ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ – ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Κυβερνοασφάλεια και Επιστήμη Δεδομένων»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Ανάπτυξη Συνεργατικής Πλατφόρμας για την Κεντρική Διαχείριση Κυβερνοεπιθέσεων.** **Development of a Collaborative Platform for Centralized Incident Response Management.**
Ονοματεπώνυμο Φοιτητή	Χρυσικός Νικόλαος Νεκτάριος
Πατρώνυμο	Αναστάσιος
Αριθμός Μητρώου	ΜΠΚΕΔ2250
Επιβλέπων	**Παναγιώτης Κοτζανικολάου, Καθηγητής**

Ημερομηνία Παράδοσης **Δεκέμβριος 2024**

Τριμελής Εξεταστική Επιτροπή

Παναγιώτης Κοτζανικολάου Καθηγητής	Μιχαήλ Ψαράκης Αν. Καθηγητής	Κωνσταντίνος Πατσάκης Αν. Καθηγητής

Περιεχόμενα

Πίνακας Εικόνων

Πίνακας Πινάκων

Περίληψη

Η παρούσα διατριβή εστιάζει στην ανάπτυξη μίας πλατφόρμας διαχείρισης κυβερνοεπιθέσεων η οποία έχει ως κύρια χαρακτηριστικά την συνεργασία, το συντονισμό και την ανταλλαγή πληροφοριών για την κεντρική διαχείριση περιστατικών σε εθνικό και διεθνές επίπεδο, μεταξύ αναλυτών πολλών διαφορετικών ομάδων αντιμετώπισης περιστατικών. Ο βασικός στόχος μίας τέτοιας προσέγγισης είναι , η παροχή μίας κοινής επιχειρησιακής εικόνας, που με κατάλληλα εργαλεία, θα κατευθύνει τον ειδικό προς τις ενέργειες που πρέπει να ακολουθήσει, ώστε να διαχειριστεί και να αποκαταστήσει γρήγορα, αποτελεσματικά και άμεσα κάθε περιστατικό. Μία τέτοια προσέγγιση θα δίνει τη δυνατότητα στην ομάδα αντιμετώπισης περιστατικών κυβερνοασφάλειας να αυτοματοποιεί τις ενέργειες που πρέπει να εκτελέσει, ώστε να μειωθεί στο ελάχιστο η συνέπεια ενός περιστατικού και να υπάρχει, όπου απαιτείται, άμεση ανθρώπινη παρέμβαση. Παρουσιάζονται αναλυτικά η αρχιτεκτονική της πλατφόρμας καθώς και τα εργαλεία που αποτελούν τα δομικά στοιχεία της, καθώς και ο τρόπος επικοινωνίας και ανταλλαγής δεδομένων μεταξύ των εργαλείων, οι δυνατότητες και ο ρόλος τους. Στην συνέχεια περιγράφεται αναλυτικά ο τρόπος υλοποίησης της πλατφόρμας τα σχετικά πλεονεκτήματα και μειονεκτήματα της, και τελικά παρουσιάζονται οι επόμενοι στόχοι και οι πιθανές μελλοντικές επεκτάσεις, που θα μπορούσαν να ενισχύσουν την αποτελεσματικότητα της προτεινόμενης πλατφόρμας στη διαχείριση των συχνά καταστρεπτικών, για τους οργανισμούς, κυβερνοεπιθέσεων.

Abstract

This thesis focuses on the development of a incident response platform whose main characteristics are the collaboration, the coordination and the exchange of information for incident management at national and international level, between analysts of different incident response teams. The main goal of this approach is the provision of a common operational view, which when combined with appropriate tools, will guide the experts towards the appropriate actions in order to manage and restore the incident timely, effectively and proactively. Following this it will automate the actions that the specialist must perform in order to minimize the required human intervention. The architecture of the proposed platform is presented, along with the tools that constitute its building blocks. their communication, data exchange methods, their capabilities and their specific role in the platform. Following, the platform implementation is then described in detail, along with its relative advantages and disadvantages. Finally, potential future extensions and modifications are presented, that may further enhance the effectiveness of the proposed platform against cyber-attacks that may cause devastating impact on the attacked organizations.

1. Εισαγωγή

Η όλο και αυξανόμενη ευαισθητοποίηση σχετικά με τις σοβαρές κυβερνοεπιθέσεις σε κρίσιμες υποδομές όσον αφορά τη συχνότητά τους, τη διακοπή της κανονικής λειτουργίας των υποδομών αυτών και τις οικονομικές απώλειες [1], έχει κινητοποιήσει τους οργανισμούς να επενδύσουν στην ασφάλειά [2] και να προετοιμαστούν καλύτερα για την αντιμετώπιση τέτοιων περιστατικών, καθιερώνοντας ολοκληρωμένες και αποτελεσματικές εκπαιδεύσεις και αγοράζοντας εργαλεία για τη παρακολούθηση δικτύων και την ανίχνευση κακόβουλου λογισμικού. Ορισμένοι οργανισμοί έχουν συστήσει ομάδες αντιμετώπισης περιστατικών ασφάλειας υπολογιστών (CSIRT). Τέτοιες ομάδες συνεισφέρουν στην αντιμετώπιση περιστατικών δηλαδή την επαναφορά κρίσιμων συστημάτων σε λειτουργία, καθώς και στη συνεργασία για την αποτελεσματική αντιμετώπιση απειλών στον κυβερνοχώρο. Ωστόσο, υπάρχουν κυβερνοεπιθέσεις, οι οποίες διενεργούνται από μια συντονισμένη ομάδα κακόβουλων χρηστών που επιτίθενται ταυτόχρονα σε πολλούς στόχους και οργανισμούς που βρίσκονται σε πολλές χώρες [3]. Σε αυτές τις επιθέσεις, τα κίνητρα των αντιπάλων αποσκοπούν συνήθως σε οικονομικό κέρδος ή στην πρόκληση προβλημάτων σε βασικές κρατικές υποδομές, και οι συγκεκριμένοι στόχοι κυμαίνονται από την κλοπή πνευματικής ιδιοκτησίας ή ευαίσθητων δεδομένων έως τη διακοπή των υπηρεσιών που παρέχονται από κρατικές υποδομές. Αυτές οι επιθέσεις είναι συντριπτικές για τους οργανισμούς, οι οποίοι πρέπει να προσπαθήσουν να τις κατανοήσουν και να ανταποκριθούν σε αυτές με ελάχιστη ή καθόλου βοήθεια και ελλειπή γνώση ως προς τον τρόπο διαχείρισης έως τώρα [4].

1.1 Περιγραφή του υπό μελέτη προβλήματος

Η καθιέρωση συνεργασίας και κοινής επιχειρησιακής εικόνας μεταξύ των οργανισμών αποτελεί βασική πρόκληση για την αποτελεσματική διαχείριση επιθέσεων στον κυβερνοχώρο [5]. Η δυσκολία αυτή προκύπτει από την πολύπλοκη φύση των συχνών δικτυακών εισβολών που επηρεάζουν πολλαπλά συστήματα και πλέον έχουν αποδειχτεί καταστρεπτικές για οργανισμούς, καθιστώντας πλέον σχεδόν αδύνατη την αντιμετώπιση μίας εκτεταμένης κυβερνοεπίθεσης μόνο από μία ομάδα ή από έναν οργανισμό.

Αρχικά, οι επηρεαζόμενοι οργανισμοί συχνά δεν γνωρίζουν ότι και άλλοι οργανισμοί έχουν στοχοποιηθεί από την ίδια ομάδα οπότε δεν προβαίνουν στην επικοινωνία μαζί τους για παροχή πληροφοριών και την εύρεση πιθανών τρόπων αντιμετώπισης. Επιπλέον, στις περιπτώσεις που υπάρχει συνεργασία μεταξύ οργανισμών για την αντιμετώπιση κάποιας κακόβουλης επίθεσης, αυτή λαμβάνει χώρα αφότου συμβεί η επίθεση, και διαρκεί μέχρι να αντιμετωπιστεί το πρόβλημα. Ως αποτέλεσμα οι συνεργασίες αυτές , όταν υπάρχουν, διαρκούν για μικρό χρονικό διάστημα το οποίο δεν συμβάλλει στην θεμελίωση μακροχρόνιων σχέσεων υποστήριξης και έγκαιρης πληροφόρησης σε κρίσιμα θέματα κυβερνοασφάλειας [6].

Προς αυτή την κατεύθυνση, έχει θεσπιστεί και η νέα οδηγία NIS2 (Network and Information Security) Directive [7] που αφορά ομάδες αντιμετώπισης περιστατικών ασφάλειας υπολογιστών (Computer Security Incident Response Team - CSIRT) υπό την Ευρωπαϊκή Ένωση. Αυτή αποτελεί συνέχεια της οδηγίας NIS που είχε θεσπιστεί το 2016, και στοχεύει ακριβώς στο να ενισχύσει και να βελτιώσει τις πρακτικές κυβερνοασφάλειας σε κρίσιμες υποδομές σε όλη την Ευρωπαϊκή Ένωση, αναδεικνύοντας κενά και αδυναμίες που αποτελούν στόχους για κακόβουλες ομάδες. Θεσμοθετήθηκε το 2022 και άρχισε να εφαρμόζεται το 2024 και για να επιτύχει ένα υψηλό επίπεδο ετοιμότητας και αποτελεσματικής αντιμετώπισης κυβερνοαπειλών σε κάθε κράτος της Ε.Ε εξασφαλίζει :

- Την ετοιμότητα των κρατών μελών, απαιτώντας από αυτά να είναι κατάλληλα εξοπλισμένα. Για παράδειγμα, με μια ομάδα αντιμετώπισης περιστατικών ασφάλειας υπολογιστών (CSIRT) και μια αρμόδια εθνική αρχή δικτύων και συστημάτων πληροφοριών,
- Τη συνεργασία μεταξύ όλων των κρατών μελών, με τη σύσταση ομάδας συνεργασίας, δηλαδή μίας ομάδας που ρόλος της είναι να επισπεύσει την υλοποίηση ενός υψηλού κοινού επιπέδου ασφάλειας για τα συστήματα δικτύων και πληροφοριών στην

Ευρωπαϊκή Ένωση και να υποστηρίζει και διευκολύνει τη στρατηγική συνεργασία και την ανταλλαγή πληροφοριών μεταξύ των κρατών μελών της ΕΕ.

- Μια κουλτούρα ασφάλειας σε όλους τους τομείς που είναι ζωτικής σημασίας για την οικονομία και την κοινωνία μας και που βασίζονται σε μεγάλο βαθμό στις Τεχνολογίες Πληροφοριών και Επικοινωνιών, όπως η ενέργεια, οι υποδομές των χρηματοπιστωτικών αγορών, η υγειονομική περίθαλψη και οι ψηφιακές υποδομές.

Αυτές οι πτυχές παρουσιάζουν μια σειρά προκλήσεων που πρέπει να αντιμετωπιστούν κατά την ανάπτυξη μίας αποτελεσματικής πλατφόρμας συνεργασίας. Πρώτον, η πλατφόρμα θα πρέπει να διευκολύνει τον συντονισμό των διαδικασιών απόκρισης και διερεύνησης μεταξύ των φορέων και ομάδων αντιμετώπισης περιστατικών από κάθε συμμετέχοντα οργανισμό. Δεύτερον, πρέπει να επιτρέπει την αποτελεσματική ανταλλαγή πληροφοριών και πόρων μεταξύ των οργανισμών. Τέλος, δεδομένης της ευαίσθητης φύσης των δεδομένων που ανταλλάσσονται, το πλαίσιο πρέπει να εξασφαλίζει αποτελεσματική διαχείριση δεδομένων και έλεγχο πρόσβασης για την προστασία των πληροφοριών που ανταλλάσσονται.

1.2 Στόχοι της Διατριβής

Ο κύριος σκοπός της παρούσας μεταπτυχιακής διατριβής είναι να υλοποιηθεί μια ολοκληρωμένη λύση συνεργατικής και αποτελεσματικής διαχείρισης κυβερνοεπιθέσεων, ώστε οι ομάδες των αναλυτών να μπορούν να συνεργάζονται αποτελεσματικά μέσα σε ένα κεντρικοποιημένο περιβάλλον, αξιοποιώντας την αυτοματοποίηση, τις πληροφορίες που λαμβάνουν σχετικά με κακόβουλες ενέργειες και απειλές και τις εγκληματολογικές δυνατότητες (forensic capabilities) για να ανταποκρίνονται με ταχύτητα ακρίβεια σε περιστατικά ασφαλείας. Πιο συγκεκριμένα :

1. **Συνεργασία μεταξύ αναλυτών για μετριασμό απειλών και χειρισμό περιστατικών**. Η πλατφόρμα θα πρέπει να διευκολύνει την απρόσκοπτη συνεργασία μεταξύ των αναλυτών κυβερνοασφάλειας, δίνοντάς τους τη δυνατότητα να μοιράζονται πληροφορίες, να συντονίζουν τις προσπάθειές τους και να εργάζονται συλλογικά για τον μετριασμό των απειλών και την επίλυση περιστατικών. Επιτρέποντας την επικοινωνία και την ανταλλαγή δεδομένων σε πραγματικό χρόνο, η πλατφόρμα θα προωθεί την ενιαία αντιμετώπιση μεταξύ γεωγραφικά διασκορπισμένων ομάδων, μειώνοντας τον χρόνο που απαιτείται για την αντιμετώπιση περιστατικών ασφαλείας. Αυτό το συνεργατικό περιβάλλον θα δώσει τη δυνατότητα στους αναλυτές να συγκεντρώνουν τεχνογνωσία, να μοιράζονται πληροφορίες σχετικά με απειλές και να αξιοποιούν ο ένας τη γνώση του άλλου, οδηγώντας σε αποτελεσματικότερο περιορισμό των απειλών και ελαχιστοποίηση των επιπτώσεων των περιστατικών στον κυβερνοχώρο σε όλους τους επηρεαζόμενους οργανισμούς.
2. **Αποτελεσματική και αποδοτική αντιμετώπιση περιστατικών.** Να είναι σχεδιασμένη με στόχο την κανονικοποίηση και διευκόλυνση των διαδικασιών απόκρισης σε περιστατικά, ώστε να επιτρέπει στους αναλυτές να εντοπίζουν, να διερευνούν και να ανταποκρίνονται γρήγορα σε περιστατικά, βελτιώνοντας τελικά τους χρόνους απόκρισης και ελαχιστοποιώντας τις ζημιές. Να συγκεντρώνει δεδομένα και ειδοποιήσεις από διάφορα εργαλεία ασφάλειας παρέχοντας μια συνεκτική επισκόπηση όλων των ενεργών περιστατικών. Αυτή η συγκεντρωτική προσέγγιση θα επιτρέψει στις ομάδες να ιεραρχούν τα περιστατικά με βάση τη σοβαρότητα, να αυτοματοποιούν επαναλαμβανόμενες εργασίες και να εστιάζουν σε απειλές υψηλής προτεραιότητας, διασφαλίζοντας ότι οι πόροι ασφαλείας χρησιμοποιούνται αποτελεσματικά και αποδοτικά.
3. **Αυτοματοποίηση των ροών εργασίας για ταχύτερο και ακριβέστερο χειρισμό.** Η πλατφόρμα θα πρέπει να προσφέρει δυνατότητες αυτοματοποίησης που επιταχύνουν τις ροές εργασίας, επιτρέποντας στους αναλυτές να ανταποκρίνονται στις απειλές γρήγορα και με ακρίβεια. Με την αυτοματοποίηση εργασιών ρουτίνας, όπως η ταξινόμηση ειδοποιήσεων, η συσχέτιση δεδομένων και οι ενέργειες αποκατάστασης σε καθημερινά συμβάντα, η πλατφόρμα μειώνει το ανθρώπινο λάθος και εξοικονομεί πολύτιμο χρόνο. Οι αναλυτές μπορούν να ρυθμίζουν τις ροές εργασίας ώστε να ενεργοποιούν αυτοματοποιημένες απαντήσεις όταν πληρούνται ορισμένες συνθήκες, επιτρέποντας τον γρήγορο περιορισμό των απειλών και αφήνοντας τους αναλυτές ελεύθερους να επικεντρωθούν σε πιο σύνθετες εργασίες.

4. **Ανταλλαγή πληροφοριών για κακόβουλο λογισμικό με χρήση πρωτοκόλλων STIX/TAXII.** Για να καταστεί δυνατή η αποτελεσματικότερη ανταλλαγή πληροφοριών σχετικά με απειλές, η πλατφόρμα πρέπει να υποστηρίζει την ανταλλαγή πληροφοριών που σχετίζονται με κακόβουλο λογισμικό χρησιμοποιώντας πρωτόκολλα STIX/TAXII (Structured Threat Information Expression / trusted automatic intelligent information exchange) [8]. Αυτά τα πρωτόκολλα επιτρέπουν την τυποποιημένη και ασφαλή ανταλλαγή Indicators of Compromise (IOC) και δεδομένων που σχετίζονται με απειλές μεταξύ οργανισμών. Με τη διευκόλυνση της ασφαλούς και αποτελεσματικής ανταλλαγής πληροφοριών σχετικά με απειλές, η πλατφόρμα θα διασφαλίζει ότι οι οργανισμοί μπορούν να παραμένουν ενημερωμένοι σχετικά με τις τελευταίες απειλές και τεχνικές αντιμετώπισης, οδηγώντας σε μια προληπτική προσέγγιση στην άμυνα κατά του κακόβουλου λογισμικού και άλλων εξελισσόμενων απειλών.

5. **Ψηφιακή εγκληματολογία και συλλογή δεδομένων για παραβιασμένους πελάτες.** Η πλατφόρμα πρέπει να διευκολύνει την εκτέλεση ψηφιακής εγκληματολογίας (digital forensics), επιτρέποντας στους αναλυτές να διεξάγουν ολοκληρωμένες έρευνες σε παραβιασμένα συστήματα. Αυτή η δυνατότητα θα επιτρέπει στους αναλυτές να εντοπίζουν τη βασική αιτία ενός συμβάντος, να κατανοούν την πλήρη έκταση μιας παραβίασης και να πραγματοποιούν έρευνες μετά το συμβάν με συγκεκριμένα δεδομένα, τα οποία συμβάλλουν προφανώς σε μια ενδελεχή και αποτελεσματική διαδικασία αντιμετώπισης συμβάντων.

6. **Κλιμακούμενη (scalable) ανάλυση για ταχεία αξιολόγηση δεδομένων και δράση.** Για περιστατικά μεγάλης κλίμακας, η πλατφόρμα πρέπει να υποστηρίζει κλιμακούμενη ανάλυση, επιτρέποντας στους αναλυτές να αξιολογούν γρήγορα τα δεδομένα και να αποκτούν πληροφορίες που μπορούν να αξιοποιηθούν. Επεξεργαζόμενη ένα ευρύ φάσμα παρατηρήσιμων στοιχείων - όπως διευθύνσεις IP, κατακερματισμούς αρχείων (hashes) και ονόματα τομέων (domain names)- σε μεγάλα σύνολα δεδομένων, η πλατφόρμα θα επιτρέπει στις ομάδες ασφαλείας να εντοπίζουν ανωμαλίες, και να συσχετίζουν αποτελεσματικά τα ευρήματα τους.

1.3 Δομή της διατριβής

Η παρούσα εργασία έχει αναπτυχθεί σε επτά κεφάλαια, τα οποία περιγράφουν τις ανάγκες και τις απαιτήσεις που οδήγησαν στην υλοποίηση της διατριβής, τους βασικούς της στόχους, τις διαθέσιμες και δημοφιλείς λύσεις στον τομέα της διαχείρισης περιστατικών κυβερνοεπιθέσεων, την δομή και την αρχιτεκτονική της λύσης που αναπτύχθηκε και τέλος παρουσιάζεται ένα Case Study Scenario στο οποίο διαφαίνονται οι δυνατότητες της πλατφόρμας. Πιο συγκεκριμένα :

Κεφάλαιο 1 - Εισαγωγή : Στο πρώτο κεφάλαιο παρουσιάζεται το θέμα της εργασίας και το πλαίσιο στο οποίο αναπτύσσεται. Αρχικά, περιγράφεται ένα βασικό ζήτημα που εντοπίζεται στην διαχείριση κυβερνοεπιθέσεων, το οποίο είναι η ελλιπής συνεργατικότητα και επικοινωνία μεταξύ ομάδων CSIRT στην αντιμετώπιση περιστατικών. Στην συνέχεια αναλύονται οι βασικοί στόχοι της διατριβής, οι οποίοι προσανατολίζονται στην υλοποίηση μίας ολοκληρωμένης λύσης διαχείρισης κυβερνοεπιθέσεων, η οποία όμως θα στηρίζεται αλλά και θα διευκολύνει την συνεργασία και την επικοινωνία των ομάδων και τέλος παρουσιάζεται μια σύντομη περιγραφή της δομής της διατριβής ανά κεφάλαιο.

Κεφάλαιο 2 - Ανασκόπηση Σχετικής Βιβλιογραφίας: Στο δεύτερο κεφάλαιο παρουσιάζονται οι κυριότερες κατηγορίες εργαλείων ασφάλειας και στην συνέχεια αναφέρονται οι σημαντικότερες εμπορικές λύσεις ασφάλειας, τα βασικά χαρακτηριστικά και δυνατότητες τους, και στο τέλος πραγματοποιείται μια συνοπτική σύγκριση μεταξύ τους με την χρήση συγκεντρωτικού πίνακα που παρουσιάζει τις δυνατότητες τους ως εργαλεία ασφάλειας.

Κεφάλαιο 3 - Προτεινόμενη Αρχιτεκτονική : Στο τρίτο κεφάλαιο περιγράφονται λεπτομερώς τα εργαλεία που χρησιμοποιούνται για την υλοποίηση της πλατφόρμας, τα κύρια χαρακτηριστικά τους, και η κατηγορία στην οποία ανήκουν. Στην συνέχεια, ακολουθεί σύγκριση της προτεινόμενης λύσης με της εμπορικές του 2^{ου} κεφαλαίου, και στο τέλος παρουσιάζεται αναλυτικά η μεθοδολογία και ο τρόπος επικοινωνίας και διασύνδεσης των εφαρμογών της πλατφόρμας

Κεφάλαιο 4 - Μέθοδος υλοποίησης της Πλατφόρμας : Στο τέταρτο κεφάλαιο, αρχικά αναγράφονται τα χαρακτηριστικά και οι προδιαγραφές του συστήματος που αναπτύχθηκε η πλατφόρμα, και στην συνέχεια ακολουθεί λεπτομερής παρουσίαση της διαδικασίας εγκατάστασης, των βασικών λειτουργιών του κάθε εργαλείου που υποβοηθά την συνοχή και την αποτελεσματικότητα της πλατφόρμας, και του τρόπου επικοινωνίας του με τα υπόλοιπα εργαλεία

Κεφάλαιο 5 - Επίδειξη λειτουργίας πλατφόρμας: Στο πέμπτο κεφάλαιο αναλύεται η διαδικασία διαχείρισης πραγματικού περιστατικού, από την λήψη ειδοποίησης, μέχρι την ανάλυση δεδομένων, την ψηφιακή εγκληματολογία και την συλλογή στοιχείων και την αντιμετώπιση του περιστατικού

Κεφάλαιο 6 - Ευρήματα εργασίας - Μελλοντικές επεκτάσεις : Στο έκτο κεφάλαιο αναφέρεται η προσφορά της προτεινόμενης λύσης, τα κύρια πλεονεκτήματα της και οι αδυναμίες της, αλλά και οι μελλοντικοί στόχοι βελτίωσης και επέκτασης που απορρέουν από τα μειονεκτήματά της.

2. Ανασκόπηση Σχετικής Βιβλιογραφίας

Αυτό το κεφάλαιο εστιάζει στην παρουσίαση των σχετικών εργαλείων που χρησιμοποιούνται διεθνώς για την διαχείριση κυβερνοεπιθέσεων και των βασικών χαρακτηριστικών και δυνατοτήτων τους. Αρχικά , αναφέρονται οι κυριότερες κατηγορίες εργαλείων ασφάλειας που μπορούν να αξιοποιηθούν σε διαδικασίες incident response :

2.1 Κατηγορίες εργαλείων ασφάλειας :

Οι βασικότερες κατηγορίες εργαλείων ασφάλειας, ανάλογα με τις δυνατότητες και τις λειτουργίες τους είναι οι ακόλουθες:

Vulnerability Scanning and Management [9] : Τα εργαλεία σάρωσης και διαχείρισης αδυναμιών ασφάλειας και ευπαθειών είναι ζωτικής σημασίας για τον εντοπισμό, την αξιολόγηση και την διαχείριση των τρωτών σημείων ενός οργανισμού. Αυτά τα εργαλεία σαρώνουν τους διακομιστές, τις βάσεις δεδομένων, τις εφαρμογές και τις συσκευές δικτύου, για να εντοπίσουν αδυναμίες που θα μπορούσαν να αξιοποιηθούν από επιτιθέμενους. Με χαρακτηριστικά όπως η βαθμολόγηση κινδύνου σε πραγματικό χρόνο, οι αυτοματοποιημένες αξιολογήσεις ευπαθειών και οι αναφορές συμμόρφωσης, τα εργαλεία αυτά διασφαλίζουν ότι τα ευάλωτα σημεία παρακολουθούνται από τον εντοπισμό έως την αποκατάσταση, συμβάλλοντας στην ελαχιστοποίηση της έκθεσης σε κινδύνους ασφαλείας.

Threat Intelligence and Detection [10]: Τα εργαλεία πληροφοριών και ανίχνευσης απειλών συλλέγουν, επεξεργάζονται και αναλύουν δεδομένα από εξωτερικές πηγές για τον εντοπισμό αναδυόμενων απειλών, όπως κακόβουλο λογισμικό, προσπάθειες phishing και προηγμένες μόνιμες απειλές (APT). Αυτά τα εργαλεία ενοποιούν πληροφορίες περί απειλών από διάφορες πηγές, επιτρέποντας στις ομάδες ασφαλείας να δίνουν προτεραιότητα και να ανταποκρίνονται γρήγορα στις σχετικές απειλές. Παρέχοντας λεπτομερείς πληροφορίες σχετικά με τις πιθανές απειλές, τα εργαλεία αυτά βοηθούν τους οργανισμούς να βρίσκονται μπροστά από τις εξελισσόμενες απειλές και να ανταποκρίνονται με προσαρμοσμένες στρατηγικές μετριασμού.

Extended Detection and Response (XDR) [11] : Οι λύσεις XDR παρέχουν μια πλήρη προσέγγιση στην ανίχνευση και αντιμετώπιση απειλών, επεκτείνοντας την προστασία πέρα από τα τελικά σημεία και συμπεριλαμβάνοντας το δίκτυο, το cloud, το email και τις πηγές δεδομένων εφαρμογών. Συγκεντρώνοντας και αναλύοντας δεδομένα από πολλαπλά εργαλεία ασφαλείας, οι πλατφόρμες XDR παρέχουν μια ενιαία εικόνα των απειλών για ολόκληρο το περιβάλλον, επιτρέποντας στις ομάδες ασφαλείας να ανιχνεύουν και να ανταποκρίνονται αποτελεσματικότερα σε σύνθετες επιθέσεις. Τα εργαλεία XDR χρησιμοποιούν τεχνητή νοημοσύνη και μηχανική μάθηση (ML) για τη συσχέτιση δεδομένων από διαφορετικές πηγές, βοηθώντας τους αναλυτές να εντοπίζουν μοτίβα κακόβουλης δραστηριότητας και να ανταποκρίνονται γρήγορα. Οι πλατφόρμες XDR έχουν σχεδιαστεί για τον διευκόλυνση και τυποποίηση των λειτουργιών ασφαλείας, ενσωματώνοντας την ανίχνευση, τη διερεύνηση και την απόκριση σε μια ενιαία λύση.

Endpoint Detection and Response (EDR) [12] : Τα εργαλεία EDR επικεντρώνονται στην παρακολούθηση, τον εντοπισμό και την αντιμετώπιση απειλών σε τελικά σημεία, όπως υπολογιστές, διακομιστές και φορητές συσκευές. Με τη συνεχή συλλογή και ανάλυση δεδομένων τελικών σημείων, οι πλατφόρμες EDR βοηθούν στον εντοπισμό ασυνήθιστης συμπεριφοράς ή ανωμαλιών που μπορεί να υποδεικνύουν πιθανή επίθεση. Αυτά τα εργαλεία παρέχουν δυνατότητες όπως τις αυτοματοποιημένες ειδοποιήσεις και την ταχεία αντιμετώπιση περιστατικών, επιτρέποντας στις ομάδες ασφαλείας να απομονώσουν τα επηρεαζόμενα τελικά σημεία, να αφαιρέσουν το κακόβουλο λογισμικό και να διερευνήσουν τη βασική αιτία των περιστατικών σε ελάχιστο χρόνο. Οι λύσεις EDR είναι απαραίτητες για την προστασία από προηγμένες απειλές, ιδίως σε αποκεντρωμένα ή απομακρυσμένα περιβάλλοντα εργασίας, όπου τα τελικά σημεία είναι ευάλωτα.

Network Detection and Response (NDR) [13] : Οι λύσεις Network Detection and Response παρακολουθούν την κυκλοφορία του δικτύου σε πραγματικό χρόνο χρησιμοποιώντας αλγορίθμους τεχνητής νοημοσύνης και ML για τον εντοπισμό ύποπτης δραστηριότητας και την

ανίχνευση πιθανών απειλών για την ασφάλεια. Αυτά τα εργαλεία αναλύουν δεδομένα πακέτων και μοτίβα κίνησης, αναζητώντας ανωμαλίες, ασυνήθιστες ροές δεδομένων και ενδείξεις επιθέσεων, όπως η διαρροή δεδομένων. Τα εργαλεία NDR είναι ιδιαίτερα αποτελεσματικά στον εντοπισμό απειλών που μπορεί να παρακάμπτουν τους παραδοσιακούς ελέγχους ασφαλείας, όπως οι επιθέσεις κρυπτογραφημένης κυκλοφορίας.

Managed Detection and Response (MDR) [11] : Οι υπηρεσίες διαχείρισης ανίχνευσης και απόκρισης προσφέρουν δυνατότητες εξωτερικής παρακολούθησης, ανίχνευσης και απόκρισης σε περιστατικά κυβερνοασφάλειας, τις οποίες συνήθως διαχειρίζονται τρίτοι πάροχοι ασφάλειας. Οι υπηρεσίες MDR είναι επωφελείς για οργανισμούς που μπορεί να μην διαθέτουν τους πόρους ή την εσωτερική τεχνογνωσία για τη λειτουργία ενός κέντρου επιχειρήσεων ασφαλείας (SOC) 24 ώρες το 24ωρο. Οι πάροχοι MDR χρησιμοποιούν συνήθως έναν συνδυασμό τεχνολογιών EDR, NDR και SIEM, μαζί με εξειδικευμένους αναλυτές που παρακολουθούν για απειλές και χειρίζονται την αντιμετώπιση περιστατικών για τον πελάτη. Οι υπηρεσίες MDR παρέχουν στους οργανισμούς ενισχυμένη κάλυψη ασφαλείας, εξειδικευμένη πληροφόρηση για απειλές και ταχεία απόκριση σε πιθανά περιστατικά, καθιστώντας τις ιδανικές για επιχειρήσεις όλων των μεγεθών.

Cloud Security [14] : Η ασφάλεια του νέφους περιλαμβάνει μια σειρά εργαλείων και υπηρεσιών που έχουν σχεδιαστεί για την προστασία των δεδομένων, των εφαρμογών και των υποδομών που βασίζονται στο νέφος, από απειλές στον κυβερνοχώρο. Η κατηγορία αυτή περιλαμβάνει εργαλεία Cloud Access Security Broker (CASB), τα οποία παρέχουν πρόσβαση και έλεγχο των δεδομένων σε εφαρμογές cloud και τη διαχείριση ταυτότητας. Τα εργαλεία ασφάλειας cloud αντιμετωπίζουν προκλήσεις, όπως η προστασία των δεδομένων, η κανονιστική συμμόρφωση και ο έλεγχος πρόσβασης σε δεδομένα σε περιβάλλοντα πολλαπλών cloud και υβριδικά περιβάλλοντα. Καθώς οι οργανισμοί συνεχίζουν να υιοθετούν τεχνολογίες cloud, αυτές οι λύσεις είναι ζωτικής σημασίας για την εξασφάλιση εφαρμογών και υποδομών cloud-native.

Intrusion Detection and Prevention (IDPS) [15] : Τα συστήματα ανίχνευσης και πρόληψης εισβολών (IDPS) παρακολουθούν τη δραστηριότητα του δικτύου και του συστήματος για ενδείξεις μη εξουσιοδοτημένης πρόσβασης ή κακόβουλης συμπεριφοράς. Μια λύση IDPS επιθεωρεί την κυκλοφορία δικτύου σε πραγματικό χρόνο, χρησιμοποιώντας έναν συνδυασμό υπογραφών, ανίχνευσης ανωμαλιών και ευρετικών μεθόδων για τον εντοπισμό γνωστών απειλών και ασυνήθιστων μοτίβων. Όταν εντοπίζεται μια πιθανή απειλή, το σύστημα μπορεί να ειδοποιεί τις ομάδες ασφαλείας, να καταγράφει το συμβάν ή ακόμη και να μπλοκάρει την κακόβουλη κυκλοφορία. Τα εργαλεία IDPS είναι πολύτιμα για την προστασία από επιθέσεις που βασίζονται στο δίκτυο, παρέχοντας ένα κρίσιμο επίπεδο άμυνας που συμβάλλει στην αποτροπή μη εξουσιοδοτημένης πρόσβασης και παραβίασης δεδομένων.

Digital Forensics [16] : Τα εργαλεία ψηφιακής εγκληματολογίας χρησιμοποιούνται για τη συλλογή, τη διατήρηση και την ανάλυση ηλεκτρονικών αποδεικτικών στοιχείων μετά από ένα περιστατικό ασφαλείας. Τα εργαλεία αυτά υποστηρίζουν τις έρευνες με την ανάκτηση και την εξέταση δεδομένων από διάφορες ψηφιακές συσκευές, συμπεριλαμβανομένων υπολογιστών, κινητών τηλεφώνων και συστημάτων δικτύου. Οι λύσεις ψηφιακής εγκληματολογίας μπορούν να βοηθήσουν στην αποκάλυψη της πηγής και του πεδίου εφαρμογής μιας επίθεσης, στον εντοπισμό των δεδομένων που έχουν τεθεί σε κίνδυνο και στη συλλογή νομικά υπερασπίσιμων αποδεικτικών στοιχείων για πιθανή δίωξη. Παρέχοντας τη δυνατότητα ολοκληρωμένης ανάλυσης των αρχείων καταγραφής συστήματος, των δεδομένων αρχείων και της δραστηριότητας του χρήστη, τα εργαλεία ψηφιακής εγκληματολογίας διαδραματίζουν ζωτικό ρόλο στην αντιμετώπιση και διερεύνηση περιστατικών μετά από συμβάντα.

Governance, Risk, and Compliance (GRC) [17] : Τα εργαλεία Διακυβέρνησης, Κινδύνου και Συμμόρφωσης βοηθούν τους οργανισμούς να διαχειρίζονται τη συμμόρφωση με τις κανονιστικές διατάξεις και να ευθυγραμμίζουν τις πρακτικές ασφαλείας με τα πρότυπα και τις πολιτικές του κλάδου. Οι λύσεις GRC διευκολύνουν την αξιολόγηση κινδύνων, τη διαχείριση πολιτικών και την υποβολή εκθέσεων συμμόρφωσης, οι οποίες είναι απαραίτητες για τους οργανισμούς σε κλάδους με υψηλές κανονιστικές ρυθμίσεις, όπως η υγειονομική περίθαλψη, η χρηματοδότηση και η διακυβέρνηση. Τα εργαλεία αυτά επιτρέπουν στους οργανισμούς να εντοπίζουν και να αξιολογούν πιθανούς κινδύνους, να αναπτύσσουν στρατηγικές αντιμετώπισης

και να διασφαλίζουν ότι πληρούν τις νομικές και κανονιστικές απαιτήσεις. Το λογισμικό GRC υποστηρίζει επίσης τη συνεχή παρακολούθηση της συμμόρφωσης, βοηθώντας τους οργανισμούς να προσαρμόζονται στους νέους κανονισμούς και να αποφεύγουν πρόστιμα.

Security Information and Event Management (SIEM) [18] : Οι λύσεις SIEM συλλέγουν και συγκεντρώνουν δεδομένα καταγραφής από διάφορες πηγές δικτύου, όπως διακομιστές, εφαρμογές, τείχη προστασίας και τελικά σημεία, παρέχοντας μια συγκεντρωτική εικόνα των συμβάντων ασφαλείας σε ολόκληρο τον οργανισμό. Με την ενοποίηση των δεδομένων καταγραφής σε μια ενιαία πλατφόρμα, τα εργαλεία SIEM βοηθούν τις ομάδες ασφαλείας να εντοπίζουν, να αναλύουν και να ανταποκρίνονται αποτελεσματικότερα σε περιστατικά ασφαλείας. Τα προηγμένα συστήματα SIEM χρησιμοποιούν μηχανική μάθηση και ανάλυση δεδομένων για τον εντοπισμό μοτίβων κακόβουλης δραστηριότητας και τη δημιουργία ειδοποιήσεων, επιτρέποντας την ταχύτερη ανίχνευση και αντιμετώπιση απειλών. Τα εργαλεία SIEM αποτελούν βασικό στοιχείο των σύγχρονων λειτουργιών ασφαλείας, παρέχοντας ορατότητα και βοηθώντας τους οργανισμούς να εντοπίζουν και να μετριάζουν τις απειλές.

Security Orchestration, Automation, and Response (SOAR) [19] : Οι πλατφόρμες SOAR εκσυγχρονίζουν και αυτοματοποιούν τις ροές εργασίας αντιμετώπισης περιστατικών, επιτρέποντας στις ομάδες ασφαλείας να ανταποκρίνονται στις απειλές πιο αποτελεσματικά και με μικρότερη ανθρώπινη επέμβαση . Αυτά τα εργαλεία ενσωματώνονται με SIEM, συστήματα πληροφοριών απειλών και άλλα συστήματα κυβερνοασφάλειας για τη συλλογή ειδοποιήσεων και την εκτέλεση αυτοματοποιημένων ενεργειών, όπως ο αποκλεισμός διευθύνσεων IP ή η απομόνωση μολυσμένων τελικών σημείων . Οι πλατφόρμες SOAR επιτρέπουν επίσης στις ομάδες ασφαλείας να να δημιουργούν αυτοματοποιημένες ροές εργασίας και να συντονίζουν τις ενέργειες αντιμετώπισης περιστατικών μεταξύ των ομάδων. Με την αυτοματοποίηση εργασιών ρουτίνας και τη μείωση των χρόνων απόκρισης, τα εργαλεία SOAR βοηθούν τους οργανισμούς να βελτιώσουν τη διαχείριση περιστατικών και την επιχειρησιακή αποδοτικότητα.

Αυτές οι κατηγορίες περιλαμβάνουν μια σειρά εργαλείων που παρέχουν ολοκληρωμένη κάλυψη για το σημερινό τοπίο της κυβερνοασφάλειας, αντιμετωπίζοντας απειλές από τον εντοπισμό ευπαθειών έως τη διαχείριση της συμμόρφωσης και την αντιμετώπιση περιστατικών.

2.2 Κυριότερες εμπορικές λύσεις διαχείρισης περιστατικών ασφάλειας :

Στην ακόλουθη ενότητα θα παρουσιάσουμε τις κυριότερες λύσεις που χρησιμοποιούνται διεθνώς για την διαχείριση και την αποκατάσταση περιστατικών ασφαλείας, ώστε να εντοπίσουμε τα βασικότερα χαρακτηριστικά τους :

IBM Security QRadar Threat detection and response solutions [20] : Το IBM Security QRadar Threat detection and response solutions είναι μια αποτελεσματική και πλήρης λύση εντοπισμού διαχείρισης και αντιμετώπισης κινδύνων. Προσφέρει αυτοματοποιημένη απόκριση σε συμβάντα, λεπτομερή διαχείριση περιπτώσεων και συνεχή παρακολούθηση του δικτύου και των υποδομών του οργανισμού επιτρέποντας στις ομάδες ασφαλείας να διαχειρίζονται αποτελεσματικά τις ειδοποιήσεις. Με το QRadar Threat detection and response solutions, οι ομάδες αποκτούν βαθύτερες γνώσεις και πλήρη εικόνα για την κατάσταση ασφαλείας του οργανισμού, επιτρέποντας μια πιο στρατηγική και άμεση ανταπόκριση σε σύνθετες απειλές στον κυβερνοχώρο. Τα κυριότερα χαρακτηριστικά του IBM Security QRadar Threat detection and response solutions είναι τα ακόλουθα :

- Δημιουργία ροών εργασίας για την γρήγορη επεξεργασία και των εμπλουτισμό των δεδομένων απειλών χωρίς την χρήση κώδικα για ταχύτερη απόκριση και λήψη αποφάσεων.
- Πλήρης δυνατότητες διαχείρισης περιστατικών και άμεσης απόκρισης.
- Δυναμικά και τροποποιήσιμα playbooks τα οποία μπορούν να προσαρμοστούν ανάλογα με το περιστατικό , καθώς τα δεδομένα του μεταβάλλονται
- Παρακολούθηση μετρήσεων και KPIs για περιστατικά και χρήστες - περιλαμβάνουν το μέσο χρόνο ανίχνευσης (MTTD) και το μέσο χρόνο ανταπόκρισης (MTTR).

- Υποστηρίζει έλεγχο συμμόρφωσης με κανονισμούς, παρακολουθώντας πάνω από 170 παγκόσμιους κανονισμούς, συμπεριλαμβανομένων των GDPR, PIPEDA, HIPAA, CCPA, μεταξύ άλλων.
- Η επιχειρησιακού επιπέδου Τεχνητή Νοημοσύνη της IBM εφαρμόζει πολλαπλά επίπεδα βαθμολόγησης κινδύνου σε κάθε IOC εντός μιας υπόθεσης (case). Οι αναλυτές ασφαλείας λαμβάνουν ειδοποίηση μόνο για τις πιο σημαντικές περιπτώσεις, ώστε να γνωρίζουν ακριβώς πού πρέπει να εστιάσουν το χρόνο και την ενέργειά τους.
- Το IBM QRadar® Network Detection and Response (NDR) βοηθά τις ομάδες ασφαλείας αναλύοντας τη δραστηριότητα του δικτύου σε πραγματικό χρόνο.

NetWitness Threat Detection, Investigation and Response [21] : Το NetWitness Threat Detection, Investigation, and Response είναι μια προηγμένη πλατφόρμα κυβερνοασφάλειας που έχει σχεδιαστεί για να παρέχει ολοκληρωμένη προστασία σε ολόκληρο το περιβάλλον IT ενός οργανισμού, συμπεριλαμβανομένων των δικτύων, των τελικών σημείων και του cloud. Συνδυάζει την υψηλής ταχύτητας επεξεργασία δεδομένων με την ανάλυση συμπεριφοράς για τον γρήγορο εντοπισμό και τη διερεύνηση εξελιγμένων απειλών. Το NetWitness αξιοποιεί τη μηχανική εκμάθηση και τα δεδομένα προηγούμενων απειλών για την ανάδειξη ύποπτων μοτίβων, βοηθώντας τις ομάδες ασφαλείας να εντοπίσουν τις ανωμαλίες, να αξιολογήσουν το εύρος των περιστατικών και να αντιδράσουν αποτελεσματικά. Οι σημαντικότερες λειτουργίες του είναι οι εξής:

- Network Detection and Response : Το NetWitness Network παρέχει ορατότητα σε πραγματικό χρόνο σε όλη την κυκλοφορία του δικτύου με πλήρη καταγραφή πακέτων, επιτρέποντάς τον εντοπισμό αναδυόμενων, στοχευμένων και άγνωστων απειλών καθώς διαδίδονται στο δίκτυο, και την παρακολούθηση των κινήσεων των επιτιθέμενων.
- Endpoint Detection and Response : Το NetWitness Endpoint παρέχει ξεκάθαρη εικόνα πέραν των βασικών λύσεων ασφάλειας τελικών σημείων, παρακολουθώντας και συλλέγοντας τη δραστηριότητα σε όλα τα τελικά σημεία - εντός και εκτός του δικτύου - ώστε να μειωθεί το κόστος και ο χρόνος της αντιμετώπισης περιστατικών.
- Security orchestration and automation (SOAR) : Το NetWitness Orchestrator είναι μια ολοκληρωμένη λύση ενορχήστρωσης και αυτοματοποίησης ασφάλειας που έχει σχεδιαστεί για να βελτιώσει την αποδοτικότητα και την αποτελεσματικότητα του κέντρου επιχειρήσεων ασφάλειας, με βελτιωμένη, αυτοματοποιημένη διαχείριση περιστατικών και αυτόματη τεκμηρίωση όλων των ενεργειών κατά τη διάρκεια της διερεύνησης.
- User and entity behavior analytics (UEBA) : Το NetWitness UEBA είναι μια προσφορά SaaS που ανιχνεύει γρήγορα άγνωστες απειλές εφαρμόζοντας προηγμένη ανάλυση συμπεριφοράς και μηχανική μάθηση σε δεδομένα που καταγράφονται από το NetWitness.

Palo Alto Intrusion Detection and Prevention [22] : Η πλατφόρμα αυτή παρέχει υπηρεσίες ανίχνευσης και πρόληψης εισβολών (IDP) μέσω των Next-Generation Firewall (NGFW) και Threat Prevention. Η λύση τους αποτελεί μέρος της λειτουργικής πλατφόρμας ασφαλείας της Palo Alto Networks, η οποία ενσωματώνει τείχος προστασίας, IDP και άλλες λειτουργίες ασφαλείας για την προστασία από γνωστές και άγνωστες απειλές. Βασικά πλεονεκτήματα της λύσης αυτής είναι:

- Ανίχνευση απειλών βάσει εφαρμογών : Σε αντίθεση με τα παραδοσιακά τείχη προστασίας που λειτουργούν με βάση τις διευθύνσεις IP και ports, το NGFW της Palo Alto αναγνωρίζει και ελέγχει τις εφαρμογές ανεξάρτητα από τη θύρα ή το πρωτόκολλο, επιτρέποντας πιο λεπτομερή ανίχνευση και πρόληψη εισβολών.
- Ενσωμάτωση πληροφοριών απειλών : Η Palo Alto χρησιμοποιεί το Threat Intelligence Cloud, το οποίο ενημερώνεται σε πραγματικό χρόνο με πληροφορίες απειλών που συλλέγονται σε όλο το δίκτυο. Αυτό περιλαμβάνει IoCs από όλο το διαδίκτυο, τα οποία βοηθούν την πλατφόρμα να αναγνωρίζει γρήγορα και να αποκλείει κακόβουλες δραστηριότητες.
- Ανάλυση συμπεριφοράς και μηχανική μάθηση : Αξιοποιώντας την ανάλυση συμπεριφοράς και τη μηχανική μάθηση, η λύση IDP της Palo Alto εντοπίζει ανωμαλίες

και πιθανές απειλές που η παραδοσιακή ανίχνευση βάσει υπογραφών μπορεί να χάσει. Αυτή η προληπτική προσέγγιση είναι ζωτικής σημασίας για τον εντοπισμό άγνωστων απειλών, επιθέσεων zero day και προηγμένων μόνιμων απειλών (APT).

- Αυτοματοποιημένη απόκριση και ενσωμάτωση SOAR: Η πλατφόρμα υποστηρίζει αυτοματοποιημένες ροές εργασίας αντιμετώπισης περιστατικών, συμπεριλαμβανομένων των ενσωματώσεων SOAR, οι οποίες διευκολύνουν τις γρήγορες και αποτελεσματικές ενέργειες αποκατάστασης. Αυτή η αυτοματοποίηση βοηθά τις ομάδες ασφαλείας να ανταποκρίνονται σε απειλές άμεσα, μειώνοντας τους χρόνους απόκρισης.
- Ανάλυση κρυπτογραφημένης κυκλοφορίας: Η λύση IDP της Palo Alto παρακολουθεί την κρυπτογραφημένη κυκλοφορία, διασφαλίζοντας ότι οι απειλές εντοπίζονται ακόμη και μέσα σε κρυπτογραφημένες επικοινωνίες. Αυτό είναι ιδιαίτερα σημαντικό, καθώς η περισσότερη κίνηση δικτύου είναι κρυπτογραφημένη και οι παραδοσιακές τεχνικές παρακολούθησης δεν μπορούν να την αναλύσουν αποτελεσματικά.
- Προηγμένη προστασία από κακόβουλο λογισμικό: Ενσωματωμένη με την υπηρεσία WildFire της Palo Alto, η λύση περιλαμβάνει δυνατότητες ανάλυσης κακόβουλου λογισμικού και sandboxing. Αυτό επιτρέπει την ανίχνευση κακόβουλου λογισμικού που αποφεύγει τη χρήση μέσω ανάλυσης συμπεριφοράς σε ελεγχόμενο περιβάλλον.

Rapid7 InsightIDR [23] : Το Rapid7 InsightIDR είναι μια πλατφόρμα ασφάλειας cloud-native με δυνατότητες για ανίχνευση και απόκριση περιστατικών, ανάλυση συμπεριφοράς χρηστών και παρακολούθηση τελικών σημείων. Σχεδιασμένο για να βοηθά οργανισμούς όλων των μεγεθών, το InsightIDR συνδυάζει τη λειτουργία SIEM, SOAR και Threat Intelligence με την XDR και την ανάλυση κίνησης δικτύου για την διευκόλυνση της ανίχνευσης απειλών και την επιτάχυνση της αντιμετώπισης περιστατικών. Συνολικά, εμφανίζει τα παρακάτω χαρακτηριστικά:

- Δυνατότητες εκτεταμένης ανίχνευσης και απόκρισης (XDR)
- Ανάλυση κίνησης που παρέχεται δικτύου βοηθά στον εντοπισμό ύποπτων δραστηριοτήτων
- Ανάλυση συμπεριφοράς χρηστών (UEBA) βελτιώνει την ταχύτητα και την ποιότητα της διερεύνησης και της απόκρισής σε παρεκκλίνουσες δραστηριότητες.
- Διαχείριση πληροφοριών ασφαλείας και συμβάντων βρίσκεται στον πυρήνα του InsightIDR, επιτρέποντας στους χρήστες να αναλύουν σύνθετα δεδομένα για ταχύτερη απόκτηση πληροφοριών και δεδομένων σχετικών με συμβάντα.
- Πλαίσιο χαρτογράφησης επίθεσης που παρέχει αναλυτική και εύληπτη εικόνα των λεπτομερειών μιας επίθεσης.
- τεχνολογία εξαπάτησης επιτιθέμενων, με την δημιουργία honeypots, ώστε να υπάρχει έγκυρη προειδοποίηση και συλλογή κρίσιμων δεδομένων πριν την έναρξη της επίθεσης.
- Παρέχει δυνατότητες αυτοματοποίησης διαδικασιών αντιμετώπισης απειλών
- Η συλλογή στοιχείων ανιχνεύσεων και συμπεριφορών επιτιθέμενων της Rapid7 αντιστοιχίζεται λεπτομερώς με το πλαίσιο ATT&CK® της MITRE, μια ανοικτή, παγκοσμίως προσβάσιμη βάση δεδομένων των τακτικών και τεχνικών των εγκληματιών του κυβερνοχώρου.

Splunk Enterprise Security [24] : Το Splunk Enterprise Security είναι μια λύση διαχείρισης πληροφοριών και συμβάντων ασφαλείας (SIEM) που παρέχει παρακολούθηση ασφαλείας σε πραγματικό χρόνο, συσχέτιση συμβάντων και ανάλυση απειλών. Με χαρακτηριστικά όπως η χαρτογράφηση της τοπολογίας απειλών και η ειδοποίηση βάσει κινδύνου, το Splunk Enterprise Security επιτρέπει στους αναλυτές ασφαλείας να εντοπίζουν και να ανταποκρίνονται σε περιστατικά ασφαλείας γρήγορα και αποτελεσματικά.

- Πίνακας ελέγχου διαχείρισης - παρέχει υψηλού επιπέδου εικόνα των αξιοσημείωτων συμβάντων σε πραγματικό χρόνο σε όλο το κέντρο επιχειρήσεων ασφαλείας.
- Ειδοποίηση βάσει κινδύνου - αποδίδει ρίσκο σε χρήστες και συστήματα και στη συνέχεια παράγει ειδοποιήσεις σε απάντηση στην υπέρβαση των ορίων ρίσκου και συμπεριφοράς.

- Threat intelligence και SOAR - δίνει τη δυνατότητα στις ομάδες να μοιράζονται απρόσκοπτα πληροφορίες για την επιτάχυνση της διερεύνησης και της απόκρισης σε περιστατικά.
- Παρέχει επιπλέον δυνατότητες εκτεταμένου εντοπισμού και απόκρισης (XDR).

Trellix Helix [25] : Το Trellix Helix, προηγουμένως γνωστό ως FireEye Helix, είναι μια πλατφόρμα λειτουργιών ασφαλείας που φιλοξενείται στο cloud και δίνει τη δυνατότητα στους οργανισμούς να διαχειρίζονται περιστατικά ασφαλείας από την ανίχνευση έως την αποκατάσταση. Με την ανάλυση της συμπεριφοράς των χρηστών και τις εκτεταμένες επιλογές ενσωμάτωσης τρίτων εφαρμογών, το Trellix Helix είναι ένα ισχυρό εργαλείο για την αυτοματοποίηση της αντιμετώπισης περιστατικών και την προληπτική άμυνα κατά των αναδυόμενων απειλών.

- Δυνατότητες ενορχήστρωσης, αυτοματοποίησης και απόκρισης ασφάλειας (SOAR) με προκατασκευασμένα εγχειρίδια playbooks.
- Εφαρμογή προηγμένων τεχνικών ανάλυσης ανίχνευσης και αποκατάστασης .
- Η ανάλυση συμπεριφοράς χρηστών και οντοτήτων (UEBA) επιτρέπει την διασύνδεση των ειδοποιήσεων προεκπαιδευμένα μοντέλα μηχανικής μάθησης για τον εντοπισμό επικίνδυνων δραστηριοτήτων.
- Δυνατότητα διασύνδεσης εφαρμογών από μια βιβλιοθήκη με πάνω από 650 εργαλεία ασφάλειας.

Τα χαρακτηριστικά και οι δυνατότητες των παραπάνω εμπορικών λύσεων συνοψίζονται στον Πίνακα 1.

solution	VSM	Threat Intelligence & Detection	XDR	EDR	NDR	MDR	Cloud Security	IDPS	Digital Forensics	GRC	SIEM	SOAR
IBM Security QRadar Solution	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
NetWitness Threat Detection, Investigation and Response		✓	✓	✓	✓		✓	✓	✓	✓	✓	✓
Palo Alto Intrusion Detection and Prevention	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Rapid7 InsightIDR		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Splunk Enterprise Security		✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
Trellix Helix	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓

Πίνακας 1. Βασικά χαρακτηριστικά των 6 λύσεων διαχείρισης και αντιμετώπισης περιστατικών ασφάλειας.

IBM Security QRadar Solution : Το IBM Security QRadar είναι μια πλατφόρμα πληροφοριών ασφαλείας που ενσωματώνεται στις υπάρχουσες υποδομές ασφαλείας για να παρέχει δυνατότητες ανίχνευσης, διερεύνησης και αντιμετώπισης απειλών. Αναλύοντας τα δεδομένα καταγραφής και τη δραστηριότητα ροής δικτύου, το QRadar βοηθά τους οργανισμούς να εντοπίζουν γρήγορα ύποπτη συμπεριφορά και να δίνουν προτεραιότητα στις απειλές. Οι λειτουργίες του SIEM επιτρέπουν στις ομάδες ασφαλείας να ενοποιούν δεδομένα καταγραφής από διάφορες πηγές, ενώ οι δυνατότητες SOAR παρέχουν αυτοματοποιημένες ροές εργασίας για την διευκόλυνση της αντιμετώπισης περιστατικών. Το QRadar υποστηρίζει επίσης την παρακολούθηση της συμμόρφωσης, προσφέροντας αναφορές που βοηθούν τους οργανισμούς να ανταποκρίνονται στις κανονιστικές απαιτήσεις, και παρέχει ενσωματώσεις cloud security και vulnerability scanning για την κάλυψη υβριδικών και multi-cloud περιβαλλόντων.

NetWitness Threat Detection, Investigation, and Response : Το NetWitness προσφέρει μια ολοκληρωμένη πλατφόρμα για τον εντοπισμό, τη διερεύνηση και την αντιμετώπιση απειλών στον κυβερνοχώρο σε πολύπλοκα περιβάλλοντα πληροφορικής. Γνωστό για τις δυνατότητες XDR, SIEM και ανίχνευσης και απόκρισης δικτύου (NDR), το NetWitness δίνει τη δυνατότητα στους οργανισμούς να συλλέγουν και να αναλύουν δεδομένα από τελικά σημεία, δίκτυα και αρχεία καταγραφής σε πραγματικό χρόνο, παρέχοντας μια πλήρη εικόνα των περιστατικών ασφαλείας. Χρησιμοποιεί μηχανική εκμάθηση για ανίχνευση βάσει συμπεριφοράς, ενισχύοντας την ιεράρχηση απειλών. Το NetWitness υποστηρίζει επίσης υπηρεσίες managed detection and response (MDR) και περιλαμβάνει δυνατότητες IDPS, επιτρέποντας την ισχυρή παρακολούθηση της ασφάλειας, ειδικά σε υβριδικές υποδομές IT. Οι λειτουργίες SOAR που διαθέτει απλοποιούν την αντιμετώπιση περιστατικών, δίνοντας τη δυνατότητα στις ομάδες να ενεργούν ταχύτερα.

Palo Alto Intrusion Detection and Prevention : Η Palo Alto Networks προσφέρει ένα προηγμένο σύστημα ανίχνευσης και πρόληψης εισβολών (IDPS) ως μέρος της εκτεταμένης σουίτας ασφαλείας της, ικανό να παρακολουθεί και να προστατεύει τόσο τα περιβάλλοντα εντός των εγκαταστάσεων όσο και τα περιβάλλοντα cloud. Αξιοποιώντας τις πληροφορίες απειλών από το Cortex XDR, η πλατφόρμα εντοπίζει και μετριάζει τις απειλές σε δίκτυα και τελικά σημεία, καθιστώντας την ιδανική λύση για την ανίχνευση και την αντιμετώπιση απειλών. Με πρόσθετες δυνατότητες SOAR, το Palo Alto επιτρέπει στις ομάδες ασφαλείας να αυτοματοποιούν τις απαντήσεις σε περιστατικά, μειώνοντας το χειροκίνητο φόρτο εργασίας. Η πλατφόρμα είναι επίσης κατάλληλη για την ασφάλεια cloud, καθιστώντας την ένα ευέλικτο εργαλείο για την ασφάλεια περιβαλλόντων πολλαπλών cloud, ενώ προσφέρει απρόσκοπτη ενσωμάτωση πληροφοριών απειλών (Threat Intelligence).

Rapid7 InsightIDR : Το Rapid7 InsightIDR είναι μια ολοκληρωμένη πλατφόρμα ανίχνευσης και απόκρισης που έχει σχεδιαστεί για να ενοποιεί τις δυνατότητες ανίχνευσης και απόκρισης τελικών σημείων (EDR), πληροφοριών απειλών και SIEM σε μια ενιαία, επεκτάσιμη λύση. Χτισμένο ως πλατφόρμα cloud-native, το InsightIDR παρέχει πληροφορίες σε πραγματικό χρόνο στα τελικά σημεία και τη δραστηριότητα του δικτύου, δίνοντας τη δυνατότητα στις ομάδες να ανιχνεύουν και να ανταποκρίνονται γρήγορα σε πιθανές απειλές. Η ανάλυση συμπεριφοράς χρηστών (UEBA) επιτρέπει τον γρήγορο εντοπισμό ασυνήθιστης δραστηριότητας, ενώ η ενσωματωμένη λειτουργία SOAR αυτοματοποιεί τις συνήθεις εργασίες αντιμετώπισης περιστατικών. Με τα χαρακτηριστικά IDPS, το Rapid7 InsightIDR βοηθά τους οργανισμούς να διασφαλίσουν το δίκτυο, παρέχοντας ασφάλεια τόσο για περιβάλλοντα cloud όσο και για περιβάλλοντα στις εγκαταστάσεις.

Splunk Enterprise Security : Το Splunk Enterprise Security είναι μια αποτελεσματική λύση SIEM που επιτρέπει στους οργανισμούς να αποκτήσουν πληροφορίες για πιθανές απειλές, ενοποιώντας δεδομένα καταγραφής και συμβάντων από πολλαπλές πηγές. Η πλατφόρμα υποστηρίζει τη διαχείριση περιστατικών και συνεργάζεται με πηγές πληροφοριών απειλών για να αυξήσει τις δυνατότητες ανίχνευσης. Η συμβατότητα του Splunk με το cloud και τα χαρακτηριστικά διακυβέρνησης, ρίσκου και συμμόρφωσης (GRC) το καθιστούν πολύτιμο εργαλείο για οργανισμούς. Με την λειτουργία SOAR, το Splunk Enterprise Security επιτρέπει στις ομάδες να αυτοματοποιούν τις απαντήσεις και να διαχειρίζονται αποτελεσματικά τις ροές εργασίας, βελτιώνοντας σημαντικά τους χρόνους απόκρισης και μειώνοντας την απαιτούμενη χειρωνακτική εργασία των ομάδων ασφαλείας.

Trellix Helix : Το Trellix Helix, είναι μια ευέλικτη πλατφόρμα λειτουργιών ασφαλείας που συνδυάζει δυνατότητες SIEM, EDR, NDR και SOAR για να παρέχει έλεγχο των περιστατικών ασφαλείας από άκρη σε άκρη. Αξιοποιώντας τις εκτεταμένες δυνατότητες threat intelligence και μηχανικής μάθησης, το Helix μπορεί να ανιχνεύει και να ανταποκρίνεται σε προηγμένες απειλές σε ολόκληρο το δίκτυο ενός οργανισμού. Η αρχιτεκτονική του που βασίζεται στο cloud το καθιστά κατάλληλο για υβριδικά περιβάλλοντα και υποστηρίζει την ανίχνευση και την πρόληψη εισβολών για τη διασφάλιση των περιμέτρων του δικτύου. Με μεγάλη έμφαση σε Threat Intelligence, το Helix επιτρέπει το προληπτικό threat hunting, ενώ οι λειτουργίες SOAR του δίνουν τη δυνατότητα στις ομάδες να αυτοματοποιούν ροές εργασίας, βελτιώνοντας τους χρόνους απόκρισης σε περιστατικά.

2.3 Εργαλεία ανοιχτού κώδικα

Στην παρούσα ενότητα παρουσιάζονται τα εργαλεία που απαρτίζουν την προτεινόμενη πλατφόρμα, και τα βασικά χαρακτηριστικά τους :

Iris Digital Forensics and Incident Response [26] : Το Iris DFIR είναι μια πλατφόρμα ψηφιακής εγκληματολογίας και αντιμετώπισης περιστατικών προσαρμοσμένη για τις έρευνες μετά από περιστατικά. Παρέχει δομημένες ροές εργασίας για την οργάνωση και ανάλυση ψηφιακών αποδεικτικών στοιχείων από συστήματα που έχουν παραβιαστεί, επιτρέποντας στους αναλυτές να διεξάγουν ενδελεχείς ελέγχους και δραστηριότητες αντιμετώπισης συμβάντων. Το Iris DFIR είναι ιδιαίτερα επωφελές για την εγκληματολογική ανάλυση μετά την εκδήλωση ενός συμβάντος, εστιάζοντας στη συλλογή, τη διατήρηση και την εξέταση αντικειμένων για την καλύτερη κατανόηση της φύσης και της προέλευσης μιας απειλής στον κυβερνοχώρο. Βασικά χαρακτηριστικά του Iris DFIR είναι:

- Η διαχείριση δεδομένων συμβάντων και η δομημένη συλλογή αποδεικτικών στοιχείων .
- Εργαλεία ανάλυσης για την κατανόηση του πεδίου και του χρονοδιαγράμματος του συμβάντος .
- Διευκόλυνση συνεργασίας για τη διενέργεια ομαδικών ερευνών .
- Διαχείριση ροής εργασιών για βελτιωμένη αντιμετώπιση περιστατικών .
- Επεκτάσιμη και υποστηρίζει την ενσωμάτωση με άλλα εργαλεία αντιμετώπισης συμβάντων.

Κύρια κατηγορία : **Digital Forensics and Incident Response**

TheHive Cortex [27] : Το TheHive Cortex είναι μια αποτελεσματική πλατφόρμα αντιμετώπισης περιστατικών και ανάλυσης πληροφοριών απειλών, σχεδιασμένη για να βοηθά τις ομάδες ασφαλείας να εμπλουτίζουν, να αναλύουν και να ανταποκρίνονται στις απειλές στον κυβερνοχώρο. Με την ενσωμάτωση με άλλα εργαλεία, το Cortex επιτρέπει την ανάλυση των πληροφοριών απειλών, διευκολύνοντας τους αναλυτές να διερευνούν και να ταξινομούν τις ειδοποιήσεις. Κυριότερες δυνατότητες του είναι:

- Αυτοματοποιημένη ανάλυση δεδομένων IOCs
- Ανοιχτού κώδικα και προσαρμόσιμο για να ταιριάζει σε διάφορες περιπτώσεις χρήσης
- Πληθώρα επιλογών διασύνδεσης με εργαλεία ανάλυσης δεδομένων IOCs.

- Δυνατότητα χρήσης responders , δηλαδή εργαλείων που αντιμετωπίζουν μια απειλή (ip blocking, host isolation κλπ)
- Υποστηρίζει αυτοματοποίηση για τον εμπλουτισμό δεδομένων απειλών και την απόκριση.

Κύριες κατηγορίες : **Threat Intelligence Platform, SOAR**

Malware Information Sharing Platform [28] : Το MISP είναι μια ανοικτού κώδικα πλατφόρμα ανταλλαγής πληροφοριών σχετικά με απειλές που επιτρέπει στους οργανισμούς να συλλέγουν, να αναλύουν και να μοιράζονται δεδομένα σχετικά με απειλές, συμπεριλαμβανομένων δεικτών συμβιβασμού (IOC). Χρησιμοποιείται συνήθως για τη βελτίωση της ανίχνευσης απειλών με την ανταλλαγή σχετικών πληροφοριών μεταξύ ομάδων και οργανισμών, επιτρέποντας την προληπτική διαχείριση απειλών. Το MISP επιτρέπει την χρήση πρωτόκολλων όπως STIX/TAXII για την ανταλλαγή δεδομένων για κακόβουλο λογισμικό. Βασικά χαρακτηριστικά :

- Συλλογή και ανταλλαγή πληροφοριών σχετικά με απειλές, συμπεριλαμβανομένων των IOC .
- Υποστηρίζει STIX/TAXII για διαλειτουργικότητα και επικοινωνία με άλλες πλατφόρμες .
- Συσχέτιση των κοινών πληροφοριών για απειλές με σκοπό την καλύτερη κατανόηση
- Εύκολη ενσωμάτωση με άλλα εργαλεία κυβερνοασφάλειας για τον εμπλουτισμό των δεδομένων απειλών.

Κύρια κατηγορία : **Threat Intelligence Platform**

CyberChef [29] : Το CyberChef είναι ένα ευέλικτο εργαλείο που χρησιμοποιείται για μετασχηματισμό, κρυπτογράφηση, κωδικοποίηση και αποκρυπτογράφηση δεδομένων. Επιτρέπει στους αναλυτές να χειρίζονται και να επεξεργάζονται δεδομένα σε διάφορες μορφές, καθιστώντας το χρήσιμο για μια σειρά εργασιών όπως την αποκωδικοποίηση πληροφοριών . Το CyberChef είναι ένα απαραίτητο εργαλείο για τους εγκληματολογικούς αναλυτές που χρειάζονται γρήγορους μετασχηματισμούς κατά τη διάρκεια ερευνών. Κύριες λειτουργίες και χαρακτηριστικά του είναι :

- Λειτουργίες κρυπτογράφησης, αποκρυπτογράφησης και κωδικοποίησης δεδομένων .
- Εργαλεία χειρισμού δεδομένων, όπως κατακερματισμός και συμπίεση.
- Εκτεταμένη βιβλιοθήκη «συνταγών» δηλαδή αλυσιδωτών μετασχηματισμών για τη τροποποίηση δεδομένων .
- Απλή, διαδικτυακή διεπαφή για γρήγορες λειτουργίες δεδομένων .

Κύρια κατηγορία : **Digital Forensics**

Mattermost [30] : Το Mattermost είναι μια πλατφόρμα επικοινωνίας ανοικτού κώδικα που παρέχει ασφαλή ανταλλαγή μηνυμάτων και συνεργασία για ομάδες, καθιστώντας την χρήσιμη για τον συντονισμό των ενεργειών αντιμετώπισης περιστατικών. Προσφέρει ασφαλή κανάλια επικοινωνίας όπου οι αναλυτές μπορούν να μοιράζονται ευρήματα, να κλιμακώνουν περιστατικά και να παρακολουθούν την κατάσταση της έρευνας. Το Mattermost έχει τις εξής δυνατότητες:

- Ασφαλή κανάλια επικοινωνίας σε πραγματικό χρόνο για ομάδες.
- Δυνατότητα κοινής χρήσης αρχείων, αποδεικτικών στοιχείων και λεπτομερειών περιστατικού.
- Δυνατότητα ενσωμάτωσης εφαρμογών για την επαύξηση των λειτουργιών του και την βελτίωση της ασφάλειας (εφαρμογές όπως το antivirus ClamAV για την εξέταση των αρχείων που αναρτώνται στα κανάλια)
- Δημιουργία ροών εργασίας τύπου playbook που διευκολύνει και αυτοματοποιεί ενέργειες σε διάφορα περιστατικά.

Κύρια κατηγορία : **Collaboration and Communication**

Velociraptor [31] : Το Velociraptor είναι ένα εργαλείο παρακολούθησης τελικών σημείων και ψηφιακής εγκληματολογίας που έχει σχεδιαστεί για τη συλλογή δεδομένων από πολλαπλά τελικά σημεία. Παρέχει λεπτομερή ορατότητα στη δραστηριότητα των τελικών σημείων σε πραγματικό χρόνο και είναι πολύτιμο για την ψηφιακή εγκληματολογία, επιτρέποντας στις ομάδες να

συλλέγουν και να αναλύουν δεδομένα από δυνητικά παραβιασμένα συστήματα. Ο ελαφρύς σχεδιασμός του Velociraptor και η φύση του ανοιχτού κώδικα το καθιστούν δημοφιλές για παρακολούθηση και εγκληματολογική ανάλυση τερματικών σημείων μεγάλης κλίμακας. Βασικά χαρακτηριστικά:

- Συλλογή δεδομένων τελικού σημείου για εγκληματολογική ανάλυση.
- Αναζητήσεις βάσει ερωτημάτων (με την χρήση ειδικά σχεδιασμένης γλώσσας VQL - Velociraptor Query Language) για ταχεία ανάκτηση δεδομένων .
- Επεκτάσιμη για την παρακολούθηση μεγάλου αριθμού τερματικών σημείων .
- Ανοικτού κώδικα και υψηλή δυνατότητα προσαρμογής για διάφορες χρήσεις .
- Αποτελεσματική συλλογή δεδομένων.

Κύριες κατηγορίες: **Digital Forensics and Incident Response (DFIR), EDR**

Wazuh [32] : Το Wazuh είναι μια πλατφόρμα παρακολούθησης SIEM και ασφάλειας ανοικτού κώδικα που προσφέρει δυνατότητες ανάλυσης αρχείων καταγραφής, ανίχνευσης απειλών και αντιμετώπισης περιστατικών. Παρακολουθεί υποδομές cloud και on-premises, ανιχνεύοντας απειλές σε πραγματικό χρόνο και βοηθώντας στη συμμόρφωση με κανονισμούς και διεθνής οδηγίες ασφάλειας. Το Wazuh υποστηρίζει διαχείριση αρχείων καταγραφής, παρακολούθηση ασφαλείας και έλεγχο ακεραιότητας αρχείων, καθιστώντας το ένα ευέλικτο εργαλείο για την ανίχνευση απειλών και την παρακολούθηση της συμμόρφωσης. Βασικές λειτουργίες του είναι :

- Δυνατότητες ανίχνευσης απειλών και ειδοποίησης σε πραγματικό χρόνο.
- Ανάλυση αρχείων καταγραφής και συσχέτιση συμβάντων.
- Παρακολούθηση ακεραιότητας αρχείων για ανάγκες συμμόρφωσης συμφώνως κανονισμών.
- Ενσωματωμένη ανίχνευση και σάρωση ευπαθειών.
- Ανοιχτού κώδικα, προσαρμόσιμο SIEM για ολοκληρωμένη παρακολούθηση της ασφάλειας.
- Παρέχει δυνατότητες ασφάλειας νέφους

Κύριες κατηγορίες: **XDR, SIEM, Threat Intelligence & Detection, GRC, Cloud Security, Vulnerability Management**

Kape [33] : Το Kape είναι ένα εργαλείο ψηφιακής εγκληματολογίας που χρησιμοποιείται κυρίως για τη συλλογή και ανάλυση δεδομένων σε εκτεθειμένα τελικά σημεία. Με την χρήση των Targets, δηλαδή έτοιμων πακέτων αναζήτησης δεδομένων βοηθά στην αυτοματοποίηση της συλλογής αποδεικτικών στοιχείων, επιτρέποντας στους αναλυτές να συλλέγουν δεδομένα γρήγορα και αποτελεσματικά για ανάλυση. Το Kape είναι ιδανικό για έρευνες ψηφιακής εγκληματολογίας, επιτρέποντας στους αναλυτές να εξάγουν δεδομένα από πολλαπλές πηγές σε ένα τελικό σημείο και να τα επεξεργάζονται για χρήση στην αντιμετώπιση περιστατικών. Το Kape προσφέρει:

- Γρήγορη συλλογή δεδομένων από παραβιασμένα συστήματα .
- Χρήση πληθώρας διαφορετικών πακέτων συλλογής δεδομένων (targets) , που εξυπηρετούν τις ανάγκες των αναλυτών για όλες τις περιπτώσεις.
- Χρήση πολλαπλών modules για την εφαρμογή εργαλείων ανάλυσης επί των συλλεχθέντων targets και εξαγωγή αποτελεσμάτων άμεσα.
- Αποτελεσματική ανάλυση δεδομένων από πολλαπλές πηγές .
- Μειώνει το χρόνο που απαιτείται για τη συλλογή δεδομένων κατά τη διάρκεια περιστατικών.
- Υποστηρίζει την ενσωμάτωση με άλλα εγκληματολογικά εργαλεία για αποστολή των δεδομένων που έχουν συλλεχθεί και ανάλυση.

Κύρια κατηγορία : **Digital Forensics**

Kuiper [34] : Το Kuiper είναι μια ψηφιακή πλατφόρμα που παρέχει στην ομάδα αναλυτών , την δυνατότητα να αναζητούν και να απεικονίζουν τα συλλεχθέντα αποδεικτικά στοιχεία (τα αποδεικτικά στοιχεία θα μπορούσαν να συλλεχθούν το Kape). Επιπλέον, μπορεί να συνεργάζεται

με άλλα εργαλεία ίδια πλατφόρμα για την επισήμανση αντικειμένων και την παρουσίασή τους σε χρονολογική σειρά, καθώς και να θέτει κανόνες για την αυτοματοποίηση της ανίχνευσης. Ο κύριος σκοπός αυτού του εργαλείου είναι να βοηθήσει στην αυτοματοποίηση των δραστηριοτήτων ψηφιακής έρευνας και να επιτρέψει προηγμένες δυνατότητες ανάλυσης με τη δυνατότητα χειρισμού μεγάλου όγκου δεδομένων. Το Kuiper έχει τα εξής χαρακτηριστικά:

- Σχεδιασμένο για ταχεία ανάλυση δεδομένων σε σενάρια μεγάλου όγκου .
- Υποστηρίζει πολλαπλές πηγές δεδομένων για εγκληματολογική ανάλυση .
- Αυτοματοποιεί τις ροές εργασίας ψηφιακής εγκληματολογίας κατά την αντιμετώπιση περιστατικών .
- Φιλική προς το χρήστη διεπαφή για αποτελεσματική επεξεργασία δεδομένων .

Κύρια κατηγορία: **Digital Forensics and Incident Response**

Shuffle [35] : Το Shuffle είναι μια πλατφόρμα αυτοματοποίησης ανοικτού κώδικα που έχει σχεδιαστεί για να βελτιώνει την αντιμετώπιση περιστατικών συνδέοντας εργαλεία ασφαλείας και αυτοματοποιώντας ροές εργασίας. Ενσωματώνεται με διάφορες λύσεις κυβερνοασφάλειας, επιτρέποντας στις ομάδες να αυτοματοποιούν τις επαναλαμβανόμενες εργασίες και να βελτιώνουν την αποτελεσματικότητα των δραστηριοτήτων απόκρισης. Η ευελιξία του Shuffle το καθιστά κατάλληλο για τη δημιουργία σύνθετων ροών εργασίας που επιταχύνουν τη διαλογή και την απόκριση σε περιστατικά. Δυνατότητες :

- Αυτοματοποίηση των ροών εργασίας ασφάλειας για τη μείωση του χρόνου απόκρισης .
- Ενσωματώνεται με άλλα εργαλεία για βελτιωμένη αντιμετώπιση περιστατικών .
- Πλατφόρμα αυτοματοποίησης ανοικτού κώδικα και προσαρμόσιμη .

Κύρια κατηγορία : **SOAR**

Suricata [36] : Το Suricata είναι ένα σύστημα ανίχνευσης και πρόληψης εισβολών ανοικτού κώδικα (IDPS) που παρακολουθεί την κυκλοφορία του δικτύου για τον εντοπισμό και την πρόληψη απειλών στον κυβερνοχώρο. Χρησιμοποιεί μεθόδους ανίχνευσης βάσει κανόνων, καθιστώντας το αποτελεσματικό για τον εντοπισμό γνωστών μοτίβων επίθεσης στην κυκλοφορία του δικτύου. Η ευελιξία και η δυνατότητα προσαρμογής του Suricata το καθιστούν δημοφιλή επιλογή για οργανισμούς που αναζητούν ισχυρές δυνατότητες παρακολούθησης δικτύου. Χαρακτηριστικά :

- Ανίχνευση και πρόληψη εισβολών μέσω παρακολούθησης πακέτων.
- Ανίχνευση βάσει κανόνων για τον εντοπισμό γνωστών μοτίβων επίθεσης .
- Υποστηρίζει ανάλυση κίνησης σε πραγματικό χρόνο και καταγραφή πακέτων .
- Ανοιχτού κώδικα με εκτεταμένη υποστήριξη από την κοινότητα .
- Εύκολα προσαρμόσιμο για συγκεκριμένες ανάγκες ασφάλειας δικτύου.

Κύριες κατηγορίες **IDPS, NDR**

Αυτά τα ποικίλα εργαλεία κυβερνοασφάλειας προσφέρουν εξειδικευμένες δυνατότητες σε θέματα ψηφιακής εγκληματολογίας, πληροφοριών απειλών, παρακολούθησης δικτύου και αυτοματοποίησης - το καθένα από αυτά είναι απαραίτητο για έναν ολοκληρωμένο εντοπισμό και αντιμετώπιση περιστατικών. Ενσωματώνοντας τα μοναδικά τους πλεονεκτήματα, τα εργαλεία αυτά μπορούν να αποτελέσουν μια συνεκτική λύση για τη διαχείριση και τον μετριασμό περιστατικών ασφαλείας, βοηθώντας τους οργανισμούς να εντοπίζουν γρήγορα, να ανταποκρίνονται και να προσαρμόζονται στις αναδυόμενες απειλές. Τα παραπάνω σε συνδυασμό με τη συνεργατική διαχείριση κυβερνοεπιθέσεων που παρέχεται από το IRIS συνθέτουν τη προτεινόμενη πλατφόρμα η οποία επιτρέπει την απρόσκοπτη συνεργασία και την άμεση ανταλλαγή πληροφοριών μεταξύ ειδικών, τόσο σε επίπεδο οργανισμού, όσο σε εθνικό και διεθνές επίπεδο, που πλέον αποτελεί αδήριτη ανάγκη στην κυβερνοάμυνα. Στον Πίνακα 2 συγκρίνεται η προτεινόμενη πλατφόρμα, που αποτελείται από τα εργαλεία ανοιχτού κώδικα αυτής της ενότητας, με τα εμπορικά εργαλεία της ενότητας 2.2.

solution	VSM	Threat Intelligence & Detection	XDR	EDR	NDR	MDR	Cloud Security	IDPS	Digital Forensics	GRC	SIEM	SOAR
IBM Security QRadar Solution	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
NetWitness Threat Detection, Investigation and Response		✓	✓	✓	✓		✓	✓	✓	✓	✓	✓
Palo Alto Intrusion Detection and Prevention	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Rapid7 InsightIDR		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Splunk Enterprise Security		✓	✓	✓	✓	✓	✓	✓		✓	✓	✓
Trellix Helix	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
Custom Solution	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Πίνακας 2 Σύγκριση των 6 παραπάνω λύσεων με την ανεπτυγμένη πλατφόρμα.

3. Προτεινόμενη αρχιτεκτονική

Στο ακόλουθο κεφάλαιο περιγράφεται η προτεινόμενη αρχιτεκτονική για την κεντρική διαχείριση και αντιμετώπιση περιστατικών ασφάλειας και κυβερνοεπιθέσεων που αναπτύχθηκε στην διατριβή. Έχοντας συνοψίσει τα χαρακτηριστικά και τις δυνατότητες των πιο διαδεδομένων εργαλείων διαχείρισης κυβερνοεπιθέσεων, διερευνήθηκαν και επιλέχθηκαν οι κατάλληλες επιμέρους εφαρμογές ανοιχτού κώδικα (open source), οι οποίες απαρτίζουν την πλατφόρμα διαχείρισης κυβερνοεπιθέσεων. Καθένα από αυτά τα επιμέρους εργαλεία έχει πολλαπλούς ρόλους και δυνατότητες. Βασικό χαρακτηριστικό της πλατφόρμας είναι η αποτελεσματική διάχυση της πληροφορίας και των δεδομένων, το οποίο σημαίνει ότι δεν λαμβάνουν όλα τα επιμέρους συστήματα τις ίδιες πληροφορίες, αλλά αυτές που μπορούν να αξιοποιήσουν. Στην συνέχεια παρουσιάζονται αναλυτικά, τα απαιτούμενα χαρακτηριστικά της πλατφόρμας, ο τρόπος διασύνδεσης και η ροή των δεδομένων στις εφαρμογές.

3.1 Ανάλυση Απαιτήσεων Υλοποίησης

Στην ακόλουθη ενότητα παρουσιάζονται τα απαιτούμενα χαρακτηριστικά ασφάλειας και λειτουργικότητας που θα πρέπει να διαθέτει η πλατφόρμα και τα εργαλεία που προσδίδουν τις εκάστοτε δυνατότητες ώστε να μπορεί να ανταποκριθεί αποτελεσματικά στις απαιτήσεις ενός επιχειρησιακού περιβάλλοντος με πολλαπλές και πολύμορφες απειλές.

Συνεργασία στο χειρισμό και την αντιμετώπιση περιστατικών : Η αντιμετώπιση περιστατικών απαιτεί απρόσκοπτη συνεργασία μεταξύ ομάδων αναλυτών . Το Mattermost διευκολύνει την ασφαλή επικοινωνία και τις ενημερώσεις εργασιών. Το IRIS DFIR οργανώνει τις ενέργειες της ομάδας παρέχοντας ένα δομημένο πλαίσιο για ψηφιακή εγκληματολογία και την αντιμετώπιση περιστατικών.

Ασφαλής ανταλλαγή πληροφοριών για απειλές : Η ανταλλαγή δεικτών παραβίασης (IOC) και άλλων πληροφοριών για απειλές πρέπει να είναι ασφαλής και να τηρεί τυποποιημένα πρωτόκολλα όπως το STIX/TAXII για να αποτρέπεται η διαρροή δεδομένων και να διασφαλίζεται η διαλειτουργικότητα. Το MISP επιτρέπει τη δομημένη ανταλλαγή πληροφοριών, με την χρήση των πρωτοκόλλων STIX/TAXII.

Αυτοματοποίηση επαναλαμβανόμενων εργασιών : Για τη βελτίωση της αποδοτικότητας, ελαχιστοποίηση του χρόνου απόκρισης και τη μείωση του ανθρώπινου σφάλματος, η αυτοματοποίηση επαναλαμβανόμενων εργασιών, είναι ζωτικής σημασίας. Το Shuffle αυτοματοποιεί ροές εργασίας, ενσωματώνοντας εργαλεία όπως το Cortex για τον εμπλουτισμό των δεδομένων των IOC και το Velociraptor για τη συλλογή artifacts από τα τελικά σημεία.

Παρακολούθηση και ανίχνευση σε πραγματικό χρόνο : Η ανίχνευση και η αντιμετώπιση απειλών σε πραγματικό χρόνο είναι ζωτικής σημασίας για τον περιορισμό περιστατικών πριν αυτά κλιμακωθούν. Το Suricata παρακολουθεί την κυκλοφορία του δικτύου για την ανίχνευση εισβολών, ενώ το Wazuh παρέχει παρακολούθηση σε επίπεδο τελικού σημείου και ανίχνευση ανωμαλιών. Μαζί, προσφέρουν μια ολοκληρωμένη εικόνα επιτρέποντας την προληπτική διαχείριση απειλών.

Ολοκληρωμένη ψηφιακή εγκληματολογία : Η διερεύνηση περιστατικών απαιτεί την χρήση εργαλείων Digital Forensics για τη συλλογή και ανάλυση των artifacts ενός τελικού σημείου. Το Velociraptor και το KAPE διευκολύνουν την ταχεία συλλογή και ανάλυση αντικειμένων από τα τελικά σημεία, ενώ το IRIS DFIR προσφέρει ένα εμπεριστατωμένο πλαίσιο επεξεργασίας και διαχείρισης των συλλεχθέντων δεδομένων επιτρέποντας τον εντοπισμό επιθέσεων και την αξιολόγηση της προσβολής.

Κεντρική επικοινωνία : Η αποτελεσματική αντιμετώπιση περιστατικών εξαρτάται και βασίζεται στην κεντρική επικοινωνία για την ευθυγράμμιση των ενεργειών των μελών της ομάδας διαχείρισης σχετικά με τις εργασίες και τα ευρήματα. Το Mattermost παρέχει μια ασφαλή και συγκεντρωτική πλατφόρμα για ανταλλαγή μηνυμάτων σε πραγματικό χρόνο, διασφαλίζοντας ότι όλοι οι ενδιαφερόμενοι παραμένουν ενήμεροι.

Ευέλικτες , προσαρμόσιμες και επεκτάσιμες ροές εργασίας : Οι οργανισμοί απαιτούν ροές εργασίας που προσαρμόζονται στις ιδιαίτερες ανάγκες τους και μπορούν να κλιμακώνονται με τις αυξανόμενες απαιτήσεις. Το Shuffle προσφέρει προσαρμογή ροής εργασιών με drag-and-drop, επιτρέποντας στους χρήστες να προσαρμόζουν τις διαδικασίες τους σε κάθε περίπτωση.

Ανάλυση δεδομένων σε πραγματικό χρόνο : Η άμεση ανάλυση αρχείων καταγραφής και αντικειμένων είναι ζωτικής σημασίας για την αποκάλυψη κακόβουλης δραστηριότητας και την αποτελεσματική αντίδραση. Η Kuiper επεξεργάζεται δεδομένα ροής για πληροφορίες σε πραγματικό χρόνο, ενώ η Suricata αναλύει άμεσα την κυκλοφορία του δικτύου για τον εντοπισμό ύποπτων μοτίβων, εξασφαλίζοντας τον γρήγορο εντοπισμό απειλών.

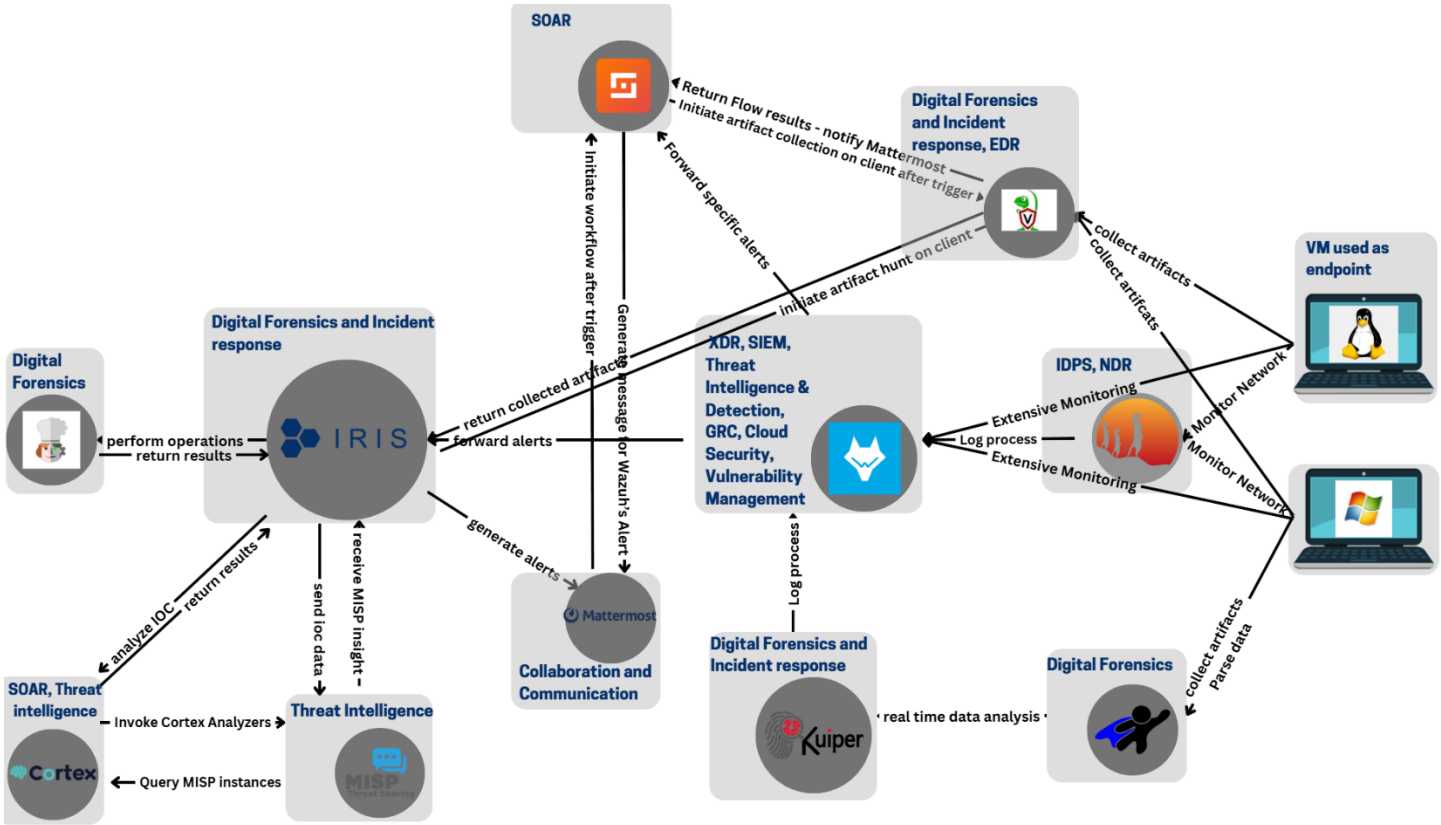
Κανονιστική συμμόρφωση : Οι οργανισμοί πρέπει να τηρούν τους κανονισμούς προστασίας δεδομένων κατά το χειρισμό και την ανταλλαγή ευαίσθητων πληροφοριών. Το Wazuh διασφαλίζει την ευθυγράμμιση του οργανισμού και των διαδικασιών του με τις κανονιστικές απαιτήσεις με την χρήση των Governance Risk and Compliance λειτουργιών του.

Επεκτάσιμη αρχιτεκτονική : Μια κλιμακούμενη αρχιτεκτονική είναι απαραίτητη για την προσαρμογή στον αυξανόμενο όγκο δεδομένων και τις ενσωματώσεις. Το Shuffle επιτρέπει την εύκολη κλιμάκωση με την ενσωμάτωση πρόσθετων εργαλείων και ροών εργασίας, ενώ το Wazuh και το Velociraptor υποστηρίζουν την συνεχή παρακολούθηση σε μεγάλα δίκτυα με πολυάριθμα τελικά σημεία, διασφαλίζοντας ότι η πλατφόρμα αναπτύσσεται μαζί με τις οργανωτικές ανάγκες.

Συγκεντρωτική καταγραφή: Η κεντρική συλλογή αρχείων καταγραφής είναι απαραίτητη για την επίγνωση της κατάστασης και την ανάλυση μετά από κάποιο περιστατικό. Το Wazuh ενοποιεί τα αρχεία καταγραφής τελικών σημείων, ενώ το Suricata παρακολουθεί το δίκτυο και προωθεί τα δεδομένα καταγραφής του στο Wazuh για περαιτέρω ανάλυση.

Συνοψίζοντας, η προτεινόμενη πλατφόρμα θα πρέπει να χαρακτηρίζεται από **διαλειτουργικότητα**, ενσωματώνοντας απρόσκοπτα διαφορετικά εργαλεία όπως τα Suricata, Velociraptor και MISP για την ενοποίηση των ροών εργασίας και την ενίσχυση της επιχειρησιακής συνεργατικότητας. Ο **αρθρωτός** σχεδιασμός της διασφαλίζει ότι κάθε εργαλείο -όπως το Wazuh για την παρακολούθηση τελικών σημείων ή το Cortex για τον εμπλουτισμό δεδομένων των IOCs- είναι ανεξάρτητο αλλά **διαλειτουργικό**, επιτρέποντας την ευέλικτη αντικατάσταση του με άλλο εφάμιλλών δυνατοτήτων ή επέκταση του. Η **αυτοματοποίηση** αποτελεί βασικό χαρακτηριστικό, διευκολύνοντας την εκτέλεση επαναλαμβανόμενων εργασιών, όπως η ταξινόμηση ειδοποιήσεων και ο εμπλουτισμός IOC, επιτρέποντας έτσι στους αναλυτές να επικεντρωθούν σε κρίσιμες λειτουργίες. Οι δυνατότητες **επιτήρησης πραγματικού χρόνου** εξασφαλίζουν συνεχή παρακολούθηση και γρήγορο μετριασμό των απειλών, αξιοποιώντας εργαλεία όπως το Suricata για ανάλυση δικτύου και το Wazuh για ανίχνευση απειλών στα τελικά σημεία. Η **ασφαλής επικοινωνία** παρέχεται με τη χρήση των Mattermost και MISP, όπου το τελευταίο χρησιμοποιεί κρυπτογράφηση και τυποποιημένα πρωτόκολλα όπως το **STIX/TAXII** για τη διασφάλιση ευαίσθητων δεδομένων. Η πλατφόρμα υποστηρίζει έλεγχο και διαχείριση περιστατικών διαφόρων λειτουργικών συστημάτων χειριζόμενη αποτελεσματικά περιστατικά τόσο σε συστήματα Windows όσο και σε συστήματα Linux για ολοκληρωμένη κάλυψη. Επιπλέον, η **επεκτασιμότητά** της, που τροφοδοτείται από εργαλεία όπως το Wazuh και το Shuffle, επιτρέπει στην πλατφόρμα να αναπτύσσεται με τις οργανωτικές ανάγκες, ενσωματώνοντας απρόσκοπτα επιπλέον τελικά σημεία, ροές εργασίας και ενσωματώσεις.

3.2 Δομή πλατφόρμας - ροή δεδομένων



Εικόνα 1. Ροή δεδομένων μεταξύ των εφαρμογών της πλατφόρμας.

Στην εικόνα 1 παρουσιάζεται η ροή των δεδομένων μεταξύ των εργαλείων της πλατφόρμας. Σκοπός είναι η ανταλλαγή πληροφοριών μεταξύ του εκάστοτε συστήματος, ώστε όλες οι ομάδες αναλυτών να έχουν μια πλήρη εικόνα για το περιστατικό και να διευκολύνεται η εργασία του αναλυτή, καθώς ο ίδιος κατευθύνεται σε έναν σωστό γρήγορο αποτελεσματικό και αυτοματοποιημένο τρόπο διαχείρισης. Πιο συγκεκριμένα έχουμε :

Iris – Cortex : Η κεντρική πλατφόρμα επικοινωνεί άμεσα με το Cortex και παρέχει την δυνατότητα μεταφοράς δεδομένων των IOCs για την επεξεργασία τους από τους analyzes που χρησιμοποιεί. Τα δεδομένα αυτά μπορεί να είναι διαφόρων τύπων, όπως ip, hash, domain name, url, registry κλπ. Μόλις ληφθούν τα δεδομένα από το Cortex τότε δημιουργείται μία νέα εργασία ανάλυσης η οποία είναι προσβάσιμη από το Dashboard του. Ταυτόχρονα μπορούν να εκτελούνται πολλαπλές αναλύσεις δεδομένων στο Cortex. Μόλις κάποια ολοκληρωθεί (είτε επιτυχώς είτε όχι) τότε τα αποτελέσματά της είναι προσβάσιμα μέσω του Iris.

Iris – Misp : Το Iris έχει την δυνατότητα να λαμβάνει πληροφορίες από την βάση δεδομένων του MISP. Επιτρέπει στους αναλυτές να έχουν πρόσβαση σε σχετικά με το IOC δεδομένα για πρότερες απειλές και περιστατικά τα οποία συμβάλλουν καταλυτικά στην διερεύνηση. Η διαδικασία αυτή μπορεί να αυτοματοποιηθεί, έτσι ώστε με την δημιουργία νέου IOC ή την ενημέρωση των δεδομένων ήδη υπάρχοντος, να λαμβάνονται οι σχετικές πληροφορίες από το MISP.

Iris-Cyberchef : Σε αυτή την περίπτωση, τα εργαλεία και το γραφικό περιβάλλον του Cyberchef είναι άμεσα προσβάσιμα από το Iris. Το Cyberchef μπορεί να χρησιμοποιηθεί κατά την διαδικασία της διαχείρισης ενός περιστατικού, καθώς παρέχει την δυνατότητα στον αναλυτή να αποκωδικοποιήσει κρυπτογραφημένα δεδομένα , να αναζητήσει γνωστές υπογραφές

κακόβουλου λογισμικού με την χρήση συναρτήσεων κατακερματισμού (hashing functions) και να πραγματοποιήσει σύνθετες και πολύπλοκες διαδικασίες αυτόματα με την χρήση “συνταγών” (recipes) δηλαδή αλυσιδωτών μετασχηματισμών και πράξεων σε δεδομένα, χωρίς να χρειαστεί να μεταβεί σε διαφορετική πλατφόρμα από το Iris.

Cortex-MISP : Η διασύνδεση των δύο εφαρμογών ενισχύει την διάδοση δεδομένων στα εργαλεία της πλατφόρμας, ώστε αυτά , εφόσον είναι δυνατόν, να τα εμπλουτίσουν και να προσδώσουν μια καθολική και ακριβή εικόνα στον αναλυτή αναφορικά με το περιστατικό ή την απειλή. Το Misp έχει την δυνατότητα να αποστέλλει τα δεδομένα των IOCs στο Cortex για ανάλυση, όπως ακριβώς και το Iris. Αυτό είναι απαραίτητο, διότι δεν είναι αποκλειστική πηγή δεδομένων του MISP το IRIS, αλλά μπορεί κάποιος χρήστης να το συνδυάσει και με άλλες εφαρμογές ή να το χρησιμοποιήσει αυτόνομα. Καθώς όμως το MISP αποτελεί ένα ισχυρό εργαλείο Threat Intelligence , κρίνεται καθοριστική και η επικοινωνία του με το Cortex ώστε να υπάρχει η δυνατότητα να λαμβάνονται δεδομένα για κάποιο IOC και να εμπλουτίζεται ακόμα περισσότερο η αναφορά που επιστρέφει το Cortex μέσω του Iris στον χρήστη.

Iris-Mattermost : Το Mattermost έχει καθοριστικό ρόλο και διευκολύνει καταλυτικά την επικοινωνία των μελών εντός ενός SOC / CSIRT. Παρέχει την δυνατότητα ενημέρωσης σχετικά με αλλαγές σε δεδομένα του Iris (δημιουργία νέου Alert, ενημέρωση IOC, διαγραφή κάποιου Asset κλπ) σε πραγματικό χρόνο. Επιπλέον υπάρχει η επιλογή ενημέρωσης συγκεκριμένων μόνο καναλιών του Mattermost, τα οποία θα σχετίζονται με την ενημέρωση αυτή (IT, legal department, operations κλπ). Τέλος το Mattermost έχει την επιλογή δημιουργίας και χρήσης Playbooks τα οποία μπορούν να περιγράφουν και να συντονίζουν τις ενέργειες που θα πρέπει να εκτελέσουν οι εμπλεκόμενες ομάδες σε κάθε περιστατικό.

Iris-Velociraptor : Το Velociraptor παρέχει την δυνατότητα παρακολούθησης της δραστηριότητας των endpoints σε πραγματικό χρόνο, επιτρέποντας την έγκαιρη ανίχνευση απειλών μέσω της συλλογής artifacts. Όταν ενσωματώνεται με το IRIS, οι κρίσιμες ειδοποιήσεις των endpoints μπορούν να μεταφερθούν απρόσκοπτα σε cases του IRIS, επιτρέποντας στις ομάδες να αντιδράσουν ταχύτερα στις συνεχιζόμενες επιθέσεις, πραγματοποιώντας τις απαιτούμενες ενέργειες σε πραγματικό χρόνο.

Wazuh – Iris : Κύρια πηγή ειδοποιήσεων του Iris για περιστατικά είναι το Wazuh. Το Wazuh μπορεί να παρακολουθεί για ειδοποιήσεις παραβίασης ασφαλείας με τους διάφορους μηχανισμούς που διαθέτει και να δημιουργεί alerts με την χρήση ενός ruleset που διαθέτει. Αν κάποιο από αυτά τα alerts είναι σημαντικό, τότε τό Wazuh μπορεί να αποστείλει τα δεδομένα του alert αυτού στο Iris και να δημιουργηθεί εκεί νέο alert το οποίο έπειτα μπορεί να το διαχειριστεί κατάλληλα ο αναλυτής.

Suricata-Wazuh: Το Suricata υπερέχει στην ανίχνευση απειλών στο δίκτυο, εντοπίζοντας κακόβουλες δραστηριότητες, όπως απόπειρες εισβολής και επιθέσεις DDoS μέσω της ανάλυσης της κίνησης δικτύου. Με την ενσωμάτωση με το Wazuh, οι ειδοποιήσεις και τα αρχεία καταγραφής του Suricata μπορούν να εισαχθούν στην κεντρική πλατφόρμα του Wazuh, παρέχοντας ευρύτερη εικόνα για τις ομάδες ασφαλείας. Σε περίπτωση που υπάρξει ειδοποίηση από το Suricata για προσβολή υψηλής επικινδυνότητας, τότε η ειδοποίηση αυτή θα μεταφερθεί στο Wazuh και έπειτα θα δημιουργηθεί alert στο Iris, με τα αντίστοιχα δεδομένα.

Kape-Kuiper-Wazuh : Το KAPE μπορεί να συλλέγει γρήγορα δεδομένα από πολλαπλά endpoints. Τα συλλεχθέντα δεδομένα μπορούν στη συνέχεια να τροφοδοτηθούν στο Kuiper για αυτοματοποιημένη ανάλυση επιταχύνοντας τη διαδικασία διερεύνησης. Η ανάλυση του Kuiper παρέχει στις ομάδες ασφαλείας άμεσα πληροφορίες σχετικά με δυνητικά κακόβουλη δραστηριότητα, όπως ασυνήθιστες συνδέσεις, ύποπτη δραστηριότητα διεργασιών ή τροποποιήσεις μητρώου. Η ενσωμάτωση του Wazuh σε αυτή την περίπτωση, επιτρέπει τη συγκέντρωση αυτών των αναλυμένων αντικειμένων και των πληροφοριών για περαιτέρω ανάλυση, με την χρήση αποκωδικοποιητών και ruleset επί των αρχείων καταγραφής που έχουν δημιουργηθεί από το Kuiper.

Shuffle : Το Shuffle επιτρέπει την αυτοματοποίηση διαδικασιών διαχείρισης κυβερνοεπιθέσεων . Με το εύχρηστο γραφικό περιβάλλον που διαθέτει , το ευρύ φάσμα

εργαλείων κυβερνοασφάλειας που έχει ενσωματώσει και την δυνατότητα που παρέχει για την υλοποίηση πολλαπλών παράλληλων Workflows, κρίνεται απαραίτητο για την αποτελεσματική και έγκυρη αντιμετώπιση είτε περιστατικών ρουτίνας, είτε πιο σύνθετων προβλημάτων. Στην συγκεκριμένη περίπτωση το Shuffle έχει επικοινωνεί με το Wazuh, Velociraptor και Mattermost, έτσι ώστε όταν δημιουργηθεί ένα συγκεκριμένο alert, να σταλεί ειδική ειδοποίηση στο Mattermost, και αν θεωρηθεί απαραίτητο από τους αναλυτές, μέσω του Mattermost σε πραγματικό χρόνο, να ενεργοποιηθεί διαδικασία emergency (το Velociraptor συλλέγει άμεσα συγκεκριμένα artifacts από τον client που δημιούργησε την ειδοποίηση).

Συμπερασματικά, στο παρόν κεφάλαιο περιεγράφηκαν λεπτομερώς τα εργαλεία που απαρτίζουν την πλατφόρμα διαχείρισης κυβερνοεπιθέσεων που αναπτύχθηκε. Με τη διασύνδεση εξειδικευμένων εργαλείων όπως τα IRIS DFIR, Wazuh, Cortex, Cyberchef , Suricata, MISP, Shuffle και Mattermost η πλατφόρμα αυτή παρέχει ένα συνεκτικό πλαίσιο για συνεργατική διαχείριση περιστατικών κυβερνοασφάλειας. Κάθε εργαλείο παρέχει μοναδικές λειτουργίες - από την ανάλυση κακόβουλου λογισμικού έως την παρακολούθηση σε πραγματικό χρόνο, την ανταλλαγή πληροφοριών σχετικά με απειλές και την αυτοματοποίηση. Με αυτές τις ενοποιήσεις, οι οργανισμοί μπορούν να διαχειρίζονται και να ανταποκρίνονται αποτελεσματικότερα σε περιστατικά ασφαλείας, επιτυγχάνοντας ισχυρή ανθεκτικότητα απέναντι στις απειλές και διασφαλίζοντας τη συμμόρφωση με τα κανονιστικά πρότυπα.

4. Υλοποίηση Πλατφόρμας

Στο παρόν κεφάλαιο θα παρουσιαστεί αρχικά το πλαίσιο και οι συνθήκες που απαιτήθηκαν για να αναπτυχθεί η πλατφόρμα που περιεγράφηκε στο προηγούμενο κεφάλαιο και στην συνέχεια θα αναλυθεί λεπτομερώς η διαδικασία υλοποίησης της πλατφόρμας.

4.1 Χαρακτηριστικά πλαισίου ανάπτυξης πλατφόρμας :

Η διαμόρφωση του υλικού που ήταν διαθέσιμη για την ανάπτυξή της πλατφόρμας διαδραμάτισε καθοριστικό ρόλο στις επιλογές ρυθμίσεων, καθώς είχε περιορισμούς πόρων. Με τη χρήση 16 GB μνήμης DDR5 SDRAM 2667 MHz, υποστηρίχθηκαν όλα τα εργαλεία που απαρτίζουν την πλατφόρμα, πληρώντας όμως αναγκαστικά μόνο τις ελάχιστες απαιτήσεις. Ο τετραπύρηνος επεξεργαστής AMD Ryzen 7 3750H που χρησιμοποιήθηκε, με ενσωματωμένα γραφικά Radeon Vega Mobile Graphics, ανταποκρίθηκε πλήρως στις απαιτήσεις τις πλατφόρμας, και η ενσωμάτωση της GPU NVIDIA GeForce GTX 1650 επέτρεψε την πραγματοποίηση παράλληλης επεξεργασίας με επιτάχυνση GPU. Ο αποθηκευτικός χώρος 512 GB με την χρήση 512 GB PCIe NVMe M.2 SSD ήταν επαρκής για την ανάπτυξη της πλατφόρμας και ανταποκρινόταν στις απαιτήσεις ταχύτητας.

Από την πλευρά του λογισμικού, η διαμόρφωση αυτού του περιβάλλοντος απαιτούσε τη ρύθμιση βασικών στοιχείων για την ανάπτυξη των εφαρμογών. Απαιτήθηκε η ενεργοποίηση του Windows Hypervisor Platform και του WSL (Windows Subsystem for Linux - Υποσύστημα Windows για Linux) εισήγαγε δυνατότητες εικονικοποίησης (virtualization) των Windows, επιτρέποντας την εγκατάσταση και την χρήση διανομές Linux παράλληλα με τα Windows. Η εγκατάσταση του Ubuntu 22.04 LTS μέσω του WSL ήταν απαραίτητη ώστε να είναι εφικτή η υποστήριξη εργαλείων ανοικτού κώδικα και εφαρμογών σε απομονωμένο περιβάλλον (container). Στη συνέχεια, το σύστημα Docker για τη διαχείριση containers εγκαταστάθηκε σε αυτή την διανομή Ubuntu, επιτρέποντας την ανάπτυξη containerized εφαρμογών και την αρθρωτή διαχείριση των εργαλείων ασφαλείας. Το Docker [22] είναι μια πλατφόρμα λογισμικού που επιτρέπει την δημιουργία, την δοκιμή και την ανάπτυξη εφαρμογών. Το Docker περικλείει το λογισμικό σε τυποποιημένες μονάδες που ονομάζονται και έχουν όλα όσα χρειάζεται το λογισμικό για να τρέξει, συμπεριλαμβανομένων βιβλιοθηκών, εργαλείων συστήματος, κώδικα και χρόνου εκτέλεσης. Τέλος, απαιτήθηκε η δημιουργία μίας Εικονικής Μηχανής (Virtual Machine) χρησιμοποιώντας το VirtualBox , η οποία διαθέτει λογισμικό Ubuntu 24.04 και θα χρησιμοποιηθεί ως Endpoint κατά την παρουσίαση της πλατφόρμας (demo).

4.2 Λεπτομερής παρουσίαση υλοποίησης πλατφόρμας:

Σε αυτή την ενότητα θα παρουσιαστεί η διαδικασία εγκατάστασης, η διαμόρφωση και ενσωμάτωση του εκάστοτε εργαλείου στην πλατφόρμα:

4.2.1 Iris DFIR

Το Iris αποτελεί το βασικό εργαλείο της πλατφόρμας, με το οποίο ενσωματώνονται τα υπόλοιπα εργαλεία έτσι ώστε να επαυξήσουν τις δυνατότητες του, ως Digital Forensics and Incident Response tool, και να προσδώσουν και νέες λειτουργίες, όπως XDR, IDPS κλπ, ώστε εν τέλη να διαμορφωθεί μία ολοκληρωμένη λύση, με σημείο αναφοράς το Iris. Για την εγκατάσταση του θα χρησιμοποιήσουμε την Dockerized έκδοση που παρέχεται στην επίσημη σελίδα του [26] . Για να κατεβάσουμε τοπικά το περιεχόμενο του αντίστοιχου repository [38] εκτελούμε την εντολή :

git clone https://github.com/dfir-iris/iris-web.git

Στην συνέχεια αφού μεταβούμε στον φάκελο iris-web , δημιουργούμε το .env file βάσει του env.model που περιέχει απαραίτητες μεταβλητές που χρειάζονται κατά την δημιουργία της στοίβας containers που απαιτούνται για το Iris, ως εξής :

cp .env.model .env

Έπειτα δημιουργούμε τα containers που απαιτούνται με την εντολή :

Docker-compose build

Και τα εκκινούμε :

Docker-compose up.

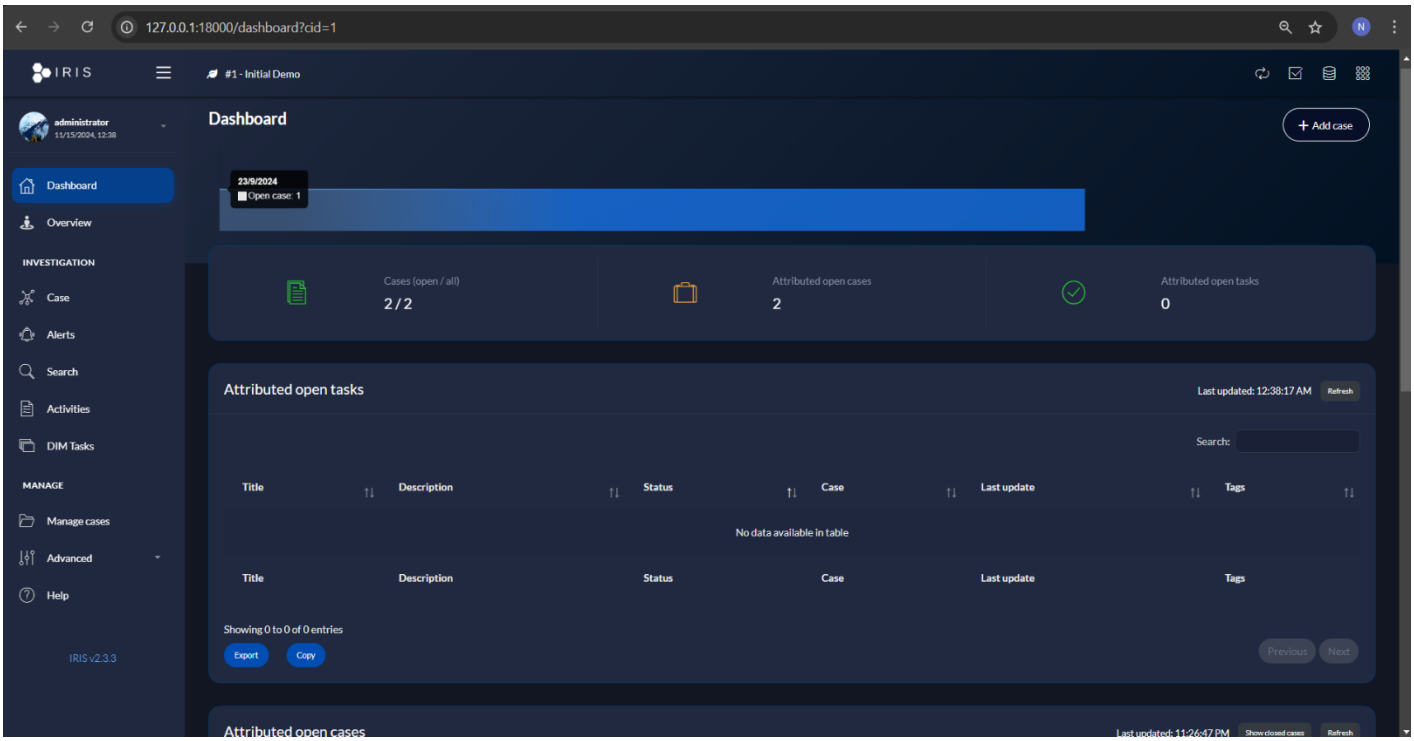
Η εντολή docker-compose χρησιμοποιεί το αρχείο docker-compose.yml. Το αρχείο docker-compose.yml είναι ένα αρχείο ρυθμίσεων που χρησιμοποιείται για τον ορισμό και τη διαχείριση εφαρμογών Docker πολλαπλών containers. Αυτό το αρχείο, γραμμένο σε γλώσσα YAML (Yet Another Markup Language), καθορίζει τον τρόπο κατασκευής και εκτέλεσης πολλαπλών Docker containers μαζί, επιτρέποντάς σας οριστούν υπηρεσίες και δίκτυα για ένα project [38].

Πλέον το Iris είναι προσβάσιμο στο url http://127.0.0.1:18000

Το προκαθορισμένο όνομα χρήστη είναι administrator , και για τον κωδικό πρόσβασης, ο οποίος εμφανίζεται μόνο την πρώτη φορά που θα εκκινηθούν τα containers του Iris, θα πρέπει να εκτελεστεί η εντολή :

docker compose logs app | grep 'admin'.

Στον κώδικα των βασικών δομών του Iris (modules , custom attributes κλπ) έχουν εκτελεστεί τροποποιήσεις, ώστε να ενσωματωθούν αρμονικά κάποια εργαλεία, τα οποία τα παρουσιαστούν αργότερα.



Εικόνα 2 Αρχικό Dashboard του Iris

Στην παραπάνω εικόνα φαίνεται το αρχικό πλαίσιο που θα εμφανιστεί στον χρήστη κατά την είσοδο του στην πλατφόρμα του Iris.

4.2.2 TheHive Cortex

Η διαδικασία εγκατάστασης του Cortex είναι παρόμοια με αυτή του Iris, καθώς χρησιμοποιεί docker containers. Συνεπώς αρχικά θα πρέπει να αποθηκεύσουμε τοπικά το περιεχόμενο του TheHive-Project / Cortex repository [24] ως εξής :

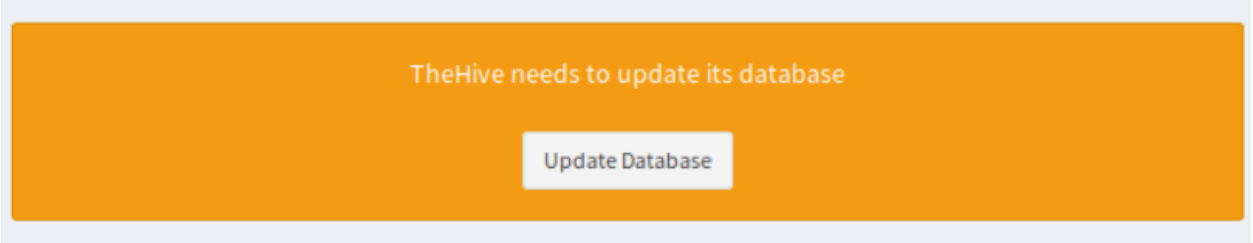
git clone https://github.com/TheHive-Project/cortex.git

Στην συνέχεια να μεταβούμε στον φάκελο cortex/docker/cortex όπου και βρίσκεται το docker-compose.yml αρχείο που θα χρησιμοποιήσουμε για την δημιουργία των containers. Έτσι αφού μεταβούμε στον φάκελο αυτό, εκτελούμε τις παρακάτω εντολές :

docker-compose build

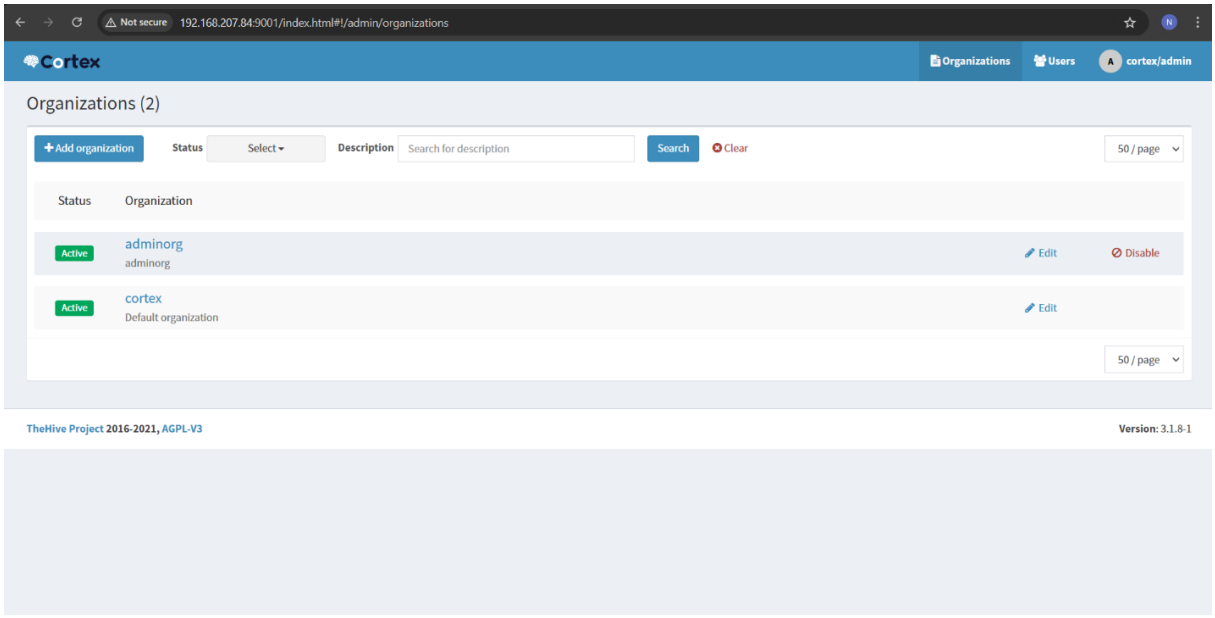
docker-compose up

Ακολούθως, θα συνδεθούμε στο web UI που βρίσκεται στο http://<ip>:9001. Καθώς το Cortex χρησιμοποιεί το ElasticSearch για να αποθηκεύει τους χρήστες του, την πρώτη φόρα που θα συνδεθούμε στο Cortex UI, θα πρέπει να δημιουργήσουμε την βάση δεδομένων, πατώντας Update Database στο παρακάτω πλαίσιο που θα εμφανιστεί :



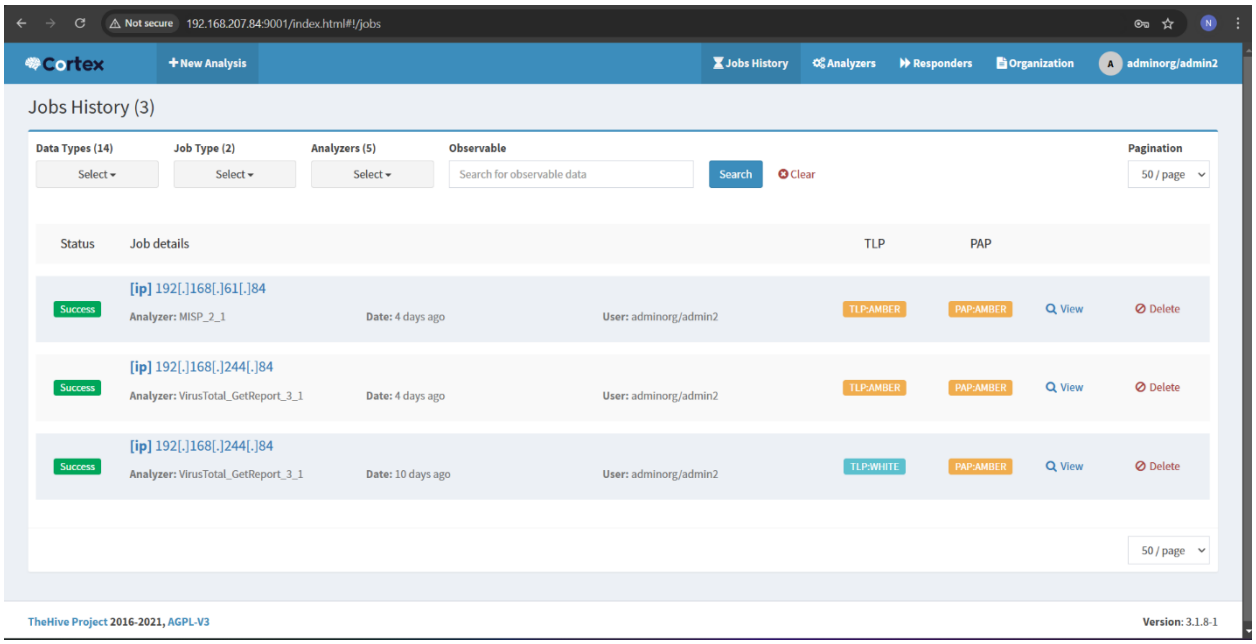
Εικόνα 3 Δημιουργία βάσης δεδομένων του Elasticsearch κατά την πρώτη σύνδεση στο Cortex.

Στην συνέχεια, αφού δημιουργηθεί η βάση, καλούμαστε να δημιουργήσουμε τον πρώτο χρήστη, ο οποίος έχει τα καθήκοντα του Super Administrator. Για να εισάγουμε τα στοιχεία του χρήστη αυτού, εμφανίζεται μία φόρμα, με Login (Username), Name και Password.Αφότου δημιουργήσουμε τον χρήστη και συνδεθούμε με τα στοιχεία που επιλέξαμε, τότε θα οδηγηθούμε στην κεντρική σελίδα του Cortex όπως φαίνεται παρακάτω :



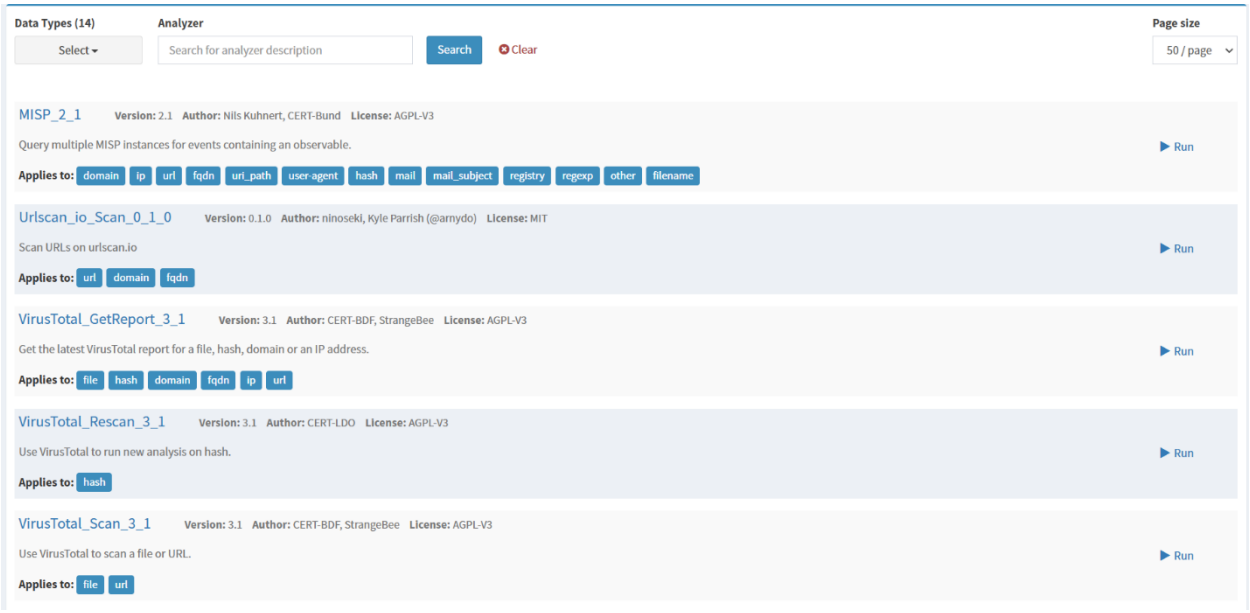
Εικόνα 4 Κεντρική σελίδα του Cortex

Για να μπορέσουμε να χρησιμοποιήσουμε τα εργαλεία ανάλυσης του Cortex, πρέπει αρχικά να δημιουργήσουμε έναν οργανισμό, και στην συνέχεια έναν χρήστη με κατάλληλα δικαιώματα σε αυτόν τον οργανισμό. Όταν δημιουργήσουμε χρήστη και ορίσουμε και σε αυτόν τα στοιχεία σύνδεσης, και δικαιώματα read, analyze, orgadmin τότε μπορούμε να συνδεθούμε ξανά ως αυτός ο χρήστης, και τότε θα έχουμε την εξής εικόνα :



Εικόνα 5 Είσοδος στο cortex με δικαιώματα read,analyze,orgadmin

Έτσι λοιπόν πλέον όπως παρατηρούμε υπάρχει η δυνατότητα έναρξης νέας ανάλυσης, αλλά και διαχείρισης των ενεργοποιημένων εργαλείων ανάλυσης και απόκρισης σε κάποιο περιστατικό. Τα εργαλεία ανάλυσης που έχουμε ενεργοποιήσει στην συγκεκριμένη περίπτωση είναι :



Εικόνα 6 Ενεργοποιημένοι αναλυτές του Cortex

Παρατηρούμε ότι διαφορετικοί αναλυτές είναι σχεδιασμένη για την διαχείριση διαφορετικών τύπων δεδομένων, για παράδειγμα, η χρήση του VirusTotal για ανάλυση μέσω του Cortex, έχει υλοποιηθεί μόνο για ανάλυση αρχείων και URL, ενώ οι δυνατότητες που παρέχονται από το MISP είναι περισσότερο εκτεταμένες, καθώς υποστηρίζει περισσότερους τύπους δεδομένων.

Συνολικά υπάρχουν διαθέσιμα 112 εργαλεία ανάλυσης και 39 εργαλεία απόκρισης. Κάθε εργαλείο απαιτεί συγκεκριμένες ρυθμίσεις να οριστούν ώστε να ενεργοποιηθεί όπως API KEY, ή απαιτούμενα πιστοποιητικά κλπ.

Στην περίπτωση που επιθυμούμε να αναλύσουμε δεδομένα που έχουμε συλλέξει, που αποτελεί την βασική λειτουργία του Cortex, τότε επιλέγοντας New Analysis που φαίνεται στην εικόνα 3 , οδηγηθούμε στο εξής πλαίσιο :

Εικόνα 7 Πλαίσιο εισαγωγής δεδομένων προς ανάλυση.

Οι βασικές παράμετροι που θα πρέπει να οριστούν είναι :

- TLP (Traffic Light Protocol) Το TLP είναι ένα πρωτόκολλο που έχει σχεδιαστεί για να διευκολύνει την ανταλλαγή ευαίσθητων πληροφοριών, με διαφορετικά επίπεδα που υποδεικνύουν τον τρόπο χειρισμού και διάδοσης των πληροφοριών. Βοηθά να διασφαλιστεί ότι οι πληροφορίες κοινοποιούνται στο κατάλληλο κοινό χωρίς να κινδυνεύει η ευρύτερη έκθεση. Οι επιλογές επιπέδων είναι White, Green, Amber και RED με σειρά αυξανόμενης ευαισθησίας πληροφοριών.
- PAP (Permissible Actions Protocol) Το PAP χρησιμοποιείται για να περιγράψει τις ενέργειες που επιτρέπονται στα δεδομένα που έχουν διαμοιραστεί, όσον αφορά το χειρισμό και τη διάδοση. Διαθέτει τα ίδια επίπεδα με το TLP.

Παραπάνω συνοψίζονται οι βασικές λειτουργίες και τα χαρακτηριστικά του Cortex. Αναφορικά με την ενσωμάτωση του στο IRIS, αυτή υλοποιήθηκε με την ανάπτυξη κώδικα javascript εντός των IOC custom attributes:

```
"Cortex": {
    "Data Type": {
        "type": "html",
        "id": "data_type",
        "mandatory": true,
        "value": "<label>Data Type</label><select id='data_type' class='selectpicker form-control' data-live-search='true' title='Select Data Type'><option value='domain'>Domain</option><option value='fqdn'>FQDN</option><option value='hash'>Hash</option><option value='ip'>ip</option><option value='other'>Other</option><option value='url'>URL</option><option value='user agent'>User Agent</option></select><script>$('#data_type').selectpicker();</script>",
        "on_change": "updateAnalyzers"
    },
```

```
"Analyzers": {
    "type": "html",
    "mandatory": true,
    "value": "<label>Available Analyzers</label><select id='selectAnalyzers' class='selectpicker form-control'></select><script src='https://cdnjs.cloudflare.com/ajax/libs/bootstrap-select/1.13.1/js/bootstrap-select.min.js'></script><script>$('#selectAnalyzers').selectpicker({liveSearch: true,title: 'Analyzer',style: 'btn-outline-white'}); $('#data_type').on('change', function () { updateAnalyzers(); }); function updateAnalyzers() { var data_type = $('#data_type').val(); $('#selectAnalyzers').empty(); fetch(`http://192.168.244.84:9001/api/analyzer/type/${data_type}`, { method: 'GET', headers: { 'Authorization': 'Bearer 1c7JkptOcl/tvNfrvlpCmxRkKMGwm6Bg' } }).then(response => { return response.json(); }).then(data => { for (let i = 0; i < data.length; i++) { $('#selectAnalyzers').append(`<option value='${data[i].id}'>${data[i].analyzerDefinitionId}</option>`); } $('#selectAnalyzers').selectpicker('refresh'); }); } updateAnalyzers(); </script>"
},
"Data Input": {
    "type": "html",
    "id": "data_input",
    "mandatory": true,
    "value": "<label>Data Input</label><select id='data_input_analyzer' class='selectpicker form-control'></select><input type='text' id='data_input' class='selectpicker form-control'><button style = 'margin-top : 18px' class='btn btn-primary' onclick='analyzeData()'>Analyze Data</button><script>var $data_input;function analyzeData() {var selectedAnalyzer = $('#selectAnalyzers').val();$data_input = document.getElementById('data_input').value;const apiKey = '1c7JkptOcl/tvNfrvlpCmxRkKMGwm6Bg';const csrf_token = '91464de230a81cbd2a171c5f525124426c07a543-1703063492103-186872a6d16ac5e888b25d4c';const cortexUrlid = `http://192.168.244.84:9001/api/analyzer/${selectedAnalyzer}/run`;const requestBody = {data: $data_input, dataType: $('#data_type').val(), tlp: 0, csrf_token: csrf_token};fetch(cortexUrlid, {method: 'POST', headers: {'Authorization': `Bearer ${apiKey}`, 'Content-Type': 'application/json', 'X-CORTEX-XSRF-TOKEN': csrf_token}, body: JSON.stringify(requestBody)}).then(response => {if (!response.ok) {throw new Error(`Request failed. Server responded with status ${response.status}: ${response.statusText}`);}return response.json();}).then(data => {console.log('Server response:', data);}).catch(error => {console.error('Error:', error.message);});}</script>"
},
"Jobs": {
    "type": "html",
    "id": "jobDropdown",
    "value": "<label>Select Job</label><select id='selectJob' class='selectpicker form-control'></select><script src='https://cdnjs.cloudflare.com/ajax/libs/bootstrap-select/1.13.1/js/bootstrap-select.min.js'></script><script>$('#selectJob').selectpicker({liveSearch: true, title: 'Job ID', style: 'btn-outline-white'}); fetchJobData(); function fetchJobData() { const apiKey = '1c7JkptOcl/tvNfrvlpCmxRkKMGwm6Bg'; fetch('http://192.168.244.84:9001/api/job', { method: 'GET', headers: { 'Authorization': `Bearer ${apiKey}` } }) .then(response =>
```

response.json()) .then(data => { for (let i = 0; i < data.length; i++) { $('#selectJob').append(`<option value='${data[i]._id}'>${data[i]._id} -${data[i].data}-${data[i].status}</option>`); } $('#selectJob').selectpicker('refresh'); }) .catch(error => { console.error('Error fetching job data:', error.message); }); }</script>"

},

"ViewJobResults": {

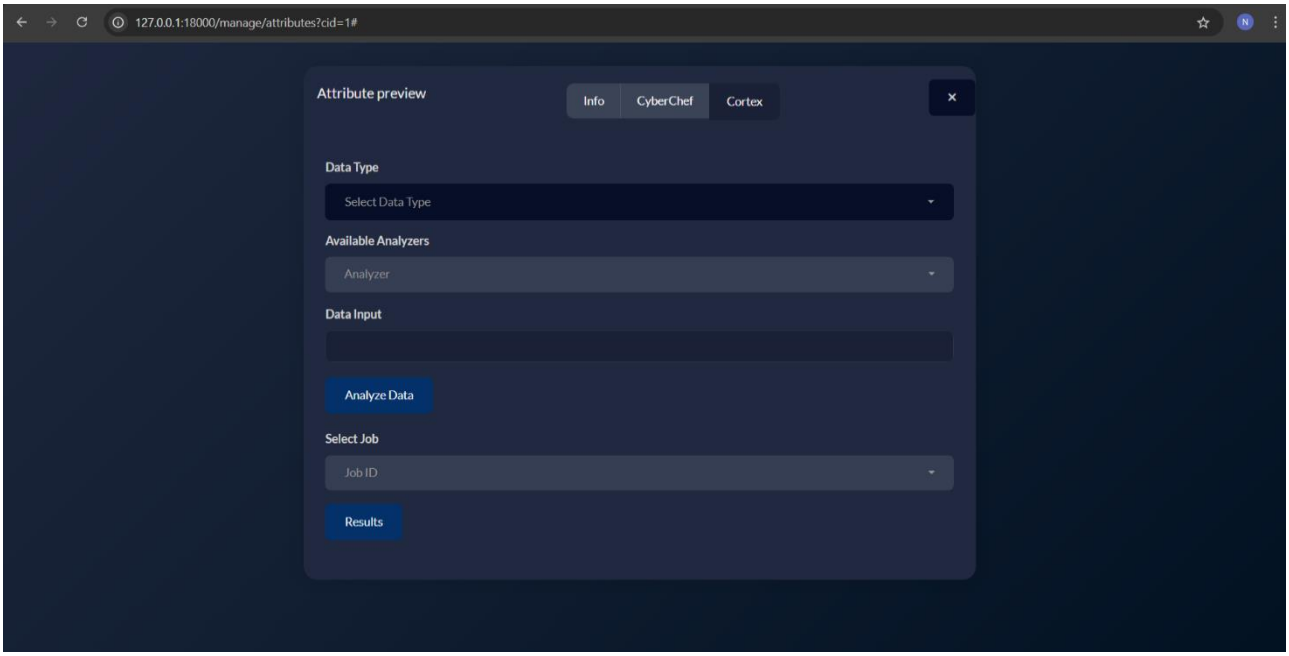
"type": "html",

"id": "viewJobResults",

"value": "<button id='testButton' class='btn btn-primary'>Results</button><div id='testModal' style='display: none; position: fixed; top: 50%; left: 50%; transform: translate(-50%, -50%); background-color: #30163d; padding: 20px; color: white; border: 1px solid #ccc; border-radius: 5px; max-width: calc(100vw - 200px); max-height: calc(100vh - 200px);'> <button id='closeButton' style='background: none; border: none; cursor: pointer;'>X</button> <h2>Job ID</h2> Selected Job ID: <pre id='jobResults' style='white-space: pre-wrap; max-height: 150px; overflow-y: auto;'></pre><script>document.getElementById('testButton').addEventListener('click', openTestModal); document.getElementById('closeButton').addEventListener('click', closeTestModal); function openTestModal() { document.getElementById('testModal').style.display = 'block'; document.getElementById('selectedJobID').innerText = $('#selectJob').val(); const apiKey = '1c7JkptOcl/tvNfrvlpCmxRkKMGwm6Bg'; const JobID = $('#selectJob').val(); const cortexUrljob = `http://192.168.244.84:9001/api/job/${JobID}/waitreport?atMost=5minute`; fetch(cortexUrljob, { method: 'GET', headers: { 'Authorization': `Bearer ${apiKey}` } }) .then(response => { if (!response.ok) { throw new Error(`Request failed. Server responded with status ${response.status}: ${response.statusText}`); } return response.json(); }) .then(data => { document.getElementById('jobResults').innerText = JSON.stringify(data, null, 2); }) .catch(error => { console.error('Error:', error.message); }); } function closeTestModal() { document.getElementById('testModal').style.display = 'none'; } </script> "

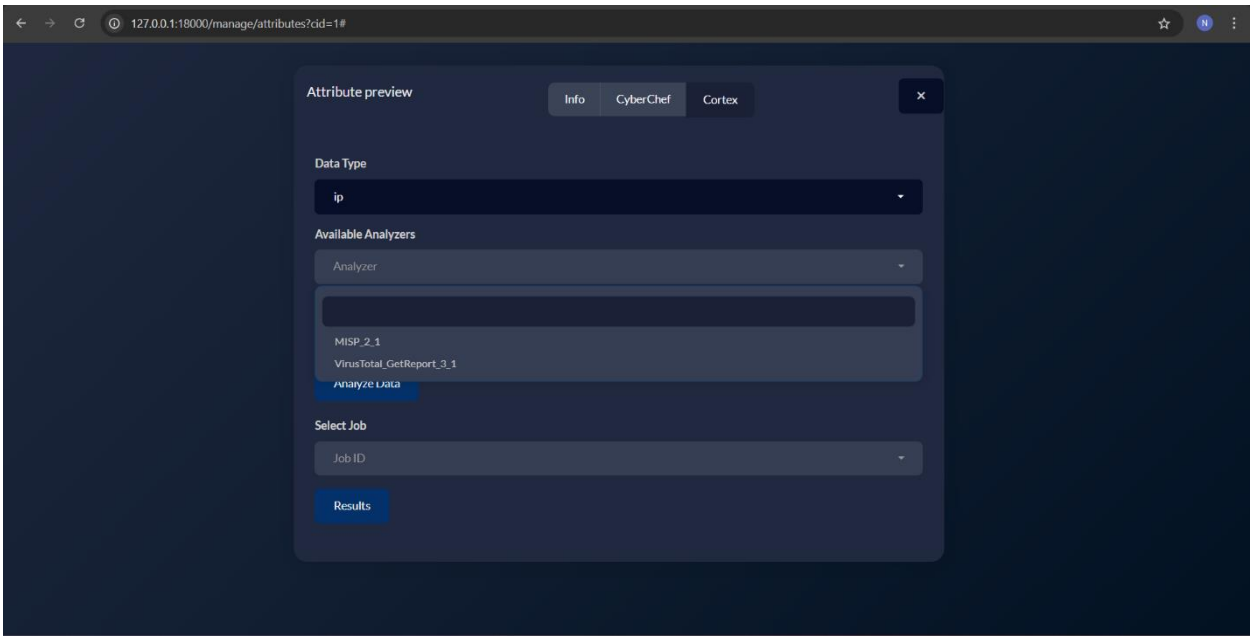
}

Ο παραπάνω κώδικας δημιουργεί το ακόλουθο πλαίσιο:



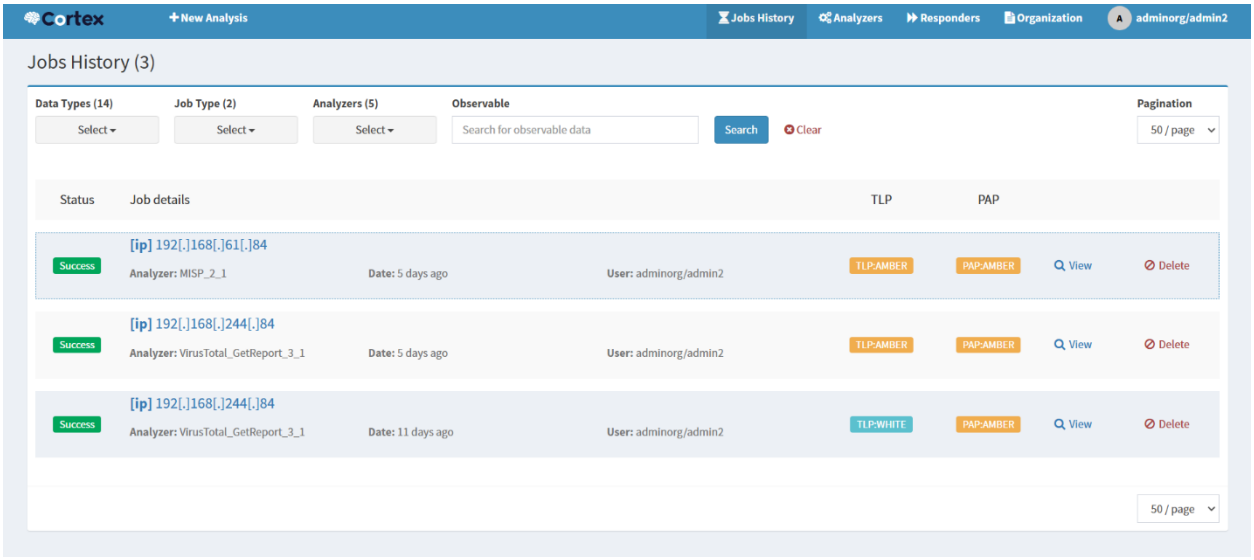
Εικόνα 8 Διεπαφή χρήσης αναλυτών του Cortex στο Iris.

Αρχικά, θα πρέπει να ορίσουμε τον τύπο δεδομένων που επιθυμούμε να αναλύσουμε, στο πεδίο Data Type. Ανάλογα με τον τύπο που θα επιλέξουμε, θα εμφανιστούν και τα κατάλληλα εργαλεία ανάλυσης.



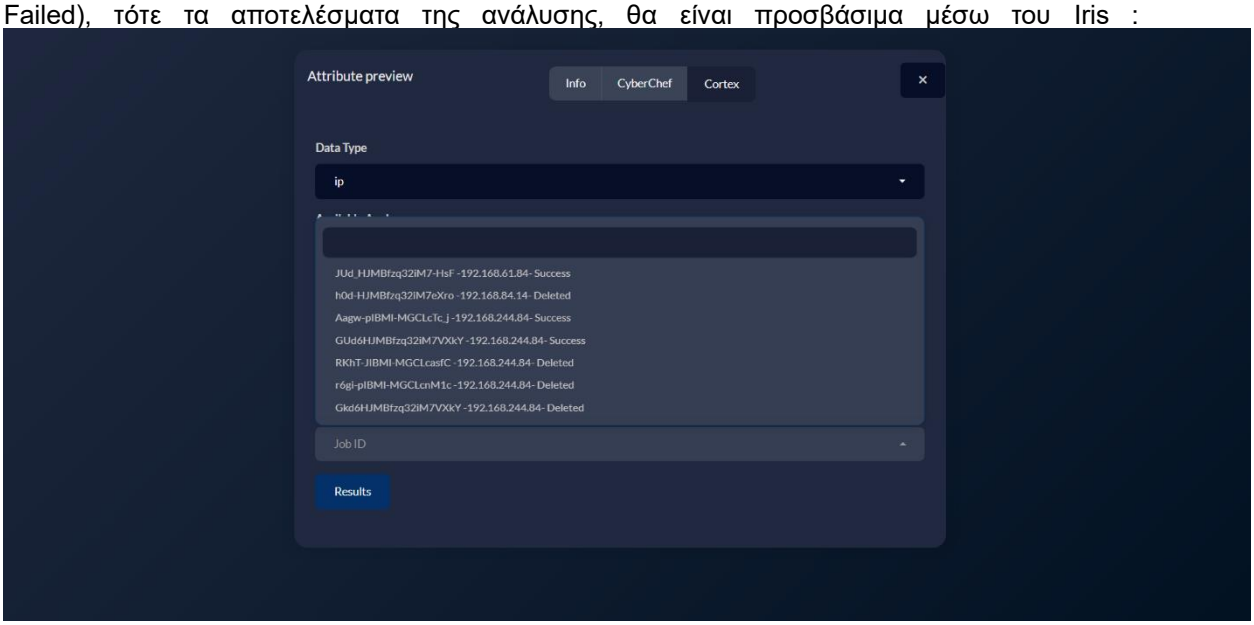
Εικόνα 9 Επιλογή εργαλείου ανάλυσης

Στην συγκεκριμένη περίπτωση επιλέξαμε να αναλύσουμε δεδομένα τύπου ip, και τα διαθέσιμα εργαλεία είναι το MISP και VirusTotal. Αφού επιλέξουμε εργαλείο τότε εισάγουμε την ip που επιθυμούμε στο πεδίο Data Type, και μετά πραγματοποιούμε την ανάλυση. Η ανάλυση της ip θα εμφανιστεί ως εργασία στο Cortex όπως φαίνεται παρακάτω :



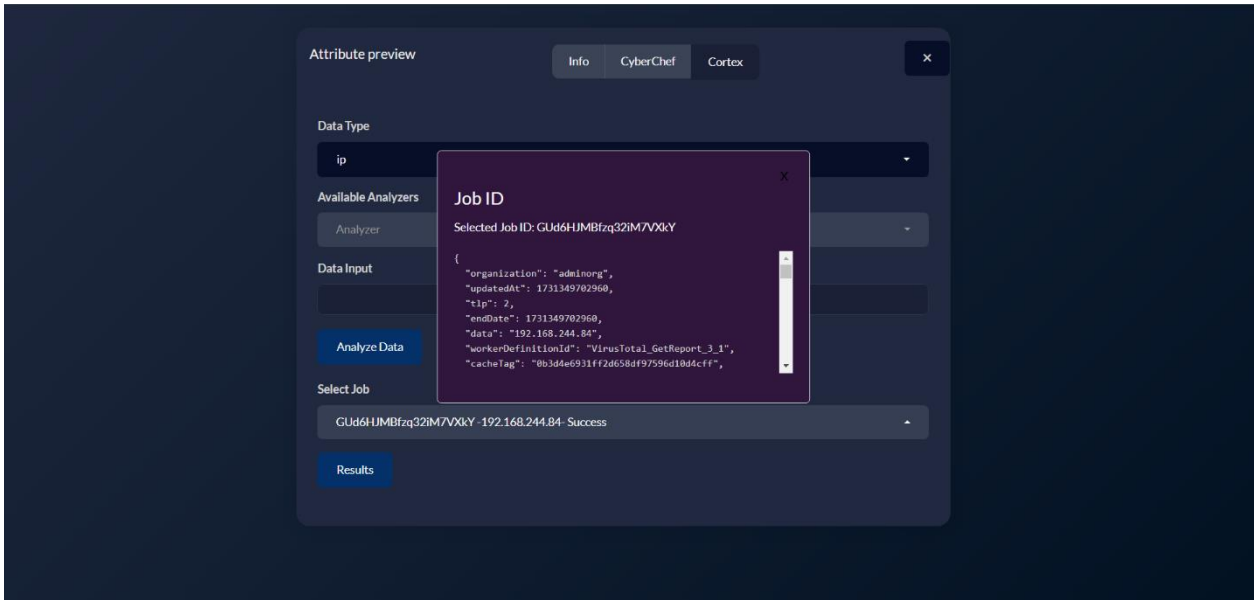
Εικόνα 10 Εμφάνιση ανάλυσης στο Cortex

Όταν ολοκληρωθεί (δηλαδή η κατάστασή της μεταβληθεί από InProgress σε Success ή Failed), τότε τα αποτελέσματα της ανάλυσης, θα είναι προσβάσιμα μέσω του Iris :



Εικόνα 11 Επιλογή ανάλυσης προς εμφάνιση αποτελεσμάτων

Μπορούμε να επιλέξουμε την ανάλυση που επιθυμούμε καθώς όπως φαίνεται διατηρείται ιστορικό αναλύσεων, και να προβάλουμε τα αποτελέσματά της :



Εικόνα 12 Αποτελέσματα επιλεγμένης ανάλυσης.

Η παραπάνω υλοποίηση διευρύνει τις δυνατότητες και τις επιλογές που παρέχονται για την χρήση του cortex μέσω του Iris , καθώς του επιτρέπει διαδραστικά να επιλέξει εργαλείο ανάλυσης ανάλογα με τον τύπο δεδομένων που επιθυμεί να εξετάσει, και να λάβει άμεσα τα αποτελέσματα της ανάλυσης μετά το πέρας αυτής.

4.2.3 Malware Sharing Information Platform (MISP)

Η διαδικασία εγκατάστασης του MISP ακολουθεί την ίδια τακτική με τα προηγούμενα εργαλεία. Θα κατεβάσουμε το περιέχομενο του αντίστοιχου github repository [28] :

git clone https://github.com/coolacid/docker-misp.git

Έπειτα θα μεταβούμε στον φάκελο docker-misp, θα δημιουργήσουμε και θα εκκινήσουμε τα αντίστοιχα containers που απαρτίζουν το compose stack του MISP, ως εξής :

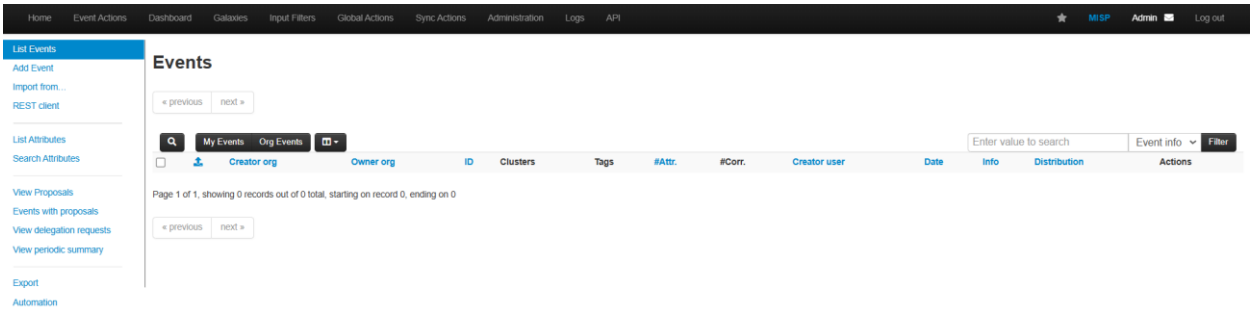
docker-compose build

docker-compose up

Το MISP είναι διαθέσιμο στο port 443 , οπότε θα μεταβούμε στο url : https://localhost . Τα προεπιλεγμένα στοιχεία σύνδεσης είναι

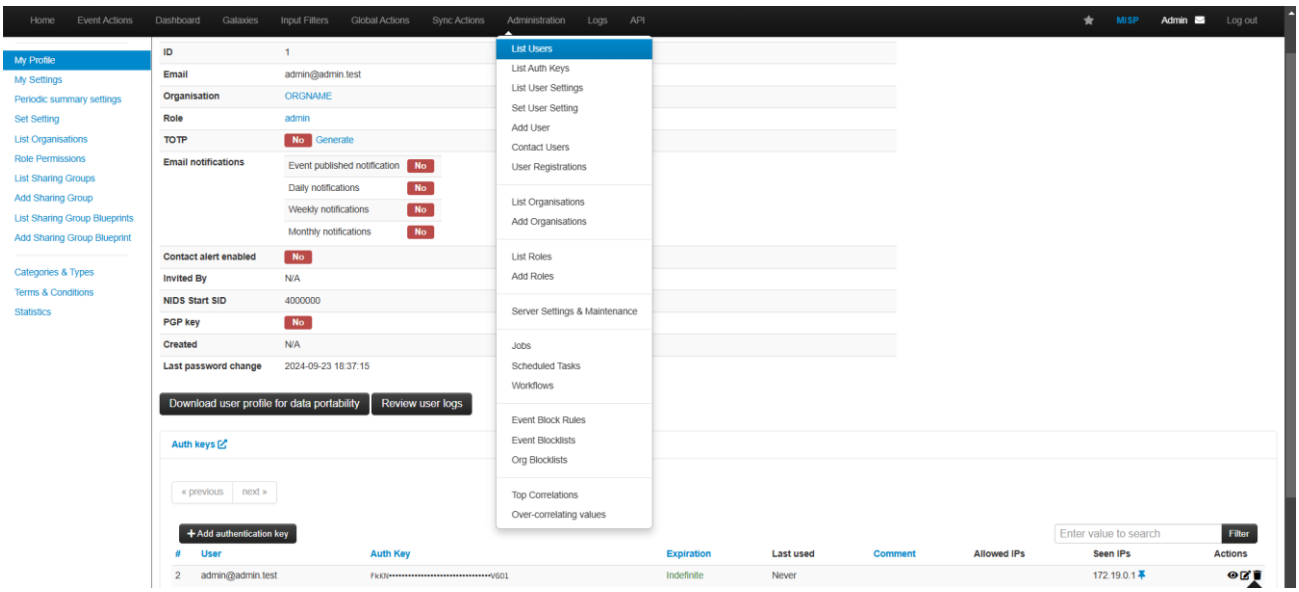
- Όνομα χρήστη : admin@admin.test
- Κωδικός πρόσβασης : admin

Αφού συνδεθεί ο χρήστης, θα μεταβεί στην αρχική σελίδα του MISP :



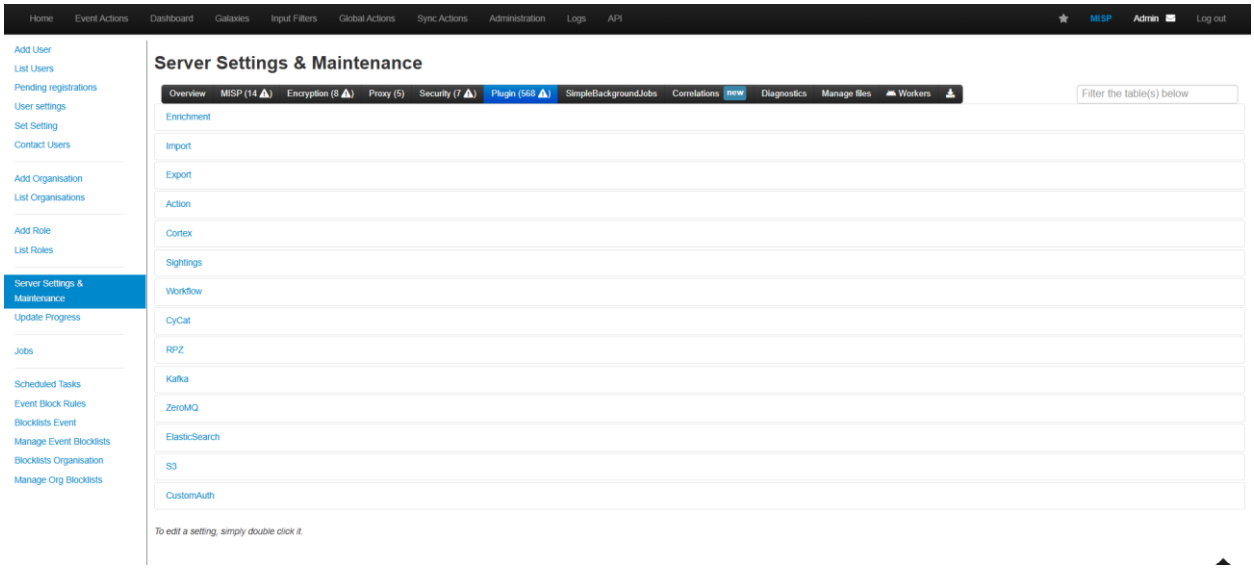
Εικόνα 13 Αρχική σελίδα του MISP

Για να μπορέσουμε να υλοποιήσουμε ενσωμάτωση του MISP με οποιοδήποτε εργαλείο, θα πρέπει αρχικά να δημιουργήσουμε API Key για τον χρήστη. Με αυτόν τον σκοπό, θα μεταβούμε στο προφίλ του χρήστη και υπό το πεδίο Auth Keys, θα επιλέξουμε την προσθήκη API Key :

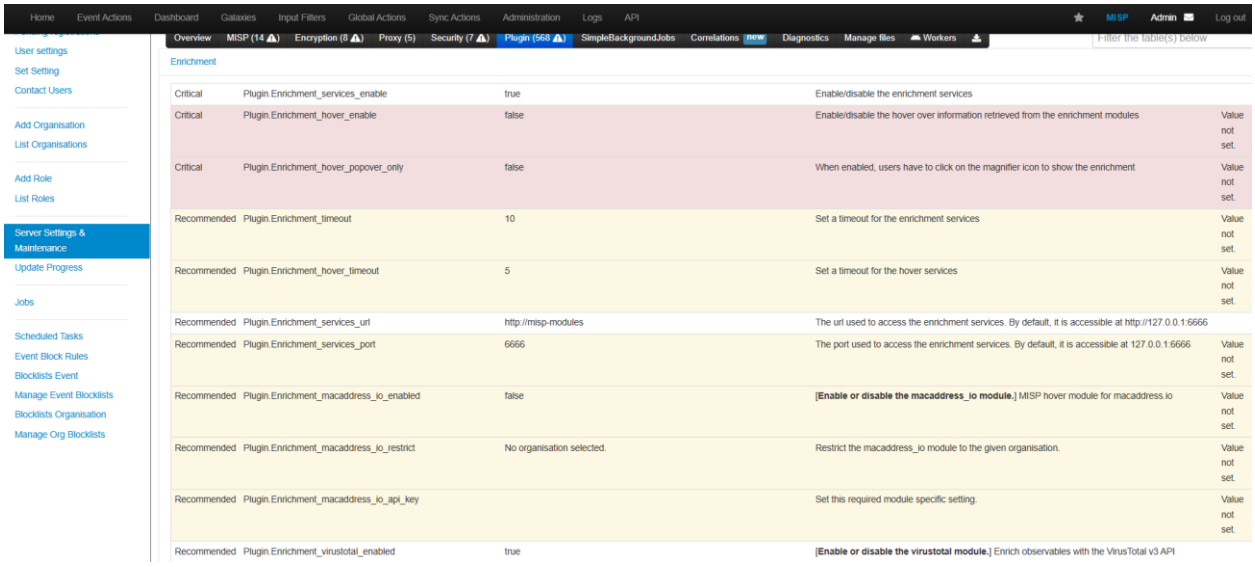


Εικόνα 14 Δημιουργία API key στο MISP

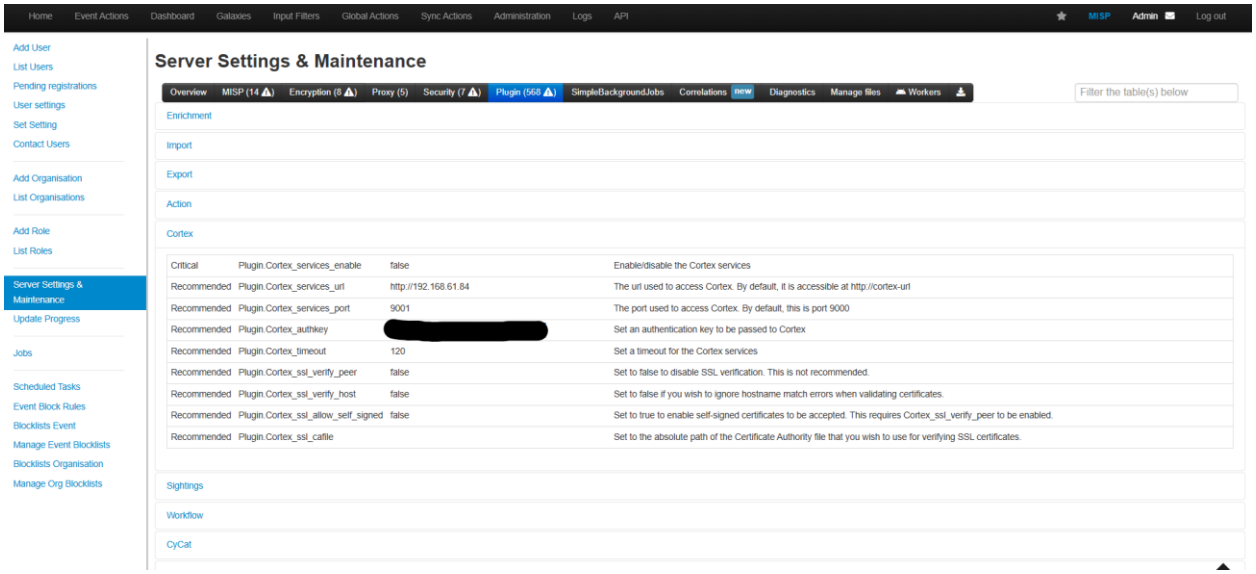
Στην συνέχεια θα ενεργοποιήσουμε plugins τα οποία επιτρέπουν την ενσώματωση επιπλέον εργαλείων ανάλυσης στο MISP και τον περαιτέρω εμπλουτισμό των δεδομένων του. Το MISP διαθέτει συνολικά 568 plugins. Σε αυτή την περίπτωση θα ενεργοποιήσουμε το virustotal από τα enrichment plugins, και το cortex, όπως φαίνεται παρακάτω :



Εικόνα 15 Επεκτάσεις λειτουργικότητας του MISP



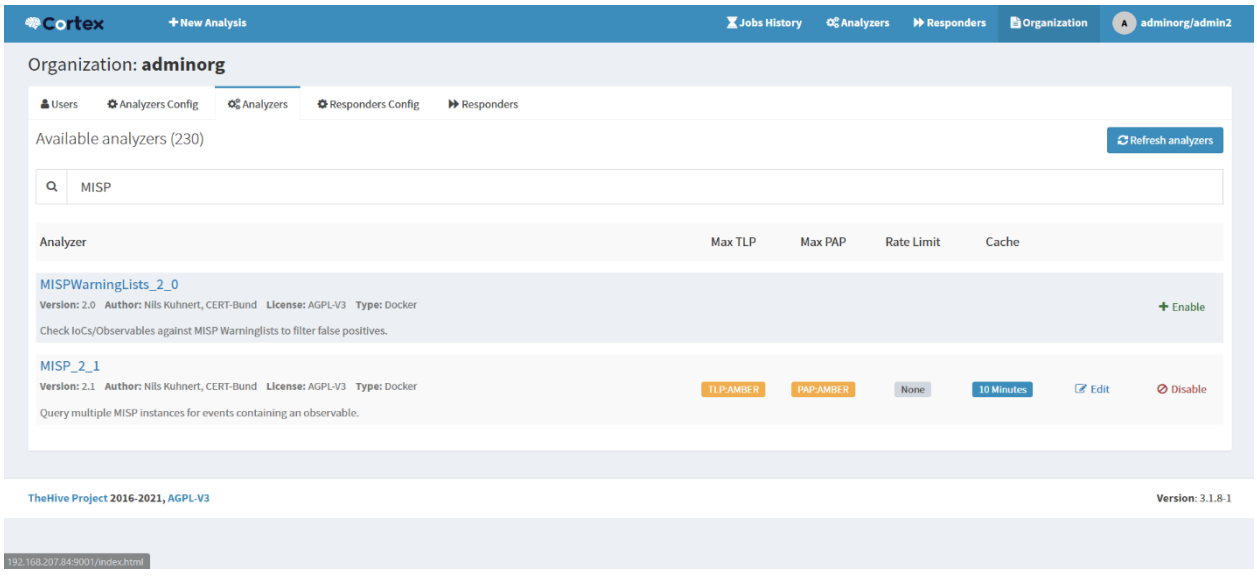
Εικόνα 16 Ενεργοποίηση επέκτασης χρήσης του VirusTotal μέσω του MISP



Εικόνα 17 Ενεργοποίηση επέκτασης χρήσης του Cortex μέσω του MISP

Όπως περιγράφεται και στο σχεδιάγραμμα ροής πληροφοριών και δεδομένων της πλατφόρμας, η επικοινωνία Cortex-MISP είναι αμφίρροπη. Στην εικόνα 16 πραγματοποιείται η σύνδεση του MISP με το Cortex, ώστε να επιτραπεί η χρήση των εργαλείων ανάλυσης του Cortex, για επαύξηση και συμπλήρωση των πληροφοριών που διαθέτει το MISP για κάποιο Observable.

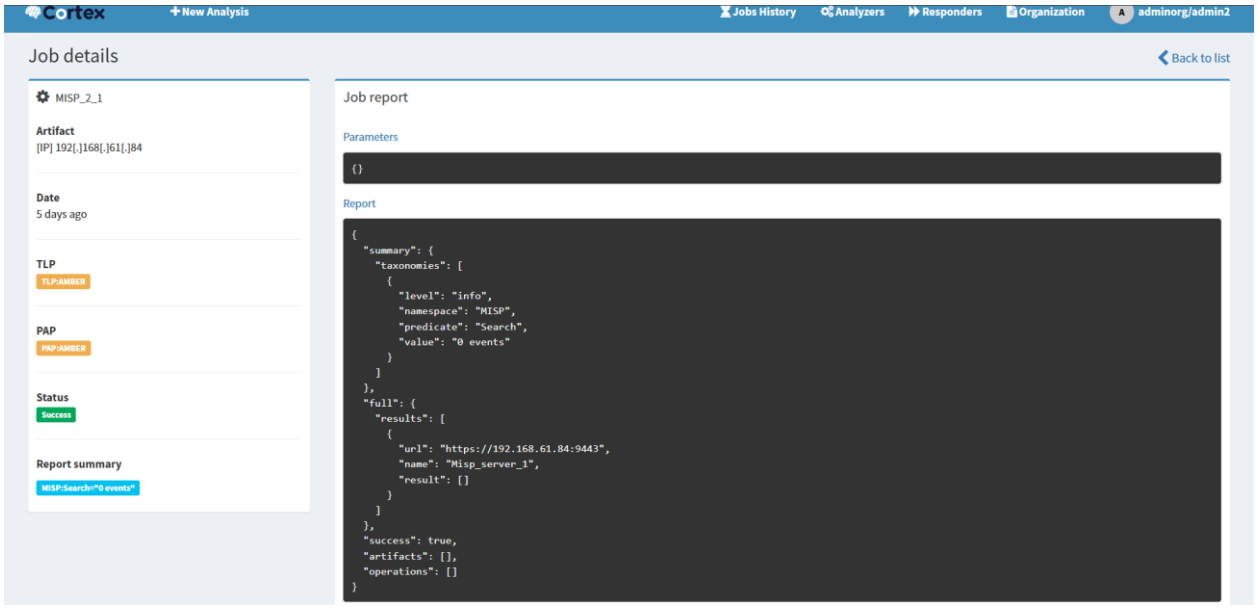
Από την άλλη πλευρά, όπως παρουσιάστηκε και προηγουμένως, είναι εφικτός ο εμπλουτισμός των δεδομένων ενός observable από τη βάση δεδομένων του MISP, μέσω του Cortex. Στο Cortex έως τώρα έχουν αναπτυχθεί δύο τρόποι διασύνδεσης του MISP (δύο flavors του MISP).



Εικόνα 18 Επεκτάσεις του MISP εντός του Cortex.

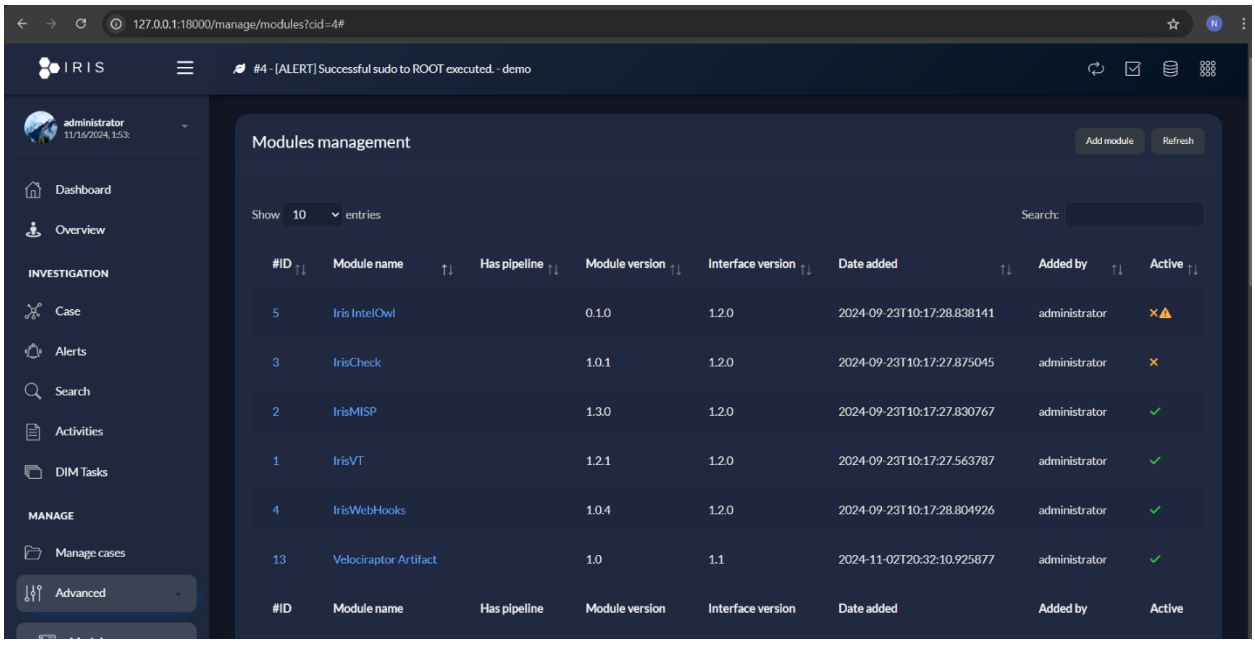
Όπως φαίνεται παραπάνω (εικόνα 16) υπάρχει δυνατότητα ερώτησης την βάσης δεδομένων του MISP για την εύρεση events που περιέχουν το συγκεκριμένο στοιχείο, και σύγκριση του στοιχείου αυτού με την MISP Warniglist για να αποκλειστούν τα ψευδώς θετικά περιστατικά.

Χρησιμοποιώντας το MISP μέσω του Cortex, για την αναζήτηση μίας ip για πάραδειγμα, θα λάβουμε αναφορά της ακόλουθης μορφής :



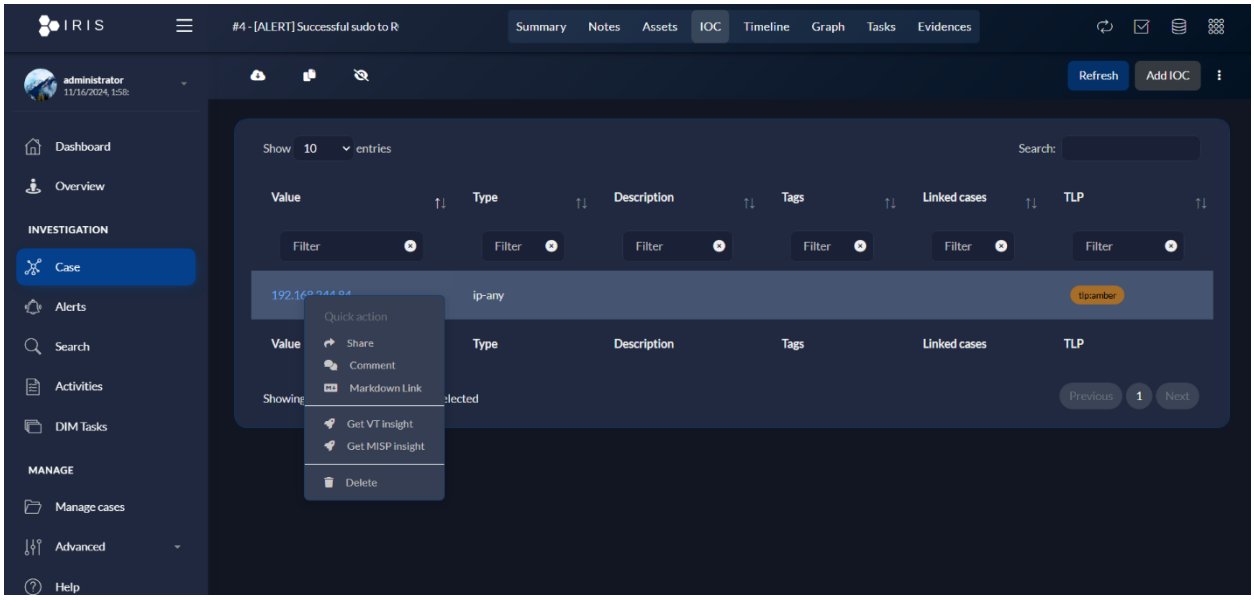
Εικόνα 19 Αναφορά αναζήτησης στοιχείου στην βάση του MISP

Τέλος, το MISP ενσωματώνεται και στο Iris, μέσω του προσαρμοσμένου module που υπάρχει :



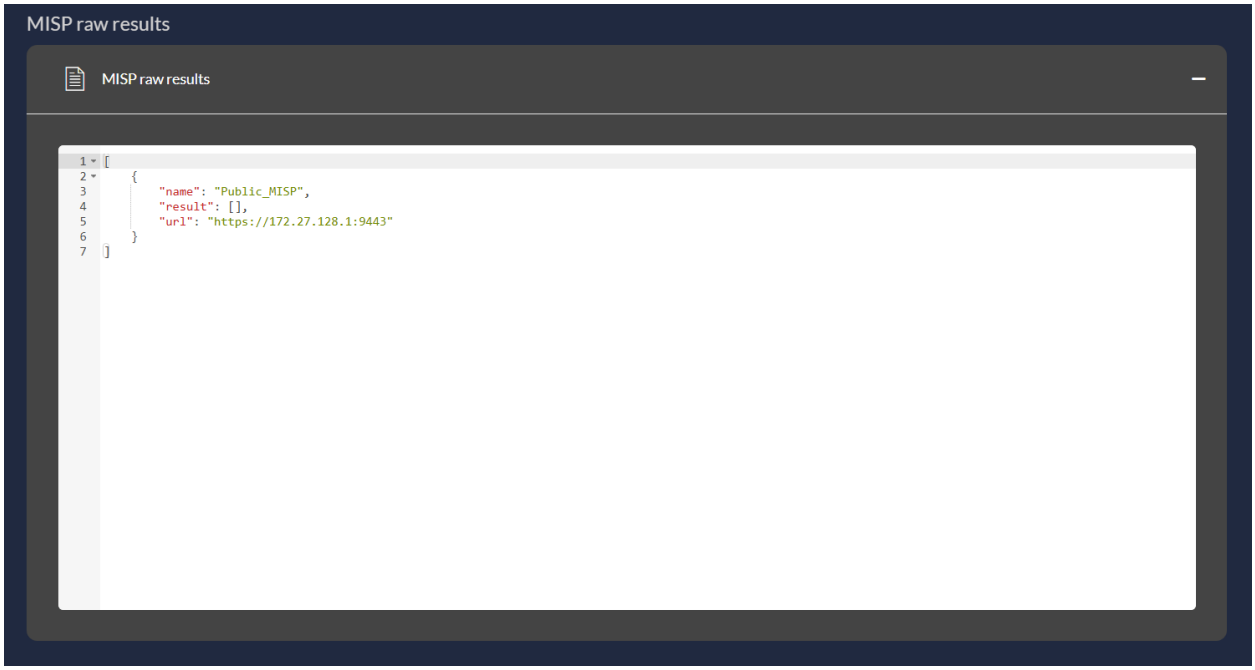
Εικόνα 20 MISP module στο IRIS

Για την επιτυχή επικοινωνία, αρκεί να ορίσουμε το url του MISP και το API key που δημιουργήσαμε προηγουμένως. Τότε, θα μπορούμε να λαμβάνουμε δεδομένα του MISP σχετικά με το IOC του IRIS, που επιλέγουμε :



Εικόνα 21 Εμπλουτισμός των δεδομένων ενός IOC του IRIS με την χρήση του MISP

Η αναφορά του MISP που θα λάβουμε θα είναι της μορφής :



Εικόνα 22 Αναφορά MISP εντός του IRIS.

4.2.4 Cyberchef

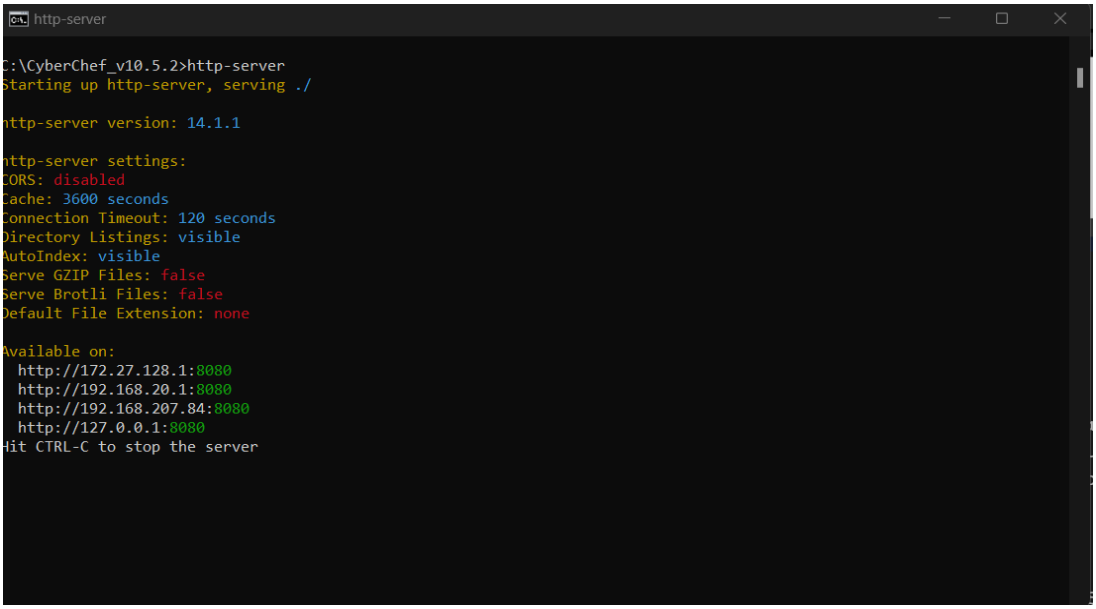
Σε αυτή την περίπτωση δεν ακολουθείται η ίδια διαδικασία με τα προηγούμενα 3 εργαλεία. Θα χρησιμοποιήσουμε http server στο port 8080. Αρχικά θα πρέπει να εγκαταστήσουμε το

περιβάλλον Node.js [41] και στην συνέχεια θα εγκαταστήσουμε το απαραίτητο πακέτο http-server ως εξής :

npm install -g http-server

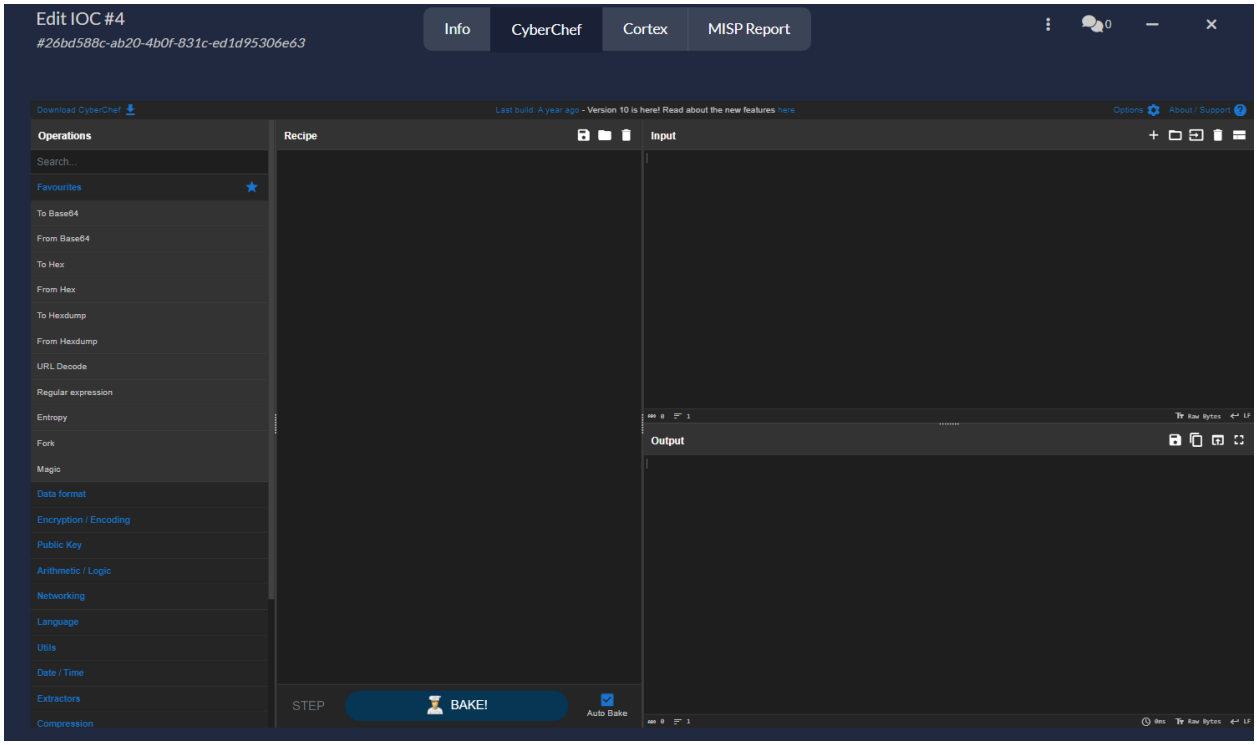
αφού εγκατασταθεί, τότε θα μεταβούμε στο Cyberchef [42] και στο τερματικό θα τρέξουμε την εντολή :

http-server



Εικόνα 23 ΄Εναρξη του http server του CyberChef.

Το CyberChef έχει ενσωματωθεί στο IRIS με κατάλληλο τρόπο ώστε ο χρήστης να μπορεί να αξιοποιήσει πλήρως τις απεριόριστες δυνατότητες του επεξεργασίας, μετατροπής δεδομένων που παρέχει. Οπότε παρέχεται το εξής περιβάλλον στον χρήστη :



Εικόνα 24 Χρήση του CyberChef εντός του IRIS

Το Cyberchef έχει ενσωματωθεί ώστε να είναι προσβάσιμο εύκολα από τα δεδομένα ενός IOC,ώστε ο αναλυτής να μεταφέρει τα δεδομένα του άμεσα στο πλαίσιο του CyberChef και να τα επεξεργάζεται.

Η παραπάνω λειτουργία επιτυγχάνεται με την προσθήκη του CyberChef ως Custom Attribute των IOCs του IRIS , ομοίως με την ενσωμάτωση του Cortex :

```
"CyberChef": {
    "Iframe": {
        "type": "html",
        "value": "<iframe src='http://127.0.0.1:8080/CyberChef_v10.5.2.html' width='170%' height='1000px' frameborder='0' style='transform: scale(0.6); transform-origin: 0 0; overflow-x: scroll;'></iframe>"
    }
}
```

4.2.5 Mattermost

Για την εφαρμογή Mattermost θα χρησιμοποιηθούν docker containers. Αρχικά θα κατεβάσουμε τα απαραίτητα αρχεία :

git clone https://github.com/mattermost/docker

και θα δημιουργήσουμε το αρχείο .env με τις μεταβλητές περιβάλλοντος, βάσει του env.example:

cp env.example .env

Στο αρχείο .env , θα πρέπει να τροποποιήσουμε το Domain Name και MATTERMOST_IMAGE σε mattermost-team-edition.

Στην συνέχεια θα δημιουργήσουμε τους παρακάτω φακέλους, και θα θέσουμε τις άδειες τους, όπως περιγράφεται στον οδηγό εγκατάστασης [28] :

mkdir -p ./volumes/app/mattermost/{config,data,logs,plugins,client/plugins,bleve-indexes}

sudo chown -R 2000:2000 ./volumes/app/mattermost

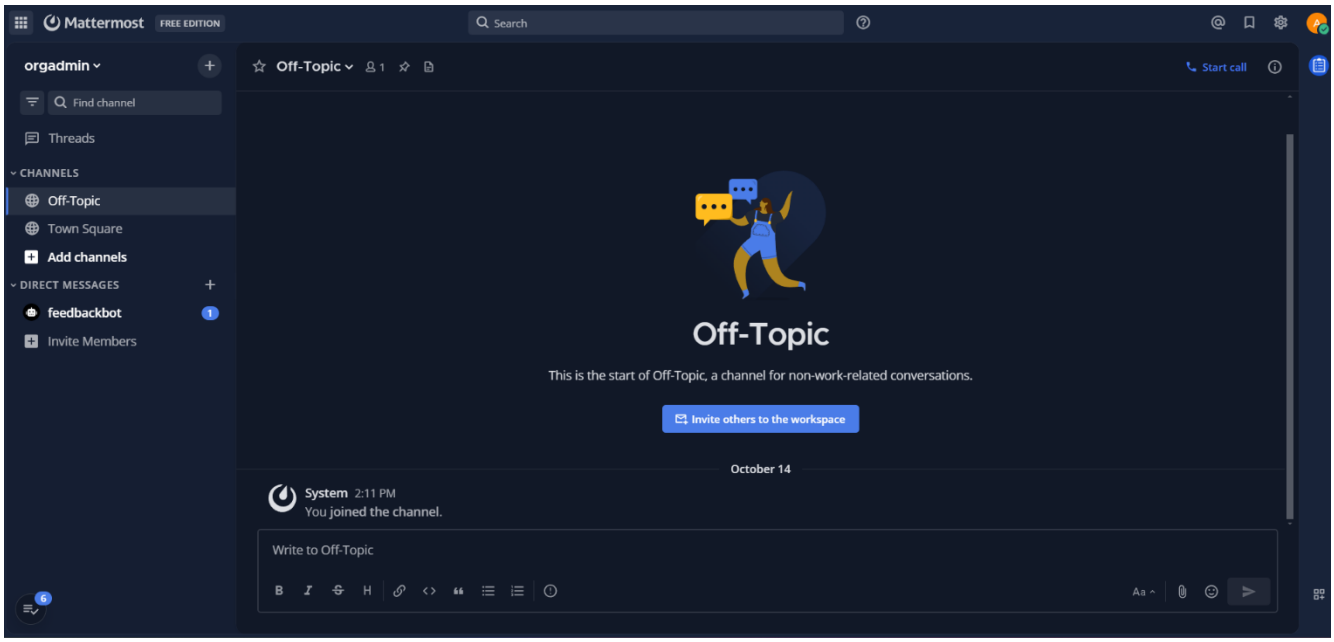
Έχοντας πραγματοποιήσει τις απαραίτητες τροποποιήσεις , πλέον μπορουμε να αναπτύξουμε το Mattermost, ως εξής :

sudo docker compose -f docker-compose.yml -f docker-compose.without-nginx.yml up -d

Σε αυτή την υλοποίηση , δεν θα χρησιμοποιήσουμε reverse proxy (nginx) οπότε το Mattermost θα είναι προσβάσιμο στο url : http://<ip>:8065

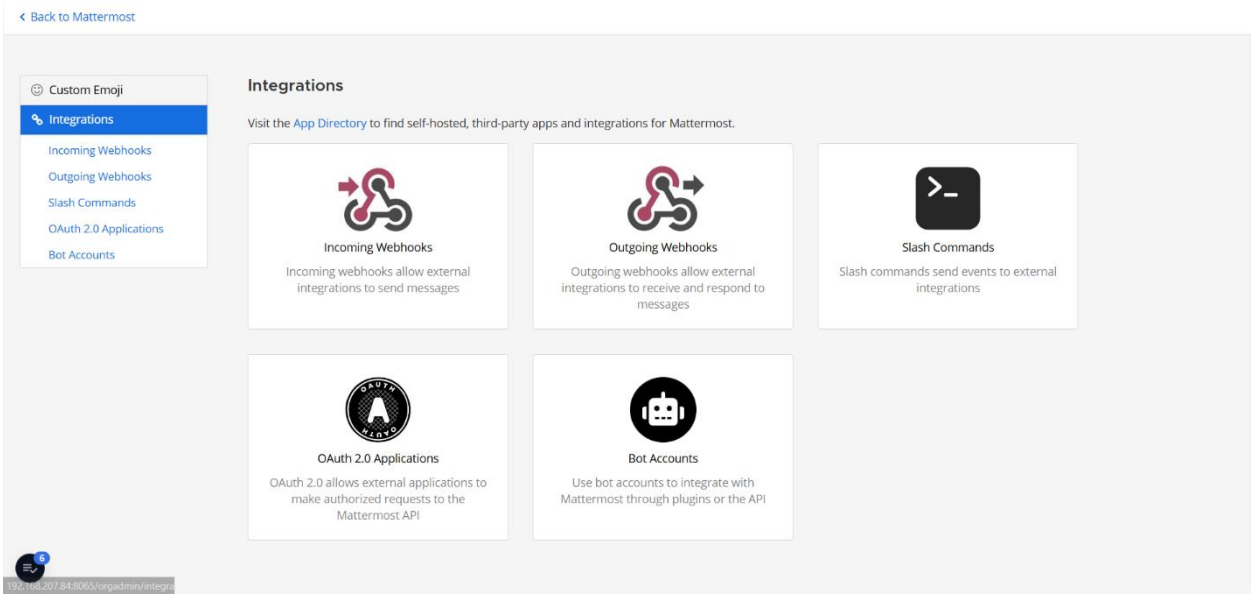
Τα στοιχεία πρόσβασης του Mattermost είναι : admin/password

Μετά την σύνδεση του, ο χρήστης θα μεταβεί στην κεντρική σελίδα, όπως φαίνεται παρακάτω :



Εικόνα 25 Κεντρική σελίδα Mattermost

Αριστερά στην κεντρική σελίδα, είναι προσβάσιμα τα διάφορα κανάλια, και μέλη των καναλιών για αποστολή μηνυμάτων. Για την υλοποίηση ενσωματώσεων, υπάρχει επιλογή ορισμού εισερχόμενων webhooks αλλά και εξερχόμενων, για την αποστολή μηνύματος όταν εκπληρωθεί κάποια συνθήκη :



Εικόνα 26 Εισερχόμενα και Εξερχόμενα Webhooks του Mattermost.

Αναφορικά με τα εισερχόμενα webhooks, για την δημιουργία τους αρκεί να οριστεί, τίτλος του webhook, περιγραφή και κανάλι που θα σταλεί το εισερχόμενο μήνυμα και μετά θα λάβουμε το αντίστοιχο url. Για παράδειγμα το url για αποστολή μηνυμάτων και εκτέλεση ενεργειών για το κανάλι Town Square είναι :

http://192.168.207.84:8065/hooks/mtnm1mosifyu9ebekxpnywajsa

Το παραπάνω URL θα χρησιμοποιηθεί για την υλοποίηση της επικοινωνίας IRIS-Mattermost. Όπως φαίνεται στην εικόνα 19, θα χρησιμοποιήσουμε το module IrisWebHooks και θα εφαρμόσουμε την εξής διαμόρφωση :

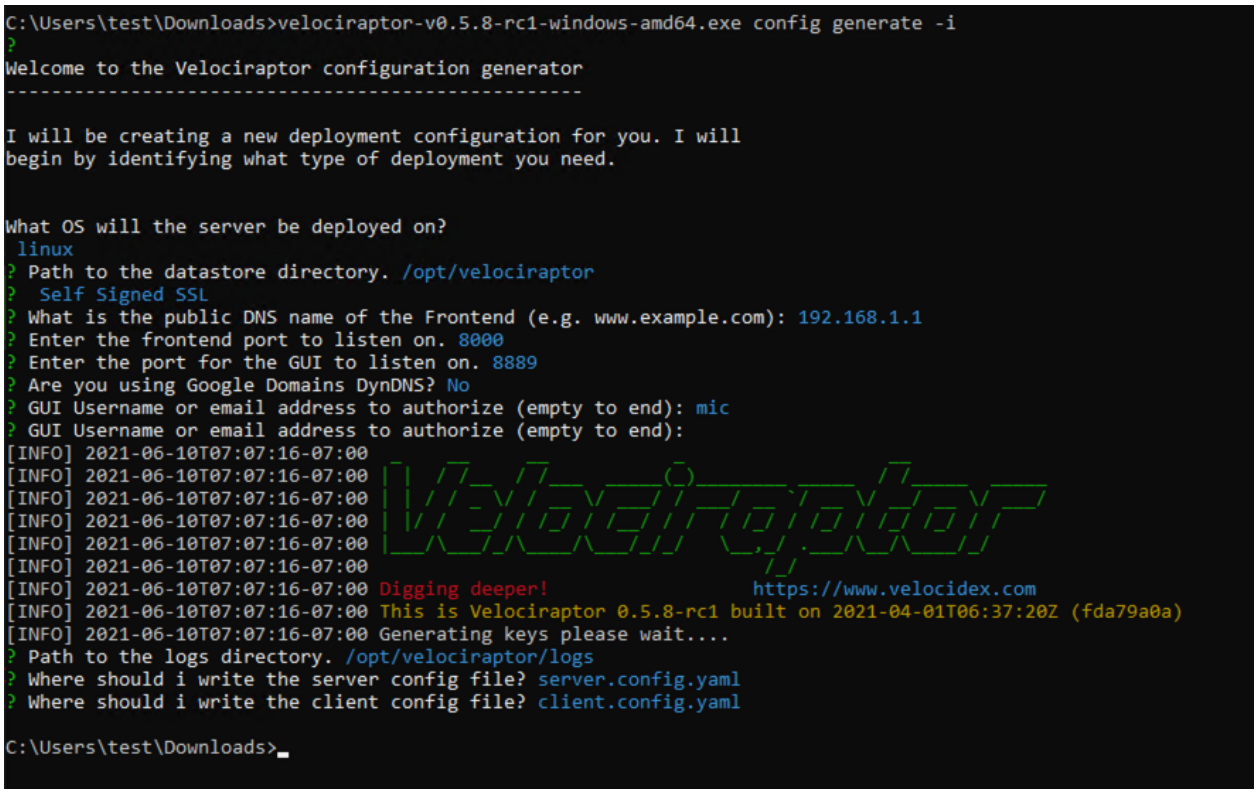
```
{
    "webhooks": [
    {
        "name": "Mattermost",
        "active": true,
        "trigger_on": ["on_postload_ioc_update"],
        "request_url": "http://192.168.244.84:8065/hooks/mtnm1mosifyu9ebekxpnywajsa",
        "request_rendering": "markdown",
        "use_rendering": true,
        "request_body": {
  "text": "IOC was updated"
}
    }  ]
}
```

Με αυτόν τον τρόπο, όταν πραγματοποιείται κάποια ενημέρωση IOC εντός του IRIS, θα αποστέλλεται το μήνυμα «IOC was updated» στο κανάλι Town Square του Mattermost.

4.2.6 Velociraptor

Το Velociraptor θα εγκατασταθεί ως υπηρεσία, με την χρήση του αντίστοιχου εκτελέσιμου που λαμβάνουμε από την επίσημη σελίδα [31]. Αρχικά θα πρέπει να δημιουργήσουμε κατάλληλα αρχεία διαμόρφωσης χρησιμοποιώντας το εκτελέσιμο αρχείο που κατεβάσαμε:

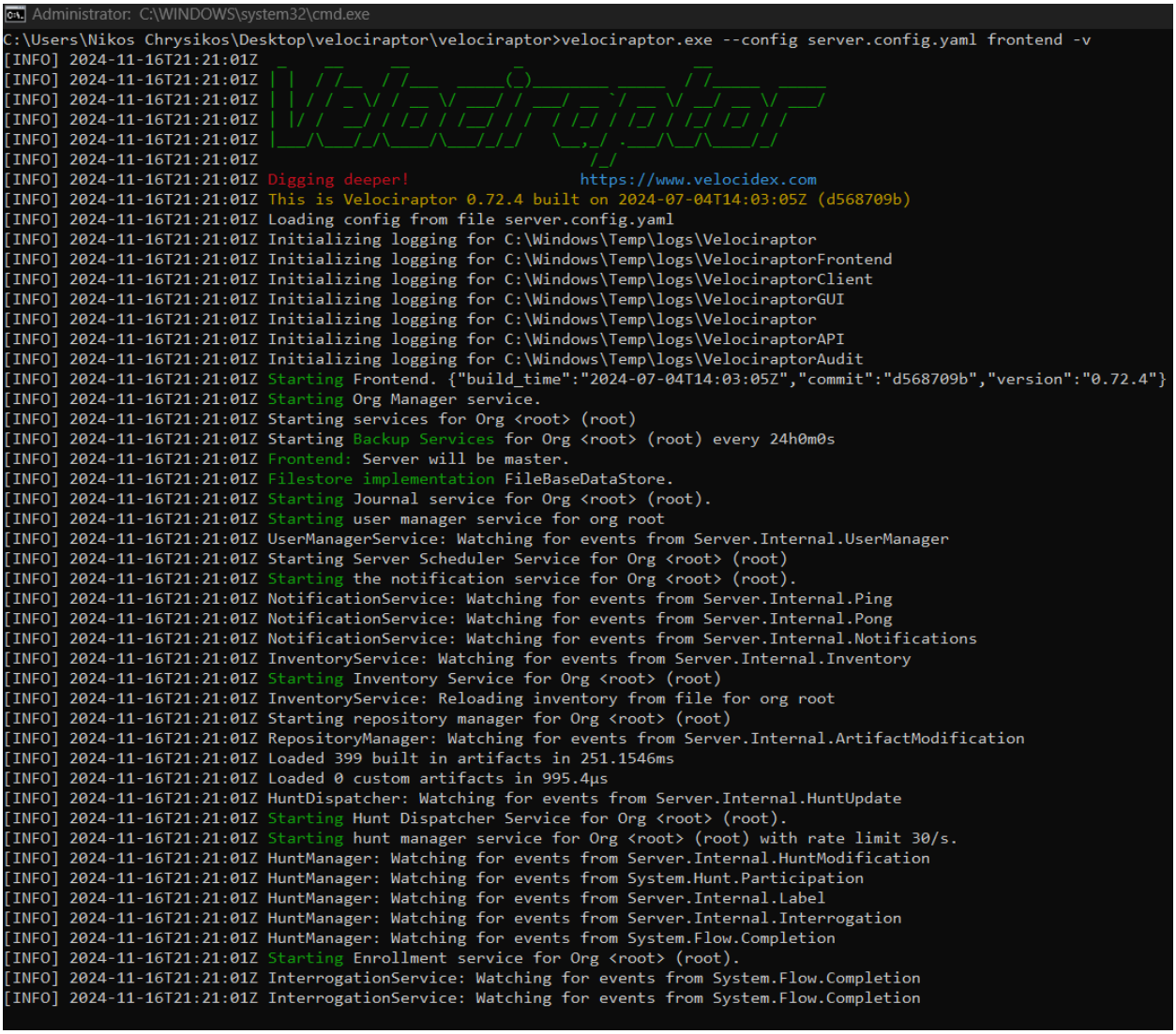
Velociraptor.exe config generate -i



Εικόνα 27 Δημιουργία των configuration files για το Velociraptor [31].

Ακολουθούμε τις παραπάνω επιλογές εκτός από το λειτουργικό σύστημα που είναι Windows. Μόλις δημιουργήσουμε τα δύο αρχεία , server.config.yaml που περιέχει βασικές ρυθμίσεις για τον server και το client.config.yaml αντίστοιχα, τότε μπορούμε να ενεργοποιήσουμε τον frontend server ως εξής :

Velociraptor.exe –config server.config.yaml frontend -v

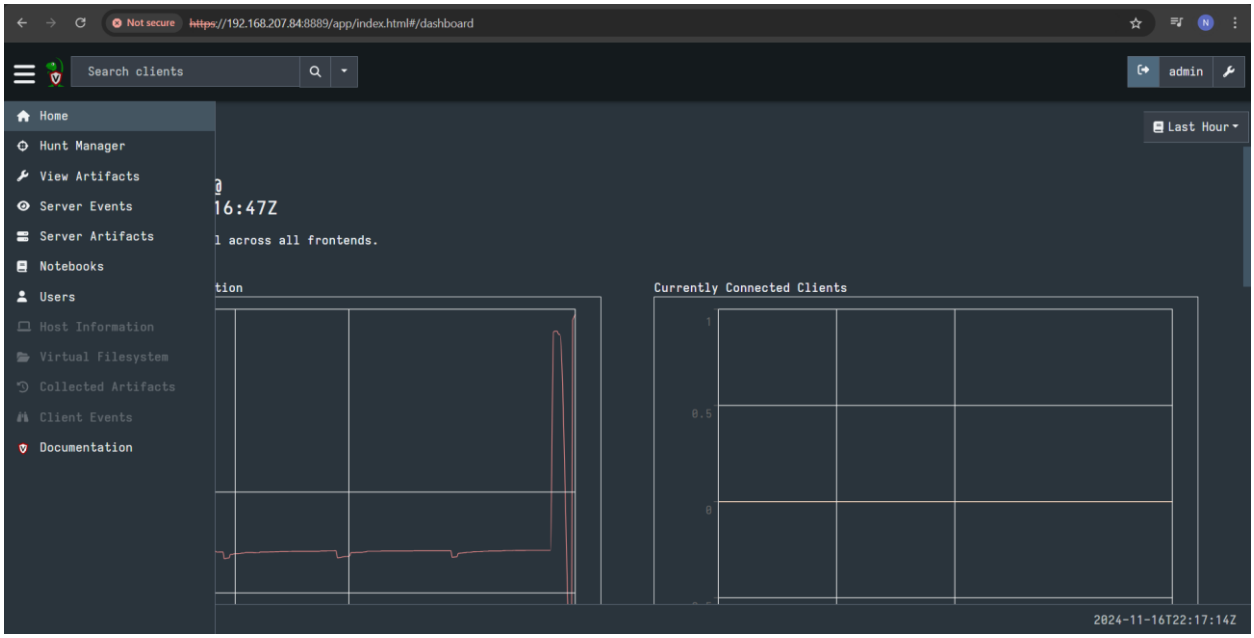


Εικόνα 28 Έναρξη frontend server του Velociraptor

Στην συνέχεια θα πρέπει να δημιουργήσουμε χρήστη :

velociraptor.exe --config server.config.yaml user add --role administrator admin admin

Με την παραπάνω εντολή δημιουργούμε χρήστη με δικαιώματα administrator, όνομα χρήστη admin και κωδικό πρόσβασης admin. Έπειτα, θα μεταβούμε στο url https://<ip>:8889 για να συνδεθούμε στο Velociraptor :

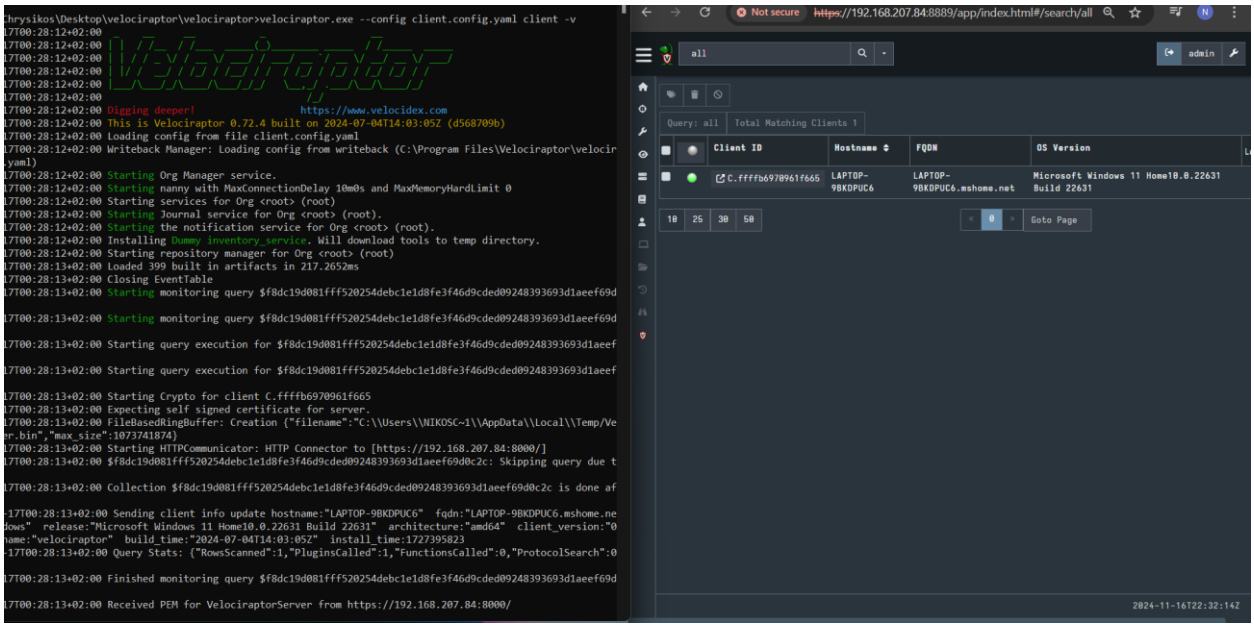


Εικόνα 29 Κεντρική σελίδα του Velociraptor

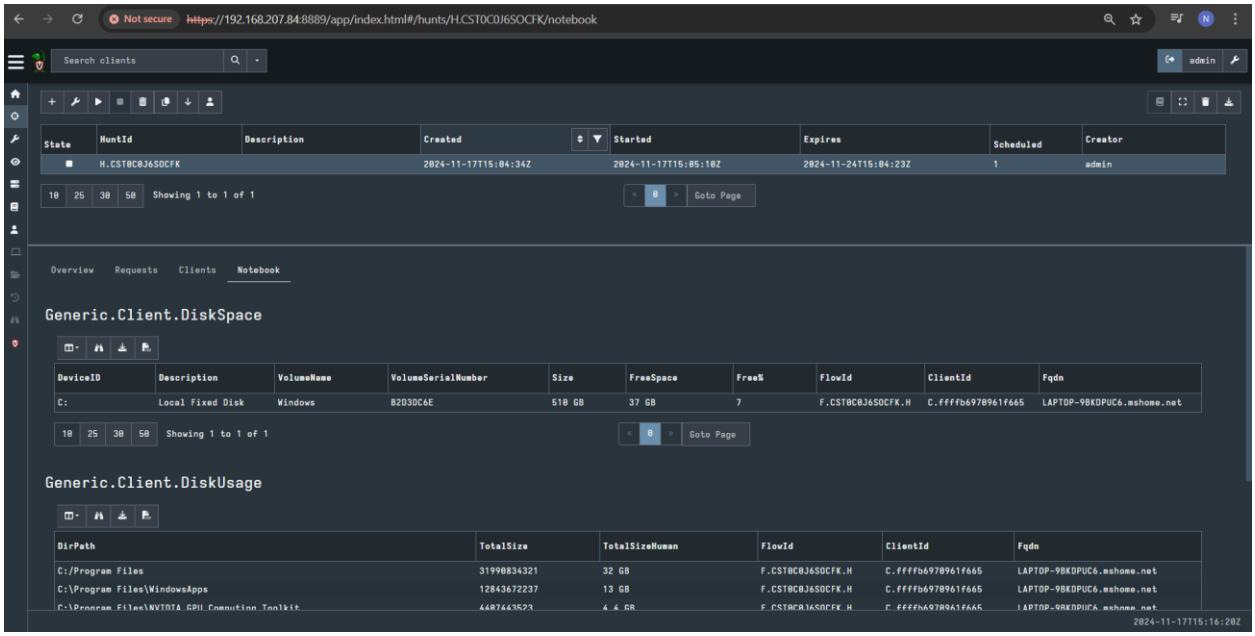
Επιπλέον, για την αναζήτηση artifacts (hunt) θα πρέπει να υπάρχει τουλάχιστον ένας πελάτης Velociraptor (Client). Με αυτό τον σκοπό , θα εκτελέσουμε τη παρακάτω εντολή :

velociraptor.exe –-config client.config.yaml client -v

Τότε, το σύστημα που λειτουργεί ως server του velociraptor, θα λειτουργεί και ως Client, επιτρέποντας την διενέργεια hunts (την συλλογή artifacts)



Εικόνα 30 Velociraptor Client



Εικόνα 31 Αποτελέσματα συλλογής των Artifacts Generic.Client.DiskSpace, Generic.Client.DiskUsage.

Δεν υπάρχει διαθέσιμο module στο IRIS που να επιτρέπει την άμεση σύνδεση του με το Velociraptor. Σε αυτή την περίπτωση θα χρησιμοποιήσουμε το custom module [44] iris-velociraptorartifact-module

Αρχικά θα πρέπει να δημιουργήσουμε api.config.yaml αρχείο. Αυτό επιτυγχάνεται με την χρήση του velociraptor.exe :

Velociraptor.exe –config server.config.yaml config api_client --name admin --role administrator api.config.yaml

1. --config server.config.yaml : περιέχει τη διαμόρφωση του server που περιέχει τα ιδιωτικά κλειδιά της CA που απαιτούνται για την υπογραφή ενός νέου πιστοποιητικού.
2. config api_client : δημιουργία πιστοποιητικού api_client
3. --name admin: Τα πιστοποιητικά αντιπροσωπεύουν ταυτότητες. Το όνομα του πιστοποιητικού θα χρησιμοποιηθεί για την ταυτοποίηση του καλούντος.
4. --role administrator: Αυτή η επιλογή θα εκχωρήσει επίσης έναν ρόλο στο όνομα του νέου πιστοποιητικού. Ο ρόλος χρησιμοποιείται για τον έλεγχο των δικαιωμάτων που μπορεί να κάνει ο καλών.

Αφού δημιουργήσουμε το api.config.yaml , θα πρέπει να το προσαρτήσουμε σε δύο containers του iris, εξής :

cp api.config.yaml /opt/iris-web/docker/api.config.yaml

Και στην συνέχεια να επεξεργαστούμε το docker-compose.yml αρχείο του iris ώστε στην επόμενη εκκίνηση του, τα containers Worker και app να συμπεριλάβουν το αρχείο διαμόρφωσης του velociraptor:

```
app:
  build:
    context: .
```

```
    dockerfile: docker/webApp/Dockerfile
  image: iriswebapp_app:latest
  command: ['nohup', './iris-entrypoint.sh', 'iriswebapp']
  volumes:
    - iris-downloads:/home/iris/downloads
    - user_templates:/home/iris/user_templates
    - server_data:/home/iris/server_data
    - "./docker/api.config.yaml:/iriswebapp/api.config.yaml:ro"

worker:
  build:
    context: .
    dockerfile: docker/webApp/Dockerfile
  image: iriswebapp_app:latest
  command: ['./wait-for-iriswebapp.sh', 'app:8000', './iris-entrypoint.sh', 'iris-worker']
  volumes:
    - iris-downloads:/home/iris/downloads
    - user_templates:/home/iris/user_templates
    - server_data:/home/iris/server_data
    - "./docker/api.config.yaml:/iriswebapp/api.config.yaml:ro"
```

Έπειτα, επανεκκινούμε το compose stack του IRIS :

```
docker-compose down
docker-compose up -d
```

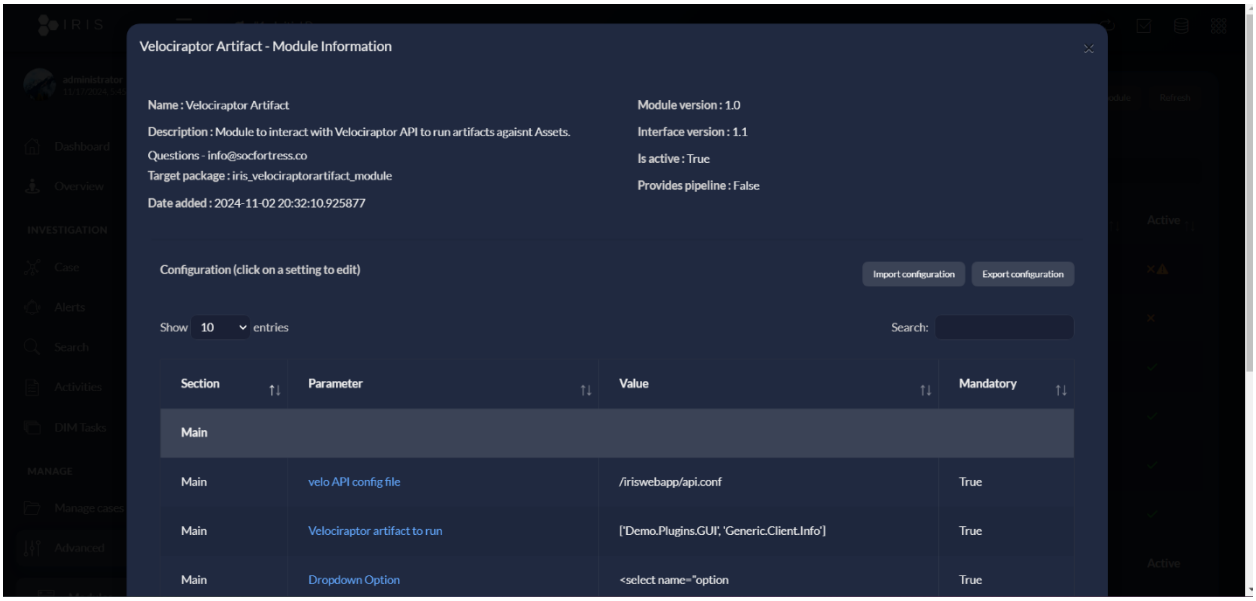
Με τα προηγούμενα βήματα, επιτρέψαμε την πραγματοποίηση api κλήσεων από το IRIS στο velociraptor, καθώς πλέον ο χρήστης administrator του IRIS διαθέτει τα κατάλληλα πιστοποιήτικα και το ιδιωτικό κλειδί, ώστε να έχει δικαιώματα administrator και στο velociraptor, και να μπορεί να ταυτοποιηθεί. Τώρα μπορούμε να κατεβάσουμε και να εγκαταστήσουμε το velociraptor :

```
git clone https://github.com/socfortress/iris-velociraptorartifact-module
cd iris-velociraptorartifact-module
```

Και για την εγκατάσταση του :

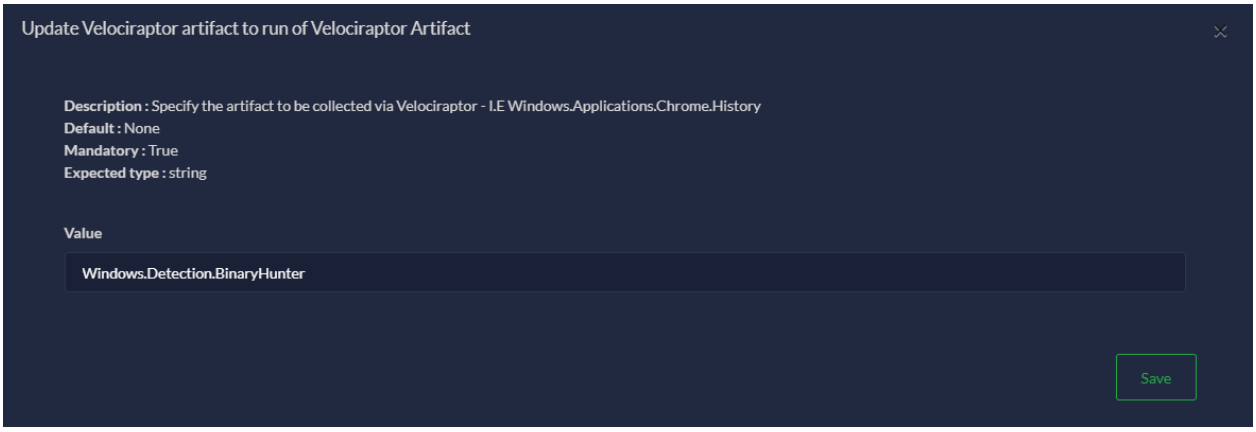
```
./buildnpush2iris.sh -a
```

Αφού ολοκληρωθεί η εγκατάσταση του module, θα μεταβούμε στα modules του IRIS και θα προσθέσουμε νέο, με το όνομα iris_velociraptorartifact_module και θα έχουμε το εξής αποτέλεσμα :



Εικόνα 31. Iris_velociraptorartifact_module

Το αρχικό module, όπως αυτό λαμβάνεται από το github repository, έχει τον ακόλουθο τρόπο ορισμού artifact προς συλλογή :



Εικόνα 32. Αρχικός τρόπος επιλογής Artifact προς συλλογή

Ωστόσο, ο παραπάνω τρόπος δεν επιτρέπει την αναζήτηση πολλαπλών artifacts, και δεν είναι αποτελεσματικός, καθώς ο αναλυτής θα πρέπει να μνημονεύει την ονομασία των artifacts, και κάποιο ορθογραφικό σφάλμα κατά την εισαγωγή ενός artifact θα οδηγήσει στην αποτυχία της συλλογής του (hunt).

Τα παραπάνω προβλήματα, επιλύει η εξής τρέχουσα υλοποίηση :

Εικόνα 33. Τρέχουσα υλοποίηση ορισμού artifacts προς συλλογή

Η παραπάνω προσέγγιση επιτρέπει την χρήση λίστας με artifacts (εδώ έχουν οριστεί 3 για την πραγματοποίηση δοκιμών λειτουργικότητας) και την ταυτόχρονη επιλογή πολλαπλών artifacts από την λίστα.

Η παραπάνω υλοποίηση επιτυγχάνεται με τις ακόλουθες τροποποιήσεις :

/iriswebapp/app/static/assets/js/iris/manage.modules.js

```
function update_param(module_id, param_name) {
  url = 'modules/get-parameter/' + decodeURIComponent(escape(window.btoa(param_name))) + case_param();
  // Load the modal content dynamically
  $('#modal_update_param_content').load(url, function (response, status, xhr) {
    if (status !== "success") {
      ajax_notify_error(xhr, url);
      return false;
    }

    if (param_name === '13##velo_artifact') {
      $('#modal_update_param_content').html(`
        <select id="dropdown_options" multiple>
          <option value="Demo.Plugins.GUI">Demo.Plugins.GUI</option>
          <option value="Generic.Client.DiskSpace">Generic.Client.DiskSpace</option>
          <option value="Generic.Client.Info">Generic.Client.Info</option>
        </select>
        <input type="text" id="selected_options" readonly>
      `);
      $('#dropdown_options').change(function () {
        var selectedOptions = $(this).val();  // This returns an array of selected options
      });
      $('#dropdown_options').off("focusout").on("focusout", function () {
        var selectedOptions = $(this).val(); // Get the selected options
        if (selectedOptions) {
          var data = {
            parameter_value: selectedOptions,
            csrf_token: $('#csrf_token').val()
          };
          post_request_api('modules/set-parameter/' + decodeURIComponent(escape(window.btoa(param_name))), JSON.stringify(data))
          .done((data) => {
            if (notify_auto_api(data)) {
```

```
                module_detail(module_id);
                refresh_modules(true);
                $('#modal_update_param').modal('hide');
            }
        });
        return false;
    }});

} else {
    // Handle other params in the usual way
    $('#submit_save_parameter').off("click").on("click", function () {
        var data = {};

        // Use ACE editor if present
        if ($('#editor_detail').length != 0) {
            editor = ace.edit("editor_detail");
            data['parameter_value'] = editor.getSession().getValue();
            data['csrf_token'] = $('#csrf_token').val();
        } else {
            data = $('#form_update_param').serializeObject();

            // Handle checkbox value
            if ($('#parameter_value').attr('type') == "checkbox") {
                data['parameter_value'] = $('#parameter_value').prop('checked');
            }
        }

        // API request to save other parameters
        post_request_api('modules/set-parameter/' +
decodeURIComponent(escape(window.btoa(param_name))), JSON.stringify(data))
        .done((data) => {
            if (notify_auto_api(data)) {
                module_detail(module_id);
                refresh_modules(true);
                $('#modal_update_param').modal('hide');
            }
        });
```

```
            return false;
        });
    }
    $('#modal_update_param').modal({ show: true });
 });
}
```

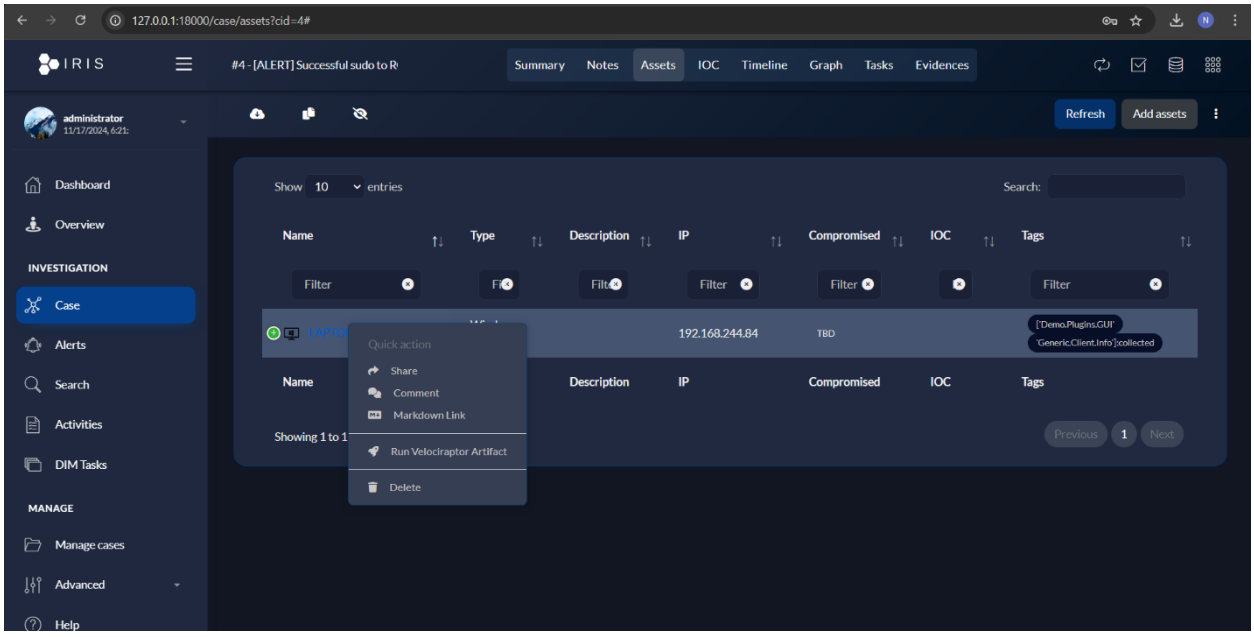
Με τον παραπάνω κώδικα, τροποποιούμε την δομή των modules, στην περίπτωση του velociraptor artifact module, έτσι ώστε να προβάλλεται μια html λίστα για την επιλογή του artifact.

Στην συνέχεια θα πρέπει να τροποποιήσουμε και το custom module ώστε να μπορεί να διαχειρίζεται περισσότερα από ένα artifacts :

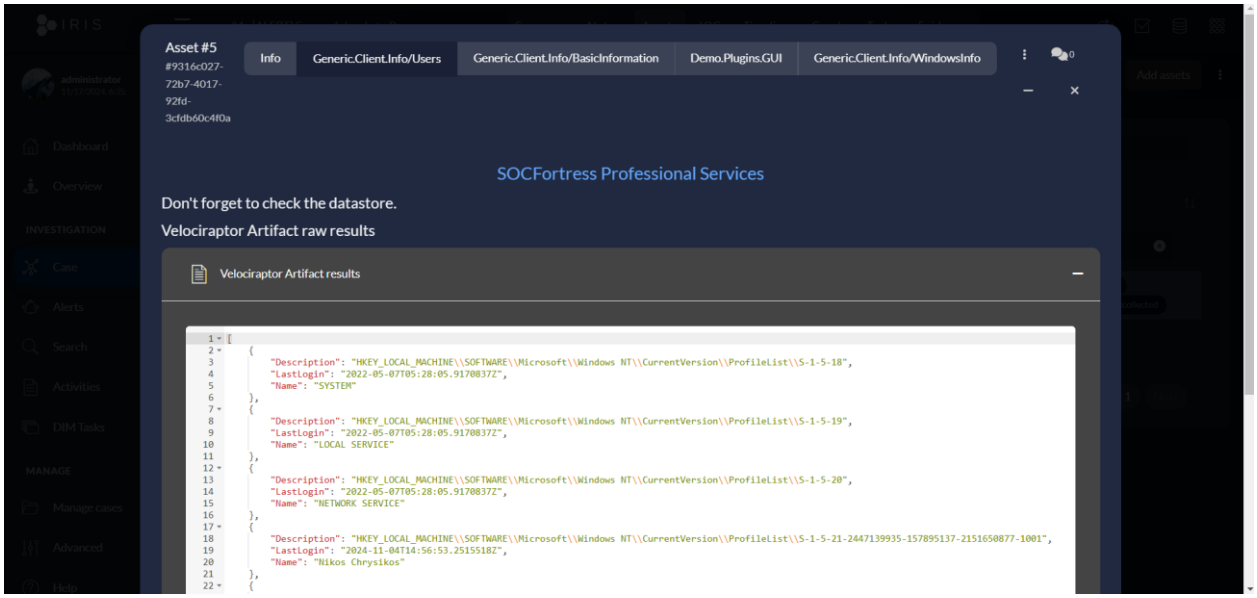
/opt/venv/lib/python3.9/site-packages/iris_velociraptorartifact_module/velociraptorartifact_handler/velociraptorartifact_handler.py

```
        artifact_str = "[" + ", ".join(f"'{item}'" for item in artifact) + "]"
        init_query = ("SELECT collect_client(client_id='" + client_id + "', artifacts=" + artifact_str + ") FROM scope()" )
 request = api_pb2.VQLCollectorArgs(max_wait=1,Query=[api_pb2.VQLRequest(Name="Query",VQL=init_query)])
```

Πλέον , μπορούμε να χρησιμοποιήσουμε το iris-velociraptor module για την συλλογη artifacts από assets του IRIS :



Εικόνα 34. Συλλογή artifacts από Asset



Εικόνα 35. Αποτελέσματα συλλογής Artifacts

4.2.7 Wazuh

Για την εγκατάσταση του Wazuh θα ακολουθήσουμε τις οδηγίες από την επίσημη ιστοσελίδα [45] . Αρχικά θα κατεβάσουμε δύο αρχεία , το wazuh-certs-tool.sh και το config.yml :

curl -sO https://packages.wazuh.com/4.9/wazuh-certs-tool.sh

curl -sO https://packages.wazuh.com/4.9/config.yml

και στην συνέχεια, θα επεξεργαστούμε το config.yml ώστε να θέσουμε τις κατάλληλες παραμέτρους :

```
nodes:
  indexer:
    - name: localhost
      ip: 127.0.0.1
  server:
    - name: localhost
      ip: 127.0.0.1
  dashboard:
    - name: localhost
      ip: 127.0.0.1
```

και στην συνέχεια θα χρησιμοποιήσουμε το Wazuh-certs-tool.sh για την δημιουργία των απαραίτητων πιστοποιητικών :

bash ./wazuh-certs-tool.sh -A

Η παραπάνω εντολή θα δημιουργήσει φάκελο με τα πιστοποιητικά, λαμβάνοντας υπόψη τις ρυθμίσεις του config.yml.

Η αρχιτεκτονική του Wazuh βασίζεται σε 3 αλληλένδετους κόμβους :

- Wazuh-Indexer
- Wazuh-Manager
- Wazuh-Dashboard

Επομένως στα ακόλουθα βήματα θα εγκαταστήσουμε τους παραπάνω κόμβους, και θα τους διαμορφώσουμε κατάλληλα.

Wazuh-Indexer

Για την εγκατάσταση του Wazuh-Indexer έχουμε :

apt-get -y install wazuh-indexer

Αφού ολοκληρωθεί η εγκατάσταση, θα τροποποιήσουμε τις παραμέτρους του /etc/wazuh-indexer/opensearch.yml κατάλληλα, βάσει των παραμέτρων που θέσαμε στο config.yml.

Στην συνέχεια θα μεταφέρουμε τα πιστοποιητικά στο Wazuh-indexer και θα δώσουμε κατάλληλα δικαιώματα

NODE_NAME=localhost

mkdir /etc/wazuh-indexer/certs

tar -xf ./wazuh-certificates.tar -C /etc/wazuh-indexer/certs/ ./$NODE_NAME.pem ./$NODE_NAME-key.pem ./admin.pem ./admin-key.pem ./root-ca.pem

mv -n /etc/wazuh-indexer/certs/$NODE_NAME.pem /etc/wazuh-indexer/certs/indexer.pem

mv -n /etc/wazuh-indexer/certs/$NODE_NAME-key.pem /etc/wazuh-indexer/certs/indexer-key.pem

chmod 500 /etc/wazuh-indexer/certs

chmod 400 /etc/wazuh-indexer/certs/*

chown -R wazuh-indexer:wazuh-indexer /etc/wazuh-indexer/certs

Για να ενημερωθεί ο Wazuh-Indexer για τα νέα πιστοποιητικά θα πρέπει να εκτελέσουμε την εντολή :

/usr/share/wazuh-indexer/bin/indexer-security-init.sh

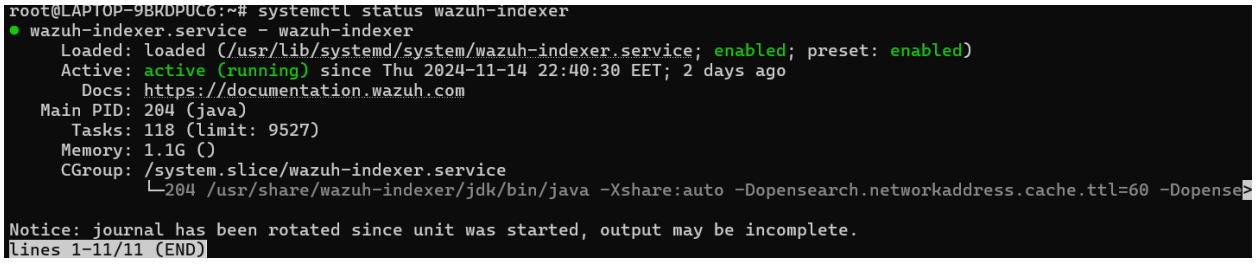
και τέλος θα ενεργοποιήσουμε την υπηρεσία του Wazuh-Indexer :

systemctl daemon-reload

systemctl enable wazuh-indexer

systemctl start wazuh-indexer

Έτσι θα έχουμε :



Εικόνα 36. Ενεργοποιημένη υπηρεσία του Wazuh-Indexer

Στην συνέχεια θα προχωρήσουμε στην εγκατάσταση του Wazuh-manager :

apt-get -y install wazuh-manager

Επιπλέον θα χρειαστεί να εγκαταστήσουμε την εφαρμογή filebeat [31] που συλλέγει, επεξεργάζεται και προωθεί δεδομένα καταγραφής από διάφορες πηγές σε ένα κεντρικό σημείο για περαιτέρω ανάλυση.

apt-get -y install filebeat

curl -so /etc/filebeat/filebeat.yml https://packages.wazuh.com/4.9/tpl/wazuh/filebeat/filebeat.yml

‘Επειτα θα δημιουργήσουμε filebeat keystore για να αποθηκεύσουμε τους κωδικούς σύνδεσης.

filebeat keystore create

Και θα εισάγουμε όνομα χρήστη και κωδικό πρόσβασης :

echo admin | filebeat keystore add username --stdin --force

echo admin | filebeat keystore add password --stdin --force

Τώρα θα κατεβάσουμε alerts template για το Wazuh Indexer :

curl -so /etc/filebeat/wazuh-template.json https://raw.githubusercontent.com/wazuh/wazuh/v4.9.2/extensions/elasticsearch/7.x/wazuh-template.json

chmod go+r /etc/filebeat/wazuh-template.json

και θα εγκαταστήσουμε το Wazuh module για το Filebeat :

curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-0.4.tar.gz | tar -xvz -C /usr/share/filebeat/module

Ακολούθως, όπως και προηγουμένως, θα πρέπει να εγκαταστήσουμε τα πιστοποιητικά :

NODE_NAME=localhost

mkdir /etc/filebeat/certs

tar -xf ./wazuh-certificates.tar -C /etc/filebeat/certs/ ./$NODE_NAME.pem ./$NODE_NAME-key.pem ./root-ca.pem

mv -n /etc/filebeat/certs/$NODE_NAME.pem /etc/filebeat/certs/filebeat.pem

mv -n /etc/filebeat/certs/$NODE_NAME-key.pem /etc/filebeat/certs/filebeat-key.pem

chmod 500 /etc/filebeat/certs

chmod 400 /etc/filebeat/certs/*

chown -R root:root /etc/filebeat/certs

Εφόσον επιθυμούμε να χρησιμοποιήσουμε vulnerability detection capability του Wazuh :

echo 'admin' | /var/ossec/bin/wazuh-keystore -f indexer -k username

echo 'admin' | /var/ossec/bin/wazuh-keystore -f indexer -k password

Αφού έχουμε ακολουθήσει τα προηγούμενα βήματα , μπορούμε να ενεργοποιήσουμε τις υπηρεσίες του Wazuh-manager και Filebeat :

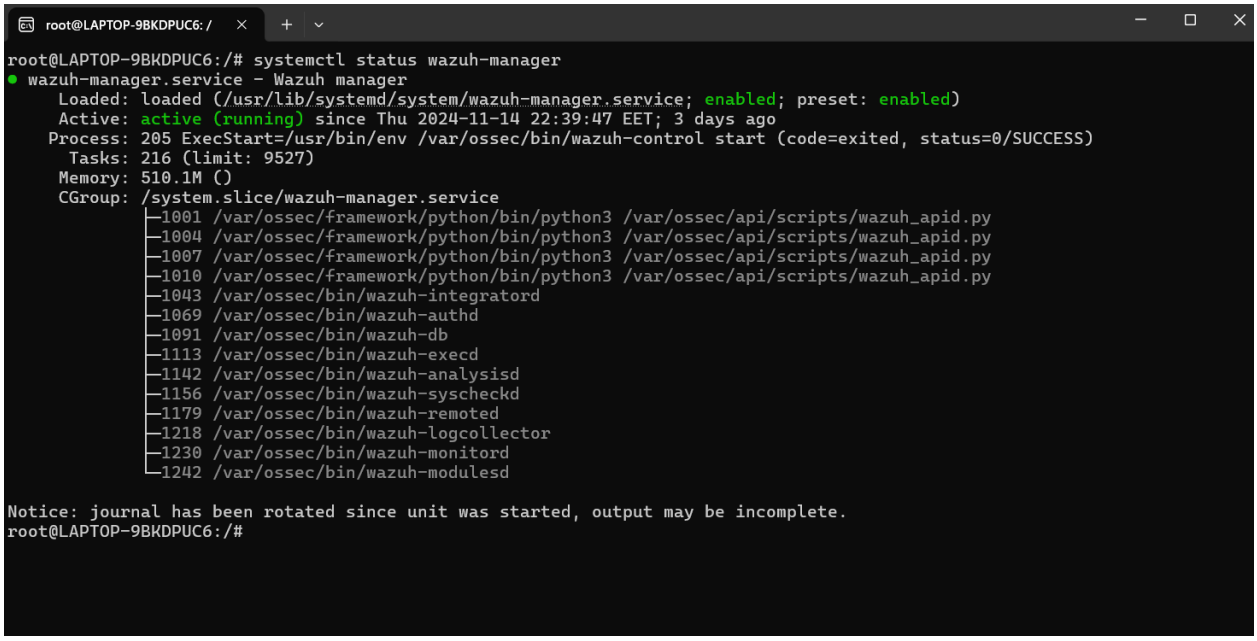
systemctl daemon-reload

systemctl enable wazuh-manager

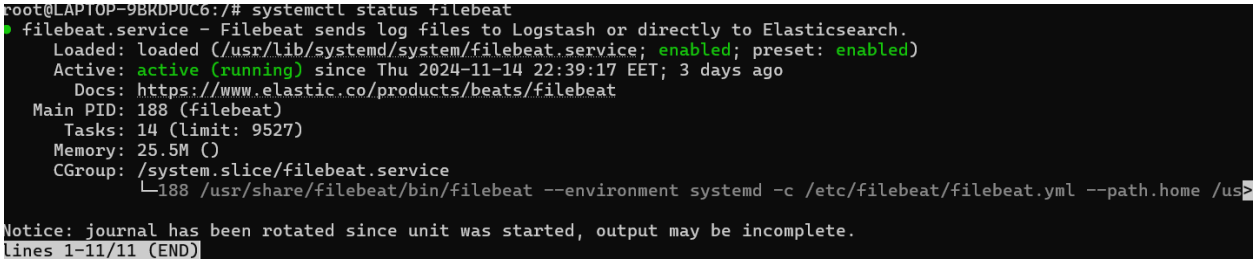
systemctl enable filebeat

systemctl start wazuh-manager

systemctl start filebeat



Εικόνα 37. Ενεργοποιημένη υπηρεσία του Wazuh-manager



Εικόνα 38. Ενεργοποιημένη υπηρεσία του Filebeat

Wazuh Dashboard

Αρχικά θα εγκαταστήσουμε τα απαραίτητα πακέτα :

apt-get install debhelper tar curl libcap2-bin

Και στην συνέχεια θα εγκαταστήσουμε το wazuh-dashboard :

apt-get -y install wazuh-dashboard

Και θα τροποποιήσουμε το αρχείο διαμόρφωσης του Wazuh dashboard θέτοντας server.host: 0.0.0.0 για να δέχεται συνδέσεις από όλες τις ip.

Ακολούθως, θα εγκαταστήσουμε τα απαραίτητα πιστοποιητικά :

NODE_NAME=localhost

mkdir /etc/wazuh-dashboard/certs

tar -xf ./wazuh-certificates.tar -C /etc/wazuh-dashboard/certs/ ./$NODE_NAME.pem ./$NODE_NAME-key.pem ./root-ca.pem

mv -n /etc/wazuh-dashboard/certs/$NODE_NAME.pem /etc/wazuh-dashboard/certs/dashboard.pem

mv -n /etc/wazuh-dashboard/certs/$NODE_NAME-key.pem /etc/wazuh-dashboard/certs/dashboard-key.pem

chmod 500 /etc/wazuh-dashboard/certs

chmod 400 /etc/wazuh-dashboard/certs/*

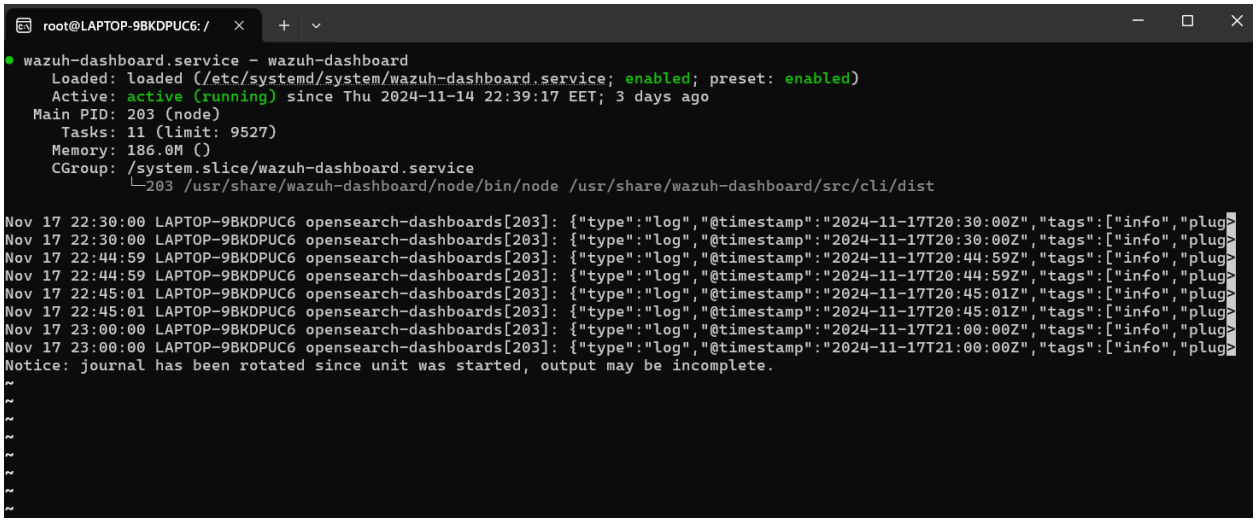
chown -R wazuh-dashboard:wazuh-dashboard /etc/wazuh-dashboard/certs

και θα ενεργοποιήσουμε την υπηρεσία wazuh-dashboard :

systemctl daemon-reload

systemctl enable wazuh-dashboard

systemctl start wazuh-dashboard



Εικόνα 39. Ενεργοποιημένη υπηρεσία του Wazuh Dashboard

Τέλος θα χρησιμοποιήσουμε το Wazuh-passwords tool για την παραγωγή κωδικών πρόσβασης για το Wazuh dashboard :

/usr/share/wazuh-indexer/plugins/opensearch-security/tools/wazuh-passwords-tool.sh --api --change-all --admin-user wazuh --admin-password Wazuh

Και το αναμενόμενο αποτέλεσμα είναι της μορφής :

INFO: The password for user admin is yWOzmNA.?Aoc+rQfDBcF71KZp?1xd7IO

INFO: The password for user kibanaserver is nUa+66zY.eDF*2rRl5GKdgLxvgYQA+wo

INFO: The password for user kibanaro is 0jHq.4i*VAgclnqFiXvZ5gtQq1D5LCcL

INFO: The password for user logstash is hWW6U45rPoCT?oR.r.Baw2qaWz2iH8Ml

INFO: The password for user readall is PNt5K+FpKDMO2TlxJ6Opb2D0mYl*I7FQ

INFO: The password for user snapshotrestore is +GGz2noZZr2qVUK7xbtqjUup049tvLq.

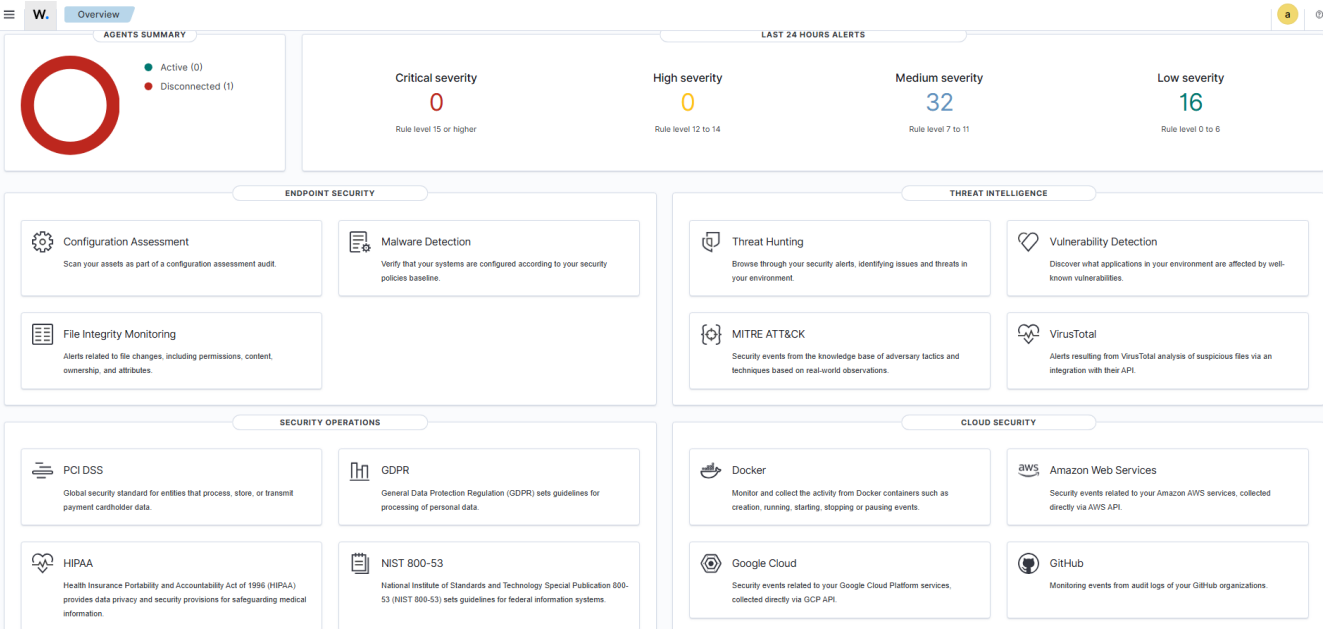
WARNING: Wazuh indexer passwords changed. Remember to update the password in the Wazuh dashboard and Filebeat nodes if necessary, and restart the services.

INFO: The password for Wazuh API user wazuh is JYWz5Zdb3Yq+uOzOPyUU4oat0n60VmWI

INFO: The password for Wazuh API user wazuh-wui is +fLddaCiZePxh24*?jC0nyNmgMGCKE+2

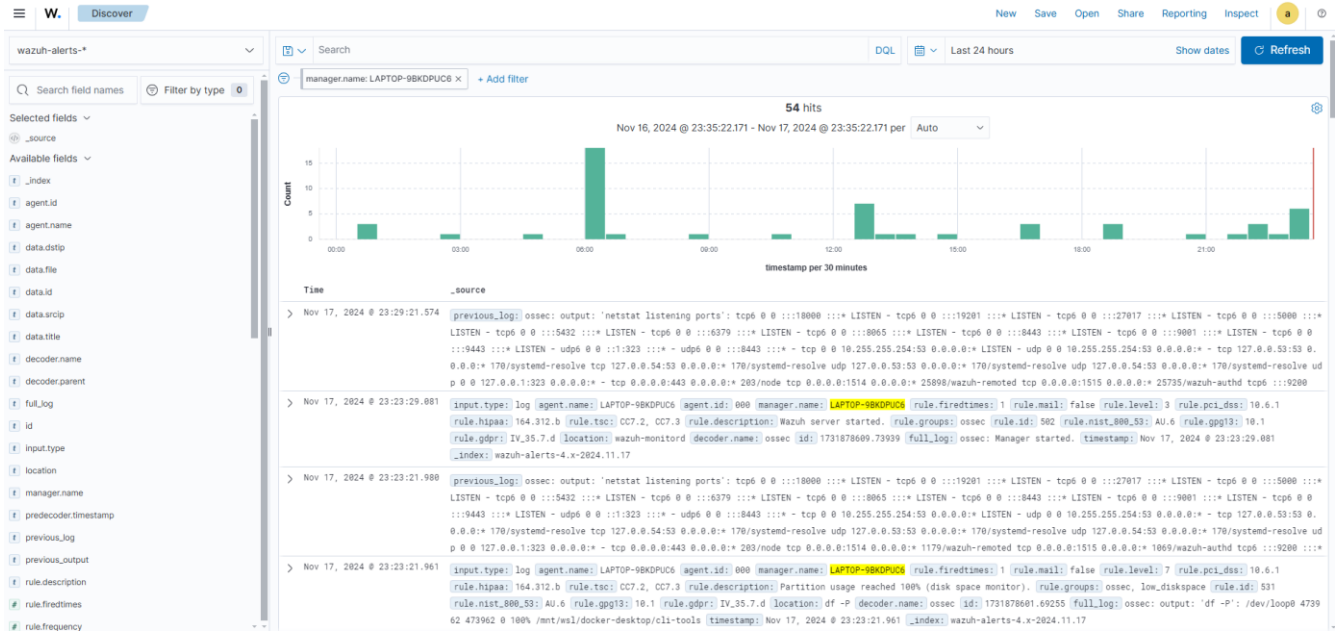
INFO: Updated wazuh-wui user password in wazuh dashboard. Remember to restart the service.

Οπότε πλέον μπορούμε να συνδεθούμε στο Wazuh Dashboard , στο url https://<ip> με όνομα χρήστη : admin και κωδικός πρόσβασης : yWOzmNA.?Aoc+rQfDBcF71KZp?1xd7IO.

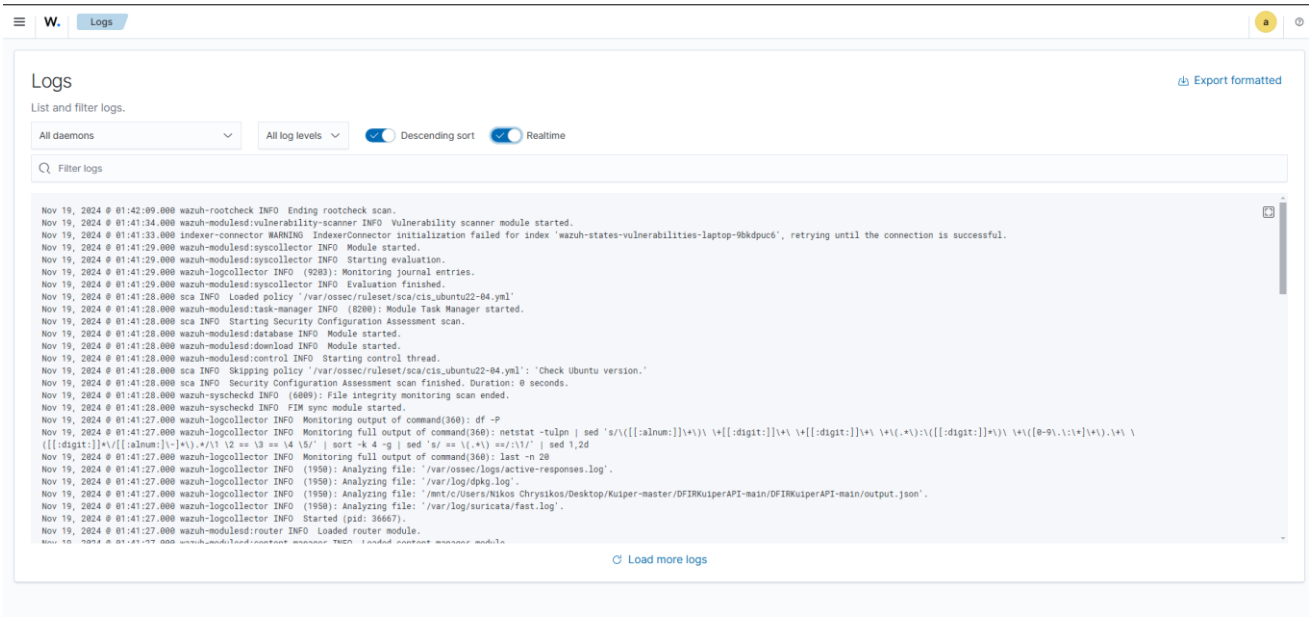


Εικόνα 40. Wazuh Dashboard

Μόλις συνδεθούμε στο Wazuh Dashboard άμεσα θα παρατηρήσουμε τις βασικότερες παροχές του, δηλαδή Endpoint Security, Threat Intelligence, Cloud Security και Security Operations (GRC), αλλά τις ειδοποιήσεις του τελευταίου 24ωρου, που είναι ομαδοποιημένες βάση βαρύτητας. Τέλος μπορούμε να παρακολουθούμε και πόσοι Wazuh agents είναι συνδεδεμένη και επικοινωνούν με τον server .



Εικόνα 41. Αναλυτική αναφορά των ειδοποιήσεων του τελευταίου 24ωρου.



Εικόνα 42. Καταγραφή δεδομένων του wazuh manager

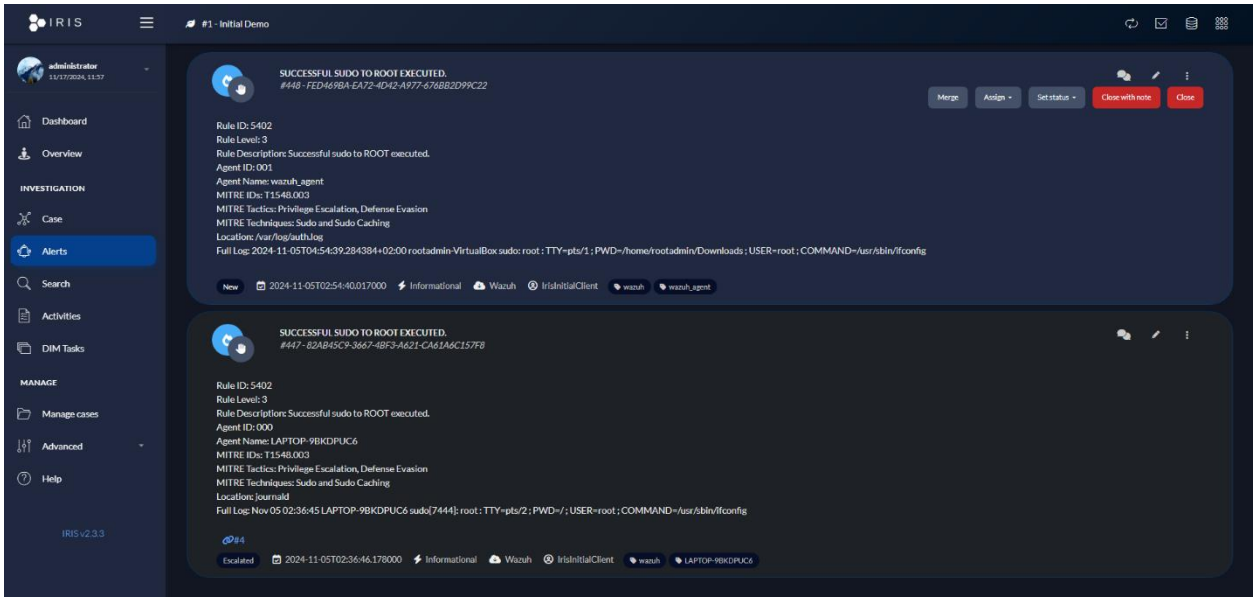
Στην εικόνα 42 εντοπίζουμε βασικές λειτουργίες του Wazuh manager , όπως η συλλογή δεδομένων από διάφορα log files όπως το suricara fast.log και Kuiper Api output.json .

Αναφορικά με την επικοινωνία του Wazuh με το IRIS, αυτή θεμελιώνεται με την προώθηση ειδοποιήσεων του Wazuh προς το Iris.

Η διασύνδεση αυτή υλοποιείται με την τροποποίηση του αρχείου /var/ossec/etc/ossec.conf ως εξής :

```
<integration>
  <name>custom-iris.py</name>
  <hook_url>http://127.0.0.1:18000/alerts/add</hook_url>
  <rule_id>5402</rule_id>
  <api_key>2iBypcmRiG_YR2SWB3ILn-zbFHOCAwTB4epjnuxFL5CIv4bC0aTpm6HLmRKnZN0J1D1x_aCAWHCkXTZiXpN9IA</api_key>
  <alert_format>json</alert_format>
</integration>
```

Προσθέτοντας τον παραπάνω κώδικα επιτρέπουμε την προώθηση ειδοποιήσεων με id 5402 (sudo execution under root) από το Wazuh στο IRIS. Αυτή η παράμετρος έχει τεθεί για τις ανάγκες της παρουσίασης. Επιπλέον θα πρέπει να δημιουργήσουμε το custom-iris.py για να υλοποιηθεί η διασύνδεση, όπως περιγράφεται στην σελίδα του Wazuh [32]. Έτσι, θα επιτευχθεί η δημιουργία ειδοποιήσεων στο IRIS από Wazuh.



Εικόνα 43. Ειδοποιήσεις από το Wazuh στο IRIS.

4.2.8 Kuiper.

Για την εγκατάσταση και την χρήση του Kuiper θα χρησιμοποιήσουμε docker containers. Η διαδικασία εγκατάστασης , όπως περιγράφεται στο github repository [48] είναι η εξής :

git clone https://github.com/DFIRKuiper/Kuiper.git

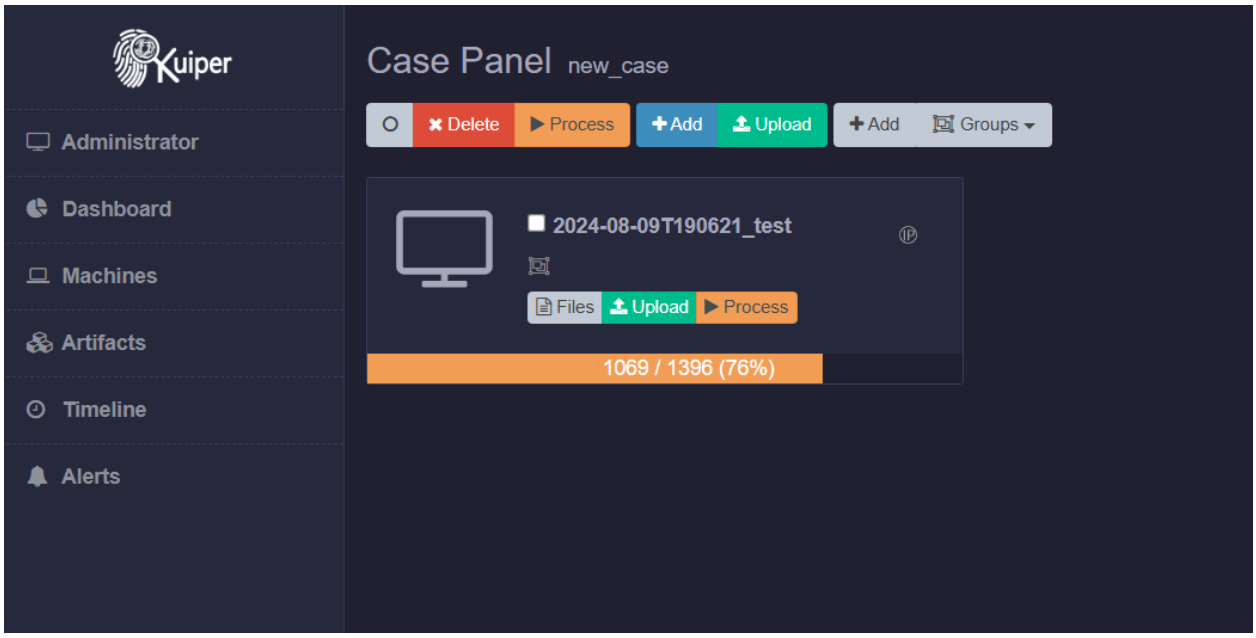
cd Kuiper

docker-compose build

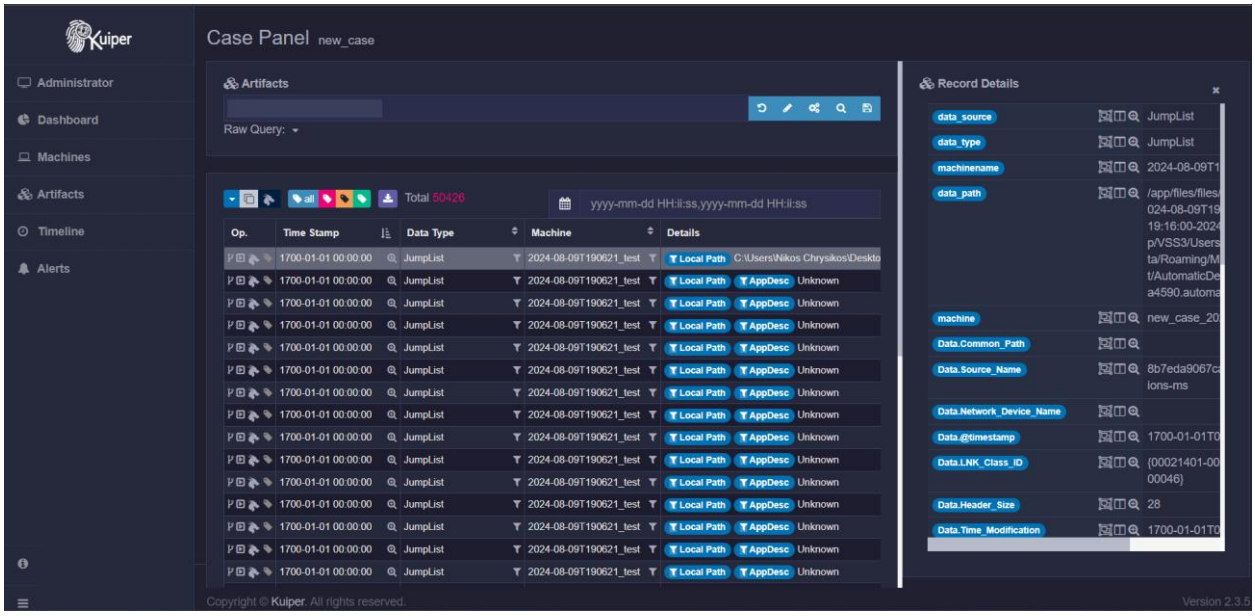
docker-compose up -d

Τότε, το Kuiper θα είναι προσβάσιμο στο url : http://<ip>:5000

Εικόνα 44. Αρχική σελίδα του Kuiper.



Εικόνα 45. Artifacts συλλεγμένα με την χρήση του KAPE.



Εικόνα 46. Αποτέλεσμα ανάλυσης των artifacts του new_case

Στις εικόνες 44-46 παρατηρούμε την ανάπτυξη ενός case του Kuiper, του οποίου τα δεδομένα έχουν ληφθεί από το KAPE που θα παρουσιαστεί αργότερα. Στην εικόνα 46 εντοπίζουμε τα δεδομένα και οι πληροφορίες που εξήχθησαν από την ανάλυση των artifacts που πραγματοποιήθηκε στην εικόνα 45. Τα αποτελέσματα αυτά , με την χρήση API μπορούν τα εξαχθούν και να αποθηκευτούν, ώστε να είναι προσβάσιμο από το Wazuh προς περαιτέρω ανάλυση. Αυτό επιτυγχάνεται ως εξής [49] :

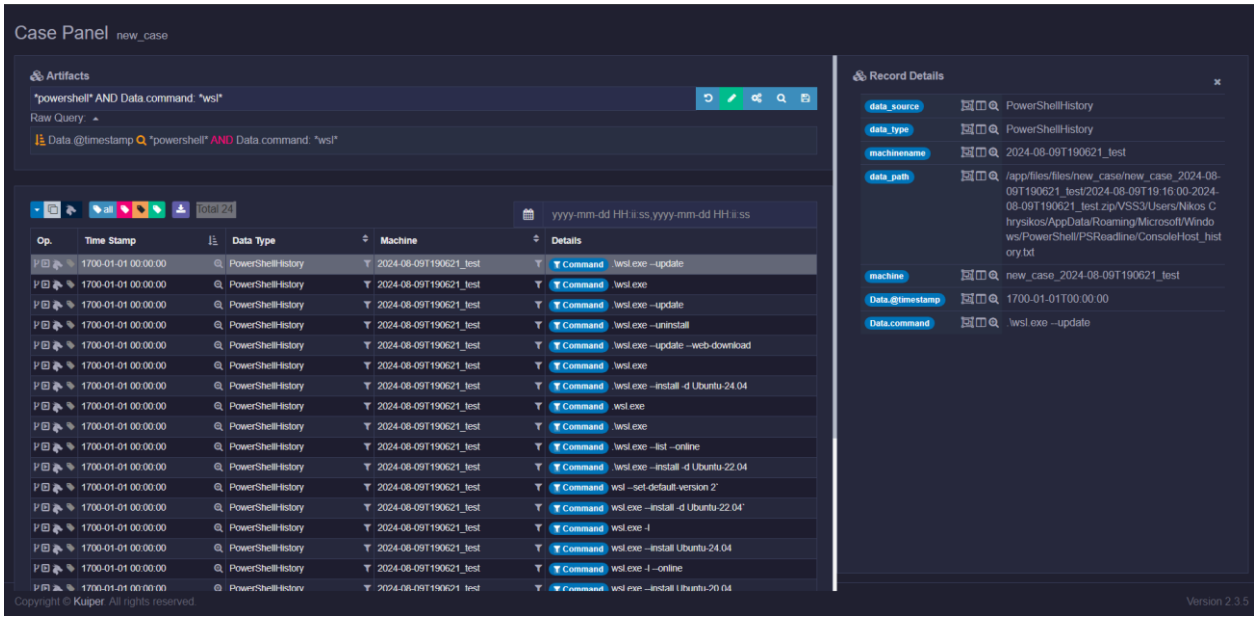
git get https://github.com/DFIRKuiper/DFIRKuiperAPI.git

cd DFIRKuiperAPI

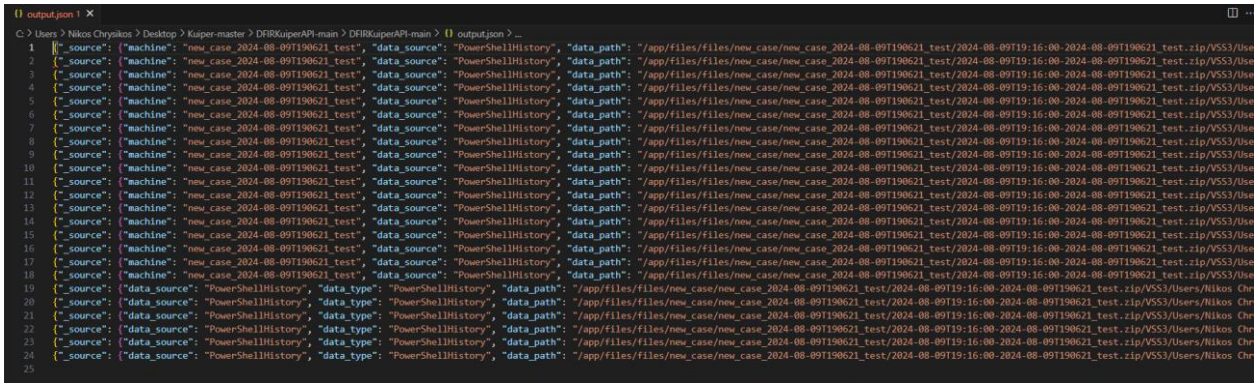
python GetFieldsScript.py -c new_case -f * -o output.json -u http://192.168.207.84:5000/api/ -t "API_TOKEN" -q "*powershell* AND Data.command:*wsl*"

Εικόνα 47. Χρήση του Kuiper API για την εξαγωγή δεδομένων από Case βάσει ερωτήματος.

Με την παραπάνω εντολή, λαμβάνουμε από τα αποτελέσματα της ανάλυσης τα δεδομένα που επιστρέφονται από το ερώτημα : *powershell* AND Data.command: *wsl* , δηλαδή να χρησιμοποιείται στο powershell εντολή σχετικά με το wsl.



Εικόνα 48. Αποτελέσματα ερωτήματος στο Kuiper.



Εικόνα 49. Εξαγωγή αποτελεσμάτων από το Kuiper.

Τέλος, τα δεδομένα του output.json προωθούνται στο Wazuh, όπως φαίνεται και από την εικόνα 42. Η επικοινωνία του Kuiper-Wazuh επιτυγχάνεται με την προσθήκη στο ossec.conf του παρακάτω κώδικα :

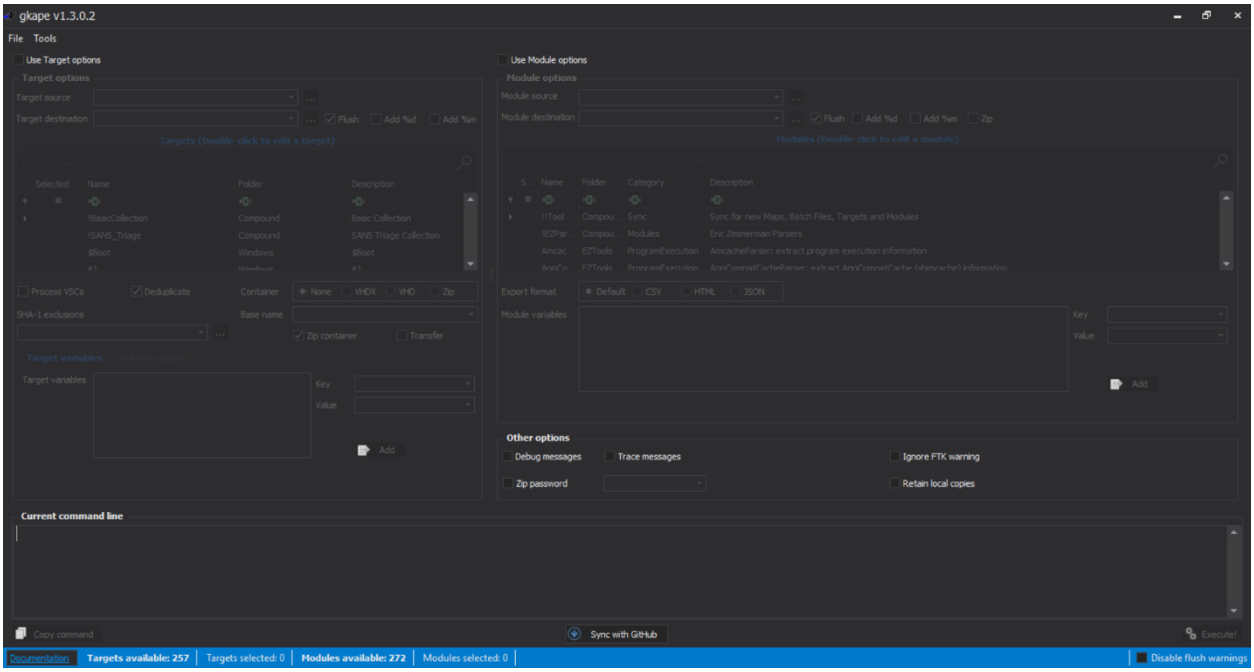
```
<localfile>
  <log_format>json</log_format>
  <location>/mnt/c/Users/Nikos Chrysikos/Desktop/Kuiper-master/DFIRKuiperAPI-main/DFIRKuiperAPI-main/output.json</location>
  <only-future-events>no</only-future-events>
</localfile>
```

Η παράμετρος only-future-events, όταν είναι ενεργή, εξετάζει το περιεχόμενο του αρχείου, από την στιγμή που ενεργοποιήθηκε ο Wazuh-manager και όχι από την αρχή του, συνεπώς, την απενεργοποιούμε αφού επιθυμούμε σε κάθε περίπτωση ο Wazuh manager να αναλύει όλες τις εγγραφές του output.json. Συνοψίζοντας λοιπόν, η επικοινωνία IRIS-Kuiper επιτυγχάνεται έμμεσα, μέσω του Wazuh.

4.2.9 Kape

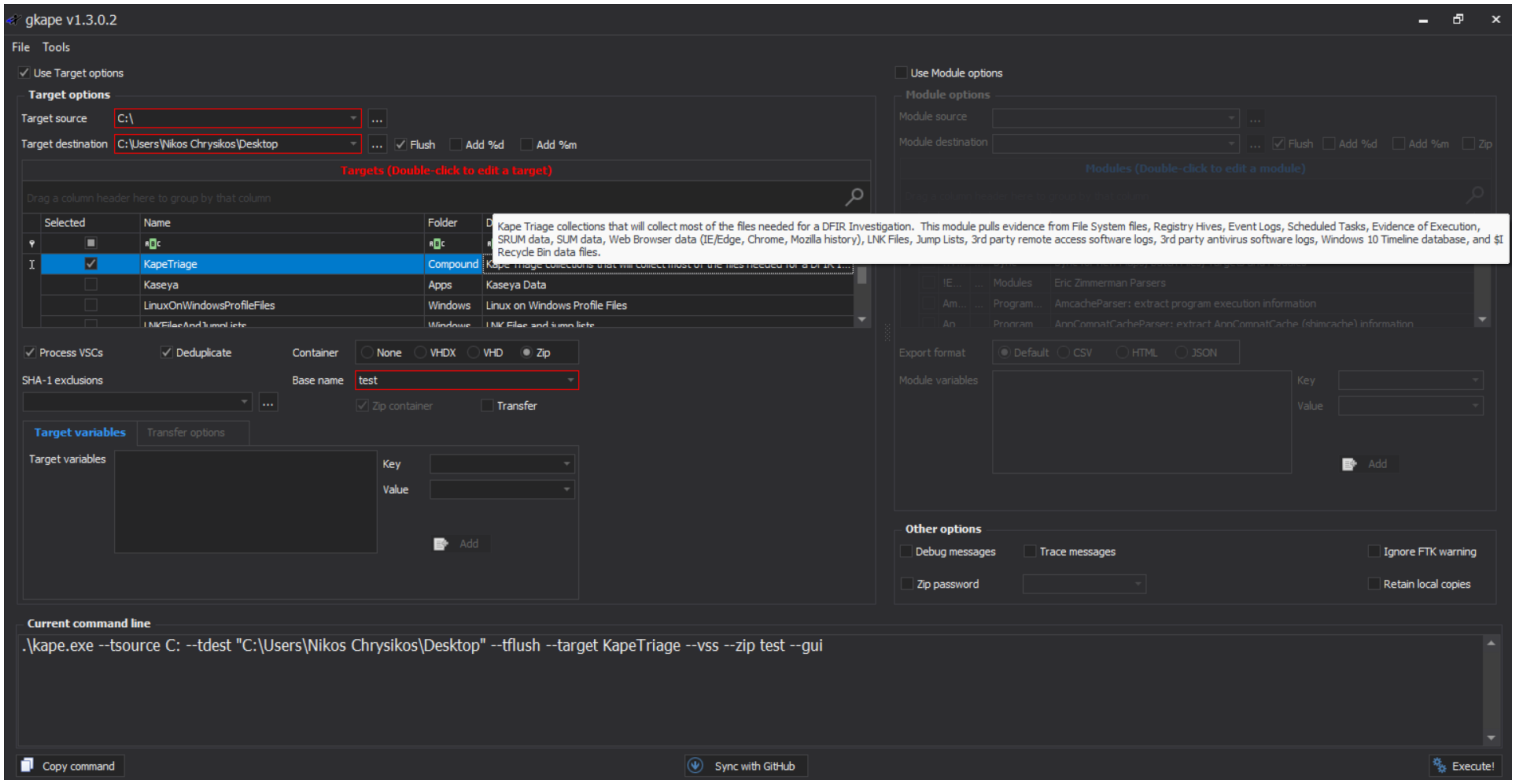
Το Kape δεν απαιτεί εγκατάσταση. Αρκεί να κατεβάσουμε το zip αρχείο από την επίσημη σελίδα [50] και να εκτελέσουμε το gkape.exe αρχείο που περιέχει.

Τότε θα εμφανιστεί το γραφικό περιβάλλον του KAPE :



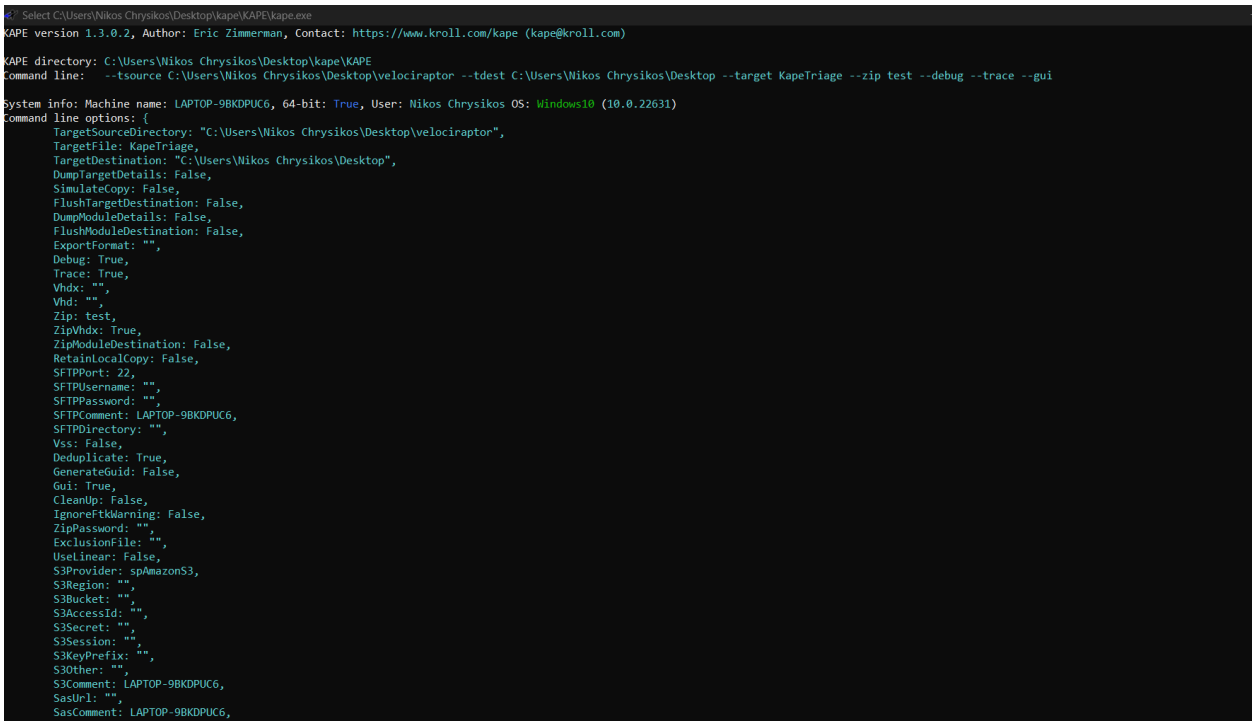
Εικόνα 50. Γραφικό περιβάλλον KAPE

Όπως παρατηρούμε, το KAPE διαθέτει 2 βασικές λειτουργίες, την χρήση των targets και των modules. Στην υλοποίηση αυτή, το KAPE χρησιμοποιείται ως εργαλείο συλλογής artifacts, οπότε θα χρησιμοποιήσουμε τα targets. Αρκεί λοιπόν να ορίσουμε Target Source, δηλαδή τον root φάκελο από τον οποίο θα ξεκινήσει η συλλογή στοιχείων, Target Destination δηλαδή το σημείο στο οποίο θα αποθηκευτούν τα αποτελέσματα, και προαιρετικά μπορούμε να εξετάσουμε τα volume shadow copies αν αυτά υπάρχουν , και να διαγράφουμε τα διπλότυπα αρχεία. Αφού ορίσουμε τις παραπάνω παραμέτρους, θα πρέπει να επιλέξουμε target. Υπάρχουν 257 διαφορετικά targets διαθέσιμα με διαφορετικούς συνδυασμούς φακέλων και αρχείων προς αναζήτηση. Συνεπώς ανάλογα με τις απαιτήσεις της περίστασης μπορούμε να χρησιμοποιήσουμε τον κατάλληλο συνδυασμό από targets :



Εικόνα 51. Ορισμός παραμέτρων συλλογής artifacts.

Αφού επιλέξουμε targets, τότε μπορούμε εκτελέσουμε την συλλογή των artifacts :



Εικόνα 52. Συλλογή στοιχείων με την χρήση του KAPE

Αφού ολοκληρωθεί η συλλογή τους, τότε μπορούμε να τα αναρτήσουμε στο Kuiper για περαιτέρω ανάλυση, όπως παρουσιάστηκε και προηγουμένως. Επιπλέον ανάλυση, εκτός από το Kuiper, μπορεί να πραγματοποιηθεί με την χρήση των modules του KAPE, δηλαδή διαφόρων προγραμμάτων που χρησιμοποιεί. Το KAPE συνολικά διαθέτει 272 modules.

4.2.10 Suricata

Για την εγκατάσταση του Suricata θα ακολουθήσουμε τα ακόλουθα βήματα [51] :

sudo apt-get install software-properties-common

sudo add-apt-repository ppa:oisf/suricata-stable

sudo apt-get update

Αρχικά , η πρώτη εντολή, sudo apt-get install software-properties-common, εξασφαλίζει ότι το σύστημά διαθέτει τα απαραίτητα εργαλεία για το χειρισμό software repositories. Στη συνέχεια, η εντολή sudo add-apt-repository ppa:oisf/suricata-stable προσθέτει το Suricata Stable στο σύστημά. Τέλος η εντολή sudo apt-get update ανανεώνει το packet index για να συμπεριλάβει το Suricata repository που μόλις προστέθηκε.

Στην συνέχεια , μπορούμε να εγκαταστήσουμε το Suricata :

sudo apt-get install suricata

και για να το ενεργοποιήσουμε :

sudo systemctl start suricata

```
root@LAPTOP-9BKDPUC6:~# systemctl status suricata
● suricata.service - LSB: Next Generation IDS/IPS
     Loaded: loaded (/etc/init.d/suricata; generated)
     Active: active (running) since Thu 2024-11-14 22:39:17 EET; 4 days ago
       Docs: man:systemd-sysv-generator(8)
    Process: 197 ExecStart=/etc/init.d/suricata start (code=exited, status=0/SUCCESS)
      Tasks: 14 (limit: 9527)
     Memory: 133.2M ()
     CGroup: /system.slice/suricata.service
             └─331 /usr/bin/suricata -c /etc/suricata/suricata.yaml --pidfile /var/run/suricata.pid --af-packet -D -vvv

Notice: journal has been rotated since unit was started, output may be incomplete.
root@LAPTOP-9BKDPUC6:~#
```

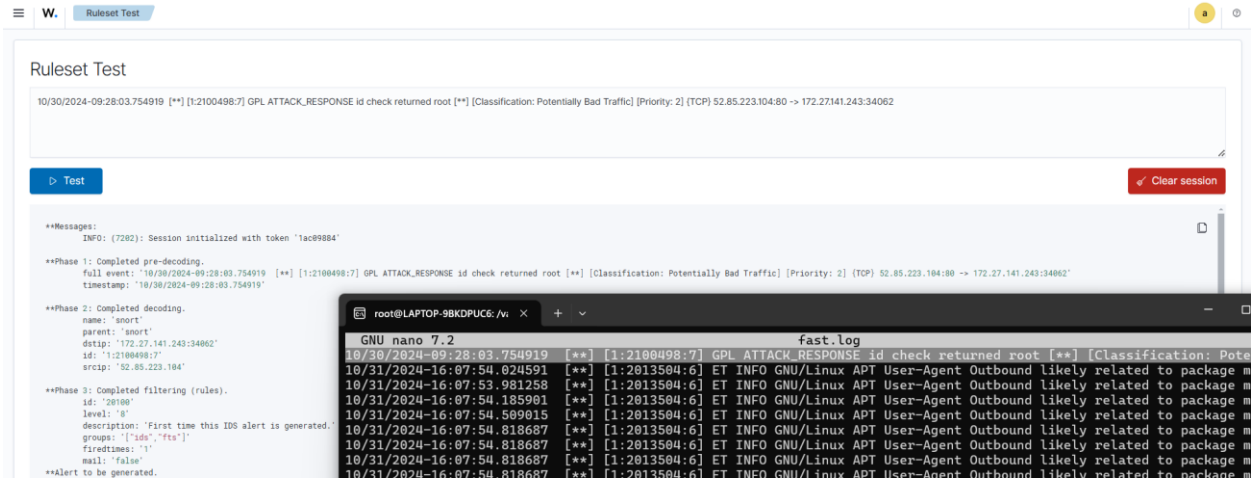
Εικόνα 53. Ενεργοποίηση της υπηρεσίας Suricata

Πλέον το suricata παρακολουθεί το δίκτυο στο endpoint που έχει εγκατασταθεί. Οι κανόνες που χρησιμοποιεί βρίσκονται σε προκαθορισμένη θέση : /var/lib/suricata/rules/suricata.rules. Αναφορικά με τα log files που διατηρεί, έχουμε :

- **eve.json** : Ένα αρχείο καταγραφής σε μορφή JSON που περιέχει λεπτομερείς πληροφορίες συμβάντων, όπως ειδοποιήσεις, αιτήματα HTTP, ερωτήματα DNS, TLS handshakes και άλλα. Είναι ιδιαίτερα προσαρμόσιμο και έχει σχεδιαστεί για ενσωμάτωση με εργαλεία SIEM.
- **fast.log** : Ένα απλοποιημένο, αναγνώσιμο αρχείο καταγραφής που περιέχει μόνο πληροφορίες ειδοποιήσεων σε συνοπτική μορφή, χρήσιμο για βασική παρακολούθηση ειδοποιήσεων ή ανάλυση σε πραγματικό χρόνο.
- **stats.log** : Ένα αρχείο καταγραφής που συνοψίζει στατιστικά στοιχεία επιδόσεων για το Suricata, όπως ρυθμούς επεξεργασίας πακέτων, χρήση μνήμης και χαμένα πακέτα, και ενημερώνεται περιοδικά.
- **suricata-start.log** : Ένα αρχείο καταγραφής που καταγράφει πληροφορίες σχετικά με τη διαδικασία εκκίνησης του Suricata, συμπεριλαμβανομένων ζητημάτων διαμόρφωσης, ενεργοποιημένων λειτουργιών και μηνυμάτων αρχικοποίησης.
- **suricata.log** : Το κύριο αρχείο καταγραφής που καταγράφει γενικές πληροφορίες χρόνου εκτέλεσης, σφάλματα, προειδοποιήσεις και άλλα μηνύματα σχετικά με τη λειτουργία του

Suricata. Βοηθά στη διάγνωση προβλημάτων ή στην παρακολούθηση της δραστηριότητας του Suricata

Από τα παραπάνω log files, επιλέγουμε την παρακολούθηση του fast.log από το Wazuh, όπως φαίνεται στην εικόνα 42.



Εικόνα 54 . Ανάλυση εγγραφών του Suricata από το Wazuh

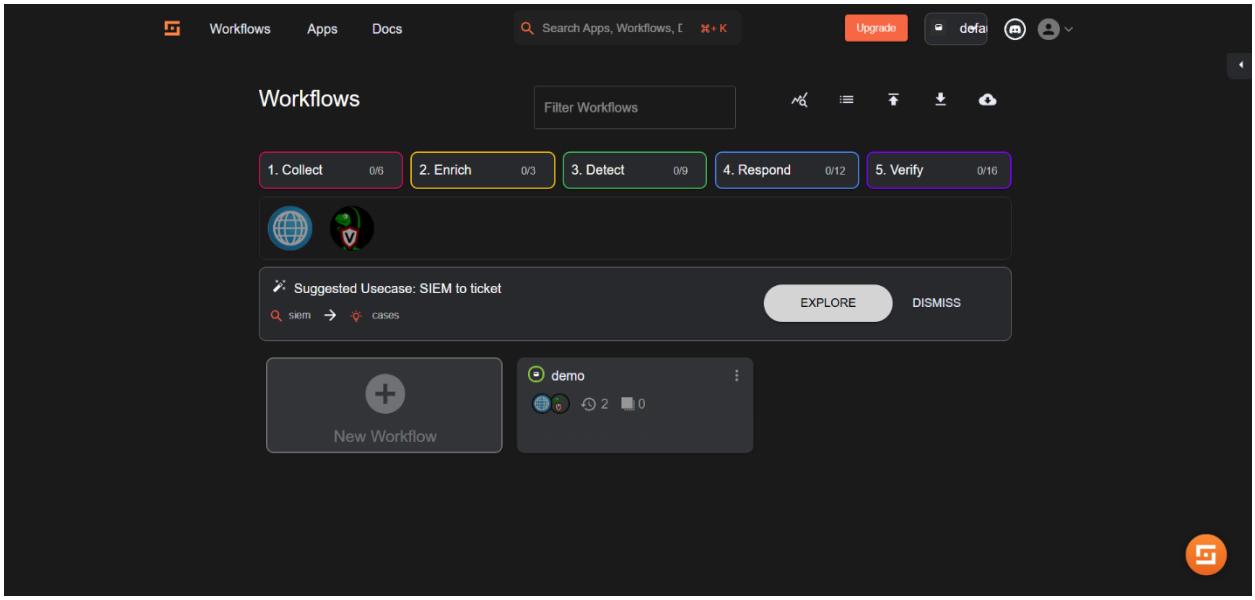
Στην παραπάνω εικόνα παρατηρούμε πως υπάρχει ήδη αποκωδικοποιητής και κανόνες που μπορούν να επεξεργαστούν εγγραφές της μορφής του fast.log . Έτσι alerts από το Suricata περνούν στο Wazuh, και αν απαιτηθεί, προωθούνται και στο Iris.

4.2.11 Shuffle

Για την υλοποίηση του Shuffle χρησιμοποιήσαμε docker. Από [37] θα κατεβάσουμε το πιο πρόσφατο release (σε zip μορφή). Στην συνέχεια θα επεξεργαστούμε το .env αρχείο και θα θέσουμε στην μεταβλητή OUTER_HOSTNAME την τρέχουσα ip. Έπειτα μπορούμε να δημιουργήσουμε το compose stack του shuffle και να ενεργοποιήσουμε τα αντίστοιχα containers :

docker-compose up -d

Τότε το Shuffle θα είναι διαθέσιμο στο url https://<ip>:3443. Όταν συνδεθούμε για πρώτη φορά, θα δημιουργήσουμε και νέο χρήστη, ορίζοντας και τους κωδικούς πρόσβασης. Αφού ολοκληρώσουμε αυτό το στάδιο, και συνδεθούμε με τα στοιχεία που ορίσαμε , θα μπορούμε να δημιουργήσουμε workflows στο shuffle :



Εικόνα 55. Αρχική σελίδα Shuffle

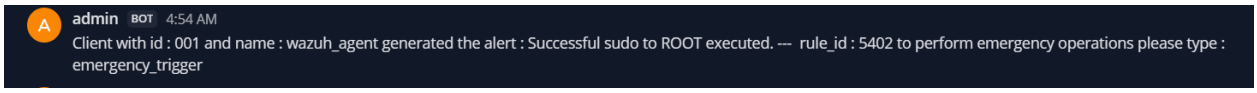
Το Shuffle είναι μια ευέλικτη πλατφόρμα αυτοματοποίησης, ανοιχτού κώδικα, που έχει σχεδιαστεί για την διευκόλυνση των λειτουργιών ασφαλείας και των ροών εργασίας. Επιτρέπει στους χρήστες να δημιουργούν, να προσαρμόζουν και να εκτελούν αυτοματοποιημένες ροές εργασίας χωρίς να χρειάζονται εκτεταμένες δεξιότητες σε γλώσσες προγραμματισμού. Με την άμεση ενσωμάτωση με ένα ευρύ φάσμα εργαλείων, συμπεριλαμβανομένων των SIEMs, των SOARs και των πλατφορμών threat intelligence, το Shuffle δίνει τη δυνατότητα στους οργανισμούς να συνδέουν διαφορετικά συστήματα και να ενορχηστρώνουν σύνθετες διαδικασίες με ευκολία. Η διεπαφή drag-and-drop καθιστά εύληπτο τον σχεδιασμό ροών εργασίας που αυτοματοποιούν επαναλαμβανόμενες εργασίες, βελτιώνουν τους χρόνους απόκρισης σε περιστατικά και βελτιώνουν τη συνολική επιχειρησιακή αποδοτικότητα. Αυτή ακριβώς την λειτουργία του θα εκμεταλλευτούμε και στην πλατφόρμα , δηλαδή, αρχικά θα αναπτύξουμε μια αυτοματοποιημένη ροή απόκρισης σε ειδοποίηση από το Wazuh:

Εικόνα 56. Workflow αντιμετώπισης ειδοποιήσεων από το Wazuh.

Στο παραπάνω Workflow , αρχικά ο Wazuh alerts webhook κόμβος ανιχνεύει τις ειδοποιήσεις του Wazuh. Έχουμε διαμορφώσει κατάλληλα τον κώδικα του /var/ossec/etc/ossec.conf του Wazuh έτσι ώστε να προωθεί τις ειδοποιήσεις του με id 5402 στο Shuffle :

```
<integration>
  <name>shuffle</name>
  <hook_url>https://192.168.40.84:3443/api/v1/hooks/webhook_1eebd0e7-8ae2-410d-8eaf-89b7a1e9e538</hook_url>
  <rule_id>5402</rule_id>
  <alert_format>json</alert_format>
</integration>
```

Μόλις ληφθεί κάποια ειδοποίηση, το webhook του Wazuh την προωθεί στον κόμβο trigger mattermost. Ο κόμβος αυτός δημιουργεί ειδοποίηση στο Mattermost με την εξής μορφή :



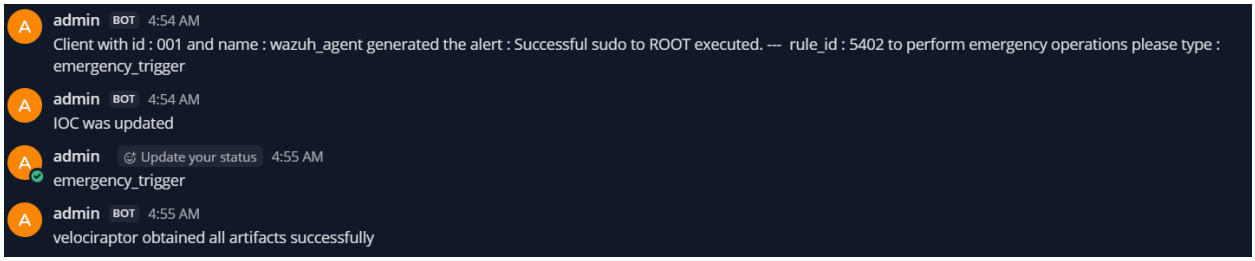
Εικόνα 57. Ειδοποίηση στο Mattermost για έναρξη «emergency» διαδικασιών.

Η παραπάνω ειδοποίηση περιγράφει ότι ο Client Wazuh_agent - ο οποίος έχει εγκατασταθεί σε εικονική μηχανή, για να προσομοιάζει endpoint - δημιούργησε ειδοποίηση με τίτλο Successful sudo to ROOT executed και κωδικό 5402. Αν επιθυμούμε να εκτελέσουμε emergency διαδικασίες, τότε αρκεί να γράψουμε με αυτό το κανάλι : emergency_trigger. Τότε θα ειδοποιηθεί ο κόμβος Mattermost input της εικόνας 55 , ώστε να ξεκινήσει η έκτακτη συλλογή artifacts από το συγκεκριμένο endpoint. Αυτό επιτυγχάνεται με την χρήση VQL (Velociraptor Query Language) ως εξής :

```
LET artfs = ('Generic.Client.DiskSpace','Generic.Client.Info/BasicInformation')
LET collection <= collect_client(
   client_id='C.a9946fccc53b22d7',
   artifacts=artfs, env=dict())
LET _ <= SELECT * FROM watch_monitoring(artifact='System.Flow.Completion')
WHERE FlowId = collection.flow_id
LIMIT 1
LET res <= SELECT * FROM foreach(
row = artfs,
query = {SELECT * FROM source(
  client_id=collection.request.client_id,
  flow_id=collection.flow_id,
  artifact=_value)})
SELECT * FROM res
```

Όπου με την μεταβλητή artfs δηλώνουμε τα artifacts προς συλλογή και με client_id τον velociraptor client που έχει εγκατασταθεί στο συγκεκριμένο endpoint. Οπότε μόλις ολοκληρωθεί η συλλογή των artifacts, αποστέλλεται ειδοποίηση στο mattermost : velociraptor obtained all artifacts successfully ολοκληρώνοντας την emergency διαδικασία.

Συνοπτικά, το σύνολο των ειδοποιήσεων που θα έχουμε στο mattermost, από κανόνα με id 5402 είναι :



Εικόνα 58. Ειδοποιήσεις του Mattermost σε emergency case.

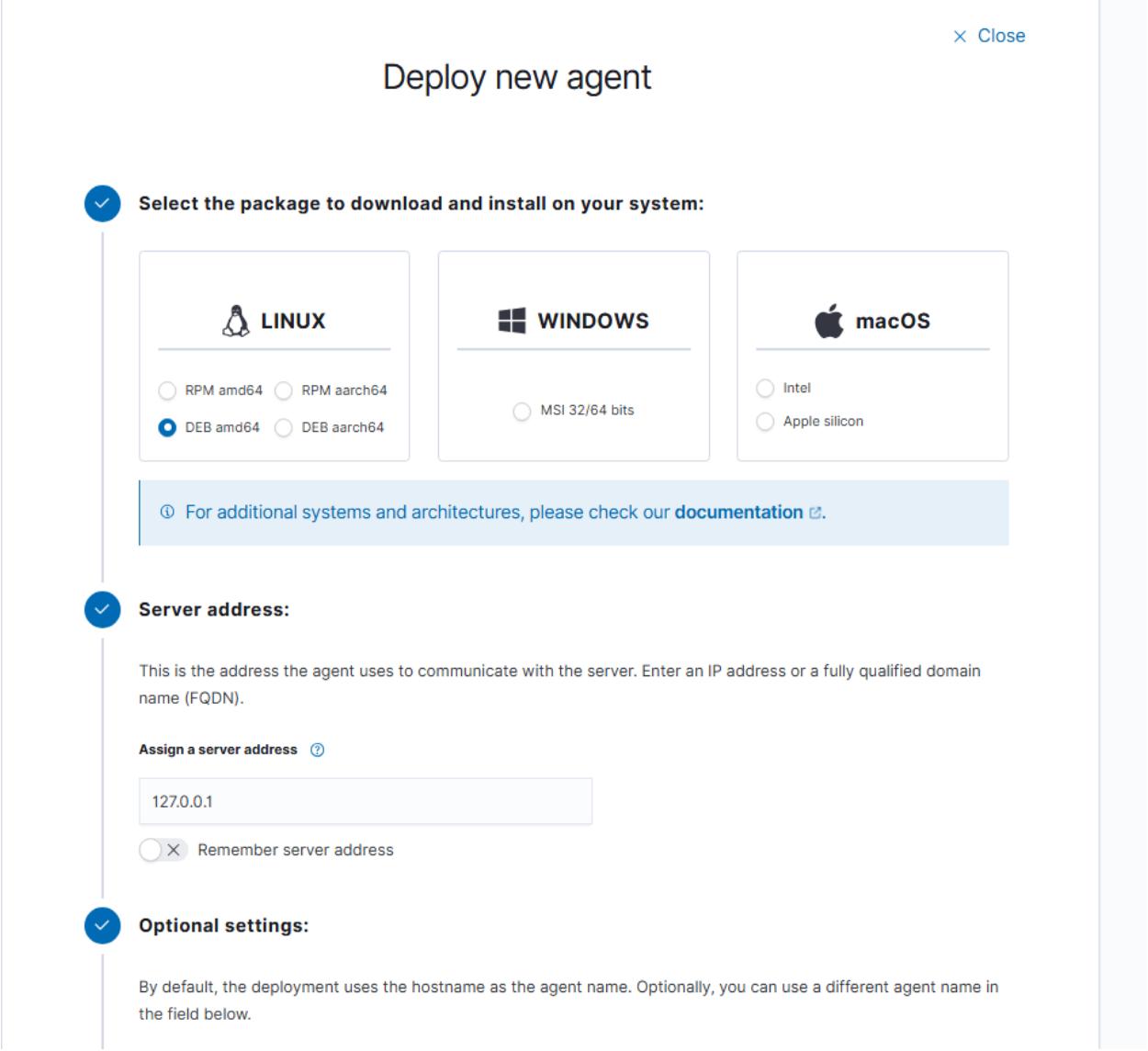
Αρχικά θα λάβουμε την ειδοποίηση για τον συγκεκριμένο κανόνα του Wazuh πως ενεργοποιήθηκε, και στην συνέχεια (IOC was updated) θα ενημερωθούμε από το IRIS πως το alert αυτό έχει προωθεί. Έπειτα, αφού ενεργοποιήσουμε την διαδικασία emergency γράφοντας emergency_trigger και όταν ολοκληρωθεί η συλλογή στοιχείων θα λάβουμε την τελική ειδοποίηση πως τερμάτισε η διαδικασία επιτυχώς.

4.2.12 Εικονική μηχανή ως Endpoint.

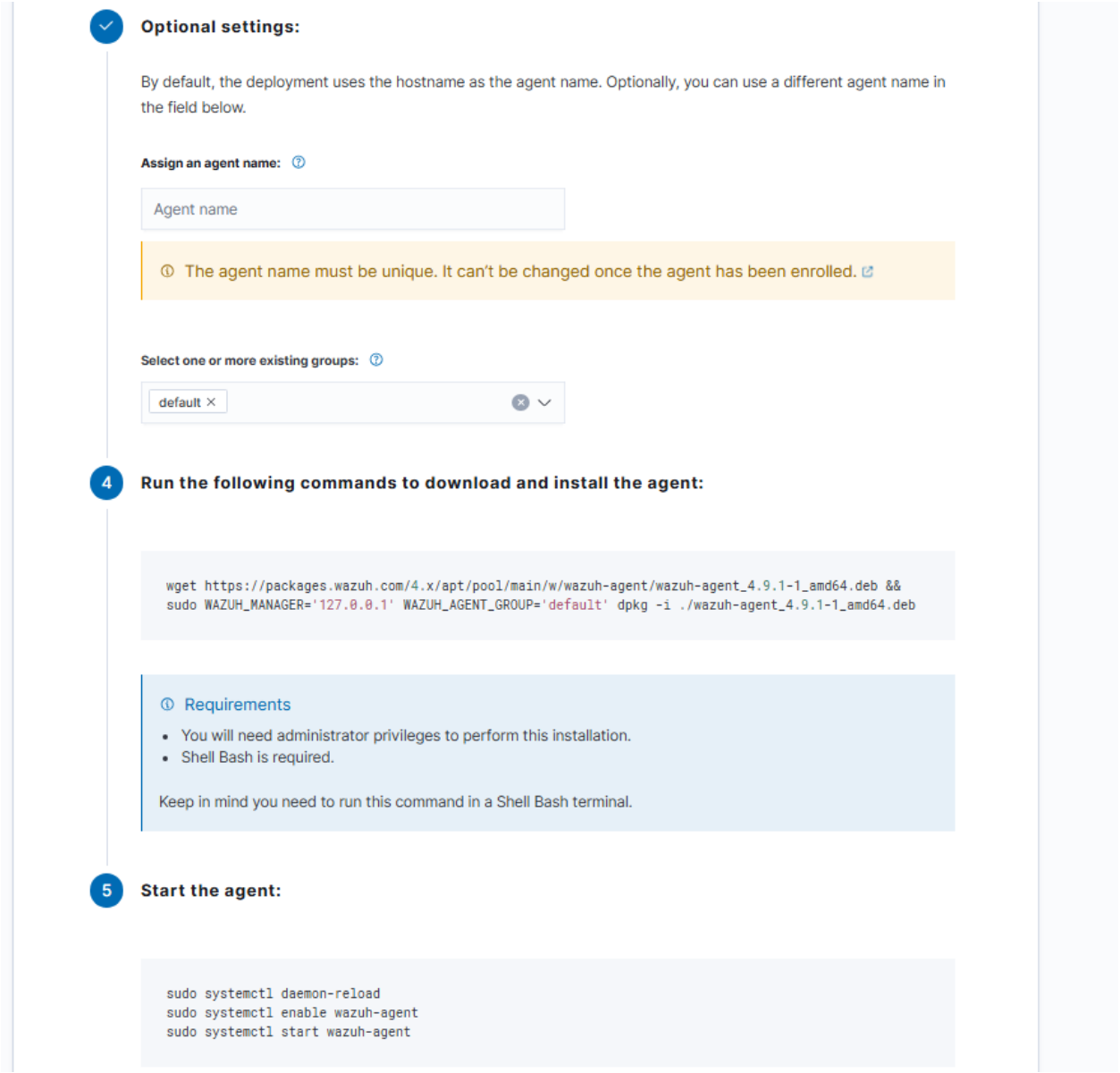
Για την υλοποίηση ενός endpoint, ώστε να παρουσιαστούν οι δυνατότητες επιτήρησης του Wazuh και του Velociraptor σε endpoint, χρησιμοποιήσαμε εικονική μηχανή. Πιο συγκεκριμένα θα χρησιμοποιήσουμε το λογισμικό VirtualBox [53] με λειτουργικό σύστημα διανομής Ubuntu 24.04. Αφού λοιπόν εγκαταστήσουμε το VirtualBox, δημιουργήσουμε μία εικονική μηχανή, ορίσουμε ως λειτουργικό Linux διανομής Ubuntu 24.04 , ορίσουμε και τις επιπλέον παραμέτρους (αριθμός επεξεργαστών , μνήμη κλπ) και την εκκινήσουμε , τότε θα έχουμε :

Εικόνα 59. Εικονική μηχανή που θα χρησιμοποιηθεί ως endpoint

Στα ακόλουθα βήματα θα δημιουργήσουμε έναν Wazuh agent, ο οποίος θα εγκατασταθεί στο virtual machine, και έναν velociraptor client, ώστε να καταστεί δυνατή η παρακολούθηση του endpoint. Αρχικά για τον Wazuh agent έχουμε :



Εικόνα 60. Wazuh Agent Deployment



Εικόνα 61. Wazuh Agent Deployment (συνέχεια)

Η εγκατάσταση του Wazuh agent θα πραγματοποιηθεί μέσω του Wazuh Dashboard, καθώς υπάρχει η επιλογή για δημιουργία νέου agent. Ορίζοντας τις παραπάνω παραμέτρους, προκύπτουν οι εντολές εγκατάστασης .

Για την περίπτωση του velociraptor, οι διαδικασία εγκατάστασης του client, είναι η εξής :

Δημιουργία ενός Debian πακέτου με ενσωματωμένο αρχείο ρυθμίσεων :

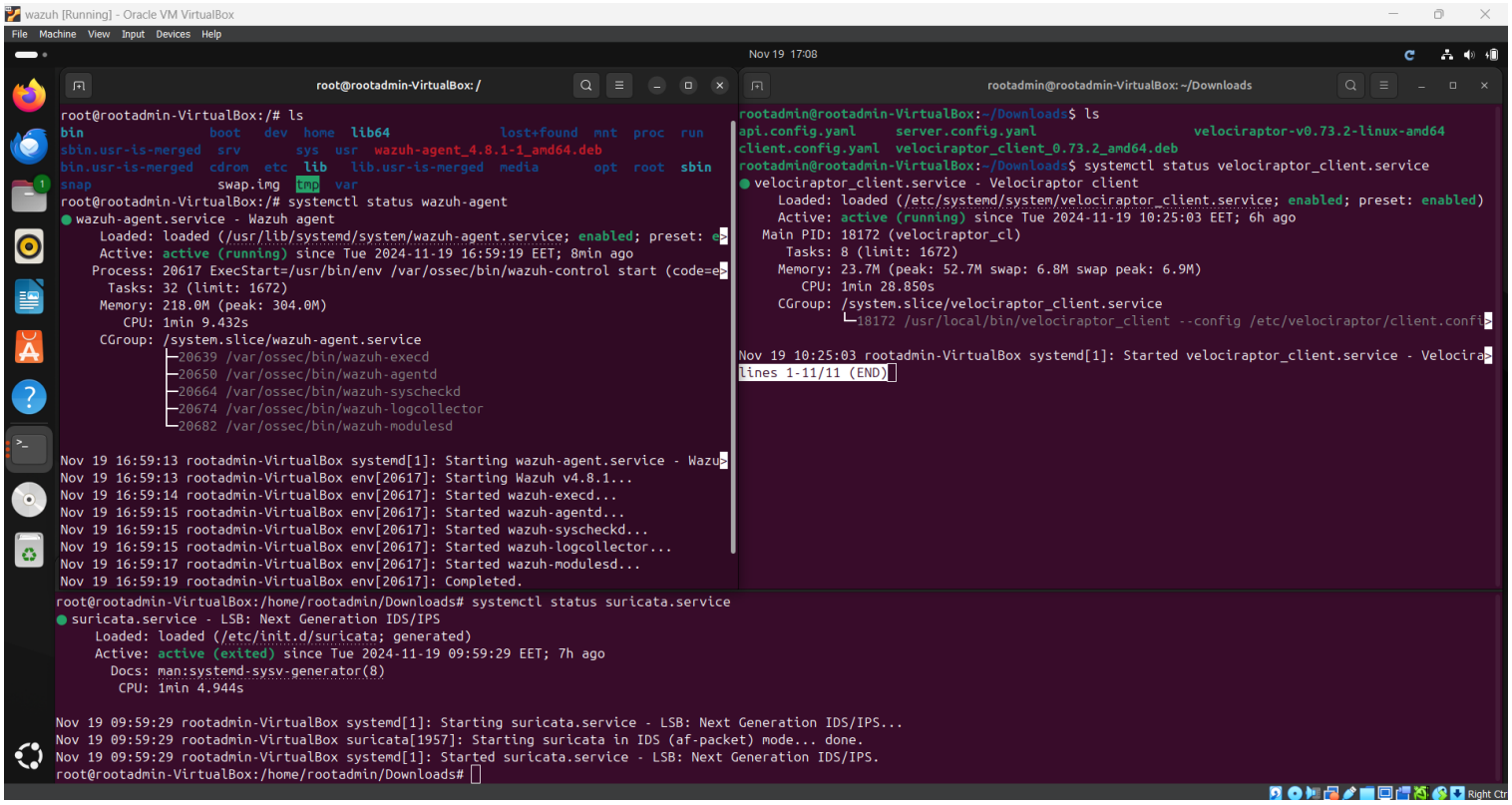
velociraptor-vx.x.x-linux-amd64 --config client.config.yaml debian client

Εγκατάσταση του πακέτου :

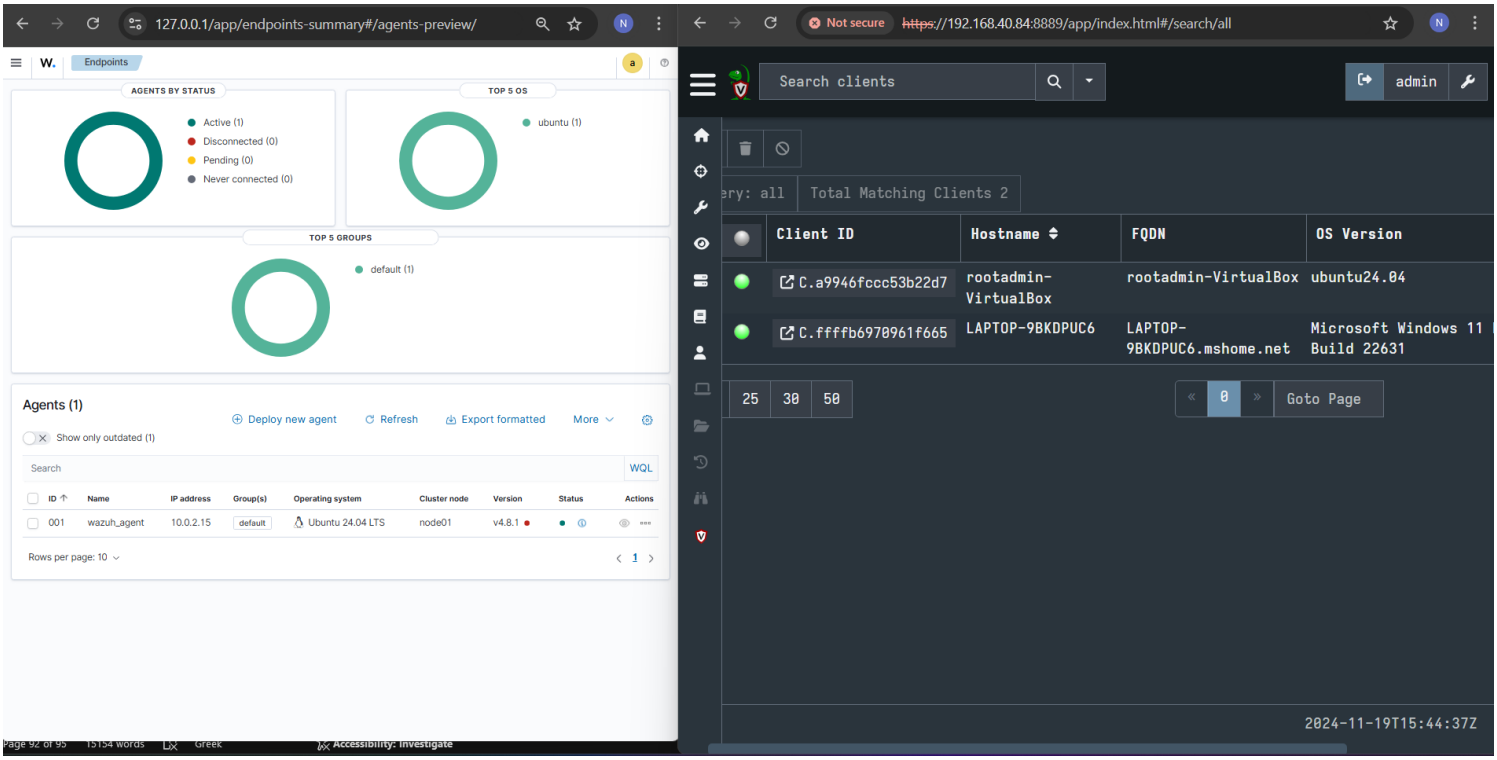
sudo dpkg -i velociraptor_x.x.x_client.deb

Τέλος έχουμε εγκαταστήσει και το Suricata για επιπλέον δυνατότητες NDR του endpoint, και το Wazuh-agent παρακολουθεί τα αρχεία καταγραφής του, όπως και στον host.

Συνολικά λοιπόν έχουμε :



Εικόνα 62. Υπηρεσίες Wazuh-agent, Velociraptor Client και Suricata στην εικονική μηχανή - endpoint.



Εικόνα 63. Παρακολούθηση του Wazuh agent και velociraptor client μέσα από τα αντίστοιχα Dashboards.

Στις εικόνες 60 και 61 παρουσιάζεται η διασύνδεση του Wazuh και του Velociraptor με Endpoints. Η ίδια διαδικασία μπορεί να πραγματοποιηθεί για περισσότερα από ένα συστήματα, επιτρέποντας την πλήρη παρακολούθηση τους για παραβιάσεις ασφάλειας.

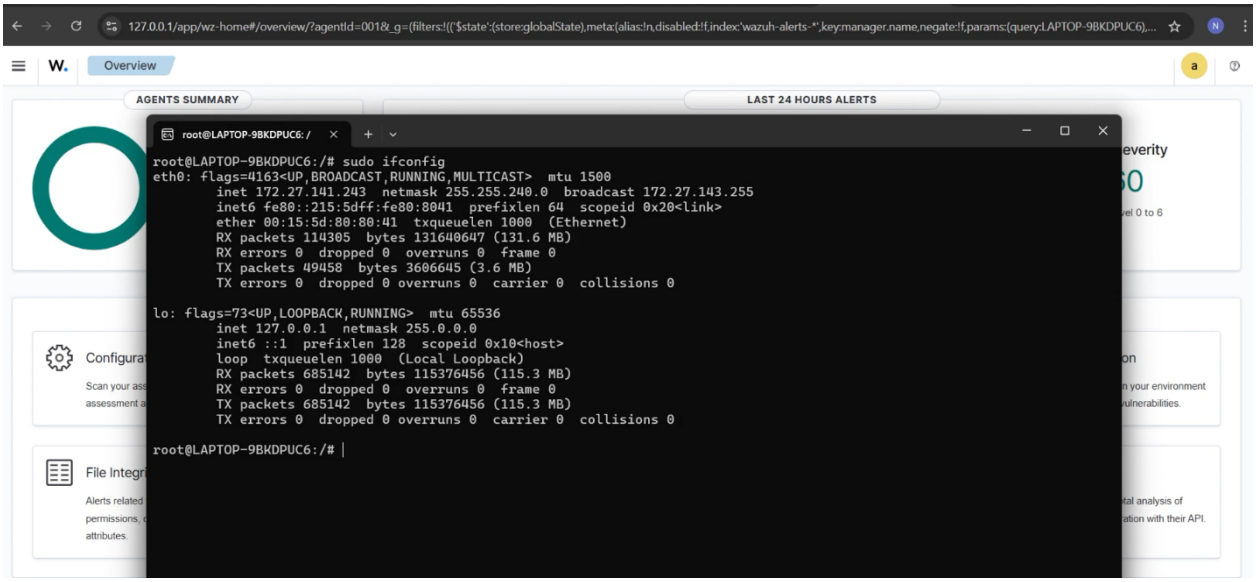
Συνολικά, στο κεφάλαιο αυτό παρουσιάστηκε ο τρόπος εγκατάστασης, διασύνδεσης και η βασικές λειτουργίες των εργαλείων ασφάλειας που απαρτίζουν την πλατφόρμα. Για την επιλογή τους εργαλείων καθοριστικό ρόλο είχαν οι ιδιότητες και οι παροχές τους, έτσι ώστε συνδυαστικά να υλοποιήσουν μία πλατφόρμα διαχείρισης κυβερνοεπιθέσεων, αντάξιας των commercial λύσεων. Βασικό χαρακτηριστικό της πλατφόρμας αυτής είναι ο modular σχεδιασμός της, ο οποίος επιτρέπει την αντικατάσταση των εργαλείων της με οποιοδήποτε εργαλείο παρόμοιων ιδιοτήτων επιθυμεί ο εκάστοτε οργανισμός καθιστώντας της ευπροσάρμοστη σε ποικίλες συνθήκες.

5. Επίδειξη λειτουργίας πλατφόρμας.

Σε αυτό το κεφάλαιο θα παρουσιαστεί η δυνατότητα παρακολούθησης και η διαδικασία προσδιορισμού, διαχείρισης και αντιμετώπισης ενός περιστατικού ασφάλειας και στον host αλλά και στην εικονική μηχανή - endpoint. Το συγκεκριμένο περιστατικό, θα είναι εκτέλεση της εντολής sudo (superuser do) από root πού έχει ήδη δικαιώματα διαχειριστή. Τέτοια ενέργεια δημιουργεί ειδοποίηση στο Wazuh με περιγραφή : Successful sudo to ROOT executed. , κωδικό κανόνα που ενεργοποιήθηκε : 5402 και επίπεδο επικινδυνότητας : 3. Σκοπός είναι να χρησιμοποιηθούν και να παρουσιαστεί η λειτουργία όσο το δυνατόν περισσότερων εργαλείων της πλατφόρμας, καθώς πρόκειται για ένα μεμονωμένο γεγονός, και η πλατφόρμα είναι σχεδιασμένη να διαχειρίζεται και να αποκρίνεται σε ένα ευρύ φάσμα περιστατικών.

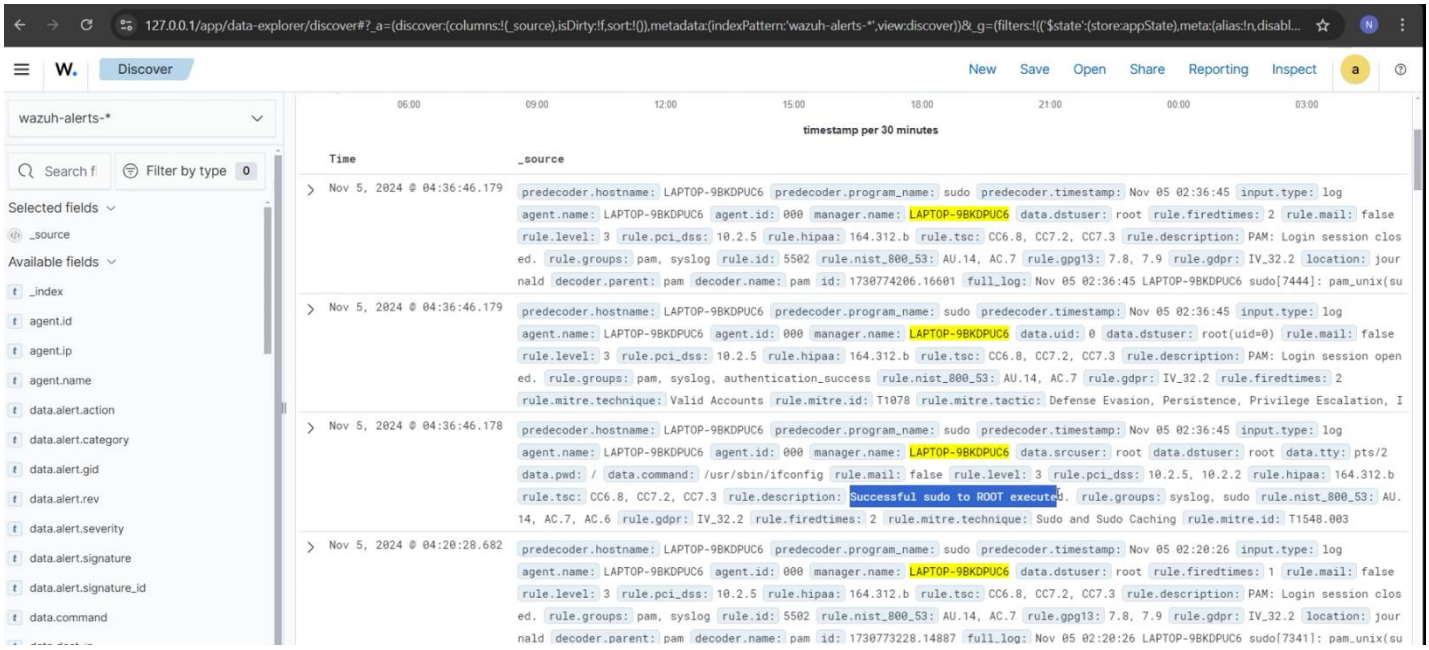
Αρχικά λοιπόν, θα εκτελεστεί η παρακάτω εντολή (Εικόνα 64) με δικαιώματα διαχειριστή στο wsl command line:

sudo ifconfig



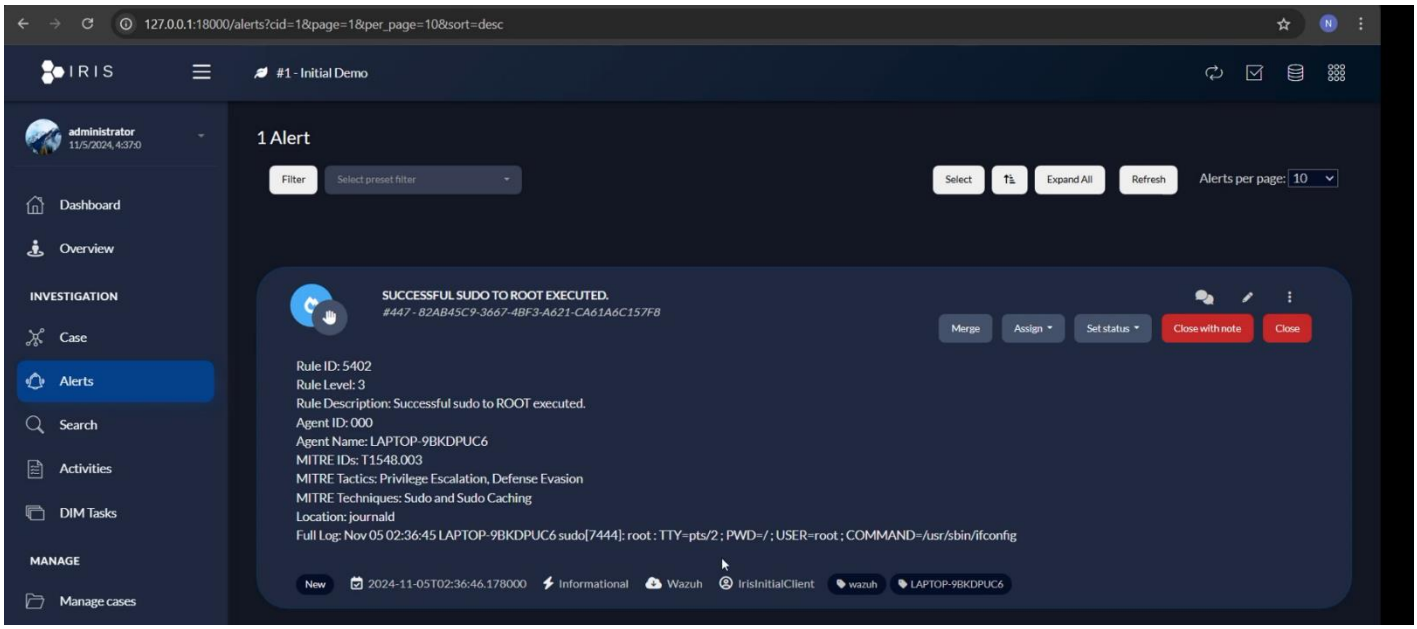
Εικόνα 64. Εκτέλεση της εντολής sudo ifconfig με δικαιώματα διαχειριστή

Στην συνέχεια θα εξετάσουμε το Wazuh Dashboard για να εντοπίσουμε την ειδοποίηση που δημιουργήθηκε :



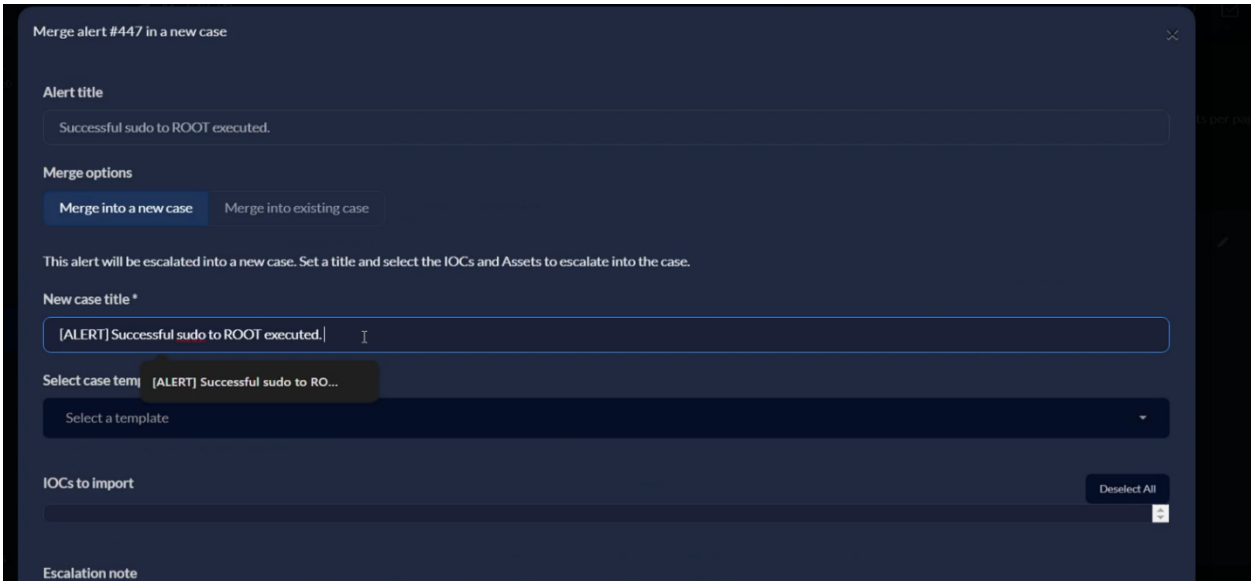
Εικόνα 65. Successful sudo to ROOT execution ειδοποίηση για την εκτέλεση της εντολής

Έπειτα, η ειδοποίηση αυτή θα προωθεί στο IRIS :



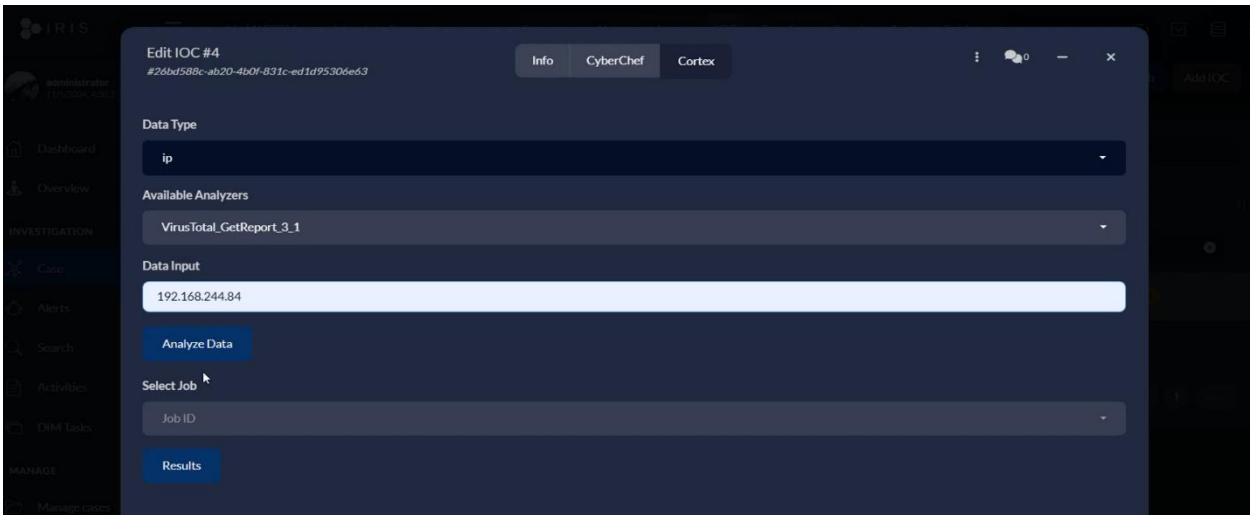
Εικόνα 66. Προώθηση ειδοποίησης Successful sudo to ROOT execution στο IRIS.

Επόμενη ενέργεια είναι να δημιουργήσουμε νέο Case από την συγκεκριμένη ειδοποίηση :

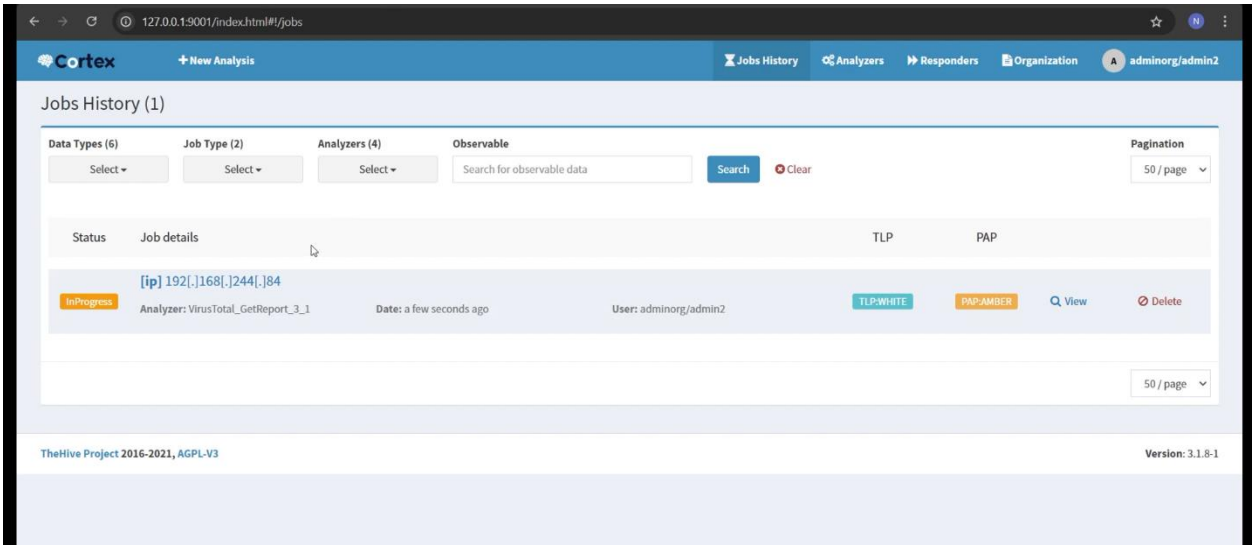


Εικόνα 67. Δημιουργία νέου Case από την ειδοποίηση Successful sudo to ROOT execution

Στην συνέχεια, ανάλογα με τα δεδομένα που διαθέτουμε σε κάθε περίπτωση, μπορούμε να δημιουργήσουμε Asset και IOC για το Case. Για αυτό το περιστατικό, θα δημιουργήσουμε νέο windows computer asset με το όνομα του συστήματος που δημιούργησε την ειδοποίηση δηλαδή LAPTOP-9BKDPUC6 και την διεύθυνση του, που στην συγκεκριμένη περίσταση ήταν 192.168.244.84.Επόμενη ενέργεια είναι να δημιουργήσουμε IOC τύπου ip και να εισάγουμε την παραπάνω διεύθυνση. Έτσι θα μπορούμε να χρησιμοποιήσουμε τα εργαλεία ανάλυσης του Cortex για το συγκεκριμένο IOC :

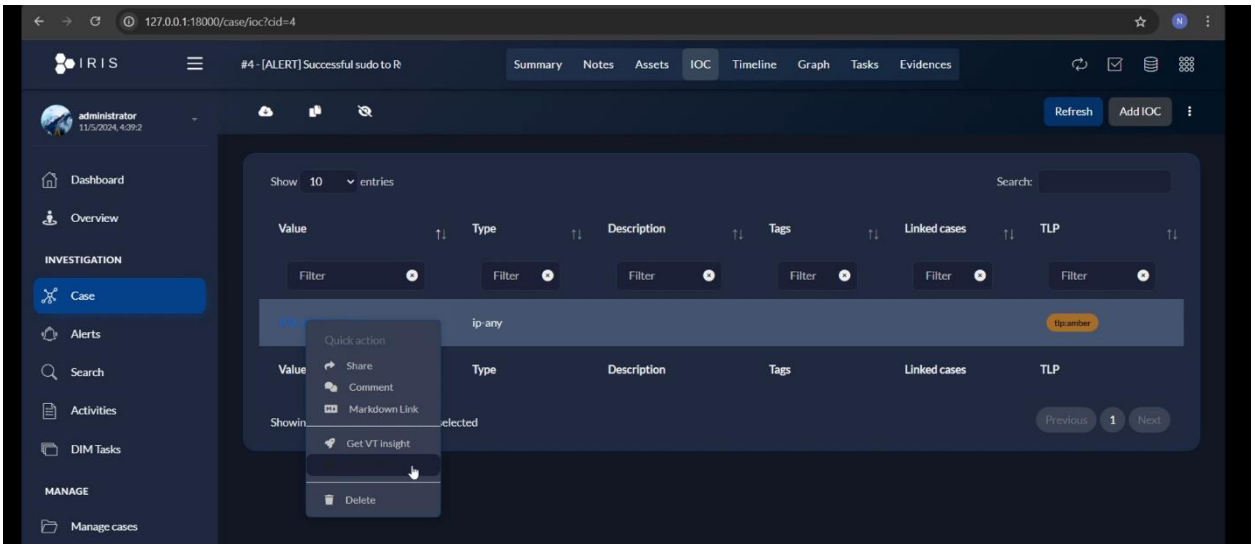


Εικόνα 68. Χρήση Cortex για την ανάλυση του IOC.



Εικόνα 69. Δημιουργία εργασίας ανάλυσης της ip στο Cortex, μέσω του IRIS.

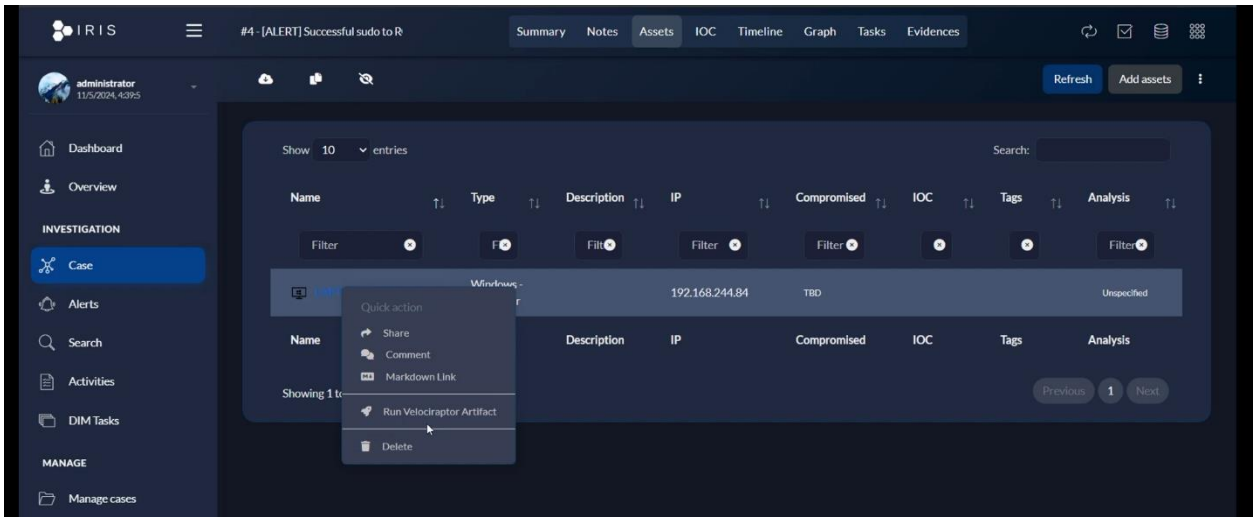
Άκολούθως, μπορούμε να εμπλουτίσουμε τα δεδομένα του IOC με σχετικές πληροφορίες από το MISP, αν υπάρχουν :



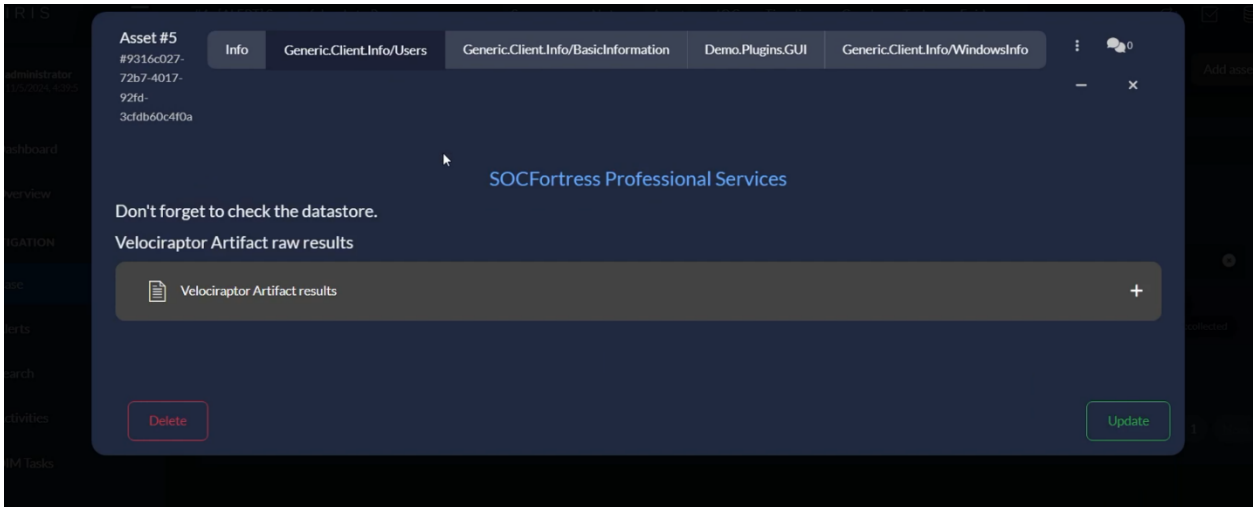
Εικόνα 70. Λήψη σχετικών δεδομένων με το IOC από το MISP.

Εικόνα 71. Αποτελέσματα χρήσης του IRIS MISP module.

Στην συγκεκριμένη περίπτωση, καθώς δεν έχουμε εισάγει καμία πληροφορία για περιστατικά στην βάση του MISP, επιστρέφεται κενό αποτέλεσμα. Επόμενο βήμα είναι να συλλέξουμε artifacts από το συγκεκριμένο endpoint, με την χρήση του velociraptor :



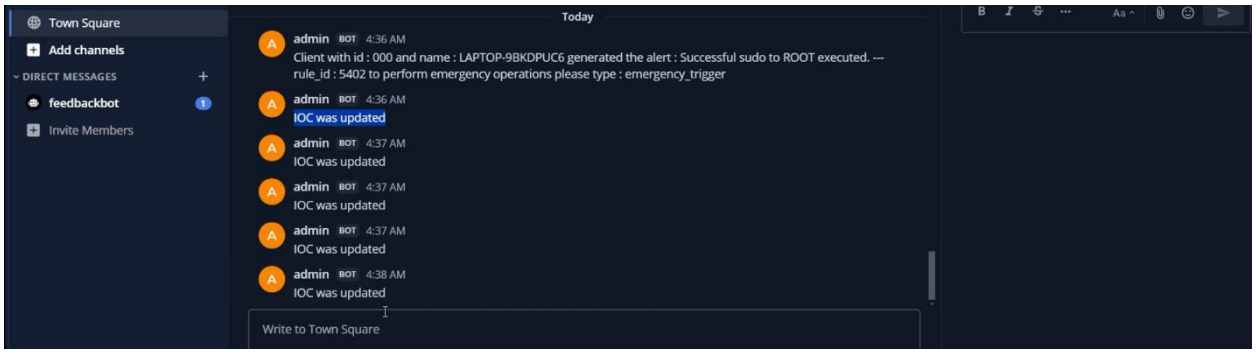
Εικόνα 72. Χρήση του velociraptor για την συλλογή των artifacts.



Εικόνα 73. Αποτελέσματα συλλογής των artifacts.

Παρατηρούμε πως στο asset παρουσιάζονται δύο είδη αποτελεσμάτων, ευρήματα του Generic.Client.Info και του Demo.Plugins.GUI, διαπιστώνοντας με αυτόν τον τρόπο, την σωστή λειτουργία της τροποποίησης του Velociraptor Module.

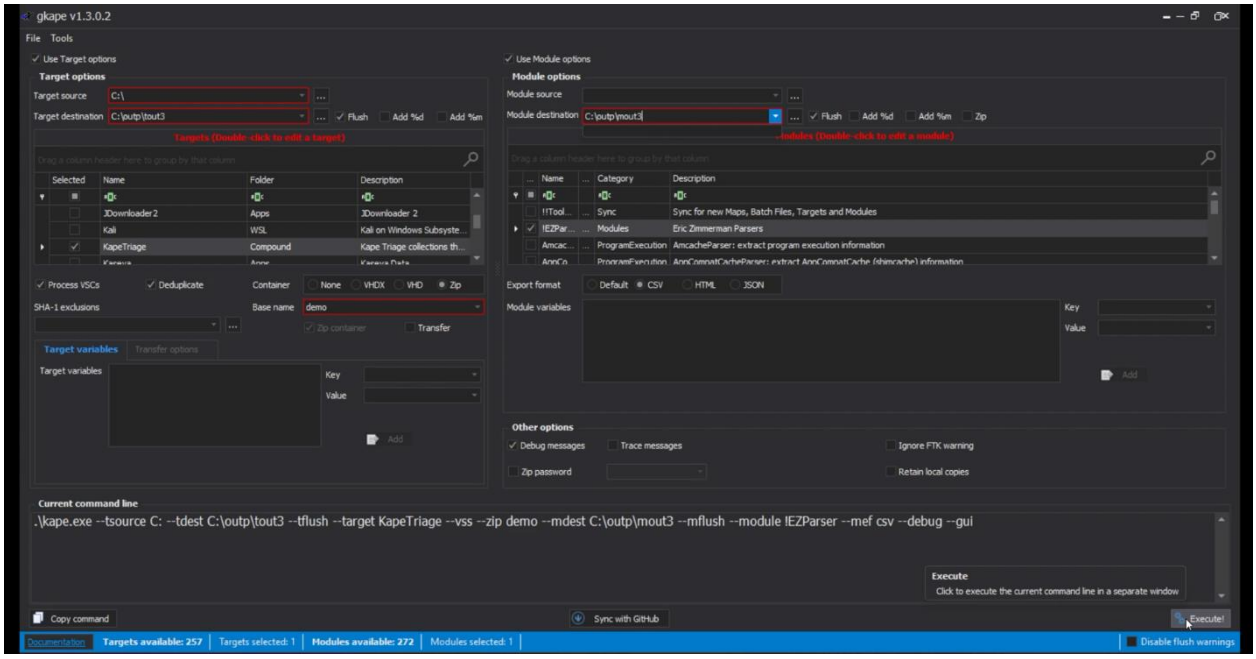
Στην συνέχεια θα εξετάσουμε το Mattermost για σχετικές ειδοποιήσεις :



Εικόνα 74. Ειδοποιήσεις Mattermost

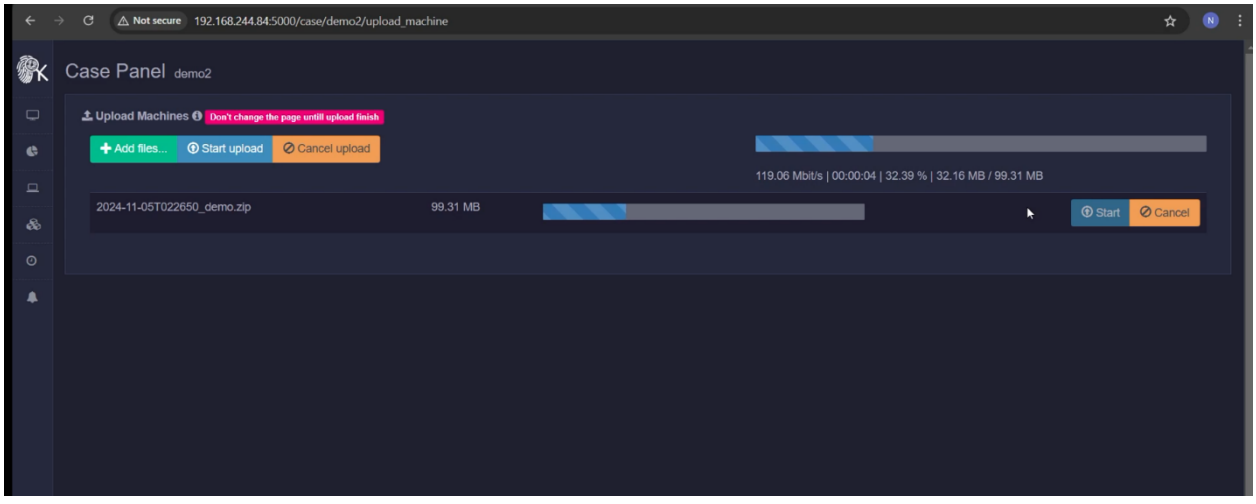
Εδώ εντοπίζουμε δύο είδη ειδοποιήσεων, η πρώτη ειδοποίηση που αναφέρεται στην emergency διαδικασία του Shuffle που θα παρουσιαστεί αργότερα, και την dummy ειδοποίηση IOC was updated, που για σκοπούς ελέγχου λειτουργικότητας, έχει τεθεί να δημιουργείται σε όλες τις ενέργειες που πραγματοποιούνται στο IRIS (δημιουργια alert, case, asset, ioc κλπ).

Έπειτα θα χρησιμοποιήσουμε το KAPE, για περαιτέρω συλλογή στοιχείων :



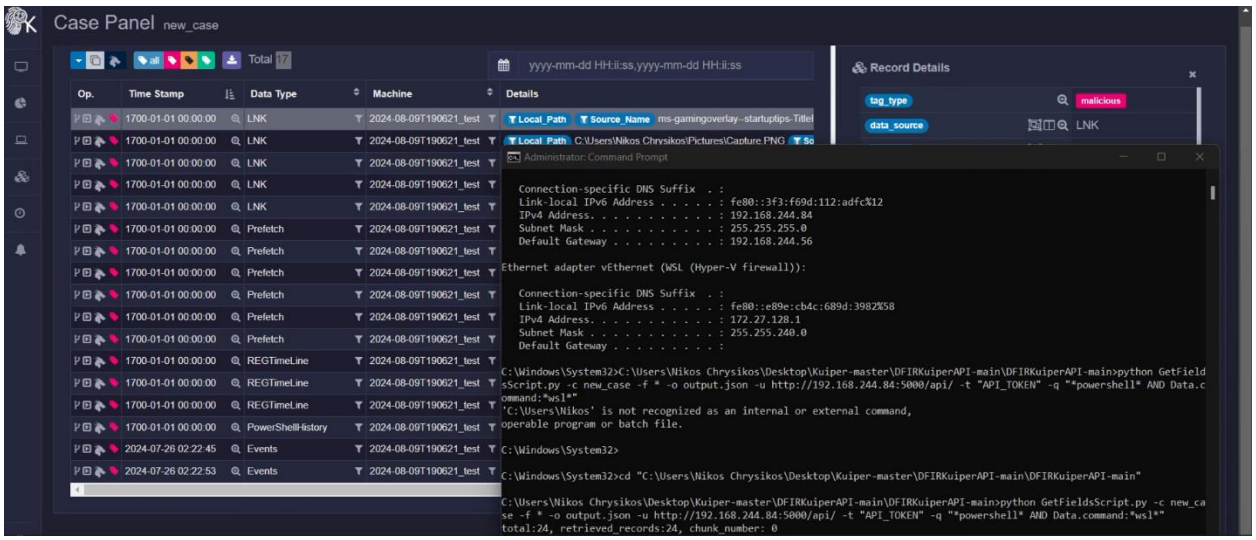
Εικόνα 75. Χρήση του KAPE για την συλλογή artifacts, και την ανάλυση τους με την χρήση module.

Στην παραπάνω εικόνα παρουσιάζεται η χρήση του KAPE στην συγκεκριμένη περίπτωση. Το KAPE θα συλλέξει τα δεδομένα που θα εντοπίσει το επιλεγμένο target (KapeTriage) στον δίσκο C, και θα τα αποθηκεύσει συνολικα σε συμπιεσμένο φάκελο με το όνομα demo. Θα εξετάσει επιπλέον και Volume Shadow Copies αν υπάρχουν, και θα διαγράψει διπλότυπες εγγραφές. Επιπλέον θα χρησιμοποιηθεί και το Module !EZParser για την ανάλυση των συλλεχθέντων στοιχείων και παραγωγή αποτελεσμάτων από το KAPE. Ωστόσο δεν σημειώνουν ιδιαίτερο ενδιαφέρον, καθώς το Kuiper που θα χρησιμοποιήσουμε στο επόμενο βήμα πραγματοποιεί βαθύτερη και πιο αποτελεσματική και πρακτική ανάλυση. Έτσι λοιπόν θα δημιουργήσουμε νέο case στο Kuiper και θα αναρτήσουμε τα δεδομένα που συλλέξαμε με το KAPE :



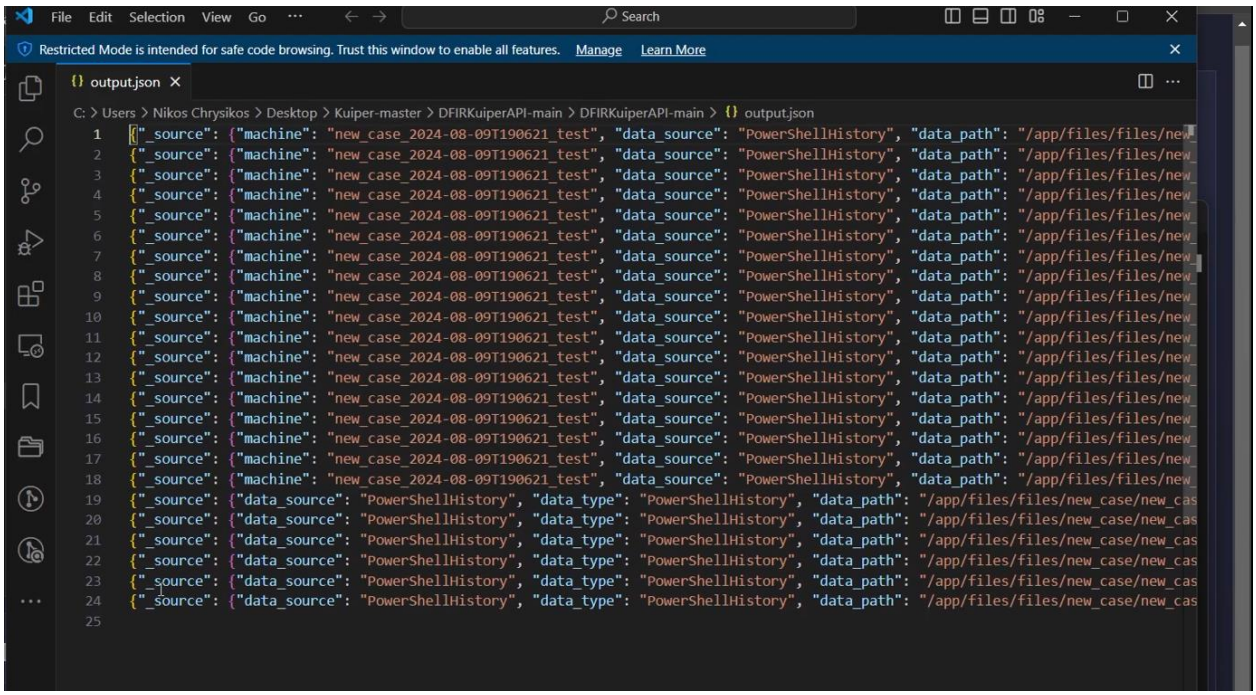
Εικόνα 76. Ανάρτηση συλλεχθέντων δεδομένων του KAPE στο Kuiper για ανάλυση.

Αφού ολοκληρωθεί η ανάρτηση τους, τότε μπορούμε να τα αναλύσουμε και να λάβουμε τα εξής artifacts :



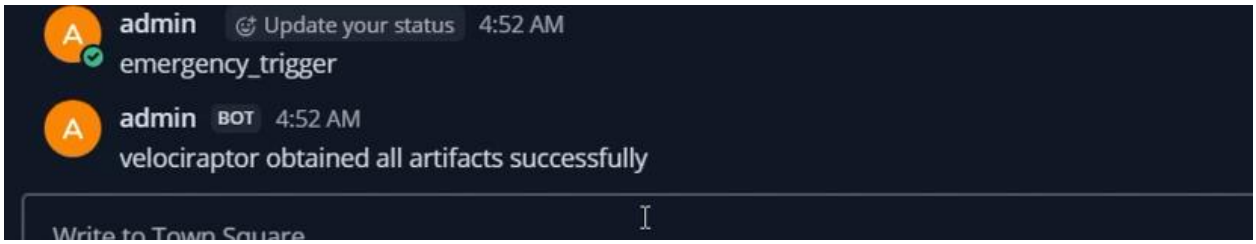
Εικόνα 77. Εξαγωγή των artifacts ενδιαφέροντος ,που δημιουργήθηκαν από την ανάλυση δεδομένων του KAPE, σε μορφή json

Στην παραπάνω εικόνα αρχικά φαίνονται τα αποτελέσματα της ανάλυσης του Kuiper. Στην συνέχεια χρησιμοποιούμε το αρχείο python GetFieldsScript ώστε να επεξεργαστούμε τα artifacts αυτά, και με την χρήση ερωτήματος, να αποθηκεύσουμε σε μορφή json αυτά που μπορεί να μας ενδιαφέρουν. Εδώ αποθηκεύουμε artifacts που σχετίζονται με την εκτέλεση εντολής wsl σε powershell.



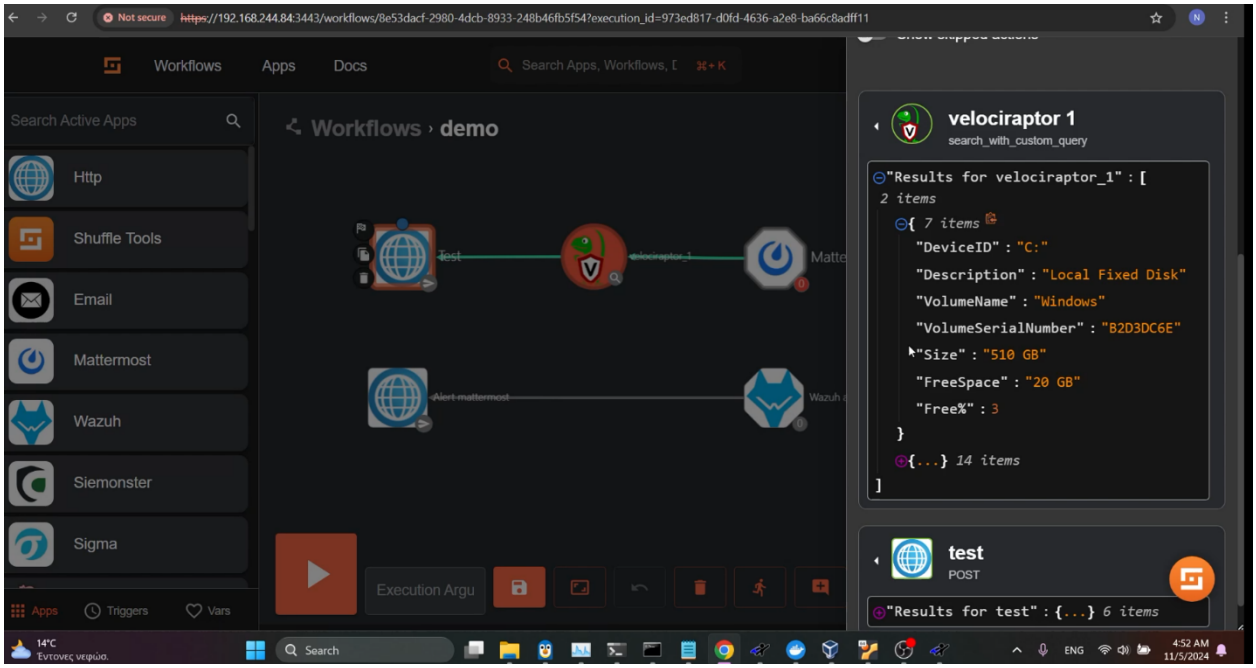
Εικόνα 78. Artifacts του Kuiper σε επεξεργάσιμη μορφή json

Αφού έχουμε πραγματοποιήσει την συλλογή δεδομένων από το σύστημα ενδιαφέροντος, πλέον μπορούμε να προβούμε σε διαδικασία emergency (θα μπορούσε να περιλαμβάνει τον αποκλεισμό του συστήματος από το δίκτυο). Έτσι, όπως έχει περιγραφεί, για την ενεργοποίηση της διαδικασίας, αρκεί να γράψουμε emergency_trigger στο κανάλι Town Square του Mattermost :



Εικόνα 79. Ενεργοποίηση και ολοκλήρωση διαδικασίας emergency

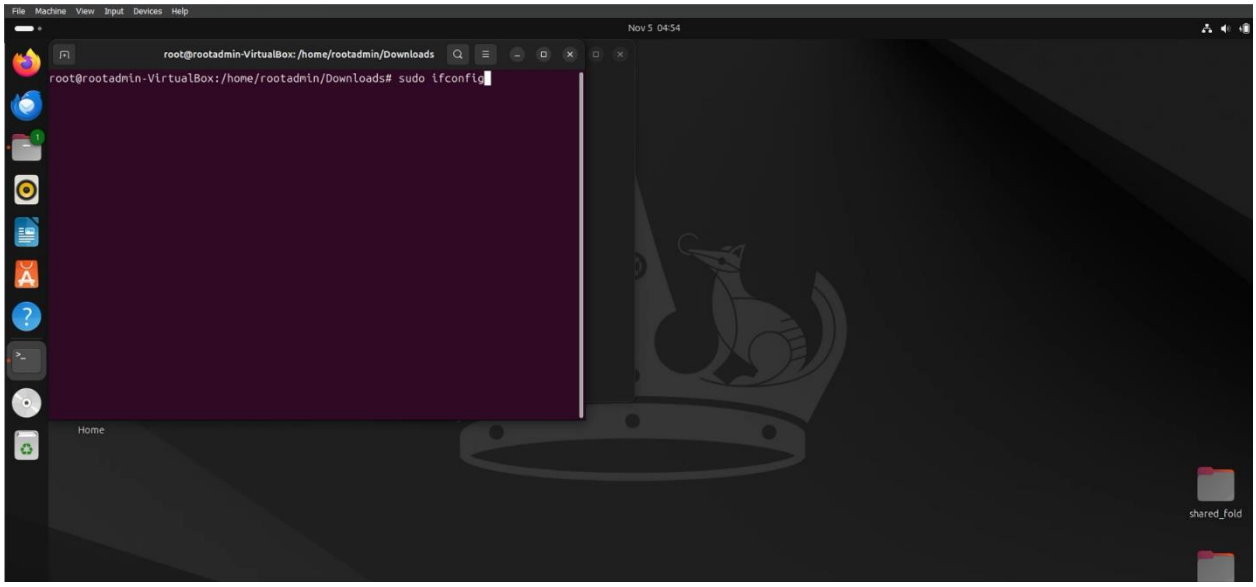
Το μήνυμα velociraptor obtained all artifacts successfully υποδεικνύει ότι η διαδικασία emergency ολοκληρώθηκε επιτυχώς και τα artifacts συγκεντρώθηκαν από το velociraptor :



Εικόνα 80. Αποτελέσματα συλλογής artifacts από το Velociraptor.

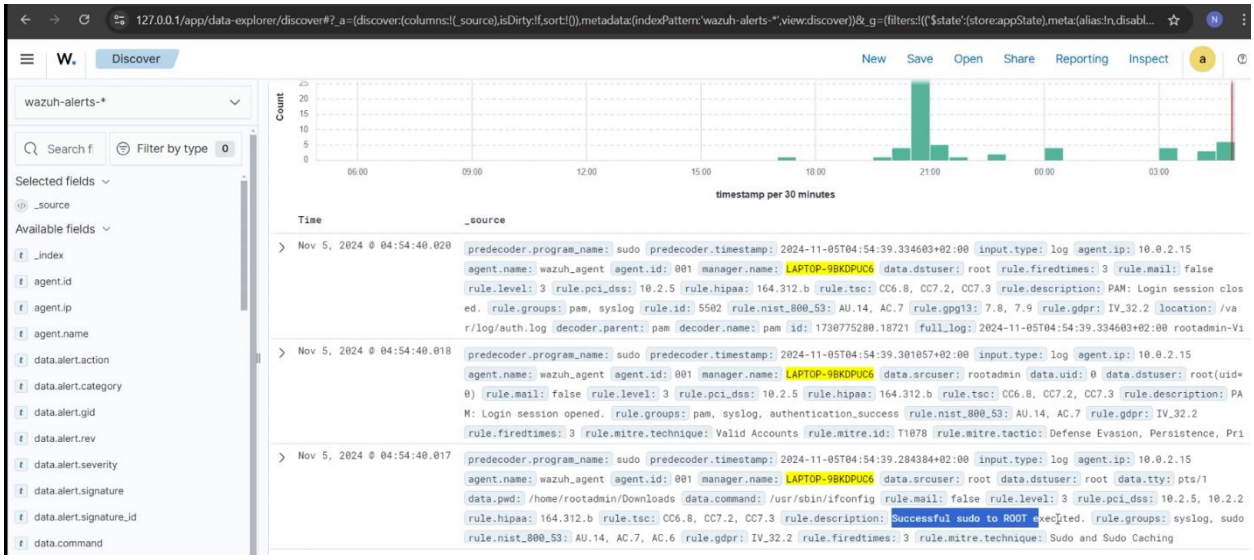
Σε αυτή την υλοποίηση, το velociraptor έχει προγραμματιστεί ώστε να συλλέγει δύο artifacts, Client.Generic.DiskSpace και Client.Generic.DiskUsage, και να παρουσιάζει τα αποτελέσματα τους.

Με αυτό το βήμα ολοκληρώνεται η παρουσίαση για την λειτουργία της πλατφόρμας σε περιστατικό στον host. Απομένει να εκδηλωθεί η αποτελεσματικότητα της στην επιτήρηση διαφορετικού endpoint. Τον ρόλο αυτόν διαδραματίζει η εικονική μηχανή που χρησιμοποιούμε , με λογισμικό Linux διανομής Ubuntu 24.04. Συνεπώς και σε αυτή την περίπτωση θα ακολουθήσουμε την ίδια διαδικασία (το περιστατικό θα είναι Successful sudo to ROOT execution):



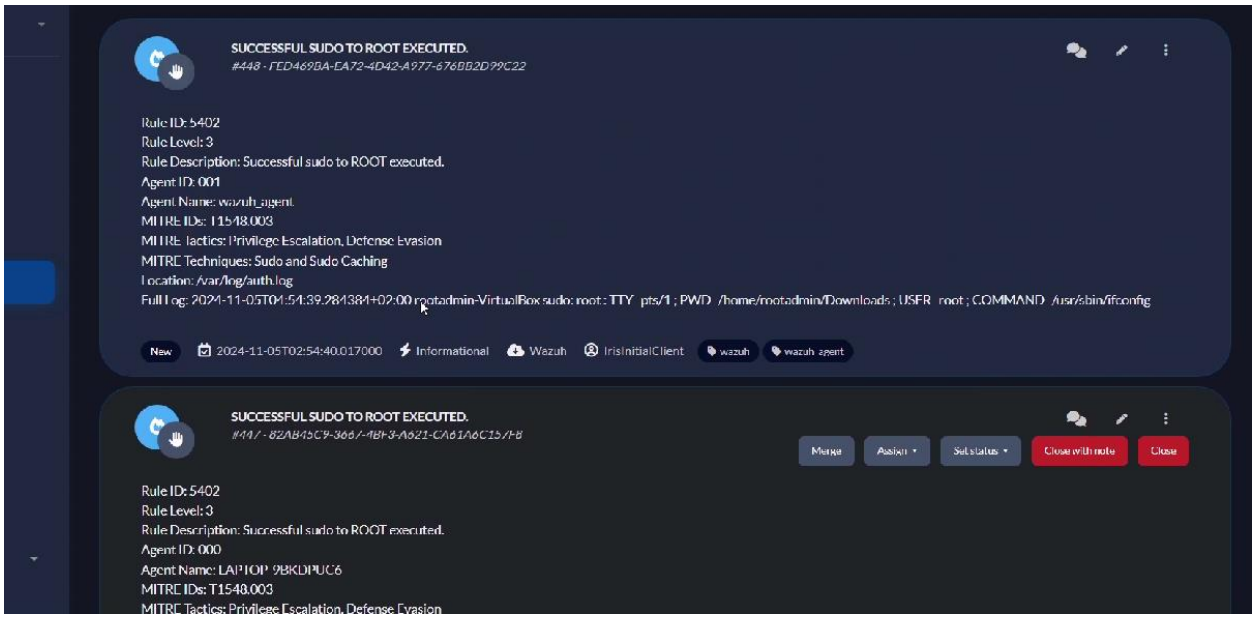
Εικόνα 81. Εκτέλεση εντολής sudo ifconfig με δικαιώματα διαχειριστή στην εικονική μηχανή

Όπως είναι αναμενόμενο, θα έχει δημιουργηθεί ειδοποίηση από τον Wazuh agent και είναι προσβάσιμη στο Dashboard :



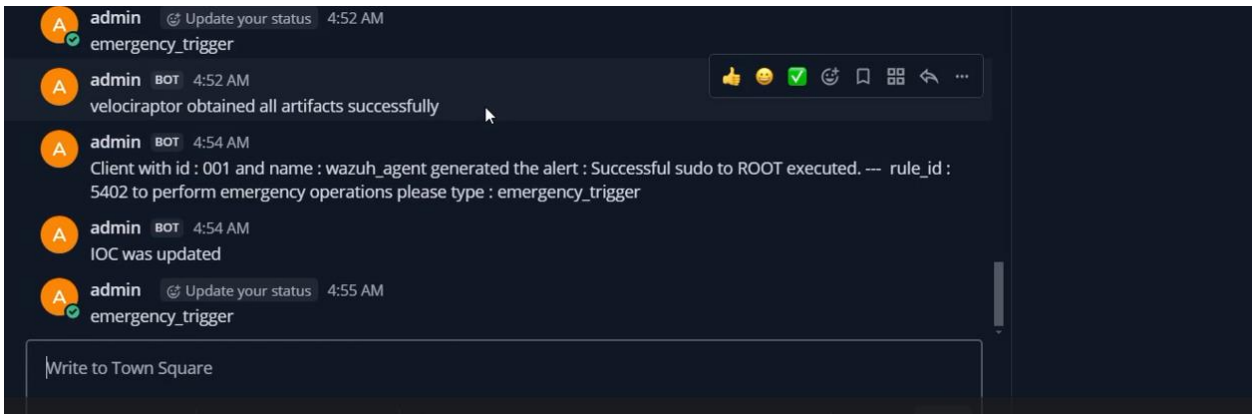
Εικόνα 82. Ειδοποίηση Successful sudo to ROOT execution από Wazuh agent της εικονικής μηχανής.

Στην συνέχεια, όπως και στην περίπτωση του Host, θα δημιουργηθεί ειδοποίηση στο IRIS.



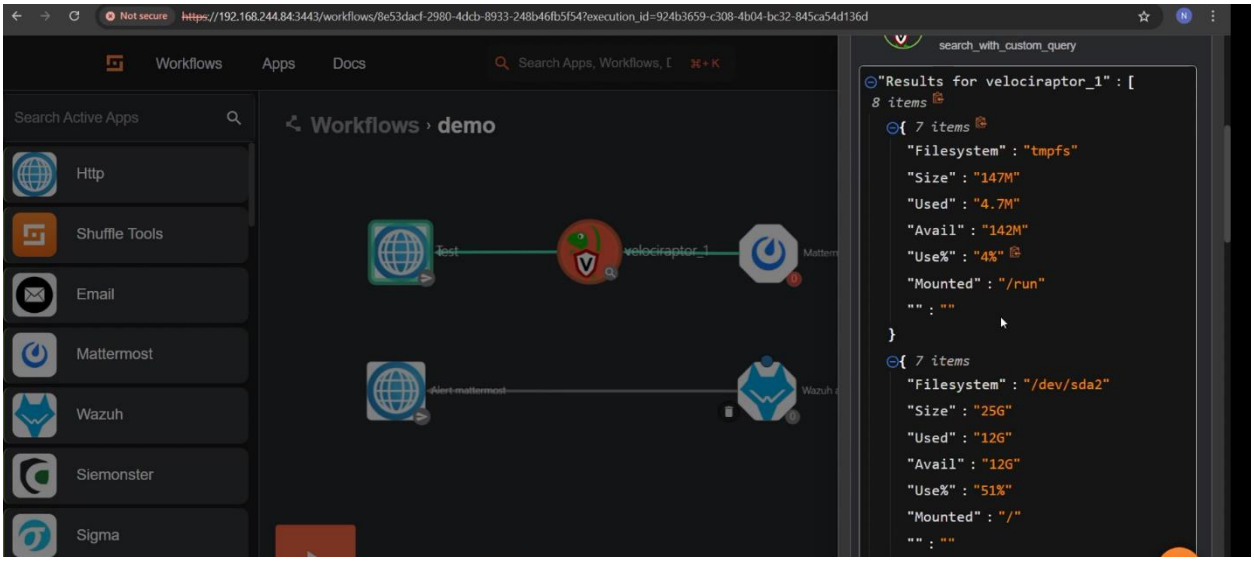
Εικόνα 83 . Προώθηση ειδοποίησης στο IRIS από το Wazuh

Στην συνέχεια, η ανάλυση των δεδομένων ακολουθεί την ίδια διαδικασία (χρήση Cortex και MISP για ανάλυση IoC, χρήση Velociraptor για την συλλογή artifacts του Asset). Δεν είναι δυνατή η χρήση του KAPE και συνεπώς του Kuiper, σε αυτήν την περίπτωση, λόγω του λειτουργικού συστήματος, που δεν υποστηρίζεται από τα targets του KAPE. Συνεπώς επόμενο βήμα θα είναι η εκτέλεση της emergency διαδικασίας για την συλλογή των artifacts από το endpoint.



Εικόνα 84. Ενεργοποίηση emergency διαδικασίας για πελάτη με id : 001, και όνομα Wazuh_agent

Παρατηρούμε λοιπόν πως το Velociraptor συγκέντρωσε επιτυχώς τα artifacts που έχουν οριστεί, ολοκληρώνοντας επιτυχώς την διαδικασία



Εικόνα 85. Αποτελέσματα συλλογής artifacts Client.Generic.DiskUsage και Client.Generic.DiskSpace για την εικονική μηχανή

Στην παραπάνω παρουσίαση δεν συμπεριλήφθηκαν τα εργαλεία CyberChef και Suricata, διότι δεν προέκυψε ανάγκη μετατροπής δεδομένων και το Suricata δεν διαθέτει κανόνα που να εντοπίζει την ενέργεια αυτή. Επιπλέον, τα αποτελέσματα της ανάλυσης του Kuiper, δεν δημιούργησαν κάποια σχετική ειδοποίηση στο Wazuh, το οποίο παρακολουθεί το αρχείο output.json, όπως φαίνεται και στην εικόνα 42.

6. Ευρήματα εργασίας και βασικά συμπεράσματα

6.1 Συνεισφορά της εργασίας

Στην εργασία αυτή παρουσιάστηκε ο σχεδιασμός και την υλοποίηση μιας ολοκληρωμένης λύσης που αποσκοπεί στη βελτίωση της αντιμετώπισης περιστατικών, στην υποστήριξη συνεργατικών ενεργειών μεταξύ ομάδων και φορέων κυβερνοασφάλειας και στη διευκόλυνση της ανταλλαγής πληροφοριών σχετικά με το κακόβουλο λογισμικό. Με την εισαγωγή καινοτόμων προσεγγίσεων, η εργασία αυτή επιδιώκει να δώσει τη δυνατότητα στους οργανισμούς να ενισχύσουν ακόμα περισσότερο τα μέτρα ασφαλείας τους και να ανταποκριθούν ταχύτερα και αποτελεσματικότερα στις απειλές στον κυβερνοχώρο με βασικό θεμέλιο την συνεργατικότητα και την έγκαιρη και έγκυρη πληροφόρηση. Συνεπώς η συνεισφορά της παρούσας διατριβής είναι μια πλατφόρμα συλλογικής διαχείρισης κυβερνοεπιθέσεων με τα παρακάτω χαρακτηριστικά :

Ποικιλομορφία εργαλείων ασφάλειας για ολοκληρωμένη κάλυψη : Η πλατφόρμα ενσωματώνει εργαλεία όπως IRIS DFIR, TheHive Cortex και Wazuh, προσφέροντας μια ολοκληρωμένη λύση που περιλαμβάνει την ανίχνευση, διερεύνηση, απόκριση και διαχείριση περιστατικών. Κάθε εργαλείο προσφέρει μοναδικές δυνατότητες - από τη συλλογή πληροφοριών για απειλές (MISP) έως την παρακολούθηση τελικών σημείων (Velociraptor και Wazuh) και την ψηφιακή εγκληματολογία (KAPE) - δημιουργώντας ένα αποτελεσματικό πλαίσιο για τον χειρισμό ποικίλων προκλήσεων κυβερνοασφάλειας.

Αποτελεσματική συνεργασία και επικοινωνία : Το Iris και το Mattermost εξασφαλίζει επικοινωνία σε πραγματικό χρόνο και απρόσκοπτη συνεργασία μεταξύ των ομάδων αντιμετώπισης περιστατικών. Αυτό ενισχύει τον συντονισμό και μειώνει τους χρόνους απόκρισης, ιδίως κατά τη διάρκεια κρίσιμων περιστατικών.

Ανταλλαγή πληροφοριών για κακόβουλο λογισμικό με χρήση STIX/TAXII : Η ενσωμάτωση της τυποποιημένης ανταλλαγής πληροφοριών σχετικά με απειλές με την χρήση του MISP, ιδίως μέσω των πρωτοκόλλων STIX (Structured Threat Information Expression) και TAXII (Trusted Automated Exchange of Indicator Information), ενισχύει την ικανότητα της πλατφόρμας να ανταλλάσσει με ασφάλεια πληροφορίες σχετικά με απειλές με άλλα συστήματα. Αυτή η ανταλλαγή είναι ζωτικής σημασίας για να παραμείνουμε μπροστά από τις αναδυόμενες απειλές και παρέχει μια κοινή γλώσσα για την περιγραφή των απειλών στον κυβερνοχώρο, επιτρέποντας στους οργανισμούς να επικοινωνούν και να ενεργούν αποτελεσματικά βάσει των πληροφοριών για τις απειλές.

Αυτοματοποιημένες ροές εργασίας : Με το Shuffle, η πλατφόρμα υποστηρίζει την ενορχήστρωση εργασιών ασφάλειας και την αυτοματοποίηση ροών εργασίας, επιτρέποντας την αυτοματοποίηση επαναλαμβανόμενων εργασιών. Αυτό βελτιώνει την αποδοτικότητα και επιτρέπει στους αναλυτές να επικεντρωθούν σε δραστηριότητες υψηλής προτεραιότητας.

Διευρυμένες δυνατότητες ανίχνευσης και απόκρισης. Οι δυνατότητες εκτεταμένης ανίχνευσης και απόκρισης (Extended Detection and Response - XDR) που παρέχονται από το Wazuh επιτρέπουν στην πλατφόρμα να συγκεντρώνει και να αναλύει δεδομένα από πολλαπλά επίπεδα ασφαλείας, συμπεριλαμβανομένων των τελικών σημείων, των δικτύων και των εφαρμογών. Το XDR βοηθά τις ομάδες ασφαλείας να ανιχνεύουν και να ανταποκρίνονται αποτελεσματικότερα στις απειλές, παρέχοντας μια γενική εικόνα των συμβάντων ασφαλείας σε ολόκληρο τον οργανισμό. Με τη συσχέτιση δεδομένων από διάφορες πηγές, το XDR παρέχει ευκρινές πλαίσιο γύρω από τα περιστατικά, επιτρέποντας ακριβέστερη ανίχνευση απειλών και ταχύτερη επίλυση περιστατικών.

Παρακολούθηση και ασφάλεια endpoints με συστήματα ανίχνευσης και πρόληψης εισβολών (IDPS). Η παρακολούθηση και η ασφάλεια των τελικών σημείων που παρέχεται από το Wazuh και το Suricata, που συμπληρώνεται από συστήματα ανίχνευσης και πρόληψης εισβολών, διαδραματίζει καθοριστικό ρόλο στη διασφάλιση των μεμονωμένων συσκευών και συστημάτων εντός ενός δικτύου. Με τη συνεχή παρακολούθηση των τελικών σημείων, η πλατφόρμα μπορεί να ανιχνεύσει ανώμαλη συμπεριφορά ή κακόβουλη δραστηριότητα σε

επίπεδο συσκευής, αποτελώντας συχνά την πρώτη γραμμή άμυνας. Το IDPS ενισχύει αυτή την άμυνα εντοπίζοντας και αποκλείοντας ύποπτη κυκλοφορία ή δραστηριότητες δικτύου σε πραγματικό χρόνο.

Παρακολούθηση συμμόρφωσης με κανονιστικό πλαίσιο. Η πλατφόρμα παρέχει την δυνατότητα παρακολούθησης της συμμόρφωσης των λειτουργιών ασφαλείας με τους κανονισμούς και τα πρότυπα του κλάδου με την χρήση του Wazuh, όπως ο GDPR, το PCI DSS και άλλες ειδικές απαιτήσεις. Η πλατφόρμα βοηθά τους οργανισμούς να παρακολουθούν τη συμμόρφωση μέσω αυτοματοποιημένων ελέγχων, αρχείων καταγραφής ελέγχου και μηχανισμών αναφοράς. Με τη συνεχή αξιολόγηση του κατά πόσον οι έλεγχοι ασφαλείας ευθυγραμμίζονται με τις κανονιστικές εντολές, οι οργανισμοί μπορούν να εντοπίζουν κενά συμμόρφωσης, να μειώνουν τον κίνδυνο κανονιστικών κυρώσεων και να διασφαλίζουν ότι οι πρακτικές χειρισμού δεδομένων είναι σύμφωνες με τις νομικές υποχρεώσεις. Αυτή η προληπτική προσέγγιση της συμμόρφωσης ενισχύει την ασφάλεια, ενώ παράλληλα καλλιεργεί την εμπιστοσύνη με τα ενδιαφερόμενα μέρη και τους πελάτες.

Ανοιχτού κώδικα εργαλεία και διαλειτουργικότητα : Όλα τα εργαλεία της πλατφόρμας είναι ανοικτού κώδικα και σε μεγάλο βαθμό διαλειτουργικά, μειώνοντας το κόστος και επιτρέποντας παράλληλα την προσαρμογή στις ανάγκες του οργανισμού.

Αρθρωτή προσέγγιση : Η συγκεκριμένη υλοποίηση της πλατφόρμας επιτρέπει την διατήρηση της λειτουργικότητας της με την τροποποίηση ή την αλλαγή των εργαλείων της με άλλα, παρόμοιων ιδιοτήτων, όπως για παράδειγμα, ανάλογα με τις απαιτήσεις του εκάστοτε οργανισμού, το Suricata θα μπορούσε να αντικατασταθεί από εργαλεία τύπου IDPS όπως το Snort ή το Zeek.

Τα παραπάνω χαρακτηριστικά μαζί αποτελούν μια πλατφόρμα που όχι μόνο βελτιώνει την αντιμετώπιση περιστατικών, αλλά και ενισχύει τη συνεργασία, την ανταλλαγή δεδομένων και τη συμμόρφωση με τις κανονιστικές διατάξεις, τα οποία είναι ζωτικής σημασίας στις σύγχρονες λύσεις κυβερνοασφάλειας. Συγκεντρωτικά λοιπόν, η πλατφόρμα που αναπτύχθηκε στην συγκεκριμένη μεταπτυχιακή διατριβή, απαρτίζεται από εργαλεία με διαφορετικές και απαραίτητες λειτουργίες και δυνατότητες για τις ομάδες αντιμετώπισης και διαχείρισης περιστατικών, τα οποία συνδυάζονται αρμονικά και ανταλλάσσουν πληροφορίες και δεδομένα, ώστε τελικά να δημιουργηθεί ένα πλήρες δίκτυο εφαρμογών διαχείρισης κυβερνοεπιθέσεων.

6.2 Περιορισμοί και μελλοντικής επεκτάσεις

Καθώς η πλατφόρμα συνδυάζει πολλαπλά εργαλεία αποτελεσματικά και αποτελεί αντάξια λύση με τις προαναφερθείσες commercial επιλογές στο 2ο κεφάλαιο, δεν είναι απαλλαγμένη από αδυναμίες και ελλείψεις. Πιο συγκεκριμένα , τα βασικότερα μειονεκτήματα της συγκεκριμένης υλοποίησης είναι :

- **Δυσκολία εκμάθησης της πλατφόρμας :** Κάθε εργαλείο έχει τη δική του διεπαφή και συγκεκριμένο σύνολο λειτουργιών, γεγονός που θα μπορούσε να αποτελέσει εμπόδιο στην πλήρη κατανόηση και χρήση της πλατφόρμας από αναλυτές
- **Εγκατάσταση και συντήρηση που απαιτεί πολλούς πόρους :** Η πολυπλοκότητα της πλατφόρμας με την πληθώρα των εργαλείων και τις απαιτήσεις σε πόρους που διαθέτουν μπορεί να καταστήσει την εγκατάσταση, τη συντήρηση και την αντιμετώπιση προβλημάτων απαιτητική.
- **Προβλήματα επιδόσεων σε επέκταση εφαρμογής σε μεγαλύτερη κλίμακα**: Για οργανισμούς με πολύ μεγάλο όγκο δεδομένων ή αρκετά εκτεταμένες υποδομές, η πλατφόρμα ενδέχεται να αντιμετωπίσει συμφόρηση επιδόσεων, ιδίως σε εργασίες παρακολούθησης και ανάλυσης δεδομένων σε πραγματικό χρόνο.
- **Εξάρτηση από εργαλεία ανοικτού κώδικα :** Ενώ τα εργαλεία ανοικτού κώδικα παρέχουν πλεονεκτήματα κόστους, ενδέχεται να μην διαθέτουν την υποστήριξη επιχειρηματικού επιπέδου που προσφέρουν οι εμπορικές λύσεις, γεγονός που θα μπορούσε να αποτελέσει ανησυχία ασφάλειας στους οργανισμούς.

Οι σημαντικότεροι μελλοντικοί στόχοι απορρέουν από τα παραπάνω μειονεκτήματα της πλατφόρμας και προσανατολίζονται στο να τα αντιμετωπίσουν στον δυνατό καλύτερο βαθμό. Αρχικά κρίνεται απαραίτητο να υλοποιηθεί μια ολοκληρωμένη διαδικασία εγκατάστασης και διασύνδεσης των επιμέρους εφαρμογών, και ρύθμισης των παραμέτρων τους ώστε τελικά να διαμορφώνεται η πλατφόρμα με τα απαιτούμενα χαρακτηριστικά και να είναι έτοιμη προς χρήση. Στην συνέχεια θα πρέπει να γίνουν βήματα προς ακόμη μεγαλύτερη ενοποίηση των εφαρμογών, ώστε εν τέλη , στο επίπεδο που είναι εφικτό, η διαχείριση όλων των εργαλείων να πραγματοποιείται μέσω μίας κοινής πλατφόρμας - από την διαχείριση των ειδοποιήσεων του iris, μέχρι την επιλογή των modules του Kape και τον ορισμό ροών εργασίας στο Shuffle - η οποία θα διευκολύνει πολύ περισσότερο τους αναλυτές. Επιπλέον, το πρόβλημα των υπολογιστικών πόρων θα μπορούσε να επιλυθεί με μια προσέγγιση δυναμικής δέσμευσης πόρων, δηλαδή κάθε εφαρμογή να δεσμεύει ελάχιστους πόρους, εκτός αν χρησιμοποιείται. Τέλος, βασικές λειτουργίες της πλατφόρμας, όπως ο εντοπισμός απειλών και ανωμαλιών, αλλά και διαδικασίες απόκρισης σε περιστατικά, όπως ο ορισμός κανόνων, θα μπορούσε να εμπλουτιστεί με την χρήση μοντέλων μηχανικής και βαθιάς μάθησης, ώστε να εντοπίζονται και να διαχειρίζονται αυτόματα άγνωστα και zero day περιστατικά. Η υλοποίηση των παραπάνω στόχων και επεκτάσεων δυνατότητων της πλατφόρμας, θα την καταστήσουν μια ακόμη πιο ανταγωνιστική και αξιόλογη λύση κυβερνοασφάλειας που θα συνδυάζει χαρακτηριστικά και δυνατότητες επιπέδου εμπορικών λύσεων, μαζί με το πλεονέκτημα που ήδη κατέχει, καθώς επιτρέπει την συλλογική διαχείριση κυβερνοεπιθέσεων και μετατρέπει ένα σχέδιο διαχείρισης, από κείμενο σε συγκεκριμένες αυτοματοποιημένες δράσεις.

Βιβλιογραφικές αναφορές και πηγές διαδικτύου.

[1] https://www.statista.com/chart/32341/worldwide-reported-losses-connected-to-cybercrime/

[2] https://www.statista.com/statistics/991304/worldw60ide-cybersecurity-spending/

[3] Spalević, Ž. (2014). Cyber security as a global challenge today. *Singidunum Journal of Applied Sciences*, 687-692.

[4] Ioannou, M., Stavrou, E., & Bada, M. (2019, June). Cybersecurity culture in computer security incident response teams: Investigating difficulties in communication and coordination. In *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)* (pp. 1-4). IEEE.

[5] Mallick, M.A.I. and Nath, R., 2024. Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. *World Scientific News*, *190*(1), pp.1-69.

[6] Settanni, G., Skopik, F., Shovgenya, Y., Fiedler, R., Carolan, M., Conroy, D., Boettinger, K., Gall, M., Brost, G., Ponchel, C. and Haustein, M., 2017. A collaborative cyber incident management system for European interconnected critical infrastructures. *Journal of Information Security and Applications*, *34*, pp.166-182.

[7] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555

[8] Wang, G., Huo, Y. and Ma, Z.M., 2019. Research on university's cyber threat intelligence sharing platform based on new types of stix and taxii standards. *Journal of Information Security*, *10*(4), pp.263-277.

[9] Tundis, A., Mazurczyk, W. and Mühlhäuser, M., 2018, August. A review of network vulnerabilities scanning tools: Types, capabilities and functioning. In *Proceedings of the 13th international conference on availability, reliability and security* (pp. 1-10).

[10] Tounsi, W. and Rais, H., 2018. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & security*, *72*, pp.212-233.

[11] George, A.S., Sagayarajan, S., Baskar, T. and George, A.H., 2023. Extending detection and response: how MXDR evolves cybersecurity. *Partners Universal International Innovation Journal*, *1*(4), pp.268-285.

[12] Hassan, W.U., Bates, A. and Marino, D., 2020, May. Tactical provenance analysis for endpoint detection and response systems. In *2020 IEEE Symposium on Security and Privacy (SP)* (pp. 1172-1189). IEEE.

[13] Syrjälä, A., 2023. Exploring network detection and response technologies: understanding the role of network detection and response and comparing features of available products.

[14] Singh, A. and Chatterjee, K., 2017. Cloud security issues and challenges: A survey. *Journal of Network and Computer Applications*, *79*, pp.88-115.

[15] Azeez, N.A., Bada, T.M., Misra, S., Adewumi, A., Van der Vyver, C. and Ahuja, R., 2020. Intrusion detection and prevention systems: an updated review. *Data Management, Analytics and Innovation: Proceedings of ICDMAI 2019, Volume 1*, pp.685-696.

[16] Ghazinour, K., Vakharia, D.M., Kannaji, K.C. and Satyakumar, R., 2017, September. A study on digital forensic tools. In *2017 IEEE international conference on power, control, signals and instrumentation engineering (ICPCSI)* (pp. 3136-3142). IEEE.

[17] Papazafeiropoulou, A. and Spanaki, K., 2016. Understanding governance, risk and compliance information systems (GRC IS): The experts view. *Information Systems Frontiers*, *18*, pp.1251-1263.

[18] González-Granadillo, G., González-Zarzosa, S. and Diaz, R., 2021. Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. *Sensors*, *21*(14), p.4759.

[19] Vast, R., Sawant, S., Thorbole, A. and Badgujar, V., 2021, April. Artificial intelligence based security orchestration, automation and response system. In *2021 6th International Conference for Convergence in Technology (I2CT)* (pp. 1-5). IEEE.

[20] https://www.ibm.com/threat-detection-response?lnk=flatitem

[21] https://www.netwitness.com/solutions/netwitness-platform/

[22] https://www.paloaltonetworks.com/network-security/advanced-threat-prevention

[23] https://www.rapid7.com/products/insightidr/

[24] https://www.rapid7.com/products/insightidr/features/

[25] https://www.trellix.com/products/

[26] https://dfir-iris.org/

[27] https://github.com/TheHive-Project/Cortex

[28] https://www.misp-project.org/

[29] https://github.com/gchq/CyberChef

[30] https://mattermost.com/

[31] https://docs.velociraptor.app/

[32] https://wazuh.com/

[33] https://www.kroll.com/en/services/cyber-risk/incident-response-litigation-support/kroll-artifact-parser-extractor-kape

[34] https://github.com/DFIRKuiper/Kuiper

[35] https://shuffler.io/

[36] https://suricata.io/

[37]https://aws.amazon.com/docker/#:~:text=Docker%20is%20a%20software%20platform,tools%2C%20code%2C%20and%20runtime.

[38] https://github.com/dfir-iris/iris-web

[39] https://github.com/TheHive-Project/cortex

[40] https://github.com/coolacid/docker-misp

[41] https://nodejs.org/en

[42] https://www.majorgeeks.com/files/details/cyberchef.html

[43] https://docs.mattermost.com/install/install-docker.html

[44] https://github.com/socfortress/iris-velociraptorartifact-module

[45] https://documentation.wazuh.com/current/installation-guide/wazuh-indexer/step-by-step.html

[46] https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-overview.html

[47] https://wazuh.com/blog/enhancing-incident-response-with-wazuh-and-dfir-iris-integration/

[48] https://github.com/DFIRKuiper/Kuiper

[49] https://github.com/DFIRKuiper/DFIRKuiperAPI#GetFieldsScript

[50] https://www.kroll.com/en/services/cyber-risk/incident-response-litigation-support/kroll-artifact-parser-extractor-kape

[51] https://docs.suricata.io/en/latest/install.html#advanced-installation

[52] https://github.com/Shuffle/Shuffle/releases

[53] https://www.virtualbox.org/