο μας, δεν έχουν ίδιες μορφές καταγραφής καθώς και δομής δεδομένων. Αυτό έχει ως αποτέλεσμα να δυσκολεύει σε μεγάλο βαθμό την δυσκολία κατά την διαδικασία κανονικοποίησης και τυποποίησης των δεδομένων. Χωρίς να έχουμε κάνει τις κατάλληλες κινήσεις για να ενσωματώσουμε τα δεδομένα με σωστό τρόπο, το SIEM μπορεί να μην μπορέσει να αναγνωρίσει σωστά τους κινδύνους που εξελίσσονται με αποτέλεσμα να βρεθούμε εκτεθειμένοι. Καλό θα ήταν να γίνει μια μελέτη για την σωστή ενσωμάτωση και διαχείριση διαφορετικών πηγών δεδομένων, ώστε να μπορέσει να μεγιστοποιηθεί η αξία της τεχνολογίας SIEM.
- **Περιορισμοί Επεκτασιμότητας** : Η ανάπτυξη ενός οργανισμού είναι ένα χαρακτηριστικό το οποίο θα συμβαίνει φυσικά όσο ο οργανισμός συνεχίσει να υπάρχει και συνεχίζει να εξελίσσεται. Δεν θα πρέπει να ξεχνάμε πως με την ανάπτυξη του αναπτύσσονται ταυτόχρονα και άλλες υπηρεσίες, υποδομές καθώς και μέθοδοι εισβολής σε συστήματα και εφαρμογές. Γι αυτό τον λόγο θα πρέπει να είμαστε σε θέση να γνωρίζουμε πως μαζί με την εξέλιξη του οργανισμού θα πρέπει ταυτόχρονα να υπάρχει η δυνατότητα επεκτασιμότητας της τεχνολογίας SIEM που έχουμε ενσωματώσει. Θα πρέπει να είναι σε θέση να μπορεί να υπερασπιστεί μεγαλύτερο όγκο δεδομένων και αναγκών που θέλουμε να καλύψουμε. Γι αυτό καλό θα ήταν να γνωρίζουμε το κατα πόσο μπορεί να επεκταθεί και να προσαρμοστεί η τεχνολογία SIEM που θα ενσωματώσουμε, στο μέλλον.
- **Κανονισμοί διατήρησης και συμμόρφωσης** : Τα συστήματα SIEM συλλέγουν έναν μεγάλο όγκο δεδομένων από πολλά σημεία εντός του δικτύου. Πέρα όμως από την συλλογή τους παρέχουν και την δυνατότητα διατήρησής αυτών των δεδομένων. Χωρίς την θέσπιση κανόνων για την διατήρηση αυτών των όγκων δεδομένων, ο οργανισμός μπορεί να υπερχειλίσει με δεδομένα τα οποία είναι πλέον αχρείαστα και ως αποτέλεσμα επιβαρύνουν το κόστος αποθήκευσης που είναι πολύ σημαντικό στοιχείο για έναν οργανισμό. Ο οργανισμός θα πρέπει να θέσει κάποιου κανόνες που σχετίζονται με την διατήρηση όλων αυτών των δεδομένων. Θα πρέπει να βρεθεί μια χρυσή τομή ώστε να γίνεται σωστή εκκαθαριση των αχρείαστων στοιχείων καθώς και σαφής διατήρηση των στοιχείων που είναι απαραίτητα για την συμμόρφωση.

Θα πρέπει να κατανοήσουμε πως η διαδικασία εγκατάστασης, διαμόρφωσης και διατήρησης μιας τεχνολογίας SIEM δεν αποτελούν μια εύκολη διαδικασία. Θα πρέπει να δώσουμε μεγάλη σημασία :

- Στις υπολογιστικές δυνατότητες των συστημάτων και εφαρμογών που χρησιμοποιούνται στο δικτυο μας.
- Στην σωστή μελέτη και ανάλυση των διαφόρων μορφών που έχουν τα δεδομένα μας στα διάφορα αυτά σημεία.
- Στην σταδιακή και ταυτόχρονη εξέλιξη των συστημάτων μας με την τεχνολογία SIEM
- Στο να κάνουμε έναν σωστό προϋπολογισμό του κόστους που μπορεί να χρειαστεί να έχουμε.

### 2.2.5 Τι θέλουμε να πετύχουμε

Η ενσωμάτωση μιας SIEM τεχνολογίας δεν αποτελεί μια απλή λύση ασφάλειας. Είναι μια τεχνολογία η οποία απαιτεί αφοσίωση, προσοχή στις λεπτομέρειες, σωστή θέσπιση κανόνων και συνεχή παρακολούθηση. Με την σωστή διαμόρφωση της, ένας οργανισμό μπορεί να επωφεληθεί σε μεγάλο βαθμό απέναντι σε θέματα ασφάλειας πληροφοριακών συστημάτων. Σίγουρα δεν θα πρέπει να αγνοήσουμε και αρνητικά χαρακτηριστικά και τις προκλήσεις που συνοδεύονται με την ενσωμάτωση της. Στόχοι κατα την ενσωμάτωσης της είναι:

- Αρχικά, ο βασικότερος λόγος που θέλουμε να ενσωματώσουμε μια τέτοια τεχνολογία στα συστήματα μας είναι για να έχουμε μια πλήρη εικόνα για το πόσο σωστά επιτυγχάνονται οι κανόνες ασφαλείας τους οποίους έχουμε θέσει. Είναι σημαντικό να κάνουμε πάντα μια αυτοκριτική στις διαμορφώσεις και τους κανόνες που έχουμε θέσει ώστε να είμαστε πάντα σε θέση να μπορούμε να ανταπεξέλθουμε σε οποιαδήποτε ευπάθεια ή να ανακαλύψουμε κάποιο κενό σημείο που μας ξέφυγε. Με αυτό τον τρόπο είμαστε πιο ξεκάθαροι απέναντι στις επιλογές που θέλουμε να πάρουμε και μπορούμε να είμαστε σε θέση να γνωρίζουμε ακριβώς που θα πρέπει να δώσουμε την απαραίτητη προσοχή.
- Επίσης θα γνωρίσουμε καλύτερα τις ελλείψεις που μπορεί να υπάρχουν στα συστήματα μας. Είναι σημαντικό να γνωρίζουμε ποιες είναι οι δυνατότητες που μας παρέχονται για να μπορέσουμε να πετύχουμε τις επιθυμητές αλλαγές και αναπτύξεις τόσο στα συστήματα όσο και στις δυνατότητες που μπορεί να αναπτύξει το SIEM.
- Θα μπορούμε να γνωρίζουμε την εξέλιξη των γεγονότων σε πραγματικό χρόνο. Είναι πολύ σημαντικό όταν αναφερόμαστε σε ένα πανεπιστημιακό τμήμα , το οποίο απαρτίζεται από έναν μεγάλο αριθμό φοιτητών και καθηγητών να εξασφαλίζεται η ασφάλεια των προσωπικών τους δεδομένων. Επίσης υπάρχουν πολλές υπηρεσίες, όπως η υπηρεσία vpn του τμήματος, οι οποίες παρέχονται δωρεάν όμως πρέπει να τηρούνται κάποιοι κανόνες. Με την ενσωμάτωση μιας SIEM τεχνολογίας, μέσω της δυνατότητας ειδοποίησης για τυχόν απειλές ή παραβίασης κανόνων ασφαλείας, μπορούμε να λαμβάνουμε εγκαίρως τα κατάλληλα μέτρα προστασίας, να αποφεύγουμε εγκαίρως ενδεχόμενους κινδύνους καθώς και να επισημαίνουμε με μεγαλύτερη ακρίβεια τους κανόνες συμμόρφωσης.

### 2.2.6 Τύποι τεχνολογιών SIEM[4]

- **Open Source SIEM :** Οι ανοιχτού κώδικα λύσεις SIEM αποτελούν μια πολύ καλή λύση για οργανισμούς που θέλουν να κάνουν το ξεκίνημα τους στην ενσωμάτωση τεχνολογιών ανάλυσης και αποτροπής επιθέσεων. Το περιβάλλον τους είναι ιδανικό για να μπορέσουν να γίνουν τα κατάλληλα πειράματα ώστε να μπορέσουμε να καταλάβουμε πραγματικά τι θα χρειαστεί να παρακολουθούμε καθώς και με ποιόν τρόπο θα πρέπει να αναλάβουμε δράση κατά τον εντοπισμό κακόβουλης συμπεριφοράς. Ωστόσο με την πάροδο του χρόνου και με την αύξηση των αναγκών που μπορεί να εμφανιστούν μελλοντικά, ολοένα και θα αυξάνεται ο βαθμός δυσκολίας και απαιτήσεων.
- **Free SIEM :** Οι δωρεάν λύσεις SIEM βοηθούν αρκετά στον προϋπολογισμό ενός οργανισμού τόσο σε επίπεδο κόστους και πόρων όσο και σε επίπεδο φιλικότητας και ευκολίας προς νέους χρήστες. Ωστόσο δεν μπορούν να αποτελέσουν μια σταθερή λύση για έναν οργανισμό καθώς ο αριθμός των εργαλείων που προσφέρουν είναι περιορισμένος. Γι αυτό σίγουρα σε ένα ξεκίνημα μπορούν να βοηθήσουν στην κατανόηση και ενασχόληση στον τομέα της αποτροπής

επιθέσεων όμως μελλοντικά είναι σχεδόν σίγουρο ότι θα χρειαστεί η αντικατάσταση τους με κάποια άλλη πιο ισχυρή επιλογή.

- **Enterprise SIEM** : Οι επιχειρησιακές λύσεις SIEM , όπως μπορούμε να καταλάβουμε από την ονομασία τους, παρέχουν ένα μεγάλο όγκο εργαλείων, πολύ ισχυρά χαρακτηριστικά, ευκολία στην χρήση καθώς και πολύ καλή τεχνική υποστήριξη. Παρόλες τις πολλές δυνατότητες που μπορούν να προσφέρουν, δεν τις καθιστά φιλικές απέναντι σε όλους τους οργανισμούς. Πολλά εργαλεία που προσφέρουν αυτές οι τεχνολογίες απευθύνονται καθαρά σε οργανισμούς μεγάλου μεγέθους. Ενσωματώνοντας μια τέτοια τεχνολογία σε οργανισμούς μικρότερου βεληνεκούς αποδεικνύεται πως αποτελούν πολύ δαπανηρές λύσεις.

Έχοντας λοιπόν αναφέρει τα χαρακτηριστικά και τις δυνατότητες κάθε λύσης SIEM που μπορούμε να χρησιμοποιήσουμε θα πρέπει να αναλογιστούμε τα εξής πριν ενσωματώσουμε οποιαδήποτε λύση :

- Το κόστος και τους πόρους που μπορούμε να διαθέσουμε.
- Το πόσο έμπειροι ή όχι είμαστε απέναντι σε συστήματα αποτροπής επιθέσεων.
- Ποιές ανάγκες θέλουμε να εξυπηρετήσουμε.

## 2.3 Intrusion Detection Systems

### 2.3.1 Ορισμός IDS

Το IDS (Intrusion detection system) αποτελεί ένα εργαλείο ασφάλειας πληροφοριακών συστημάτων το οποίο χρησιμοποιείται για την παρακολούθηση ύποπτης, κακόβουλης η ακόμα και παραβίασης της πολιτικής ασφαλείας του δικτύου ενός οργανισμού. Πρακτικά ένα IDS συλλέγει πληροφορίες από πολλούς και διάφορους σταθμούς του δικτύου και πραγματοποιεί διαγνώσεις για τυχόν παραβιάσεις του. Βασικός του στόχος είναι η ανακάλυψη παραβιάσεων, απόπειρες κακόβουλης επίθεσης, ύποπτες κινήσεις καθώς και τελικά η ανακάλυψη ορισμένων ανοιχτών ευπαθειών που θα μπορούσαμε να λάβουμε εγκαίρως μέτρα προστασίας. Για την επιτευξη της λειτουργικότητας και της απόδοσης του χρησιμοποιεί τρία είδη πληροφοριών [5]:

- Μακροπρόθεσμες πληροφορίες σχετικά με τις τεχνικές που χρησιμοποιήθηκαν στον παρελθόν για τον εντοπισμό εισβολών.
- Πληροφορίες διαμόρφωσης που αφορούν την τωρινή κατάσταση διαμόρφωσης των συστημάτων.
- Πληροφορίες ελέγχου που αφορούν τις διαμορφώσεις που εξελίσσονται από στιγμή σε στιγμή στα συστήματα μας.

Σημαντική προϋπόθεση για την κατανόηση και τον λόγο που εξετάζουμε τέτοιου είδους συστήματα, είναι να αναλύσουμε κάποια είδη εισβολών που μπορούμε να δεχτούμε: https://neuro.bstu.by/ai/To-dom/My_research/Paper-0-again/For-research/D-mining/Anomaly-D/Intrusion-detection/Intrusion-Detection-Intro.pdf

- Απόπειρες διαρρήξεων σε συστήματα του δικτύου
- Διείσδυση σε συστήματα ασφαλείας
- Διαρροές δεδομένων
- Άρνηση παροχής υπηρεσιών (DoS)
- Κακόβουλη και καταχρηστική χρήση συστημάτων και υπηρεσιών.

Οι τεχνικές που χρησιμοποιούνται για τα συστήματα ανίχνευσης εισβολών είναι οι εξής [6]:

- Anomaly Detection: Όπως προδίδει και η ονομασία της, η τεχνική αυτή αφορά στην ανίχνευση σημείων, δεδομένων και πληροφοριών που εμφανίζουν διάφορες ανωμαλίες σε σχέση με το υπόλοιπο σύνολο δεδομένων που γνωρίζουμε. Ωστόσο ένα μεγάλο ελάττωμα αυτής της τεχνικής είναι ότι πολλές φορές οι ανωμαλίες που μπορεί να εμφανιστούν ενδέχεται να μην αποτελούν απαραίτητα κακόβουλη χρήση όμως να επισημαίνονται ως κακόβουλες καθώς και το αντίθετο. Επίσης είναι μια αρκετά κοστοβόρα υπολογιστικά τεχνική λόγω της συνεχής παρακολούθησης και ενημέρωσης πολλών μετρήσεων των συστημάτων
- Misuse ή Signature Detection : Η τεχνική αυτή ακολουθεί την προσέγγιση εκμάθησης μοτίβων επιθέσεων η μη εξουσιοδοτημένης δραστηριότητας σε σύγκριση με προηγούμενες δραστηριότητες και έχει τελικά ως στόχο τον εντοπισμό η και ακόμα την πρόβλεψη ενός νέου μοτίβου επίθεσης στο δίκτυο μας. Το βασικό μειονέκτημα αυτής της τεχνικής είναι πως θα πρέπει να συντάξουμε ένα signature το οποίο θα πρέπει να περιλαμβάνει όλα τα πιθανά μοτίβα μιας επίθεσης καθώς και να γραφτούν τα αντίστοιχα signatures τα οποία δεν αποτελούν μοτίβα κακόβουλης δραστηριότητας.

### 2.3.2 Τύποι συστημάτων IDS

Τα συστήματα IDS χωρίζονται 5 διαφορετικούς τύπους ανάλογα με τις ανάγκες που θέλουμε να εξυπηρετήσουμε. Έτσι έχουμε τους εξής 5 τύπους [7]:

- **Network Intrusion Detection System (NIDS) :** Τα **Network Intrusion Detection Systems** ενσωματώνονται σε ένα συγκεκριμένο σημείο του δικτύου με σκοπό την εξέταση της κυκλοφορίας των δεδομένων που αποστέλλονται από όλες τις συσκευές του δικτύου. Πρακτικά η μέθοδος που ακολουθεί είναι η παρατήρηση της διερχόμενης κυκλοφορίας των δεδομένων που εξελίσσεται κατά μήκος όλως των υποδικτύων του δικτύου μας κάνοντας ταυτόχρονα τις απαραίτητες αντιστοιχίες με την συλλογή γνωστών επιθέσεων. Στην περίπτωση ανακάλυψης μίας επίθεσης, ανωμαλίας ή κακής συμπεριφοράς είναι διατεθειμένο ειδοποιήσει έγκαιρα τους διαχειριστές του δικτύου. Ένα σημείο όπου θα μπορούσε να εγκατασταθεί ένα τέτοιο σύστημα είναι το σημείο που βρίσκονται τα τείχη προστασίας του δικτύου ώστε να μπορέσει να αποτρέψει οποιαδήποτε προσπάθεια κατεδάφισης του.
- **Host Intrusion Detection System (HIDS) :** Τα **Host Intrusion Detection Systems** μπορούν να εγκατασταθούν σε ανεξάρτητους κεντρικούς υπολογιστές ή γενικότερα ανεξάρτητες συσκευές ενός δικτύου. Η σημαντική διαφορά με τα **Network Intrusion Detection Systems** είναι ότι σε αυτή την περίπτωση ο έλεγχος και η παρακολούθηση της κυκλοφορίας των εισερχόμενων και εξερχόμενων πακέτων που εναλλάσσονται αφορούν αποκλειστικά την συσκευή που έχει εγκατασταθεί. Ουσιαστικά τα συστήματα αυτά λειτουργούν σε πιο ατομικό επίπεδο. Ο τρόπος με τον οποίο λειτουργεί είναι μέσω την συλλογής αρχείων του συστήματος στην τωρινή τους κατάσταση και εν συνεχεία τα συγκρίνει με παλαιότερες τους εκδόσεις. Σκοπός τους είναι μέσω της σύγκρισης και εφόσον τα αρχεία αυτά έχουν υποστεί επεξεργασία ή ενδεχόμενη διαγραφή, να είναι σε θέση να ειδοποιήσουν εγκαίρως τον διαχειριστή για περαιτέρω παρατήρηση της κατάστασης τους. Τέτοια, λοιπόν, συστήματα μπορούν να χρησιμοποιηθούν σε μηχανήματα τα οποία αποτελούνται από δεδομένα που δεν απαιτούν επεξεργασία και δεν χρειάζεται να αλλάξει η διάταξη τους.
- **Protocol-Based Intrusion Detection System (PIDS) :** Τα **Protocol-Based Intrusion Detection Systems** όπως προδίδει και η ονομασία τους βασίζονται στην ανίχνευση εισβολών βάσει πρωτοκόλλων. Πιο συγκεκριμένα, η ενσωμάτωση του περιλαμβάνει ένα σύστημα ή έναν πράκτορα ο οποίος βρίσκεται σταθερά στο μπροστινό μέρος ενός διακομιστή. Στην συνέχεια οι ενέργειες που ακολουθεί είναι ο έλεγχος και η ερμηνεία της επικοινωνίας που

εξελίσσεται βάσει του πρωτοκόλλου που χρησιμοποιείται ανάμεσα στην συσκευή και τον διακομιστή.

- **Application Protocol-Based Intrusion Detection System (APIDS) :** Τα **Application Protocol-Based Intrusion Detection Systems** χρησιμοποιούνται για την ανίχνευση εισβολών βάσει πρωτοκόλλων εφαρμογής με την χρήση ενός πράκτορα ο οποίος βρίσκεται ανάμεσα σε μια ομάδα πολλών διακομιστών. Εντοπίζει και ερμηνεύει την επικοινωνία που εξελίσσεται σε διάφορα πρωτόκολλα εφαρμογών όπως το πρωτόκολλο SQL.
- **Hybrid Intrusion Detection System** : Τα **Hybrid Intrusion Detection Systems** δημιουργούνται από τον συνδυασμό δύο ή περισσότερων από τις προσεγγίσεις που αναφέραμε παραπάνω. Έτσι μπορούμε να καταλάβουμε ότι συνδυάζοντας προσεγγίσεις έχουμε μια πιο μεγάλη και ξεκάθαρη εικόνα στο τι πραγματικά συμβαίνει σε πολλά σημεία του δικτύου. Γι αυτό τον λόγο μπορούμε να καταλάβουμε πως αποτελεί την πιο αποτελεσματική λύση συγκριτικά με τις υπόλοιπες που αναφέραμε.

### 2.3.3 Βασικά οφέλη IDS τεχνολογιών

Έχοντας αναφέρει σε ένα γενικό πλαίσιο για το τι είναι ένα IDS και έχοντας αναφέρει του διάφορους τύπου του, θα πρέπει να αναφέρουμε το τι μπορούμε να επωφεληθούμε κατα την ενσωμάτωσή τους [7]:

- Τα IDS συστήματα μπορούν να ανιχνεύσουν οποιαδήποτε κακόβουλη δραστηριότητα και να ειδοποιήσουν εγκαίρως τους διαχειριστές των συστημάτων πριν προκληθεί ζημιά σε κάποιο υπολογιστικό σύστημα ή λογισμικό κατά μήκος όλου του δικτύου.
- Τα IDS συστήματα μπορούν να ελέγξουν για τυχόν προβλήματα που αφορούν στην απόδοση του δικτύου καθώς και να τα αντιμετωπίσουν.
- Τα IDS συστήματα μπορούν να παράξουν πληροφορίες σχετικά με την κυκλοφορία του δικτύου. Αυτό σημαίνει πως έχοντας τις απαραίτητες πληροφορίες για τις κινήσεις που εξελίσσονται στο δίκτυό μας, μπορούμε να τις χρησιμοποιήσουμε για να εντοπίσουμε τυχόν αδυναμίες ή ευπάθειες και εν συνεχεία να κάνουμε τις απαραίτητες κινήσεις για την εξάλειψη τους καθώς και για την βελτίωση της ασφάλειας του δικτύου μας.

### 2.3.4 Πλεονεκτήματα των IDS τεχνολογιών

Προηγουμένως αναφέραμε τα οφέλη που μπορούμε να εκμεταλλευτούμε με την χρήση ενός IDS. Για να κάνουμε όμως την θέση μας πιο συγκεκριμένη θα πρέπει να κάνουμε αναφορά στα θετικά χαρακτηριστικά που πετυχαίνουμε κατα την ενσωμάτωσή του [7]:

- **Γρήγορη απόκριση:** Τα συστήματα IDS βοηθούν στην γρήγορη ανίχνευση πιθανών επιθέσεων ώστε να υπάρξει άμεση ανταπόκριση από τους διαχειριστές για την αποφυγή οποιασδήποτε ζημιάς ή κινδύνου απέναντι στα συστήματα του δικτύου.
- **Ενίσχυση των ήδη υπάρχων εργαλείων προστασίας:** Τα συστήματα IDS παρέχουν μια πιο ενισχυμένη υποστήριξη η οποία ενσωματώνεται σε διαφορετικά μέτρα ασφαλείας που αφορούν τον τομέα του κυβερνοχώρου ώστε να παράξει μια πιο ολοκληρωμένη προστασία απέναντι σε κυβερνοεπιθέσεις.
- **Συνεχής παρακολούθηση κυκλοφορίας δεδομένων στο δίκτυο:** Μια σημαντική λειτουργία τους είναι η συνεχής παρακολούθηση της ροής των δεδομένων του δικτύου για πιθανές ανωμαλίες και ασυνήθιστες ενέργειες που εξελίσσονται σε αυτό. Με αυτόν τον τρόπο εξασφαλίζεται μια συνεχής επαγρύπνηση σε περιπτώσεις όπου μπορεί να εμφανιστεί οποιαδήποτε απειλή.

- **Λεπτομερείς αναφορές περιστατικών:** Παρόλο που τα συστήματα IDS δεν αναλαμβάνουν δράση απέναντι στις επιθέσεις που έχουν εντοπίσει, παρέχουν λεπτομερείς ειδοποιήσεις και αρχεία καταγραφής σχετικά με την φύση, τα χαρακτηριστικά και το σημείο της επίθεσης που εντόπισαν. Με αυτό τον τρόπο βοηθούν τους διαχειριστές του δικτύου να ενεργήσουν πιο στοχευμένα και αποδοτικά απέναντι στην απειλή που εξελίσσεται στο δίκτυο τους.

### 2.3.5 Μειονεκτήματα των IDS τεχνολογιών

Σίγουρα μια τεχνολογία IDS έχει πολλά να προσφέρει σε ένα δίκτυο ενός οργανισμού. Πέρα από μια ενίσχυση που μπορεί να ενσωματωθεί σε διάφορα μέτρα προστασίας που ήδη έχουν ληφθεί με σκοπό την ανάπτυξή τους, μας δίνει την δυνατότητα να γνωρίσουμε καλύτερα τα σημεία του δικτύου μας που εμφανίζουν ευπάθειες και δεν έχουμε αφιερώσει τον χρόνο που τους αρμόζει να για εξασφαλίσουμε τα κατάλληλα μέτρα προστασίας που πρέπει να λάβουν. Ωστόσο, θα πρέπει να λαμβάνουμε πάντα υπόψη μας και τα αρνητικά χαρακτηριστικά που μπορεί να αντιμετωπίσουμε κατά την ενσωμάτωση τους στο δίκτυο μας [7]:

- **Ψευδείς Συναγερμοί:**Ένα από τα πιο σημαντικά αρνητικά χαρακτηριστικά που εμφανίζονται στις τεχνολογίες IDS καθώς και σε άλλες τεχνολογίες τέτοιου τύπου είναι η εμφανίσεις ψευδών συναγερμών. Υπάρχει η πιθανότητα να εμφανιστούν ειδοποιήσεις για δραστηριότητες οι οποίες δεν αποτελούν κίνδυνο, ωστόσο ένα τέτοιο γεγονός θα οδηγήσει σε περιττούς ελέγχους και ανησυχία. Στην περίπτωση που μπορεί να συμβαίνουν συνεχώς τέτοια περιστατικά, θα καταστήσει την ενσωμάτωση μιας τέτοιας τεχνολογίας μη λειτουργική και αποτελεσματική για την αναβάθμιση των υπηρεσιών ασφαλείας που θέλουμε να καλύψουμε.
- **Κατανάλωση Πόρων:** Κατά την ενσωμάτωση μιας τεχνολογίας IDS δεν θα πρέπει να πάρουμε αψήφιστα το μέγεθος των πόρων που θα χρειαστεί να χρησιμοποιηθουν. Τέτοιου είδους τεχνολογίες που παρακολουθούν και καταγράφουν ένα μεγάλο όγκο δεδομένων που κυκλοφορεί σε πολλά διαφορετικά σημεία του δικτύου, χρειάζεται να χρησιμοποιεί πολλούς πόρους των συστημάτων για να κάνει αποδοτικά την δουλειά του και αυτό μπορεί να έχει ως αποτέλεσμα την επιβράδυνση των αποδόσεων του δικτύου.
- **Απαιτητική και Χρονοβόρα Συντήρηση:** Σίγουρα μια τεχνολογία IDS, πέρα από τις αρχικές διαμορφώσεις που θα κάνουμε για να μπορέσει να ενσωματωθεί ανάλογα με τις ανάγκες μας στο δίκτυο, απαιτεί και τις κατάλληλες ενημερώσεις για να μπορεί να εξελίσσεται. Οι περιπτώσεις ενημέρωσης τους πρέπει να αποτελεί τακτική διαδικασία για να μπορουν να είναι σχεδόν πάντα αποτελεσματικές, όμως αποτελεί μια πολύ χρονοβόρα διαδικασία.
- **Ελλειψη δυνατότητας αποτροπής επιθέσεων:** Άλλο ένα πολύ σημαντικό αρνητικό χαρακτηριστικό είναι το γεγονός ότι οι τεχνολογίες IDS εντοπίζουν και ειδοποιούν τους διαχειριστές για ενδεχόμενες επιθέσεις ή ανωμαλίες που ανακάλυψαν, όμως δεν υπάρχει μηχανισμός αποτροπής επιθέσεων. Αυτό σημαίνει πως για να μπορούμε να έχουμε και την δυνατότητα αποτροπής επιθέσεων θα πρέπει να ληφθούν επιπλέον μέτρα προστασίας.
- **Επίπονη διαχείριση:** Η διαδικασία ρύθμισης και διαχείρισης ενός IDS αποτελεί μια πολύπλοκη και δύσκολη διαδικασία. Τέτοιου είδους τεχνολογίες, ανάλογα με τις ανάγκες και τους στόχους που θέλουμε να πετύχουμε, μπορεί να ανεβάσουν πολύ το επίπεδο δυσκολίας και πολλές φορές μπορεί να χρειάζεται ένα πολύ καλό μορφωτικό υπόβαθρο για να υποστηρίξει μια τέτοια τεχνολογία. Πράγμα που σημαίνει πως πολλές φορές μπορεί να μην ανταποκρίνονται σε χρήστες που κάνουν το ξεκίνημα τους σε τέτοιου είδους τεχνολογίες.

Για να μπορέσουμε να αξιολογήσουμε σωστά την αποτελεσματικότητα ενός IDS θα πρέπει να πληρούνται , εάν όχι στο εκατό τις εκατό έστω σε ένα μεγάλο και ικανοποιητικό βαθμό, οι παρακάτω προϋποθέσεις :

- Θα πρέπει να υπάρχει ακρίβεια κατα τον εντοπισμό και την ειδοποίηση επιθέσεων. Αυτό σημαίνει πως ο έλεγχος θα πρέπει να πραγματοποιείται σωστά σε σημείο που θα εξαλειφθεί το ενδεχόμενο ψευδών και ανούσιων συναγερμών.
- Η απόδοση του θα μπορέσει να φανεί από το πόσο γρήγορα μπορεί να γίνεται εντοπισμός επιθέσεων. Είναι πολύ σημαντικό να υπάρχει η δυνατότητα ανίχνευσης σε πραγματικό χρόνο διότι σε περιπτώσεις που υπάρχει ενδεχόμενο χρονικής απόκλισης, μπορεί να υπάρξουν σημαντικές συνέπειες στα συστήματα μας.
- Ένα από τα πιο δύσκολα μέτρα αξιολόγησης για την αποτελεσματικότητα ενός IDS είναι η πληρότητα των πληροφοριών που γνωρίζει ένα τέτοιο σύστημα καθώς και οι δικές μας γνώσεις απέναντι στην ανίχνευση όλων των πιθανών εισβολών. Δεν μπορούμε να είμαστε σε θέση ούτε εμείς ούτε το ίδιο το σύστημα να γνωρίζουμε όλου τους τρόπους επιθέσεων που μπορούν εξελιχθούν στο δίκτυο μας. Ωστόσο, σημαντικό είναι να γνωρίζουμε τις δυνατότητες που παρέχει το σύστημα που θα επιλέξουμε και κατά πόσο μελλοντικά μπορεί να δεχθεί επεκτάσεις για την ενημέρωση και αντιμετώπιση νέων απειλών.

### 2.3.6 Διαφορές και συνύπαρξη των SIEM και IDS

Έχοντας κάνει μια λεπτομερή ανάλυση στις δύο αυτές τεχνολογίες μπορούμε με μια πρώτη ματιά να καταλάβουμε ότι και οι δυό τους έχουν ένα κοινό σκοπό, δηλαδή την ανίχνευση και την αποτροπή επιθέσεων. Ωστόσο θα πρέπει να αναφέρουμε αυτό που κάνει την διαφορά ανάμεσα σε αυτές τις τεχνολογίες. Η διαφορά ανάμεσά τους είναι πως το SIEM μπορεί να προσαρμοστεί με τέτοιο τρόπο ώστε να μπορεί να λαμβάνει προληπτικά μέτρα προστασίας απέναντι σε επιθέσεις, ενω το IDS παρέχει μόνο την δυνατότητα ανίχνευσης και αναφοράς συμβάντων. Βέβαια όπως έχουμε παρατηρήσει και στις δύο τεχνολογίες παίζει μεγάλο ρόλο η αποφυγή ψευδών ειδοποιήσεων και άσκοπων ενεργειών που μπορούν να συμβούν. Έτσι δεν μπορούμε να είμαστε σίγουροι ότι μια τεχνολογία SIEM με τα προληπτικά μέτρα που μπορεί να λάβει θα υπάρχει πάντα το σωστό αποτέλεσμα. Για αυτό ένας συνδυασμός τους μπορεί να αποδειχθεί σωτήριος. Συγκεκριμένα, ένα εργαλείο IDS το οποίο με το που ανιχνεύσει ύποπτη δραστηριότητα, ανωμαλίες καθώς και μη φυσιολογικά συμβάντα ασφαλείας μπορεί στην συνέχεια να εισάγει αυτά τα δεδομένα σε ένα SIEM το οποίο με την σειρά του μπορεί να εφαρμόσει τα κατάλληλα μέτρα που του έχουμε θέσει. Επίσης σε όλη αυτή την διαδικασία οι διαχειριστές μπορούν να έχουν μια ακόμη πιο ξεκάθαρη εικόνα για να μπορέσουν να καθορίσουν τελικά εάν αυτά τα δεδομένα αποτελούν απειλή για το δίκτυό τους. Έτσι καλό θα ήταν να μην απορρίψουμε και τις δύο λύσεις αλλά να συμβουλευτούμε λογισμικά και τεχνολογίες καθώς και να κάνουμε μια σωστή αξιολόγηση των αναγκών που θέλουμε τελικά να εξυπηρετήσουμε.

## 2.4 Τεχνολογίες Προσδιορισμού Επιθέσεων

Έχοντας κάνει μια ανάλυση γύρω από την ορολογία και τα χαρακτηριστικά των τεχνολογιών SIEM και IDS, σειρά έχει η αναζήτηση και η ανάλυση ορισμένων τεχνολογιών τους. Μέσω της αναζήτησης και της σύγκρισης των διάφορων λύσεων που θα αναλύσουμε παρακάτω, σκοπό έχουμε να βρούμε την κατάλληλη λύση τόσο σε θέμα ευχρηστίας και κόστους υποδομών όσο και και σε θέμα τεχνολογικών δυνατοτήτων και κάλυψης αναγκών που θέλουμε να εξυπηρετήσουμε.

### 2.4.1 OSSEC

Το OSSEC είναι ένα ανοιχτού κώδικα HIDS (Host-based Intrusion Detection System) το οποίο αναπτύχθηκε από την Cid. Κάποιες από τις βασικές λειτουργίες που επιτυγχάνονται κατά την ενσωμάτωση του OSSEC είναι [8][9] :

- Συσχέτιση και ανάλυση αρχείων καταγραφής
- Παρακολούθηση ακεραιότητας αρχείων
- Παρακολούθηση μητρώου του λειτουργικού συστήματος
- Ανίχνευση rootkit
- Ειδοποίηση και απόκριση σε συμβάντα σε πραγματικό χρόνο

Το OSSEC αποτελεί ένα εργαλείο προστασίας το οποίο μπορεί να χρησιμοποιηθεί από μεγάλες επιχειρήσεις ή κυβερνητικές υπηρεσίες εώς και μικρές επιχειρήσεις για την ασφάλεια των πληροφοριακών τους συστημάτων.

Τα βασικά χαρακτηριστικά για την λειτουργία του OSSEC είναι [8]:

- Ο OSSEC Server, ο οποίος χρησιμοποιείται για την διαχείριση και τον έλεγχο των εφαρμογών και των συσκευών που ανήκουν σε αυτόνομα ή κατανεμημένα δίκτυα.
- Οι πράκτορες, οι οποίοι μπορούν να εγκατασταθούν σε μια πληθώρα λειτουργικών συστημάτων.

Οι λειτουργίες που μπορεί να παρέχει η τεχνολογία OSSEC κατά την ενσωμάτωση της είναι [9]:

- Ανίχνευση εισβολών με βάση την σύγκριση και την ανάλυση αρχείων καταγραφής. Αυτό επιτυγχάνεται με την συνεχή παρακολούθηση και ανάλυση των δεδομένων που συλλέγονται από πολλαπλά σημεία κατά μήκους του δικτύου όπου καταγράφονται δεδομένα σε πραγματικό χρόνο.
- Ανίχνευση rootkit και κακόβουλου λογισμικού. Το rootkit είναι ένα είδος κακόβουλου λογισμικού που χρησιμοποιείται για την απόκτηση παράνομης πρόσβασης με δικαιώματα διαχειριστή, με σκοπό την παρακολούθηση και παράνομη παραμετροποίηση ρυθμίσεων και διαδικασιών υπολογιστικών συστημάτων χωρίς να γίνεται αντιληπτό. Το OSSEC παρέχει την δυνατότητα ανάλυσης των διεργασιών σε επίπεδο που μπορεί να ανιχνεύσει τέτοιου είδους κακόβουλα λογισμικά και εφαρμογές.
- Ενεργή απόκριση : Το OSSEC αναλύει και ανταποκρίνεται απέναντι σε επιθέσεις σε πραγματικό χρόνο. Λόγο της δυνατότητας ενσωμάτωσης του σε διάφορα σημεία κατα μήκος του δικτύου καθώς και σε άλλα εργαλεία ασφάλειας ,όπως το τείχος προστασίας, μπορεί να γνωρίζει το ακριβές σημείο στο οποίο θα πρέπει να λάβει δράση.

Οι λειτουργίες και τα χαρακτηριστικά που προσφέρουν τα συστήματα OSSEC, παρέχουν και τα κατάλληλα πλεονεκτήματα [10]:

- Απαιτήσεις συμμόρφωσης : Μέσω του ελέγχου και της ανάλυσης αρχείων καταγραφής για κακόβουλη συμπεριφορά ακόμα και χρήση μη εξουσιοδοτημένων εφαρμογών καθώς και τροποποίησης τους, ειδοποιεί και συμμορφώνει τους χρήστες με βάση τους κανόνες που πρέπει να ακολουθούν. Με αυτό τον τρόπο το OSSEC προτρέπει τους χρήστες να πληρούν τις κατάλληλες απαιτήσεις συμμόρφωσης απέναντι σε μεγάλες και σοβαρές υπηρεσίες που μπορεί να αφορούν χρηματοπιστωτικές συναλλαγές κλπ.
- Πολλαπλές Πλατφόρμες : Το OSSEC μπορεί να υλοποιηθεί σε μια μεγάλη πληθώρα εφαρμογών και συστημάτων που υποστηρίζουν διαφορετικά λειτουργικά συστήματα ή πλατφόρμες, όπως Windows, Linux, Mac κλπ.

- Ειδοποίηση και διαμόρφωση σε πραγματικό χρόνο : Οι δυνατότητες διαμόρφωσης του OSSEC ποικίλουν ανάλογα με τις ανάγκες που θέλουμε να εξυπηρετήσουμε. Η πιο σημαντική λειτουργία που πρέπει να διαμορφωθεί με σωστό και αποτελεσματικό τρόπο είναι αυτή της ειδοποίησης και αποτροπής σε πραγματικό χρόνο. Στην περίπτωση του OSSEC, διαμορφώνοντας το κατάλληλα μπορεί να ειδοποιεί τον χρήστη για κρίσιμα συμβάντα και περιστατικά, ταξινομώντας τα βάση της κρισιμότητας και τον θόρυβο των επιθέσεων μέσω mail και άλλων υπηρεσιών επικοινωνίας. Επίσης, υπάρχουν και δυνατότητες άμεσης απόκρισης προκειμένου να αντιμετωπιστούν και να αποτραπούν επιθέσεις.
- Ενσωμάτωση με την τρέχουσα υποδομή : Η ενσωμάτωση τεχνολογιών SIEM και IDS παρέχουν την δυνατότητα συγχώνευσης τους με την τρέχουσα υποδομή, χωρίς να χρειαστούν περαιτέρω αλλαγές ή αναβαθμίσεις.
- Κεντρική διαχείριση : Το OSSEC αποτελεί ένα κεντρικό σύστημα μέσω του οποίου μπορεί να δημιουργήσει και να διαχειριστεί πολιτικές σε πολλαπλά λειτουργικά και υπολογιστικά συστήματα. Πρακτικά επιτρέπεται η δυνατότητα πολιτικών για συγκεκριμένους διακομιστές ή ομάδες διακομιστών.
- Παρακολούθηση με ή χωρίς την χρήση πρακτόρων : Με την ενσωμάτωση ενός συστήματος OSSEC παρέχεται η δυνατότητα παρακολούθησης με ή χωρίς την χρήση πρακτόρων κυρίως για την παρακολούθηση δρομολογητών, τειχών προστασίας καθώς και όλων των άλλων στοιχείων δικτύωσης. Συνήθως η παρακολούθηση χωρίς την χρήση πρακτόρων αξιοποιείται σε περιβάλλοντα όπου υπάρχουν περιορισμοί βάση του λειτουργικού προγράμματος που είναι εγκατεστημένο, ώστε να εξυπηρετούν τις ανάγκες ασφαλείας και συμμόρφωσης που πρέπει να επιτυγχάνονται.

Όπως όλες οι τεχνολογίες έτσι και το OSSEC, πέρα από τις δυνατότητες και τις υπηρεσίες που μπορεί να παρέχει, δεν το καθιστά άρτιο και χωρίς ελαττώματα σύστημα. Συγκεκριμένα δύο από τα αρνητικά χαρακτηριστικά του είναι [11][12]:

- Δυσκολία κατά την αναβάθμιση μεταξύ εκδόσεων. Το κύριο πρόβλημα που μπορεί να αντιμετωπιστεί βρίσκεται στους κανόνες οι οποίοι ενδέχεται να αντικατασταθούν σε κάθε περίπτωση αναβάθμισης.
- Διεπαφή χρήστη : Το περιβάλλον διαχείρισης που προσφέρει το OSSEC δεν είναι το πιο φιλικό απέναντι σε νέους χρήστες. Είναι αρκετά συντηρητικό και μπορεί να αποτελέσει μια δύσχρηστη λύση για κάποιον αρχάριο.
- Πολυπλοκότητα διαμόρφωσης : Η εγκατάσταση και διαμόρφωση του OSSEC δεν αποτελεί μια γρήγορη και εύκολη διαδικασία. Αντιθέτως αποτελεί μια επίπονη διαδικασία και πολλές φορές είναι απαραίτητη η συνεχής προσπάθεια και εμπειρία για την σωστή διαμόρφωσή του.
- Χρόνος εκμάθησης : Για την πλήρη αποτελεσματικότητα και την ανάδειξη των ικανοτήτων που μπορεί να προσφέρει το OSSEC είναι απαραίτητη η εμπειρία και η συνεχής εκμάθηση των λειτουργιών του από τον χρήστη. Αυτό σημαίνει πως στα αρχικά στάδια αξιοποίηση των λειτουργιών του, ένας αρχάριος χρήστης ίσως να μην μπορέσει να αξιοποιήσει όλες τις δυνατότητες που θέλει να υλοποιήσει. Για να μπορέσει να φτάσει σε ένα επίπεδο ώστε να υλοποιήσει και να αξιοποιήσει αποτελεσματικά όλα τα χαρακτηριστικά του OSSEC θα πρέπει να επενδύσει πολύ χρόνο και μελέτη για την κατανόηση του.
- Ελλιπής Υποστήριξη σε Windows : Ένα πολύ σημαντικό αρνητικό χαρακτηριστικό είναι πως το OSSEC δεν υποστηρίζεται πλήρως σε όλα τα λειτουργικά συστήματα. Τα Windows αποτελούν παράδειγμα σε αυτό το αρνητικό χαρακτηριστικό καθώς υποστηρίζεται μόνο η λειτουργία server-agent του OSSEC.

### 2.4.2 OSSIM

Το OSSIM (Open Source Security Information Management) είναι ένα ανοιχτού κώδικα λογισμικό το οποίο χρησιμοποιείται για την διαχείριση πληροφοριών και συμβάντων ασφαλείας. Βασικό του χαρακτηριστικό είναι η δυνατότητα συνδυασμού διαφόρων εργαλείων με σκοπό την βοήθεια στην διαχείριση, προς τους διαχειριστές του δικτύου, σε θέματα ασφάλειας υπολογιστικών συστημάτων, ανίχνευσης εισβολών καθώς και σε θέματα πρόληψης.

Ως βασικό του στόχο , το OSSIM προσφέρει μια ολοκληρωμένη εικόνα όλων των στοιχείων που αφορούν στην ασφάλεια των πληροφοριακών μας συστημάτων. Αυτό επιτυγχάνεται με τον συνδυασμό:

- Της διαχείρισης καταγραφών δεδομένων των συστημάτων καθώς και δίνοντας την δυνατότητα επέκτασης με την χρήση διαφόρων plugins
- Της ανακάλυψης και διαχείρισης διαφόρων περιουσιακών στοιχείων που συλλέγονται από τα κατάλληλα συστήματα ασφαλείας και ανίχνευσης.

Το OSSIM λειτουργεί χρησιμοποιώντας τρία βασικά στοιχεία. Τον server, το framework και τους πράκτορες. Για την διαχείριση των ενεργειών που θέλουμε να πραγματοποιήσουμε παρέχεται μια web-based διεπαφή και για την διαδικασία διαμόρφωσης των αναγκών μας γίνεται μέσω διαφόρων αρχείων διαμόρφωσης. Ο τρόπος με τον οποίο λειτουργεί επιτυγχάνεται με την χρήση πρακτόρων οι οποίοι συλλέγουν πληροφορίες από διάφορες επεκτάσεις (plugins) και εν συνεχεία τα αποστέλλει στον server. Το πιο σημαντικό χαρακτηριστικό για την λειτουργικότητα του είναι οι τρόποι συλλογής δεδομένων. Υπάρχουν τρεις τρόποι με τους οποίους το OSSIM συλλέγει δεδομένα και η συλλογής τους γίνεται με σένσορες [13]:

- 1ος Τρόπος: Επεξεργασία δεδομένων καταγραφής (log data) όπως το syslog
- 2ος Τρόπος: Παθητική παρακολούθηση δικτύου σε ένα δικτυακό τμήμα παρακολουθόντας την κυκλοφορία του δικτύου μέσω μιας ασύμμετρης διεπαφής.
- 3ος Τρόπος: Αποστολή ερωτημάτων σε κάποιο εργαλείο όπως το tcpwatch. Το tcpwatch είναι ένα εργαλείο γραμμένο σε γλώσσα Python το οποίο χρησιμοποιείται για την παρακολούθηση προωθημένων συνδέσεων TCP ή συνδέσεις μεσολάβησης HTTP.

Όπως μπορούμε να καταλάβουμε η χρήση διαφόρων εργαλείων και επεκτάσεων αποτελούν βασικό ρόλο για την επίτευξη της λειτουργικότητας του OSSIM.
Κάποια από αυτές τις επεκτάσεις είναι [13]:

- **Arpwatch** : Χρησιμοποιείται για την ανίχνευση διαφόρων ανωμαλιών που αφορούν την mac address
- **P0f** : Χρησιμοποιείται για παθητική ανίχνευση του λειτουργικού συστήματος καθώς και ανάλυση αλλαγών που έχουν γίνει σε αυτό.
- **Pads** : Χρησιμοποιείται για την ανίχνευση ανωμαλιών σε διάφορα services.
- **Nessus** : Χρησιμοποιείται για την αξιολόγηση ευπαθειών καθώς και την διασταύρωση συσχετίσεων.

Μια ακόμα επέκταση που μπορεί να χρησιμοποιηθεί είναι το OSSEC που αναφέραμε παραπάνω. Έτσι μπορούμε να καταλάβουμε πως παρέχεται μια μεγάλη ευελιξία κατά την ενσωμάτωση του OSSIM με άλλες τεχνολογίες και επεκτάσεις. Ωστόσο η χρησιμοποίηση όλων αυτών των τεχνολογιών, παρόλο που δίνει την δυνατότητα να θέσουμε πιο συγκεκριμένα τον σκοπό μας, αποτελούν αναγκαίο κομμάτι για την επίτευξη των στόχων μας. Πράγμα που μελλοντικά θα αποτελέσει τόσο κοστοβόρα σε πόρους λύση όσο και εγκυκλοπεδικά εφόσον θα χρειαστεί να

επενδύσουμε χρόνο στην ανάλυση και μελέτη για να μπορέσουμε να ενσωματώσουμε τελικά αυτές τις τεχνολογίες.

**Πλεονεκτήματα OSSIM**

Κάποια από τα θετικά χαρακτηριστικά που μπορούμε να επωφεληθούμε με την ενσωμάτωση του OSSIM είναι [14]:

- Το OSSIM παρέχει την δυνατότητα ειδοποιήσεων που αφορούν απειλές για κακόβουλο κώδικα και γενικότερα κίνδυνο που αφορά όλη την κυκλοφορία του δικτύου. Η πολύτιμη βοήθεια που παρέχουν οι ειδοποιήσεις συμβάλουν στην λήψη προληπτικών μέτρων ασφαλείας.
- Η δυνατότητα επεκτασιμότητας του με άλλα εργαλεία και εφαρμογές ασφαλείας καθώς και η συγχώνευση του με άλλα IDS συστήματα, το καθιστά μια ολοκληρωμένη λύση ασφαλείας ανάλογα με τις ανάγκες του κάθε οργανισμού.
- Ένα πολύ σημαντικό χαρακτηριστικό του OSSIM είναι η προηγμένη δυνατότητα συσχέτισης και αξιολόγησης ευπαθειών. Ένα τέτοιου είδους χαρακτηριστικό αποτελεί ζωτικής σημασίας για την διατήρηση της ασφάλειας ενός δικτύου.
- Το OSSIM παρέχει μια ολοκληρωμένη δυνατότητα ενσωμάτωσης πληροφοριών που αφορούν απειλές ώστε να υπάρξει ενισχυμένη πολιτική ασφάλειας σε όλο το μήκος του δικτύου καθώς και ορθή τήρηση των κανόνων ασφαλείας.
- Η δυνατότητα εντοπισμού και αποκατάστασης περιστατικών ασφαλείας είναι ο βασικότερος λόγος κατά την ενσωμάτωση του OSSIM. Η δυνατότητες που παρέχει το OSSIM για την αντιμετώπιση απειλών και κινδύνων είναι αποδοτικές και αποτελεσματικές.

Μειονεκτήματα OSSIM

Οι δυνατότητες που προσφέρει το OSSIM είναι πολύ σημαντικές και βοηθούν πλήρως για την σωστή και αποτελεσματική καταπολέμηση ευπαθειών και κινδύνων που μπορεί να προκύψουν στο δίκτυο. Όμως δεν θα πρέπει να μην λάβουμε υπόψη και κάποια χαρακτηριστικά που μπορεί να δυσκολέψουν και να φανούν λιγότερο αποδοτικά από ότι νομίζαμε [14]:

- Σε περιπτώσεις όπου υπάρχει μεγάλη κίνηση στο δίκτυο, οι χρόνοι απόκρισης του OSSIM ενδέχεται να είναι αργοί. Αυτό σημαίνει πως οι ειδοποιήσεις για περιστατικά ασφαλείας που μπορεί να προκύψουν, θα αποτελέσουν πρόκληση καθώς μπορεί να υπάρξουν καθυστερήσεις που μπορεί να αποβούν μοιραίες.
- Ένα πολύ σημαντικό χαρακτηριστικό που αναφέραμε στα θετικά χαρακτηριστικά του OSSIM είναι η δυνατότητα επεκτασιμότητας του με άλλα εργαλεία και εφαρμογές ασφαλείας. Ωστόσο πολλές φορές είναι απαραίτητη η ενσωμάτωση άλλων εργαλείων για να αποτελέσει μια ολοκληρωμένη λύση με δυνατότητα απόκρισης σε πραγματικό χρόνο.
- Η διαδικασία εγκατάστασης του OSSIM μπορεί να αποτελέσει μια χρονοβόρα και πολύπλοκη διαδικασία καθώς και να χρειαστούν επαναλαμβανόμενες προσπάθειες για την διαμόρφωσή του.
- Το OSSIM δεν αποτελεί μια οικονομική λύση. Έχοντας ανταγωνιστές που παρέχουν τις ίδιες ή και παραπάνω δυνατότητες σε σχέση με αυτό, υποβαθμίζεται αυτόματα η αξία και προσβασιμότητα του απέναντι τους.
- Ένα από τα συχνά φαινόμενα που μπορεί να αντιμετωπίσει κάποιος, είναι οι ψευδείς συναγερμοί. Δεν αποτελεί ένα χαρακτηριστικό που δεν εμφανίζεται σε άλλες λύσεις ασφαλείας, ωστόσο χρειάζεται να σημειωθεί.

### 2.4.3 SNORT

Άλλη μια ανοιχτού κώδικά λύση που θα πρέπει να λάβουμε υπόψιν είναι το Snort. Το Snort είναι ένα εργαλείο ανοιχτού κώδικα το οποίο αποτελείται από έναν συνδυασμό συστημάτων ανίχνευσης (IDS) και πρόληψης εισβολών (IPS). Ο τρόπος με τον οποίο λειτουργεί το Snort είναι μέσω της συνεχής παρακολούθησης της κυκλοφορίας των δεδομένων μέσα στο δίκτυο καθώς και την συνεχή καταγραφή και ανάλυση των πακέτων. Για να καταλάβουμε τον τρόπο με τον οποίο λειτουργεί το Snort θα πρέπει να περιγράψουμε τα βασικά του χαρακτηριστικά [11]:

- Ανάλυση πακέτων : Το Snort εξετάζει μεμονωμένα, κάθε πακέτο δεδομένων που κυκλοφορεί μέσα στο δίκτυο. Εν συνεχεία ξεκινάει μια διαδικασία σύγκρισης των πακέτων δεδομένων με μια βάσεις δεδομένων που αποτελείται από γνωστές επιθέσεις.
- Ανίχνευση απειλών : Σε δεύτερο στάδιο εξετάζει το κατά πόσο μπορεί να ταιριάζει με τα χαρακτηριστικά μιας γνωστής επίθεσης και σε περίπτωση που ανιχνεύσει οποιαδήποτε ομοιότητα με αυτή, δημιουργεί ειδοποίηση για να ενημερώσει εγκαίρως την ομάδα διαχείρισης για να ληφθούν τα κατάλληλα μέτρα προστασίας.
- Πρόληψη απειλών : Πέρα από την δημιουργία ειδοποιήσεων, παρέχει την δυνατότητα σε ορισμένες περιπτώσεις να μπλοκάρει τα κακόβουλα πακέτα ώστε να μην δημιουργηθεί επίθεση προς το δίκτυο. Ωστόσο για να μπορέσει να εκτελέσει μια τέτοιου είδους ενέργεια θα πρέπει να ρυθμιστεί και να διαμορφωθεί σωστά από την ομάδα διαχείρισης του δικτύου.

Το Snort αποτελεί και αυτό με την σειρά του μια δημοφιλή και έμπιστη λύση σε συστήματα ανίχνευσης εισβολών σε δίκτυο, γι αυτό τον λόγο θα πρέπει να αναφερθούμε στα πλεονεκτήματα που μπορεί να μας προσφέρει με την ενσωμάτωσή του [15]:

- **Επεκτασιμότητα** : Το Snort έχει την δυνατότητα να ενσωματωθεί σε οποιοδήποτε σημείο του δικτύου. Δεν υπάρχει κάποιος περιορισμός που να αποτρέπει την δυνατότητα εφαρμογής του σε κάποιο σημείο του δικτύου.
- **Ευελιξία** : Το Snort μπορεί να υλοποιηθεί σε διάφορα λειτουργικά συστήματα όπως Linux, Windows και MacOS.
- **Ζωντανή παρακολούθηση σε πραγματικό χρόνο** : Ένα από τα βασικότερα θετικά χαρακτηριστικά που προσφέρεται με την ενσωμάτωση του Snort είναι η ζωντανή παρακολούθηση συμβάντων σε πραγματικό χρόνο. Αυτό το χαρακτηριστικό αποτελεί ζωτικής σημασίας για την ομάδα διαχείρισης του δικτύου καθώς μπορεί να επιβλέπει και να λαμβάνει άμεση δράση απέναντι σε απειλές και κινδύνους που συμβαίνουν σε πραγματικό χρόνο.
- **Ταχύτητα εντοπισμού και αντιμετώπισης συμβάντων ασφαλείας :** Πέρα από την δυνατότητα παρακολούθησης συμβάντων σε πραγματικό χρόνο, χάρη στην δυνατότητα επέκτασης του σε οποιοδήποτε κόμβο κατά μήκος του δικτύου, το Snort μπορεί να χρησιμοποιηθεί με άλλες τεχνολογίες ασφαλείας όπως ένα τείχος προστασίας για την αντιμετώπιση ευπαθειών που μπορεί να συμβαίνουν σε αυτές και να μην γίνονται άμεσα αντιληπτές.
- **Αρθρωτός Μηχανισμός Ανίχνευσης :** Το Snort χρησιμοποιεί αισθητήρες κατά μήκος του δικτύου για την ανίχνευση ευπαθειών σε διάφορα σημεία. Οι αισθητήρες αυτοί μπορούν να παρακολουθούν πολλαπλά μηχανήματα και εφαρμογές από μία και μόνο τοποθεσία με στόχο την διαπίστωση μη εξουσιοδοτημένων προσπαθειών παραβίασης του δικτύου και άλλων περιστατικών ασφαλείας.

Παρά τα θετικά του χαρακτηριστικά, το Snort περιέχει και κάποιες προκλήσεις τις οποίες δεν πρέπει να παραμερίσουμε. Πιο συγκεκριμένα [11][16]:

- **Πολυπλοκότητα** : Όπως οι περισσότερες λύσεις συστημάτων ανίχνευσης και αποτροπής επιθέσεων δεν αποτελούν μια εύκολη διαδικασία ενσωμάτωσης και διαμόρφωσης. Το Snort δεν αποτελεί εξαίρεση στον κανόνα. Η διαδικασία διαμόρφωσης και διαχείρισης του Snort αποτελεί μια πολύπλοκη και επίπονη διαδικασία και ειδικότερα σε προγραμματιστές οι οποίοι δεν έχουν την κατάλληλη εμπειρία σε θέματα ασφάλειας δικτύων.
- **Δυσκολία παρακολούθησης σε μεγάλα δίκτυα και ταχύτητες δικτύου** : Ένα βασικό μειονέκτημα του Snort είναι η δυσκολία παρακολούθησης δικτύων με μεγάλη έκταση. Επιπροσθέτως, σε δίκτυα που υπάρχουν υψηλές ταχύτητες επικοινωνίας, αποτυγχάνει στην ανίχνευση ορισμένων πακέτων.
- **Κανόνες** : Πέρα από την πολυπλοκότητα που θα συναντήσει κάποιος κατά την ενσωμάτωση και διαμόρφωση του Snort, πολύπλοκη και επίπονη διαδικασία αποτελεί η δημιουργία και θέσπιση των κανόνων. Οι κανόνες αποτελούν βασικό χαρακτηριστικό σε όλες τις τεχνολογίες SIEM και IDS καθώς οι κανόνες είναι αυτοί που υλοποιούν και διαμορφώνουν τα χαρακτηριστικά ασφαλείας του δικτύου.
- **Ειδοποιήσεις** : Μια σημαντική λειτουργία που προσφέρουν τα IDS συστήματα είναι η δυνατότητα ειδοποιήσεων σε περιστατικά ασφαλείας. Στην περίπτωση του Snort, οι ειδοποιήσεις δεν αποτελούν ένα από τα δυνατά χαρακτηριστικά της τεχνολογίας. Θα πρέπει να υπάρξει βελτίωση τόσο σε επίπεδο εγκυρότητας όσο και σε επίπεδο ανάλυσης των λεπτομερειών με πιο σαφή και ξεκάθαρο τρόπο.
- **Ανάγκες επεκτασιμότητας :** Παρόλο που το Snort μπορεί να σταθεί μόνο του ως μια καλή IDS λύση απέναντι σε πολλά περιστατικά ασφαλείας, πολλές φορές κρίνεται αναγκαίος ο συνδυασμός του με άλλα εργαλεία και εφαρμογές ασφαλείας για την βελτίωση της προστασίας του δικτύου.

### 2.4.4 Wazuh

Το Wazuh είναι μια δωρεάν ανοιχτού κώδικα πλατφόρμα η οποία παρέχει μια ενοποιημένη λύση προστασίας, με δυνατότητες XDR και SIEM συστημάτων. Η αρχιτεκτονική του δομή αποτελείται από έναν βασικό πράκτορα και τρία κεντρικά στοιχεία. Πιο συγκεκριμένα [17][18]:

- Τον διακομιστή Wazuh
- Τον δείκτη Wazuh
- Το ταμπλό Wazuh

Οι δυνατότητες προστασίας που προσφέρει το Wazuh δεν περιορίζονται μόνο σε περιβάλλοντα που βρίσκονται στις εγκαταστάσεις ενός οργανισμού, αλλά και σε virtualized καθώς και cloud-based περιβάλλοντα.
Βασικός στόχος κατά την ενσωμάτωση του Wazuh σε ένας οργανισμό είναι η πλήρη προστασία στοιχείων και δεδομένων ασφαλείας από διάφορες απειλές, ανεξάρτητα από το μέγεθος του οργανισμού πράγμα που είναι πολύ σημαντικό ειδικά σε επιχειρήσεις μικρού μεγέθους.

Με την ενσωμάτωση του Wazuh σε έναν οργανισμό παρέχονται οι εξής δυνατότητες [19] :

- Security analytics : Συλλογή, συγκέντρωση και επεξεργασία των δεδομένων ασφαλείας για εντοπισμό εισβολών, απειλών και γενικότερα κακόβουλης συμπεριφορές.

- Ανίχνευση Εισβολών : Οι πράκτορες του Wazuh σαρώνουν τα συστήματα αναζητώντας κακόβουλο λογισμικό, rootkits καθώς και ανωμαλίες. Μπορούν επίσης να εντοπίσουν κρυφά αρχεία και διεργασίες.
- Ανάλυση αρχείων καταγραφής : Οι πράκτορες του συλλέγουν και διαβάζουν τα αρχεία καταγραφής των συστημάτων και τα προωθούν στον διαχειριστή του δικτύου για περαιτέρω ανάλυση βασιζόμενος πάντα στους κανόνες ασφαλείας που έχουν τεθεί.
- Παρακολούθηση ακεραιότητας αρχείων : Υπάρχει συνεχής παρακολούθηση του συστήματος αρχείων για τυχόν αλλαγές που αφορούν το περιεχόμενο, τα δικαιώματα, τα χαρακτηριστικά τους και χρειάζονται προσοχή.
- Ανιχνευτής επιθέσεων : Οι πράκτορες συλλέγουν και αποστέλλουν δεδομένα απογραφής λογισμικού στον διακομιστή, όπου πραγματοποιείται μια διαδικασία συσχέτισης τους με ενημερωμένες βάσεις δεδομένων CVE(Common Vulnerabilities and Exposures) προκειμένου να εντοπιστεί κακόβουλο λογισμικό.
- Αξιολόγηση διαμόρφωσής : Το Wazuh πραγματοποιεί μια ολοκληρωμένη παρακολούθηση σε ότι αφορά τις ρυθμίσεις διαμόρφωσης των εφαρμογών ώστε να υπάρχει πλήρη συμβατότητα τους με βάσει τα προτυπα και τις πολιτικές ασφαλείας του οργανισμού. Πρακτικα εκτελούνται περιοδικές σαρώσεις των εφαρμογών που είναι ευάλωτες, δεν έχουν ενημερωθεί ή δεν έχουν ρυθμιστεί με τα κατάλληλα μέτρα ασφαλείας.

Το Wazuh βασίζεται σε 3 βασικά στοιχειά [19]:

- Τους πράκτορες : Εγκαθίστανται σε τελικούς σταθμούς του δικτύου, όπως σταθεροί ή φορητοί υπολογιστές, virtual machines, servers με σκοπό την παροχή πρόληψης, ανίχνευσης και αποκρισης απέναντι σε απειλές και επιθέσεις. Τα λειτουργικά συστήματα που μπορεί να υποστηρίξει είναι :
    - Windows
    - Linux
    - MacOs
    - Solaris
    - HP-UX
    - AIX

- Wazuh Server : Τα δεδομένα των πρακτόρων συλλέγονται και μεταφέρονται στον Wazuh Server. Στην συνέχεια γίνεται η ανάλυση και επεξεργασία των δεδομένων, μέσω διαδικασιών αποκωδικοποίησης και κανόνων, για την αναζήτηση γνωστών ευπαθειών.
- Elastic Stack : Το Elastic Stack αποτελεί μια ενοποιημένη σουίτα εργαλείων τα οποία χρησιμοποιούνται για την εξόρυξη, μεταφορά, ανάλυση και την οπτικοποίηση των δεδομένων. Κάποια από αυτά τα εργαλεία είναι :
    - Firebeat
    - Elastic Search
    - Kibana.

Η αρχιτεκτονική δομή του Wazuh βασίζεται κυρίως σε πράκτορες, οι οποίοι βρίσκονται κατά κόρων σε end points κατά μήκος του δικτύου με σκοπό την συνεχή παρακολούθηση και προώθηση δεδομένων ασφαλείας στον κεντρικό διαχειριστή του δικτύου. Συσκευές και εργαλεία που δεν έχω την δυνατότητα χρήσης πρακτόρων, όπως τα τείχη προστασίας ή οι δρομολογητές, καλούνται να προωθήσουν τα δεδομένα ασφαλείας και καταγραφής μέσω Syslog. Εφόσον έχουν συγκεντρωθεί δεδομένα τόσο από τους πράκτορες, όσο και από τα υπόλοιπα εργαλεία, σειρά έχει ο διαχειριστής του

δικτύου να τα αποκωδικοποιήσει και να τα αναλύσει και τελικά να μεταβιβάσει τα αποτελέσματα του σε ένα Elasticsearch για αποθήκευση[19].

Κάποια από τα πλεονεκτήματα που μπορούμε να αποκτήσουμε με την ένταξη του Wazuh για την προστασία των πληροφοριακών συστημάτων μας είναι [20]:

- Η συσχέτιση MITRE ATT&CK καθώς και η εύκολη ενσωμάτωση του το καθιστούν πολύτιμο για συνδυασμό με άλλα περιβάλλοντα καθώς και με cloud και τοπικές εφαρμογές. Το MITRE ATT&CK είναι μια βάση δεδομένων που περιέχει τακτικές και τεχνικές περιστατικών ασφαλείας. Η βάση ATT&CK χρησιμοποιείται για την ανάπτυξη μοντέλων επιθέσεων ενώ το MITRE ,μέσω της δημιουργίας του ATT&CK, επιλύει τα περιστατικά ασφαλείας που δημιουργούνται[32].
- Προσφέρει ισχυρά χαρακτηριστικά όπως το ELK που χρησιμοποιείται για έρευνες, σαρωσεις ευπαθειών και ανίχνευση εισβολών. Το ELK είναι ακρωνύμιο που σημαίνει ElasticSearch, Logstach και Kibana. Πιο συγκεκριμένα το ElasticSearch αποτελεί τον πυρήνα του ELK και χρησιμοποιείται ως μια μηχανή αναζήτησης και ανάλυσης μεγάλου όγκου δεδομένων, το Logstach αναλαμβάνει την επεξεργασία και την ανάλυση των δεδομένων και το Kibana αποτελεί την διεπαφή όπου χειρίζεται ο χρήστης[33].
- Λόγο της φύσης του που είναι ανοιχτού κώδικα και δωρεάν, τα καθιστά οικονομικά αποδοτικότερο σε σχέση με άλλες λύσεις ασφάλειας.
- Άλλα πολύτιμα χαρακτηριστικά που περιλαμβάνει το Wazuh είναι η δυνατότητα επεκτασιμότητας του σε άλλες πλατφόρμες, ενσωματωμένες δυνατότητες ανίχνευσης κακόβουλου λογισμικού, διαχείριση αποθεμάτων και ευπαθειών.
- Η πλατφόρμα του Wazuh παρέχει μια ολοκληρωμένη λύση για την διαχείριση της συμμόρφωσης του δικτύου, τους ενσωματωμένους κανόνες και την δυνατότητα ορισμού προσαρμοσμένων κανόνων για την ανίχνευση κακόβουλων δραστηριοτήτων.

Παρόλα τα θετικά χαρακτηριστικά που μπορεί να προσφέρει το Wazuh κατά την ενσωμάτωση του, δεν θα πρέπει να παραμερίσουμε και κάποια από τα αρνητικά χαρακτηριστικά και τις δυσκολίες που μπορεί να αντιμετωπίσουμε [20]:

- Ένα από τα αρνητικά χαρακτηριστικά που θα κληθούμε να αντιμετωπίσουμε με την ενσωμάτωση του Wazuh είναι η δυσκολία και δυσχρηστία περιστατικών σε πραγματικό χρόνο. Το επίπεδο δυσκολίας μπορεί να επηρεαστεί ανάλογα με το λειτουργικό σύστημα που θα επιλέξουμε να εγκαταστήσουμε το Wazuh καθώς και λόγω έλλειψης πληροφοριών απέναντι στην αντιμετώπιση απειλών, πολλές φορές θα απαιτηθεί αναζήτηση από τους διαχειριστές για την διαχείριση περιστατικών.
- Πολλές φορές διαδικασίες που αφορούν την διαμόρφωση και την ανάπτυξη του Wazuh, μπορούν να αποδειχθούν ιδιαίτερα πολύπλοκες και χρονοβόρες καθώς κρίνεται απαραίτητη η χειροκίνητη ρύθμιση, πράγμα που κάποιες φορές απαιτεί και τεχνογνωσία κατά την υλοποίηση των ρυθμίσεων.
- Ένα ζήτημα που μπορεί να απασχολήσει μελλοντικά η ενσωμάτωση του Wazuh σε ένα δίκτυο είναι η δυνατότητες επεκτασιμότητας του. Λόγο αυτού του αρνητικού χαρακτηριστικού του περιορίζονται πόλλες από τις δυνατότητες που μπορεί να παρέχει, όπως η αποτελεσματική και αποδοτική διαχείριση μεγάλου όγκου αρχείων καταγραφής.
- Οι δυνατότητες τεχνικής υποστήριξης σε διάφορα θέματα που μπορεί να αφορούν είτε το τεχνικό κομμάτι του Wazuh είτε άλλες φορές την άμεση αντιμετώπιση μιας απειλής, μπορεί να αποτελέσει μια χρονοβόρα διαδικασία και κάποιες φορές μπορεί να μην καταφέρει να

προσφέρει κάποια ουσιαστική βοήθεια. Αυτό σημαίνει πως οι διαχειριστές του Wazuh θα πρέπει να έχουν κάποιες στοιχειώδεις γνώσεις σε τέτοιου είδους συνθήκες.
- Λόγο της δωρεάν και ανοιχτού κώδικα φύσης του, όπως είναι αναμενόμενο, το Wazuh στερείται ορισμένων χαρακτηριστικών και λειτουργιών που μπορεί να προσφέρουν άλλες επιχειρηματικές λύσεις. Κάποιες από αυτές τις δυνατότητες αφορούν τεχνικές τεχνητής νοημοσύνης, ολοκληρωμένοι μηχανισμοί αναφοράς και άλλα.

Κάποιοι πολύ σημαντικοί λόγοι που το Wazuh θα αποτελούσε μια καλή λύση για την ενσωμάτωση του σε έναν οργανισμό είναι [21]:
- Ευκολία χρήσης : Το Wazuh αποτελεί μια λύση η οποία μπορεί να λειτουργήσει οπουδήποτε και οποτεδήποτε παρέχοντας μεγάλη ευελιξία στον διαχειριστή του δικτύου, λόγο της δυνατότητας του να μπορεί να χρησιμοποιηθεί ως cloud ή υβριδική υπηρεσία.
- Επεκτασιμότητα : Δεν υπάρχει περιορισμό στο μέγεθος ενός οργανισμού. Το Wazuh μπορεί να ανταποκριθεί και να προσαρμοστεί σε όλα τα είδη και μεγέθη οργανισμών.
- Ολοκληρωμένη λύση : Με μια τεράστια πληθώρα υπηρεσιών και περιπτώσεων, το Wazuh μπορεί να βοηθήσει πλήρως στην διαχείριση της ασφάλειας συστημάτων, καθιστώντας το ως μία ολοκληρωμένη λύση ασφάλειας.
- Ενισχυμένη απόδοση : Οι πράκτορες που παρέχονται μπορούν να εγκατασταθούν και να αναπτυχθούν σε υπολογιστές, εικονικές μηχανές και στα περισσότερα λειτουργικά συστήματα παρέχοντας μέγιστη απόδοση.

### 2.4.5 Συγκριτική ανάλυση των τεχνολογιών

Έχοντας λοιπόν αναλύσει τα πλεονεκτήματα και τα μειονεκτήματα των δύο αυτών τεχνολογιών, θα πρέπει να περάσουμε σε μια συγκριτική ανάλυση για να καταλήξουμε τελικά στην επιλογή της τεχνολογίας που θα ενσωματώσουμε.

Αρχικά θα πρέπει να αναφέρουμε κάποια χαρακτηριστικά που θα πρέπει να λάβουμε υπόψη πριν την τελική μας επιλογή :
- Θα πρέπει η τεχνολογία που θα χρησιμοποιήσουμε να είναι δωρεάν και ανοιχτού κώδικα. Φυσικά μία λύση η οποία απαιτεί κάποιο χρηματικό κόστος μπορεί να παρέχει κάποιες παραπάνω δυνατότητες και ευκολίες σε σχέση με μια δωρεάν επιλογή, όμως μελλοντικά μπορεί να υπάρχουν ανάγκες που μπορεί να μην μπορεί να τις εξυπηρετήσει ή να χρειάζεται η ενσωμάτωση κάποιων επιπλέων μηχανισμών. Πράγμα που μπορεί να κάνει μια τέτοια τεχνολογία ακόμη πιο κοστοβόρα και ακόμη πιο μη αποτελεσματική λόγο του χρηματικού της κόστους.
- Θα πρέπει να υπάρχει ένα περιβάλλον ευελιξίας και ευχρηστίας απέναντι ακόμα και σε χρήστες που δεν έχουν το επιστημονικό υπόβαθρο σε τέτοιου είδους τεχνολογίες. Με λίγα λόγια, θα πρέπει να αποτελείται από ένα περιβάλλον το οποίο θα είναι φιλικό σε νέους χρήστες ώστε να μπορέσουν να μάθουν και στην συνέχεια να ενσωματώσουν τις αλλαγές που θέλουν να κάνουν εύκολα. Αυτό δεν σημαίνει απαραίτητα ότι στο ξεκίνημα είτε και μελλοντικά δεν θα υπάρξουν δυσκολίες, απλός θα είναι ένα πολύ καλό εφόδιο να υπάρχει ένα σχετικά καλό επίπεδο δυσκολίας όπου δεν θα δυσκολέψει πολύ στα ξεκινηματα της ενσωμάτωσης σε τέτοιου είδους τεχνολογίες.
- Θα πρέπει να υπάρχει τόσο βιβλιογραφική όσο και υποστήριξη από διάφορες κοινότητες χρηστών που χρησιμοποιούν τέτοιου είδους τεχνολογίες. Η βιβλιογραφία καθώς και η υποστήριξη της κοινότητας μιας τεχνολογίας αποτελούν ζωτική σημασία για την κατανόηση και την επίλυση απορίων και προβλημάτων που μπορούν να προκύψουν. Θα πρέπει να έχουμε

πάντα τα κατάλληλα μέσα για να μπορούμε να συμβουλευτούμε διαφορετικές τεχνικές καθώς και να ενημερωνόμαστε για νέες λύσεις που μπορεί να δημοσιευτούν.

- Θα πρέπει η τεχνολογία που θα χρησιμοποιήσουμε να μην είναι κοστοβόρα απέναντι στους υπολογιστικούς πόρους που χρησιμοποιούμε. Η τεχνολογία που θα επιλέξουμε καθώς και οι μελλοντικές επεκτάσεις που μπορεί να χρησιμοποιηθούν για την επίτευξη κάποιων στόχων θα πρέπει να έρχονται σε μία ισορροπία απέναντι στους υπολογιστικούς πόρους που παρέχουμε. Δεν θα ήταν καλή η επιλογή μιας τεχνολογίας η οποία θα εκμεταλλεύεται πολλούς από μόνη της διότι μελλοντικά μπορεί να αποδειχθεί αναγκαία η ενσωμάτωση επεκτάσεων οι οποίες και εκεινες με την σειρά τους μπορεί να χρειάζονται υπολογιστικούς πόρους.

Σε δεύτερο στάδιο θα πρέπει να γίνει μια αναφορά στα κοινά θετικά χαρακτηριστικά που προσφέρουν οι παραπάνω τεχνολογίες :

- Όλες οι τεχνολογίες που αναφέρθηκαν παραπάνω, έχουν ως βασικότερο χαρακτηριστικό την ανίχνευση και την ανάλυση κακόβουλων επιθέσεων και ευπαθειών σε ένα δίκτυο. Το χαρακτηριστικό αυτό προσφέρει καλύτερη και πιο στοχευμένη ορατότητα στην ομάδα διαχείρισης του δικτύου. Με αυτό τον τρόπο μπορεί να υπάρξει βελτίωση στην κατανόηση και την αναβάθμιση των μέτρων ασφαλείας που έχουν παρθεί.
- Η ενσωμάτωση των τεχνολογιών αυτών δεν περιορίζεται σε ένα υπολογιστικό σύστημα, μια συσκευή δικτύου ή μια εφαρμογή, αλλά σε όλους τους πιθανούς κόμβους κατά μήκος του δικτύου. Υπάρχει μια πιο εξονυχιστική παρακολούθηση ακόμα και σε σημεία που θεωρούμε ότι δεν τίθεται απαραίτητη προσοχή. Ακόμη, μια σημαντική ιδιότητα των τεχνολογιών αυτών είναι η δυνατότητα συνύπαρξης με άλλα εργαλεία ασφαλείας όπως τα τείχη ασφαλείας, για την ακόμη καλύτερη διεύρυνση περιστατικών ασφαλείας.
- Ένα επίσης σημαντικό χαρακτηριστικό είναι ότι αποτελούν λύσεις δωρεάν ανοιχτού κώδικά. Μια λύση επί πληρωμή, δεν εγγυάται απαραίτητα ότι θα παρέχει περισσότερες δυνατότητες και ανέσεις σε σχέση με μια δωρεάν λύση. Πολλές φορές οι δωρεάν λύσεις παρέχουν περισσότερες ελευθερίες και συμβάλλουν σημαντικά στον προϋπολογισμό του κόστους.
- Όλες οι λύσεις που αναφέρθηκαν, παρέχουν ένα μεγάλο φάσμα ευπαθειών και απειλών που μπορούν να διαχειριστούν. Με την εγκατάσταση τους παρέχεται ένα μεγάλο πλήθος κανόνων και βάσεις δεδομένων με γνωστές επιθέσεις ώστε να συμβάλλουν άμεσα στην αντιμετώπιση διαφόρων κινδύνων. Επιπροσθέτως, παρέχουν μεγάλη ελαστικότητα και ευελιξία στην δημιουργία νέων σύνθετων κανόνων καθώς και δυνατότητες επεκτασιμότητας με άλλες εφαρμογές ασφαλείας.
- Σημαντικότερο χαρακτηριστικό που προσφέρουν είναι η δυνατότητα ειδοποίησης και απόκρισης σε πραγματικό χρόνο απέναντι σε επιθέσεις. Πρέπει κάθε είδους επίθεσης να εξουδετερώνεται όσο πιο γρήγορα και αποτελεσματικά γίνετε ώστε να μην υπάρχουν σημαντικές ζημιές σε δεδομένα και συστήματα. Επίσης κρατάει ενήμερη την ομάδα διαχείρισης του δικτύου οποιαδήποτε στιγμή, ώστε να αναλάβει άμεση δράση για την καταπολέμηση των κινδύνων που εξελίσσονται.

Ωστόσο η αναφορά των θετικών χαρακτηριστικών που μπορούμε να επωφεληθούμε με την ενσωμάτωση τέτοιων τεχνολογιών, δεν σημαίνει απαραίτητα πως δεν θα έρθουμε αντιμέτωποι με χαρακτηριστικά που μπορούν να καταστήσουν κάποιες καταστάσεις αρκετά επίπονες :

- Παρόλο που οι περισσότερες τεχνολογίες SIEM που έχουμε αναφέρει παρέχουν πολλές δυνατότητες και ευκολίες σε νέους χρήστες, δεν σημαίνει πως αυτές οι δυνατότητες μπορούν να φανούν αντάξιες των προσδοκιών για πάντα. Χρειάζεται συνεχής μελέτη και υλοποίηση κανόνων για να μπορεί μια τεχνολογία SIEM να είναι σε ετοιμότητα απέναντι σε κινδύνους.

- Η εγκατάσταση και η συνύπαρξη με διάφορα pluggins και extensions πολλές φορές αποτελεί απαραίτητη προϋπόθεση για την αποτελεσματική λειτουργία ορισμένων τεχνολογιών. Έτσι, υπάρχει περίπτωση να αξιοποιηθούν περισσότεροι πόροι από όσους υπολογίζαμε και επιπροσθέτως να χρειαστεί περισσότερη μελέτη και εξειδίκευση στα extensions και pluggins που πρέπει να εγκατασταθούν.
- Η δυνατότητα ειδοποίησης και αποτροπής επίθεσης σε πραγματικό χρόνο, δεν αποτελεί μια εύκολη και έγκυρη διαδικασία. Πιο συγκεκριμένα, η υλοποίηση τους είναι μια χρονοβόρα και επίπονη διαδικασία και απαιτεί πολλές φορές γνωστικό υπόβαθρο. Επίσης, ακόμα και με την σωστή υλοποίηση τους, δεν σημαίνει ότι δεν θα υπάρξουν ψευδείς συναγερμοί ή να μην μπορέσει να αποτραπεί μια επίθεση αυτόματα. Σε όλα αυτά τα σενάρια θα πρέπει να έχει γίνει σωστή μελέτη των χαρακτηριστικών που προσφέρει το δίκτυο σε σύγκριση με τις δυνατότητες που μπορεί να καλύψει η τεχνολογία SIEM που θα ενσωματωθεί.

Με βάση τα χαρακτηριστικά των τεχνολογιών που αναλύσαμε και με μια σύντομη αλληλεπίδραση με τον περιβάλλον της επίσημης σελίδας, για κάθε τεχνολογία ξεχωριστά, καταλλήξαμε στην ενσωμάτωση της τεχνολογίας Wazuh. Βάση της έρευνας που έγινε ξεχωριστά για κάθε τεχνολογία SIEM που αναφέρθηκε, η τεχνολογία Wazuh και η επίσημη της σελίδα παρείχαν :

- Λεπτομερείς πληροφορίες για τις δυνατότητες και τα τεχνικά χαρακτηριστικά
- Μεγάλη βιβλιογραφική και τεχνική βοήθεια σε θέματα σύνταξης εντολών και υλοποίησης τους
- Εύχρηστο και φιλικό περιβάλλον για αρχάριους χρήστες
- Πλήρως ενημερωμένη και άρτια δομημένη επίσημη σελίδα

Επίσης ένα χαρακτηριστικό που αποτελεί υψίστης σημασίας για τα επόμενα βήματα ενσωμάτωσης του Wazuh, είναι η μεγάλη πληθώρα οπτικοακουστικού υλικού από την κοινότητα, που βοηθούν σε μεγάλο βαθμό στα στάδια εγκατάστασης, προσαρμογής, πειραματισμού προσομοίωσης επιθέσεων με σκοπό την ανάδειξη των δυνατοτήτων του Wazuh. Σίγουρα, όλα αυτά αποτελούν βασικά χαρακτηριστικά για την επιλογή της συγκεκριμένης τεχνολογίας, όμως αυτό δεν σημαίνει πως δεν θα υπάρξουν οι ανάλογες απαιτήσεις κατά την διάρκεια του πειραματισμού.

## 2.5 Επίλογος

Ανακεφαλαιόνοντας, οι τεχνολογίες SIEM, αποτελούν μια ολοκληρωμένη λύση ασφαλείας. Μπορούν να εφαρμοστούν και να συνυπάρχουν με οποιοδήποτε υπολογιστικό σύστημα και εφαρμογή καθώς και άλλα εργαλεία ασφαλείας, σε όλο το μήκος ενός δικτύου. Τα θετικά τους χαρακτηριστικά δεν θα πρέπει να επισκιάζουν τις προκλήσεις που μπορεί να αντιμετωπιστούν. Στόχος είναι η σταδιακή μελέτη και συνεχής εξέλιξης τους απέναντι σε ευπάθειες και κινδύνους που παραμονεύουν. Επίσης, πρέπει τα κριτήρια επιλογής της κατάλληλης τεχνολογίας που θέλουμε να ενσωματώσουμε, να είναι σε επίπεδο που μπορούμε να ανταπεξέλθουμε και να έχουμε εύκολη πρόσβαση και δυνατότητα σε βιβλιογραφία για την άμεση αντιμετώπιση απειλών που δεν ξέρουμε πως να διαχειριστούμε. Γι αυτό η τελική επιλογή θα πρέπει να γίνει με προσοχή και να πληρεί σε ένα αξιοπρεπεί βαθμό τις προϋποθέσεις που απαιτούμε.

# Κεφάλαιο 3ο: Ενσωμάτωση και πειραματισμός με το Wazuh

## 3.1 Εισαγωγή

Σε θεωρητικό κομμάτι, καταλαβαίνουμε πως όλες οι τεχνολογίες SIEM μπορούν να φανούν πολύ χρήσιμες και κάποιες φορές αναγκαίες για την αναβάθμιση των συστημάτων ασφαλείας ενός οργανισμού. Επίσης, οι περισσότερες τεχνολογίες SIEM, δεν περιορίζονται ανάλογα με το μέγεθος, τις δυνατότητες ή το κόστος τους απέναντι σε έναν οργανισμό. Υπάρχουν πολλές λύσεις και μεγάλη προσαρμοστικότητα απέναντι σε κάθε μέγεθος και προϋπολογισμό για κάθε οργανισμό. Σίγουρα δεν αποτελούν πάντα μια εύκολη και εύχρηστη διαδικασία σε όλα τα στάδια ενσωμάτωσης και παραμετροποίησης τους, όμως με σταδιακή μελέτη και συνεχή προσπάθεια για αναβάθμιση τους, μπορούν να αποδώσουν πολύτιμη βοήθεια για την ασφάλεια ενός δικτύου.

Στην παρούσα εργασία επιλέχθηκε η ενσωμάτωση της τεχνολογίας Wazuh. Οι λόγοι που οδήγησαν σε αυτή την επιλογή είναι πως το Wazuh παρέχει ένα πολύ φιλικό περιβάλλον για νέους χρήστες, αποτελεί ολοκληρωμένη λύση SIEM και παρέχει μια μεγάλη βιβλιογραφία και βοήθεια τόσο από την κοινότητα που την χρησιμοποιεί, όσο και από την επίσημη σελίδα της η οποία παρέχει σημαντικό υλικό για τα πρώτα βήματα καθώς και μεταγενέστερα, χάρη στο εύχρηστο περιβάλλον της και την άρτια εξήγηση των λειτουργιών που θέλουμε να ενσωματώσουμε.

Συνοπτικά, πέρα από το θεωρητικό κομμάτι και την τελική επιλογή της τεχνολογίας που θα ενσωματώσουμε, στο παρακάτω κεφάλαιο θα αναφερθούμε και σε τεχνικά κομμάτια των τεχνολογιών SIEM καθώς και πως υλοποιούνται με βάση την τεχνολογία Wazuh. Επίσης θα την εγκαταστήσουμε και θα κάνουμε ορισμένα πειράματα, βήμα βήμα, ώστε να αντλήσουμε ορισμένα αποτελέσματα για να καταλήξουμε στο κατά πόσο σημαντική και αποτελεσματική είναι τελικά η ενσωμάτωσή του στο δίκτυο του τμήματος.

## 3.2 Wazuh Rules

Το Wazuh , όπως και κάθε σύστημα SIEM, πραγματοποιεί μια συνεχή αποθήκευση και ανάλυση δεδομένων και αρχείων καταγραφής. Εν συνεχεία ακολουθεί η συσχέτιση όλων αυτών των δεδομένων με μοτίβα απειλών ή επιθέσεων με σκοπο να εξακριβωθεί αν εξελίσσεται κάποιος κίνδυνος στο δίκτυο. Το εργαλείο το οποίο βοηθάει στην διαδικασία συσχέτισης των δεδομένων με πιθανές απειλές, για την εξακρίβωση κινδύνων είναι οι κανόνες (Rules). Τα rules αποτελούν θεμελιώδη μονάδα ανάλυσης και ταξινόμησης δεδομένων ασφαλείας. Καθορίζουν τις συνθήκες κατά τις οποίες ένα συμβάν θεωρείται κακόβουλο ή προκαλεί ανωμαλία και μέσω αυτών των συνθηκών αναλαμβάνουν δράση ενεργοποιόντας ειδοποιήσεις ή αποτρέποντας τον κίνδυνο. Είναι σημαντικό να αναφέρουμε πως ασχέτος με το μοντέλο που μπορεί να επιλέξει κάποιος, είτε με χρήση agent ή χωρίς, το Wazuh πραγματοποιεί πλήρη εφαρμογή των κανόνων και στα δύο μοντέλα που μπορεί να ενσωματωθεί.[22] Κάθε rule χρησιμοποιείται για διαφορετικό σκοπό και μπορεί να αναλαμβάνει δυσκολότερα συμβάντα ασφαλείας. Για να μπορέσει να γίνει ένας σωστός καταμερισμός των rules, κατηγοριοποιούνται ανάλογα με το επίπεδο επικινδυνότητας που μπορεί να προκαλέσει μια απειλή. Τα επίπεδα επικινδυνότητας κυμαίνονται από το 0 εώς το 16, όπου το 0 είναι για περιπτώσεις που οριακά δεν θα εμφανιστούν ειδοποιήσεις στον Wazuh και το 16 είναι για περιπτώσεις χρειάζεται άμεση δράση και δεν υπάρχουν περιθώρια για λανθασμένες κινήσεις. Καλό θα ήταν να αναφέρουμε λεπτομερώς όλα τα επίπεδα επικινδυνότητας, βασισμένοι στην επίσημη σελίδα του Wazuh [23]:

- 0 για περιστατικά που δεν χρειάζεται να πραγματοποιηθεί καμία ενέργεια.
- 2 για περιστατικά που αναφέρονται σε ειδοποιήσεις για την κατάσταση του συστήματος. Δεν έχουν κάποια σημασία για την ασφάλεια και δεν εμφανίζονται στον Wazuh
- 3 για περιστατικά επιτυχούς συμβάντων, όπως επιτυχής σύνδεση μέσω SSH.
- 4 για περιστατικά που αναφέρονται σε σφάλματα που προκαλούνται κυρίως κατά την διάρκεια δοκιμής ή εγκατάστασης λογισμικού, καθώς και σε αχρησιμοποίητες εφαρμογές ή προγράμματα.
- 5 για περιστατικά όπου ο χρήστης έχει προκαλέσει λανθασμένες κινήσεις, όπως αποτυχημένες προσπάθειες πληκτρολόγησης κωδικού πρόσβασης.
- 6 για περιστατικά επιθέσεων χαμηλής σημασίας. Σε αυτή την περίπτωση μπορούν να εμφανιστούν επιθέσεις που να περιέχουν κάποιο είδος ιού, όμως σε επίπεδο που δεν επηρεάζει το σύστημα.
- 7 για περιστατικά επιθέσεων χαμηλής σημασίας. Μπορεί να αναφέρονται σε περιστατικά που εμφανίζουν σφάλμα και κάποια από αυτά έχουν κάποια σημασία για την ασφάλεια.
- 8 για περιστατικά που περιλαμβάνουν ενέργειες που απαιτούν την χρήση μεθόδων ασφάλειας
- 9 για περιστατικά που απαιτούν την χρήση μεθόδων ασφαλείας. Εμφανίζονται κυρίως σε περιπτώσεις επανειλημμένων λανθασμένων ενεργειών καθώς και σε περιπτώσεις σφαλμάτων που εντοπίζονται στον admin.
- 10 για περιστατικά πολλαπλών αποτυχημένων προσπαθειών σύνδεσης με λανθασμένους κωδικούς πρόσβασης. Αυτό το στάδιο συχνά υποδηλώνει επίθεση.
- 11 για περιστατικά που σχετίζονται με τροποποίηση αρχείων και δεδομένων. Αυτό το στάδιο υποδηλώνει συχνά επιτυχημένη επίθεση.
- 12 για περιστατικά επιθέσεων με αντίκτυπο σε εφαρμογές.
- 13 για περιστατικά που εμφανίζουν μοτίβο επίθεσης. Σε αυτό το επίπεδο αναφερόμαστε σε επιθέσεις με σοβαρό αντίκτυπο και δυνατότητα επέκτασης της.
- 14 για περιστατικά που υποδεικνύεται επίθεση. Αναφερόμαστε σε επιθέσεις που μπορεί να καταστρέψουν ένα σύστημα ή μια υπηρεσία.
- 15 για περιστατικά που είναι κρίσιμα και χρειάζονται άμεση καταπολέμηση. Σε αυτή την περίπτωση δεν υπάρχουν περιθώρια λανθασμένων κινήσεων.

Τα επίπεδα επικινδυνότητας, με τον τρόπο τον οποίο έχουν υλοποιηθεί, βοηθούν αρκετά στην κατηγοριοποίηση των περιστατικών ασφαλείας που εξελίσσονται, παίζοντας καθοριστικό ρόλο σε περιπτώσεις επιθέσεων καθώς μπορούμε να αντλήσουμε πληροφορίες για την φύση της επίθεσης και το κατά πόσο κρίσιμη είναι ώστε να αναλάβουμε δράση την στιγμή που χρειάζεται.

### 3.2.1 Σύνταξη Wazuh Rule

Η δήλωση του επιπέδου επικινδυνότητας,κατά την σύνταξη ενός rule, γίνεται μέσω της ιδιότητας level και τον αριθμό του επιπέδου. Πιο συγκεκριμένα τα rules του Wazuh συντάσονται σε μορφή XML και κάθε rule αποτελείται συνήθως από τα εξής στοιχεία [24][25]:

- <rule> : Δήλωση νέου κανόνα καθώς και τις επιλογές ορισμού του.
- <description> : Περιέχει μια περιγραφή του κανόνα, σχετικά με τον σκοπό που θέλει να εξυπηρετήσει. Χρησιμοποιείται κυρίως κατά την δημιουργία προσαρμοσμένων κανόνων.
- <group> : Χρησιμοποιείται για την κατηγοριοποίηση των κανόνων.
- <field> : Καθορίζει τα πεδία δεδομένων καταγραφής που θα αξιολογηθούν βάσει των συνθηκών.

Για να μπορέσουμε όμως να δούμε στην πράξη πως ακριβώς συντάσσεται ένα rule, μπορούμε να πάρουμε ως παράδειγμα το παρακάτω και να κάνουμε την ανάλυση μας.

**<group name="limits,">**

```
<rule id="100234" level="3">
  <if_sid>230</if_sid>
  <field name="alert_type">normal</field>
  <description>The file limit set for this agent is $(file_limit). Now, $(file_count) files are being monitored.</description>
 </rule>
</group>
```

Παρατηρώντας το παραπάνω κομμάτι σύνταξης ενός rule, μπορούμε να διακρίνουμε με μεγαλύτερη ακρίβεια πως ακριβώς επιτυγχάνεται η σύνταξή του. Πιο συγκεκριμένα[25]:

- Στο group υπάρχει το πεδίο name κατα το οποίο θα δηλωθεί η ομάδα που θα κατηγοριοποιηθεί το rule.
- Στο rule υπάρχει το πεδίο id το οποίο αναφέρεται στον μοναδικό αναγνωριστικό κωδικό που θα έχει ο κανόνας και το πεδίο level για τον καθορισμό επίπεδου σοβαρότητας.
- Εντός του πεδίου rule υπάρχουν 3 πεδία :
    - Το if_sid χρησιμοποιείται για την εφαρμογή του κανόνα, εφόσον έχει ενεργοποιηθεί προηγουμένως ο κανόνας που αναγράφεται, δηλαδή στην περίπτωση μας ο 230.
    - Το field που περιέχει το πεδίο name το οποίο χρησιμοποιείται για την δήλωση του ονόματος του field.
    - Το description που χρησιμοποιείται για την περιγραφή του rule.

Κατά την διαδικασία εγκατάστασης και ενσωμάτωσης του Wazuh σε ένα δίκτυο, γίνετε και η εγκατάσταση μιας μεγάλης πληθώρας προεγκατεστημένων κανόνων οι οποίοι καλύπτουν ένα πολύ μεγάλο φάσμα ευπαθειών και επιθέσεων που μπορεί να προκύψουν. Ωστόσο θα πρέπει να σημειώσουμε πως το Wazuh παρέχει και την δυνατότητα σύνταξης κανόνων προσαρμοσμένων κανόνων. Οι προσαρμοσμένοι κανόνες μπορεί να αποτελούν προσθήκη νέων κανόνων αλλά και παραλλαγή ήδη υπάρχων κανόνων. Οι χρησιμοποίηση προκαθορισμένων κανόνων αρκούν σε ένα αρχικό στάδιο ενσωμάτωσης του Wazuh. Βοηθούν στην κατανόηση περιστατικών ασφαλείας καθώς και αντιμετώπισης τους. Ωστόσο, καταλαβαίνουμε πως με την πάροδο του χρόνο και όσο οι ανάγκες για καλύτερες μεθόδους ασφαλείας αυξάνονται, δεν γίνεται να αποφευχθεί η δημιουργία προσαρμοσμένων κανόνων. Ο λόγος είναι γιατί οι προσαρμοσμένοι κανόνες, όπως προδίδει και η ονομασία τους, μπορούν να προσαρμοστούν ανάλογα με τις ανάγκες που θέλουμε να εξυπηρετήσουμε. Οπότε όσο αυξάνονται η ανάγκες για πιο στοχευμένα μέτρα ασφαλείας, τόσο θα αυξάνεται και η ανάγκη για δημιουργία προσαρμοσμένων κανόνων. Γι αυτό τον λόγο είναι σημαντική η γνώση σύνταξης ενός rule[26].

## 3.3 Wazuh Agent και Agentless Monitoring

Σε μια ευρύτερη έννοια, ο όρος agent εισήχθει για να περιγράψει ένα στοιχείο λογισμικού που ενσωματώνεται σε κάποιο υπολογιστικό σύστημα με σκοπό την εκτέλεση ορισμένων καθηκόντων του χρήστη.[27] Στην περίπτωση του Wazuh και γενικότερα στην ασφάλεια πληροφοριακών συστημάτων, η ενσωμάτωση ενός πράκτορα αποτελεί σημαντικό ρόλο για την συλλογή δεδομένων, ενέργειες εντοπισμού και απόκρισης απέναντι σε περιστατικά ασφαλείας. Ο λόγος για τον οποίο παίζουν ένα τόσο σημαντικό ρόλο στην παρακολούθηση γεγονότων ασφαλείας, είναι διότι παρέχουν άμεση και λεπτομερή ενημέρωση των συστημάτων στα οποία εγκαθίσταται. Έτσι μπορεί να δημιουργηθεί ένα περιβάλλον ασφαλείας, κατά το οποίο το Wazuh θα μπορέσει να δημιουργήσει μια πλήρη και λεπτομερή εικόνα σχετικά με την φύση, τον βαθμό επικινδυνότητας καθώς και την προέλευση μιας επίθεσης. Επιπροσθέτως, θα παρέχει πληροφορίες σχετικά με τους τρόπους αντιμετώπισης και εξάλειψης της επίθεσης[28].

Πέρα από την δυνατότητα τροφοδοσίας ενός agent σε ένα σύστημα για παρακολούθηση, το Wazuh παρέχει επιπλέον την δυνατότητα agentless monitoring. Όπως προδίδει και η ονομασία του, το

agentless monitoring αναφέρεται στην παρακολούθηση συστημάτων χωρίς την χρήση πρακτόρων. Ουσιαστικά, για την επίτευξη της δυνατότητας agentless monitoring, το Wazuh συνδέεται με ένα απομακρυσμένο σύστημα μέσω πρωτοκόλλων όπως το SSH.[29] Έτσι μπορούμε να καταλάβουμε πως η πληθώρα των συστημάτων δεν περιορίζεται μόνο σε υπολογιστικά συστήματα, αλλά και σε δικτυακές συσκευές ,όπως τα routers, ακόμα και σε άλλα εργαλεία ασφάλειας όπως το firewall.Οι τρόποι με τους οποίους μπορεί να λειτουργήσει το agentless monitoring που προσφέρει το Wazuh είναι είτε με την παρακολούθηση δεδομένων του απομακρυσμένου συστήματος, ώστε να παρατηρηθούν ανωμαλίες ή αλλαγές που μπορεί να επιφέρουν κίνδυνο, είτε με την δυνατότητα εκτέλεσης εντολών όπου ανάλογα με την φύση των αποτελεσμάτων δημιουργούνται τα κατάλληλα μηνύματα ασφαλείας στον Wazuh.[30]
Παρόλο που παρέχεται η δυνατότητα agentless monitoring από το Wazuh, δεν σημαίνει πως αποτελεί και την βέλτιστη λύση ασφαλείας. Υπάρχουν πολλοί παράγοντες που μπορούν να δυσκολέψουν την διαδικασία του agentless monitoring, όπως η αργή κίνηση δικτύου με αποτέλεσμα να υπάρχουν καθυστερήσεις απέναντι σε περιστατικά ασφαλείας που μπορεί να είναι κρίσιμα.Σίγουρα η εγκατάσταση agent σε πολλά υπολογιστικά συστήματα και εργαλεία ασφάλειας, μπορεί να αποτελεί μια χρονοβόρα διαδικασία καθώς και μια διαδικασία που απαιτεί κάποιους υπολογιστικούς πόρους, έστω και ελάχιστους, ωστόσο διασφαλίζει την σίγουρη, έγκυρη και άμεση αποστολή των δεδομένων ασφαλείας που χρειαζόμαστε. Γι αυτό τον λόγο, πριν την υλοποίηση οποιασδήποτε από τις δύο λύσεις του Wazuh θα πρέπει να γίνει μια σωστή και προσεκτική προσέγγιση ανάλογα με τις απαιτήσεις ασφαλείας, την διαθεσιμότητα των πόρων και το περιβάλλον προστασίας που θέλουμε να δημιουργήσουμε.
Στην παρούσα πτυχιακή εργασία, το πειραματικό πλαίσιο το οποίο δημιουργήθηκε για την προσομοίωση επιθέσεων και ανταπόκρισης τους, δημιουργήθηκε ένα μοντέλο Wazuh με την χρήση agent. Οι λόγοι για τον οποίους χρησιμοποιήθηκε η χρήση agent είναι για να παρακολουθήσουμε την διαδικασία εγκατάστασης, πως συμπεριφέρεται με τον Wazuh Server και για να την άμεση παρακολούθηση και προβολή των αποτελεσμάτων.

### 3.4 Πειραματισμός με το Wazuh

Σε μια πτυχιακή εργασία, η συλλογή και συγγραφή του θεωρητικού σκέλους, αποτελεί τη θεμελιώδη βάση για την ανάλυση και την ερμηνεία φαινομένων που μελετώνται. Η παρουσίαση θεωριών, εννοιών και διαφόρων ερευνών διαμορφώνει ένα πλαίσιο κατανόησης και παρέχει την δυνατότητα εμβάθυνσης στο γνωστικό αντικείμενο που αναλύεται. Ωστόσο, η αξία που μπορεί να έχει το θεωρητικό κομμάτι μιας εργασίας, δεν μπορεί να θεωρηθεί πλήρης χωρίς την αντίστοιχη εφαρμογή του στην πράξη.
Το πρακτικό κομμάτι μιας πτυχιακής εργασίας, όπως προδίδει και το όνομα του, αναλαμβάνει την χρησιμοποίηση όλων αυτών των θεωρητικών αρχών που έχουν αναλυθεί και τις εφαρμόζει στην πράξη ώστε να τεκμηριώσει πλήρως το υπόβαθρό τους. Μέσα από διάφορες πρακτικές που μπορούν να υλοποιηθούν όπως πειραματισμός, μελέτη περίπτωσης ή ανάλυση δεδομένων, δίνετε η δυνατότητα επιβεβαίωσης όλων των θεωρητικών πληροφοριών που καταγράφηκαν. Έτσι, καταλαβαίνουμε πως τόσο η θεωρία όσο και η πράξη λειτουργούν συμπληρωματικά η μια με την άλλη, με την πρώτη να βοηθάει στην εξέλιξη της επιστημονικής σκέψης και την δεύτερη να την τεκμηριώνει.
Στην παρούσα ενότητα θα εξετάσουμε και θα δημιουργήσουμε ένα πειραματικό περιβάλλον με στόχο την τεκμηρίωση όλων των πληροφοριών που καταγράφηκαν στο θεωρητικό κομμάτι της εργασίας, συμβάλοντας στην ολιστική κατανόηση των τεχνολογιών SIEM και πιο συγκεκριμένα του εργαλείου Wazuh.

### 3.4.1 Πειραματικό Περιβάλλον

Σκοπός του πειραματικού περιβάλλοντος που θέλουμε να δημιουργήσουμε, είναι η αναπαράσταση ενός δικτύου και η προσομοίωση επιθέσεων σε αυτό. Για την δημιουργία αυτού του δικτύου χρειάζονται τρια βασικά συστατικά :

- Συστήματα διαχείρισης του δικτύου. Σε αυτά τα συστήματα θα γίνει η εγκατάσταση των εργαλείων ασφαλείας που θέλουμε να ενσωματώσουμε και να αντλήσουμε όλες τις πληροφορίες για τα οφέλη και τα αποτελέσματα που προσφέρουν.
- Συστήματα που ανήκουν στο δίκτυο. Σκόπος αναπαράστασης αυτών των συστημάτων είναι για να δέχονται επιθέσεις και γενικότερα να απεικονίζονται ως θύματα για την εκτέλεση επιθέσεων.
- Συστήματα για την αναπαράσταση επιθέσεων. Τα συγκεκριμένα συστήματα θα λειτουργούν ως κακόβουλες μηχανές για να πραγματοποιούν επιθέσεις στα συστήματα του δικτύου, ώστε να δούμε κατά πόσο ανταποκρίνονται τα εργαλεία ασφάλειας που ενσωματώσαμε.

Έχοντας δημιουργήσει και εξηγήσει θεωρητικά το πειραματικό πλαίσιο που θέλουμε να δημιουργήσουμε και σε συνδυασμό με τις θεωρητικές αρχές που έχουμε αναλύσει, μπορούμε να αναπαραστήσουμε :

- Επιθέσεις
- Αντιμετώπιση Επιθέσεων
- Εξήγηση Επιθέσεων
- Αποτροπή Επιθέσεων

Όλες αυτές οι αναπαραστάσεις, αποτελούν την πρακτική τεκμηρίωση όλων των θεωρητικών αρχών που έχουμε αναλύσει και βοηθούν στην ανάπτυξη και πλήρη κατανόηση τους.
Για την επίτευξη της δημιουργίας αναπαράστασης του δικτύου, των συστημάτων ασφαλείας και των συστημάτων δημιουργίας επιθέσεων είναι απαραίτητη η δημιουργία εικονικών μηχανών (Virtual Machines). Ο λόγος που χρησιμοποιήθηκαν εικονικές μηχανές είναι αυτονόητος καθώς μπορούν πολλές μηχανές να τρέχουν σε ένα σύστημα και επίσης δεν θέλουμε να επηρεαστούν τα πραγματικά συστήματα σε πρώτο στάδιο. Επίσης μπορούμε με ελάχιστους πόρους να πετύχουμε σημαντικά αποτελέσματα σχετικά με τους πειραματισμούς που θέλουμε να πραγματοποιήσουμε. Συγκεκριμένα δημιουργήθηκαν τρεις εικονικές μηχανές όπου η κάθε έχει ξεχωριστό ρόλο από την άλλη :

- Εικονική μηχανή για την εγκατάσταση του Wazuh. Η συγκεκριμένη εικονική μηχανή υλοποιήθηκε για την πλήρη εγκατάσταση του εργαλείου Wazuh. Ο σκοπός της είναι η δυνατότητα εντοπισμού, ανάλυσης και αποτροπής επιθέσεων.
- Εικονική μηχανή για την αναπαράσταση συστήματος του δικτύου και εγκατάστασης του Wazuh Agent. Όπως είναι λογικό, θα πρέπει να υπάρχει ένα σύστημα το οποίο θα δέχεται επιθέσεις και θα αποστέλλει μηνύματα ασφαλείας στον Wazuh Manager.
- Εικονική μηχανή για την δημιουργία επιθέσεων. Μια μηχανή για την αναπαράσταση και εκτέλεση επιθέσεων απέναντι στον Wazuh Agent, πάντα σε πλαίσια πειραματισμού.

Οι εικονικές μηχανές που δημιουργήθηκαν για την εγκατάσταση του Wazuh και το Wazuh Agent είναι υλοποιημένες σε λειτουργικό σύστημα Ubuntu, ενώ η εικονική μηχανή για την δημιουργία και αναπαράσταση επιθέσεων είναι υλοποιημένη σε Kali Linux. Συνοπτικά, το Kali Linux αποτελεί ένα λειτουργικό σύστημα Unix το οποίο έχει προεγκατεστημένες εντολές επιθέσεων και χρησιμοποιείται κυρίως για δοκιμές ασφαλείας και ethical hacking. Οπότε αποτελεί σημαντικό εργαλείο για τον πειραματισμό μας.
Τα τεχνικά χαρακτηριστικά που είχε κάθε εικονική μηχανή ήταν:

- 2 Πυρηνες
- 4 GB RAM
- 30+ GB Storage

Σε θέμα δικτύου, κάθε εικονική μηχανή είχε δύο κάρτες δικτύου :

- 1 κάρτα δικτύου για NAT ώστε να είναι συνδεδεμένες με το διαδίκτυο
- 1 κάρτα δικτύου για εσωτερικό δίκτυο ώστε να επικοινωνούν μεταξύ τους, χωρίς να υπάρξουν επιπλοκές με άλλες μηχανές και δίκτυα.

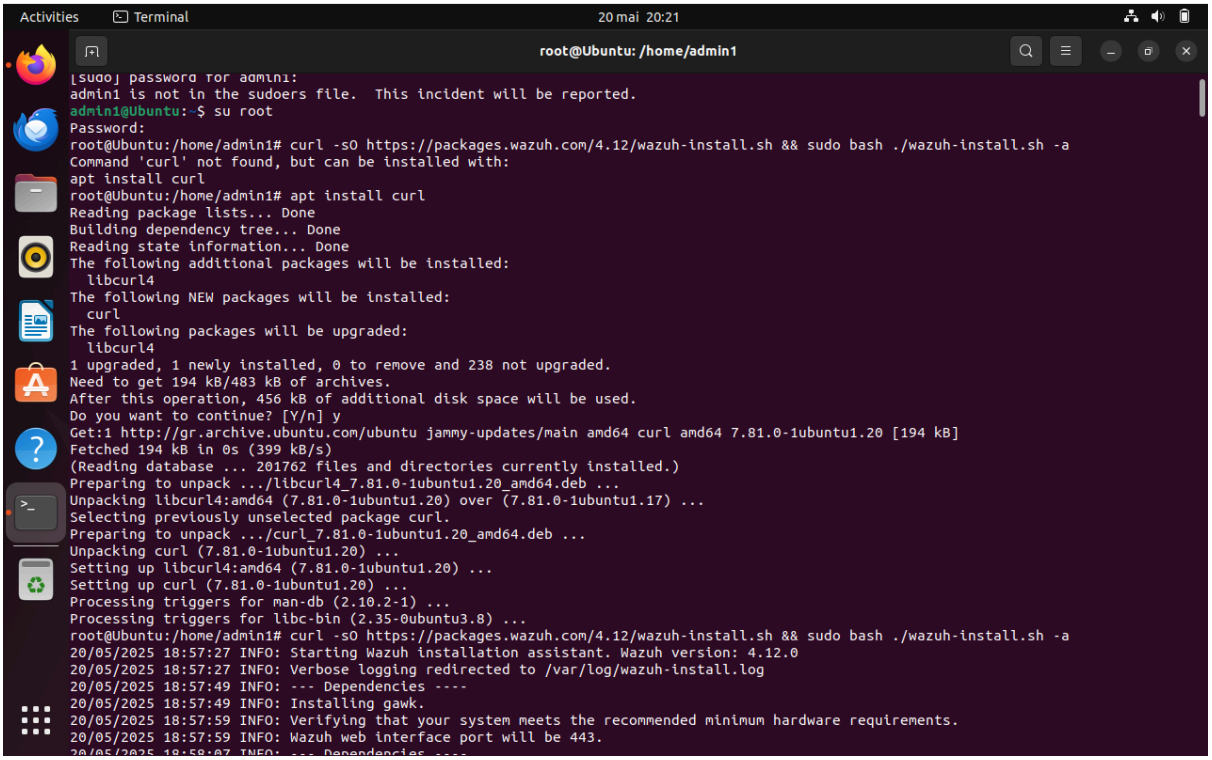
Η παρατήρηση για την προσθήκη δύο καρτών δικτύου για το κάθε σύστημα αποτελεί σημαντική καθώς πρέπει να διευκρινίσουμε πως θα μοιάζει η αρχιτεκτονική του δικτύου που θα δημιουργήσουμε για πειραματισμό. Το εσωτερικό δίκτυο που δημιουργήσαμε είναι το 10.10.10.0/24 και η IP που πήρε το κάθε σύστημα είναι :

- 10.10.10.10 για την μηχανή Kali Linux
- 10.10.10.11 για το Wazuh
- 10.10.10.12 για τον Wazuh Agent

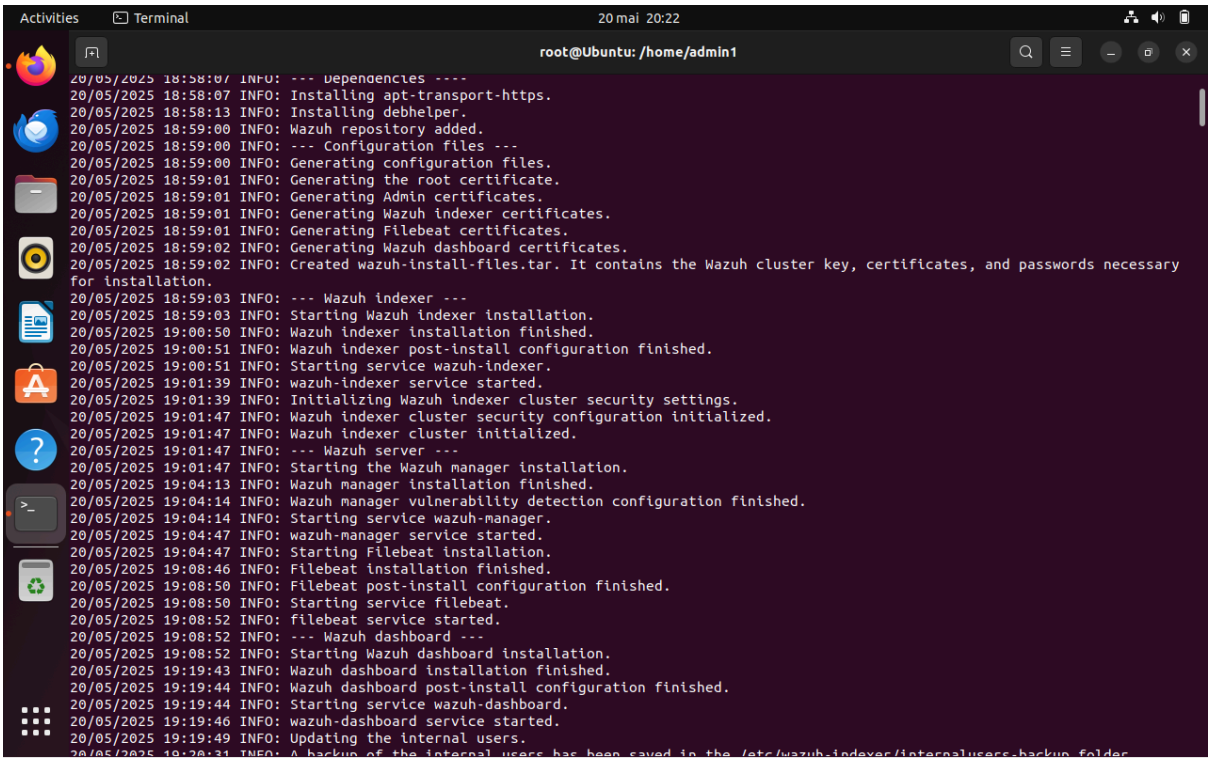
### 3.4.2 Εγκατάσταση Wazuh και Components

Εφόσον έχουμε ολοκληρώσει την προεργασία για την δημιουργία των εικονικών μας μηχανών και έχουμε εγκαταστήσει το λειτουργικό πρόγραμμα για την κάθε μια, περνάμε στο στάδιο εγκατάστασης των εργαλείων ασφαλείας που χρειάζεται η κάθε μηχανή.
Στην πρώτη εικονική μηχανή και εφόσον έχουμε εγκατάσταση του λειτουργικού προγράμματος και την διαμόρφωση των ρυθμίσεων σε ότι αφορά το δίκτυο της, περνάμε στο στάδιο εγκατάστασης του Wazuh. Μέσω του επίσημου ιστότοπου του Wazuh υπάρχει εντολή για να το κατεβάσουμε. εντολή εκτελείται μέσω του root και έχοντας εγκαταστήσει την εντολή curl και είναι η curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh && sudo bash ./wazuh-install.sh -a. Εκτελώντας την παραπάνω εντολή ξεκινάει η διαδικασία εγκατάσταση του Wazuh. Όπως θα παρατηρήσουμε στις παρακάτω εικόνες, γίνεται εγκατάσταση διαφόρων εργαλείων του Wazuh, πιο συγκεκριμένα [31]:

- Wazuh Indexer : Αποτελεί το εργαλείο αποθήκευσης ειδοποιήσεων που δημιουργούνται από τον Wazuh Server και παρέχει την δυνατότητα αναζήτησης και ανάλυσης δεδομένων
- Wazuh Server : Χρησιμοποιείται για την ανάλυση δεδομένων που λαμβάνονται από τους πράκτορες και την δημιουργία ειδοποιήσεων σε περιπτώσεις απειλών ή ανωμαλιών. Μπορεί να χρησιμοποιηθεί και απομακρυσμένα για την διαχείριση και παρακολούθηση πρακτόρων.
- Wazuh Dashboard : Το συγκεκριμένο εργαλείο αποτελεί μια διεπαφή απεικόνισης συμβάντων ασφαλείας με την δυνατότητα οπτικοποίησης τους. Με αυτό τον τρόπο βοηθάει τους χρήστες για την καλύτερη παρακολούθηση και ανάγνωση δεδομένων ασφαλείας, τρωτών σημείων και άλλων αποτελεσμάτων που προκύπτουν σε περιπτώσεις απειλής ή ανωμαλιών.
- Certificates για την χρήση κάθε εργαλείου

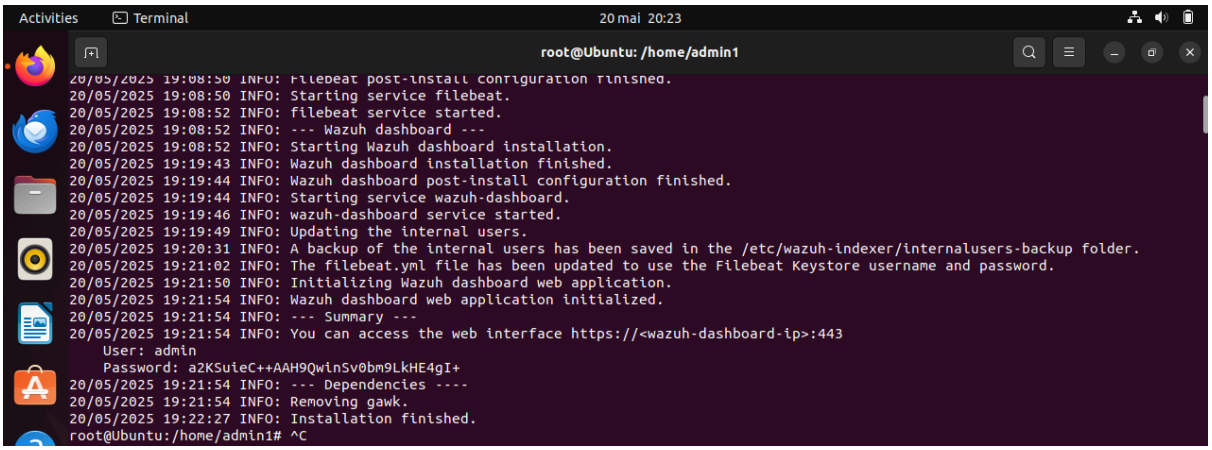



**Εικόνα 3.1 : Εγκατάσταση Wazuh**




**Εικόνα 3.2 : Εγκατάσταση Wazuh**

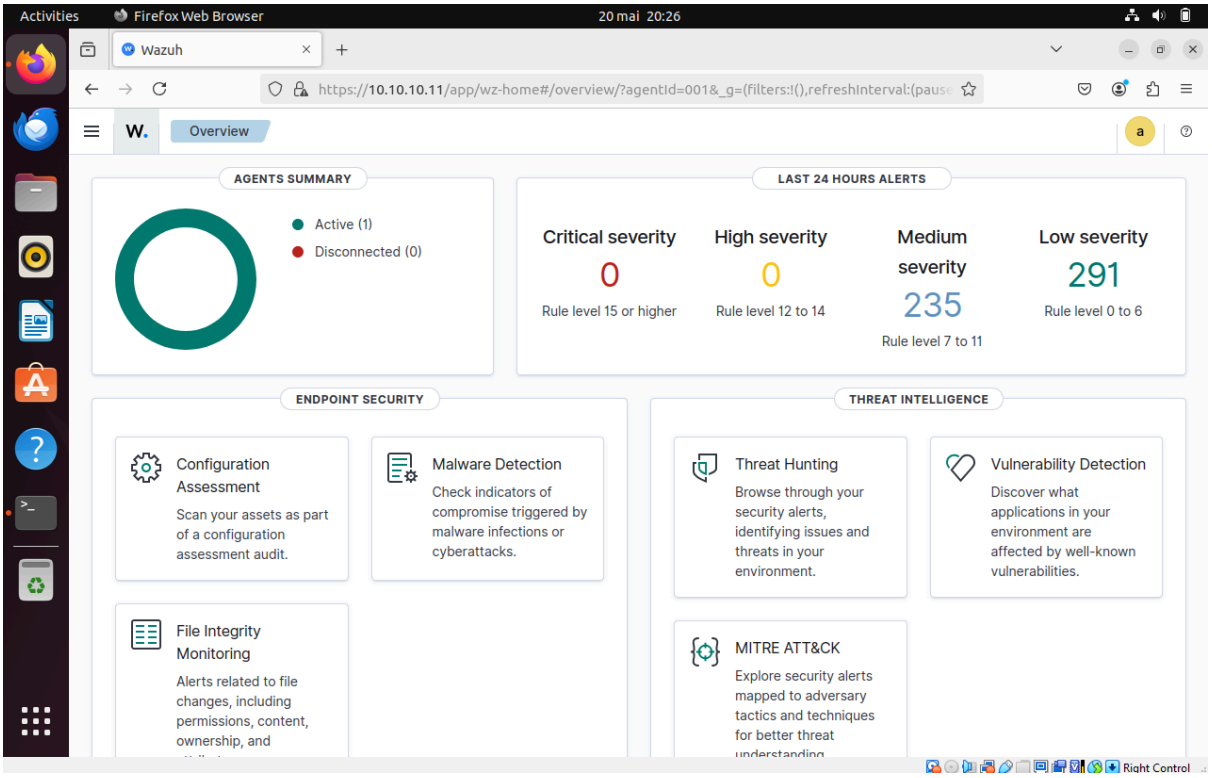
Με την ολοκλήρωση εγκατάστασης του Wazuh δημιουργείται ένας χρήστης για την πρόσβαση στο περιβάλλον διαχείρισης του, όπως φαίνεται στην παρακάτω εικόνα.




**Εικόνα 3.3 : Ολοκλήρωση εγκατάστασης Wazuh και δημιουργία χρήστη**

Για να μπορέσουμε να συνδεθούμε στο περιβάλλον διαχείρισης του Wazuh αυτό που χρειάζεται να κάνουμε είναι να πληκτρολογήσουμε την ip του εσωτερικού μας δικτύου και να συμπληρώσουμε τα στοιχεία που δημιούργησε με την εγκατάστασή του. Επίσης να σημειωθεί πως μπορούμε να αποκτήσουμε πρόσβαση με οποιαδήποτε ip έχει το σύστημα μας.

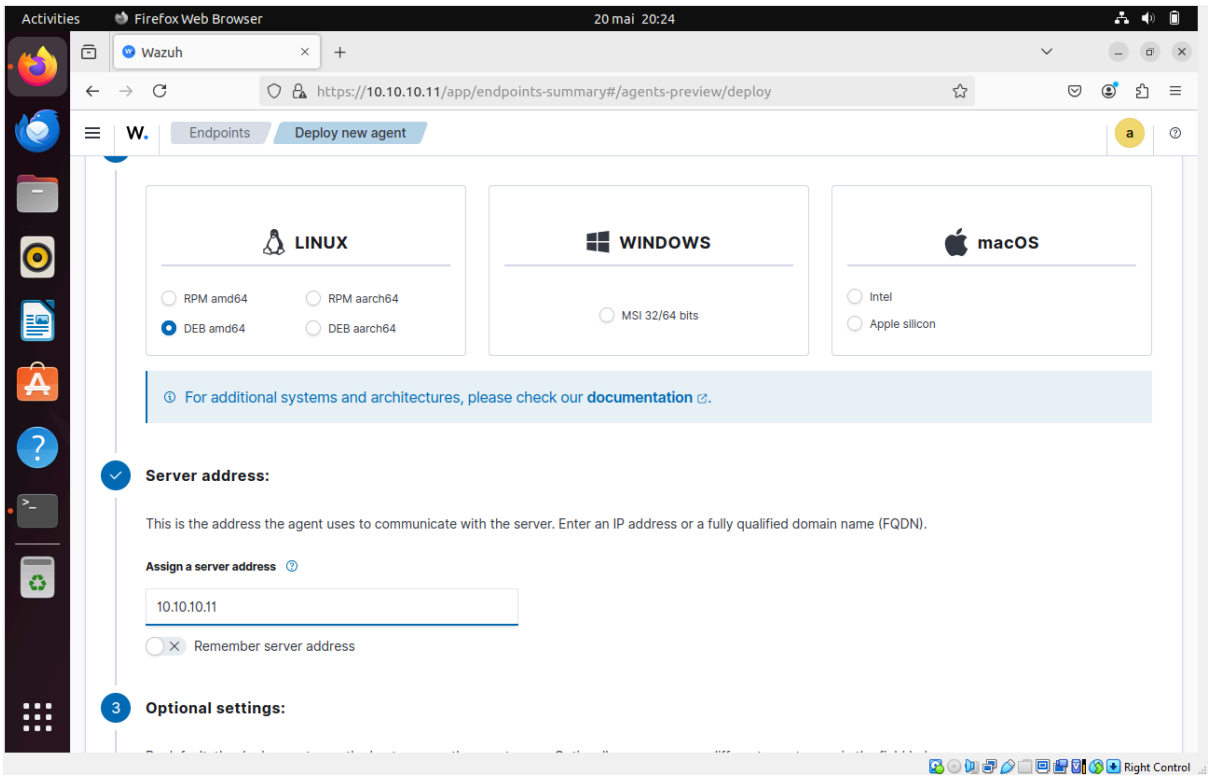
Εφόσον όλα πάνε καλά τότε συνδεόμαστε στο περιβάλλον διαχείρισης του όπως στην επόμενη εικόνα.



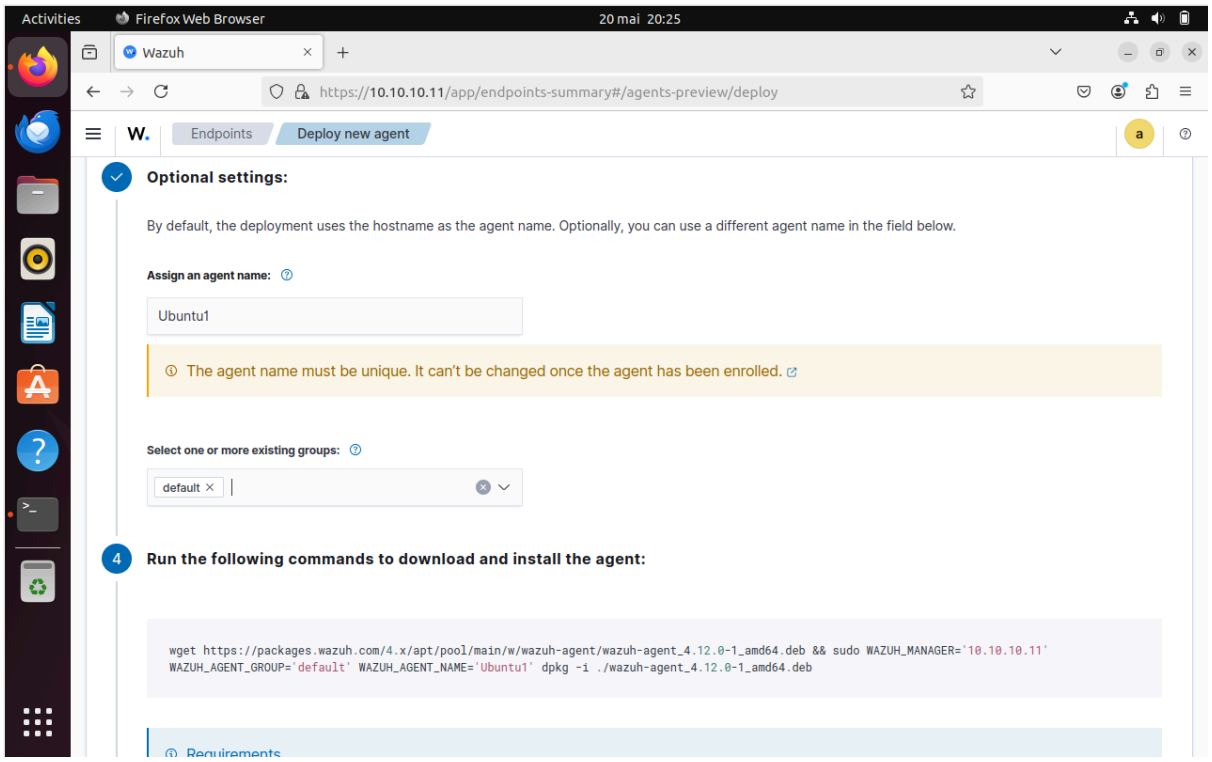

**Εικόνα 3.4 : Περιβάλλον διαχείρισης Wazuh**

Σε δεύτερο στάδιο, θα πρέπει να εγκαταστήσουμε έναν πράκτορα.

Στην 2η εικονική μηχανή που δημιουργήσαμε ακολουθούμε τα ίδια βήματα εγκατάστασης και διαμόρφωσης του λειτουργικού συστήματος καθώς και δικτύωσης. Ωστόσο για να μπορέσουμε να εγκαταστήσουμε τον πράκτορα σε αυτό το σύστημα θα χρειαστεί η λειτουργία του συστήματος Wazuh. Μέσω του διαχειριστικού περιβάλλοντος επιλέγουμε την προσθήκη ενός νέου πράκτορα και μας κατευθύνει στο παρακάτω μενού επιλογών.




**Εικόνα 3.5 : Εγκατάσταση Agent**




**Εικόνα 3.6 : Εγκατάσταση Agent**

Στην συνέχεια ακολουθούμε τα εξής βήματα:

- Επιλέγουμε στο πεδίο Linux την επιλογή DEB amd64

- Συμπληρώνουμε στο κενό του Server Address την IP του Manager (στην δική μας περίπτωση το 10.10.10.11)
- Ονομάζουμε τον πράκτορα και τον κατατάσσουμε σε ένα γκρουπ πρακτόρων, εαν υπάρχει αλλιώς αφήνουμε την προεπιλογή
- Εφόσον έχουμε συμπληρώσει τις παραπάνω πληροφορίες δημιουργείται μια εντολή που την τρέχουμε στην μηχανή του πράκτορα για την εγκατάσταση του.

Με την εκτέλεση της εντολής λαμβάνουμε τα εξής αποτελέσματα :

```
root@Agent:/home/agent# wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.12.0-1_amd64.deb && sudo WAZUH
_MANAGER='10.10.10.11' WAZUH_AGENT_GROUP='default' WAZUH_AGENT_NAME='Ubuntu' dpkg -i ./wazuh-agent_4.12.0-1_amd64.deb
--2025-05-20 19:50:00--  https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.12.0-1_amd64.deb
Resolving packages.wazuh.com (packages.wazuh.com)... 13.224.186.40, 13.224.186.100, 13.224.186.32, ...
Connecting to packages.wazuh.com (packages.wazuh.com)|13.224.186.40|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 11963008 (11M) [application/vnd.debian.binary-package]
Saving to: 'wazuh-agent_4.12.0-1_amd64.deb.2'

wazuh-agent_4.12.0- 100%[==================>]  11,41M  7,83MB/s    in 1,5s

2025-05-20 19:50:02 (7,83 MB/s) - 'wazuh-agent_4.12.0-1_amd64.deb.2' saved [11963008/11963008]

(Reading database ... 202204 files and directories currently installed.)
Preparing to unpack .../wazuh-agent_4.12.0-1_amd64.deb ...
Unpacking wazuh-agent (4.12.0-1) over (4.12.0-1) ...
Setting up wazuh-agent (4.12.0-1) ...
root@Agent:/home/agent# sudo systemctl daemon-reload
root@Agent:/home/agent# sudo systemctl enable wazuh-agent_4.12.0-1_amd64.deb
Failed to enable unit: Unit file wazuh-agent_4.12.0-1_amd64.deb.service does not exist.
root@Agent:/home/agent# sudo systemctl enable wazuh-agent
root@Agent:/home/agent# sudo systemctl start wazuh-agent
```

**Εικόνα 3.7 : Εγκατάσταση Agent**

Αυτό σημαίνει πως τα πακέτα για την εγκατάσταση του πράκτορα, εγκαταστάθηκαν με επιτυχία.
Για να μπορέσει ο πράκτορα να τεθεί σε λειτουργία αρκεί να ακολουθήσουμε τα παρακάτω βήματα :


**Εικόνα 3.8 : Ενεργοποίηση Agent**

Εκτελόντας τις παραπάνω εντολές, πλέον ο πράκτορας είναι σε λειτουργία.

### 3.4.3 Προσομοίωση Επιθέσεων

Από την στιγμή που ολοκληρώθηκε η διαδικασία εγκατάστασης του Wazuh Manager και του Wazuh Agent, αυτό που μας απομένει να δούμε είναι κατά πόσο σωστά έγινε η εγκατάσταση τους και πλέον να μπορέσουμε να παρατηρήσουμε το κατά πόσο καλά δουλεύουν.Δημιουργούμε την τρίτη εικονική μηχανή και εγκαθιστούμε το λειτουργικό σύστημα Kali Linux. Εν συνεχεία πραγματοποιούμε τις κατάλληλες διαμορφώσεις σχετικά με την δικτύωση του και πλέον είμαστε έτοιμοι για πειραματισμό.

Μια προσομοίωση που θα μπορούσαμε να πραγματοποιήσουμε είναι οι συνεχείς προσπάθειες για σύνδεση μέσω ssh. Γι να μπορέσουμε να εκτελέσουμε το παραπάνω παράδειγμα, θα πρέπει αρχικά να δημιουργήσουμε την υπηρεσία SSH μέσω της εικονικής μηχανής που έχουμε εγκαταστήσει τον Wazuh Agent, ώστε να μπορέσουμε να αντλήσουμε τα αποτελέσματα. Η εντολή που χρησιμοποιήθηκε για την δημιουργία SSH είναι η
**sudo apt install openssh-server -y,** όπως φαίνεται και στην παρακάτω φωτογραφία.

```
root@Agent:/home/agent# sudo apt install openssh-server -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  ncurses-term openssh-client openssh-sftp-server ssh-import-id
Suggested packages:
  keychain libpam-ssh monkeysphere ssh-askpass molly-guard
The following NEW packages will be installed:
  ncurses-term openssh-server openssh-sftp-server ssh-import-id
The following packages will be upgraded:
  openssh-client
1 upgraded, 4 newly installed, 0 to remove and 238 not upgraded.
Need to get 751 kB/1.654 kB of archives.
After this operation, 6.050 kB of additional disk space will be used.
Get:1 http://gr.archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-sftp-server amd64 1:8.9p1-3ubuntu0.
Get:2 http://gr.archive.ubuntu.com/ubuntu jammy-updates/main amd64 openssh-server amd64 1:8.9p1-3ubuntu0.13 [4
Get:3 http://gr.archive.ubuntu.com/ubuntu jammy-updates/main amd64 ncurses-term all 6.3-2ubuntu0.1 [267 kB]
Get:4 http://gr.archive.ubuntu.com/ubuntu jammy/main amd64 ssh-import-id all 5.11-0ubuntu1 [10,1 kB]
Fetched 751 kB in 1s (539 kB/s)
Preconfiguring packages ...
(Reading database ... 202204 files and directories currently installed.)
Preparing to unpack .../openssh-client_1%3a8.9p1-3ubuntu0.13_amd64.deb ...
Unpacking openssh-client (1:8.9p1-3ubuntu0.13) over (1:8.9p1-3ubuntu0.10) ...
Selecting previously unselected package openssh-sftp-server.
Preparing to unpack .../openssh-sftp-server_1%3a8.9p1-3ubuntu0.13_amd64.deb ...
Unpacking openssh-sftp-server (1:8.9p1-3ubuntu0.13) ...
Selecting previously unselected package openssh-server.
Preparing to unpack .../openssh-server_1%3a8.9p1-3ubuntu0.13_amd64.deb ...
Unpacking openssh-server (1:8.9p1-3ubuntu0.13) ...
Selecting previously unselected package ncurses-term.
Preparing to unpack .../ncurses-term_6.3-2ubuntu0.1_all.deb ...
Unpacking ncurses-term (6.3-2ubuntu0.1) ...
Selecting previously unselected package ssh-import-id.
Preparing to unpack .../ssh-import-id_5.11-0ubuntu1_all.deb ...
Unpacking ssh-import-id (5.11-0ubuntu1) ...
```

**Εικόνα 3.9 : Εγκατάσταση SSH**

Εφόσον έχουμε κάνει εγκατάσταση τον SSH server ελέγχουμε εάν είναι ενεργός με την εντολή sudo systemctl status ssh και βλέπουμε εάν είναι active όπως στην παρακάτω εικόνα.

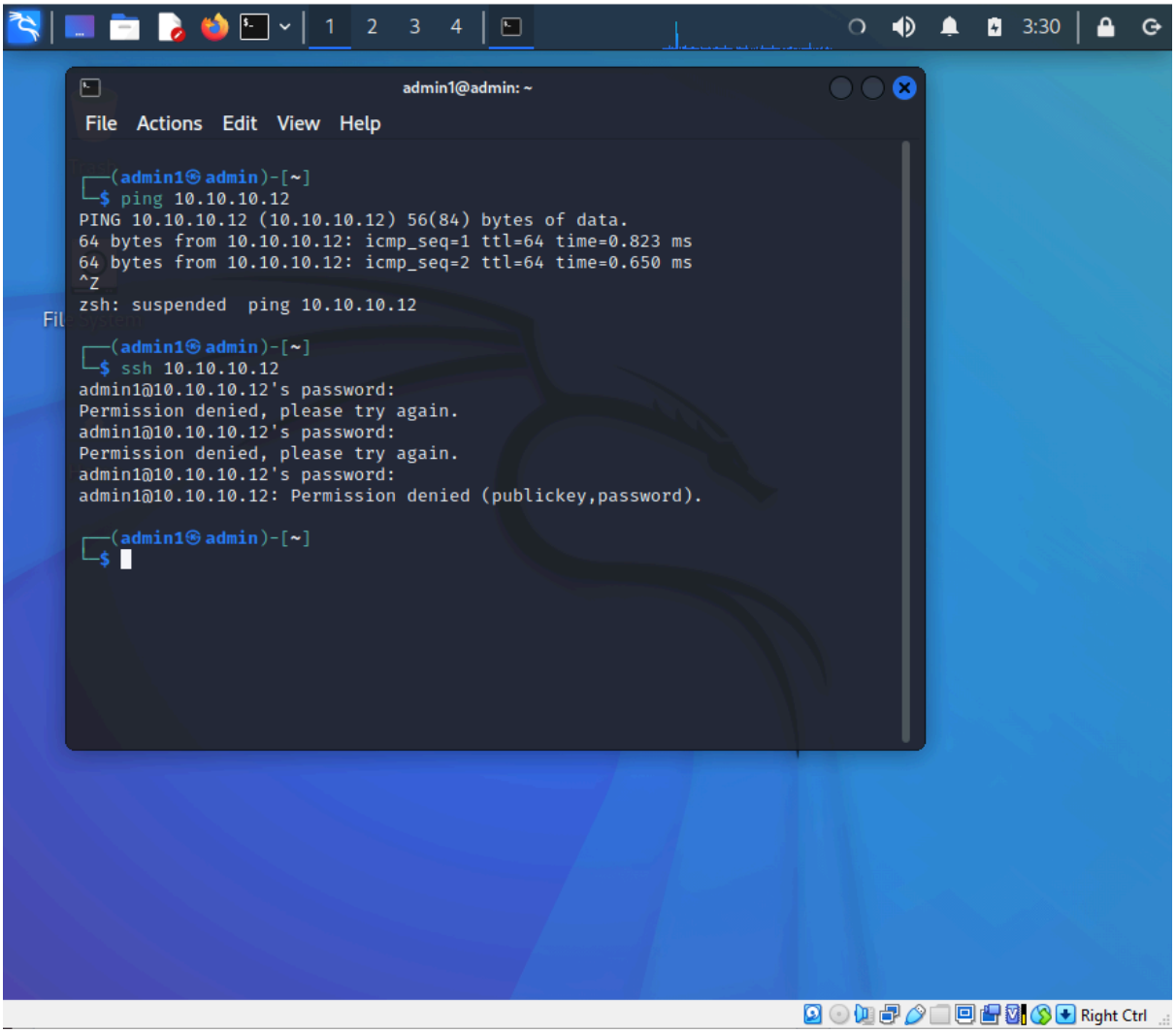
```
root@Agent:/home/agent# sudo systemctl status ssh
* ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: e>
     Active: active (running) since Tue 2025-05-20 19:56:51 EEST; 25s ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 11041 (sshd)
      Tasks: 1 (limit: 4608)
     Memory: 1.7M
        CPU: 23ms
     CGroup: /system.slice/ssh.service
             `-11041 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

mai 20 19:56:51 Agent systemd[1]: Starting OpenBSD Secure Shell server...
mai 20 19:56:51 Agent sshd[11041]: Server listening on 0.0.0.0 port 22.
mai 20 19:56:51 Agent sshd[11041]: Server listening on :: port 22.
mai 20 19:56:51 Agent systemd[1]: Started OpenBSD Secure Shell server.
lines 1-16/16 (END)
[1]+  Stopped                 sudo systemctl status ssh
```

**Εικόνα 3.10 : Εγκατάσταση SSH**

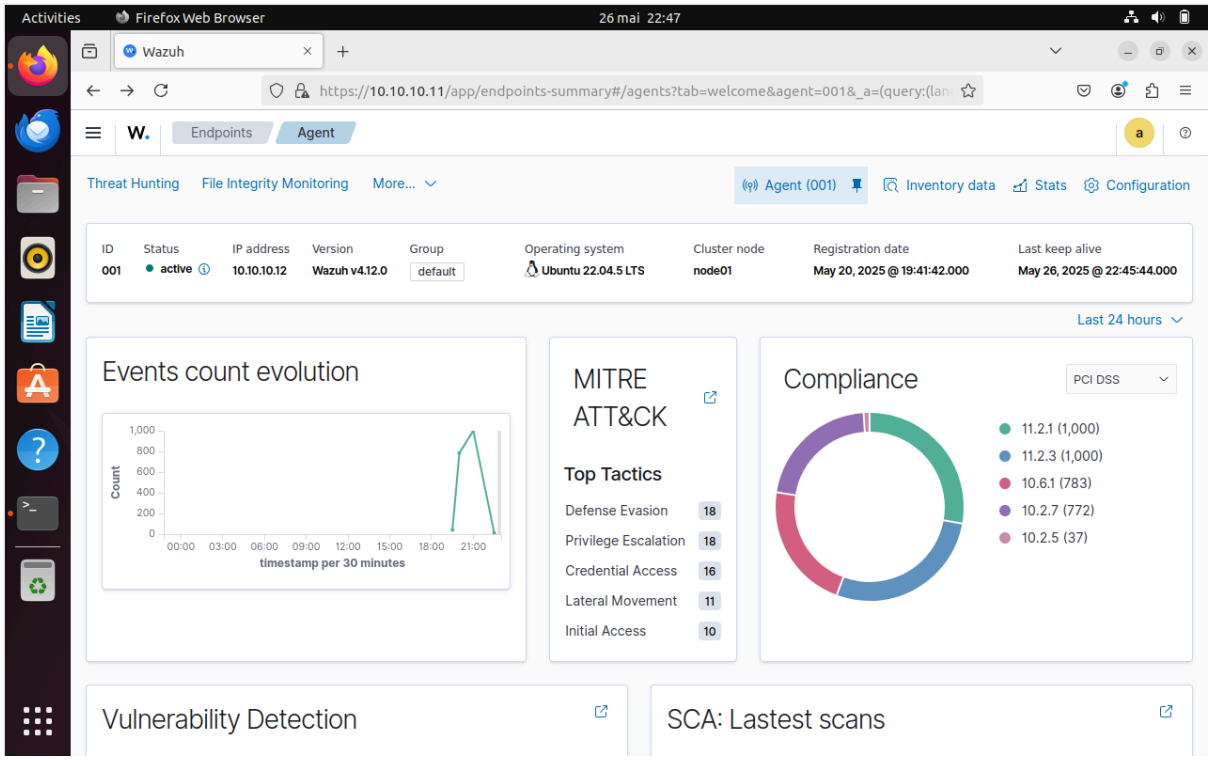
Συνδεόμαστε στην εικονική μηχανή Kali Linux και επιχειρούμε να συνδεθούμε μέσω SSH στον Agent. Σε κάθε προσπάθεια βάζουμε λανθασμένο κωδικό ώστε να εμφανιστούν μηνύματα

αποτυχημένων προσπαθειών σύνδεσης για να δούμε τα αντίστοιχα αποτελέσματα στο Wazuh.



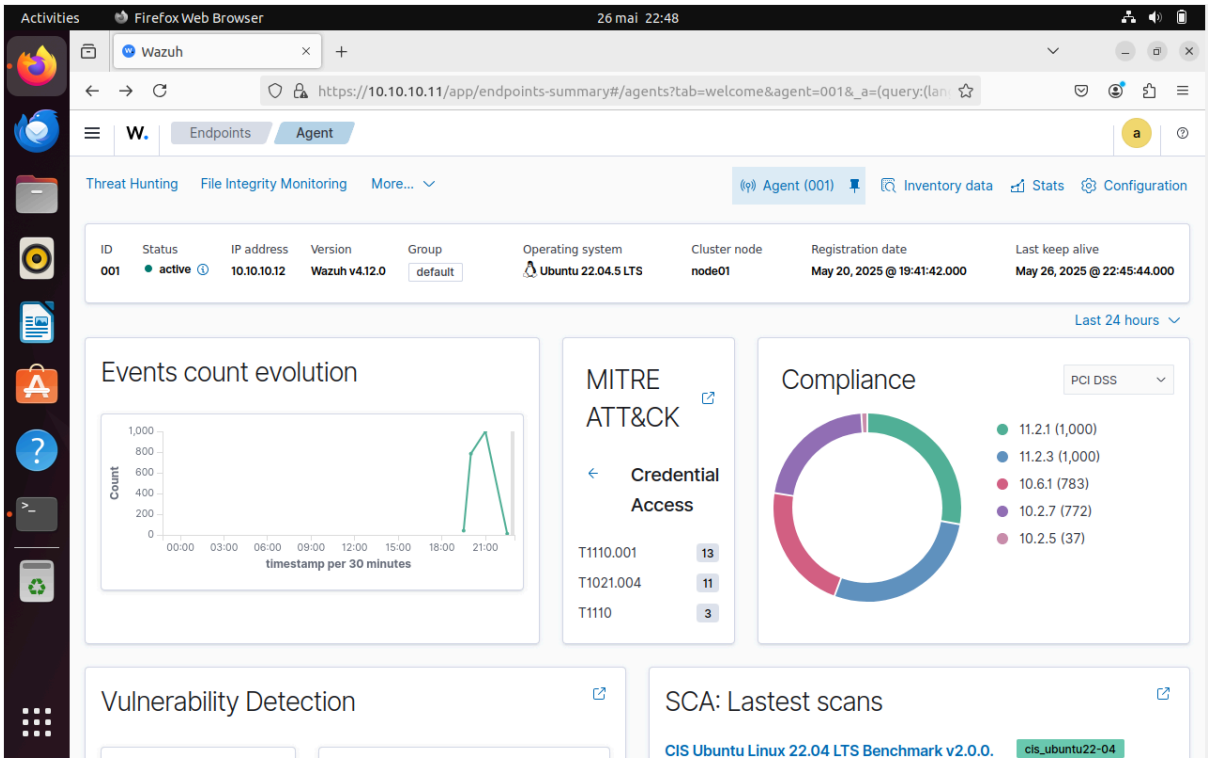

**Εικόνα 3.11 : Διαδικασία πολλαπλών λανθασμένων προσπαθειών σύνδεσης**

Επιστρέφουμε στην εικονική μηχανή του Wazuh και μπαίνουμε στο περιβάλλον διαχείρισης του Agent. Στην εικόνα που ακολουθεί μας ενδιαφέρει το πλαίσιο MITRE ATT&CK στο οποίο αναγράφονται όλα τα περιστατικά που συλλέχθηκαν από τον Agent. Πιο συγκεκριμένα μας ενδιαφέρει η επιλογή Credential Access καθώς το πείραμα μας αφορά λανθασμένη προσθήκη στοιχείων πρόσβασης.



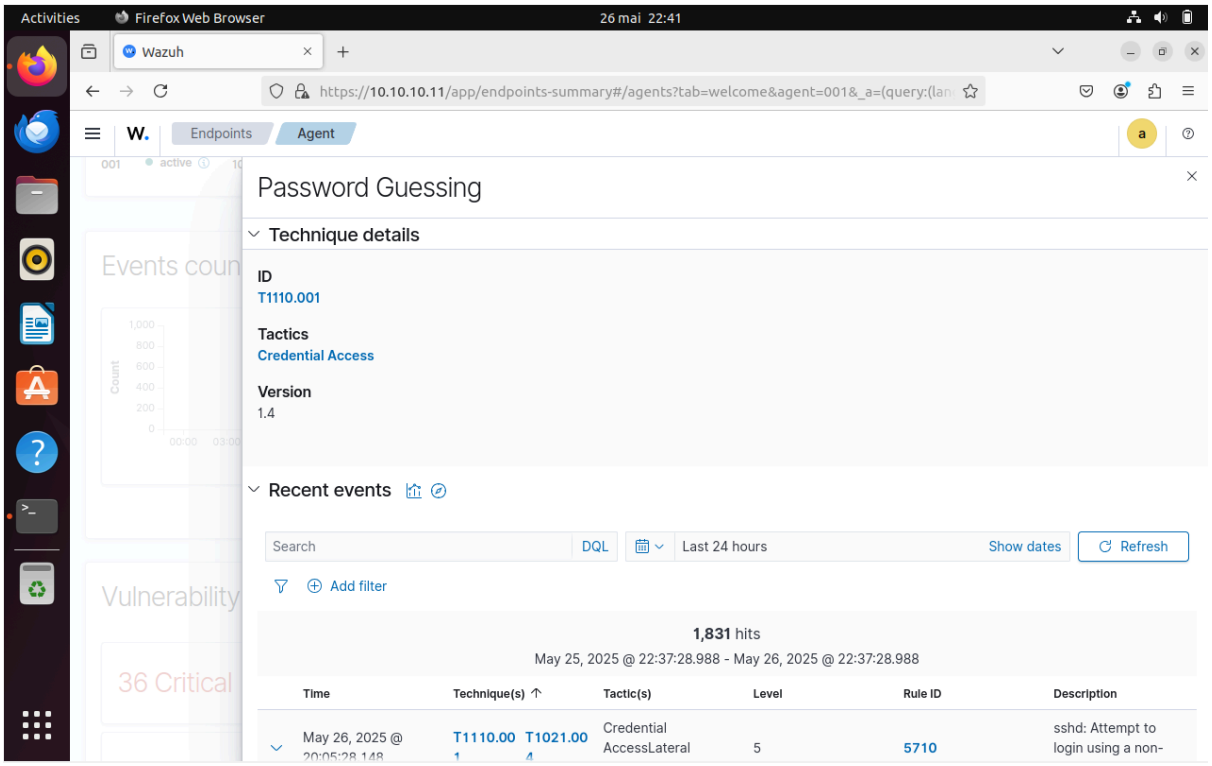

**Εικόνα 3.12 : Περιβάλλον διαχείρισης Agent και MITRE ATT&CK**

Πατώντας την επιλογή Credential Access μας εμφανίζονται στοιχεία σχετικά με την υπηρεσία και τους τρόπους με τους οποίους πραγματοποιήθηκε η επίθεση. Επίσης για κάθε συγκεκριμένη πληροφορία υπάρχει ένα id για τον προσδιορισμό κάθε υπηρεσίας και τρόπου επιθέσεως.



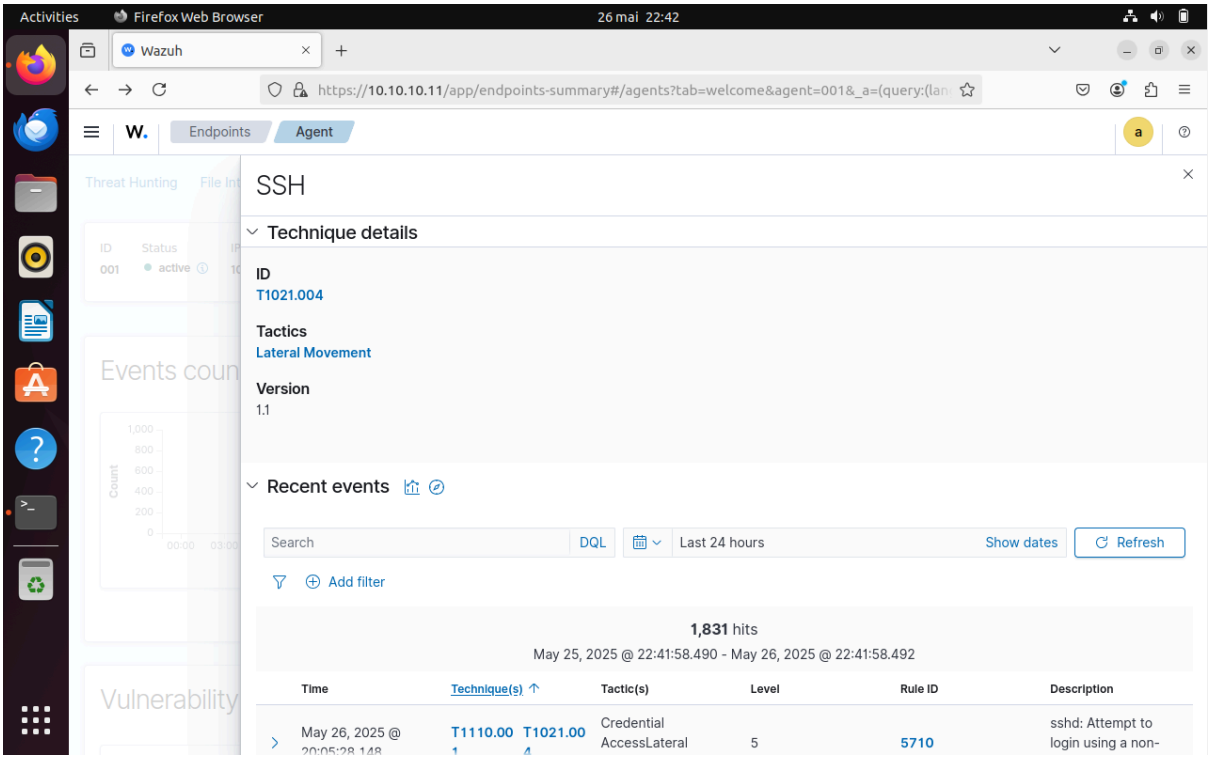
**Εικόνα 3.13 : Περιβάλλον διαχείρισης Agent και MITRE ATT&CK**

Το ID T1110.001 αναφέρεται στην μέθοδο Password Guessing. Ουσιαστικά μας αναφέρει πως ο χρήστης προσπάθησε να μαντέψει τον κωδικό πρόσβασης για την πρόσβαση του στο SSH.



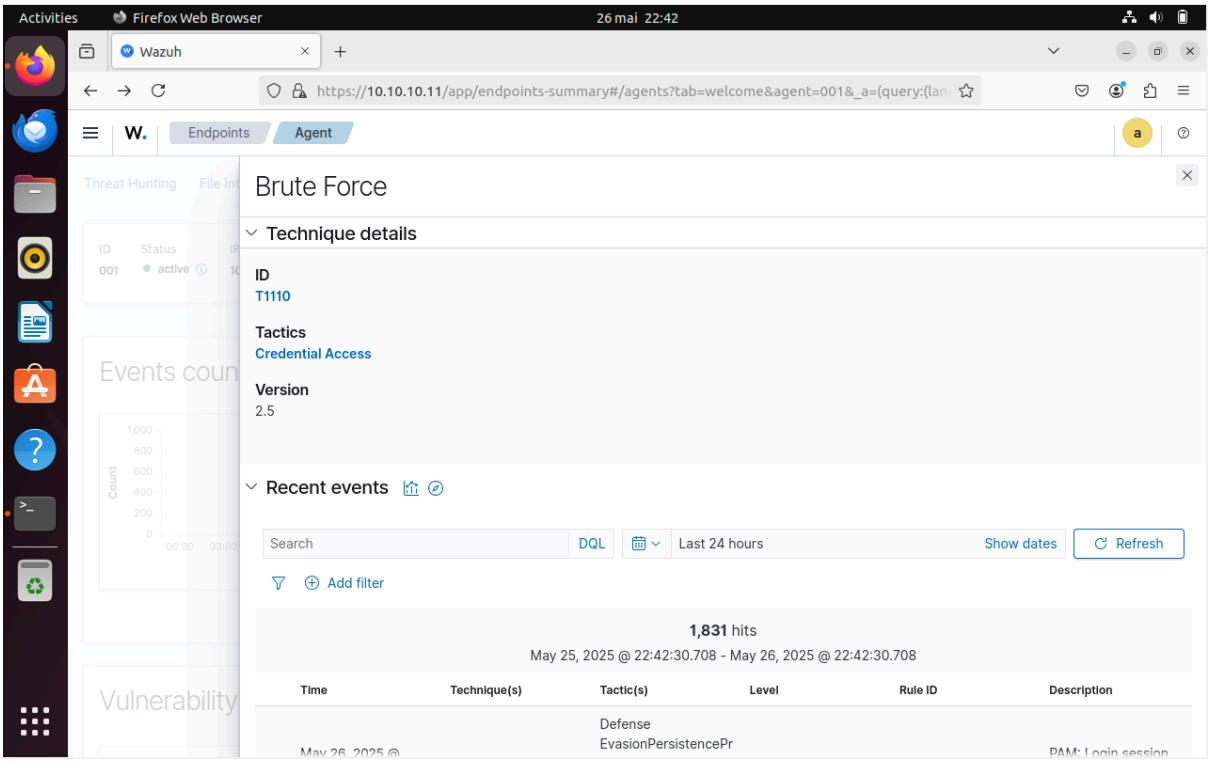

**Εικόνα 3.14 : Αποτελέσματα επίθεσης**

Το ID T1021.004 αναφέρεται στην υπηρεσία SSH. Δηλαδή γίνετε αναφορά στην υπηρεσία όπου πραγματοποιήθηκε η επίθεση.



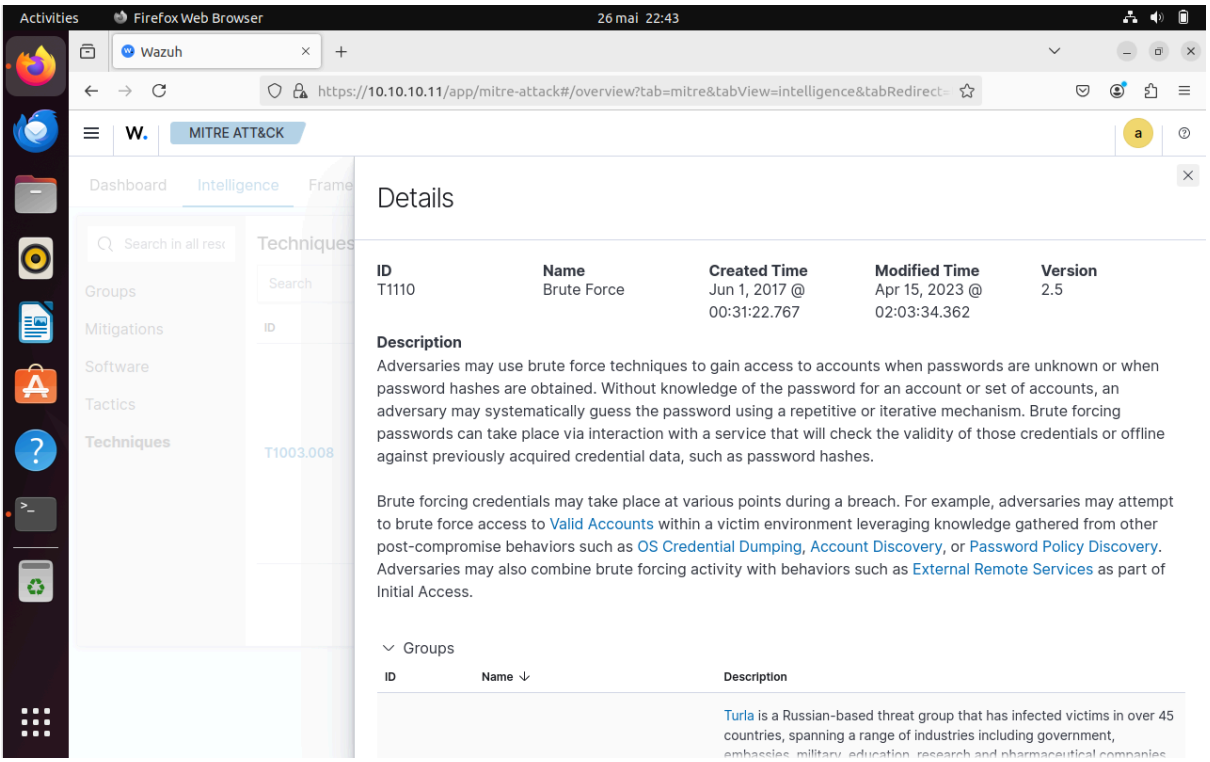
**Εικόνα 3.15 : Αποτελέσματα επίθεσης**

Το ID T1110 αναφέρεται στην μέθοδο υλοποίησης επίθεσης που γίνεται μέσω Brute Force. Με αυτό τον τρόπο θέλει να δικαιολογήσει ότι η επίθεση πραγματοποιήθηκε με μεθόδους Brute Force.




**Εικόνα 3.16 : Αποτελέσματα επίθεσης**

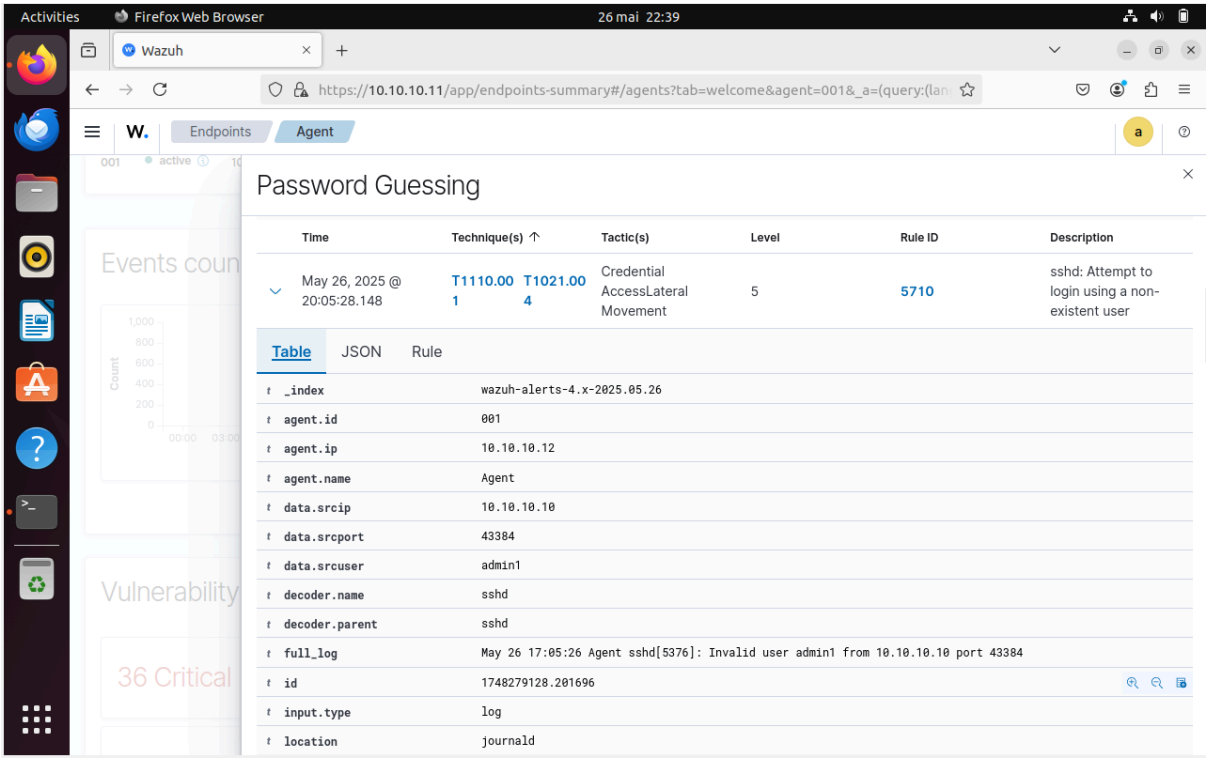
Επίσης ένα πάρα πολύ σημαντικό χαρακτηριστικό που προσφέρει το Wazuh είναι πως πατώντας πάνω στο ID, παρέχει αναλυτικές πληροφορίες για την μέθοδο επίθεσης όπως φαίνεται στην παρακάτω εικόνα.

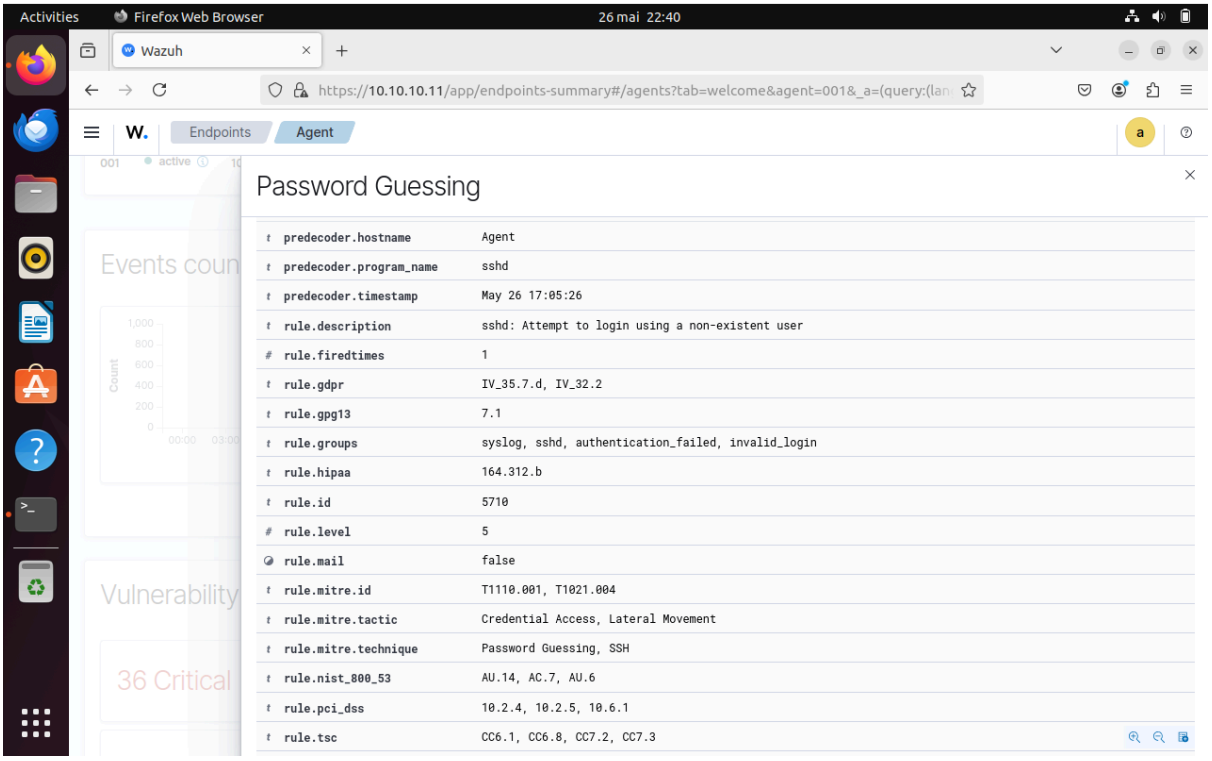



**Εικόνα 3.17 : Αποτελέσματα επίθεσης**

Το Wazuh συλλέγει ένα τεράστιο πλήθος γεγονότων που εξελίσσονται σε ένα δίκτυο. Πατώντας σε ένα από τα γεγονότα που έχει αποθηκεύσει, μπορούμε να παρατηρήσουμε πόσο αναλυτικό μπορεί να γίνει σχετικά με την απειλή την οποία δέχτηκε και τι εξηγήσεις μπορεί να δώσει. Πληροφορίες που μπορεί να δώσει είναι :

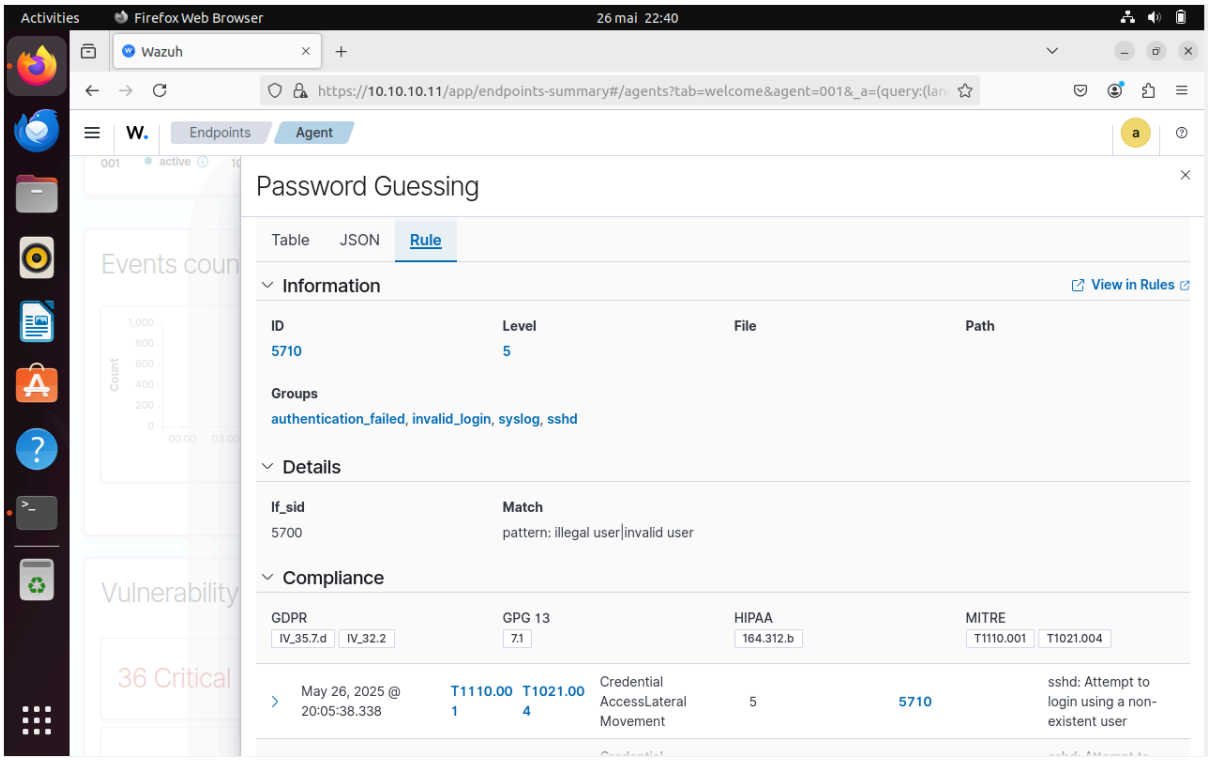
- Από ποιόν προέκυψε η επίθεση
- Ποιός δέχθηκε την επίθεση
- Με ποιόν τρόπο επιτέθηκε
- Σε ποιά ομάδα κανόνων ανήκει η συγκεκριμένη επίθεση
- Πληροφορίες που αφορούν χρονική περίοδο εξέλιξης της επίθεσης


Activities
Firefox Web Browser
26 mai 22:39
Wazuh
https://10.10.10.11/app/endpoints-summary#/agents?tab=welcome&agent=001&_a=(query:(lan
Endpoints
Agent
Password Guessing
Time
Technique(s)
Tactic(s)
Level
Rule ID
Description
May 26, 2025 @ 20:05:28.148
T1110.001
T1021.004
Credential Access Lateral Movement
5
5710
sshd: Attempt to login using a non-existent user
Table
JSON
Rule
_index wazuh-alerts-4.x-2025.05.26
agent.id 001
agent.ip 10.10.10.12
agent.name Agent
data.srcip 10.10.10.10
data.srcport 43384
data.srcuser admin1
decoder.name sshd
decoder.parent sshd
full_log May 26 17:05:26 Agent sshd[5376]: Invalid user admin1 from 10.10.10.10 port 43384
id 1748279128.201696
input.type log
location journald


Activities
Firefox Web Browser
26 mai 22:40
Wazuh
https://10.10.10.11/app/endpoints-summary#/agents?tab=welcome&agent=001&_a=(query:(lan
Endpoints
Agent
Password Guessing
predecoder.hostname Agent
predecoder.program_name sshd
predecoder.timestamp May 26 17:05:26
rule.description sshd: Attempt to login using a non-existent user
rule.firedtimes 1
rule.gdpr IV_35.7.d, IV_32.2
rule.gpg13 7.1
rule.groups syslog, sshd, authentication_failed, invalid_login
rule.hipaa 164.312.b
rule.id 5710
rule.level 5
rule.mail false
rule.mitre.id T1110.001, T1021.004
rule.mitre.tactic Credential Access, Lateral Movement
rule.mitre.technique Password Guessing, SSH
rule.nist_800_53 AU.14, AC.7, AU.6
rule.pci_dss 10.2.4, 10.2.5, 10.6.1
rule.tsc CC6.1, CC6.8, CC7.2, CC7.3

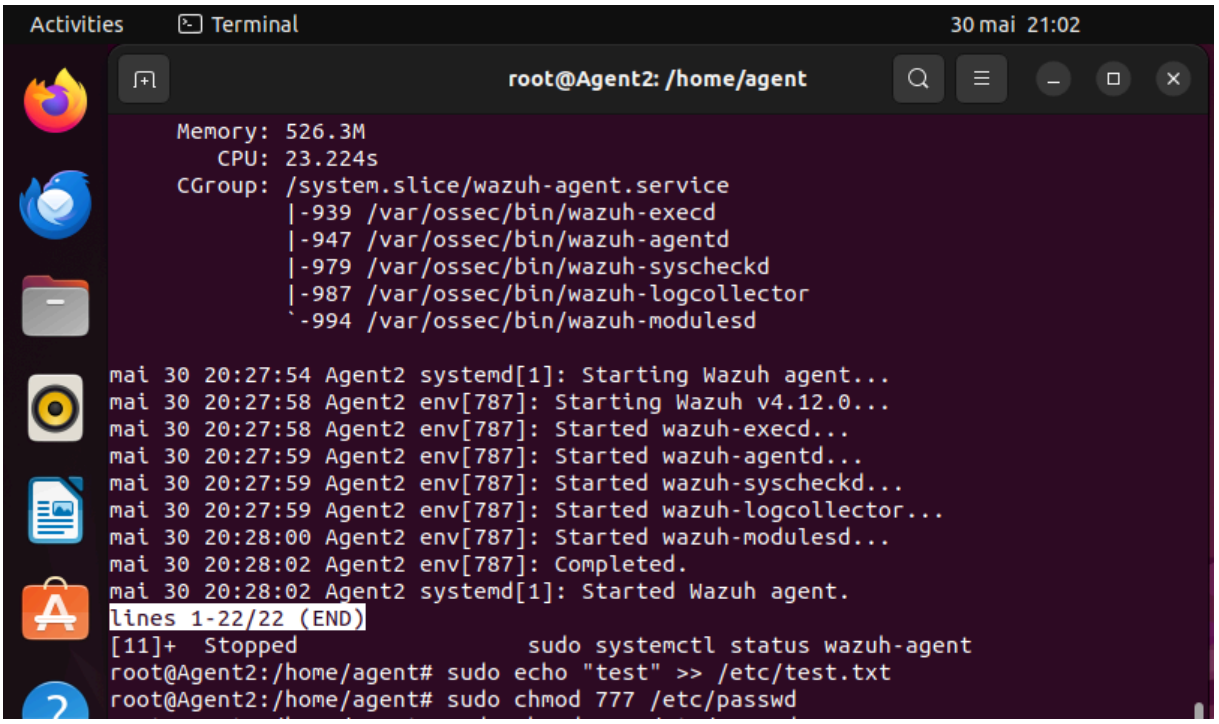
**Εικόνα 3.18 : Αποτελέσματα επίθεσης**

Επίσης, πατώντας στο πεδίο Rule, παρέχονται σημαντικές πληροφορίες για το ID του ,επίπεδο επικινδυνότητας του καθώς και τα group κανόνων που ανήκει.



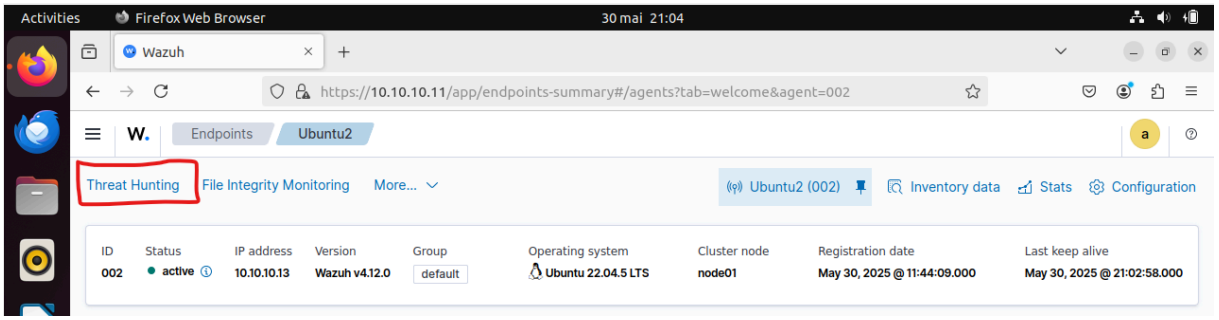

**Εικόνα 3.14 : Αποτελέσματα επίθεσης**

Για να μπορέσουμε να αναδείξουμε την κατηγοριοποίηση των κανόνων και το κατά πόσο εντατική παρακολούθηση πραγματοποιεί ο Wazuh, αρκεί να κάνουμε μια απλή αλλαγή δικαιωμάτων ενός αρχείου. Συγκεκριμένα πραγματοποιήθηκε αλλαγή των δικαιωμάτων για το αρχείο passwd του Wazuh Agent όπως φαίνεται στην παρακάτω εικόνα.



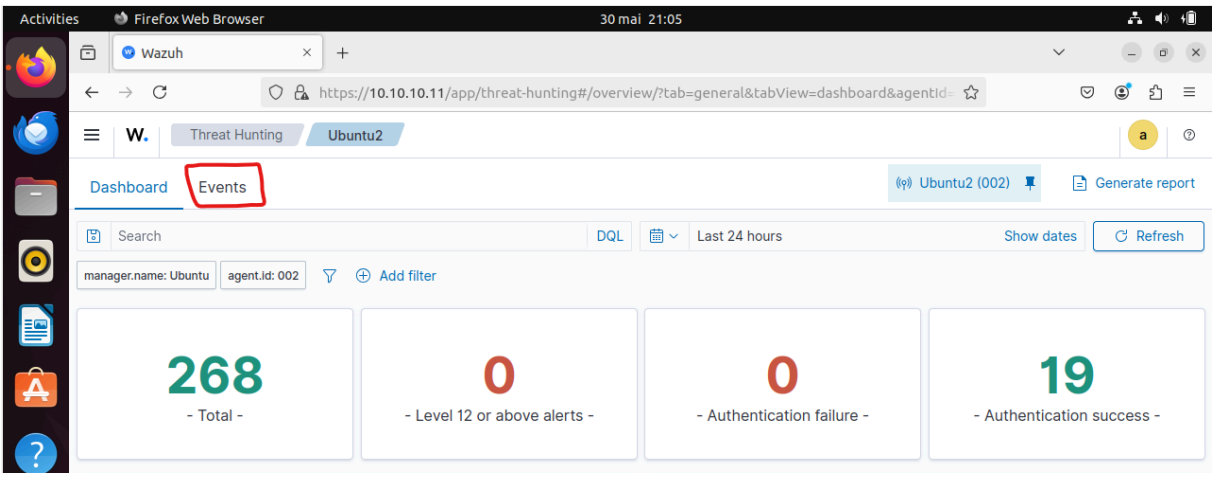

**Εικόνα 3.15 : Αλλαγή δικαιωμάτων στο αρχείο passwd**

Εν συνεχεία ανατρέχουμε στο Wazuh dashboard και κατευθυνόμαστε στο περιβάλλον διαχείρισης του Agent. Επιλέγουμε την επιλογή Threat Hunting που βρίσκεται στο πάνω δεξιά μέρος του dashboard.



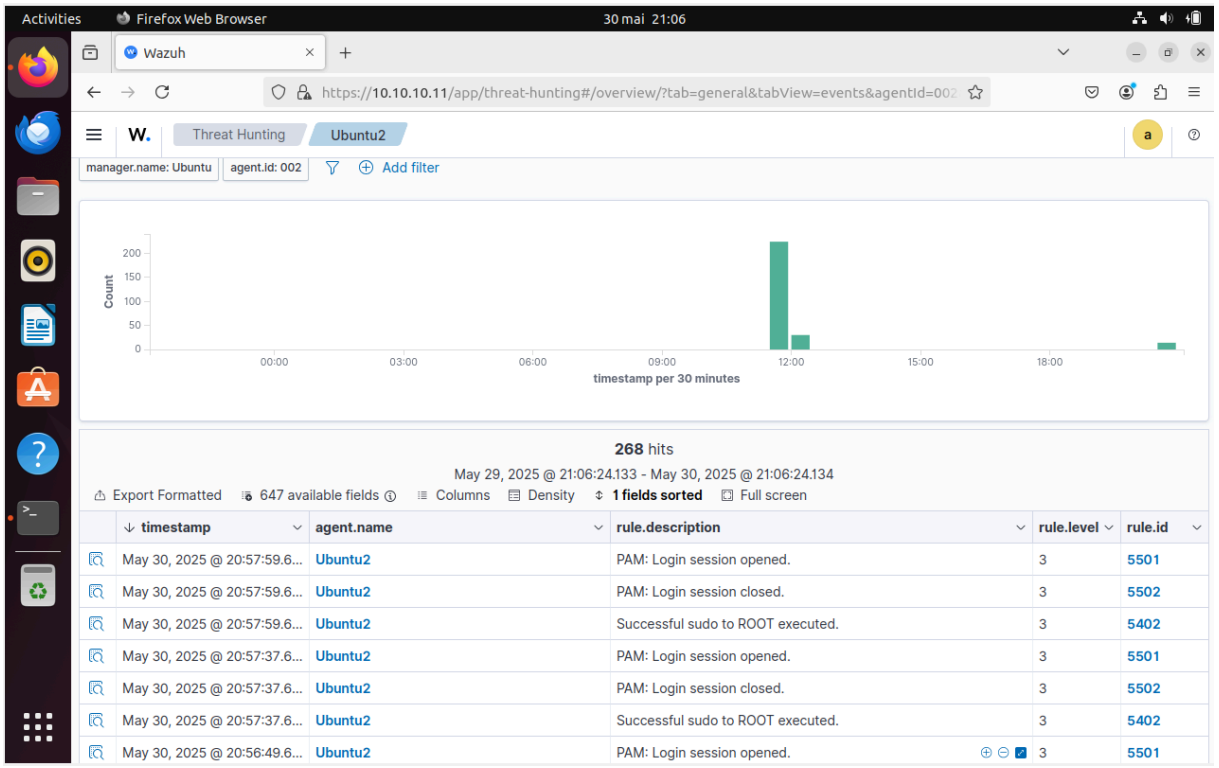

**Εικόνα 3.16 : Threat Hunting**

Μεταφερόμαστε στο περιβάλλον διαχείρισης του Theat Hunting και επιλέγουμε το Events.



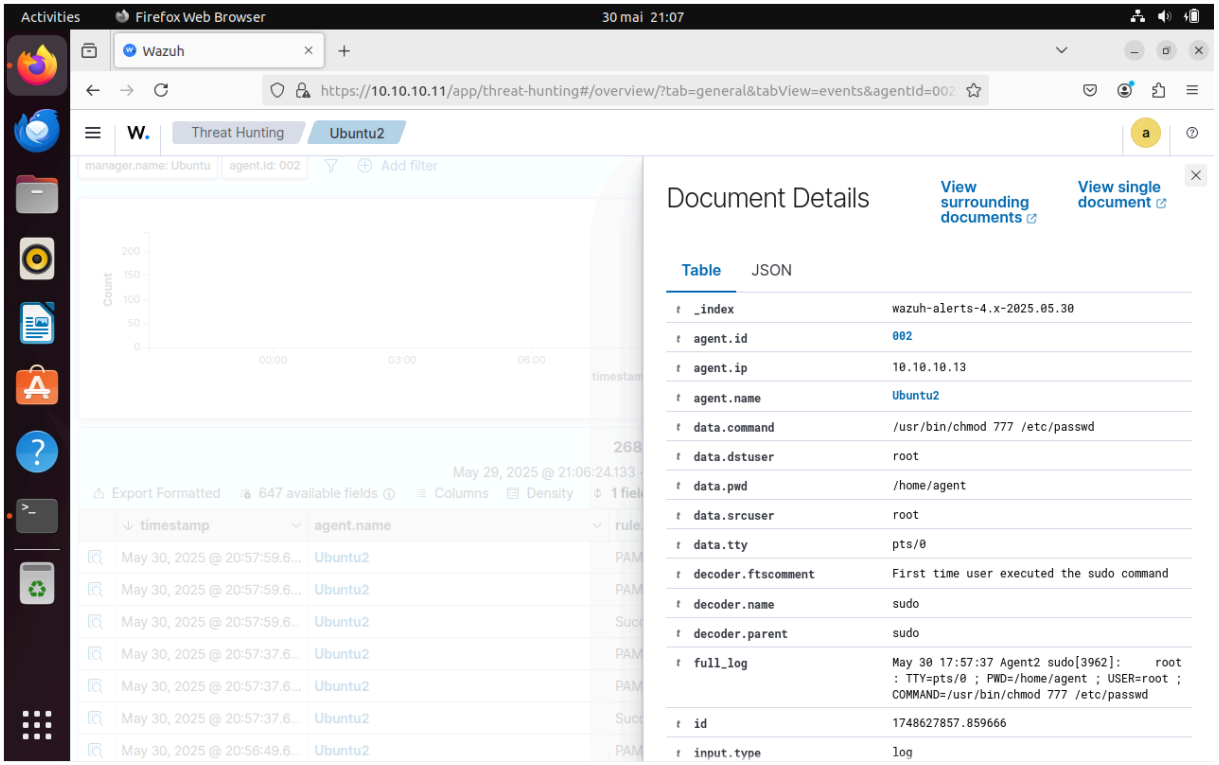
**Εικόνα 3.17 : Επιλογή Events**

Μόλις επιλέξουμε το Events, εμφανίζεται ένας κατάλογος με όλες τις κινήσεις που πραγματοποιήθηκαν και εντοπίστηκαν από τον Wazuh. Δεν αποτελούν απαραίτητα περιστατικά επίθεσης. Όπως προαναφέραμε θα εξετάσουμε ένα παράδειγμα αλλαγής δικαιωμάτων ώστε να δούμε τι μπορεί να εμφανίσει.

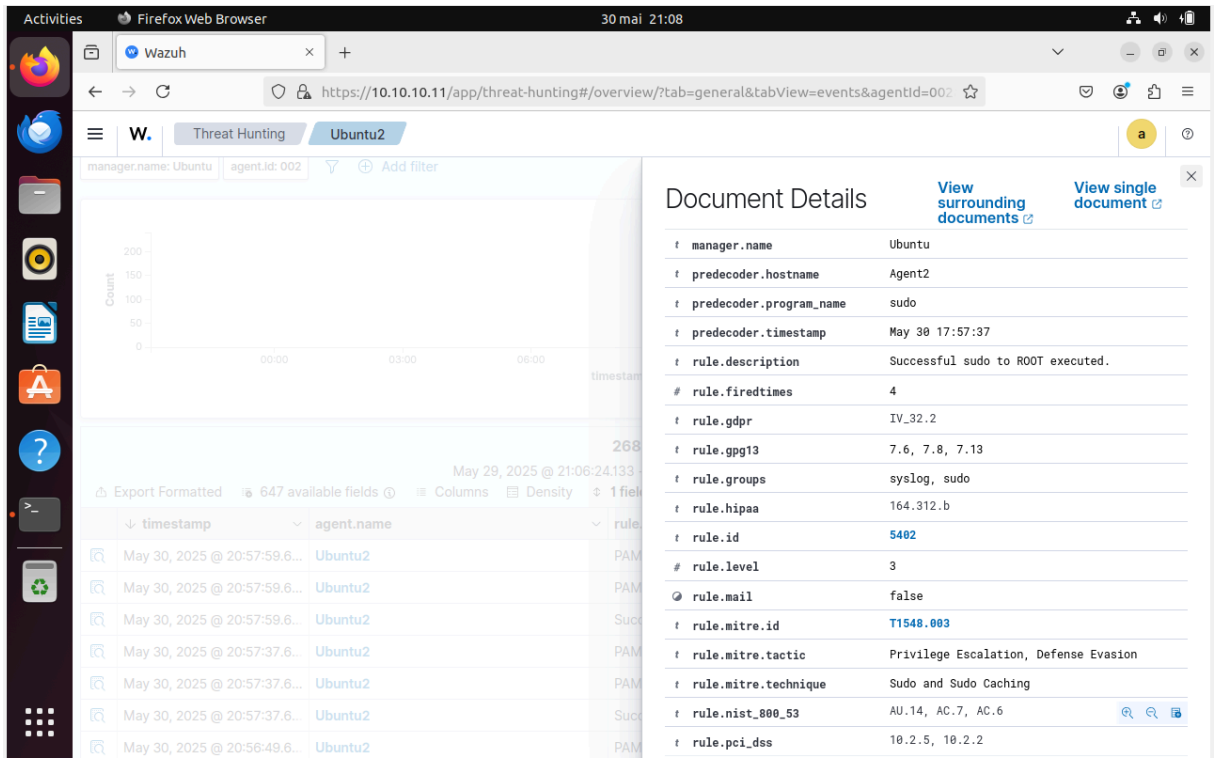



**Εικόνα 3.18 : Αποτελέσματα εντοπισμού**

Πατώντας την τρίτη επιλογή μπορούμε να διακρίνουμε ότι εντόπισε επιτυχημένη εκτέλεση sudo εντολής. Εάν πατήσουμε για περισσότερες πληροφορίες μας εμφανίζεται η παρακάτω καρτέλα.




**Εικόνα 3.19 : Αποτελέσματα εκτέλεσης εντολής sudo**




**Εικόνα 3.20 : Αποτελέσματα εκτέλεσης εντολής sudo**

Παρατηρόντας τις παραπάνω εικόνες μπορούμε να διακρίνουμε ότι παρέχει σημαντικές πληροφορίες έστω και με την εκτέλεση μιας απλής εντολής. Στο πεδίο full_log αναγράφεται πλήρως η εντολή που εκτελέσαμε.

Έστω και με την υλοποίηση ενός τόσο απλού παραδείγματος, μπορούμε να καταλάβουμε πως το Wazuh πραγματοποιεί ένα ενδελεχεί έλεγχο όλων των κινήσεων που πραγματοποιούνται, ανεξαρτήτως επιπέδου επικινδυνότητας.

### 3.4.4 Συμπεράσματα Αποτελεσμάτων

Έστω και με την εφαρμογή ενός πειράματος μπορούμε να καταλάβουμε τις δυνατότητες και τις πληροφορίες που μπορεί να μας προσφέρει το Wazuh τόσο σε επίπεδο εκμάθησης σε συστήματα εντοπισμού και αποτροπής επιθέσεων όσο και σε πρακτικά οφέλη του δικτύου. Εννοείτε πως υπάρχει μια τεράστια γκάμα εργαλείων, rules και άλλων υπηρεσιών που παρέχει το Wazuh για την επίτευξη μιας ολοκληρωμένης λύσης ασφάλειας. Η σοβαρότητα και οι πληροφορίες που παρέχουν τα rules, η δυνατότητα ενσωμάτωσης agent σχεδόν σε όλα τα σημεία ενός δικτύου αλλά και η δυνατότητα agentless monitoring μπορούν όχι μόνο να αναβαθμίσουν τους κανόνες πειθαρχίας που χρησιμοποιούνται απέναντι στις υπηρεσίες ενός οργανισμού αλλά ταυτόχρονα να έρθει σε επαφή και να αναβαθμίσει τα ήδη υπάρχοντα εργαλεία και μέτρα ασφάλειας.

# Κεφάλαιο 4ο: Συμπεράσματα και προτάσεις βελτίωσης

Εφόσον έχουμε ολοκληρώσει την θεωρητική ανάλυση των τεχνολογιών SIEM αλλά και την τελική επιλογή, ενσωμάτωση και πειραματισμό της τεχνολογίας Wazuh, ακολουθούν τα συμπεράσματα και οι παρατηρήσεις που προέκυψαν. Στο τέλος του κεφαλαίου παρατίθενται προτάσεις σχετικά με την εφαρμογή της τεχνολογίας SIEM στο δίκτυο του τμήματος ΜΠΗΣ καθώς και το κατά πόσο χρήσιμη για την ασφάλεια του δικτύου του θα ήταν η συνύπαρξη με άλλα εργαλεία ασφαλείας όπως το firewall. Οι παραπάνω προτάσεις αποτελούν λειτουργίες που θα μπορούσαν να υλοποιηθούν και να ενσωματωθούν πλήρως στο δίκτυο του τμήματος ΜΠΗΣ.

## 4.1 Συμπεράσματα

Με την παρούσα πτυχιακή εργασία πραγματοποιήθηκε μια προσπάθεια ανάδειξης των τεχνολογιών SIEM ως ένα πολύ σημαντικό και βασικό εργαλείο για την ενίσχυση της ασφάλειας πληροφοριακών συστημάτων. Μέσα από σταδιακή μελέτη και περιγραφή της τεχνολογίας SIEM, συγκριτικής ανάλυσης τεχνολογιών SIEM και τελικά η επιλογή και ο πειραματισμός με την τεχνολογία Wazuh, έστω και σε ένα περιορισμένο περιβάλλον διαχείρισης, επιβεβαίωσε την λειτουργικότητα και τα οφέλη που μπορούν να προσφέρουν οι τεχνολογίες SIEM σε περιστατικά εντοπισμού και αποτροπής επιθέσεων.

Η εγκατάσταση του Wazuh καθώς και ο πειραματισμός με την χρήση Agent, βοήθησε αρκετά στην παρατήρηση της διαδικασίας συλλογής, ανάλυσης και ερμηνείας περιστατικών ασφαλείας όπου μπορούν να εφαρμοστούν σε οποιοδήποτε σημείο ενός δικτύου. Επιπροσθέτως, η δυνατότητα παρακολούθησης σε πραγματικό χρόνο, τα rules και οι πολιτικές ασφαλείας που χρησιμοποιήθηκαν καθώς και η προσομοίωση επιθέσεων συνέβαλαν καθοριστικά στην ορθή αξιολόγηση της αποτελεσματικότητας του.

Σίγουρα η διαδικασία διαμόρφωσης, οι τεχνικές προκλήσεις, οι περιορισμοί πόρων και η έλλειψη εξειδίκευσης δεν κατέστησαν εύκολη την δημιουργία του πειραματικού περιβάλλοντος. Ωστόσο, τα οφέλη που προσέφερε το Wazuh κατά την ενσωμάτωση του υπερτερούν σημαντικά. Οι δυνατότητες αποτροπής επίθεσης, ενισχυμένης παρακολούθησης, συμμόρφωση με τους κανόνες και η κεντρική διαχείριση αποτελούν ισχυρά θετικά χαρακτηριστικά για έναν οργανισμό που αποσκοπεί στην ισχυροποίηση των συστημάτων ασφαλείας του απέναντι σε επιθέσεις.

## 4.2 Μελλοντικές Επεκτάσεις

Η υλοποίηση και η έρευνα σε πρακτικό επίπεδο εφαρμόστηκαν σε ένα οικιακό περιβάλλον με την χρήση εικονικών μηχανών. Ένας από τους στόχους που θα θέλαμε να πετύχουμε μελλοντικά, είναι η πλήρης ενσωμάτωση και λειτουργία στο δίκτυο του τμήματος ΜΠΗΣ. Το τμήμα ΜΠΗΣ αποτελείται από ένα μεγάλο αριθμό υπολογιστικών συστημάτων που αφορούν την διεξαγωγή εργαστηριακών τμημάτων. Επίσης υπάρχει ένας μεγάλος αριθμός δικτυακών συσκευών και server για την εξυπηρέτηση και την ασφαλή χρήση του διαδικτύου και των διάφορων άλλων υπηρεσιών του τμήματος. Είναι σημαντικό να αναφέρουμε πως πέρα από την συλλογή και χρήση πολλών ευαίσθητων πληροφοριών, που αφορούν διάφορα προσωπικά στοιχεία φοιτητών και καθηγητών, υπάρχει και μια μεγάλη πληθώρα υπηρεσιών που χρησιμοποιούνται τόσο για την μελέτη και την δυνατότητα εκτέλεσης πειραμάτων, όσο και για την ασφάλεια πληροφοριακών συστημάτων. Πριν από την διαδικασία πειραματισμού σε οικιακό περιβάλλον έγιναν σημαντικές ενέργειες για την συνύπαρξη τεχνολογιών SIEM με υπόλοιπα εργαλεία ασφαλείας του δικτύου όπως το firewall που

χρησιμοποιείται. Πιο συγκεκριμένα, το δίκτυο του τμήματος ΜΠΗΣ χρησιμοποιεί το firewall pfSense. Το pfSense αποτελεί μια δωρεάν και ανοιχτού κώδικά λύση firewall η οποία είναι πολύ χρήσιμη και αποδοτική. Είναι βασισμένο στο FreeBSD και διακρίνεται για τις δυνατότητες που παρέχει, την ευελιξία του καθώς και για το γραφικό περιβάλλον διαχείρισης που το καθιστά προσβάσιμο ακόμα και σε μη εξειδικευμένους χρήστες. Χρησιμοποιείται ευρέως σε δίκτυα, είτε μικρής είτε μεγάλης έκτασης, και αποτελεί αξιόπιστη λύση για την προστασία και την παρακολούθηση ενός δικτύου[34]. Η έκδοση που είναι εγκατεστημένο το pfSense στο δίκτυο του τμήματος είναι η 2.4.4, ενώ η τελευταία έκδοση που κυκλοφορεί είναι 2.8.0. Θα μπορούσε, να πραγματοποιηθεί λοιπόν μια διαδικασία ενημέρωσης του pfSense στην νεότερη έκδοση του και μέσω της ενσωμάτωσης και χρήσης των εργαλείων που προσφέρει το Wazuh, να δημιουργηθεί ένα περιβάλλον συνύπαρξης των δύο αυτών τεχνολογιών, αναβαθμίζοντας έτσι σε έναν ευρύτερο βαθμό τα επίπεδα ασφαλείας πληροφοριακών συστημάτων του δικτύου του τμήματος.

Πιο συγκεκριμένα, η φύση του Wazuh,όπως και των περισσότερων τεχνολογιών SIEM, επιτρέπει την παρακολούθηση και διασύνδεση με οποιονδήποτε κόμβο ενός δικτύου. Αυτό δεν σημαίνει απαραίτητα ότι ο κόμβος πρέπει να αποτελεί πληροφοριακό σύστημα ή δικτυακή συσκευή. Τα διάφορα εργαλεία ασφαλείας, όπως και το firewall, αποτελούν σημαντικά σημεία κατά τα οποία ο Wazuh μπορεί να παρακολουθήσει και αναλύσει δεδομένα, διότι αποτελούν άμεσοι μεσολαβητές περιστατικών ασφαλείας.Ένα από τα εργαλεία ασφαλείας το οποίο μπορεί να υποστηρίξει το Wazuh είναι το pfSense[35]. Έτσι το Wazuh θα μπορούσε να συνδεθεί με το pfSense με σκοπό την αποστολή δεδομένων καταγραφής και εν συνεχεία να πραγματοποιείται ανάλυση των δεδομένων αυτών για περιστατικά που αφορούν απόπειρες εισβολής, σάρωσης θηρών, αποτυχημένες προσπάθειες σύνδεσης και άλλες ύποπτες δραστηριότητες. Ένα τέτοιο σενάριο μπορεί να επιτευχθεί με ή χωρίς την χρήση Wazuh Agent όπου θα λειτουργεί ως ένα σύστημα συλλογής και ανάλυσης δεδομένων καταγραφής. Επίσης θα μπορούσαν να υλοποιηθούν προσαρμοσμένα rules ώστε να λαμβάνουμε με μεγαλύτερη ακρίβεια τα αποτελέσματα που μας ενδιαφέρουν.

Το Wazuh παρέχει την δυνατότητα Active Response. Στην πράξη, το Active Response είναι ένα εργαλείο που χρησιμοποιείται από τους διαχειριστές του Wazuh, για την αυτοματοποίηση ορισμένων εντολών οι οποίες εκτελούνται όταν πληρούνται συγκεκριμένα κριτήρια ασφαλείας, όπως για παράδειγμα η συνεχείς αποτυχημένες προσπάθειες σύνδεσης [36]. Το Active Response παρέχει μια μεγάλη πληθώρα προκαθορισμένων κανόνων. Μέσα σε αυτούς του κανόνες περιέχονται και κανόνες που αφορούν firewalls όπως το firewall-drop το οποίο χρησιμοποιείται για την προσθήκη μιας ip διεύθυνσης στον πίνακα iptables στην λίστα deny[37].

Για να μπορέσουμε να γίνουμε πιο συγκεκριμένοι με το πως θα μπορέσει να λειτουργήσει το Active Response μπορούμε να συμβουλευτούμε την επίσημη σελίδα του Wazuh η οποία περιέχει σημαντικές πληροφορίες σχετικά με το Active Response που χρησιμοποιεί καθώς και παραθέτει κώδικα υλοποίησης του. Για παράδειγμα, έστω ότι πραγματοποιείται μια επίθεση μορφής Brute Force μέσω SSH στο pfSense, μπορεί να υλοποιηθεί το κατάλληλο script το οποίο θα μπορεί να δημιουργήσει ένα alert για την ειδοποίηση της ομάδας διαχείρισης του δικτύου. Μέσα σε αυτό το script που θα δημιουργηθεί μπορεί να γίνει η προσθήκη του κανόνα firewall-drop ώστε η διεύθυνση που πραγματοποιεί αποτυχημένες προσπάθειες σύνδεσης, να αποκλείεται από το iptable και εν συνεχεία από το pfSense. Επίσης θα μπορούσε να δημιουργηθεί και το αντίστοιχο alert που θα προειδοποιεί την προσπάθεια Brute Forcing[38].

Μέσω των παραπάνω τεχνικών που αναλύθηκαν μπορούμε να καταλάβουμε πως η συνύπαρξη των δύο αυτών τεχνολογιών όχι μόνο μπορεί να καταστεί εφικτή, αλλά μπορεί να προσφέρει σημαντικά

πλεονεκτήματα στην αναβάθμιση των συστημάτων ασφαλείας του δικτύου όπως η μείωση του χρόνου αντίδρασης σε περιστατικά ασφαλείας, μείωση της ανάγκης ανθρώπινης παρέμβασης καθώς και την δημιουργία ενός πιο προσαρμοσμένου περιβάλλοντος ασφάλειας ανάλογα με τους πόρους και τις δυνατότητες του οργανισμού. Οι δυνατότητες του Wazuh να μπορεί να διεισδύσει σε οποιονδήποτε κόμβο ενός δικτύου με σκοπό την παρακολούθηση, συλλογή, εντοπισμό και αποτροπή επιθέσεων σε συνδυασμό με τις δυνατότητες ενός ισχυρού και αξιόπιστου τείχους προστασίας όπως το pfSense μπορούν να δημιουργήσουν ένα οικοσύστημα ασφάλειας το οποίο θα μπορεί να αποτρέπει με μεγάλη ταχύτητα διάφορους κινδύνους αλλά και με την δυνατότητα προσαρμογής τους ανάλογα με τις απαιτήσεις που θέλουμε να πετύχουμε, μπορούμε να λαμβάνουμε τις κατάλληλες ειδοποιήσεις και απαντήσεις για τους λόγους που συνέβησαν και ποιά μέτρα προστασίας έλαβαν χώρα.

Ένα σημαντικό εργαλείο που θα πρέπει να μελετήσουμε σε μεγαλύτερο βάθος, είναι τα rules και η σύνταξή τους. Σε έναν οργανισμό όπως το τμήμα ΜΠΗΣ, παρέχονται πολλές υπηρεσίες τόσο σε φοιτητές, όσο και σε καθηγητές του τμήματος. Κάποιες από αυτές τις υπηρεσίες είναι η παροχή βάσεων δεδομένων, VPN server καθώς και άλλες. Σκοπός αυτών των υπηρεσιών είναι να χρησιμοποιούνται για καθαρά ακαδημαϊκούς σκοπούς. Ωστόσο, υπάρχουν πολύ εύκολοι τρόποι ώστε κάποιος να τους χρησιμοποιήσει με καταχρηστικό τρόπο. Για παράδειγμα, η υπηρεσία VPN μπορεί να χρησιμοποιηθεί πολύ εύκολα για το κατέβασμα πειρατικού περιεχομένου. Σε μια τέτοια περίπτωση, εκτός από τις ποινές που μπορεί να επωμιστεί ο εκάστοτε χρήστης, ακόμα πιο σκληρές θα είναι οι ποινές που θα δεχθεί το τμήμα. Πέρα από τις οικονομικές ή δικαστικές επιπτώσεις που μπορεί να επιβληθούν, χάνεται αυτόματα η αξιοπιστία των συστημάτων ασφαλείας του τμήματος. Γι αυτό τον λόγο θα μπορούσαμε να επεκτείνουμε την μελέτη μας και σε επίπεδο δημιουργίας πολιτικών ασφαλείας διότι σίγουρα οι εξωτερικοί παράγοντες συνήθως αποτελούν τον μεγαλύτερο κίνδυνο, όμως και οι εσωτερικοί παράγοντες πρέπει να συμμορφόνονται ανάλογα με τους κανόνες και την πολιτική ασφαλείας που επικρατεί.

Τέλος, θα μπορούσαμε να αναφέρουμε σε ένα γενικότερο πλαίσιο πως θα ήταν ακόμα καλύτερο να γίνουν δοκιμές και με άλλες τεχνολογίες SIEM καθώς και ενσωμάτωση άλλων εργαλείων ασφαλείας. Θα πρέπει να υπάρχει μια συνεχής αναζήτηση και εξέλιξη στο θέμα της ασφάλειας πληροφοριακών συστημάτων. Όπως έχει αποδειχθεί, οι κίνδυνοι και τα περιστατικά ασφαλείας ολοένα και αυξάνονται και πολλές φορές βρίσκονται τρόποι ώστε να μην γίνονται εύκολα αντιληπτοί. Γι αυτό θα πρέπει η έρευνα για νέες λύσεις ασφάλειας και ο πειραματισμός, να μην σταματάνε.

# ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Miloslavskaya, N. (2018). Analysis of SIEM Systems and Their Usage in Security Operations and Security Intelligence Centers. In: Samsonovich, A., Klimov, V. (eds) Biologically Inspired Cognitive Architectures (BICA) for Young Scientists. BICA 2017. Advances in Intelligent Systems and Computing, vol 636

[2]Exabeam. “Five SIEM Benefits Unveiled: Strengthening Security and Streamlining Operations” [Online] Available : https://www.exabeam.com/explainers/siem/five-siem-benefits-unveiled-strengthening-security-and-streamlining-operations

[3] “Top Challenges in Implementing SIEM Solutions” https://www.logsign.com/blog/top-challenges-in-implementing-siem-solutions/

[4] Core Security “What is SIEM?” [Online] Available :

https://www.coresecurity.com/siem

[5] Debar, Hervé. (2009). An Introduction to Intrusion-Detection Systems.

[6] An Introduction to Intrusion Detection by Aurobindo Sundaram

[7] GeeksForGeeks. “Intrusion Detection System (IDS)” [Online] Available: https://www.geeksforgeeks.org/intrusion-detection-system-ids/

[8] A. Sawant, "A Comparative Study of Different Intrusion Prevention Systems," *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)*, Pune, India, 2018, pp. 1-5, doi: 10.1109/ICCUBEA.2018.8697500.

[9] OSSEC Official Site. “About OSSEC HIDS”[Online]. Available: : https://www.ossec.net/about/

[10]Intrusion Detection with OSSEC Anafcheh, Ali (2018)

[11]A BRIEF STUDY AND COMPARISON OF, OPEN SOURCE INTRUSION DETECTION SYSTEM TOOLS 1 SURYA BHAGAVAN AMBATI, 2DEEPTI VIDYARTHI

[12]”Tripwire Open Source vs OSSEC: Is This Tripwire Alternative Right for You?” https://www.upguard.com/blog/tripwire-open-source-vs-ossec-which-is-right-for-you

[13] OSSIM Open Source Security Information Management Brian E. Lavender Sac State CSC 250, Spring 2008 Final Project 2008

[14] PeerSpot. “AlienVault OSSIM pros and cons” [Online]. Available: https://www.peerspot.com/products/alienvault-ossim-pros-and-cons

[15] “Signature Based Intrusion Detection System Using SNORT” Vinod Kumar Research Scholar, School of ICT Gautam Buddha University Dr. Om Prakash Sangwan Faculty, School of ICT Gautam Buddha University

[16] PeerSpot.“Cisco Sourcefire SNORT pros and cons” [Online]. Available: https://www.peerspot.com/products/cisco-sourcefire-snort-pros-and-cons

[17] Wazuh Documentation. “Getting started with Wazuh.” [Online]. Available: https://documentation.wazuh.com/current/getting-started/index.html

[18]Wazuh Documentation. “Components.” [Online]. Available:

https://documentation.wazuh.com/current/getting-started/components/index.html
[19] Stanković, S., Gajin, S., & Petrović, R. (2022). A Review of Wazuh tool capabilities for detecting attacks based on log analysis. *No Nama Agent Integrity File Added Delete Modified*, *1*.
[20] PeerSpot."Wazuh pros and cons"[Online]. Available:
https://www.peerspot.com/products/wazuh-pros-and-cons
[21]Wazuh Documentation. "Our Customers." [Online]. Available:
https://wazuh.com/our-customers/
[22]Wazuh Documentation. "Data Analysis." [Online]. Available:
https://documentation.wazuh.com/current/user-manual/ruleset/index.html
[23]Wazuh Documentation. "Rules Classification." [Online]. Available:
https://documentation.wazuh.com/current/user-manual/ruleset/rules/rules-classification.html
[24]Wazuh Documentation. "Rules." [Online]. Available:
https://documentation.wazuh.com/current/user-manual/ruleset/rules/index.html
[25]Wazuh Documentation. "Rules Syntax." [Online]. Available:
https://documentation.wazuh.com/current/user-manual/ruleset/ruleset-xml-syntax/rules.html
[26]Wazuh Documentation. "Custom Rules." [Online]. Available:
https://documentation.wazuh.com/current/user-manual/ruleset/rules/custom.html
[27]Nwana, H.S., Ndumu, D.T. (1997). An introduction to agent technology. In: Nwana, H.S., Azarmi, N. (eds) Software Agents and Soft Computing Towards Enhancing Machine Intelligence. Lecture Notes in Computer Science, vol 1198. Springer, Berlin, Heidelberg.
https://doi.org/10.1007/3-540-62560-7_35
[28]Wazuh Documentation. "Wazuh Agent." [Online]. Available:
https://documentation.wazuh.com/current/user-manual/agent/index.html
[29]Wazuh Documentation. "Agentless monitoring." [Online]. Available:
https://documentation.wazuh.com/current/user-manual/agentless-monitoring/index.html
[30]Wazuh Documentation. "How it works." [Online]. Available:
https://documentation.wazuh.com/current/user-manual/capabilities/agentless-monitoring/how-it-works.html#how-it-works
[31]Wazuh Documentation. "Installation guide." [Online]. Available:
https://documentation.wazuh.com/current/installation-guide/index.html
[32]MITRE ATT&CK Official Site. [Online]. Available:
https://attack.mitre.org/
[33]ninjaOne "What Is ELK Stack? A Guide to Elasticsearch, Logstash, & Kibana." [Online]. Available : https://www.ninjaone.com/blog/what-is-elk-stack/
[34]pfSense, "Getting Started." [Online]. Available :
https://www.pfsense.org/getting-started/
[35]Wazuh Documentation. "Monitoring network devises with Wazuh." [Online]. Available:
https://wazuh.com/blog/monitoring-network-devices/
[36]Wazuh Documentation. "Active Response." [Online]. Available:
https://documentation.wazuh.com/current/user-manual/capabilities/active-response/index.html
[37]Wazuh Documentation. "Default active response scripts." [Online]. Available:
https://documentation.wazuh.com/current/user-manual/capabilities/active-response/default-active-response-scripts.html
[38]Wazuh Documentation. "Blocking SSH brute-force attack with Active Response." [Online]. Available:
https://documentation.wazuh.com/current/user-manual/capabilities/active-response/ar-use-cases/blocking-ssh-brute-force.html