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

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Σύγκριση Προληπτικής και Αντιδραστικής Κυβερνοάμυνας: Προληπτική Αναζήτηση Κυβερνοαπειλών** **Hunting the Cyber Threat, Reactive vs Proactive Cyber Defense**
Ονοματεπώνυμο Φοιτητή	**Γουρζουλίδης Χρήστος**
Πατρώνυμο	**Δημήτριος**
Αριθμός Μητρώου	**ΜΠΚΣΑ/ 19006**
Επιβλέπων	**Παναγιώτης Κοτζανικολάου, Αναπληρωτής Καθηγητής**

Ημερομηνία Παράδοσης **Ιανουάριος 2022**

Τριμελής Εξεταστική Επιτροπή

Παναγιώτης Κοτζανικολάου	Χρήστος Δουληγέρης	Δέσποινα Πολέμη
Αναπληρωτής Καθηγητής	Καθηγητής	Καθηγήτρια

Περιεχόμενα

Πίνακας εικόνων

Ευχαριστίες

Ολοκληρώνοντας με την εκπόνηση της μεταπτυχιακής μου διατριβής, θα ήθελα να ευχαριστήσω ιδιαίτερα τον κ. Κοτζανικολάου Παναγιώτη και τον κ. Παπαγεωργίου Σπυρίδων για την καθοδήγηση και την βοήθεια τους. Επιπλέον, θα ήθελα να ευχαριστήσω θερμά τους γονείς μου, φίλους και συνεργάτες για την πολύτιμη βοήθεια και υποστήριξη τους καθ' όλη την διάρκεια των σπουδών μου.

Περίληψη

Σκοπός της μεταπτυχιακής διατριβής είναι η προληπτική κυβερνοάμυνα και πως μπορεί ένας οργανισμός να την αναπτύξει με εργαλεία ανοιχτών πηγών (open source). Εγκαθίστανται όλα τα απαραίτητα εργαλεία για την εφαρμογή της και παρουσιάζονται οι τακτικές, τεχνικές και οι διαδικασίες που χρησιμοποιούν οι επιτιθέμενοι στον κυβερνοχώρο καθώς και τα μοντέλα των κυβερνοεπιθέσεων. Τα εργαλεία περιλαμβάνουν την συλλογή πληροφοριών για κυβερνοαπειλές (cyber threat intelligence), το κέντρο επιχειρησιακής ασφάλειας (SOC) που αφορούν την οργάνωση, την ανάλυση και την εξειδίκευση των πληροφοριών των απειλών για πιθανές ή τρέχουσες κυβοερνοεπιθέσεις που στοχοποιούν έναν οργανισμό. Ως αποτέλεσμα θα έχουμε μια υποδομή προληπτικής αναζήτησης απειλών που θα ανιχνεύει, θα συλλέγει και θα οργανώνει τα περιστατικά απειλών στον κυβερνοχώρο.

Λέξεις κλειδιά

Cyber Threat Hunting, Reactive Cyber Defense, Proactive Cyber Defense, Security Operations Center, Security Onion, MISP, Minemeld, Cyber Kill Chain, Cyber Threat Intelligence, RITA, Cyber Security

Abstract

The purpose of the master's thesis is the process of hunting the cyber threat inside an organization and how an organization can develop it with open-source tools. All the necessary tools for the application of the proactive cyber defense are installed and the tactics, techniques and procedures used by cyber attackers are presented, as well as the different models for identification and prevention of cyber intrusions activity. Tools include the collection of information about cyber threats and the security operations center that includes the organization, analysis and specialization of threat information related to possible or ongoing cyber-attacks that target an organization. As a result, we will have an infrastructure that will detect, collect, and organize cyber threat incidents.

Keywords

Cyber Threat Hunting, Reactive Cyber Defense, Proactive Cyber Defense, Security Operations Center, Security Onion, MISP, Minemeld, Cyber Kill Chain, Cyber Threat Intelligence, RITA, Cyber Security

Κεφάλαιο 1 – Εισαγωγή

Στην ψηφιακή εποχή, η ασφάλεια στον κυβερνοχώρο, αποτελεί βασικό στοιχείο για την προστασία των πληροφοριών ενός οργανισμού. Οι κυβερνοεπιθέσεις αποτελούν πλέον μια από τις σοβαρότερες απειλές παγκοσμίως και είναι ιδιαιτέρα σημαντικό, οργανισμοί κάθε βεληνεκούς να αναπτύσσουν μεθόδους πρόληψης, διερεύνησης και δίωξης ενός κυβερνοεγκλήματος.

Η ομαλή εκτέλεση των δραστηριοτήτων των σύγχρονων οργανισμών βασίζεται στην απρόσκοπτη λειτουργία των πληροφοριακών τους συστημάτων αλλά και στην προστασία των πληροφοριών που επεξεργάζονται. Η συνεχώς αυξανόμενη εμφάνιση παραγόντων που είναι δυνατόν να οδηγήσουν σε παραβίαση της ασφάλειας πληροφοριών και διακοπή της ομαλής τους λειτουργίας, κάνει επιτακτική την ανάγκη υιοθέτησης βέλτιστων πρακτικών και μέτρων προκειμένου να περιοριστούν οι πιθανότητες εμφάνισής τους.

Η ταχύτατα αναπτυσσόμενη εμφάνιση νέων τύπων επιθέσεων και η χρήση μεθόδων που είναι δυνατόν να παρακάμψουν τους μηχανισμούς ασφάλειας που εφαρμόζει ένας οργανισμός, καθιστά επιτακτική τη ανάγκη αυτή για την διασφάλιση όλων των επιχειρησιακών δραστηριοτήτων.

1.1 ΠΡΟΛΗΠΤΙΚΗ ΚΑΙ ΑΝΤΙΔΡΑΣΤΙΚΗ ΚΥΒΕΡΝΟΑΜΥΝΑ

Η προληπτική κυβερνοάμυνα ή προσέγγιση της ασφάλειας στον κυβερνοχώρο εντοπίζει και διορθώνει τα πιθανά τρωτά σημεία των συστημάτων ενός οργανισμού προτού αυτά γίνουν αντιληπτά και μπορούν να αξιοποιηθούν από τους επιτιθέμενους στον κυβερνοχώρο. Με λίγα λόγια, αποτελεί τις μεθόδους και τις πρακτικές που εφαρμόζει ένας οργανισμός για να αποτρέψει τις κυβερνοεπιθέσεις.

Η ασφάλεια δεν είναι απλά η χρήση κατάλληλων τεχνολογιών, γιατί αυτό απλά προβλέπει η πολιτική μας. Εστιαζόμαστε στην ανάλυση της απειλής και σε συνδυασμό με τις τακτικές, τεχνικές και διαδικασίες που ακολουθούν οι επιτιθέμενοι, προσαρμόζουμε την κυβερνοάμυνα μας.

Σκοπός του επιτιθέμενου είναι να αποκτήσει πρόσβαση στα πληροφοριακά συστήματα και να την διατηρήσει. Συνεπώς, πρέπει να εγκαταστήσει λογισμικό ελέγχου στο δίκτυο και παράλληλα, να επαναλαμβάνει τις ίδιες κινήσεις μετακίνησης στο δίκτυο του οργανισμού.

Λαμβάνοντας αυτό υπόψιν, πέρα από την περιμετρική ασφάλεια θα πρέπει να εστιαστεί η προσοχή και στην ασφάλεια των προσωπικών υπολογιστών.

Ορισμένοι αποτελεσματικοί τρόποι ασφάλειας των προσωπικών υπολογιστών είναι:

1. **Μειωμένη επιθετική επιφάνεια**
    a. Πολιτική Zero-Trust: Κανένας χρήστης δεν θα πρέπει να έχει δικαίωμα πρόσβασης στα αρχεία του οργανισμού εάν δεν ολοκληρωθεί η διαδικασία ταυτοποίησης στην προσωπική του συσκευή.
    b. Δημιουργία ισχυρών πολιτικών πρόσβασης χρηστών. Όταν παύει να ισχύει η συνεργασία των χρηστών με τον οργανισμό, θα πρέπει να αφαιρείται κάθε δικαίωμα πρόσβασης.
    c. Εφαρμογή ισχυρών πολιτικών ελέγχου ταυτότητας, για παράδειγμα έλεγχο ταυτότητας δύο παραγόντων (2FA) / Passwordless (Ταυτοποίηση χωρίς κωδικό πρόσβασης), όπου αυτό είναι εφικτό.
    d. Προστασία των αντιγράφων ασφάλειας, χρησιμοποιώντας αυστηρά πρωτόκολλα και αποθηκεύοντας τα σε παραπάνω από 1 σημεία.
    e. Διαχώριση του δικτύου σε υποδίκτυα και εφαρμογή πολιτικών για το κάθε ένα ξεχωριστά. Δημιουργώντας περισσότερα τείχη προστασίας, καθιστά δυσκολότερο το έργο των κακόβουλων χρηστών.
2. **Αρχή ελάχιστων προνομίων,** να εφαρμόζεται και να δίνονται τα ελάχιστα δικαιώματα που χρειάζονται οι χρήστες για να εκτελέσουν την εργασία τους.
3. **Επιτήρηση προσωπικών υπολογιστών,** όπως η εγκατάσταση ενός συστήματος HIDS (Host-Based Intrusion Detection System) ή/και NIDS (Network-Based Intrusion Detection System). Βέλτιστη πρακτική είναι η εφαρμογή και των 2 συστημάτων.

Η προληπτική κυβερνοάμυνα παρέχει πολλά πλεονεκτήματα μέσα στον οργανισμό και βοηθά την ομάδα ασφάλειας να:

1. Μπορεί να εντοπίσει και κατανοήσει τις αδυναμίες του οργανισμού
2. Πετύχει έγκαιρο εντοπισμό των απειλών
3. Ελέγξει την ζημιά
4. Βελτιώσει τα συστήματα προστασίας

Για μια αποτελεσματική κυβερνοάμυνα, οι οργανισμοί θα πρέπει επιπλέον να: [17]

1. Γνωρίζουν πολύ καλά τους χρήστες του δικτύου τους χρησιμοποιώντας σύγχρονα λογισμικά.
2. Κατανοούν την απειλή, από ποιους κινδυνεύουν, ποιες είναι οι τακτικές, τεχνικές και οι διαδικασίες που χρησιμοποιούν και ποιες οι επιπτώσεις μέσα στον οργανισμό.
3. Εφαρμόζουν σχέδιο ευαισθητοποίησης των χρηστών, δημιουργώντας πρόγραμμα εκπαίδευσης/κατάρτισης/ειδίκευσης για την ασφάλεια στον κυβερνοχώρο.
4. Εφαρμόζουν πολυεπίπεδη προληπτική κυβερνοασφάλεια (Συστήματα IDS,IPS,Firewall κλπ.)
5. Δημιουργήσουν και να δοκιμάσουν ένα σχέδιο διαχείρισης και αντιμετώπισης κυβερνοεπιθέσεων, τόσο σε επίπεδο δικτύου, όσο και σε επίπεδο προσωπικού υπολογιστή.

6. Αναπτύσσουν μηχανισμούς εντοπισμού κυβερνοεπιθέσεων όπως είναι το Κέντρο Αντιμετώπισης Κυβερνοπεριστατικών (SOC), η εγκατάσταση SIEM, EDR κλπ.
7. Συλλέγουν πληροφορίες για νέες κυβερνοαπειλές (Cyber Threat Intelligence).
8. Διεξάγουν ελέγχους παρείσδυσης (penetration tests) και ελέγχους ευπάθειας (vulnerability assessments) στα συστήματα του οργανισμού.
9. Εφαρμόζουν σχέδιο επιχειρησιακής συνέχειας/σχέδιο αποκατάστασης σε περίπτωση επιτυχημένης κυβερνοεπίθεσης.
10. Διαθέτουν εκπαιδευμένα άτομα σε θέματα ασφάλειας συστημάτων.

Από την άλλη πλευρά, η αντιδραστική κυβερνοάμυνα είναι ακριβώς αυτό που λέει και η λέξη, εάν συμβεί μια επίθεση και η ομάδα ασφάλειας ανταποκρίνεται ή αντιδρά στην παραβίαση. Συνήθως όταν ανακαλύπτεται μια επίθεση προχωράμε σε ενέργειες για να την αντιμετωπίσουμε, εκτιμάται η ζημιά που έχει προκληθεί και στην συνέχεια αποκαθίσταται η ζημιά αυτή. Αυτός είναι και συχνά ο τρόπος με τον οποίο σκέφτονται οι ομάδες ασφάλειας στον κυβερνοχώρο. Το πρόβλημα εδώ και είναι κάτι που αξίζει να σημειωθεί είναι το γεγονός όπου η νοοτροπία της ασφάλειας στον κυβερνοχώρο είναι μόνο αντιδραστική και καθόλου προληπτική.

Για να αξιοποιηθεί στο έπακρο και για να είναι αποτελεσματική η κυβερνοάμυνα θα πρέπει η νοοτροπία στον τομέα της κυβερνοασφάλειας να είναι και προληπτική αλλά και αντιδραστική. Είναι ζωτικής σημασίας η κατανόηση της διαφοράς διότι βοηθά τον οργανισμό να είναι πλήρως έτοιμος σε μια ενδεχόμενη απειλή.

Ορισμένοι αποτελεσματικοί τρόποι αντιδραστικής κυβερνοάμυνας είναι οι παρακάτω:

1. **Παρακολούθηση για ανωμαλίες στο δίκτυο του οργανισμού**. Τα συστήματα ανίχνευσης εισβολών εντοπίζουν αποτυχίες εξουσιοδότησης και ελέγχου ταυτότητας, κακόβουλο λογισμικό, ερωτήματα σε βάσεις δεδομένων κ.α. Αποτελούν βασικό στοιχείο για την παρακολούθηση και την αντιδραστική κυβερνοασφάλεια.
2. **Ανάλυση ψηφιακών πειστηρίων (forensics) και αντίδραση στο περιστατικό (incident response).** Μετά από μια παραβίαση, η απόκριση σε ένα περιστατικό περιλαμβάνει ενέργειες για την βασική αιτία που προκλήθηκε αυτό έτσι ώστε να διασφαλιστεί ότι δεν μπορεί η ίδια ευπάθεια να αξιοποιηθεί ξανά.
3. **Μηχανές anti-spam & anti-malware.** Κάθε συσκευή θα πρέπει να έχει λογισμικό το οποίο εμποδίζει την εγκατάσταση κακόβουλου λογισμικού στην μνήμη. Εάν το κακόβουλο λογισμικό δεν εντοπιστεί, ο οργανισμός θα πρέπει να είναι σε θέση να το καθαρίσει.
4. **Τείχος προστασίας (firewall).** Τα τείχη προστασίας μπορούν να θεωρηθούν ως λύση προληπτικής κυβερνοάμυνας λόγω της ικανότητας τους να μπλοκάρουν την ανεπιθύμητη κυκλοφορία. Μπορούν όμως να θεωρηθούν και ως μια αντιδραστική λύση εάν έχουν λανθασμένες ρυθμίσεις (όπως η ανοιχτή πρόσβαση σε πόρτες και υπηρεσίες) και βοηθήσουν έτσι την ψηφιακή ανάλυση μετά από ένα περιστατικό.

1.2 ΔΟΜΗ ΤΗΣ ΔΙΑΤΡΙΒΗΣ

Στην ενότητα αυτή προσδιορίζεται η δομή της διατριβής καθώς και το περιεχόμενο των κεφαλαίων και των υποενοτήτων τους. Η εργασία αποτελείται από επτά κεφάλαια τα οποία περιγράφονται στις παρακάτω παραγράφους.

Στο 1ο κεφάλαιο, περιγράφονται οι βασικοί ορισμοί της προληπτικής και της αντιδραστικής κυβερνοάμυνας. Επιπλέον, αναφέρονται κάποιοι βασικοί αποτελεσματικοί τρόποι ασφάλειας για τα πληροφοριακά συστήματα ενός οργανισμού. Στο τέλος του κεφαλαίου, αναφέρονται τα μηχανήματα που χρησιμοποιήθηκαν καθώς και τα αναλυτικά χαρακτηριστικά τους.

Στο 2ο κεφάλαιο, γίνεται μια επισκόπηση της προληπτικής αναζήτησης της απειλής καθώς και των μεθοδολογιών, τακτικών και τεχνικών που εφαρμόζονται στο πλαίσιο της προληπτικής κυβερνοάμυνας. Αρχικά, δίνεται ο ορισμός και περιγράφεται ο σκοπός της προληπτικής αναζήτησης της απειλής. Στην συνέχεια, δίνεται ιδιαίτερη έμφαση στην προληπτική αναζήτηση της απειλής, πως αυτή οργανώνεται και διεξάγεται από την ομάδα ασφάλειας, τι μέθοδοι μπορούν να χρησιμοποιηθούν και που αποσκοπεί. Παράλληλα, αναλύονται τρία από τα σημαντικότερα μοντέλα κυβερνοεπιθέσεων που έχουν αναπτυχθεί. Η πυραμίδα των εμποδίων για την σωστή χρησιμοποίηση του CTI (Cyber Threat Intelligence) στην ανίχνευση των απειλών του David Bianco, το ATT&CK από την εταιρεία MITRE ως μοντέλο για την τεκμηρίωση και παρακολούθηση διαφόρων τεχνικών που χρησιμοποιούν οι επιτιθέμενοι στα διάφορα στάδια μιας κυβερνοεπίθεση. Τέλος, περιγράφεται η αλυσίδα των κυβερνοεπιθέσεων (Cyber Kill Chain) από τον Lockheed Martin, που περιλαμβάνει τα στάδια μιας κυβερνοεπίθεσης και πως αυτή βοηθά στην αντιμετώπιση περιστατικών από τις ομάδες ασφάλειας.

Στο 3ο κεφάλαιο, αναλύεται η έννοια της συλλογής πληροφοριών (Cyber Threat Intelligence) όπως επίσης οι τεχνικές και οι μεθοδολογίες της συλλογής, επεξεργασίας και διαμοιρασμού των δεδομένων. Επιπρόσθετα, γίνεται μια εκτενής αναφορά στα εργαλεία MISP και Minemeld που βοηθούν σημαντικά στην αναζήτηση και συλλογή δεδομένων των απειλών στον κυβερνοχώρο.

Στο 4ο κεφάλαιο, δίνεται ο βασικός ορισμός και πληροφορίες ενός επιχειρησιακού κέντρου ασφάλειας (SOC) που τονίζουν το πόσο σημαντικό είναι να υπάρχει σε έναν οργανισμό. Στην συνέχεια γίνεται αναφορά στο Security Onion ως εργαλείο για την παρακολούθηση των κυβερνοαπειλών στα συστήματα της υποδομής.

Στο 5ο κεφάλαιο, γίνεται αναφορά στο RITA, ένα εργαλείο για την ανίχνευση επικοινωνιών C&C (Command & Control) μέσω αρχείων καταγραφής ή αρχείων PCAP. Σκοπός μέσω του RITA είναι να αναλύουμε την δικτυακή κίνηση και γενικότερα να εφαρμόσουμε μια θεμελιώδη αλλαγή στον τρόπο με τον οποίο προσεγγίζουμε τον εντοπισμό των επιθέσεων.

Στο 6ο κεφάλαιο, παρουσιάζονται και τεκμηριώνονται συνολικά τα αποτελέσματα των δοκιμών που έγιναν στο εργαστηριακό περιβάλλον και αφορούν τα εργαλεία και τις μεθοδολογίες που χρησιμοποιήθηκαν στα προηγούμενα κεφάλαια.

Στο 7ο κεφάλαιο, αναφέρονται τα συμπεράσματα της διπλωματικής εργασίας και οι μελλοντικές επεκτάσεις που μπορούν να βελτιώσουν σημαντικά την αυτοματοποίηση της προληπτικής αναζήτησης των κυβερνοαπειλών.

Τέλος, παρατίθεται η λίστα αναφορών όπου περιλαμβάνονται όλες οι πηγές που χρησιμοποιήθηκαν για την εκπόνηση της εργασίας.

1.3 ΥΛΟΠΟΙΗΣΗ ΤΗΣ ΥΠΟΔΟΜΗΣ

Στα πλαίσια της διπλωματικής εργασίας, δημιουργήθηκε ένα εργαστηριακό περιβάλλον με την χρήση εικονικών μηχανών, όπου χρησιμοποιήθηκαν εργαλεία ανοιχτών πηγών και περιλαμβάνουν την διαδικασία της προληπτικής κυβερνοάμυνας, τόσο από την πλευρά των κακόβουλων χρηστών και την εκτέλεση πολλαπλών σεναρίων επίθεσης όσο και από την πλευρά της ομάδας ασφάλειας ενός οργανισμού.

Ονομασία	Λειτουργικό Σύστημα	Δίσκος	CPU	RAM	Διεύθυνση IP
SecurityOnion (SOC)	Ubuntu 18.04	200GB	4x	12GB	192.168.50.190
MISP (Threat Intelligence Platform)	Ubuntu 18.04	25GB	1x	3GB	192.168.6.56
Minemeld	Ubuntu 16.04	25GB	2x	4GB	192.168.6.57
Windows10_ENT (Client Machine)	Windows 10 Enterprise	60GB	2x	6GB	192.168.6.50
Windows8.1_ENT (Client Machine)	Windows 8.1 Enterprise	40GB	2x	4GB	192.168.6.59
Kali Linux 2021 (Attack Machine)	Debian 5.10.13	80GB	4x	2GB	192.168.6.51
Windows 10 (Host Machine)	Windows 10 Professional	1TB NVMe	Intel Core i7	32GB	192.168.50.199

Κεφάλαιο 2 – Προληπτική Αναζήτηση Απειλής (Cyber Threat Hunting)

Η προληπτική αναζήτηση απειλών στον κυβερνοχώρο είναι μια ενεργητική διαδικασία αναζήτησης τρωτών σημείων ασφάλειας σε συστήματα, δίκτυα και υπολογιστές για την εύρεση κακόβουλων και ύποπτων δραστηριοτήτων που δεν έχουν εντοπιστεί. Έτσι, υπάρχει μια διάκριση μεταξύ της ανίχνευσης των απειλών στον κυβερνοχώρο και της προληπτικής αναζήτησης των κυβερνοαπειλών. [11][21]

Η ανίχνευση απειλών είναι μια παθητική προσέγγιση για την παρακολούθηση δεδομένων και συστημάτων για πιθανά ζητήματα ασφάλειας, αλλά εξακολουθεί να είναι απαραίτητη και μπορεί να βοηθήσει την ομάδα που είναι υπεύθυνη για την προληπτική αναζήτηση απειλών. Συνήθως, πραγματοποιείται από άτομα της μπλε ομάδας μέσα σε έναν οργανισμό εστιάζοντας σε ευπάθειες, απειλές, αξιολόγηση και αποτροπή των κυβερνοεπιθέσεων. [7]

Οι τακτικές της προληπτικής αναζήτησης των απειλών στον κυβερνοχώρο έχουν εξελιχθεί και χρησιμοποιούν νέες πληροφορίες απειλών σε δεδομένα που έχουν συλλεχθεί προηγουμένως για τον εντοπισμό και την κατηγοριοποίηση πιθανών απειλών πριν από την κυβερνοεπίθεση.
Η ομάδα ασφάλειας δεν πρέπει να θεωρεί ότι το σύστημα ασφαλείας τους είναι αδιαπέραστο. Πρέπει να παραμένει σε εγρήγορση για την επόμενη απειλή ή ευπάθεια. Αντί να κάθεται και να περιμένει να χτυπήσουν οι απειλές, η προληπτική αναζήτηση απειλών στον κυβερνοχώρο αναπτύσσει υποθέσεις που βασίζονται στη γνώση των συμπεριφορών των επιτιθέμενων και στην επικύρωση αυτών των υποθέσεων μέσω συνεχών αναζητήσεων στο περιβάλλον του οργανισμού. [21]

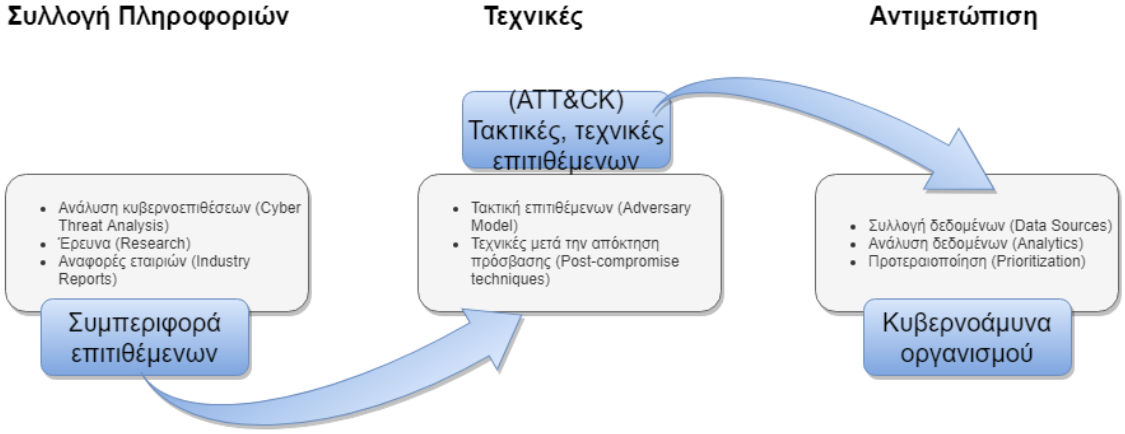
Με την προληπτική αναζήτηση των απειλών στον κυβερνοχώρο, η ομάδα ασφάλειας δεν ξεκινά από μια προειδοποίηση ή από ενδείκτες παραβίασης αλλά κοιτώντας και βαθύτερα στον οργανισμό όπως είναι η ψηφιακή σήμανση (forensics). Ξεκινώντας την αναζήτηση υποθέτουμε ότι έχει γίνει ή θα συμβεί η παραβίαση στα συστήματα του οργανισμού.

Οι βασικές αρχές ανάπτυξης κυβερνοάμυνας με βάση την απειλή είναι:

1. Αναπτύσσουμε την δυνατότητα εντοπισμού του επιτιθέμενου αφού αποκτήσει αρχική πρόσβαση.
2. Εστιαζόμαστε στην συμπεριφορά του επιτιθέμενου.
3. Χρησιμοποιούμε το μοντέλο βασισμένο στην απειλή. Είναι μια δομημένη διαδικασία με συγκεκριμένους στόχους όπως ο προσδιορισμός απαιτήσεων ασφάλειας, ο εντοπισμός απειλών και πιθανών τρωτών σημείων και η προτεραιότητα στις μεθόδους αποκατάστασης.

4. Χρησιμοποιούμε επαναλαμβανομένη μεθοδολογία. Τι χάσαμε, τι συμπεριφορά προσπαθούμε να εντοπίσουμε, συλλογή και ανάλυση πληροφοριών.
5. Εφαρμόζουμε τις τακτικές, μεθόδους και διαδικασίες σε πραγματικό περιβάλλον.

Στο παρακάτω σχεδιάγραμμα απεικονίζεται το μοντέλο κυβερνοάμυνας, βασιζόμενο στην απειλή.



Εικόνα 1 – Μοντέλο κυβερνοάμυνας με βάση την απειλή

Στο παρακάτω σχεδιάγραμμα απεικονίζεται η εφαρμογή της προληπτικής κυβερνοάμυνας, συμπεριλαμβανομένου και της προληπτικής αναζήτησης απειλών.

Εικόνα 2 - Διαδικασία προληπτικής κυβερνοάμυνας

Η διαδικασία της προληπτικής κυβερνοάμυνας, αποτελείται από 3 βασικά στάδια:

1. **Συλλογή / Ανάλυση Πληροφοριών**

   Ο κύκλος της συλλογής και ανάλυσης πληροφοριών, εστιάζεται στην ανάπτυξη μιας κατάστασης επαγρύπνησης σχετικά με τις απειλές, αδυναμίες και τα αγαθά που θα πρέπει να προστατέψουμε στον οργανισμό.

   a. **Κατεύθυνση:** Κατευθύνουμε την διάταξη των αμυντικών μας μέσων, γνωρίζοντας εκ των υστέρων τι πληροφορίες θέλουμε να συλλέξουμε από τους επιτιθέμενους, προσδιορίζοντας τα βασικά αγαθά και δεδομένα που θέλουμε να προστατέψουμε, λαμβάνοντας πάντα υπόψιν τις αδυναμίες του δικτύου μας.

   b. **Συλλογή πληροφοριών:** Συλλέγουμε όσα περισσότερα δεδομένα και πληροφορίες έχουμε. Θα πρέπει να γνωρίζουμε τι είδος πληροφορία συλλέγουμε και από ποιο σύστημα προέρχεται.

   c. **Ανάλυση:** Αναλύουμε όσα δεδομένα έχουμε συλλέξει χρησιμοποιώντας τα εργαλεία που έχουμε και με τα αποτελέσματα που παίρνουμε, βελτιώνουμε την κυβερνοάμυνα μας, εντοπίζοντας και αντιμετωπίζοντας μελλοντικές κυβερνοεπιθέσεις.

d. **Διάδοση και διαμοιρασμός:** Διαμοιράζουμε την πληροφορία που έχουμε συλλέξει από το προηγούμενο στάδιο της ανάλυσης. Μεταδίδουμε τις γνώσεις και τις τεχνικές στην ομάδα ασφάλειας που είναι υπεύθυνη για την προληπτική αναζήτηση της απειλής. Ο διαμοιρασμός της γνώσης και της πληροφορίας, είναι ένα από τα σημαντικότερα βήματα που θα πρέπει να γίνονται εσωτερικά στον οργανισμό.

2. Προληπτική αναζήτηση της απειλής

Ο κύκλος της προληπτικής αναζήτησης των απειλών επικεντρώνεται στην προληπτική και συνεχή αναζήτηση των δεδομένων για να εντοπιστούν αδυναμίες και απειλές που μπορεί να είναι κρυμμένες στο εσωτερικό του δικτύου και των συστημάτων.

a. **Προσανατολισμός:** Δείχνουμε την κατεύθυνση της προληπτικής αναζήτησης της απειλής. Αυτή ξεκινά με ένα σημείο εκκίνησης και συγκεκριμένης κατεύθυνσης. Πιθανά σημεία εκκίνησης μπορεί να είναι κάποιοι ενδείκτες παραβίασης ή μια υπόθεση η οποία θα πέσει στην αντίληψη μας και χρειάζεται περαιτέρω διερεύνηση.

b. **Ερώτηση:** Στα πλαίσια μιας κυβερνοεπίθεσης θα πρέπει να κάνουμε συνεχείς ενέργειες στα δεδομένα που έχουμε συλλέξει, όπως είναι αυτή της ερώτησης τύπου query. Χρησιμοποιώντας και αναλύοντας τα δεδομένα που έχουμε στην κατοχή μας από διάφορα συνδυαστικά εργαλεία, αποσκοπούμε στον εντοπισμό μιας προηγμένης επίθεσης. Επιπλέον τεχνικές ανάλυσης συνδυαστικών δεδομένων, μπορούν να μας βοηθήσουν για τον εντοπισμό μοτίβου κυβερνοεπιθέσεων ή ανάλυσης μιας ύποπτης συμπεριφοράς.

c. Ανάλυση: Αναλύουμε τα ίχνη των επιθέσεων και είμαστε ιδιαίτερα προσεκτικοί ώστε να εντοπίσουμε ακόμη και την δράση ενός κακόβουλου χρήστη σε μεταγενέστερη φάση της αλυσίδας κυβερνοεπιθέσεων. Στο στάδιο αυτό, συγκρίνουμε τα αποτελέσματα με αυτά που θα περιμέναμε να είχαμε και καταλήγουμε στο συμπέρασμα αν πρόκειται για φυσιολογική κατάσταση συμπεριφοράς δικτύου και συστημάτων.

d. Αναθεώρηση: Καθ’ όλη την διάρκεια της προληπτικής αναζήτησης της απειλής, απομακρύνουμε τις λιγότερο χρήσιμες πληροφορίες και εστιάζουμε σε αυτές που θα μας βοηθήσουν πραγματικά στον εντοπισμό της απειλής.

3. Αντιμετώπιση

Ο κύκλος της αντιμετώπισης αφορά στον περιορισμό της ζημιάς που έχει προκύψει από μια επιτυχημένη κυβερνοεπίθεση.

a. **Περιορισμός:** Προσπαθούμε να περιορίσουμε όσο τον δυνατόν γίνεται την πρόσβαση ή την μετακίνηση στο εσωτερικό μας δίκτυο. Οι επιτιθέμενοι στον κυβερνοχώρο αφού πάρουν την αρχική πρόσβαση, χρησιμοποιούν τεχνικές περεταίρω εισχώρησης στο δίκτυο, καθώς αναζητούν τα βασικά δεδομένα και τα περιουσιακά στοιχεία του οργανισμού.

b. **Διερεύνηση:** Διερευνούμε την έκταση της ζημιάς και πως αυτή προκλήθηκε από την απειλή, αναπτύσσουμε το σχέδιο αποκατάστασης με σκοπό την ανατροφοδότηση του κύκλου του της προληπτικής αναζήτησης της απειλής και την κατεύθυνση στο βάθος της αναζήτησης πληροφοριών.

c. **Αποκατάσταση:** Αποκαθιστούμε τις επιπτώσεις από την ζημιά που έχει προκληθεί, αποκτώντας τις κατάλληλες γνώσεις από την διαδικασία με τις οποίες τροφοδοτούμε τον κύκλο της συλλογής και ανάλυσης των πληροφοριών.

Σαφώς και η προληπτική αναζήτηση της απειλής έχει τα πλεονεκτήματα της, όμως είναι μια διαδικασία που απαιτεί ανθρώπους, τεχνολογία και κυρίως γνώση.

Αναπόφευκτα, θα πρέπει να υπάρχει αφοσίωση σε αυτό που πρέπει να γίνει ώστε να υπάρχει πράγματι κάποιο αποτέλεσμα. Εδώ γεννιούνται τα εξής ερωτήματα:

1. Αξίζει αυτή η επένδυση για τον οργανισμό;
2. Πως μπορεί να παρακολουθείται η διαδικασία αυτή στο τι πετυχαίνουμε ώστε να βρούμε τα σημεία που χρήζουν βελτίωση;

Στον παρακάτω πίνακα αναφέρονται οι βασικές μετρήσεις για μια επιτυχημένη προληπτική αναζήτησης της απειλής, τους λόγους για τους οποίους είναι σημαντικές και τι ψάχνουμε ουσιαστικά να βρούμε. Αυτό που είναι σημαντικό, είναι να μετρηθεί με όποιον τρόπο γίνεται ώστε να έχουμε πλήρη ορατότητα της πρόοδού μας. [22]

Βασικές μετρήσεις	**Γιατί είναι σημαντικές / Τι ψάχνουμε**
Αριθμός περιστατικών ανά κρισιμότητα	Δεν θα μπορέσουμε ποτέ να μάθουμε με βεβαιότητα πόσα περιστατικά συμβαίνουν στο δίκτυο μας αλλά το να παρακολουθούμε το ποσοστό που τα

	βρίσκουμε είναι μια καλή μέτρηση για το αποτέλεσμα μας.
Αριθμός των παραβιασμένων συστημάτων ανά κρισιμότητα	Μετρώντας το πόσα συστήματα έχουν παραβιαστεί ανά χρονικά διαστήματα, βοηθάει τους αναλυτές στην κατανόηση της ασφάλειας του δικτύου. Ο αριθμός αυτός μπορεί να περιλαμβάνει και τους υπολογιστές που δεν έχουν ή έχουν ελλιπής ρυθμίσεις ασφαλείας.
Χρόνος παραμονής για τυχόν περιστατικά που ανακαλύφθηκαν	Όταν αυτό είναι εφικτό, θα πρέπει να καταγραφεί για πόσο χρόνο ήταν ενεργές οι απειλές ή τα περιστατικά που βρέθηκαν στο δίκτυο. Αυτό θα βοηθήσει την ομάδα ασφάλειας στο αν αφιερώνει πολύ χρόνο σε κάποιο από στάδια της αλυσίδας κυβερνοεπιθέσεων. Ο χρόνος παραμονής έχει 3 μετρήσεις: ο χρόνος από την μόλυνση μέχρι την ανίχνευση, ο χρόνος από την ανίχνευση μέχρι την διερεύνηση και ο χρόνος από την διερεύνηση μέχρι και την αντιμετώπιση.
Ο αριθμός των κενών ασφάλειας που διορθώθηκαν	Ένας στόχος υψηλού επιπέδου για την αναζήτηση της απειλής είναι η δημιουργία αυτοματοποιημένων ανιχνεύσεων. Ο εντοπισμός και η διόρθωση των κενών ασφάλειας πρέπει να είναι μέρος της ομάδας ασφάλειας.
Εντοπισμός των κενών σε αρχεία καταγραφής που βρέθηκαν και διορθώθηκαν	Τα κενά σε αρχεία καταγραφής μπορούν να δυσκολέψουν την ομάδα ενός SOC για την επίγνωση και το πλαίσιο ασφάλειας. Εντοπίζοντας τα θα βοηθήσουν σημαντικά και την ομάδα που είναι αρμόδια για την αναζήτηση των απειλών.
Ευπάθειες που εντοπίστηκαν	Οι ευπάθειες μπορούν να οδηγήσουν σε εκμετάλλευση και η εκμετάλλευση μπορεί να οδηγήσει σε παραβίαση. Είναι πολύ σημαντικό να βρεθούν οι ευπάθειες και

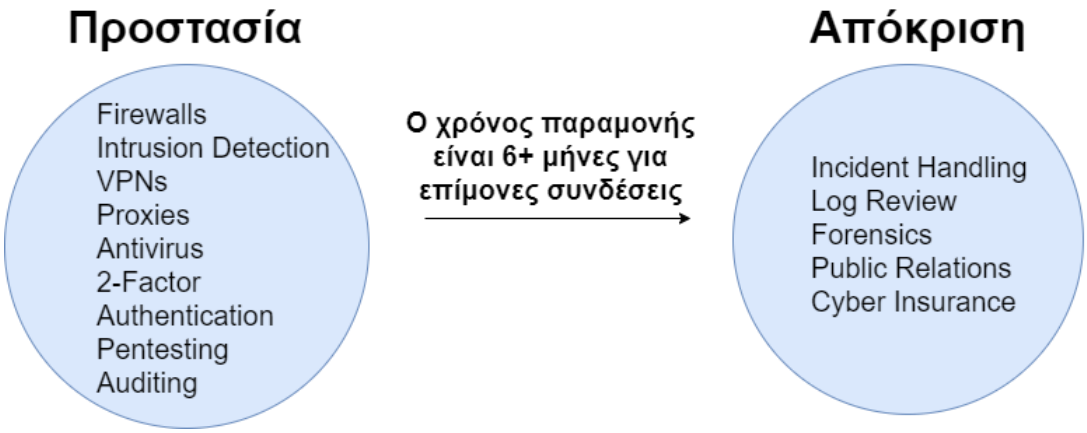
	ακόμα πιο σημαντικό είναι να καταγραφούν.
Μη ασφαλής πρακτικές που εντοπίστηκαν και διορθώθηκαν	Οι μη ασφαλής πρακτικές μπορεί να οδηγήσουν σε μη εξουσιοδοτημένη πρόσβαση και η μη εξουσιοδοτημένη πρόσβαση μπορεί να οδηγήσει σε περιστατικά. Εντοπίζοντας αυτές τις πρακτικές θα βοηθήσουν σημαντικά στην πρόληψη μελλοντικών περιστατικών.
Αριθμός των προληπτικών αναζητήσεων για κυβερνοαπειλές που έγιναν με αυτοματοποιημένο τρόπο	Δεδομένου ότι χρειάζεται να αυτοματοποιηθεί η διαδικασία του εντοπισμού, η ομάδα ασφάλειας θα πρέπει να μετατρέψει κάθε αναζήτηση απειλής να γίνεται με αυτοματοποιημένο τρόπο. Ιδανικά, για κάθε επιτυχημένη αναζήτηση απειλής θα πρέπει να διαμορφώνεται ένας κανόνας ή τουλάχιστον να καταγράφεται ένας δείκτης παραβίασης (IoC).
Εσφαλμένο θετικό ποσοστό των αναζητήσεων για απειλές που έγιναν με αυτοματοποιημένο τρόπο	Ο τρόπος με τον οποίο βρίσκεται ή φτιάχνεται ένας κανόνας για να αυτοματοποιηθεί η διαδικασία, είναι σημαντικός να καταγραφεί για να διαπιστωθεί αν απαιτούνται βελτιώσεις.
Οτιδήποτε νεότερο έχει ανακαλυφθεί	Εκτός από την ανακάλυψη ενός περιστατικού και την δημιουργία νέας απειλής, η προληπτική αναζήτηση της απειλής μπορεί να ενημερώσει τους αναλυτές για τυχόν λάθη στις ρυθμίσεις ασφάλειας που μπορεί να είναι χρήσιμα για μελλοντικές έρευνες.

Πίνακας μετρήσεων για μια επιτυχημένη προληπτική αναζήτηση της απειλής

Η παρακολούθηση τέτοιων μετρήσεων είναι ένα από τα σημαντικότερα οφέλη της προληπτικής αναζήτησης των απειλών μέσα σε έναν οργανισμό. Όπως έχει ήδη αναφερθεί, αντί να περιμένουμε να γίνει η παραβίαση ώστε να λάβουμε περισσότερες πληροφορίες για την ανάπτυξη της ασφάλειας των συστημάτων, η προληπτική αναζήτηση της απειλής μπορεί να βοηθήσει να αναλαμβάνουμε περισσότερες πρωτοβουλίες καθώς και να δημιουργήσουμε

ένα προφίλ απειλών που μπορεί να αντιμετωπίσει ο οργανισμός. Ο αριθμός των ευπαθειών καθώς και ο αριθμός των παραβιασμένων συστημάτων που εντοπίστηκαν είναι κρίσιμες πληροφορίες και ιδιαίτερα ελκυστικές για τα στελέχη ή μέλη του διοικητικού συμβουλίου.

Επιπλέον, αξίζει να σημειωθεί πως σκοπός της προληπτικής αναζήτησης της απειλής είναι να μειώσει το κενό μεταξύ της αστοχίας των μέσων προστασίας και του χρόνου απόκρισης όσο το δυνατόν περισσότερο γίνεται. Έχει αποδειχθεί πως ο χρόνος παραμονής για επίμονες συνδέσεις ξεπερνά τους 6 μήνες.



Εικόνα 3 - Σκοπός της προληπτικής αναζήτησης της απειλής

Έτσι λοιπόν, με βάση όλα τα παραπάνω, δεν αρκεί μόνο η παρακολούθηση των αρχείων καταγραφής για μια επιτυχημένη αναζήτηση της απειλής. Αυτό διότι οι επιτιθέμενοι εξελίσσονται συνεχώς, η παρακολούθηση των αρχείων καταγραφής είναι παλαιά τεχνολογία για την ανίχνευση των επιθέσεων, τα πρωτόκολλα δεν περιγράφουν το τι έχει συμβεί, το ποσοστό για εσφαλμένο θετικό γεγονός (false positive) είναι αρκετά υψηλό και έτσι θα πρέπει να βρίσκουμε νέες ιδέες και να βελτιωνόμαστε συνεχώς.

Ορισμένοι πρακτικοί τρόποι από το που μπορεί να ξεκινήσει η προληπτική αναζήτηση της απειλής είναι: [3]

- Παρακολούθηση της δικτυακής κίνησης από το διαδίκτυο και προς το εσωτερικό δίκτυο στο τείχος προστασίας (firewall).
- Συλλογή πακέτων για περεταίρω ανάλυση (αρχεία pcap)
- Ανάλυση των δεδομένων για μεγάλα χρονικά διαστήματα: Περισσότερα δεδομένα, μεγαλύτερη πιστότητα. Ελάχιστο χρονικό διάστημα οι 12 ώρες, ιδανικό το διάστημα των 24 ωρών.
- Ανάλυση των επικοινωνιών σε ζευγάρια: Για κάθε εσωτερική διεύθυνση IP, την εξωτερική διεύθυνση που συνδέεται. Δεν συστήνεται η παρακολούθηση της εσωτερικής επικοινωνίας καθότι υπάρχει μεγάλη πιθανότητα για false positive.

Αναζήτηση ασυνήθιστης συμπεριφοράς: [3][13]

- Ενδείκτες παραβίασης (IOCs): Περιλαμβάνει δεδομένα forensics (εγκληματολογική εξέταση ψηφιακών πειστηρίων), αρχεία καταγραφής και άλλους παράγοντες που μπορούν να βοηθήσουν στον εντοπισμό πιθανής κακόβουλης δραστηριότητας που έχει ήδη συμβεί.
- Ενδείκτες επίθεσης (IOAs): Παρόμοιοι με τους ενδείκτες παραβίασης, μπορούν να κατανοήσουν την επίθεση που βρίσκεται σε εξέλιξη.
- Δικτυακά ευρήματα (Network-based Artifacts): Αναζήτηση επικοινωνίας για κακόβουλα λογισμικά χρησιμοποιώντας εργαλεία για καταγραφή δικτυακής συνεδρίας, λήψη δικτυακών πακέτων κ.α.
- Συστημικά ευρήματα (Host-based Artifacts): Διερεύνηση τελικών υπολογιστών για αναζήτηση κακόβουλου λογισμικού ή δραστηριότητας στο μητρώο (registry), στα αρχεία του συστήματος, στις προγραμματισμένες εργασίες, στις υπηρεσίες που τρέχουν κατά την εκκίνηση και αλλού.

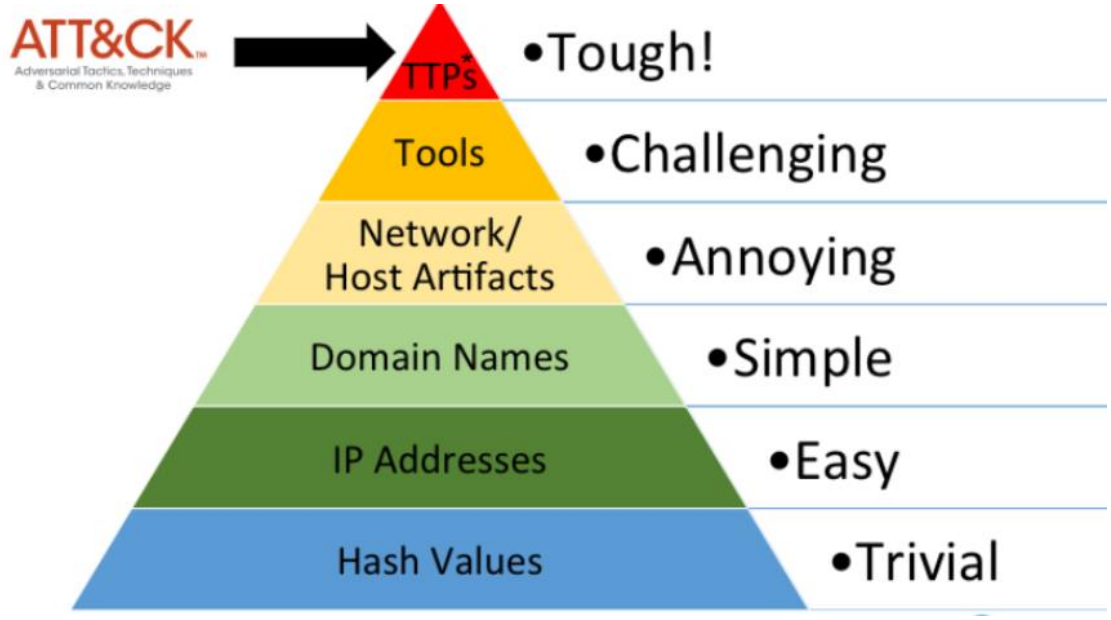
Μπορεί να βρεθεί ασυνήθιστη κίνηση, κατάχρηση πρωτοκόλλων, αναντιστοιχίες θύρας-εφαρμογής, αλλαγές στο σύστημα των αρχείων, ασυνήθιστη συμπεριφορά λογαριασμού, ασυνήθιστος όγκος ανάγνωσης βάσης δεδομένων.

Είναι επίσης σημαντικό να σημειωθεί ότι όταν ξεκινάει η αναζήτηση της απειλής για πρώτη φορά, τα ευρήματα από όλα τα παραπάνω, ενδέχεται να είναι πολλά. Αυτό συμβαίνει διότι δεν έχει γίνει προηγουμένως καμία ενέργεια προληπτικής ανίχνευσης. Αν και μπορεί στην αρχή να είναι ιδιαίτερα δύσκολο και περίεργο καθώς εξετάζονται με την πάροδο του χρόνου, βρίσκοντας νέα περιστατικά που υπήρχαν και δεν είχαν ανιχνευτεί από πριν, είναι αναμφισβήτητα καλό.

Τέλος και εφόσον έχει καθοριστεί ποιο είναι το επίπεδο ωριμότητας του οργανισμού στην προληπτική αναζήτηση της (γνώσεις, άνθρωποι, σύγχρονα λογισμικά, διαδικασίες, σκοπός) ο οργανισμός θα πρέπει να αποφασίσει στο τι πραγματικά θα αναζητήσει. [11] Καθώς η προληπτική αναζήτηση της απειλής διαφέρει από οργανισμό σε οργανισμό, στις παρακάτω ενότητες θα αναφερθούν 3 από τα γνωστότερα μοντέλα επίθεσης στον κυβερνοχώρο. Η πυραμίδα των εμποδίων του David Bianco, το εργαλείο ATT&CK της εταιρείας MITRE και η αλυσίδα κυβερνοεπιθέσεων του Lockheed Martin.

2.1 ΠΥΡΑΜΙΔΑ ΤΩΝ ΕΜΠΟΔΙΩΝ (PYRAMID OF PAIN)

Η προληπτική αναζήτηση της απειλής χρειάζεται ένα μοντέλο κυβερνοεπιθέσεων που μπορεί να αποτελέσει την βάση όταν ξεκινάει η διαδικασία αυτή. Ένα από αυτά είναι και η πυραμίδα των εμποδίων που παρουσιάστηκε για πρώτη φορά το 2013 από τον Lockheed Martin, όταν επικεντρώθηκε στην αντιμετώπιση των περαστικών και στην αντιμετώπιση απειλών με σκοπό την δυνατότητα βελτίωσης της εφαρμογής των δεικτών κυβερνοεπίθεσης. [2]



Εικόνα 4 - Η πυραμίδα των εμποδίων (Pyramid of Pain)

Στο παραπάνω διάγραμμα, κάθε επίπεδο της πυραμίδας αντιπροσωπεύει διαφορετικούς τύπους δεικτών κυβερνοεπίθεσης που μπορούν να χρησιμοποιηθούν για να ανιχνευτούν οι δραστηριότητες των επιτιθέμενων. Ο διαχωρισμός γίνεται με βάση το πόσο πιο δύσκολη θα γίνει η δουλειά τους εάν ο οργανισμός είναι σε θέση να τους αποτρέψει. Όσο ψηλότερο το επίπεδο της πυραμίδας, τόσο περισσότερο χρόνο και πόρους πρέπει να ξοδέψουν οι επιτιθέμενοι.

Για παράδειγμα, εάν ένας επιτιθέμενος χρησιμοποιεί κακόβουλο λογισμικό για να μολύνει κάποιο από τα τελικά σημεία (endpoints) και η πλευρά της ομάδας ασφάλειας χρησιμοποιεί τις τιμές κατακερματισμού (hash values) για να εντοπίσει τέτοια συμπεριφορά, χρειάζεται σχεδόν μηδαμινή προσπάθεια να ανακατασκευάσουν το λογισμικό, ώστε να πάρει διαφορετική τιμή. Αυτό έχει σαν αποτέλεσμα, η αρχική τιμή κατακερματισμού που χρησιμοποιήθηκε για την ανίχνευση του λογισμικού να καταστεί περιττή. Οι επιτιθέμενοι χρησιμοποιούν συνήθως λογισμικά και τα μεταμορφώνουν σε πραγματικό χρόνο, καθώς αυτά λαμβάνονται στα παραβιασμένα μηχανήματα. Από την άλλη πλευρά, αν χρησιμοποιείται έλεγχος ασφάλειας του δικτύου μέσω ελέγχου διευθύνσεων IP, CIDR blocks ή μπλοκάρισμα μαύρων λιστών διευθύνσεων IP για τον εντοπισμό κακόβουλης δραστηριότητας του δικτύου, τότε οι επιτιθέμενοι είναι εύκολο να μεταφέρουν την δικτυακή υποδομή (C&C) σε άλλο δίκτυο, αποδίδοντας ένα νέο εύρος διευθυνσιοδότησης με αποτέλεσμα να μην γίνονται αντιληπτοί.

Παρακάτω αναφέρονται όλα τα επίπεδα της πυραμίδας των εμποδίων και ορισμένες πληροφορίες για αυτά. [2][6]

Hash Values: Είναι εύκολο να βρεθούν και να αλλαχθούν. Οι επιτιθέμενοι χρειάζονται μηδαμινή προσπάθεια για να τα αλλάξουν ή να δημιουργήσουν μια νέα τιμή κατακερματισμού.

IP Addresses: Οι επιτιθέμενοι δεν χρησιμοποιούν την πραγματική διεύθυνση IP τους. Χρησιμοποιούν τεχνολογίες όπως είναι το VPN, το Proxy ή έναν παραβιασμένο server. Εφόσον γίνουν αντιληπτοί, χρειάζεται λίγη περισσότερη προσπάθεια και χρήματα για να τις αλλάξουν. Αυτός είναι ο λόγος που τις καθιστά 1 επίπεδο πάνω από τις τιμές κατακερματισμού.

Domain Names: Το ίδιο εύκολο όπως και οι διευθύνσεις IP για να αλλαχθεί το όνομα χώρου. Χρειάζεται καταχώρηση και συνήθως χρησιμοποιούν την υπηρεσία που προσφέρουν οι πάροχοι για να αποκρύψουν την πληροφορία whois. Χρειάζεται χρόνος για την αλλαγή στους DNS server καθώς και χρήματα. Επίσης, παρότι χρησιμοποιούν bots για την δημιουργία των ονομάτων χώρου, χρειάζεται σκέψη για το όνομα καθώς δεν είναι καθόλου εύκολο.

Network/Host Artifacts: Ευρήματα δικτύου: Ενδείκτες από ενέργειες που κάνουν οι επιτιθέμενοι στο δίκτυο. Τέτοιες ενέργειες είναι τα μοτίβα URI, SMTP επικοινωνίες, ενέργειες HTTP κ.α.
Ευρήματα συστημάτων: Ενδείκτες από ενέργειες που έγιναν στα πληροφοριακά συστήματα. Αυτά περιλαμβάνουν τις αλλαγές στο μητρώο, την μόλυνση των αρχείων κ.α.

Tools: Τα εργαλεία που χρησιμοποιούν οι επιτιθέμενοι. Αυτά μπορεί να περιλαμβάνουν εργαλεία που δημιουργούν μολυσμένα αρχεία για επιθέσεις phishing, ή δημιουργία κακόβουλων υπηρεσιών / προγραμματισμένων εργασιών για απομακρυσμένη πρόσβαση σε C&C (Command & Control) μηχάνημα. Σαφώς και είναι ανώτερο από τα υπόλοιπα επίπεδα της πυραμίδας καθώς θα πρέπει τις περισσότερες φορές να φτιάξουν τα δικά τους εργαλεία για να αποφύγουν την ανίχνευση από τα λογισμικά ανίχνευσης.

TTPs: Τεχνικές, τακτικές και διαδικασίες των επιτιθέμενων. Το ανώτερο επίπεδο της πυραμίδας και το πιο δύσκολο για την ομάδα ασφάλειας. Χρειάζεται συνδυασμός όλων των παραπάνω για να ανιχνευθούν οι τακτικές, οι τεχνικές και οι διαδικασίες των επιτιθέμενων, σε συνδυασμό με την συλλογή πληροφοριών κυβερνοαπειλών για να κατανοήσουν τους σκοπούς και τα κίνητρα των επιτιθέμενων. Αξίζει να σημειωθεί πως αν η ομάδα ασφάλειας του οργανισμού φτάσει σε αυτό το σημείο ανίχνευσης, τότε οι επιτιθέμενοι έχουν 2 μόνο επιλογές: Να παραιτηθούν από τις ενέργειες ή την αποστολή τους ή να φτιάξουν τις TTPs από την αρχή.

Τέλος, κάθε επίπεδο στην πυραμίδα των εμποδίων είναι μια ευκαιρία εντοπισμού και πρόληψης διαφόρων δεικτών κυβερνοεπιθέσεων. Οι τιμές κατακερματισμού (hash values), οι διευθύνσεις IP και τα ονόματα χώρων είναι εξαιρετικά προσπελάσιμες και μπορούν να βρεθούν

σε κοινότητες συλλογής και διαμοιρασμού πληροφορίων για νέες κυβερνοεπιθέσεις. Είναι επίσης δυνατό να βρεθούν ευρήματα συστημάτων και δικτύου, αλλά τα σύγχρονα λογισμικά ασφάλειας ενσωματώνουν την ικανότητα εντοπισμού αποτροπής τεχνικών, τεχνικών και διαδικασιών των επιτιθέμενων (TTPs). Εφόσον υπάρχουν οι δυνατότητες ανίχνευσης και πρόληψης κάθε επιπέδου της πυραμίδας, είναι σημαντικό να επικυρωθούν, προσομοιώνοντας τις επιθέσεις των κακόβουλων σε κάθε επίπεδο και αποδεικνύοντας την πραγματική αποτελεσματικότητα της ασφάλειας των συστημάτων του οργανισμού.

2.2 MITRE ATT&CK

Το MITRE ATTK&CK είναι μια παγκοσμίως προσβάσιμη βάση γνώσης τακτικών και τεχνικών που χρησιμοποιούν οι επιτιθέμενων στον κυβερνοχώρο για την επίτευξη ενός συγκεκριμένου στόχου. Το MITRE ATT&CK χρησιμοποιείται ως βάση για την ανάπτυξη συγκεκριμένων μοντέλων και μεθοδολογιών απειλών στην ευρύτερη κοινότητα του κυβερνοχώρου, όπως είναι ο ιδιωτικός τομέας, η κυβέρνηση κ.α. [16]

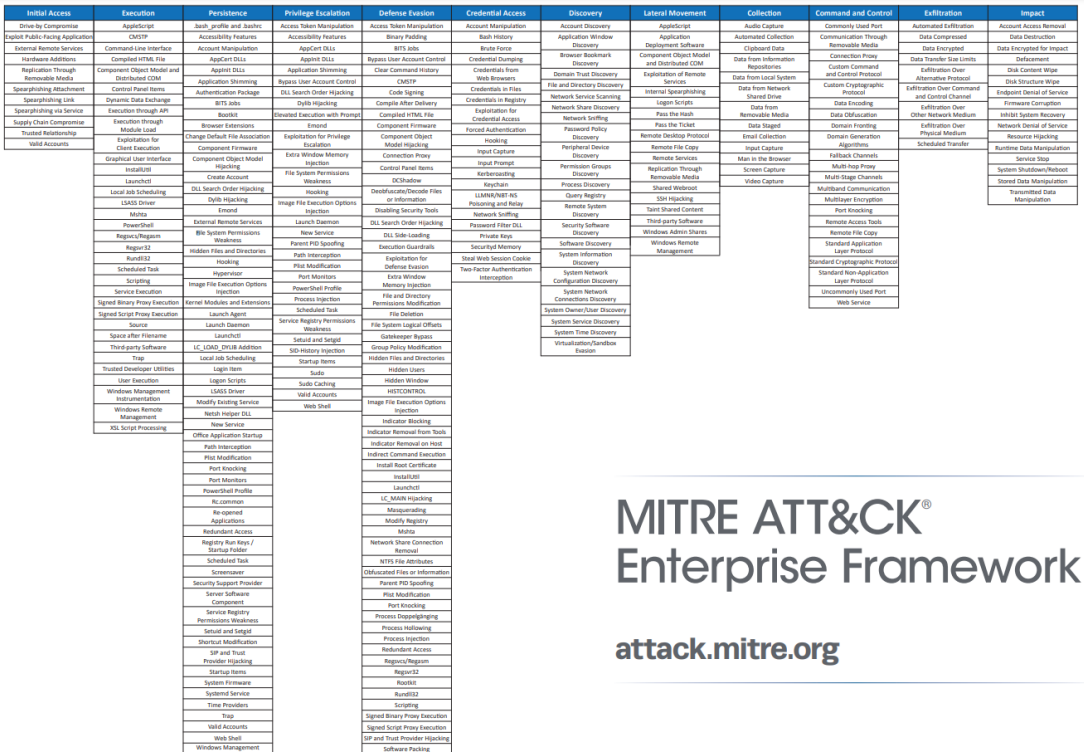
Με την δημιουργία του MITRE ATT&CK, η εταιρεία MITRE εκπληρώνει την δυνατότητα επίλυσης προβλημάτων σχετικά με τις κυβερνοεπιθέσεις για έναν ασφαλέστερο κόσμο, φέρνοντας κοινότητες ασφάλειας σε επαφή, για την ανάπτυξη και την αποτελεσματική ασφάλεια στον κυβερνοχώρο. Είναι επίσης διαθέσιμο για όλα τα λειτουργικά και σε οποιοδήποτε άτομο ή οργανισμό για χρήση χωρίς καμία χρέωση.

Η κατηγοριοποίηση των τεχνικών των επιτιθέμενων γίνεται ως εξής:

1. **Αναγνώριση (Reconnaissance):** Συλλογή πληροφοριών για τον προγραμματισμό μελλοντικών επιθέσεων, για παράδειγμα πληροφορίες του οργανισμού.
2. **Ανάπτυξη πόρων (Resource Development):** Δημιουργία πόρων για την ανάπτυξη των λειτουργιών, για παράδειγμα το στήσιμο μιας υποδομής C&C (Απομακρυσμένος έλεγχος και διαχείριση εντολών)
3. **Αρχική πρόσβαση (Initial Access):** Προσπάθεια για την πρόσβαση στο δίκτυο του οργανισμού, για παράδειγμα μια καμπάνια phishing e-mail.
4. **Εκτέλεση (Execution):** Δοκιμή του κακόβουλου κώδικα/λογισμικού, όπως για παράδειγμα η εκτέλεση ενός εργαλείου απομακρυσμένης πρόσβασης.
5. **Επιμονή (Persistence):** Προσπάθεια για διατήρηση της πρόσβασης, όπως για παράδειγμα η αλλαγή των αρχείων ρυθμίσεων.
6. **Κλιμάκωση των προνομίων (Privilege Escalation):** Προσπάθεια για απόκτηση πρόσβασης ανωτέρου επιπέδου, όπως για παράδειγμα η απόκτηση ενός λογαριασμού διαχειριστή της εταιρείας.

7. **Αμυντική αποφυγή (Defense Evasion):** Προσπάθεια αποφυγής του εντοπισμού, δηλαδή χρήση αξιόπιστων διαδικασιών για την απόκρυψη του κακόβουλου λογισμικού.
8. **Πρόσβαση διαπιστευτηρίων (Credential Access):** Κλοπή ονομάτων και κωδικών πρόσβασης λογαριασμών.
9. **Ανακάλυψη (Discovery):** Προσπάθεια για ανακάλυψη του δικτύου με αποτέλεσμα να δουν τι μπορούν να ελέγξουν.
10. **Πλευρική κίνηση (Lateral Movement):** Μετακίνηση στο δίκτυο χρησιμοποιώντας τακτικές για είσοδο και απόκτηση πρόσβασης σε πολλαπλά συστήματα.
11. **Συλλογή (Collection):** Συλλογή των δεδομένων που ενδιαφέρουν τον στόχο του αντιπάλου, δηλαδή πρόσβαση σε δεδομένα αποθήκευσης.
12. **Εντολή και έλεγχος (Command and Control):** Επικοινωνία με παραβιασμένα συστήματα που ελέγχουν, προσπαθούν να μιμηθούν την κανονική, αναμενόμενη κίνηση για να αποφύγουν τον εντοπισμό.
13. **Εξαγωγή δεδομένων (Exfiltration):** Κλοπή δεδομένων και μεταφορά σε άλλον λογαριασμό, για παράδειγμα στο cloud.
14. **Επίπτωση (Impact):** Χειρισμός, διακοπή ή καταστροφή συστημάτων και δεδομένων, όπως για παράδειγμα η κρυπτογράφηση τους (ransomware).

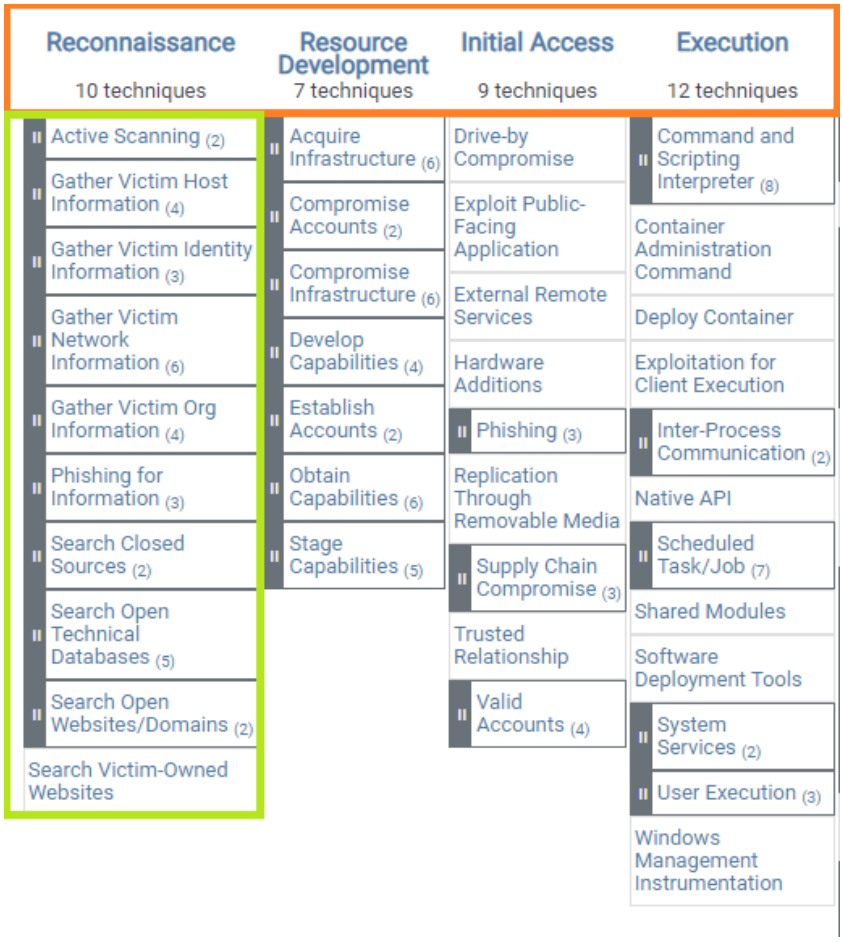
Μέσα σε κάθε τεχνική του πίνακα της MITRE υπάρχουν οι τεχνικές των επιτιθέμενων οι οποίες περιγράφουν την πραγματική δραστηριότητα που εκτελείται από αυτούς. Ορισμένες τεχνικές έχουν και υπό-τεχνικές που εξηγούν πως ένας επιτιθέμενος εκτελεί μια συγκεκριμένη τεχνική με περισσότερες λεπτομέρειες. Ο πλήρης πίνακας ATT&CK για επιχειρήσεις παρουσιάζεται παρακάτω:



Εικόνα 5 - MITRE ATT&CK (https://attack.mitre.org/matrices/enterprise)

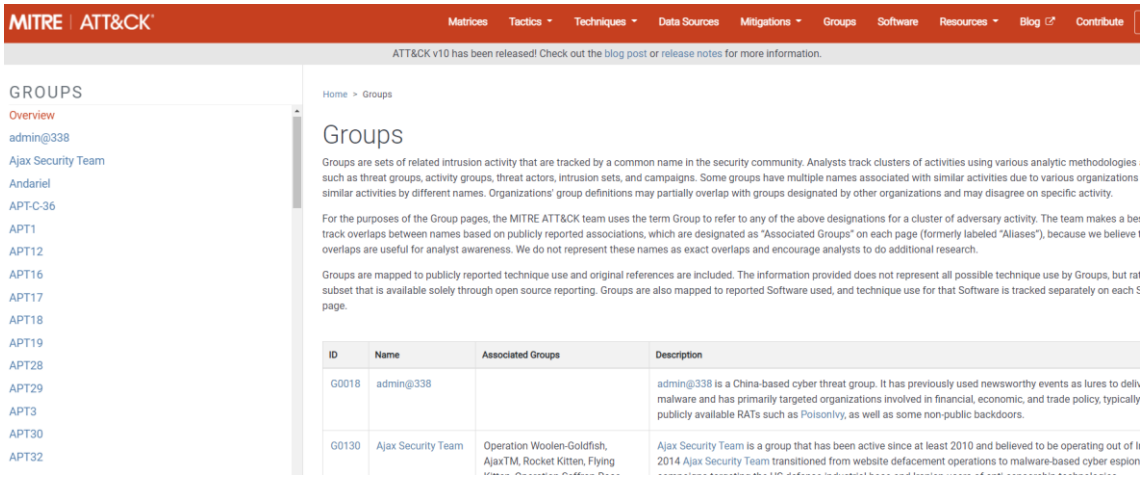
Ο παραπάνω πίνακας διαβάζεται ως εξής:

Οι τακτικές βρίσκονται στην κορυφή και οι τεχνικές, ο τρόπος με τον οποίοι οι αντίπαλου επιτυγχάνουν τις τακτικές. Η ίδια τεχνική μπορεί να βρίσκεται σε διαφορετικές τακτικές.



Εικόνα 6 - Τακτικές / Τεχνικές του πίνακα ATT&CK

Η σελίδα ομάδων απειλών στον ιστότοπο της MITRE παρέχει μια λίστα για όλες τις προηγμένες ομάδες απειλών που έχει παρακολουθήσει η εταιρεία MITRE. Για κάθε ομάδα απειλών υπάρχουν αναλυτικές λεπτομέρειες. Ορισμένες από τις λεπτομέρειες που αναφέρονται για κάθε ομάδα απειλής περιλαμβάνουν τις τακτικές και το λογισμικό που χρησιμοποιούν, καθώς και αναφορές για περισσότερη έρευνα.

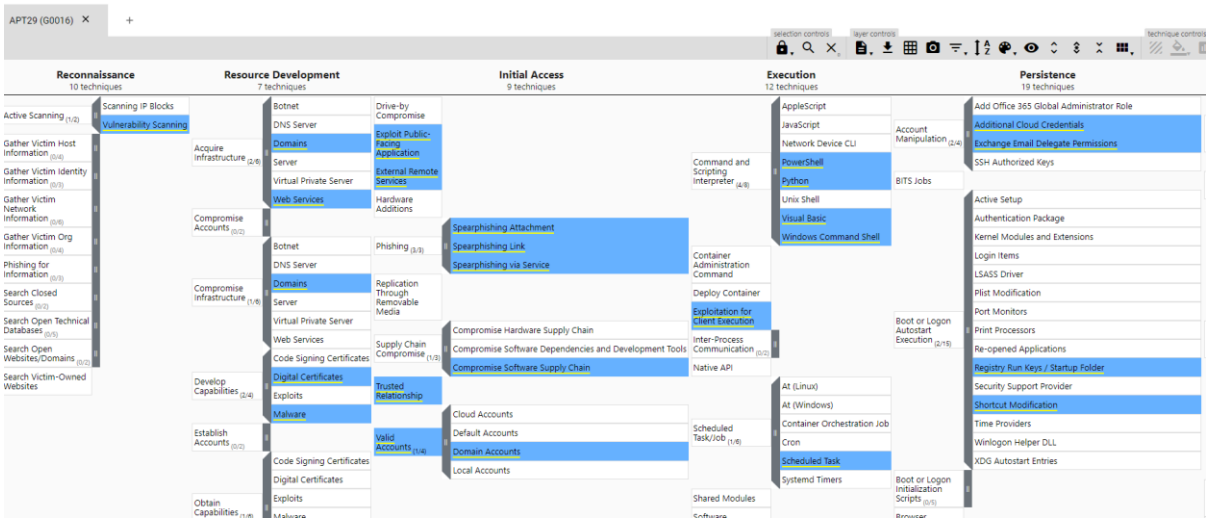


Εικόνα 7 - Σελίδα ομάδων απειλών (https://attack.mitre.org/groups/)

Επιπλέον, το εργαλείο ATT&CK Navigator, έχει σχεδιαστεί για να βοηθήσει την πλοήγηση του πίνακα ATT&CK. Ένα από τα πολλά χρήσιμα χαρακτηριστικά του είναι η χρήση των παρεχόμενων φίλτρων για την επισήμανση τεχνικών που χρησιμοποιούνται από μια συγκεκριμένη ομάδα απειλών. Αυτό είναι χρήσιμο για τον εντοπισμό των τεχνικών που μπορεί να είναι σημαντικές για τον οργανισμό.

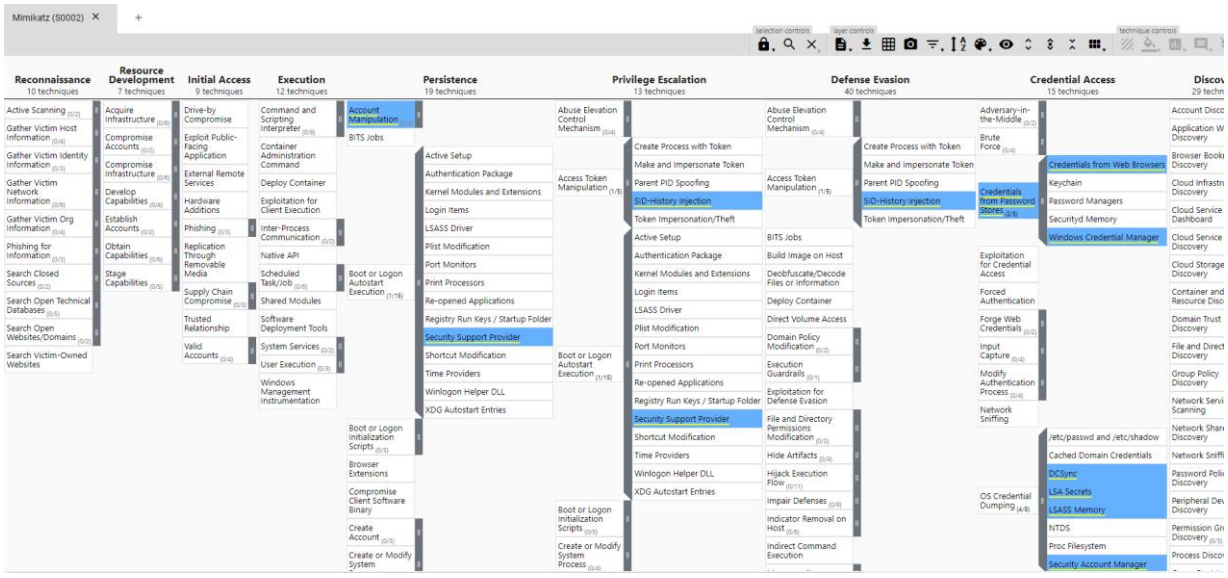
Εικόνα 8 - MITRE ATT&CK Navigator (https://mitre-attack.github.io/attack-navigator/)

Αν πάρουμε για παράδειγμα μια ομάδα κυβερνοεπιθέσεων από την σελίδα ομάδων απειλών, με την χρήση του ATT&CK Navigator, μπορούμε να δούμε σε απλούστερη μορφή τις τεχνικές και τις διαδικασίες που χρησιμοποιούν:



Εικόνα 9 - Τεχνικές και διαδικασίες συγκεκριμένης ομάδας απειλών με την χρήση του ATT&CK Navigator

Το ίδιο ισχύει και για συγκεκριμένο λογισμικό όπως είναι το Mimikatz για την απόκτηση χρηστών και των κωδικών πρόσβασης.



Εικόνα 10 - Mimikatz ATT&CK Navigator

Το ATT&CK μπορεί να βοηθήσει πολύ έναν οργανισμό να δημιουργήσει μια άμυνα απέναντι στην απειλή. Το σημαντικό είναι να γίνει η αρχή σε ότι μπορεί να πραγματοποιηθεί από την πλευρά του οργανισμού, όπως είναι η ανίχνευση, η συλλογή πληροφοριών για νέες

κυβερνοαπειλές, η προληπτική αναζήτηση της απειλής κ.α. Το σημείο εκκίνησης θα πρέπει να επιλεγεί από την ομάδα ασφάλειας του οργανισμού με βάση την λειτουργία του.

Για τον οργανισμό που δεν διαθέτει ομάδα για να πραγματοποιήσει τις επιθέσεις, η εταιρεία MITRE υποστηρίζει το CALDERA το οποίο αυτοματοποιεί και σχεδιάζει την διαδικασία αυτή και είναι διαθέσιμο για χρήση ως μια λύση ανοιχτού κώδικα.

Εικόνα 11 - MITRE / CALDERA

Επιπλέον, το CASCADE είναι ένα ακόμη ερευνητικό έργο το οποίο υποστηρίζεται από την MITRE και επιδιώκει να αυτοματοποιήσει μεγάλο μέρος της εργασίας που θα εκτελούσε η μπλε ομάδα για να προσδιορίσει το εύρος και την κακόβουλη συμπεριφορά ύποπτης συμπεριφοράς σε ένα δίκτυο, χρησιμοποιώντας τα δεδομένα κεντρικού υπολογιστή.

Ορισμένα σημεία και βέλτιστες πρακτικές που πρέπει να λάβει υπόψιν ο οργανισμός προτού χρησιμοποιήσει το ATT&CK ως μέρος της ασφάλειας των δεδομένων του είναι:

1) Επικοινωνία και διαμοιρασμός της γνώσης των τεχνικών ATT&CK στα μέλη της ομάδας.

2) Όταν πρόκειται να γίνει μια διείσδυση στα συστήματα του οργανισμού, να χρησιμοποιούνται οι πραγματικές τακτικές από την σελίδα των ομάδων απειλών της MITRE.

3) Προσδιορισμός των κενών ασφάλειας με τον πίνακα της MITRE και εφαρμογή λύσεων για αυτά.

4) Δεν θα πρέπει ποτέ να ληφθεί υπόψιν ότι εφόσον μπορεί να αμυνθεί ενάντια σε μια τεχνική με έναν τρόπο, δεν θα γίνει αντιληπτή μια διαφορετική εφαρμογή της

τεχνικής αυτής. Για παράδειγμα αν το antivirus του οργανισμού ανιχνεύσει ένα κακόβουλο λογισμικό, αυτό δεν σημαίνει σε καμία περίπτωση ότι θα πιάσει και ένα άλλο εργαλείο ίδιας τεχνικής. Θα πρέπει να είναι σε θέση και ενήμερος για τις διαφορετικές υλοποιήσεις αυτών των τεχνικών.

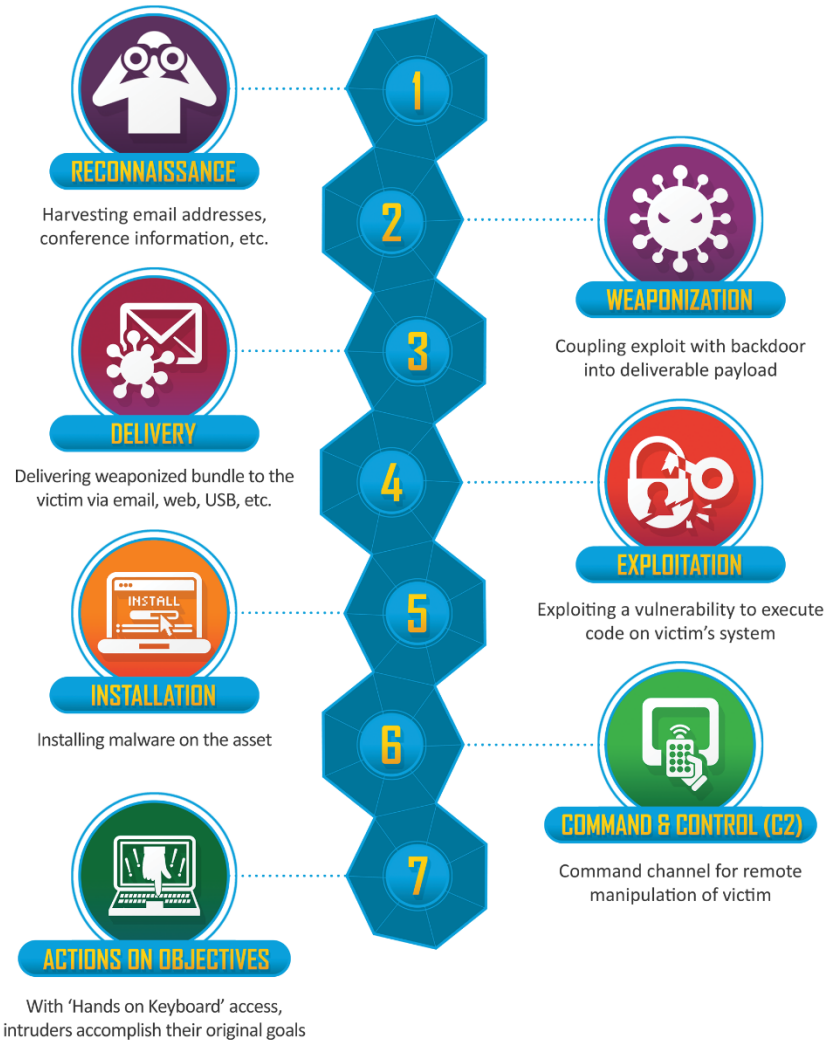
Τέλος, αξίζει να σημειωθεί πως δεν πρέπει να θεωρηθεί κακόβουλη κάθε συμπεριφορά που ταιριάζει σε μια τεχνική ATT&CK. Η διαγραφή αρχείου, για παράδειγμα, είναι μια τακτική που εφαρμόζουν οι επιτιθέμενοι για να μην γίνουν αντιληπτοί και αναφέρεται στον πίνακα ως Defense Evasion, κάτι το οποίο είναι απολύτως λογικό. Εδώ θα πρέπει ο οργανισμός να είναι σε θέση να διακρίνει τις κανονικές διαγραφές αρχείων από τις προσπάθειες ενός επιτιθέμενου που προσπαθεί να αποφύγει τον εντοπισμό. Ομοίως, ορισμένες τεχνικές ATT&CK είναι δύσκολο να εντοπιστούν όπως για παράδειγμα μια διήθηση μέσω εναλλακτικού πρωτοκόλλου. Η ικανότητα να ανακαλύπτουμε τεχνικές που είναι δύσκολο να βρεθούν, είναι το κλειδί για μια μακροπρόθεσμη στρατηγική ασφάλειας των δεδομένων του οργανισμού.

2.3 ΑΛΥΣΙΔΑ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΩΝ (CYBER KILL CHAIN)

Μια ακόμη μέθοδος για την ανάλυση των φάσεων της επίθεσης στον κυβερνοχώρο είναι και η αλυσίδα των κυβερνοεπιθέσεων (Cyber Kill Chain). Περιλαμβάνει όλα τα στάδια της δράσης των επιτιθέμενων και επιδιώκει να ορίσει και να κατηγοριοποιήσει τις ενέργειες που κάνει ο επιτιθέμενος κατά την διάρκεια μιας επίθεσης. [14]

Όπως και με το MITRE ATT&CK, οι ομάδες ασφάλειας μπορούν με την χρήση της αλυσίδας να αναγνωρίσουν συμπεριφορές επίθεσης και να τις ταξινομούν στα διάφορα στάδια της επίθεσης. Η αλυσίδα κυβερνοεπιθέσεων έχει αποδειχθεί πως μπορεί να χρησιμοποιηθεί για τον εντοπισμό και την πρόβλεψη μιας επίθεσης APT (Advanced Persistent Threat) καθώς και την αξιολόγηση της σοβαρότητας της αναζήτησης των απειλών, διασφαλίζοντας ότι εστιάζει σε όλο το φάσμα της δράσης των επιτιθέμενων.

Στην παρακάτω εικόνα απεικονίζεται η αλυσίδα των κυβερνοεπιθέσεων καθώς και οι δράσεις των επιτιθέμενων. Κάθε στάδιο σχετίζεται με έναν συγκεκριμένο τύπο δραστηριότητας σε μια επίθεση στον κυβερνοχώρο, ανεξάρτητα από το αν πρόκειται για εσωτερική ή εξωτερική επίθεση. [14]



Εικόνα 12 - Αλυσίδα κυβερνοεπιθέσεων (The Cyber Kill Chain)

Κάθε φάση της αλυσίδας είναι και μια ευκαιρία για να σταματήσει μια κυβερνοεπίθεση που βρίσκεται σε εξέλιξη. Με τα κατάλληλα εργαλεία για τον εντοπισμό και την αναγνώριση της συμπεριφοράς κάθε σταδίου, ο οργανισμός μπορεί να αμυνθεί καλύτερα από μια μελλοντική παραβίαση συστημάτων ή δεδομένων.

Σε γενικές γραμμές, και τα δύο συστήματα ακολουθούν το ίδιο μοτίβο. Η κύρια διαφορά μεταξύ των δύο είναι ότι η βάση δεδομένων ATT&CK είναι περισσότερο μια λίστα τεχνικών ανά τακτική και δεν προτείνει μια συγκεκριμένη σειρά λειτουργιών.

Κεφάλαιο 3 – Συλλογή πληροφοριών (Cyber Threat Intelligence)

Ο κλάδος της κυβερνοασφάλειας αντιμετωπίζει πολλές προκλήσεις – ολοένα και πιο επίμονοι κακόβουλοι προσπαθούν να παραβιάσουν τα συστήματα ασφαλείας με σκοπό την απόκτηση σημαντικών πληροφοριών και δεδομένων. Η έλλειψη ειδικευμένων επαγγελματιών σε έναν οργανισμό, οδηγεί σε πολλές «ξένες» πληροφορίες, ψευδείς συναγερμούς σε πολλαπλά μη συνδεδεμένα συστήματα ασφαλείας κ.α.

Παρόλο που τα επόμενα χρόνια θα δαπανηθούν πολλά δισεκατομμύρια παγκοσμίως σε προϊόντα και υπηρεσίες κυβερνοασφάλειας, αυτό δεν θα είναι αρκετό γιατί: [1]

- ✓ Τα ¾ των οργανισμών αντιμετωπίζουν προβλήματα έλλειψης δεξιοτήτων
- ✓ Το 44% των ειδοποιήσεων σε θέματα ασφάλειας δεν έχει διερευνηθεί
- ✓ Το 66% των εταιρειών παραβιάζονται τουλάχιστον 1 φορά

(Πηγές: Gartner Forecast Analysis: Information Security, Worldwide, 2Q21 Update; ESG & ISSA Research Report: The Life and Times of Cybersecurity Professionals 2021; Cisco 2021 Annual Cybersecurity Report; Ponemon Institute 2020 Cost of Data Breach Report;)

Στην σημερινή εποχή, οι ψηφιακές τεχνολογίες βρίσκονται στο επίκεντρο σχεδόν του κάθε κλάδου. Η αυτοματοποίηση και η μεγαλύτερη διασύνδεση που προσφέρουν φέρνουν τον ψηφιακό μετασχηματισμό, αλλά φέρνουν επίσης και μεγαλύτερη ευπάθεια στις επιθέσεις στον κυβερνοχώρο.

Η συλλογή πληροφοριών μέσω του Threat Intelligence βοηθά στο να ξεπεραστεί η υπερφόρτωση πληροφοριών και παρέχει τις πιο σχετικές πληροφορίες για συγκεκριμένες απειλές και πηγές επιθέσεων που συμβαίνουν στον κυβερνοχώρο. Συνήθως, είναι δύσκολο να εντοπιστούν από τους μηχανικούς ασφαλείας, οι οποίοι έχουν πρόσβαση μόνο σε πληροφορίες που αφορούν στα δικά τους δίκτυα. Επιπλέον, τους επιτρέπει να δημιουργούν προσαρμοσμένους κανόνες για την απόκτηση συγκεκριμένων πληροφοριών του οργανισμού για τους οποίους ενδιαφέρονται. Οι πολύτιμες πληροφορίες που λαμβάνουν, περιλαμβάνουν για παράδειγμα τον αριθμό των εξειδικευμένων απειλών που έχουν παρατηρηθεί παγκοσμίως, τις διευθύνσεις URL που περιέχουν κακόβουλο κώδικα, τη συμπεριφορά του κακόβουλου χρήστη και άλλα πολλά. [12]

Με λίγα λόγια, το Threat Intelligence αποτελεί την οργάνωση, την ανάλυση και την εξειδίκευση πληροφοριών των απειλών που αφορούν πιθανές ή τρέχουσες κυβοερνοεπιθέσεις που στοχοποιούν έναν οργανισμό. Επίσης, πολλοί κατασκευαστές παρέχουν πληροφορίες για κυβερνοαπειλές όπως τα εργαλεία που χρησιμοποιούνται. Κάθε ημέρα, η ομάδα ασφάλειας θα πρέπει να συλλέγει πληροφορίες όχι μόνο για ενδείκτες

παραβίασης (IOCs) αλλά για ενδείκτες επίθεσης (IOAs) και για αδυναμίες που θα μπορούσαν να εκμεταλλευτούν οι επιτιθέμενοι (IOEs). [12]

Στην παρακάτω εικόνα παρατίθενται οι μετρήσεις που δείχνουν τις μεγάλες βελτιώσεις στην ασφάλεια και την αποτελεσματικότητα ενός εργαλείου συλλογής πληροφοριών. [1]

Εικόνα 13 - Αποτελεσματικότητα εργαλείου συλλογής πληροφοριών - Πηγή: IDC

Όταν συλλέγουμε τέτοιες πληροφορίες είναι σημαντικό να τις κατηγοριοποιούμε σε τρία διαφορετικά επίπεδα όπως αυτά φαίνονται παρακάτω: [1]

Εικόνα 14 - Επίπεδα δεδομένων συλλογής πληροφοριών Threat Intelligence

Το ανώτερο και υψηλότερο επίπεδο (Strategic) παρέχει μια ευρεία επισκόπηση του τοπίου των απειλών ενός οργανισμού. Το περιεχόμενο είναι γενικά επιχειρηματικό, παρουσιάζεται μέσω αναφορών ή ενημερώσεων και είναι πολύ χρήσιμο για να ενημερώσει τα ανώτερα στελέχη για λήψη αποφάσεων. Το υλικό αυτό δεν μπορεί να δημιουργηθεί από τα συστήματα αλλά μόνο από ανθρώπους με εξειδίκευση, διότι απαιτείται χρόνος για σκέψη και αξιολόγηση νέων τακτικών, τεχνικών και διαδικασιών των επιτιθέμενων έναντι των υπάρχοντών συστημάτων ασφαλείας. Βεβαίως και αυτές οι διαδικασίες μπορούν να αυτοματοποιηθούν αλλά απαιτείται σε μεγάλο βαθμό ο ανθρώπινος παράγοντας για την ολοκλήρωση της άσκησης αυτής.

Το μεσαίο επίπεδο (Operational) περιλαμβάνει την γνώση για τις τρέχουσες κυβερνοεπιθέσεις και εκστρατείες. Παρέχει εξειδικευμένες πληροφορίες στις ομάδες ασφάλειας που βοηθούν να κατανοήσουν την φύση, την πρόθεση και το χρονοδιάγραμμα συγκεκριμένων επιθέσεων.

Το τελευταίο επίπεδο (Tactical) περιλαμβάνει πληροφορίες για τις τακτικές, τεχνικές και διαδικασίες των επιτιθέμενων και πως μπορεί ο οργανισμός να αμυνθεί σε αυτές. Χρησιμοποιείται συνήθως από την ομάδα ασφάλειας ή τους διαχειριστές των συστημάτων του οργανισμού λόγω των τεχνικών πληροφοριών.

Στην πραγματικότητα, η συλλογή πληροφοριών για κυβερνοαπειλές προσθέτει μεγάλη αξία στην ασφάλεια και τις λειτουργίες των οργανισμών ανεξαρτήτου μεγέθους. Μπορεί λοιπόν να ενσωματωθεί με τις λύσεις ασφάλειας που ήδη χρησιμοποιούν, βοηθώντας έτσι ώστε να δίνουν αυτόματα προτεραιότητα για νέες απειλές και να φιλτράρουν τις ειδοποιήσεις που λαμβάνουν.

Στις επόμενες ενότητες θα δούμε πως ο οργανισμός μπορεί να συλλέξει πληροφορίες που αφορούν κυβερνοαπειλές και θα παρουσιαστούν τα εργαλεία MISP και Minemeld ως τα εργαλεία συλλογής και διαμοιρασμού πληροφοριών.

3.1 ΕΙΣΑΓΩΓΗ ΣΤΟ MISP

Το MISP είναι μια λύση λογισμικού ανοιχτού κώδικα για τη συλλογή, αποθήκευση, διανομή και κοινή χρήση δεικτών παραβίασης στον κυβερνοχώρο σχετικά με την ανάλυση περιστατικών ασφάλειας, απειλών και την ανάλυση κακόβουλου λογισμικού. Το MISP έχει σχεδιαστεί από και για αναλυτές συμβάντων, επαγγελματιών ασφάλειας για την υποστήριξη των καθημερινών λειτουργιών τους και την αποτελεσματική κοινή χρήση πληροφοριών. [15]

Στόχος του MISP είναι να προωθήσει την ανταλλαγή δομημένων πληροφοριών στις κοινότητες ασφάλειας παγκοσμίως. Το MISP παρέχει λειτουργίες για την υποστήριξη της ανταλλαγής πληροφοριών αλλά και της συλλογής αυτών από συστήματα ανίχνευσης εισβολής δικτύου (NIDS), εργαλεία ανάλυσης αρχείων καταγραφής κ.α.

Τα βασικά πλεονεκτήματα χρήσης του MISP είναι: [15]

1. Επιτρέπει στον οργανισμό να έχει έναν πιο ισχυρό και δομημένο τρόπο αποθήκευσης των δεδομένων του σχετικά με τις απειλές που έχει να αντιμετωπίσει, όπως είναι οι διευθύνσεις IP, domain names, διευθύνσεις e-mail που σχετίζονται με απειλές κ.λπ.

2. Έχει την δυνατότητα να συνδυάζει την βάση δεδομένων με άλλες βάσεις δεδομένων MISP σε μια ενιαία μεγάλη βάση δεδομένων.

3. Υπάρχει ιστορικό γεγονότων για απειλές και παρέχεται η δυνατότητα αναζήτησης, όπου η πλατφόρμα συνδέει αυτόματα παλαιά δεδομένα με νέα γεγονότα που εισάγονται στο σύστημα. Είναι σαν μια μηχανή αναζήτησης για τα γεγονότα που απειλούν τους οργανισμούς και τι έκαναν για αυτά. Αυτό μπορεί να βοηθήσει πολύ έναν οργανισμό καθώς τον κάνει πιο γρήγορο και ευέλικτο για νέες κυβερνοαπειλές.

4. Οι προγραμματιστές του MISP κατανοούν τις προκλήσεις που παρουσιάζονται με την κοινή χρήση πληροφοριών και έχουν υλοποιήσει την ιδέα της κοινής χρήσης διαμοιρασμού πληροφοριών μεταξύ των κοινοτήτων ασφάλειας ώστε οι ερευνητές ασφάλειας να μπορούν επιλέξουν τι θα μοιραστούν και με ποιον.

5. Το MISP επιτρέπει επίσης σε έναν οργανισμό να απορροφά πληροφορίες απειλών από μια άλλη δημόσια λίστα πληροφοριών για νέες απειλές που συμμετέχουν αξιόπιστες πηγές όπως η αστυνομία και οι ερευνητές ασφάλειας (π.χ. ESET). Με

αυτόν τον τρόπο ο οργανισμός ενισχύει την ποιότητα των πληροφοριών του και μπορεί να συγκρίνει τα νέα γεγονότα που δέχεται με παλαιό ιστορικό.

Το MISP δεν είναι μόνο μια πλατφόρμα διαμοιρασμού πληροφορίων για τις απειλές στον κυβερνοχώρο αλλά ένα σημαντικό εργαλείο για περαιτέρω έρευνα των απειλών. Έχει αποδειχθεί πως είναι απαιτούμενο και χρήσιμο για έναν οργανισμό που θέλει να είναι ενημερωμένος για τις απειλές στον κυβερνοχώρο.

3.2 ΕΓΚΑΤΑΣΤΑΣΗ & ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΗ MISP

Οι απαιτούμενοι πόροι για την εγκατάσταση του MISP εξαρτούνται πολύ από τον αριθμό των χαρακτηριστικών ή γεγονότων και αν πρόκειται για μεγάλο όγκο πληροφοριών. Οι παράγοντες που θα πρέπει να εξεταστούν πριν την εγκατάσταση είναι αν η κοινότητα του οργανισμού είναι ιδιωτική και αν συλλέγεται πληροφορία από άλλες κοινότητες ή αν διαμοιράζεται η πληροφορία σε εξωτερικές κοινότητες (εμπιστευτικές ή μη). Επίσης, θα πρέπει να ληφθεί υπόψιν η πληροφορία για το αν συμπεριληφθούν αυτόματα εργαλεία που θα τροφοδοτούν το MISP.

Η εγκατάσταση μπορεί να πραγματοποιηθεί με 2 τρόπους:

1. Με την εγκατάσταση μιας έτοιμης εικονικής μηχανής από την ιστοσελίδα του MISP: https://vm.misp-project.org/latest

   Υπάρχουν διαθέσιμες εκδόσεις για τα λογισμικά VMWare και VirtualBox.

2. Εγκατάσταση μέσω docker

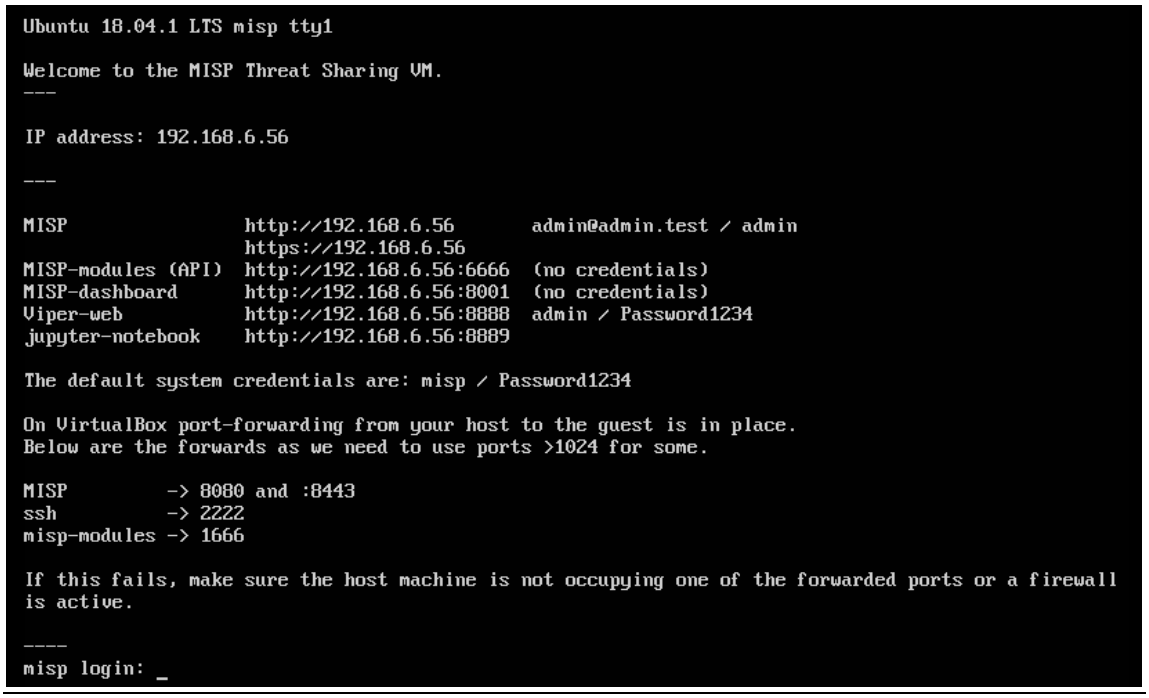
```
chrisgourz@ubuntu2020:~$ git clone https://github.com/coolacid/docker-misp.git
Cloning into 'docker-misp'...
remote: Enumerating objects: 892, done.
remote: Counting objects: 100% (203/203), done.
remote: Compressing objects: 100% (160/160), done.
remote: Total 892 (delta 89), reused 126 (delta 43), pack-reused 689
Receiving objects: 100% (892/892), 152.08 KiB | 1.13 MiB/s, done.
Resolving deltas: 100% (436/436), done.
```

Εικόνα 15 - Εγκατάσταση MISP μέσω docker (1)

```
chrisgourz@ubuntu2020:~/docker-misp$ sudo docker-compose -f docker-compose.yml up -d
dockermisp_db_1 is up-to-date
dockermisp_redis_1 is up-to-date
dockermisp_mail_1 is up-to-date
Starting dockermisp_misp_1 ...
Starting dockermisp_misp_1 ... done
```

Εικόνα 16 - Εγκατάσταση MISP μέσω docker (2)

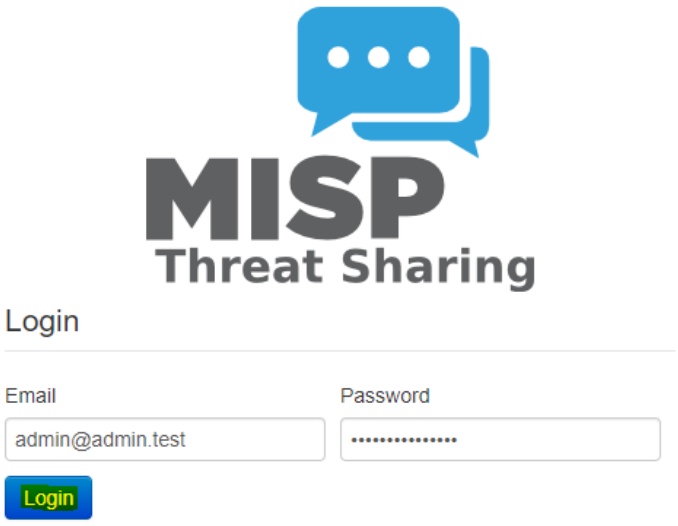
Και οι 2 τρόποι είναι απολύτως λειτουργικοί. Αν προτιμήσουμε την εγκατάσταση μέσω μιας εικονικής μηχανής, θα πάρουμε την παρακάτω εικόνα:



Εικόνα 17 - MISP Console Login

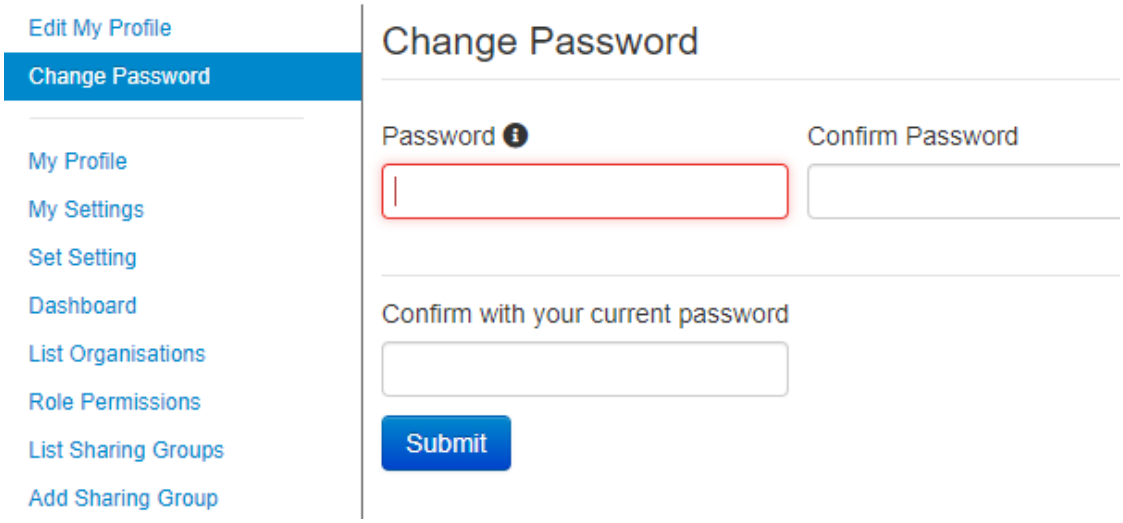
Η συγκεκριμένη έκδοση του MISP είναι βασισμένη σε Ubuntu 18.04 LTS. Στην προεπιλεγμένη προβολή αναφέρονται όλα τα στοιχεία της εγκατάστασης, καθώς και οι λογαριασμοί πρόσβασης στην πλατφόρμα.

Το δίκτυο που έχει οριστεί για το MISP είναι το 192.168.6.0/24 (NAT) και είναι διαθέσιμο τοπικά στην ιστοσελίδα https://192.168.6.56 (Διεύθυνση MISP)



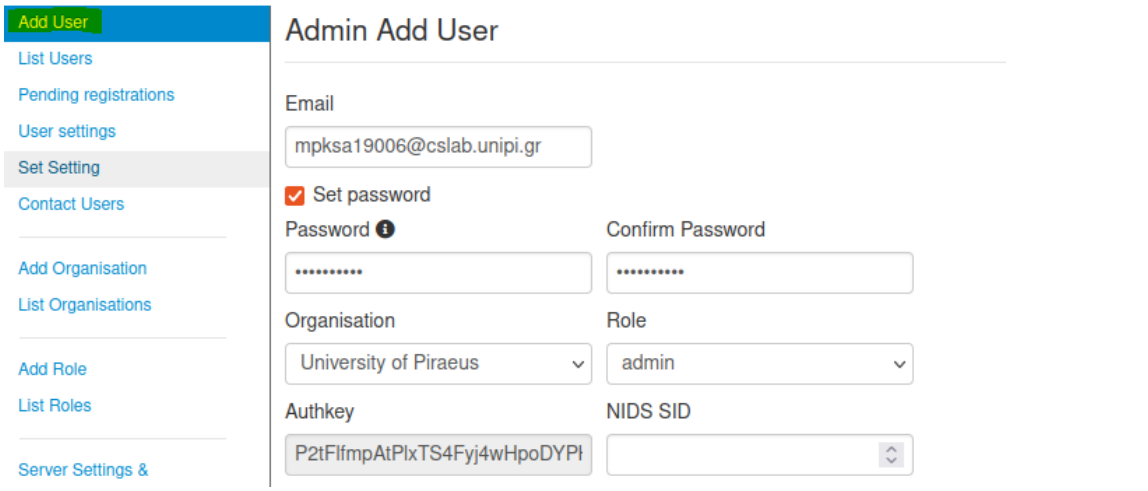
Εικόνα 18 - MISP Web Login

Οι προεπιλεγμένοι κωδικοί σύνδεσης στην πλατφόρμα κατά την 1η είσοδο μας δίνονται στην οθόνη του login της κονσόλας. Αφού κάνουμε σύνδεση, το 1ο πράγμα που θα μας ζητηθεί είναι να αλλάξουμε τον κωδικό πρόσβασης, καθώς δεν θα είναι δυνατή η λειτουργία της πλατφόρμας.



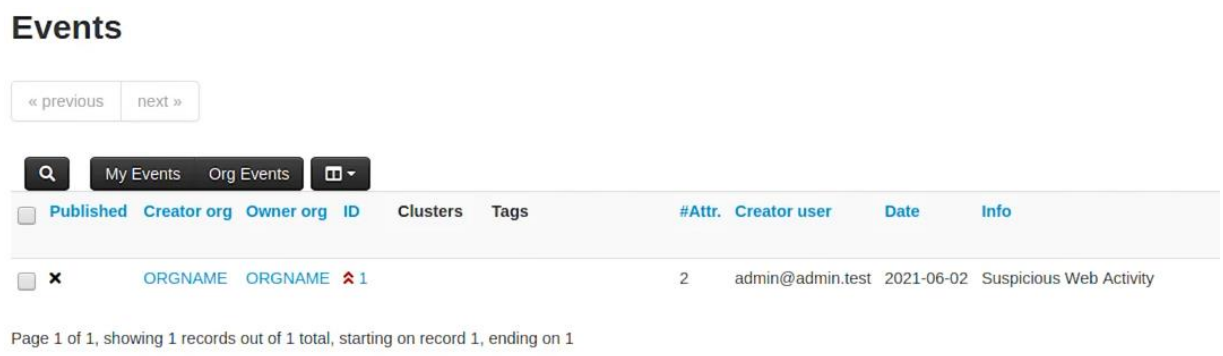
Εικόνα 19 - MISP (Change Password)

Φυσικά, μετά την αλλαγή μπορούμε να προσθέσουμε όσους χρήστες θέλουμε από την επιλογή “Add User” στο αριστερό μέρος της πλατφόρμας.



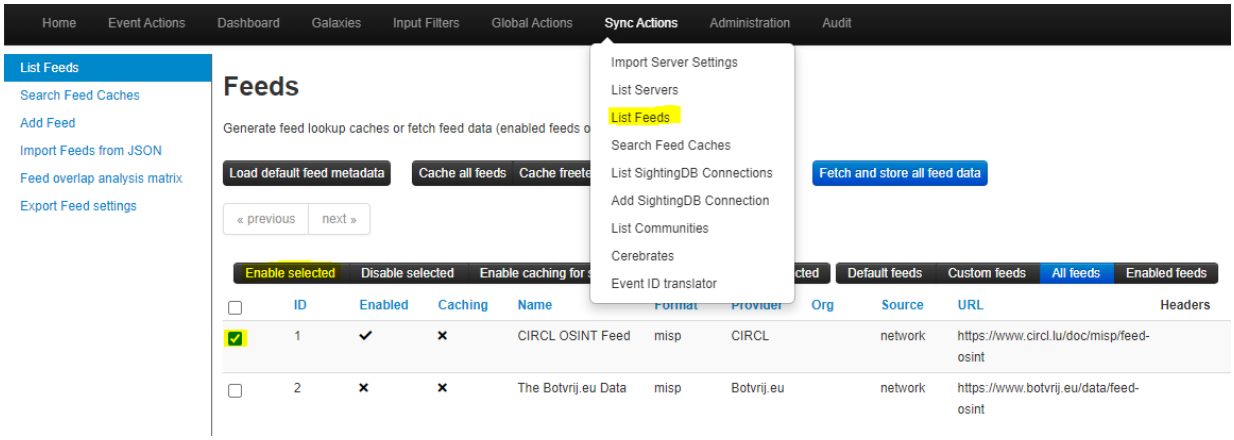
Εικόνα 20 - MISP (Add User)

Ορίζουμε τα βασικά στοιχεία όπως το e-mail, ο κωδικός πρόσβασης, τον ρόλο και τον οργανισμό και δημιουργούμε τον χρήστη. Ο κωδικός πρόσβασης θα πρέπει να πληροί την πολυπλοκότητα που έχει οριστεί στην πλατφόρμα.
Η αρχική σελίδα είναι η σελίδα των γεγονότων, δηλαδή η λίστα των γεγονότων που εισάγουμε εμείς στο MISP. Αρχικά, είναι κενή και εμφανίζεται ως εξής:



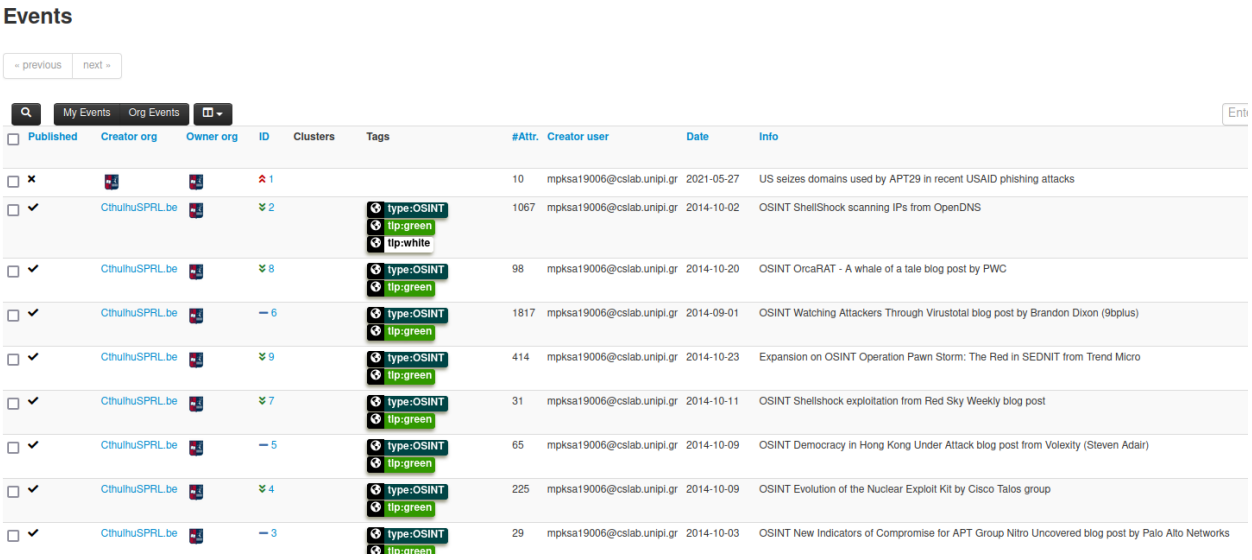
Εικόνα 21 - MISP Events

Η λίστα τροφοδότησης γεγονότων (CIRCL OSINT Feed) της εταιρείας CIRCL που είναι και η υπεύθυνη για το MISP υπάρχει από προεπιλογή και ενεργοποιείται με τον παρακάτω τρόπο:



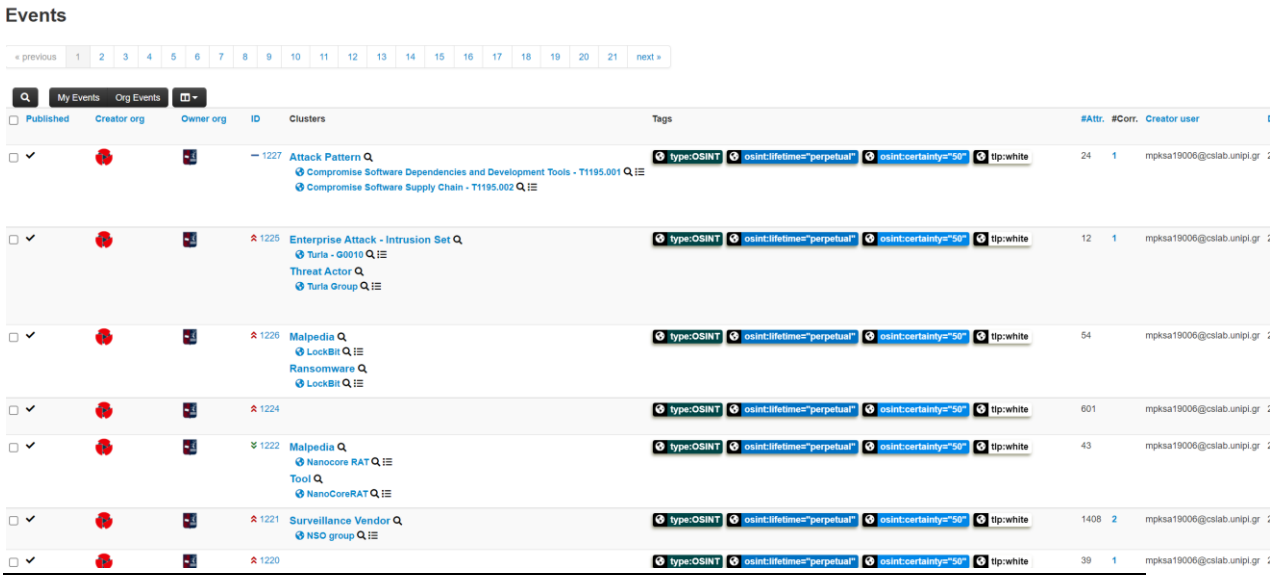
Εικόνα 22 - MISP Feeds

Αυτό θα έχει ως αποτέλεσμα να μας τροφοδοτήσει με γεγονότα που θα προέρχονται από την ομάδα OSINT της εταιρείας CIRCL.



Εικόνα 23 - MISP Events (2)

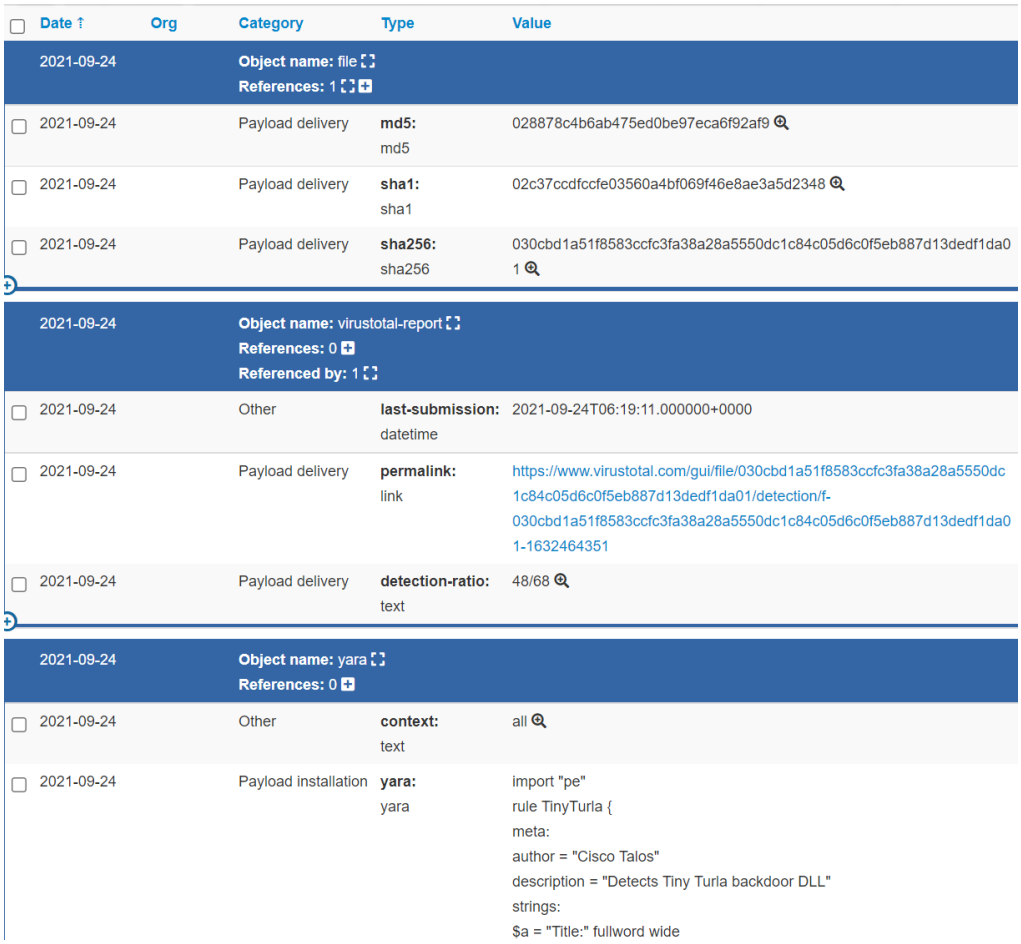
Έτσι, μετά από λίγη ώρα θα αρχίσει να φορτώνεται η πλατφόρμα μας με νέες απειλές, όπως παρακάτω:



Εικόνα 24 - MISP Events (3)

Κάθε γεγονός ορίζεται με ένα συγκεκριμένο ID όπου υπάρχουν μέσα όλες οι πληροφορίες σχετικά με αυτό. Μπορούμε να δούμε την ημερομηνία που προστέθηκε, από ποια ομάδα δημοσιεύτηκε, τον βαθμό της απειλής, τα αρχεία που σχετίζονται με αυτό (κακόβουλα .exe από την γραμμή εντολών, virustotal reports κ.α.)

Για παράδειγμα, στην παρακάτω εικόνα βλέπουμε όλα τα παραπάνω στοιχεία που αναφέραμε για το γεγονός με ID #1225. Περιλαμβάνονται hash values με κρυπτογράφηση MD5,SHA1,SHA256, την ημερομηνία που καταχωρήθηκε για έλεγχο στην σελίδα του Virustotal συμπεριλαμβανομένου και τον σύνδεσμο της ανάλυσης καθώς και τα αποτελέσματα αυτής από τα λογισμικά ασφαλείας.



Date	Org	Category	Type	Value
2021-09-24		**Object name:** file **References:** 1		
2021-09-24		Payload delivery	**md5:** md5	028878c4b6ab475ed0be97eca6f92af9
2021-09-24		Payload delivery	**sha1:** sha1	02c37ccdfccfe03560a4bf069f46e8ae3a5d2348
2021-09-24		Payload delivery	**sha256:** sha256	030cbd1a51f8583ccfc3fa38a28a5550dc1c84c05d6c0f5eb887d13dedf1da01
2021-09-24		**Object name:** virustotal-report **References:** 0 **Referenced by:** 1		
2021-09-24		Other	**last-submission:** datetime	2021-09-24T06:19:11.000000+0000
2021-09-24		Payload delivery	**permalink:** link	https://www.virustotal.com/gui/file/030cbd1a51f8583ccfc3fa38a28a5550dc1c84c05d6c0f5eb887d13dedf1da01/detection/f-030cbd1a51f8583ccfc3fa38a28a5550dc1c84c05d6c0f5eb887d13dedf1da01-1632464351
2021-09-24		Payload delivery	**detection-ratio:** text	48/68
2021-09-24		**Object name:** yara **References:** 0		
2021-09-24		Other	**context:** text	all
2021-09-24		Payload installation	**yara:** yara	import "pe" rule TinyTurla { meta: author = "Cisco Talos" description = "Detects Tiny Turla backdoor DLL" strings: $a = "Title:" fullword wide

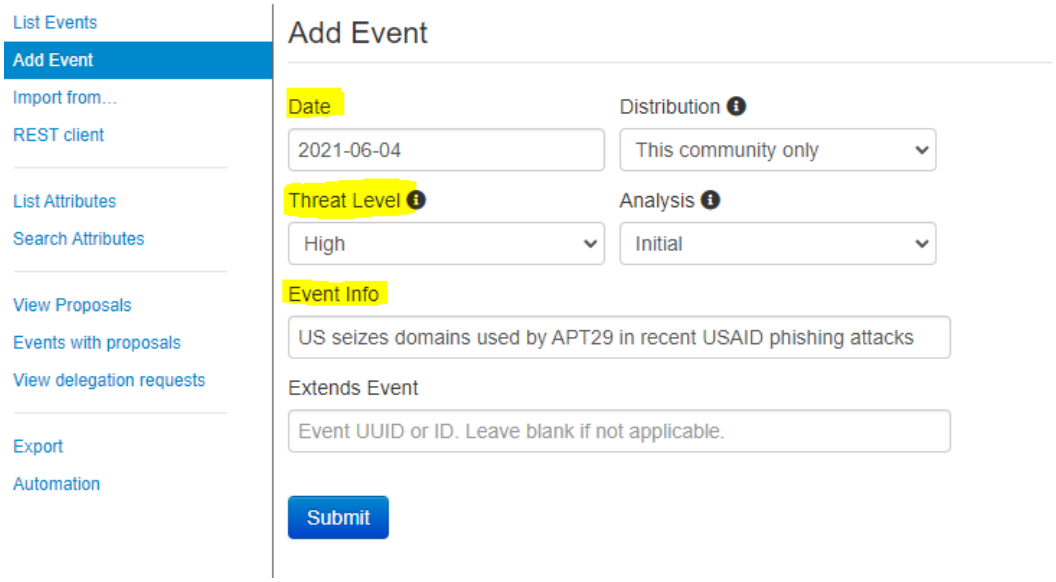
Εικόνα 25 - MISP Events (4)

Περιλαμβάνονται επίσης και οι κανόνες YARA που χρησιμοποιούνται για την ταξινόμηση και τον εντοπισμό δειγμάτων κακόβουλου λογισμικού:

```
import "pe"
rule TinyTurla {
meta:
author = "Cisco Talos"
description = "Detects Tiny Turla backdoor DLL"
strings:
$a = "Title:" fullword wide
$b = "Hosts" fullword wide
$c = "Security" fullword wide
$d = "TimeLong" fullword wide
$e = "TimeShort" fullword wide
$f = "MachineGuid" fullword wide
```

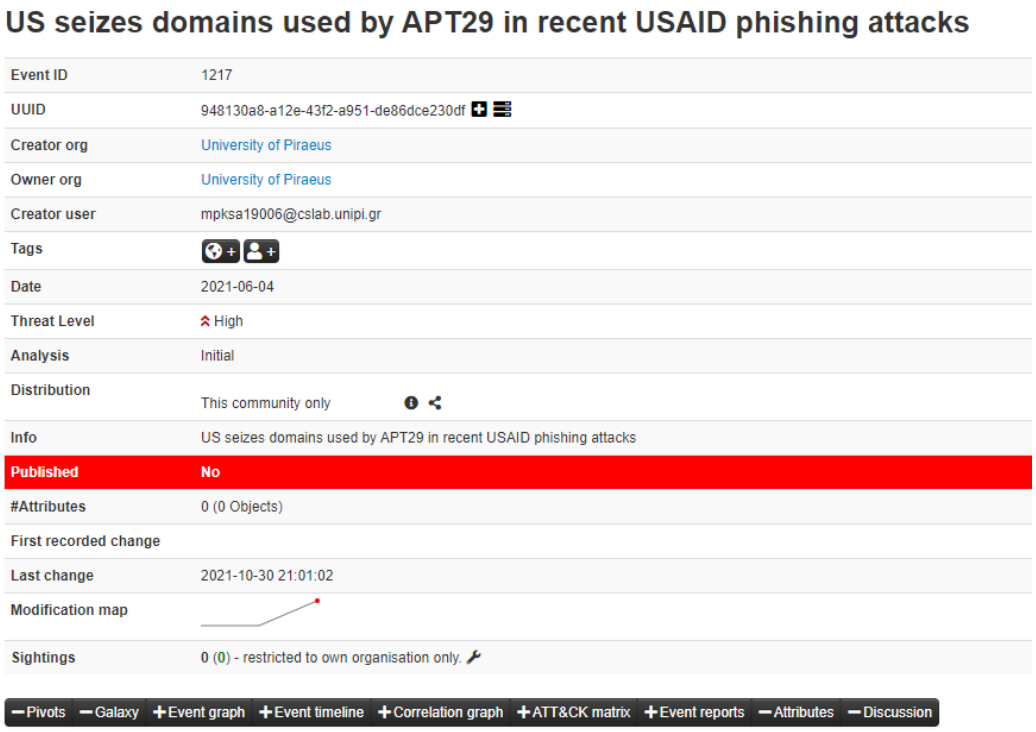
```
$g = "POST" fullword wide
$h = "WinHttpSetOption" fullword ascii
$i = "WinHttpQueryDataAvailable" fullword ascii

condition:
pe.is_pe and
pe.characteristics & pe.DLL and
pe.exports("ServiceMain") and
all of them
}
```

Αν θέλουμε να προσθέσουμε χειροκίνητα και να παρακολουθήσουμε ένα γεγονός στο MISP του οποίου πήραμε τις πληροφορίες από το διαδίκτυο, κάνουμε την εξής διαδικασία:



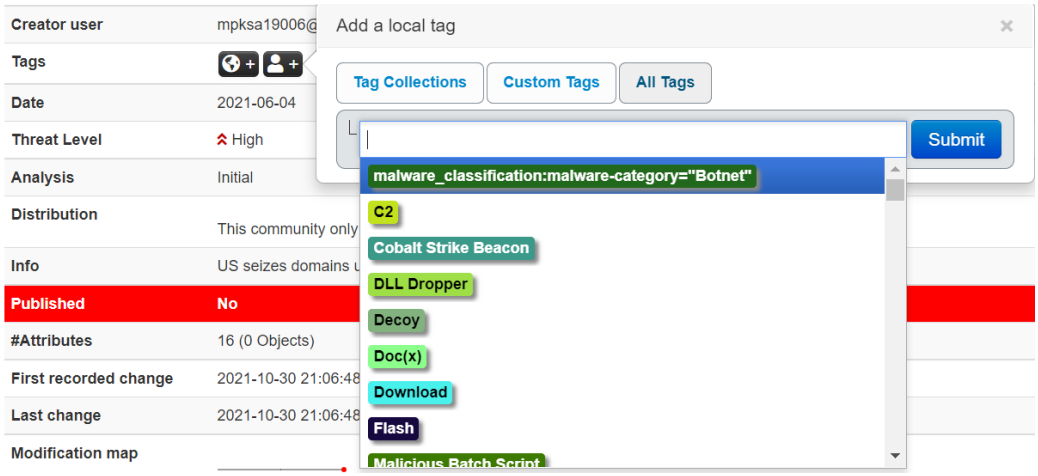
Εικόνα 26 - MISP Events (5)

Συμπληρώνοντας τα στοιχεία της ημερομηνίας, το επίπεδο της απειλής καθώς και πληροφορίες για το γεγονός, πατάμε το Submit. Η εικόνα που παίρνουμε στην συνέχεια είναι η εξής:



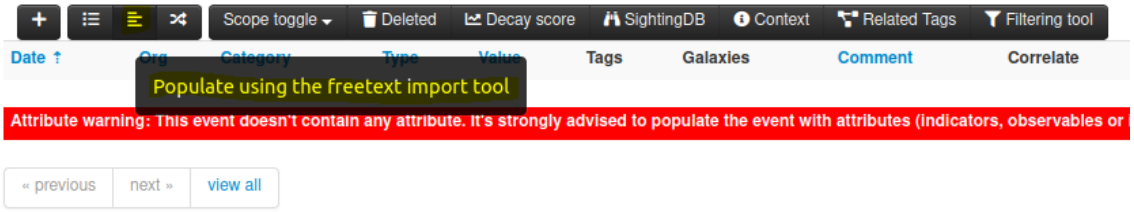
Εικόνα 27 - MISP Events (6)

Μπορούμε επίσης να κατηγοριοποιήσουμε το γεγονός αυτό, με την χρήση των tags που υπάρχουν στην πλατφόρμα:

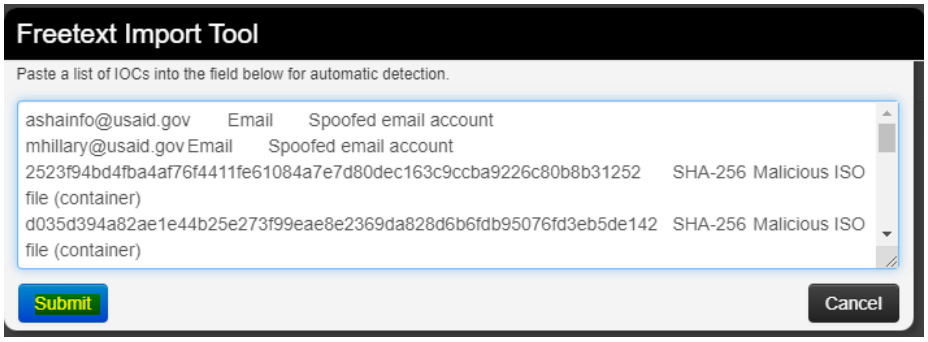


Εικόνα 28 - MISP Tags

Για την εισαγωγή των IOCs θα χρησιμοποιήσουμε το ενσωματωμένο εργαλείο που διαθέτει η πλατφόρμα:

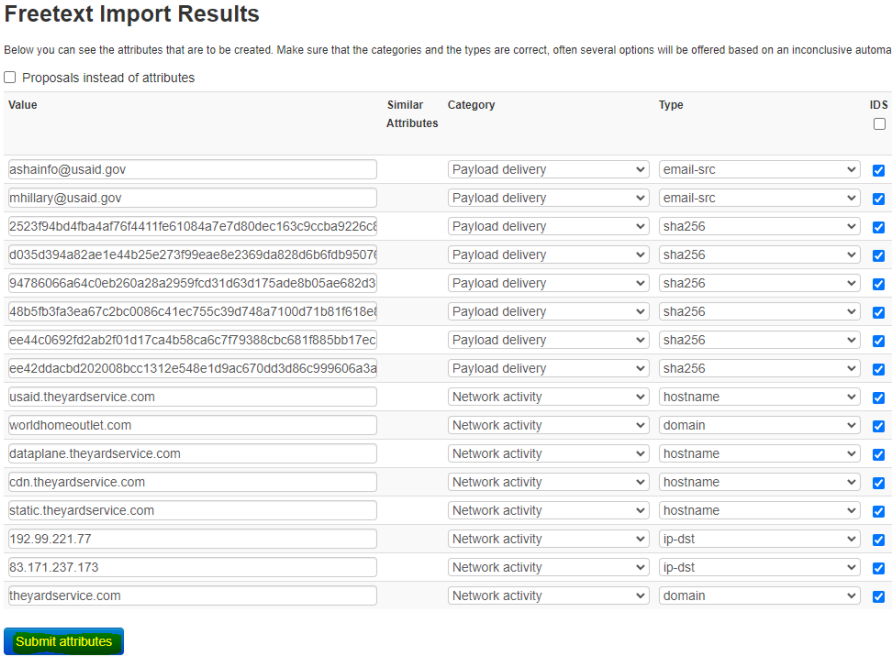


Εικόνα 29 - MISP Freetext Import Tool



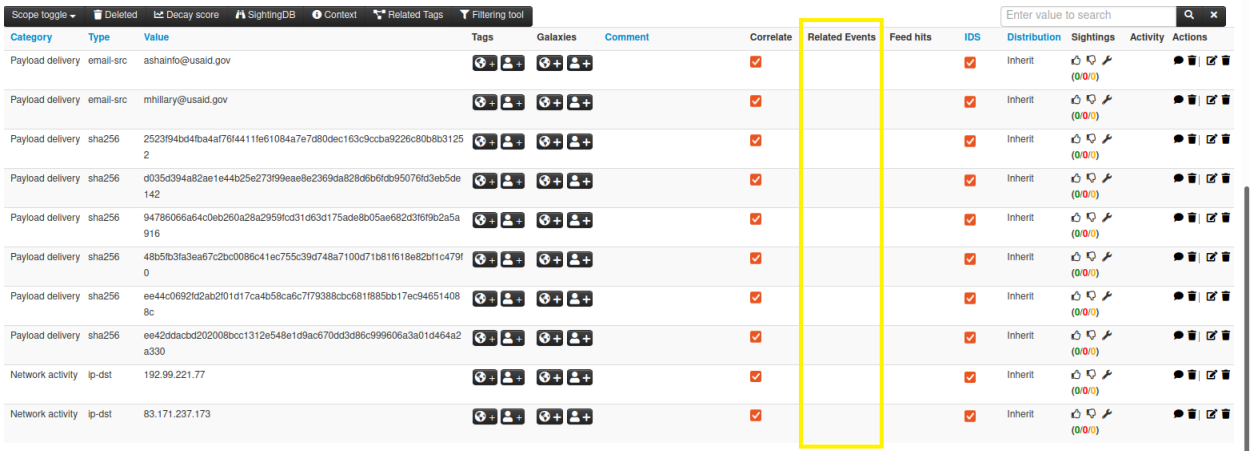
Εικόνα 30 - MISP Freetext Import Tool (2)

Με την χρήση του freetext import tool έχουμε την δυνατότητα να εισάγουμε μαζικά τα IOCs που έχουμε στην κατοχή μας. Τα αποτελέσματα που παίρνουμε, φαίνονται παρακάτω:



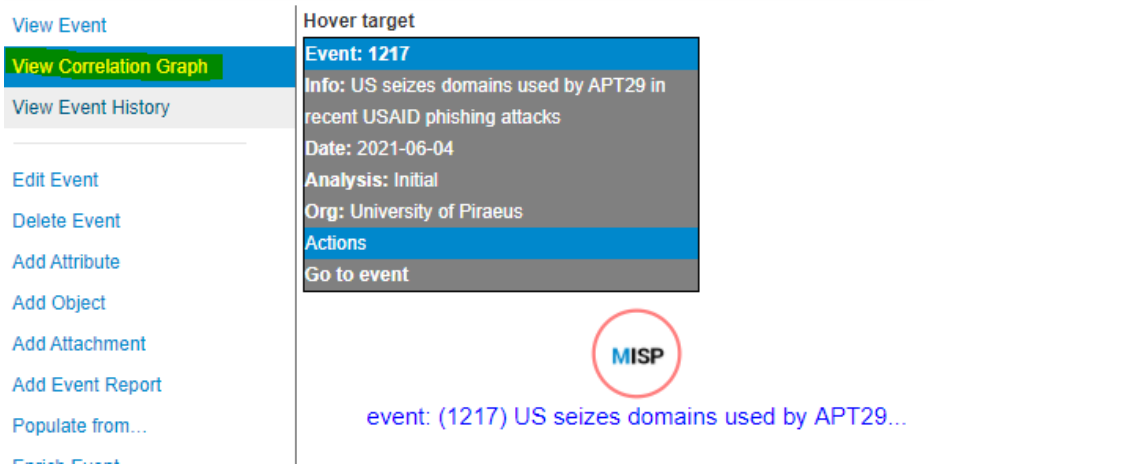
Εικόνα 31 - MISP Freetext Import Tool (3)

Αν είμαστε ικανοποιημένοι με αυτά που έχει βγάλει, πατάμε Submit attributes.
Αυτό που δίνει αξία σε μια πλατφόρμα όπως το MISP είναι το γεγονός ότι μας βγάζει την σχέση των IOCs που βάλαμε προηγουμένως, δηλαδή αν αυτά βρέθηκαν και άλλες λίστες ή γεγονότα που έχουμε ορίσει να τροφοδοτούνται στο MISP.



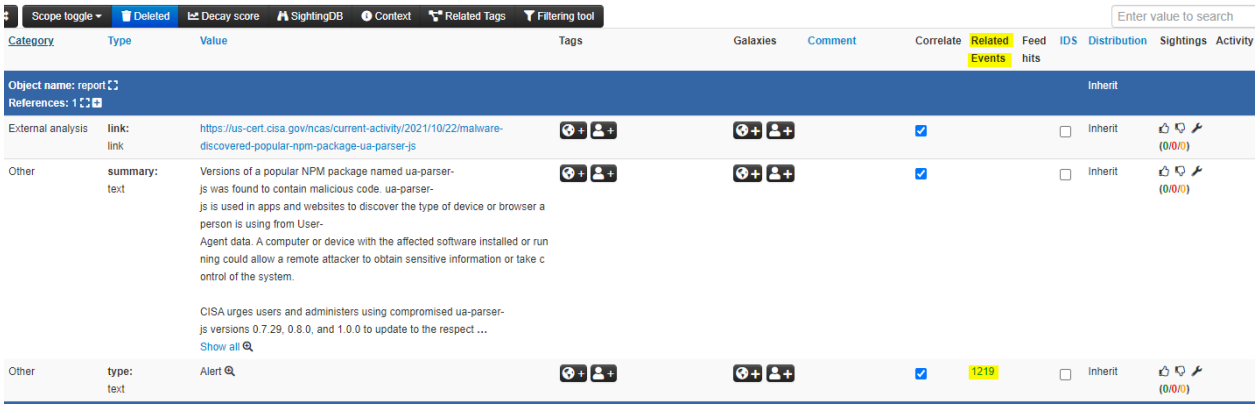
Εικόνα 32 - MISP Freetext Import Tool (4)

Και σε μορφή γραφήματος:



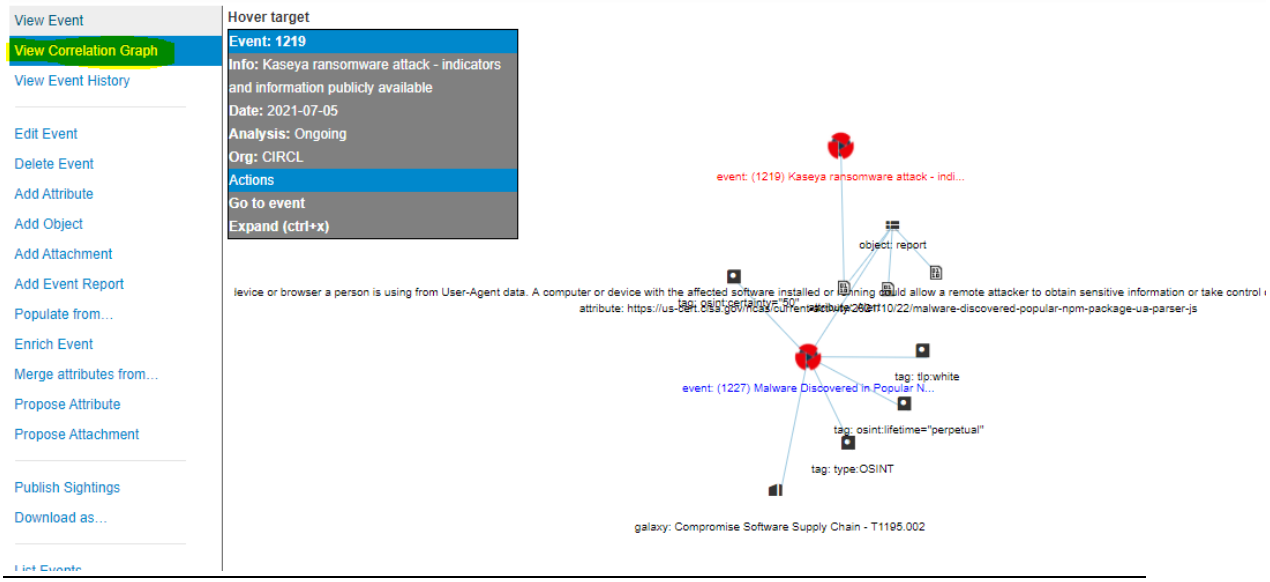
Εικόνα 33 - MISP Correlation Graph

Σε περίπτωση που υπάρχει κάποιο σχετικό γεγονός στο οποίο να έχει βρεθεί IOC που έχουμε ήδη καταχωρημένο, φαίνεται στο Related Events ως εξής:



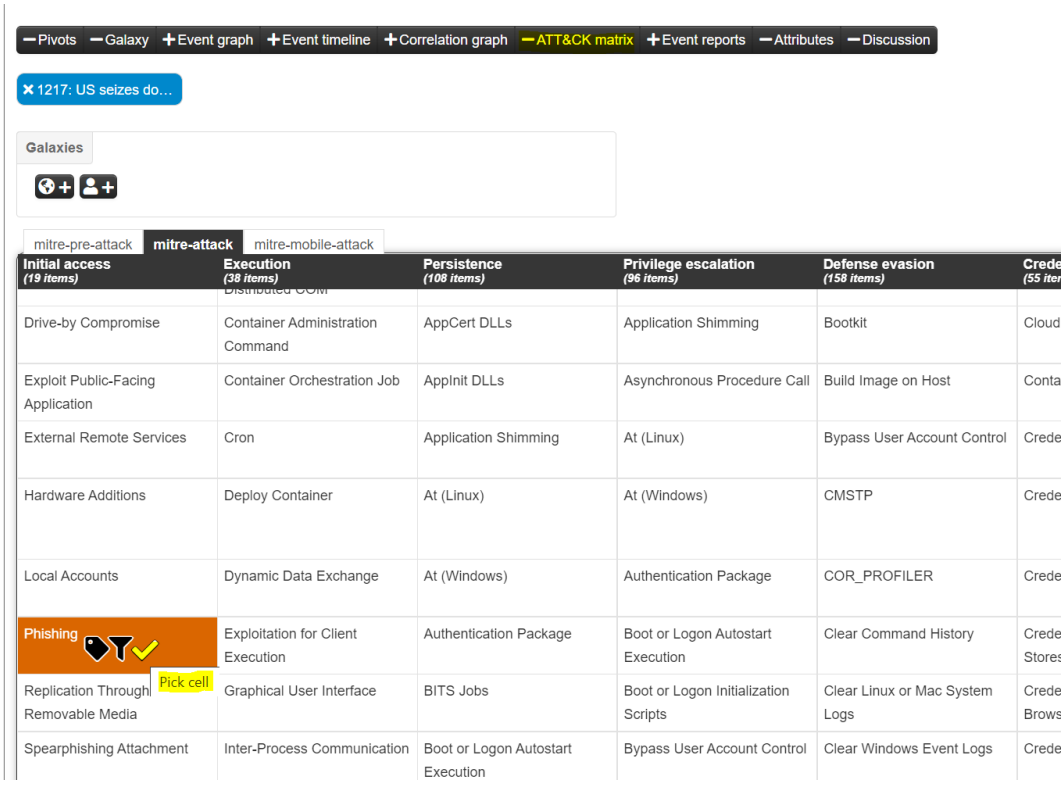
Εικόνα 34 - MISP Related Events

Για να δούμε το γράφημα και πως αυτό σχετίζεται με άλλα γεγονότα, αρκεί να πατήσουμε πάνω στο View Correlation Graph.



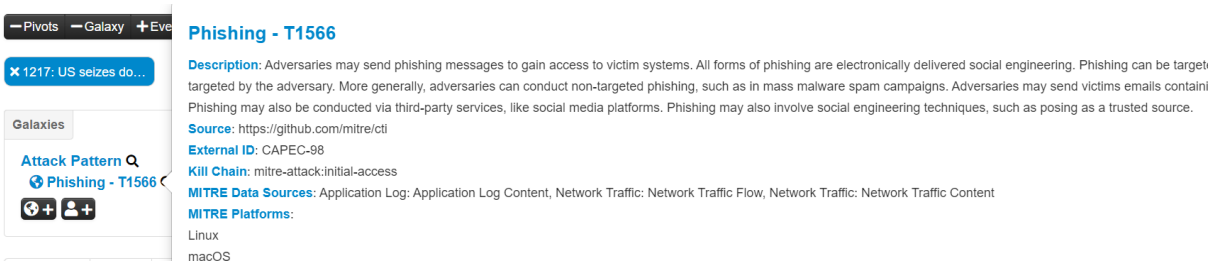
Εικόνα 35 - MISP Correlation Graph (2)

Ακόμη, έχουμε την δυνατότητα να συνδέσουμε το συγκεκριμένο γεγονός με τις τακτικές που υπάρχουν στον πίνακα της MITRE που είδαμε προηγουμένως. Ο πίνακας της MITRE υπάρχει ενσωματωμένος σε κάθε γεγονός:



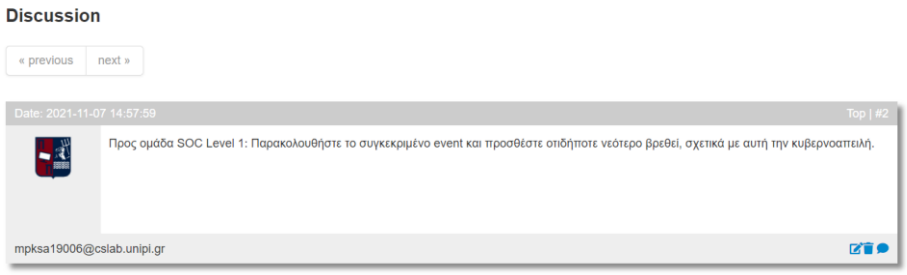
Εικόνα 36 - MISP with ATT&CK matrix

Αφού προστεθεί η τακτική αυτή, θα μας εμφανιστεί στο πεδίο των Galaxies με το μοτίβο επίθεσης που επιλέξαμε. Κάνοντας hover σε αυτό, μπορούμε να δούμε περισσότερες σχετικές πληροφορίες:



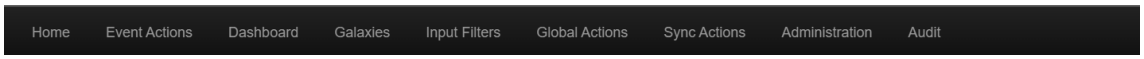
Εικόνα 37 - MISP Attack Pattern

Ακόμη, μπορούμε να προσθέσουμε σχόλια προς συζήτηση σε κάθε γεγονός για την βέλτιστη επικοινωνία και ενημέρωση μεταξύ των μελών της ομάδας:



Εικόνα 38 - MISP Discussion

Όλα τα παραπάνω αλλά και περισσότερες εξειδικευμένες ρυθμίσεις είναι διαθέσιμα για προβολή και επεξεργασία στο πάνω μέρος και κύριο μενού της πλατφόρμας. Ενδεικτικά, μπορούμε να δημιουργήσουμε κλειδιά για συνδέσεις με χρήση API με άλλες πλατφόρμες όπως θα δούμε στην επόμενη ενότητα, να δημιουργήσουμε προγραμματισμένες εργασίες, να ορίσουμε λίστες αποκλεισμού και άλλα.



Εικόνα 39 - MISP Main Menu

3.3 ΕΙΣΑΓΩΓΗ ΣΤΟ MINEMELD

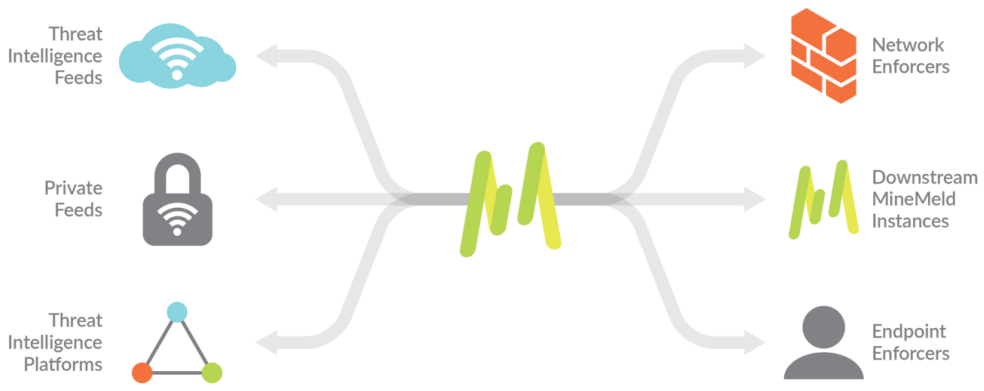
Όπως έχουμε αναφερθεί και στα προηγούμενα κεφάλαια, προκειμένου να αποτραπούν οι επιθέσεις στον κυβερνοχώρο, πολλοί οργανισμοί συλλέγουν ενδείκτες παραβίασης (IOCs) από διάφορους παρόχους πληροφοριών για κυβερνοαπειλές με σκοπό τον έλεγχο των πληροφοριακών τους συστημάτων για θέματα ασφάλειας. Δυστυχώς, οι παλαιοί τρόποι προσέγγισης συγκέντρωσης πληροφοριών για κυβερνοαπειλές γίνονται από την φύση τους με χειροκίνητες διαδικασίες, δημιουργώντας έτσι μια πολυπλοκότητα στην εργασία καθώς και παρατείνεται πολύ ο χρόνος για τον εντοπισμό και την επιβεβαίωση ύπαρξης των δεικτών παραβίασης. [18]

Το Minemeld είναι επίσης μια εφαρμογή ανοιχτού κώδικα και μπορεί να αξιοποιηθεί από έναν οργανισμό για την συγκέντρωση και κοινή χρήση πληροφοριών για τις απειλές στον κυβερνοχώρο. Είναι διαθέσιμο προς εγκατάσταση απευθείας από το GitHub είτε χειροκίνητα, εγκαθιστώντας το σε ένα VM με λειτουργικό Ubuntu Linux.

Το Minemeld εκτός από την συγκέντρωση και την συσχέτιση των πληροφοριών για κυβερνοαπειλές μπορεί επίσης να χρησιμοποιηθεί στις εξής περιπτώσεις: [18]

1. Επιβολή νέων κανόνων προστασίας, συμπεριλαμβανομένων και των διευθύνσεων που είναι καταχωρημένες στην «μαύρη» λίστα. (blacklisted URLs)
2. Αξιολόγηση της ροής των πληροφοριών για το περιβάλλον του οργανισμού.
3. Διαμοιρασμό των δεικτών παραβίασης με αξιόπιστους φορείς/συνεργάτες.
4. Προσδιορισμό των εισερχόμενων κινήσεων από κακόβουλα προγράμματα περιήγησης.
5. Παρακολούθηση διευθύνσεων IP και URL του Office365.

Μόλις συλλεχθούν οι δείκτες παραβίασης, το Minemeld μπορεί να φιλτράρει, να καταργήσει τα διπλότυπα και να ενοποιήσει τα δεδομένα από όλες τις διαφορετικές πηγές, επιτρέποντας έτσι στις ομάδες ασφάλειας να αναλύσουν ένα πιο λειτουργικό σύνολο δεδομένων.



Εικόνα 40 - Minemeld Diagram

3.4 ΕΓΚΑΤΑΣΤΑΣΗ & ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΗ MINEMELD

Προτού προχωρήσουμε στην εγκατάσταση του Minemeld, είναι σημαντικό να αυξήσουμε το επίπεδο ασφάλειας του λειτουργικού που θα χρησιμοποιήσουμε. Για το λειτουργικό Ubuntu που θα χρησιμοποιήσουμε, προτείνεται ο οδηγός που έχει αναρτηθεί και είναι διαθέσιμος για προβολή στην ιστοσελίδα του CIS (Center for Internet Security).

Αφού κάνουμε τις ενέργειες για την μεγαλύτερη ασφάλεια του λειτουργικού μας, προχωράμε στην εγκατάσταση του Minemeld ως εξής:

Βήμα 1ο. Ενημέρωση του λειτουργικού καθώς και των όλων των παρελκόμενων

Εντολή:

```
chris@Minemeld:~$ sudo apt update && sudo apt dist-upgrade -y
```

Εικόνα 41 - Εγκατάσταση Minemeld (1)

Βήμα 2ο. Ρύθμιση των πορτών στο firewall του Linux (iptables) για την σωστή λειτουργία του Minemeld

Εντολές:

```
sudo iptables -A INPUT -i lo -j ACCEPT
sudo iptables -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
sudo iptables -A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
sudo iptables -A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
sudo iptables -A INPUT -p tcp -m tcp --dport 443 -j ACCEPT
sudo iptables -A INPUT -p tcp -m tcp --dport  -j ACCEPT~
sudo iptables -A INPUT -p tcp -m tcp --dport 13514 -j ACCEPT
sudo iptables -A INPUT -p icmp -m icmp --icmp-type 0 -j ACCEPT
sudo iptables -A INPUT -p icmp -m icmp --icmp-type 3 -j ACCEPT
sudo iptables -A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
sudo iptables -A INPUT -p icmp -m icmp --icmp-type 11 -j ACCEPT
sudo iptables -P INPUT DROP
sudo iptables -P FORWARD DROP
sudo bash -c "iptables-save > /etc/iptables/rules.v4"
sudo ip6tables -A INPUT -i lo -j ACCEPT
sudo ip6tables -P INPUT DROP
sudo ip6tables -P FORWARD DROP
sudo bash -c "ip6tables-save > /etc/iptables/rules.v6"
```

Εικόνα 42 - Εγκατάσταση Minemeld (2)

Όπως φαίνεται και παραπάνω, ουσιαστικά επιτρέπουμε μόνο τις πόρτες για σύνδεση μέσω SSH, τις πόρτες για σύνδεση στο WEB UI του Minemeld καθώς και την πόρτα 13514 που χρησιμοποιείται από το ίδιο για τα system logs.

Σημείωση: Αν το Minemeld πρόκειται να χρησιμοποιηθεί σε IPV6 δίκτυο, τότε οι κανόνες θα πρέπει να προσαρμοστούν κατάλληλα. Στην συγκεκριμένη περίπτωση χρησιμοποιούμε IPV4 δίκτυο NAT 192.168.6.0/24.

Βήμα 3ο. Προσθήκη του κλειδιού GPG

Εντολή:

```
wget -qO - https://minemeld-updates.panw.io/gpg.key | sudo apt-key add -
```

Εικόνα 43 - Εγκατάσταση Minemeld (3)

Επαληθεύουμε το κλειδί ότι ταιριάζει με το «αποτύπωμα» του επίσημου κλειδιού του Minemeld:

Εντολή:

```
apt-key adv --fingerprint DD0DA1F9
```

```
chris@Minemeld:~$ apt-key adv --fingerprint DD0DA1F9
Executing: /tmp/tmp.uCD514G896/gpg.1.sh --fingerprint
DD0DA1F9
pub   4096R/DD0DA1F9 2016-07-15
      Key fingerprint = E558 CE6E 3968 0F31 8F6C  BFAC B401 E02E DD0D A1F9
uid                  Palo Alto Networks, MineMeld Team <minemeld@paloaltonetworks.com>
uid                  [jpeg image of size 3523]

pub   4096R/DD0DA1F9 2016-07-15
      Key fingerprint = E558 CE6E 3968 0F31 8F6C  BFAC B401 E02E DD0D A1F9
uid                  Palo Alto Networks, MineMeld Team <minemeld@paloaltonetworks.com>
uid                  [jpeg image of size 3523]
sub   4096R/7B630999 2016-07-15 [expires: 2022-07-15]
```

Εικόνα 44 - Εγκατάσταση Minemeld (4)

Βήμα 4ο. Προσθήκη του αποθετήριου Minemeld APT στη λίστα συστήματος και ενημέρωση του

Εντολή:

```
sudo add-apt-repository "deb http://minemeld-updates.panw.io/ubuntu xenial-minemeld main"
sudo apt update
```

Εικόνα 45 - Εγκατάσταση Minemeld (5)

Βήμα 5ο. Εγκατάσταση NGINX και REDIS που απαιτούνται από το Minemeld

Εντολή:

```
sudo apt install -y nginx redis-server
```

Εικόνα 46 - Εγκατάσταση Minemeld (6)

Βήμα 6ο. Για την εγκατάσταση του Minemeld χωρίς προβλήματα, απαιτείται η αφαίρεση της παρακάτω αρχιτεκτονικής:

```
sudo dpkg --remove-architecture i386
```

Εικόνα 47 - Εγκατάσταση Minemeld (7)

Βήμα 7ο. Προσθήκη του κλειδιού καθώς και της βιβλιοθήκης του Minemeld.

Εντολές:

```
chris@Minemeld:~$ wget -q0 - https://minemeld-updates.panw.io/gpg.key | sudo apt-key add -
```

Εικόνα 48 - Εγκατάσταση Minemeld (8)

```
chris@Minemeld:~$ sudo add-apt-repository "deb http://minemeld-updates.panw.io/ubuntu xenial-minemel
d main"
```

Εικόνα 49 - Εγκατάσταση Minemeld (9)

Βήμα 8ο. Εγκατάσταση Minemeld

Εντολή:

```
chris@Minemeld:~$ sudo apt install -o Dpkg::Options::="--force-overwrite" -y minemeld
```

Εικόνα 50 - Εγκατάσταση Minemeld (10)

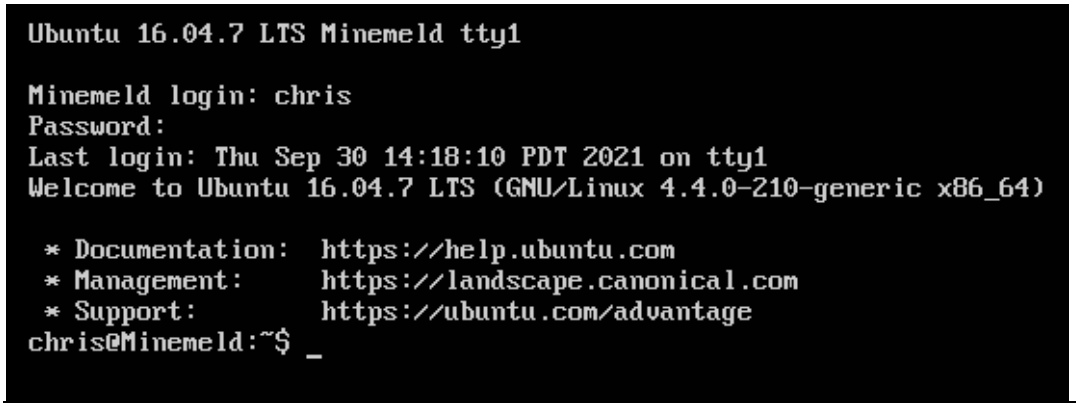
Βήμα 9ο. Επανεκκίνηση συστήματος

Εντολή:

```
chris@Minemeld:~$ sudo shutdown -r 1
```

Εικόνα 51 - Εγκατάσταση Minemeld (11)

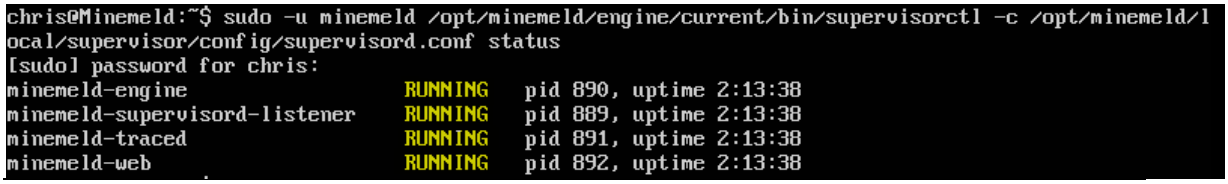
Βήμα 10ο. Login στην πλατφόρμα μέσω κονσόλας



Εικόνα 52 - Minemeld Console Login

Βήμα 11ο. Έλεγχος των υπηρεσιών του Minemeld

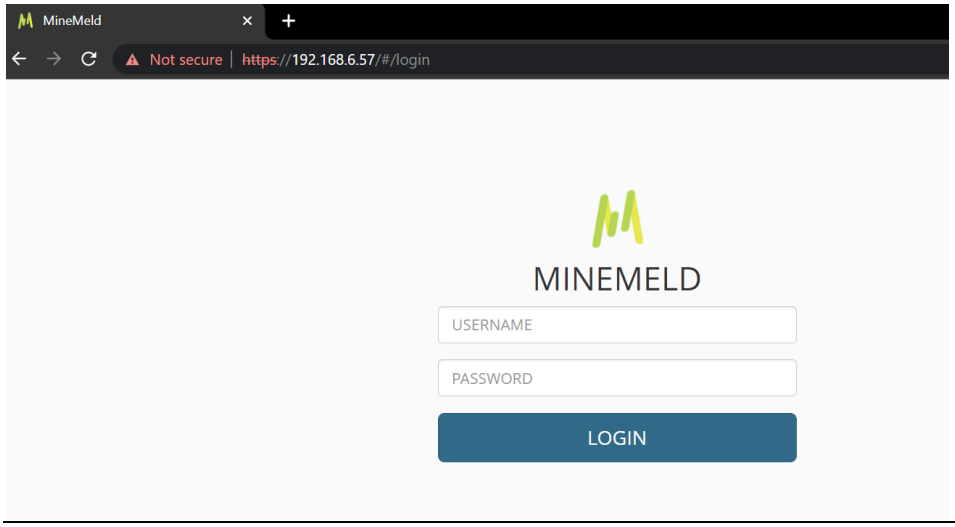
Εντολή:



Εικόνα 53 - Minemeld Check Services

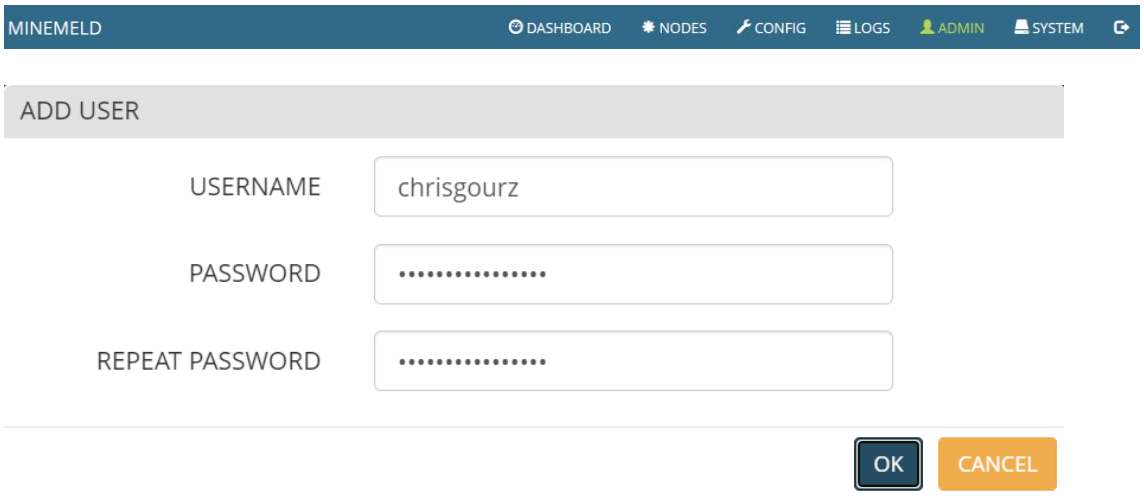
Αφού δούμε ότι τρέχουν όλες οι υπηρεσίες, μπορούμε να εισέλθουμε στην πλατφόρμα του Minemeld και να προχωρήσουμε στην παραμετροποίηση του. Είναι διαθέσιμη μέσω http:// στην διεύθυνση που δηλώσαμε κατά την εγκατάσταση.

Η πρώτη εικόνα που παίρνουμε όταν επισκεφθούμε μια νέα εγκατάσταση, είναι η παρακάτω:



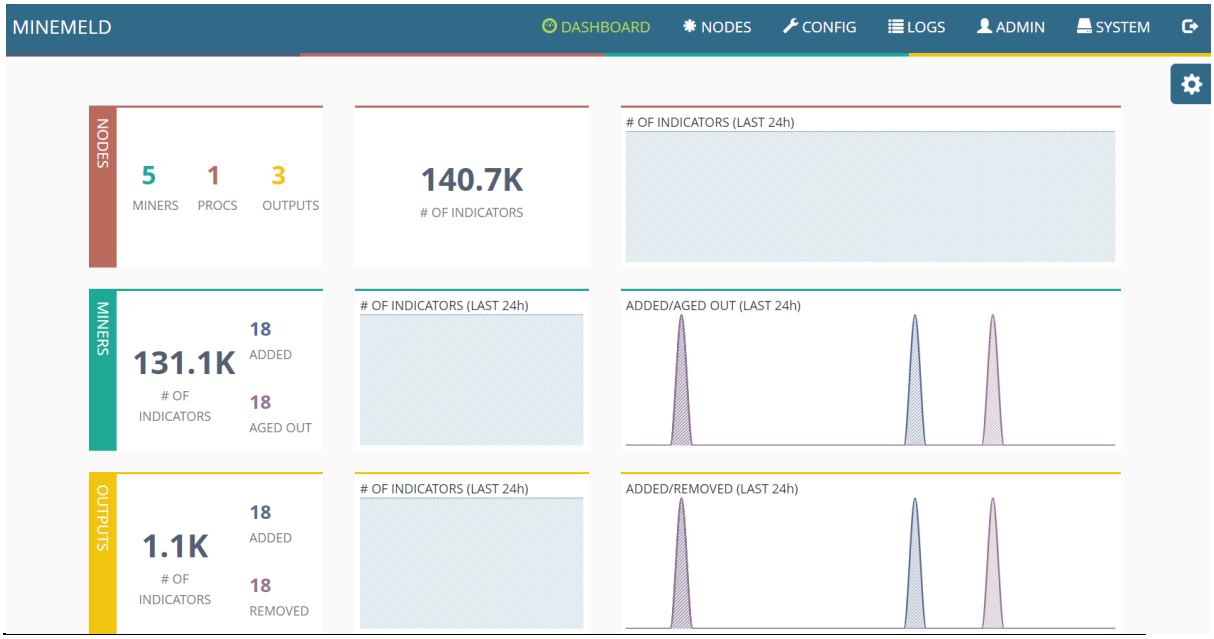
Εικόνα 54 - Minemeld WEB UI

Εδώ εισάγουμε τους προεπιλεγμένους κωδικούς πρόσβασης που μας δίνονται και στην συνέχεια, αφού κάνουμε σύνδεση, μπορούμε να φτιάξουμε όσους χρήστες θέλουμε από το μενού και την επιλογή ADMIN:



Εικόνα 55 - Minemeld Add User

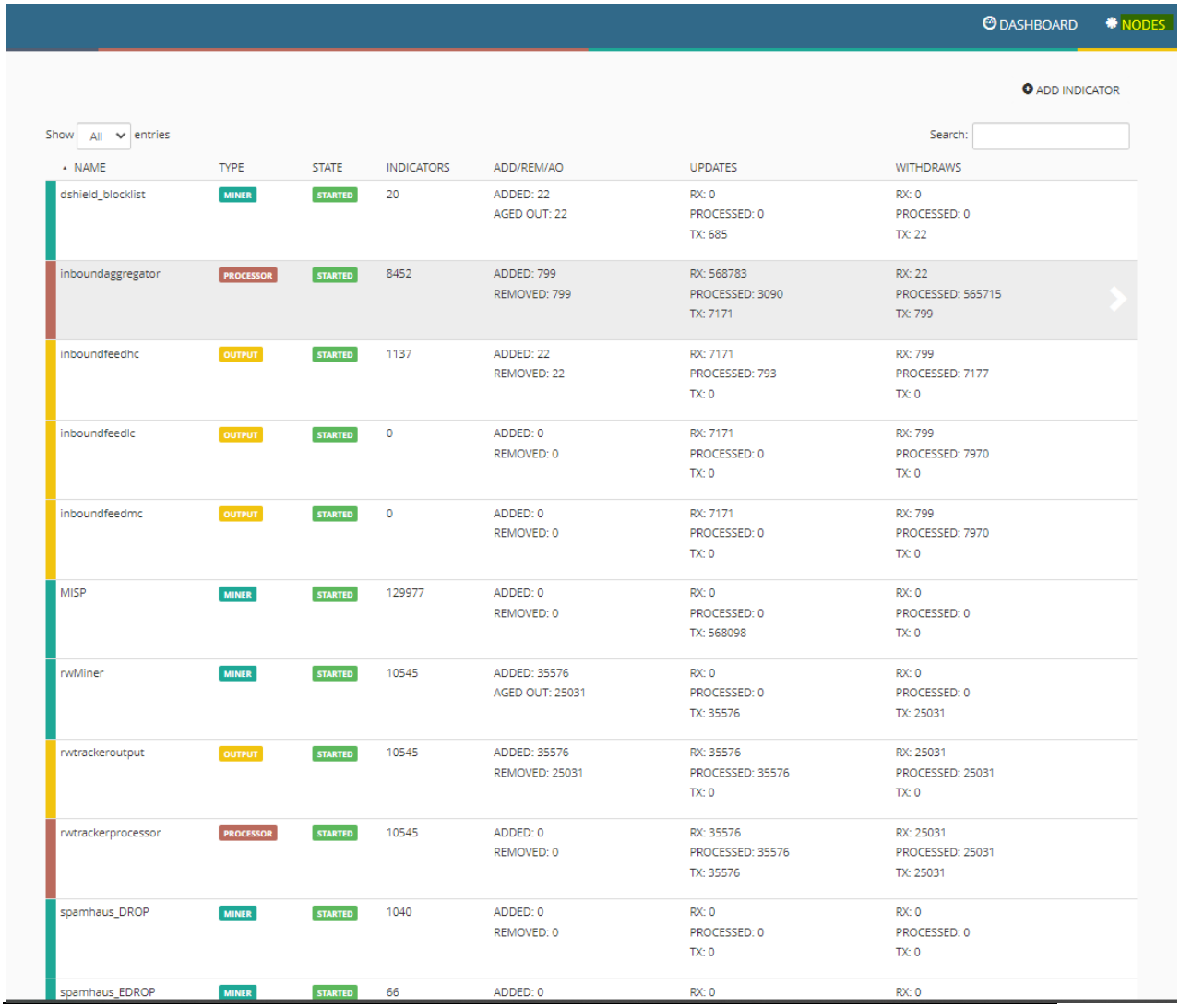
Η συνοπτική εικόνα όλων των στοιχείων (nodes, indicators, outputs) του Minemeld φαίνεται στην παρακάτω εικόνα και την επιλογή DASHBOARD:



Εικόνα 56 - Minemeld Dashboard

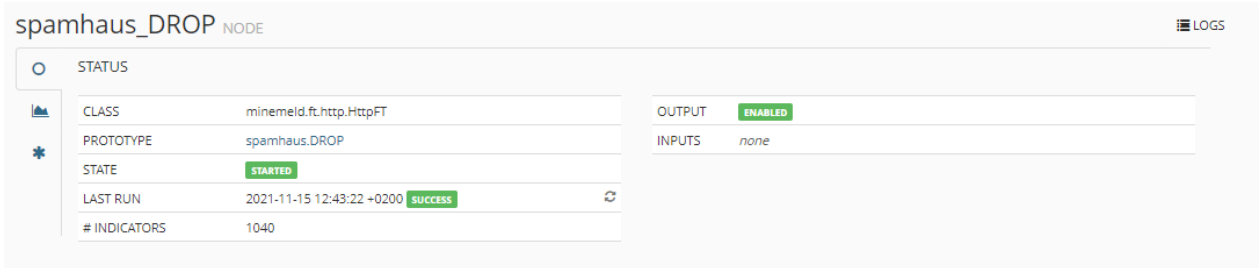
Από εδώ και στο εξής είμαστε σε θέση να παραμετροποιήσουμε το Minemeld και να ορίσουμε κόμβους (nodes) που θα μας βοηθήσουν και θα είναι χρήσιμοι για τον οργανισμό.

Η σελίδα των κόμβων (NODES) θα εμφανίσει μια λίστα με όλους τους κόμβους που έχουν ξεκινήσει και ενεργοποιούνται στο Minemeld, πόσοι δείκτες (Indicators) έχουν υποστεί επεξεργασία από έναν συγκεκριμένο κόμβο, καθώς και τι τύπος κόμβου είναι (π.χ. miner, processor, output).



Εικόνα 57 - Minemeld Nodes

Κάνοντας κλικ σε έναν κόμβο, κατευθυνόμαστε σε μια νέα σελίδα με επιλογές που περιλαμβάνουν την κατάσταση, στατιστικά στοιχεία και ένα γράφημα σύνδεσης που δείχνει από που λαμβάνει τα δεδομένα του ο κόμβος και σε ποιους άλλους κόμβους στέλνει τα δεδομένα του.



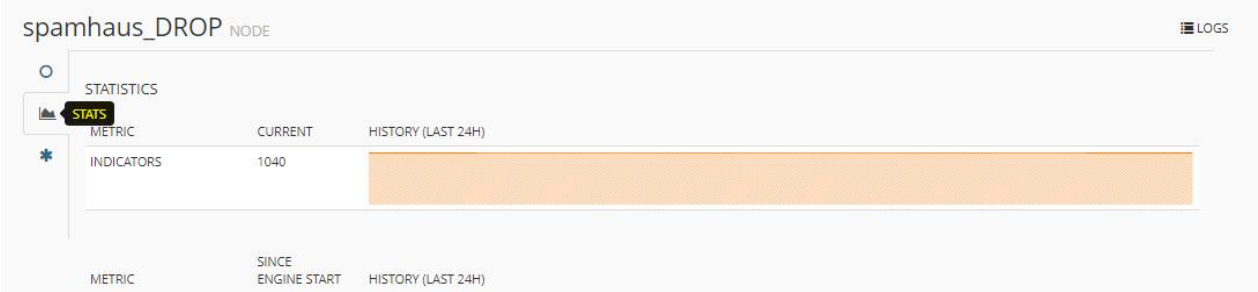
Εικόνα 58 - Minemeld Nodes (2)

Ο συγκεκριμένος κόμβος υπάρχει ήδη εγκατεστημένος στο Minemeld και σκοπός του είναι να παίρνει δεδομένα από την λίστα του SPAMHAUS. Στην λίστα με τα στοιχεία του κόμβου απεικονίζεται ο ρόλος (Class) που απεικονίζει το είδος της επεξεργασίας. Στην συγκεκριμένη περίπτωση, το “Minemeld.ft.http.HttpFT” τροφοδοτεί απλά κείμενα (plaintext) μέσω HTTP/HTTPS.

Το πρωτότυπο (Prototype) είναι αυτό είναι που καθορίζει τον τρόπο με τον οποίο λειτουργούν οι κόμβοι και σε τι είδους δεδομένα λειτουργεί.

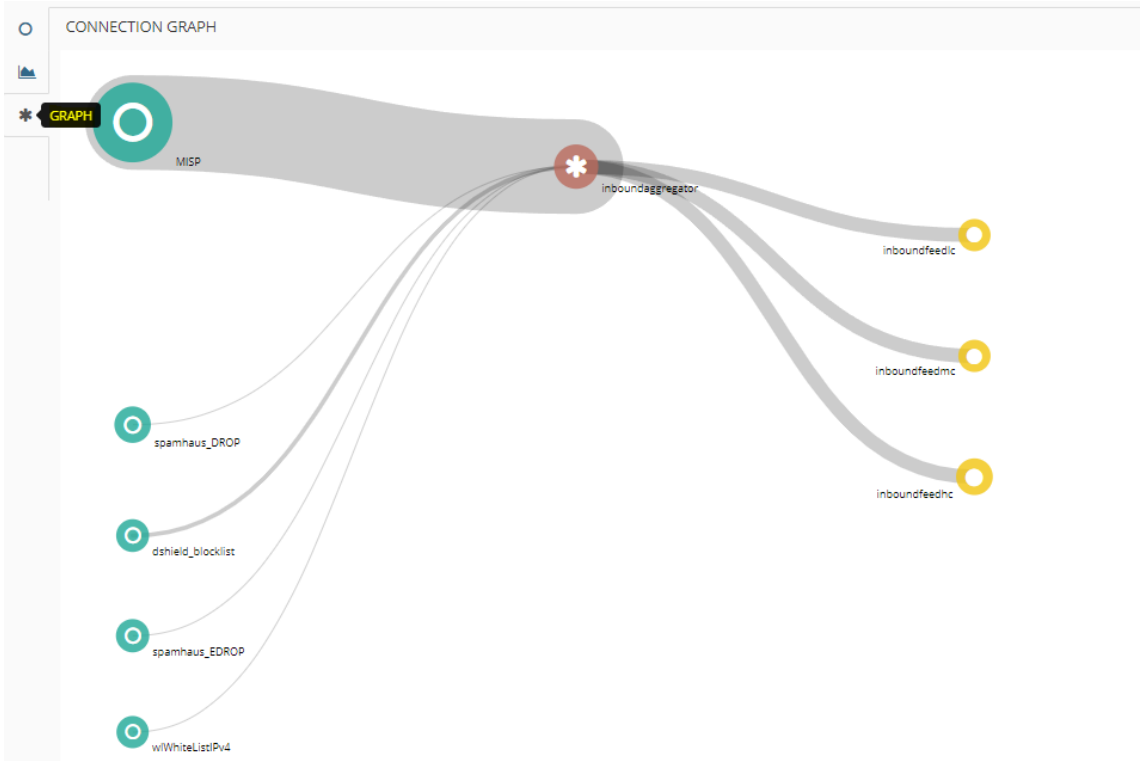
Ακόμη, αναφέρονται η κατάσταση του κόμβου, η ημερομηνία που έτρεξε τελευταία φορά καθώς και πόσους δείκτες έχει προσθέσει.

Επιλέγοντας την καρτέλα με τα στατιστικά, βλέπουμε περισσότερα στοιχεία σχετικά και με την κατάσταση του:



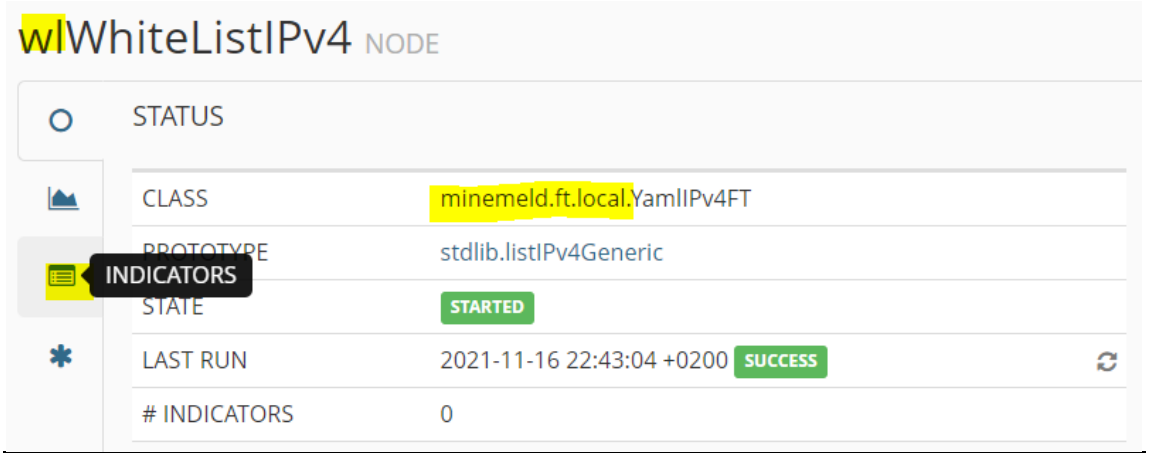
Εικόνα 59 - Minemeld Nodes (3)

Τέλος, το γράφημα που απεικονίζει τα δεδομένα που λαμβάνει ο κόμβος και σε ποιους άλλους κόμβους στέλνει τα δεδομένα του:



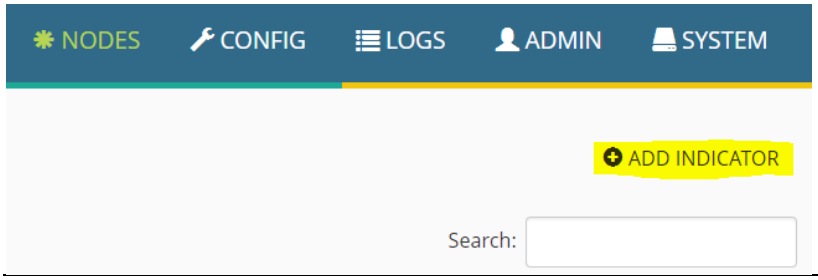
Εικόνα 60 - Minemeld Connection Graph

Στο Minemeld υπάρχουν επίσης κόμβοι που ξεκινούν με το “wl” και υποδηλώνουν κόμβους επιτρεπόμενων δεικτών (whitelist indicators). Οι κόμβοι αυτοί χρησιμοποιούν συνήθως πρωτότυπα τύπου “minemeld.ft.local.*” όπως φαίνεται και στην παρακάτω εικόνα, πράγμα που σημαίνει ότι οι χρήστες της πλατφόρμας θα πρέπει να ορίσουν χειροκίνητα τους δείκτες στον κόμβο αυτόν.



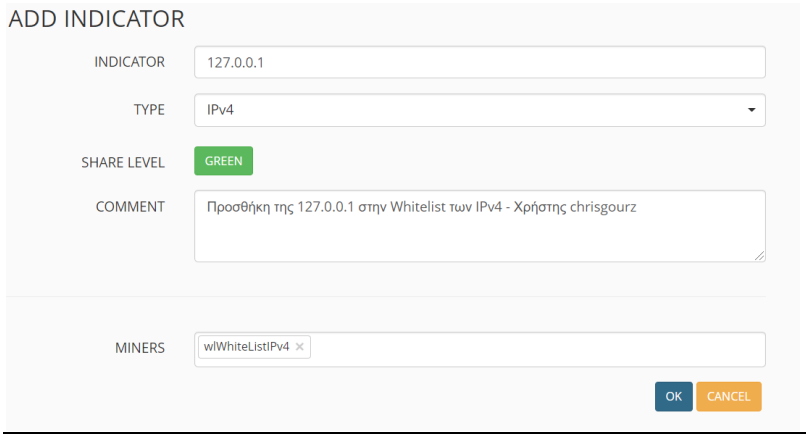
Εικόνα 61 - Minemeld Nodes (4)

Για να προσθέσουμε δείκτες στον κόμβο αυτόν, θα πρέπει απλώς να πατήσουμε στο **+ ADD INDICATOR** στην καρτέλα NODES.

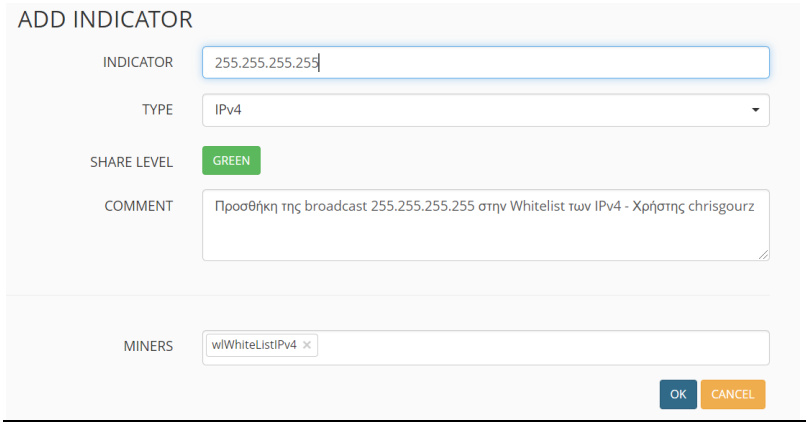


Εικόνα 62 - Minemeld Add Indicator

Εδώ μπορούμε να προσθέσουμε για παράδειγμα την διεύθυνση 127.0.0.1 που χρησιμοποιείται για loopback tests καθώς και την 255.255.255.255 που ορίζεται ως η broadcast address στα δίκτυα.

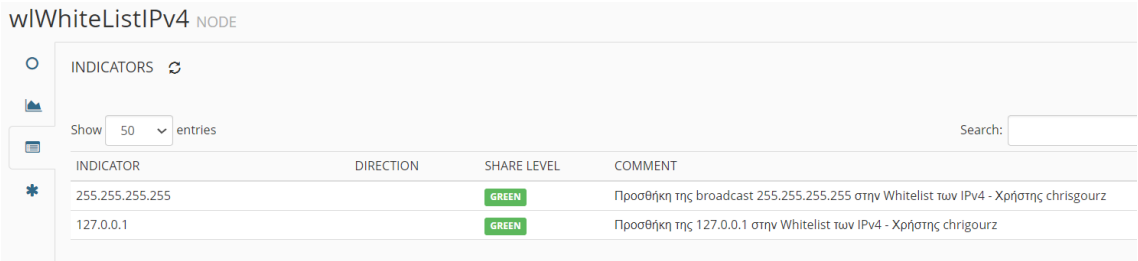


Εικόνα 63 - Minemeld Add Indicator (2)



Εικόνα 64 - Minemeld Add Indicator (3)

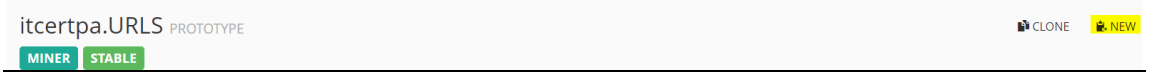
Αποτέλεσμα της ενέργειας αυτής είναι να μην βλέπουμε τους δείκτες που έχουμε προσθέσει σε καμία έξοδο (output) που σχετίζεται με τον κόμβο αυτόν.



Εικόνα 65 - Minemeld Add Indicator (4)

Στην συνέχεια, θα διαμορφώσουμε το Minemeld ώστε να επεξεργάζεται ένα αρχείο το οποίο περιέχει κακόβουλες διευθύνσεις URL από την λίστα Abuse.ch, ένα ερευνητικό πρόγραμμα του πανεπιστημίου της Βέρνης.

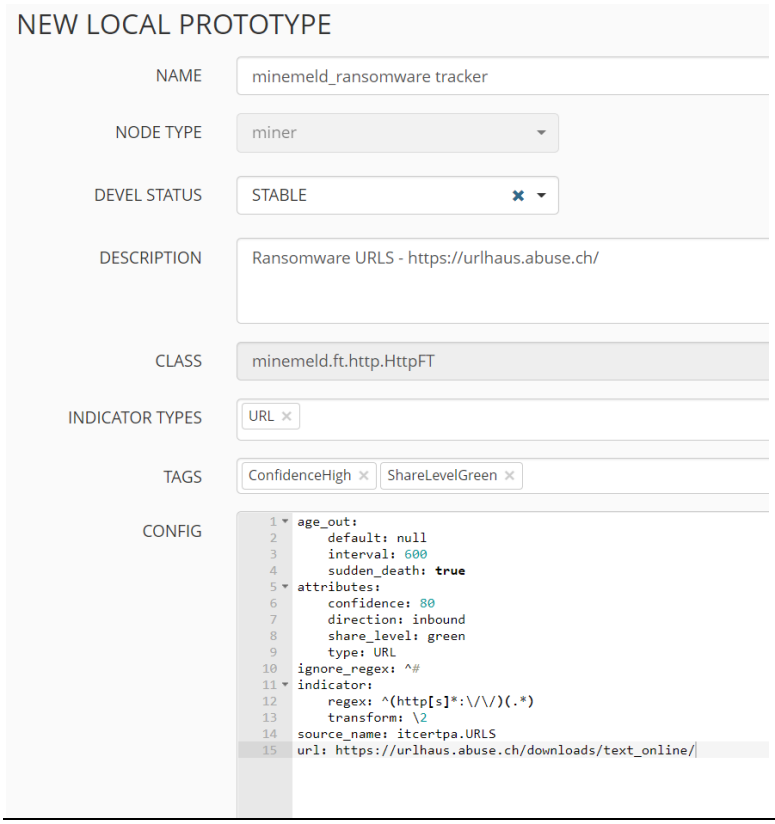
Αρχικά, πατάμε στο εικονίδιο στην καρτέλα CONFIG. Αναζητάμε το πρωτότυπο “itcertpa.URLS” και κάνουμε κλικ σε αυτό. Δημιουργούμε ένα νέο χρησιμοποιώντας αυτό το template και στην συνέχεια ορίζουμε τις παρακάτω επιλογές: [8]



Εικόνα 66 - Minemeld Prototype

```
age_out:
  default: null
  interval: 600
  sudden_death: true
attributes:
  confidence: 80
  direction: inbound
  share_level: green
  type: URL
ignore_regex: ^#
indicator:
  regex: ^(http[s]*:\/\/)(.*)
  transform: \2
source_name: itcertpa.URLS
url: https://urlhaus.abuse.ch/downloads/text_online/
```

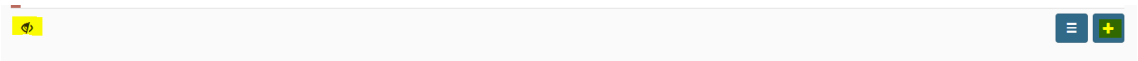
Η τελική μορφή του νέου μας πρωτοτύπου θα πρέπει να είναι όπως παρακάτω:



Εικόνα 67 - Minemeld Prototype (2)

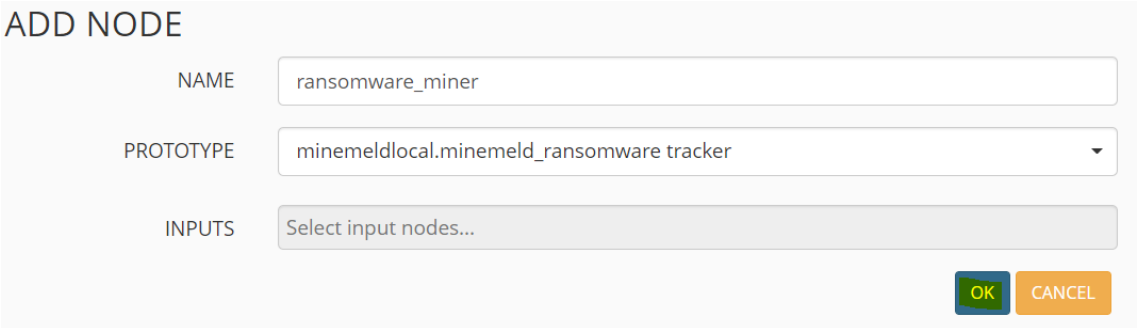
Το Minemeld χρησιμοποιεί την γλώσσα προγραμματισμού YAML για τις ρυθμίσεις των πρωτοτύπων. Αυτό το πρωτότυπο θα κατεβάσει την λίστα URLHAUS από το Abuse.ch. Στην συνέχεια με την χρήση regex θα κοπεί το http & και το https, κάτι το οποίο είναι προαιρετικό. Πατάμε στο OK και το πρωτότυπο μας έχει δημιουργηθεί.

Στην συνέχεια θα πρέπει να προσθέσουμε ένα κόμβο που θα έχει τον ρόλο του miner και θα ορίσουμε να κοιτάει το πρωτότυπο που δημιουργήσαμε προηγουμένως. Ενεργοποιούμε το advanced mode στην καρτέλα CONFIG και πατάμε στο εικονίδιο **+**



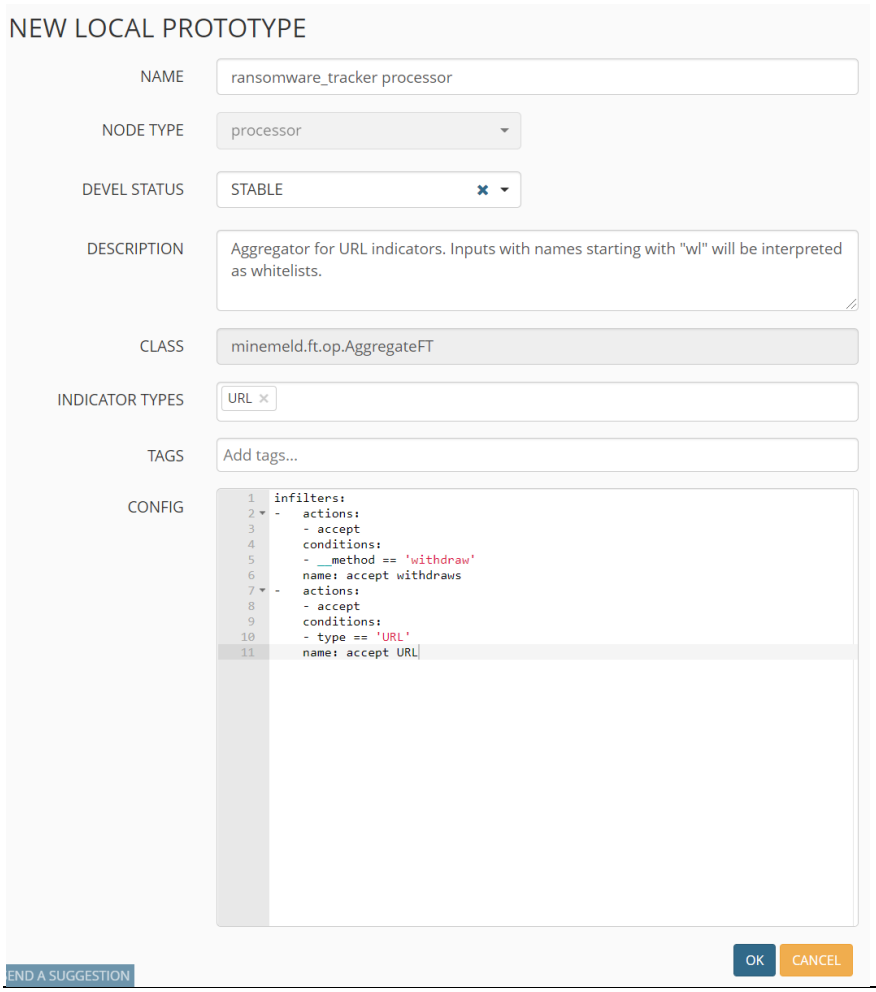
Εικόνα 68 - Minemeld Miner (1)

Δίνουμε ένα όνομα, επιλέγουμε το πρωτότυπο που δημιουργήσαμε και κάνουμε κλικ στο OK.



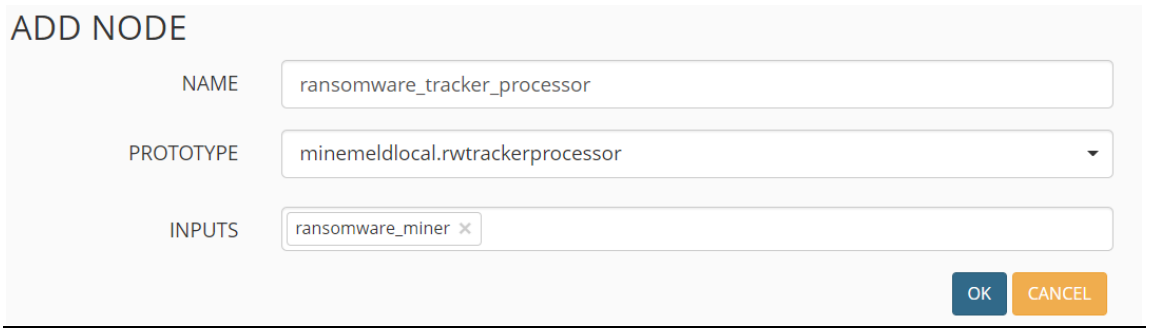
Εικόνα 69 - Minemeld Miner (2)

Τώρα θα προσθέσουμε τον επεξεργαστή του πρωτοτύπου (processor). Ο επεξεργαστής θα αφαιρέσει τις διπλότυπες καταχωρήσεις από την ροή των πληροφοριών. Πατάμε εικονίδιο ≡ στην καρτέλα CONFIG, αναζητούμε το 'stdlib.aggregatorURL' και στην συνέχεια δημιουργούμε ένα νέο με βάση αυτό. Μόλις είμαστε έτοιμοι πατάμε στο OK.



Εικόνα 70 - Minemeld Processor (1)

Προσθέτουμε τον κόμβο με τον ρόλο του miner για το πρωτότυπο αυτό: (Ενεργοποιούμε το advanced mode από το CONFIG και πατάμε στο **+**). Κάνουμε κλικ στο OK για να το προσθέσουμε.

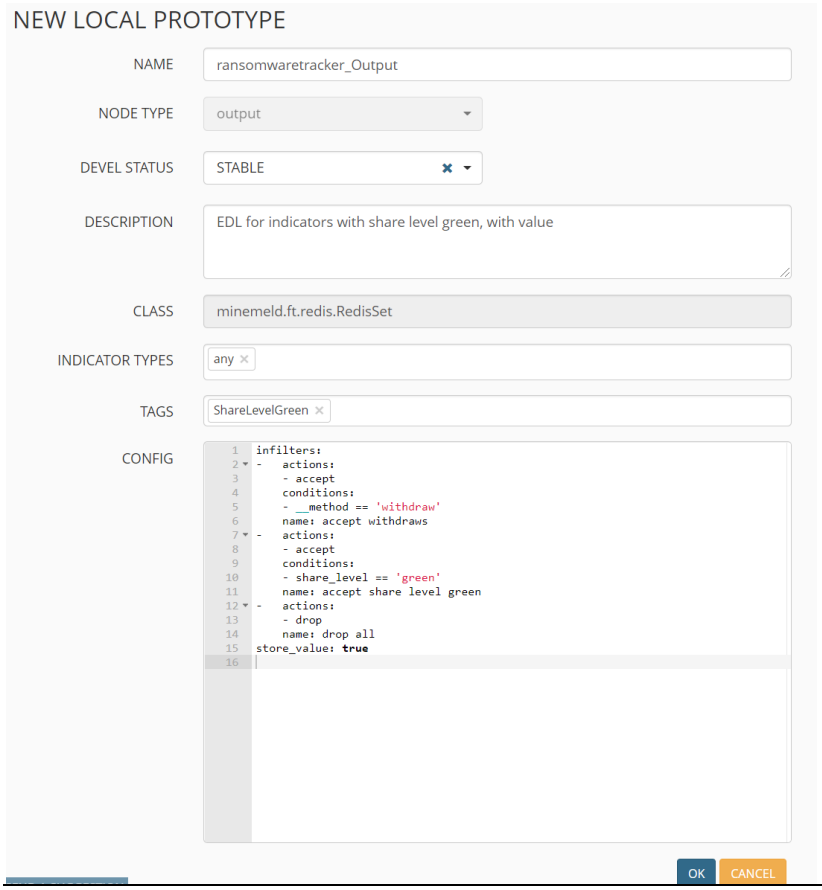


Εικόνα 71 - Minemeld Processor (2)

Έπειτα, θα δημιουργήσουμε το πρωτότυπο για το output όλων των παραπάνω. Επιλέγουμε το

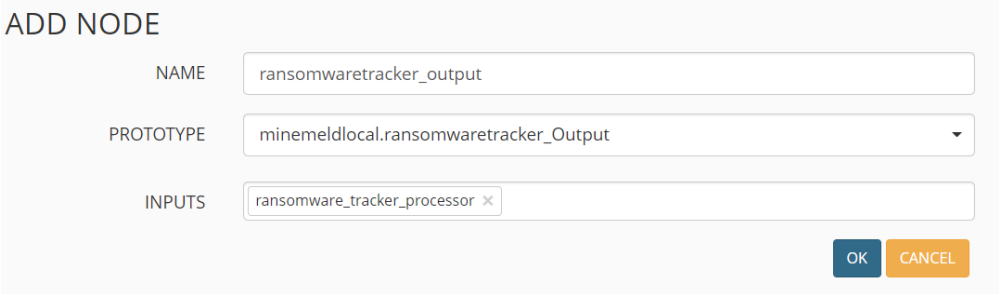
‘stdlib.feedGreenWithValue’ από την λίστα και δημιουργούμε ένα νέο με τις εξής επιλογές:

```
infilters:
-   actions:
    - accept
    conditions:
    - __method == 'withdraw'
    name: accept withdraws
-   actions:
    - accept
    conditions:
    - share_level == 'green'
    name: accept share level green
-   actions:
    - drop
    name: drop all
store_value: true
```



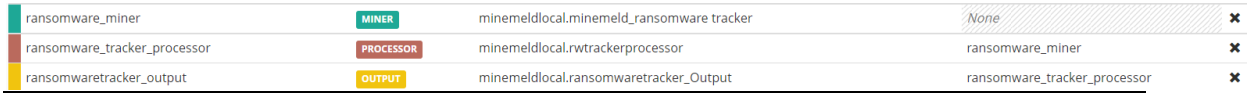
Εικόνα 72 - Minemeld Output (1)

Δημιουργούμε το miner για το πρωτότυπο που δημιουργήσαμε και κάνουμε κλικ στο OK.



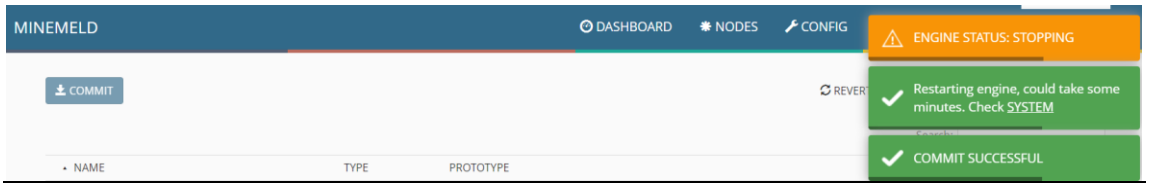
Εικόνα 73 - Minemeld Output (2)

Έτσι λοιπόν, δημιουργήσαμε όλους τους κόμβους και είμαστε έτοιμοι να πάρουμε τα URLS από την λίστα που ορίσαμε στην πλατφόρμα του Minemeld.



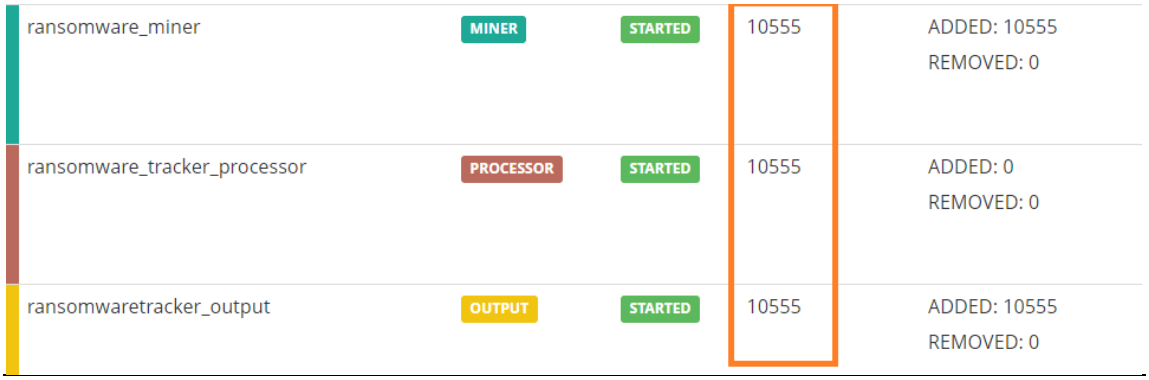
Εικόνα 74 - Minemeld Nodes

Αρκεί να πατήσουμε στο COMMIT για να εφαρμοστούν οι αλλαγές μας:



Εικόνα 75 - Minemeld Commit

Στην λίστα των κόμβων θα φαίνονται πια και οι δείκτες που φορτώνονται στην πλατφόρμα:



Εικόνα 76 - Minemeld Indicators

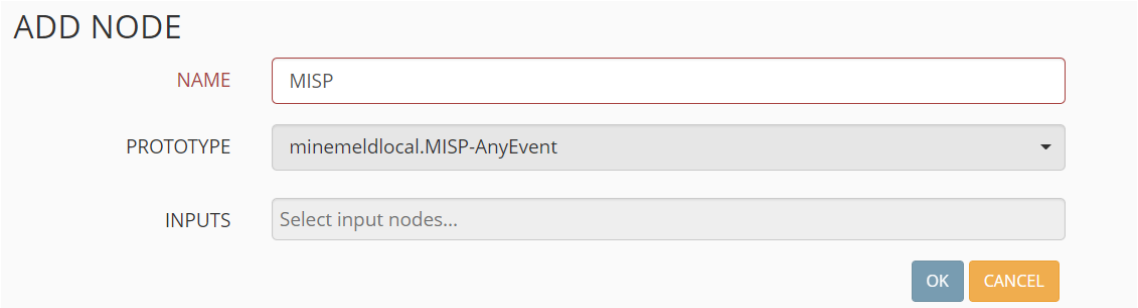
Στην συνέχεια, θα παραμετροποιήσουμε το Minemeld να παίρνει και πληροφορίες από την πλατφόρμα του MISP που εγκαταστήσαμε σε προηγούμενη ενότητα.

Δημιουργούμε ένα νέο πρωτότυπο με βάση το 'minemeldlocal.MISP-AnyEvent' που υπάρχει στο Minemeld. Ρυθμίζουμε το config αρχείο όπως παρακάτω και κάνουμε κλικ στο OK.

Στην διεύθυνση URL θα πρέπει να ορίσουμε το URL της πλατφόρμας του MISP και σε περίπτωση που δεν έχουμε δημιουργήσει self-signed certificate, ορίζουμε την επιλογή του verify_cert ως false, κάτι το οποίο δεν προτείνεται.

```
age_out:
   default: null
   sudden_death: true
attributes:
   confidence: 70
   share_leve: white
client_cert_required: false
filters:
   published: 1
   tag: tlp:white
honour_ids_flag: true
indicator_types: null
source_name: MISP
url: http://192.168.6.56
verify_cert: true
```

Δημιουργούμε ένα νέο κόμβο και ορίζουμε το πρωτότυπο 'minemeldlocal.MISP-AnyEvent' που φτιάξαμε.

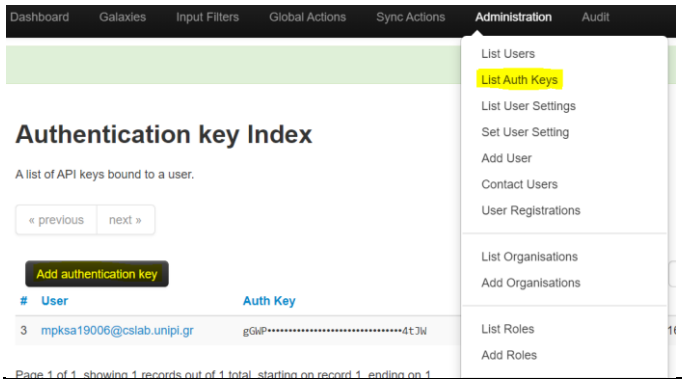


Εικόνα 77 - Minemeld-MISP Connection (1)

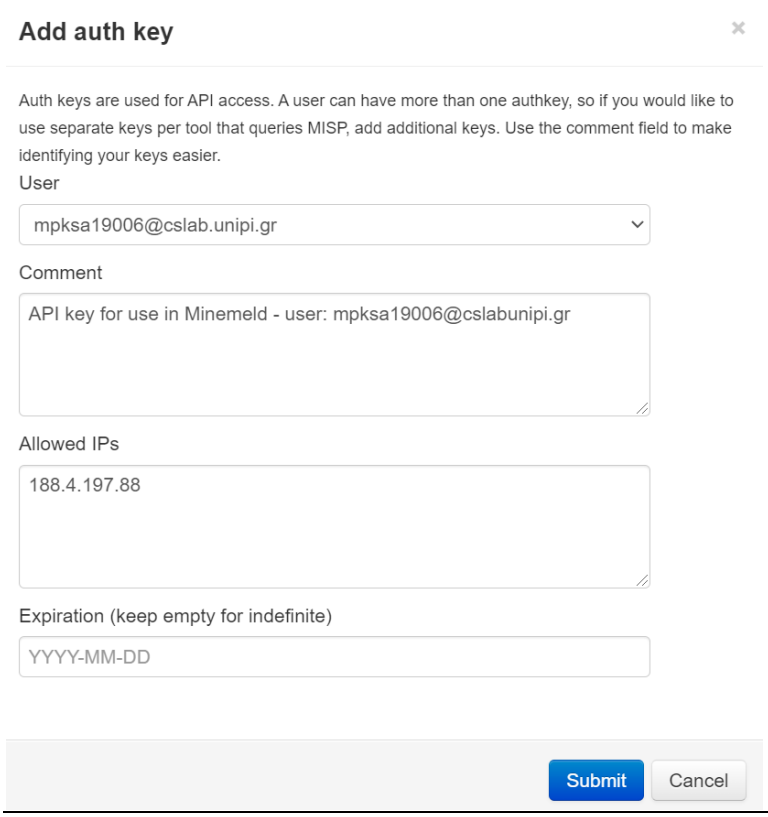
Έπειτα, πατάμε στο COMMIT για να πάρει την αλλαγή η πλατφόρμα.

Τώρα θα πρέπει να ορίσουμε και ένα κλειδί API για να μπορέσουμε να έχουμε επικοινωνία μεταξύ του Minemeld και του MISP.

Για να δημιουργήσουμε ένα API key στο MISP, αρκεί να πάμε στο Administration -> List Auth Keys -> Add authentication key:

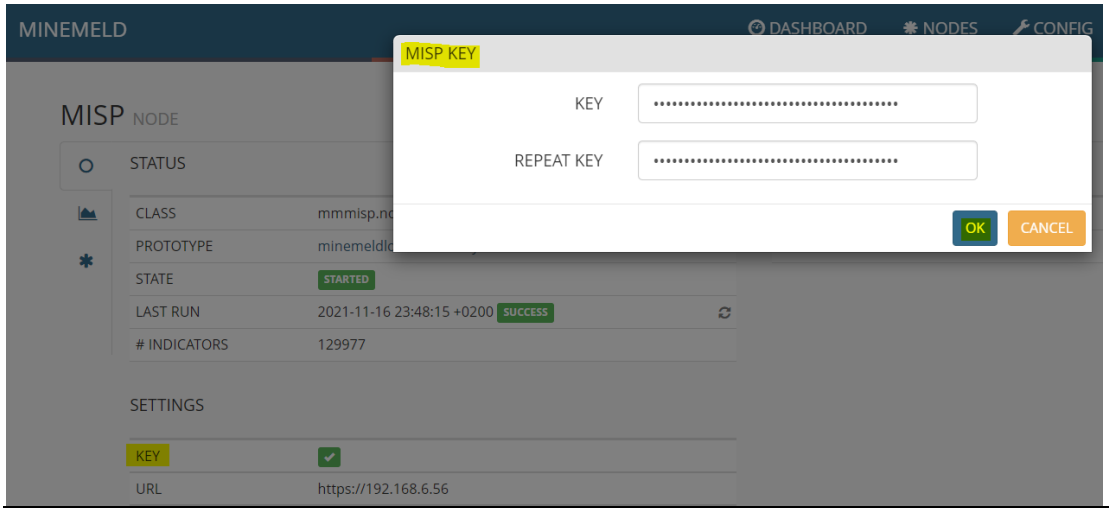


Εικόνα 78 - Minemeld-MISP Connection (2)



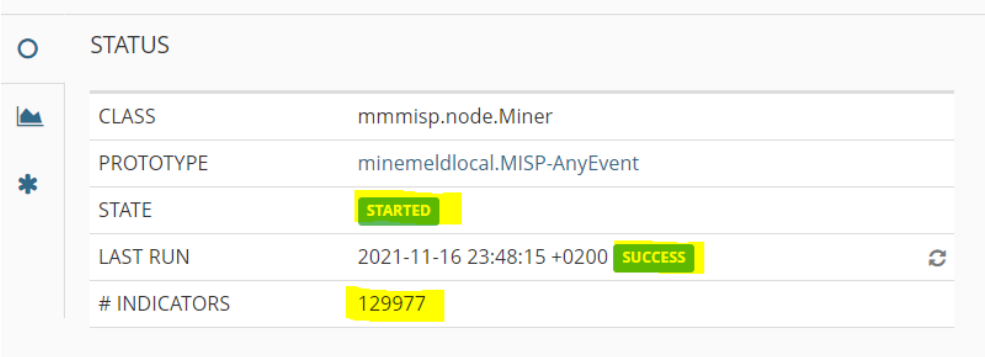
Εικόνα 79 - Minemeld-MISP Connection (3)

Στην συνέχεια, κάνουμε κλικ στον κόμβο του MISP, πατάμε στο KEY και ορίζουμε το API κλειδί που έχουμε δημιουργήσει:



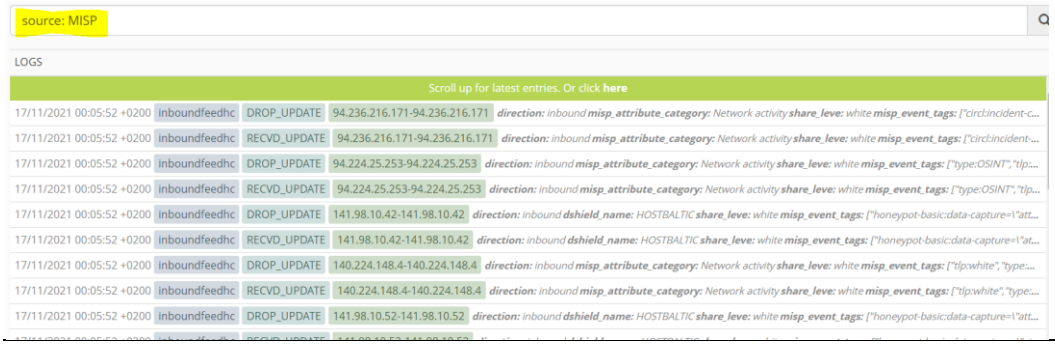
Εικόνα 80 - Minemeld-MISP Connection (4)

Αν η επικοινωνία είναι εφικτή, τότε θα μας εμφανιστεί η κατάσταση STARTED καθώς και πληροφορίες της ακριβής ημέρας και ώρας που έτρεξε τελευταία φορά και ο αριθμός των δεικτών που έχουν εισαχθεί.



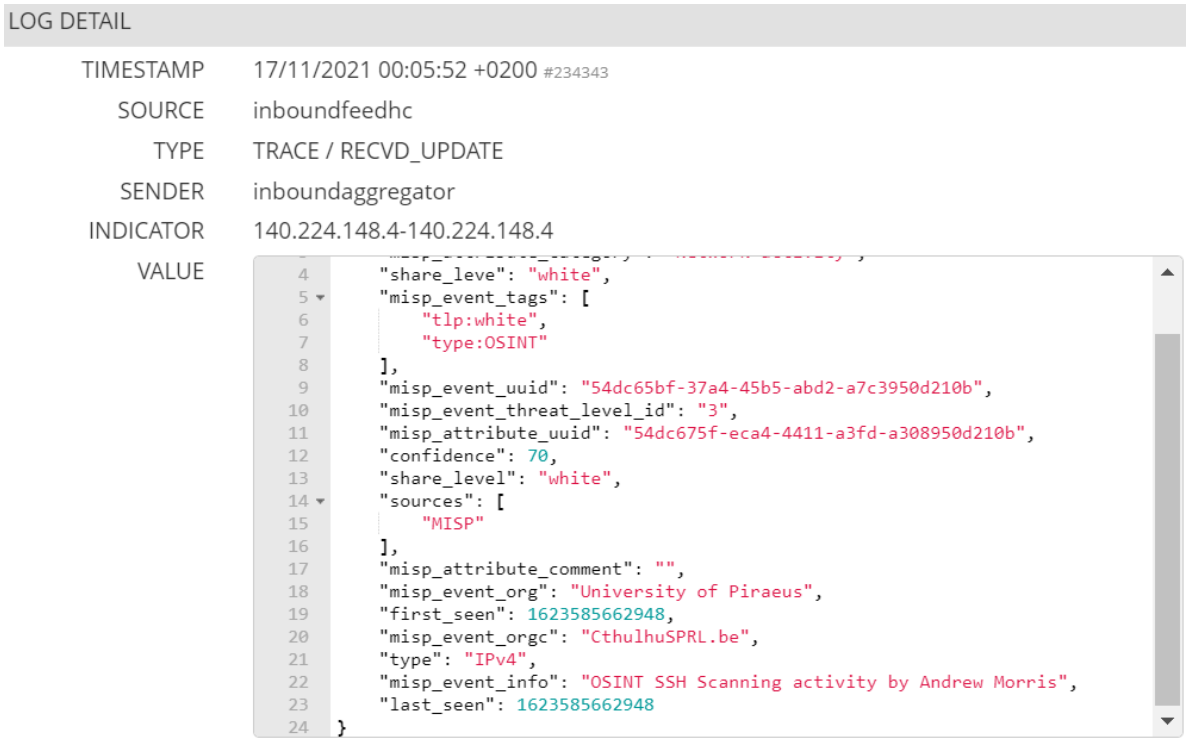
Εικόνα 81 - Minemeld-MISP Connection (5)

Έτσι, μπορούμε να πάμε στην καρτέλα των LOGS και να δούμε πληροφορίες για δείκτες που προέρχονται από την πλατφόρμα του MISP.



Εικόνα 82 - Minemeld-MISP Connection (6)

Κάνοντας κλικ πάνω σε έναν δείκτη μπορούμε φυσικά να δούμε περισσότερες πληροφορίες, έχοντας την πληροφορία σε μορφή YAML:



Εικόνα 83 - Minemeld-MISP Connection (7)

Αναλυτικές πληροφορίες για τον συγκεκριμένο δείκτη, καθώς και τα στοιχεία που το συνδέουν μπορούμε να δούμε όπως αναφέραμε σε προηγούμενη ενότητα στην πλατφόρμα του MISP.

Κεφάλαιο 4 – SOC (Security Operations Center)

Το κέντρο επιχειρήσεων ασφαλείας (SOC) είναι μια κεντρική τοποθεσία όπου μια ομάδα ασφάλειας πληροφοριών παρακολουθεί, εντοπίζει, αναλύει και αποκρίνεται σε περιστατικά ασφάλειας στον κυβερνοχώρο, συνήθως σε συνεχή βάση 24x7x365. [24]

Η ομάδα ασφαλείας, η οποία αποτελείται από αναλυτές ασφαλείας και μηχανικούς, επιβλέπει όλη τη δραστηριότητα σε διακομιστές, δίκτυα, βάσεις δεδομένων, εφαρμογές, υπολογιστές, ιστότοπους και άλλα συστήματα με μοναδικό σκοπό τον εντοπισμό πιθανών απειλών ασφαλείας και την αποτροπή αυτών το συντομότερο δυνατό. Επίσης, παρακολουθούν εξωτερικές πηγές, όπως οι λίστες απειλών που μπορεί να επηρεάσουν το επίπεδο ασφάλειας του οργανισμού. [24]

Ένα SOC δεν πρέπει μόνο να εντοπίζει απειλές, αλλά να τις αναλύει, να ερευνά την πηγή, να αναφέρει τυχόν ευπάθειες που ανακαλύφθηκαν και να σχεδιάζει πώς να αποτρέψει παρόμοια περιστατικά στο μέλλον. Με άλλα λόγια, αντιμετωπίζουν προβλήματα ασφάλειας σε πραγματικό χρόνο, ενώ αναζητούν συνεχώς τρόπους βελτίωσης του επιπέδου ασφάλειας του οργανισμού. [24]

Το SOC αποτελείται από αναλυτές και εξειδικευμένους μηχανικούς ασφαλείας, μαζί με ανθρώπους που παρακολουθούν για απειλές ασφάλειας, γνωρίζουν συγκεκριμένες διαδικασίες που πρέπει να ακολουθήσουν σε περίπτωση παραβίασης και διασφαλίζουν ότι όλα λειτουργούν ομαλά. Οι ρόλοι σε ένα SOC υιοθετούν μια ιεραρχική προσέγγιση για τη διαχείριση θεμάτων ασφάλειας, όπου οι αναλυτές και οι μηχανικοί κατηγοριοποιούνται με βάση το σύνολο δεξιοτήτων και την εμπειρία τους. [24]

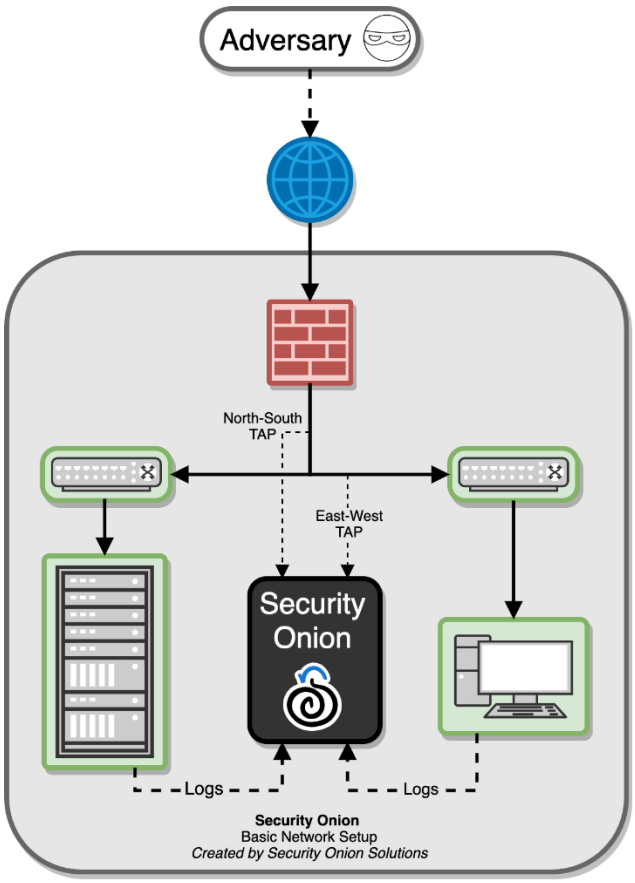
Με απλά λόγια, με την χρήση ενός SOC διαβεβαιώνουμε ότι οι απειλές θα εντοπιστούν και θα αποτραπούν σε πραγματικό χρόνο καθώς παρέχουν μια κεντρική, πλήρη εικόνα σχετικά με το επίπεδο της ασφάλειας του οργανισμού. Ακόμη, αυξάνει το επίπεδο εμπιστοσύνης του οργανισμού καθώς διασφαλίζεται το απόρρητο και τα δεδομένα των πελατών. Επιπλέον, μπορεί να μειώσει το κόστος καθώς το κόστος για την υλοποίηση ενός SOC μπορεί να θεωρηθεί μεγάλο αλλά το κόστος σχετικά με μια παραβίαση – συμπεριλαμβανομένης της απώλειας των δεδομένων μπορεί να είναι καταστροφικό για τον οργανισμό.

Στο κεφάλαιο αυτό, θα χρησιμοποιήσουμε το Security Onion, ένα λογισμικό ανοιχτού κώδικα για την παρακολούθηση των κυβερνοαπειλών.

4.1 ΕΙΣΑΓΩΓΗ ΣΤΟ SECURITY ONION

Το Security Onion είναι μια διανομή βασισμένη σε Linux για την παρακολούθηση της ασφάλειας του δικτύου και της ασφάλειας των οργανισμών από κλοπές, παραβιάσεις δεδομένων ή επιθέσεις στον κυβερνοχώρο. Μπορεί να χρησιμοποιηθεί προληπτικά για τον εντοπισμό των τρωτών σημείων αλλά και αντιδραστικά όταν πρόκειται να αντιμετωπίσουμε περιστατικά κυβερνοασφάλειας. Εργαλεία όπως το Security Onion περιλαμβάνουν το πλαίσιο, την ευφυΐα και την επίγνωση της κατάστασης του δικτύου του οργανισμού και μπορεί να βοηθήσει και να αυξήσει σημαντικά το επίπεδο ασφάλειας ενός οργανισμού. [20]

Στο παρακάτω διάγραμμα, απεικονίζεται το Security Onion σε ένα εταιρικό δίκτυο που περιλαμβάνει τείχος προστασίας, διακομιστές και τελικούς υπολογιστές χρηστών.



Εικόνα 84 - Security Onion Diagram

Το Security Onion μπορεί να παρακολουθήσει όλη την δικτυακή κίνηση του οργανισμού, να ανιχνεύσει έναν κακόβουλο που προσπαθεί να εισέλθει στο εταιρικό δίκτυο ή ακόμη και αυτόν που προσπαθεί να δημιουργήσει κέντρα ελέγχου μέσω C&C. Μπορεί επίσης να ανιχνεύσει επιθέσεις όπως η πλευρική κίνηση (lateral movement). Καθώς η κίνηση του δικτύου γίνεται ολοένα και περισσότερο κρυπτογραφημένη, είναι σημαντικό να βελτιώσουμε

την ορατότητα μας χρησιμοποιώντας τέτοια εργαλεία. Το Security Onion μπορεί να τραβήξει αρχεία καταγραφής από τους διακομιστές και τους σταθμούς εργασίας, ώστε να μας βοηθήσει στην αναζήτηση της απειλής και την προστασία μας από τους κακόβουλους χρήστες.

4.2 ΕΓΚΑΤΑΣΤΑΣΗ SECURITY ONION

Για την εγκατάσταση της δωρεάν έκδοσης του Security Onion σε δικό μας μηχάνημα (on premises) θα πρέπει να κατεβάσουμε αρχικά το ISO από την ιστοσελίδα του Security Onion στο Github και να επιβεβαιώσουμε την υπογραφή του αρχείου.

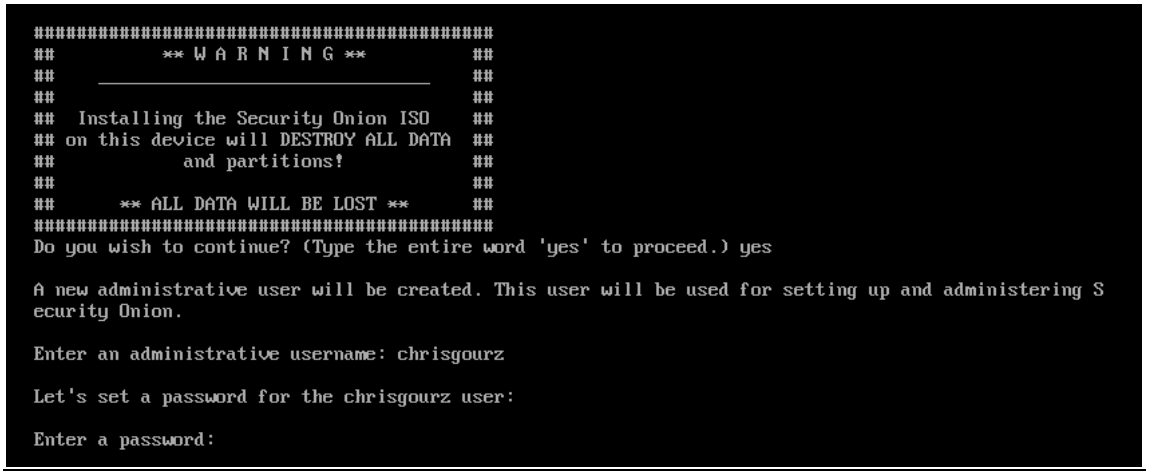
Αφού επιβεβαιώσουμε ότι το ISO αντιστοιχεί στην υπογραφή του Security Onion, είμαστε σε θέση να προχωρήσουμε στην εγκατάσταση.

Η δημιουργία του VM καθώς και τα χαρακτηριστικά που θα του δώσουμε, ποικίλουν ανάλογα την χρήση για την οποία το προγραμματίζουμε.

Βήμα 1ο. Δημιουργία του VM και εγκατάσταση Security Onion

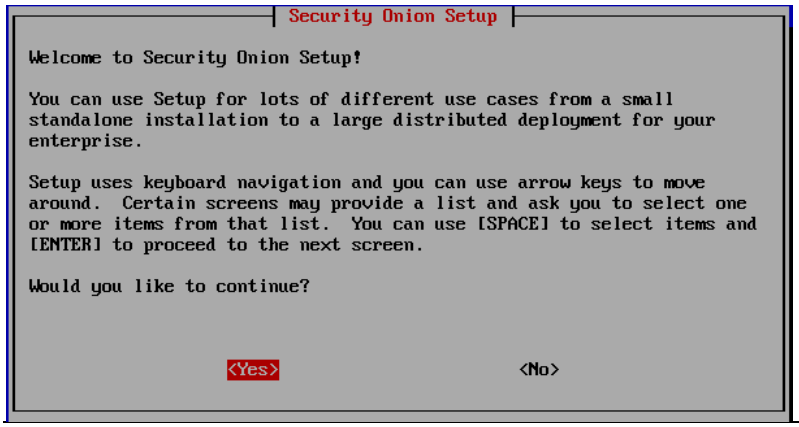
Εικόνα 85 - Εγκατάσταση Security Onion (1)

Βήμα 2ο. Δημιουργία χρήστη administrator

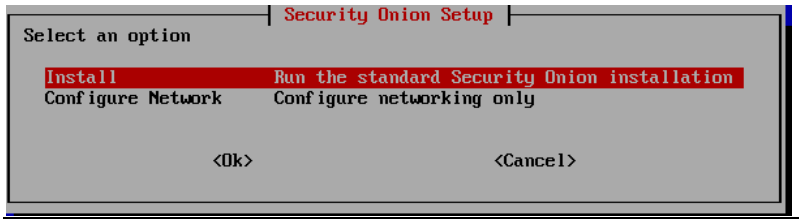


Εικόνα 86- Εγκατάσταση Security Onion (2)

Βήμα 3ο. Έναρξη εγκατάστασης του Security Onion

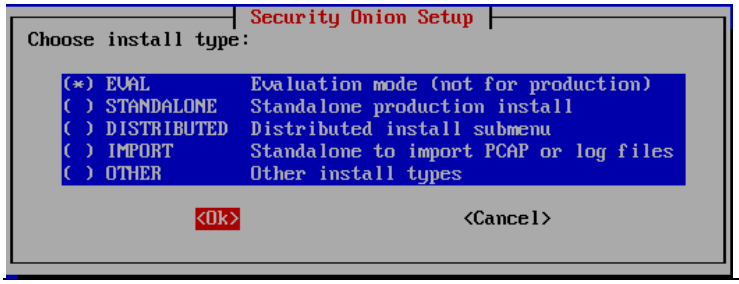


Εικόνα 87 - Εγκατάσταση Security Onion (3)



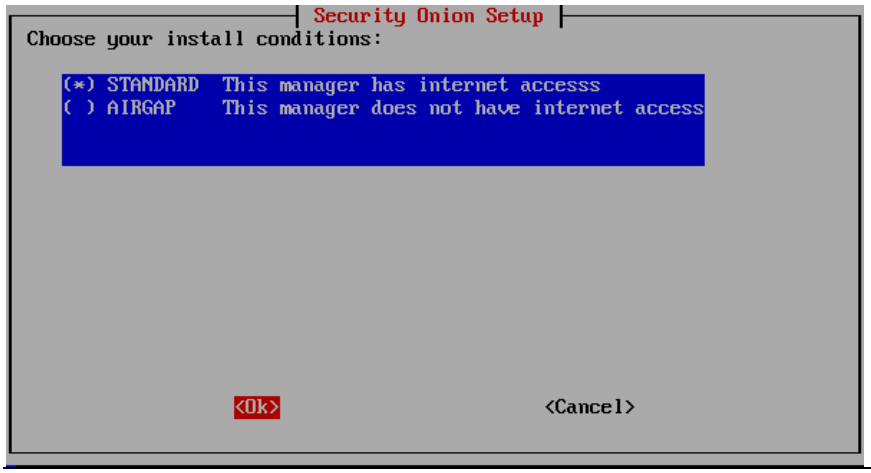
Εικόνα 88 - Εγκατάσταση Security Onion (4)

Βήμα 4ο. Επιλογή τύπου εγκατάστασης

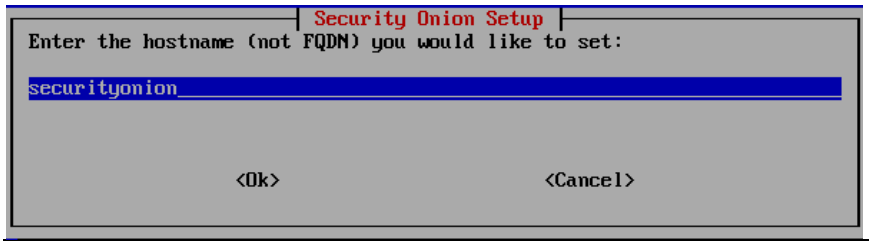


Εικόνα 89 - Εγκατάσταση Security Onion (5)

Βήμα 5ο. Επιλογή τύπου εγκατάστασης και ρύθμιση του ονόματος (hostname)

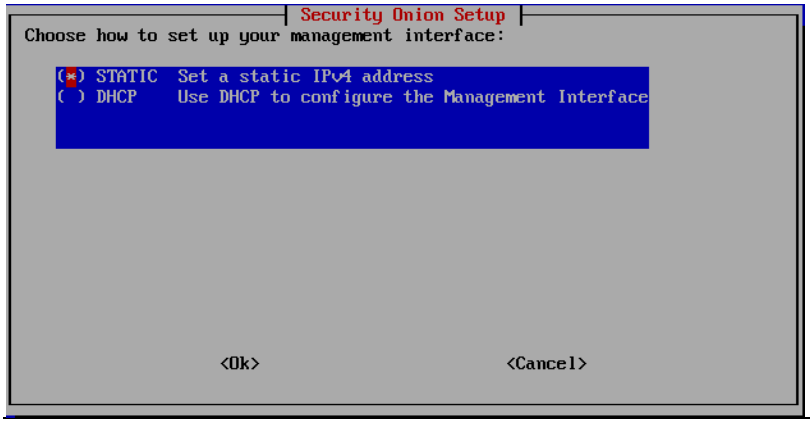


Εικόνα 90 - Εγκατάσταση Security Onion (6)

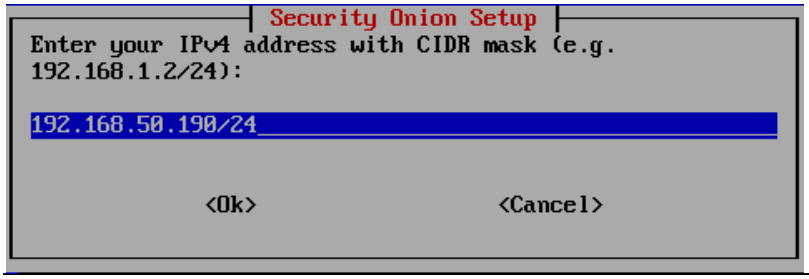


Εικόνα 91 - Εγκατάσταση Security Onion (7)

Βήμα 6ο. Ρύθμιση του δικτύου



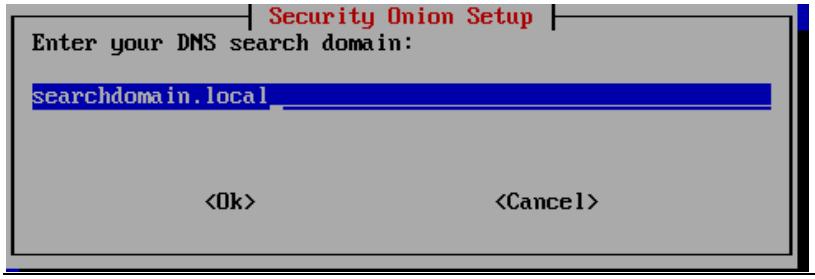
Εικόνα 92 - Εγκατάσταση Security Onion (8)



Εικόνα 93 - Εγκατάσταση Security Onion (9)

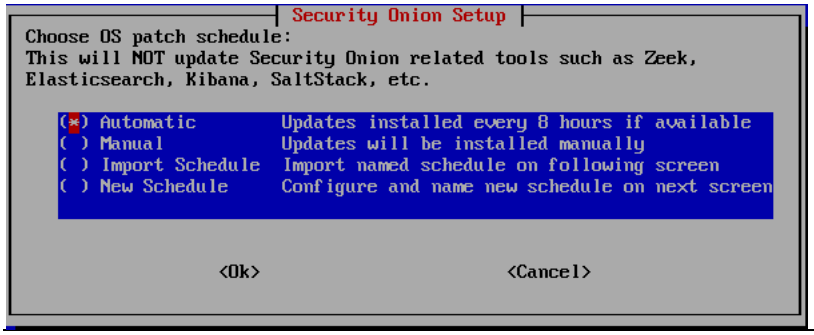
Εικόνα 94 - Εγκατάσταση Security Onion (10)

Εικόνα 95 - Εγκατάσταση Security Onion (11)



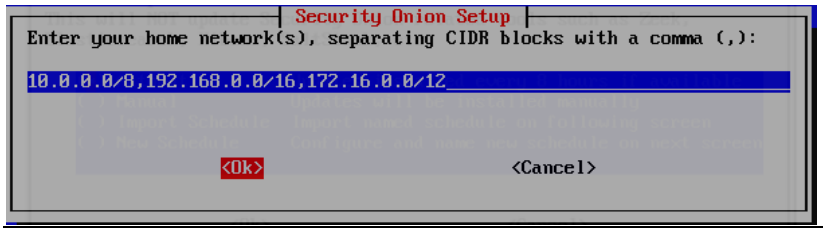
Εικόνα 96 - Εγκατάσταση Security Onion (12)

Βήμα 7ο. Ρύθμιση των ενημερώσεων για το Security Onion



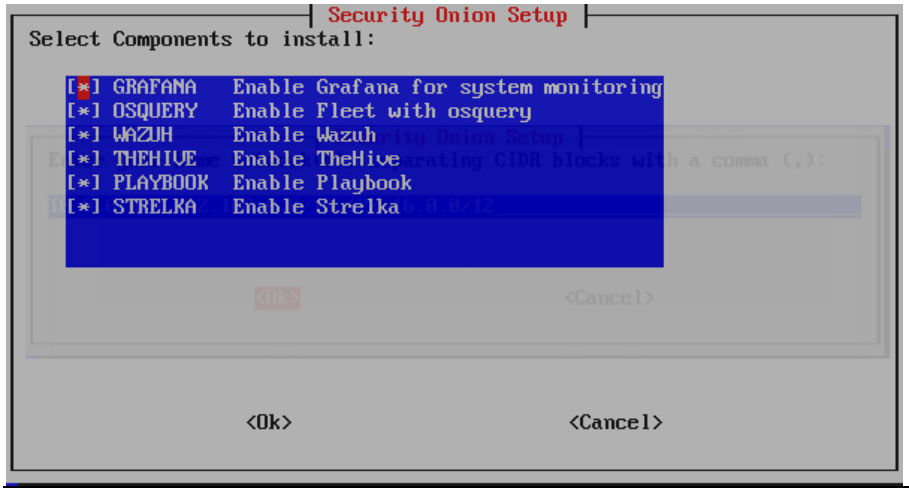
Εικόνα 97 - Εγκατάσταση Security Onion (13)

Βήμα 8ο. Θα πρέπει να ορίσουμε το εύρος του δικτύου μας, αν αυτό δεν περιλαμβάνεται παρακάτω:



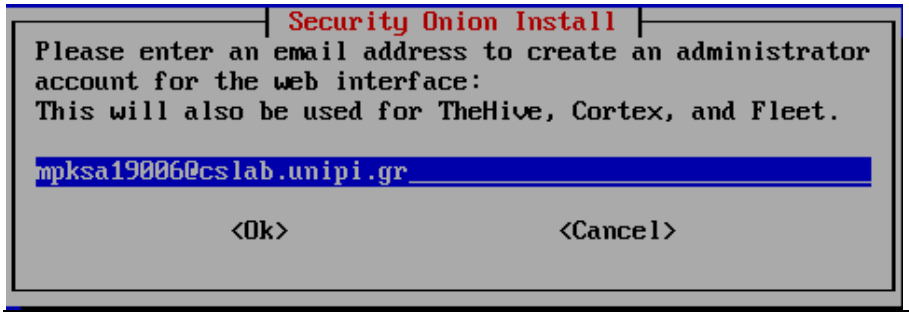
Εικόνα 98 - Εγκατάσταση Security Onion (14)

Βήμα 9ο. Επιλογή των εργαλείων που θέλουμε να εγκαταστήσουμε

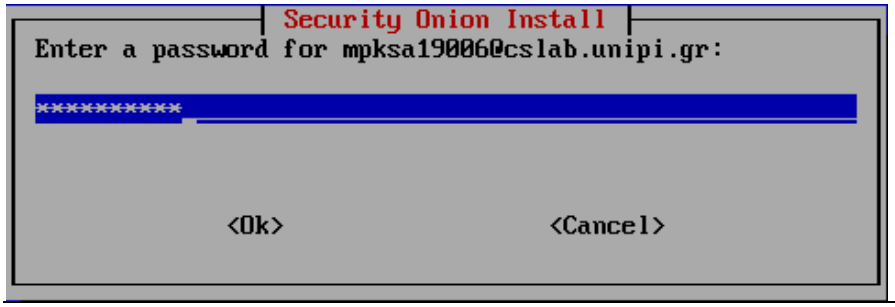


Εικόνα 99 - Εγκατάσταση Security Onion (14)

Βήμα 10ο. Δημιουργία administrator χρήστη για το WEB UI

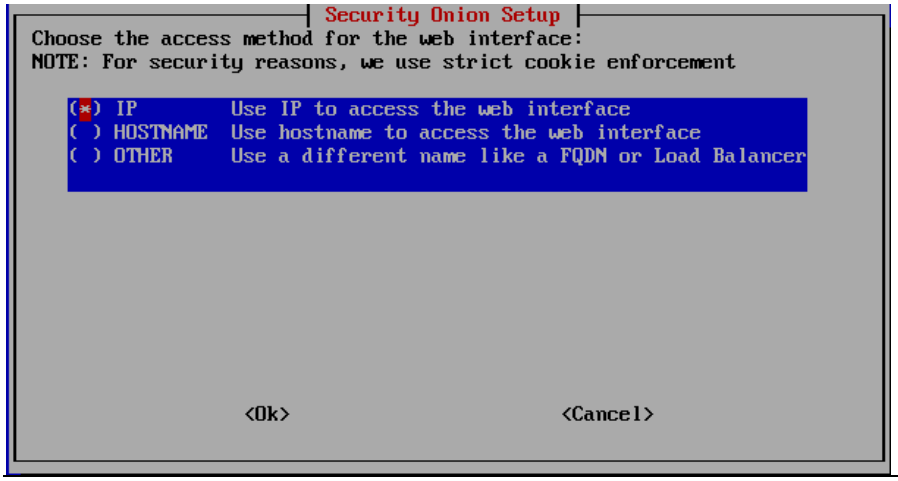


Εικόνα 100 - Εγκατάσταση Security Onion (15)

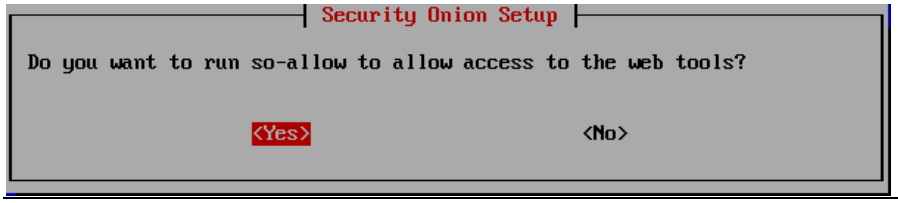


Εικόνα 101 - Εγκατάσταση Security Onion (16)

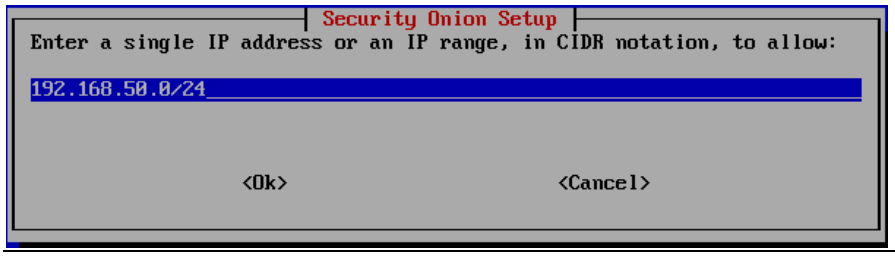
Βήμα 11ο. Επιλογή τύπου πρόσβασης στο WEB UI και ρύθμιση του εύρους των IP διευθύνσεων μας για πρόσβαση σε αυτό



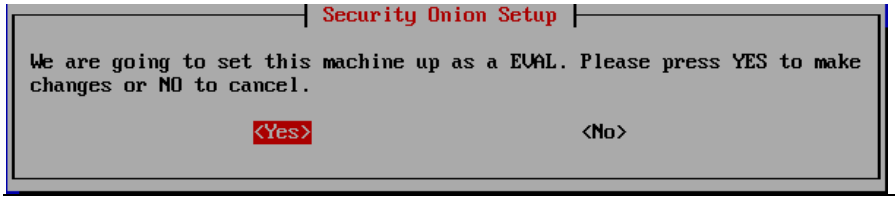
Εικόνα 102 - Εγκατάσταση Security Onion (17)



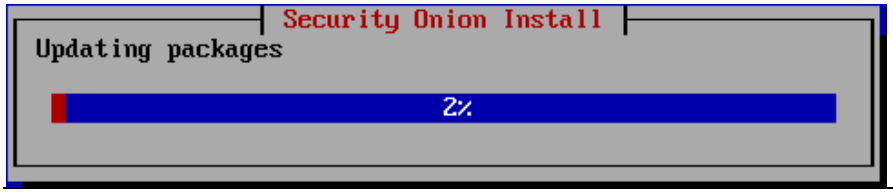
Εικόνα 103 - Εγκατάσταση Security Onion (18)



Εικόνα 104 - Εγκατάσταση Security Onion (19)

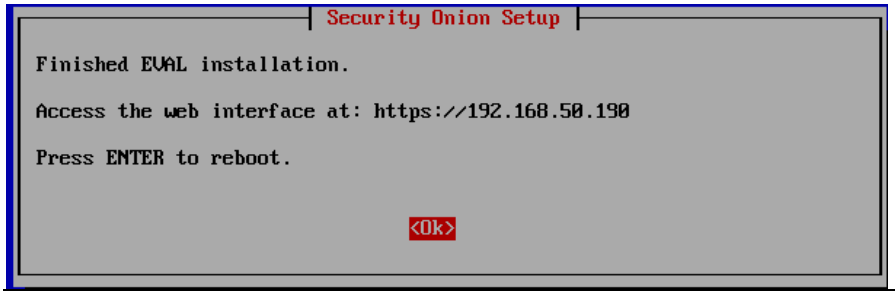


Εικόνα 105 - Εγκατάσταση Security Onion (20)



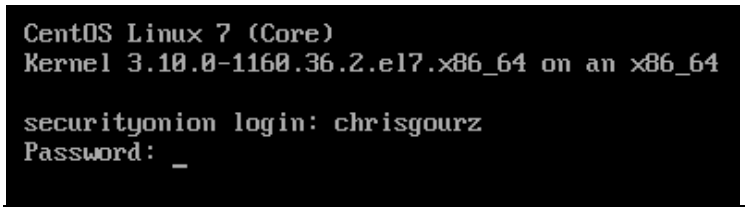
Εικόνα 106 - Εγκατάσταση Security Onion (21)

Βήμα 12ο. Ολοκλήρωση εγκατάστασης, σύνδεση μέσω της κονσόλας, έλεγχος καλής λειτουργίας και σύνδεση στο WEB UI.



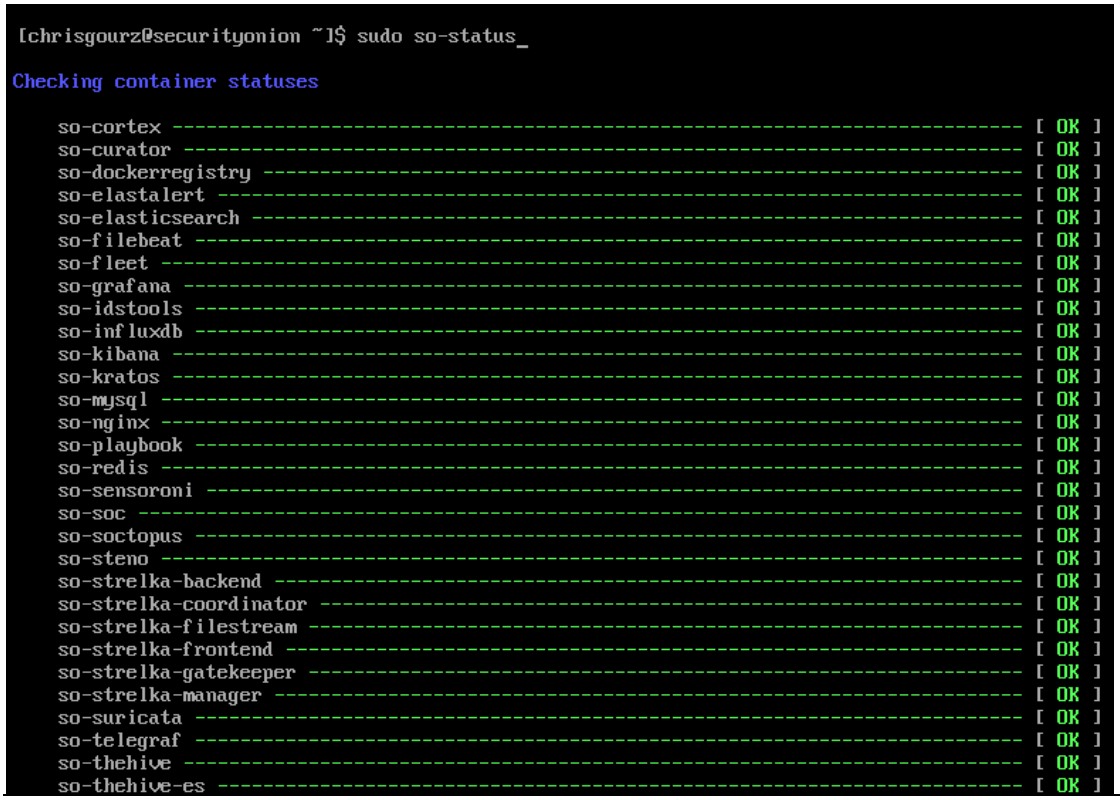
Εικόνα 107 - Εγκατάσταση Security Onion (22)

Σύνδεση μέσω της κονσόλας:



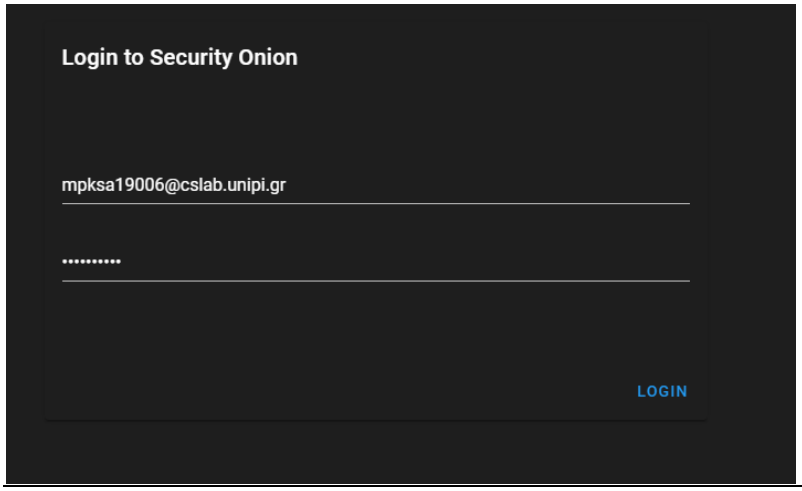
Εικόνα 108 - Security Onion Console Login

Έλεγχος της καλής λειτουργίας των υπηρεσιών του Security Onion:



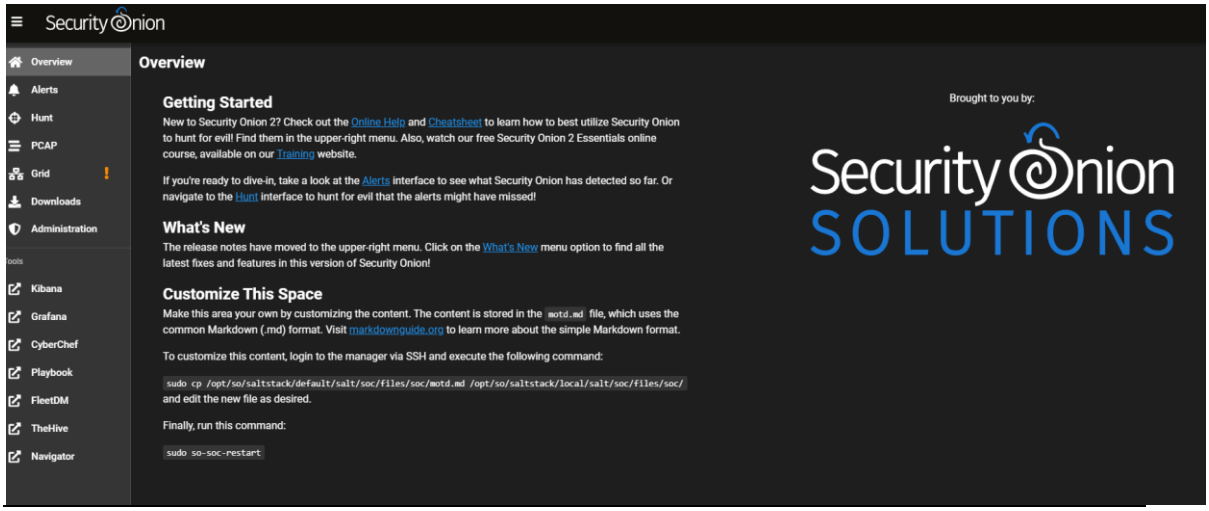
Εικόνα 109 - Security Onion Services Check

Σύνδεση στο WEB UI με την IP και τον χρήστη που ορίσαμε:



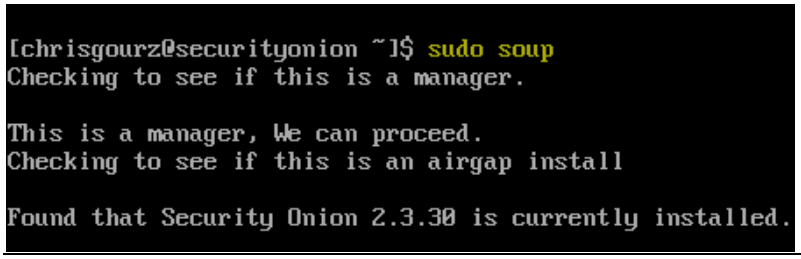
Εικόνα 110 - Security Onion WEB UI (1)

Η πρώτη εικόνα που παίρνουμε μετά την σύνδεση είναι η παρακάτω, που περιλαμβάνει όλες τις επιλογές καθώς και τα εργαλεία που έχουμε εγκαταστήσει σε αυτό.



Εικόνα 111 - Security Onion WEB UI (2)

Βήμα 13ο. Για να αναβαθμίσουμε το Security Onion, αρκεί να τρέξουμε την παρακάτω εντολή:

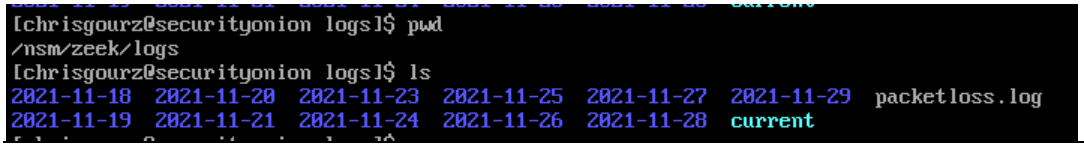


Εικόνα 112 - Security Onion Update

4.3 ΠΑΡΑΚΟΛΟΥΘΗΣΗ ΣΤΟ SECURITY ONION

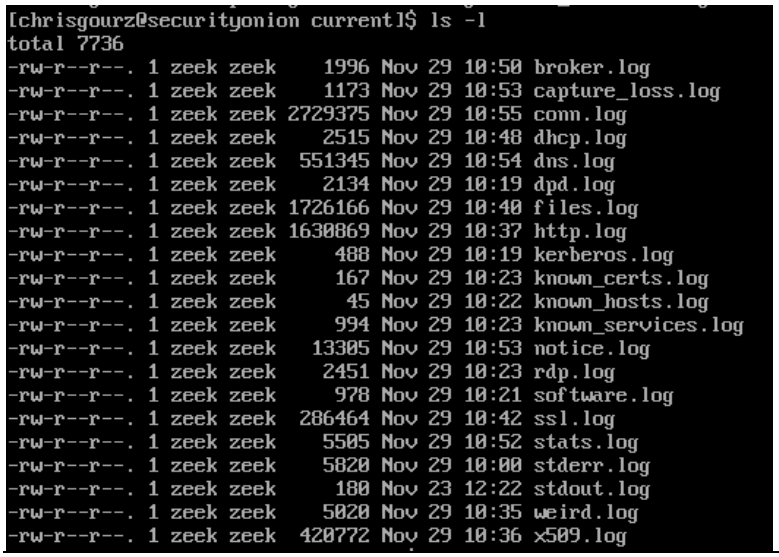
Στην συγκεκριμένη ενότητα θα πραγματοποιήσουμε ορισμένες επιθέσεις από το Kali Linux που είναι το μηχάνημα των επιθέσεων προς τα Windows μηχανήματα που έχουν τον ρόλο των τελικών υπολογιστών. Σκοπός είναι να δούμε πως μπορούμε να τις εντοπίσουμε και να τις παρακολουθήσουμε μέσα από το Security Onion.

Το Security Onion χρησιμοποιεί το zeek και τα αρχεία καταγραφής στέλνονται για ανάλυση και αποθήκευση στο ElasticSearch. Όλα τα αρχεία καταγραφής (logs) αποθηκεύονται στην τοποθεσία /nsm/zeek/logs:



Εικόνα 113 - Zeek Logs (1)

Τα αρχεία καταγραφής κατηγοριοποιούνται ανά ημέρα και ημερομηνία και μέσα σε αυτά μπορούμε να βρούμε πάλι ανά κατηγορία χωρισμένα, όπως για παράδειγμα την κίνηση DNS,HTTP και τα οποία μπορούμε να εξετάσουμε περεταίρω.



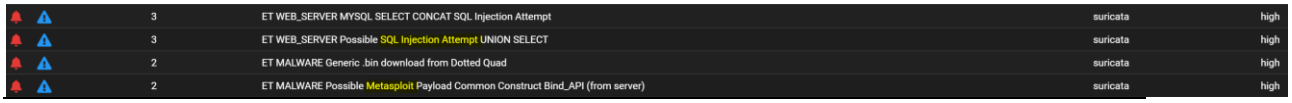
Εικόνα 114 - Zeek Logs (2)

Όλα αυτά βέβαια μπορούμε να τα δούμε και στο WEB UI του Security Onion. Είναι αρκετά παραμετροποιήσιμο και μπορούμε να ορίσουμε τα δικά μας φίλτρα, να δημιουργήσουμε τους δικούς μας πίνακες και γενικότερα να παρακολουθήσουμε τα πάντα μέσα από αυτό.

Στην σελίδα των “Alerts” βλέπουμε την κακόβουλη συμπεριφορά από το μηχάνημα των επιθέσεων προς τους τελικούς υπολογιστές. [10]

	Count	rule.name	event.module	event.severity_label
	2,269	ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	suricata	high
	2,269	ET SCAN Possible Nmap User-Agent Observed	suricata	high
	199	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt	suricata	high
	44	ET INFO Executable Download from dotted-quad Host	suricata	high
	20	GPL EXPLOIT iissamples access	suricata	high
	14	ET WEB_SPECIFIC_APPS WEB-PHP RCE PHPBB 2004-1315	suricata	high

Εικόνα 115 - Security Onion Alerts (1)

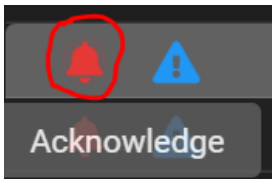


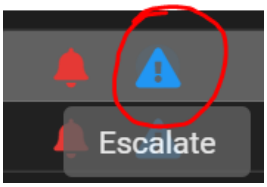
	3	ET WEB_SERVER MYSQL SELECT CONCAT SQL Injection Attempt	suricata	high
	3	ET WEB_SERVER Possible SQL Injection Attempt UNION SELECT	suricata	high
	2	ET MALWARE Generic .bin download from Dotted Quad	suricata	high
	2	ET MALWARE Possible Metasploit Payload Common Construct Bind_API (from server)	suricata	high

Εικόνα 116 - Security Onion Alerts (2)

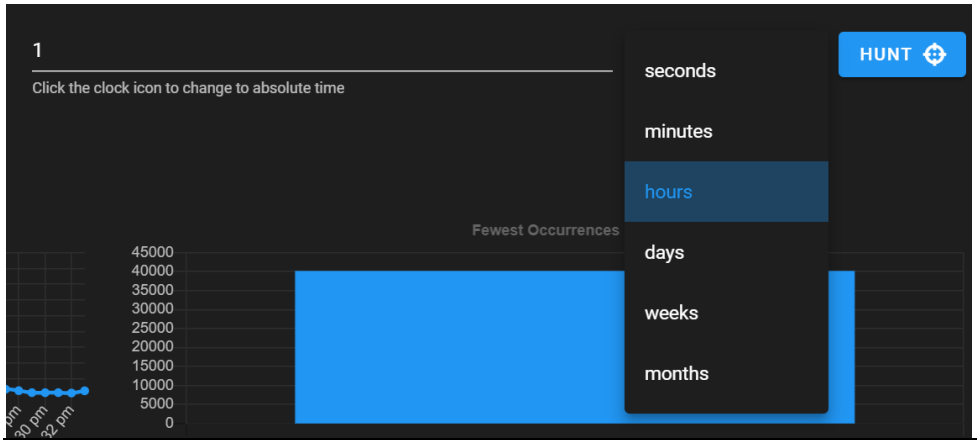
Στις παραπάνω εικόνες απεικονίζεται η κακόβουλη συμπεριφορά από το μηχάνημα των επιθέσεων προς τους τελικούς υπολογιστές. Ακόμη, φαίνονται τα εργαλεία που χρησιμοποιήθηκαν όπως είναι το nmap και το Metasploit. Περιλαμβάνει επίσης και τον αριθμό των αρχείων καταγραφής καθώς και το επίπεδο κρισιμότητας. [10]

Επιπλέον, υπάρχει η δυνατότητα εξαίρεσης-αναγνώρισης ενός alert (Acknowledge) και η επιλογή της κλιμάκωσης (Escalate) που δημιουργεί ένα καινούργιο case για περεταίρω ανάλυση. Το εργαλείο που υπάρχει προ-εγκατεστημένο είναι το TheHive.



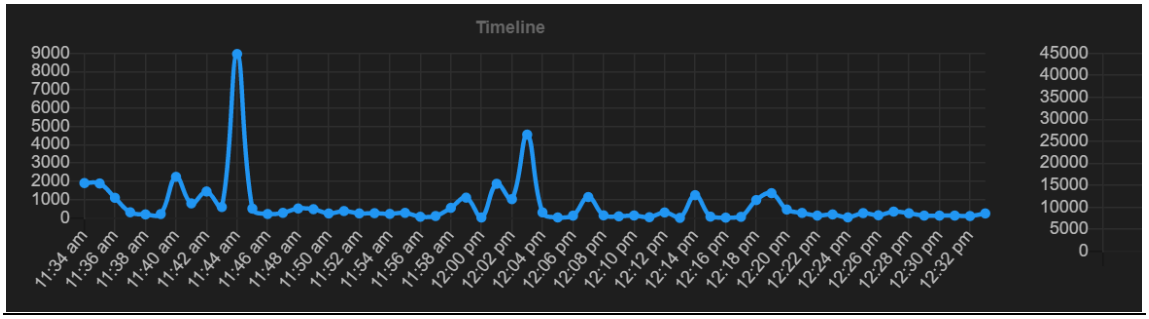


Στην σελίδα του “Hunt” υπάρχει αρχικά η επιλογή της προβολής των αρχείων καταγραφής ανά δευτερόλεπτο/ημέρα/μήνα κτλπ. Το ορίζουμε όπως μας εξυπηρετεί καθώς τα αρχεία καταγραφής ενδέχεται να είναι πάρα πολλά.

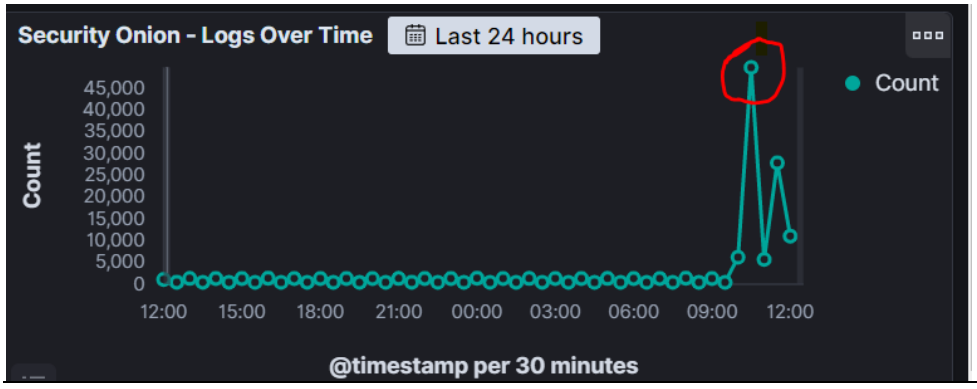


Εικόνα 117 - Security Onion Hunt (1)

Αφού ορίσουμε το διάστημα, απεικονίζονται σε μορφή διαγράμματος το σύνολο των αρχείων καθώς και το ακριβές χρονικό διάστημα που αυτά εμφανίστηκαν.



Εικόνα 118 - Security Onion Hunt (2)



Εικόνα 119 - Security Onion Hunt (3)

Με μια ματιά, βλέπουμε κάποιες σημαντικές πληροφορίες για να καταλάβουμε αρχικά τι συμβαίνει στο δίκτυο μας.

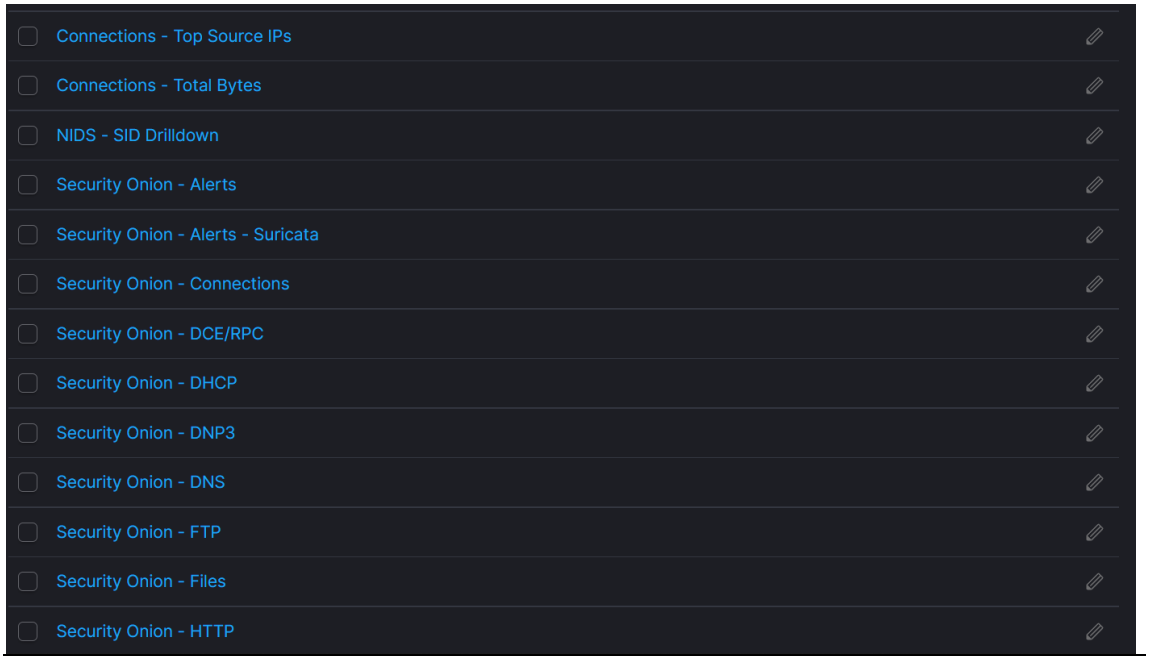
source.ip	source.port	destination.ip	destination.port	rule.name	rule.category	event.severity_label
192.168.6.51	45288	192.168.6.59	80	ET INFO Executable Download from dotted-quad Host	A Network Trojan was detected	high
192.168.6.51	45280	192.168.6.59	80	ET INFO Executable Download from dotted-quad Host	A Network Trojan was detected	high
192.168.6.51	45274	192.168.6.59	80	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt	Web Application Attack	high
192.168.6.51	45270	192.168.6.59	80	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt	Web Application Attack	high
192.168.6.51	45268	192.168.6.59	80	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt	Web Application Attack	high
192.168.6.51	45264	192.168.6.59	80	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt	Web Application Attack	high
192.168.6.51	45238	192.168.6.59	80	ET WEB_SERVER ColdFusion administrator access	Web Application Attack	high
192.168.6.51	45186	192.168.6.59	80	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt	Web Application Attack	high
192.168.6.51	45184	192.168.6.59	80	ET WEB_SERVER Script tag in URI Possible Cross Site Scripting Attempt	Web Application Attack	high

Εικόνα 120 - Security Onion Hunt (4)

source.ip	source.port	destination.ip	destination.port	rule.name	rule.category	event.severity_label
192.168.6.51	45656	192.168.6.50	445	ET SCAN MS Terminal Server Traffic on Non-standard Port	Attempted Information Leak	medium
192.168.6.51	45688	192.168.6.50	445	ET POLICY Outbound MSSQL Connection to Non-Standard Port - Likely Malware	Potentially Bad Traffic	medium
192.168.6.51	45656	192.168.6.50	445	ET SCAN MS Terminal Server Traffic on Non-standard Port	Attempted Information Leak	medium

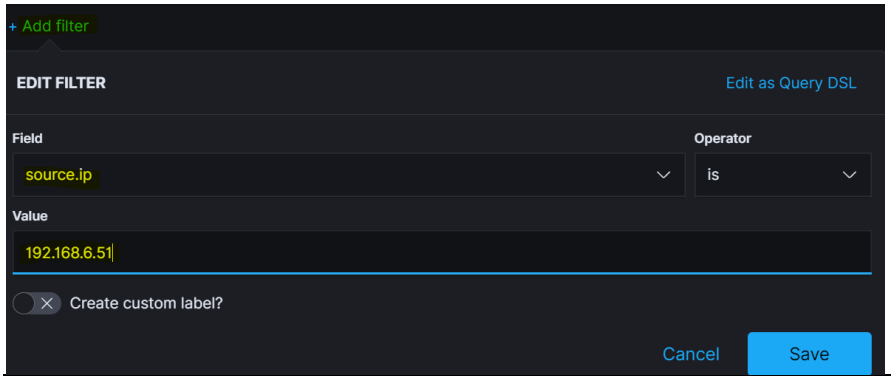
Εικόνα 121 - Security Onion Hunt (5)

Παρακάτω, απεικονίζονται κάποιοι πίνακες στην σελίδα “Dashboards” που υπάρχουν προεγκατεστημένοι στο Security Onion και μας βοηθούν να δούμε αναλυτικότερα την δικτυακή κίνηση, όσον αφορά για παράδειγμα τα alerts, τις συνδέσεις από συγκεκριμένες διευθύνσεις IP κ.ο.κ.

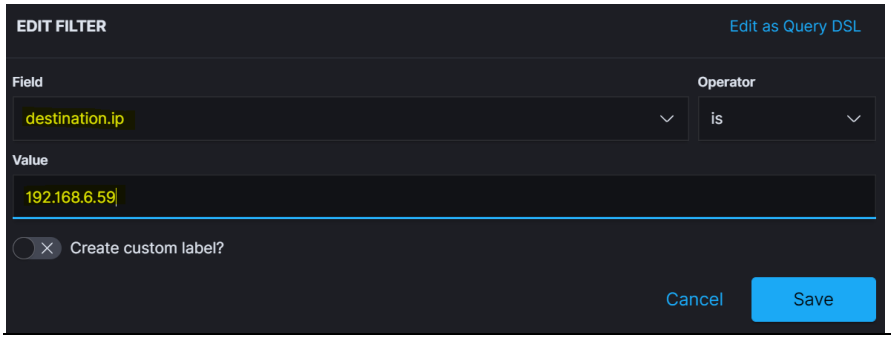


Εικόνα 122 - Security Onion Dashboards

Σε κάθε πίνακα μπορούμε να ορίσουμε ή να δημιουργήσουμε τα δικά μας φίλτρα όπως φαίνεται παρακάτω:



Εικόνα 123 - Security Onion Filtering (1)



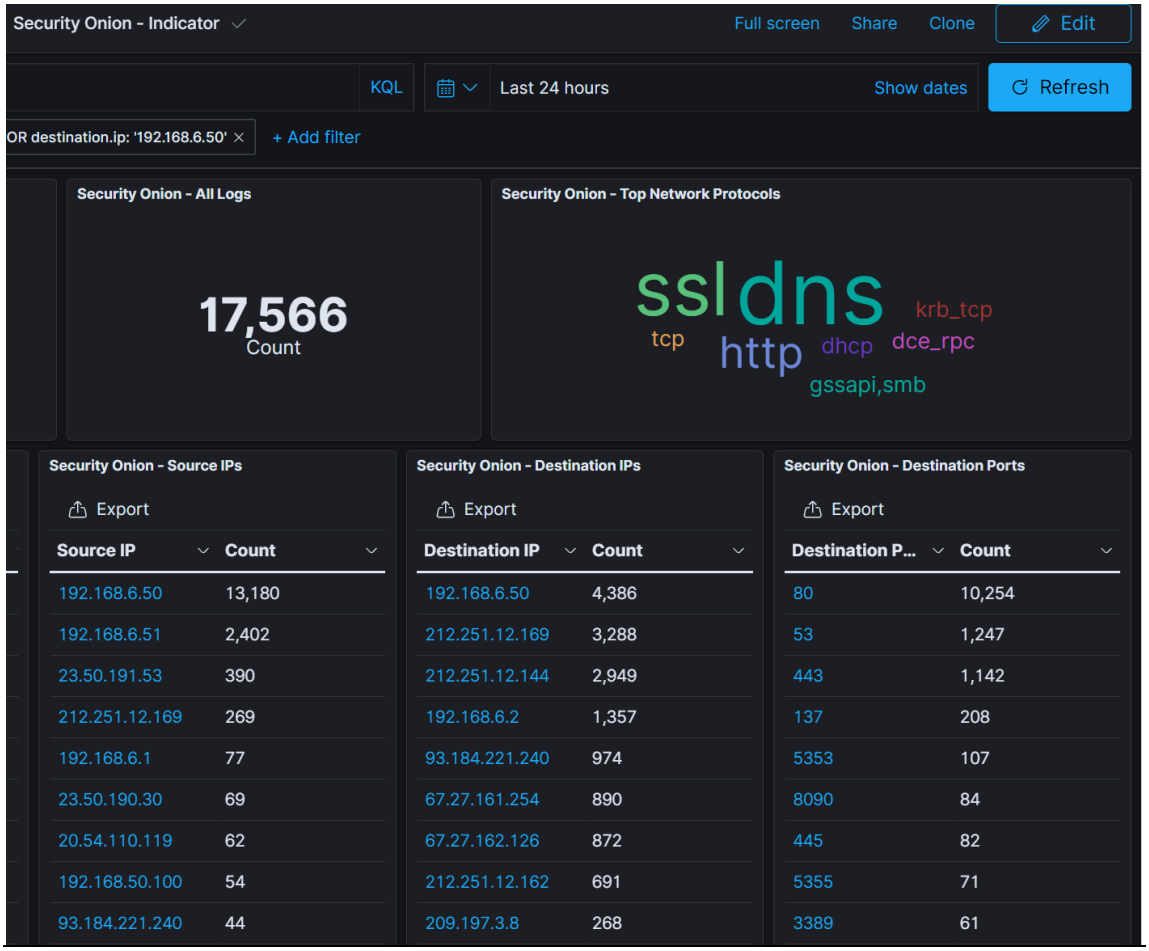
Εικόνα 124 - Security Onion Filtering (2)

Υπάρχει ακόμη και η επεξεργασία των φίλτρων μέσω query και είναι ακριβώς το φίλτρο που βάλαμε παραπάνω. Ουσιαστικά ορίσαμε να δούμε την κίνηση από το μηχάνημα των επιθέσεων προς μια συγκεκριμένη διεύθυνση IP τελικού υπολογιστή.

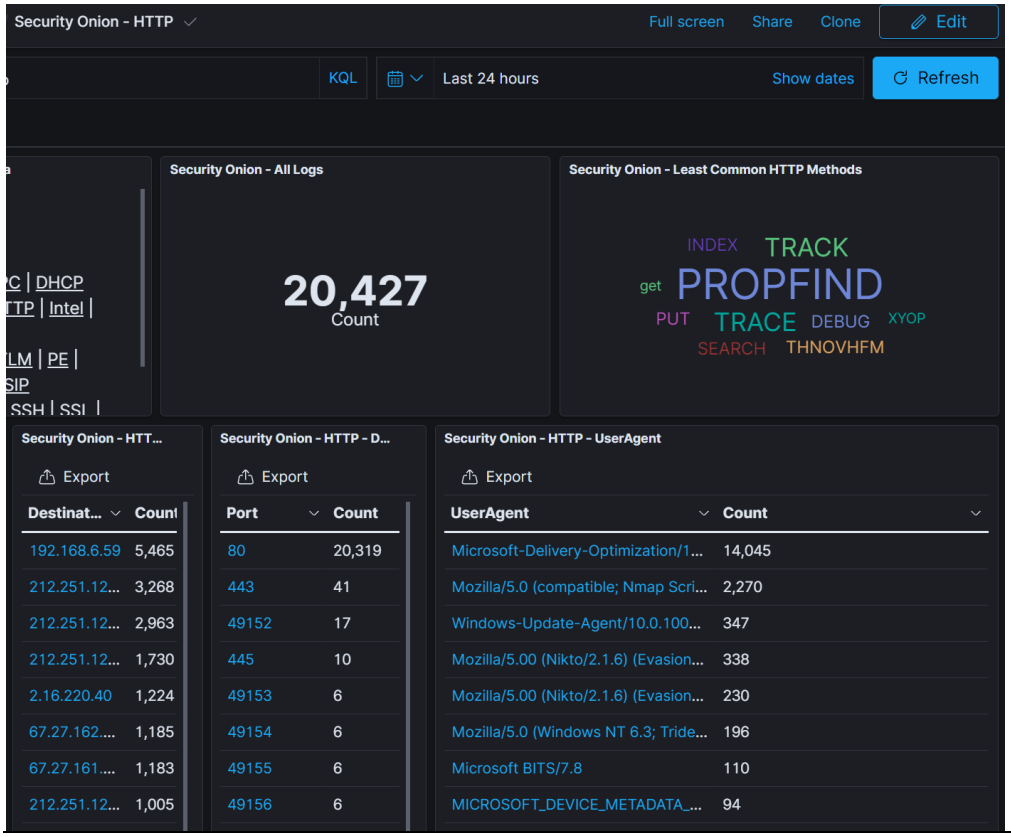
```
{
  "bool": {
    "should": [
      {
        "term": {
          "source.ip": "192.168.6.51"
        }
      },
      {
        "term": {
          "destination.ip": "192.168.6.59"
        }
      }
    ]
  }
```

```
}
```

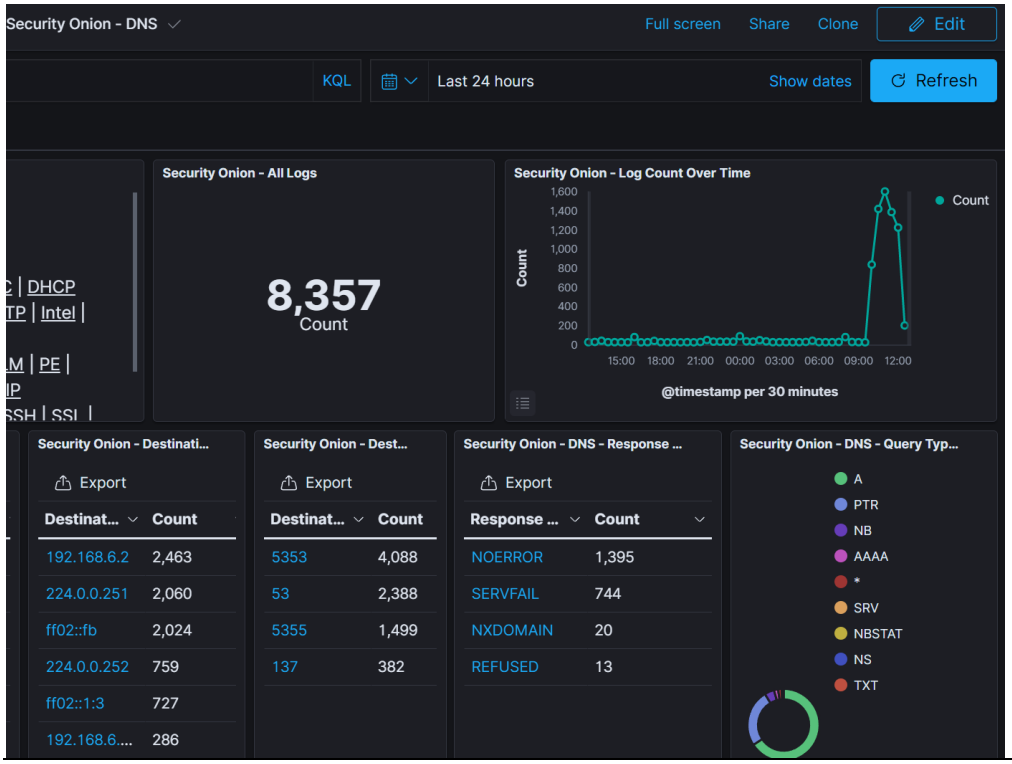
Για τις τελευταίες 24 ώρες, έχουμε τον παρακάτω πίνακα, όπου απεικονίζεται ο συνολικός αριθμός των αρχείων καταγραφής, τα δικτυακά πρωτόκολλα που χρησιμοποιήθηκαν, οι πόρτες και άλλα.



Εικόνα 125 - Security Onion Indicator



Εικόνα 126 - Security Onion HTTP Traffic



Εικόνα 127 - Security Onion DNS Traffic

Κεφάλαιο 5 – Αντιμετώπιση Κυβερνοαπειλής με χρήση του RITA

5.1 ΕΝΤΟΠΙΣΜΟΣ C&C

Μια επιτυχημένη κυβερνοεπίθεση είναι κάτι περισσότερο από το να μπει απλά ο εισβολέας στο δίκτυο του οργανισμού. Για να έχει πραγματικό όφελος θα πρέπει να διατηρήσει την πρόσβαση στα συστήματα του οργανισμού, να επικοινωνεί με άλλες συσκευές στο δίκτυο, να εκμεταλλευτεί τα ευαίσθητα δεδομένα κ.α. Για να μπορέσουμε να προστατευτούμε από τις επιθέσεις τύπου C2, θα πρέπει αρχικά να κατανοήσουμε τι είναι το C2, γνωστό και ως C&C και πως μπορεί ο οργανισμός να βρίσκει αυτά τα κρυφά κανάλια επικοινωνίας και να αμύνεται από επιθέσεις τέτοιου τύπου. [23]

Η υποδομή C2 ή C&C, είναι το σύνολο εργαλείων και τεχνικών που χρησιμοποιούν οι εισβολείς για να διατηρήσουν την επικοινωνία με παραβιασμένες συσκευές μετά την αρχική εκμετάλλευση. Οι τεχνικές και οι τακτικές διαφέρουν μεταξύ των επιθέσεων, αλλά το C2 γενικά αποτελείται από ένα ή περισσότερα κρυφά κανάλια επικοινωνίας μεταξύ των συσκευών σε μια ενιαία πλατφόρμα που ελέγχει ο εισβολέας. Αυτά τα κανάλια επικοινωνίας χρησιμοποιούνται για να εκτελέσουν κακόβουλες ενέργειες στις παραβιασμένες συσκευές, τη λήψη πρόσθετων κακόβουλων λογισμικών και τη μεταφορά των δεδομένων στον εισβολέα. [23]

Το C2 διατίθεται σε πολλές διαφορετικές μορφές και το MITRE απαριθμεί μέχρι τώρα 16 τεχνικές τύπου C2, η καθεμία με έναν αριθμό υποτεχνικών που έχουν παρατηρηθεί σε προηγούμενες επιθέσεις στον κυβερνοχώρο. Οι επιθέσεις τύπου C2 είναι δύσκολο να εντοπιστούν καθώς οι επιτιθέμενοι προσπαθούν με κάθε τρόπο να μην γίνουν αντιληπτοί από τον οργανισμό. Ωστόσο, αν η επικοινωνία αυτή γίνει αντιληπτή και διακοπεί, μπορεί να σταματήσει κάθε είδους παραβίαση που θα ακολουθούσε και να αποτρέψει την παραβίαση των δεδομένων του οργανισμού. [23]

Αρκετοί οργανισμοί διαθέτουν περιμετρική προστασία, πράγμα το οποίο καθιστά δύσκολο για έναν εισβολέα να ξεκινήσει μια σύνδεση από το διαδίκτυο προς το εσωτερικό δίκτυο του οργανισμού, χωρίς να εντοπιστεί. Ωστόσο, η εξωτερική επικοινωνία δεν παρακολουθείται ή δεν περιορίζεται τόσο συχνά. Αυτό σημαίνει πως ένα κακόβουλο λογισμικό, όπως για παράδειγμα το ηλεκτρονικό ψάρεμα (phishing) μπορεί να δημιουργήσει ένα κανάλι επικοινωνίας προς την εξερχόμενη διεύθυνση IP, η οποία θα αντιστοιχεί στην υποδομή C&C του εισβολέα.

Από τους πιο αποτελεσματικούς τρόπους για την προστασία από επιθέσεις τύπου C2, είναι ο περιορισμός και η παρακολούθηση της εξωτερικής επικοινωνίας. Για παράδειγμα, ο περιορισμός των εξερχόμενων αιτημάτων DNS μόνο σε διακομιστές που ελέγχει ο οργανισμός, μπορεί να αποτρέψει επιθέσεις τύπου DNS tunneling. Επιπλέον, αν και είναι δυσκολότερο να εντοπιστούν, τα beacons, δηλαδή η επαναλαμβανόμενη δημιουργία σύνδεσης μεταξύ 2 διευθύνσεων IP μπορεί να είναι μια ένδειξη δραστηριότητας C2. Παρακάτω, θα εγκαταστήσουμε το RITA στο Security Onion και θα χρησιμοποιήσουμε το εργαλείο σε παραδείγματα αρχείων καταγραφής για βαθύτερη ανάλυση της κίνησης του δικτύου.

5.2 ΕΓΚΑΤΑΣΤΑΣΗ ΤΟΥ RITA

Η εγκατάσταση του Security Onion περιλαμβάνει τα εργαλεία Elasticsearch, Logstash, Kibana, Suricata, Zeek, Wazuh και άλλα αρκετά εργαλεία ασφαλείας.

Στην υλοποίηση μας, θα εγκαταστήσουμε και το RITA (Real Intelligence Threat Analysis), ένα εργαλείο ανοιχτού κώδικα για την ανάλυση της κίνησης του δικτύου, που δεν είναι εγκατεστημένο από προεπιλογή. Το RITA μας βοηθά στην αναζήτηση της επαναλαμβανόμενης δημιουργίας σύνδεσης μεταξύ δύο διευθύνσεων IP εντός και εκτός του δικτύου, στην αναζήτηση των μαύρων λιστών κ.α. [5]

Η εγκατάσταση του RITA είναι απλή και γίνεται με τα παρακάτω βήματα:

Βήμα 1ο. Κατεβάζουμε το τελευταίο script εγκατάστασης και το κάνουμε εκτελέσιμο

```
[chrisgourz@securityonion ~]$ wget https://github.com/activecm/rita/releases/download/v4.4.0/install
.sh
```

Εικόνα 128 - Εγκατάσταση RITA (1)

```
[chrisgourz@securityonion ~]$ chmod +x ./install.sh
```

Εικόνα 129 - Εγκατάσταση RITA (2)

Βήμα 2ο. Εγκατάσταση του RITA, χωρίς το zeek το οποίο είναι προεγκατεστημένο

```
[chrisgourz@securityonion ~]$ sudo ./install.sh --disable-zeek
```

Εικόνα 130 - Εγκατάσταση RITA (3)

```
Brought to you by Active CounterMeasures

[-] In order to run the installer, several basic packages must be installed.
        [-] Updating packages... SUCCESS
        [-] Ensuring curl is installed... SUCCESS
        [-] Ensuring coreutils is installed... SUCCESS
        [-] Ensuring lsb-release is installed... SUCCESS
        [-] Ensuring yum-utils is installed... SUCCESS
[-] This installer will:
        [-] Install MongoDB
        [-] Update RITA at /usr/local/bin/rita
[-] Installing MongoDB... SUCCESS
[!] Starting MongoDB and enabling on startup.
[!] Starting MongoDB process completed.
[!] You can access the MongoDB shell with 'mongo'.
[!] If you need to stop MongoDB,
[!] run 'sudo systemctl stop mongod'.
[-] Sleeping to give the Mongo service some time to fully start...[-] Setting Mongo feature compatib
[-] Setting Mongo feature compatibility to 4.2... SUCCESS
[-] Installing RITA... SUCCESS
[!] /etc/rita/config.yaml may need to be updated for this version of RITA.
[!] A default config file has been created at /etc/rita/config.yaml.new.
[!] "rita test-config" may be used to troubleshoot configuration issues.

[!] To finish the installation, reload the system profile with
[!] 'source /etc/profile'.

  _ \ _ _| __ __|  \
   /   |      |   _ \
_|_\ ___|   _| _/  _\  v4.3.1

Brought to you by Active CounterMeasures

Thank you for installing RITA! Happy hunting!
[chrisgourz@securityonion ~]$ source /etc/profile
```

Εικόνα 131 - Εγκατάσταση RITA (4)

Βήμα 3ο. Βασικές εντολές χρήσης του RITA

```
$ rita h
```

```
[chrisgourz@securityonion ~]$ rita h
NAME:
   rita - Look for evil needles in big haystacks.

USAGE:
   rita [global options] command [command options] [arguments...]

VERSION:
   v4.3.1

COMMANDS:
     delete, delete-database  Delete imported database(s)
     import                   Import zeek logs into a target database
     html-report              Create an html report for an analyzed database
     show-beacons-fqdn        Print hosts which show signs of C2 software (FQDN Analysis)
     show-beacons-proxy       Print hosts which show signs of C2 software (internal -> Proxy)
     show-beacons             Print hosts which show signs of C2 software
     show-bl-hostnames        Print blacklisted hostnames which received connections
     show-bl-source-ips       Print blacklisted IPs which initiated connections
     show-bl-dest-ips         Print blacklisted IPs which received connections
     list, show-databases     Print the databases currently stored
     show-exploded-dns        Print dns analysis. Exposes covert dns channels
     show-long-connections    Print long connections and relevant information
     show-open-connections    Print open connections and relevant information
     show-strobes             Print strobe information
     show-useragents          Print user agent information
     test-config              Check the configuration file for validity
     help, h                  Shows a list of commands or help for one command

GLOBAL OPTIONS:
   --config CONFIG_FILE, -c CONFIG_FILE  Use a specific CONFIG_FILE when running this command
   --help, -h                            show help
   --version, -v                         print the version
```

Εικόνα 132 - Εγκατάσταση RITA (5)

5.3 ΧΡΗΣΗ ΤΟΥ RITA

Μετά την εγκατάσταση του RITA, θα πρέπει να ρυθμίσουμε το *InternalSubnets* από το αρχείο διαμόρφωσης /etc/rita/config.yaml

```
 GNU nano 2.3.1                File: /etc/rita/config.yaml

_ AlwaysInclude: []

  # Example: NeverInclude: ["255.255.255.255/32"]
  # This functions as a whitelisting setting, and connections involving
  # ranges entered into this section are filtered out at import time
  NeverInclude:
    - 0.0.0.0/32 # "This" Host           RFC 1122, Section 3.2.1.3
    - 127.0.0.0/8 # Loopback             RFC 1122, Section 3.2.1.3
    - 169.254.0.0/16 # Link Local          RFC 3927
    - 224.0.0.0/4 # Multicast             RFC 3171
    - 255.255.255.255/32 # Limited Broadcast     RFC 919, Section 7
    - ::1/128 # Loopback              RFC 4291, Section 2.5.3
    - fe80::/10 # Link local           RFC 4291, Section 2.5.6
    - ff00::/8 # Multicast            RFC 4291, Section 2.7

  # Example: InternalSubnets: ["10.0.0.0/8","172.16.0.0/12","192.168.0.0/16"]
  # This allows a user to identify their internal network, which will result
  # in any internal to internal and external to external connections being
  # filtered out at import time. Reasonable defaults are provided below
  # but need to be manually verified against each installation before enabling.
  InternalSubnets:
    - 10.0.0.0/8 # Private-Use Networks  RFC 1918
    - 172.16.0.0/12 # Private-Use Networks  RFC 1918
    - 192.168.0.0/16 # Private-Use Networks  RFC 1918
```

Εικόνα 133 - RITA Config

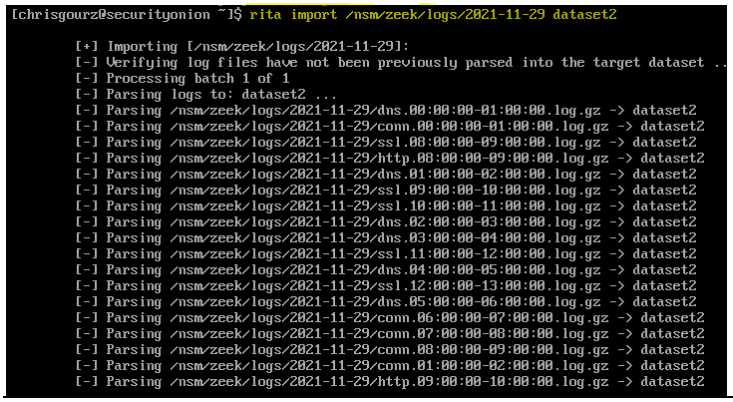
Αν το δίκτυο μας χρησιμοποιεί την διευθυνσιοδότηση τύπου RFC 1918, τότε δεν χρειάζεται να κάνουμε κάτι καθώς περιλαμβάνει από προεπιλογή τα δίκτυα αυτά.

Αφού γίνει αυτό και έχουμε στην κατοχή μας αρχεία καταγραφής μέσω του zeek, τότε είμαστε έτοιμοι να ξεκινήσουμε την αναζήτηση της απειλής.

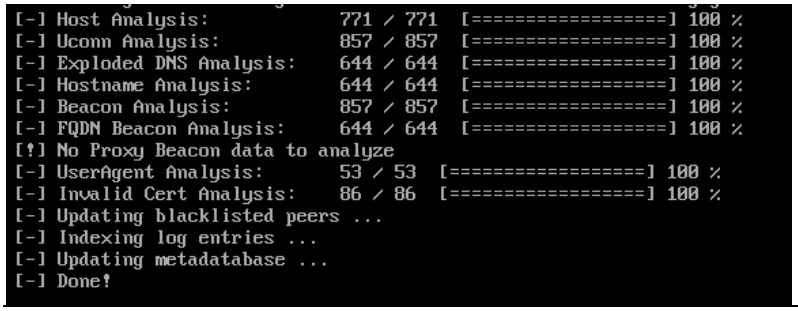
Αρχικά, θα πρέπει να εισάγουμε τα αρχεία καταγραφής που επιθυμούμε στο RITA.

Εντολή:

```
rita import path/to/your/zeek_logs dataset_name
```



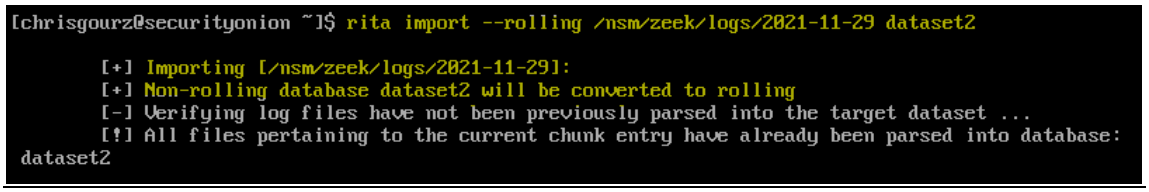
Εικόνα 134 - RITA Import



Εικόνα 135 - RITA Import (2)

Επειδή τα δεδομένα προστίθενται συνεχώς, αν θέλουμε να ενημερωθεί το ίδιο dataset τότε θα πρέπει να τρέξουμε την παρακάτω εντολή:

```
rita import --rolling /path/to/your/zeek_logs dataset_name
```



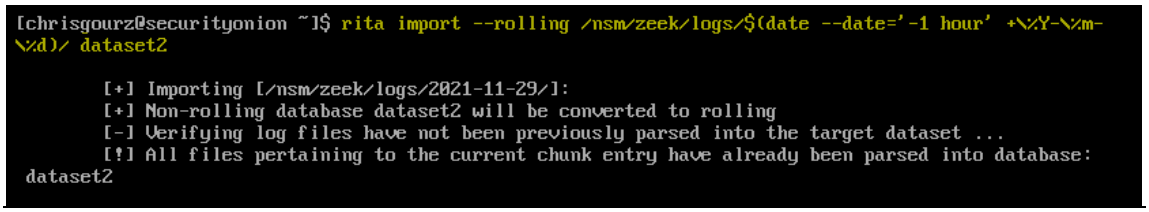
Εικόνα 136 - RITA Import (3)

Η εντολή αυτή μας επιτρέπει να αναλύουμε τα δεδομένα καταγραφής για μια συγκεκριμένη χρονική περίοδο καθώς αυτά εισέρχονται στο Security Onion. Επίσης, καθώς ολοένα και περισσότερα νέα αρχεία καταγραφής προστίθενται στην συγκεκριμένη ημερομηνία, μπορούμε να τρέχουμε την εντολή αυτή όσες φορές επιθυμούμε (για παράδειγμα ανά 1 ώρα).

Μπορούμε επίσης να έχουμε μια βάση δεδομένων η οποία θα εισάγει νέα αρχεία καταγραφής κάθε 1 ώρα και έχει πάντα αρχεία καταγραφής 24 ωρών. Τα αρχεία από το zeek αποθηκεύονται στην τοποθεσία /nsm/zeek/logs/date που σημαίνει ότι ο φάκελος αυτός θα αλλάζει κάθε ημέρα. Για να γίνει αυτό, αρκεί να τρέξουμε την παρακάτω εντολή, η οποία δημιουργεί μια προγραμματισμένη εργασία και εκτελείται κάθε 1 ώρα.

Εντολή:

```
rita import --rolling /nsm/zeek/logs/$(date --date='-1 hour' +\%Y-\%m-\%d)/ dataset_name
```



Εικόνα 137 - RITA Import (4)

Το RITA διαχωρίζει τα αρχεία καταγραφής μέσα και έξω από τις βάσεις δεδομένων σε «κομμάτια». Το κάθε «κομμάτι» αποτελεί την κάθε ώρα άρα έχουμε 24 «κομμάτια» στο χρονικό διάστημα των 24 ωρών. Αυτό μας δίνει την δυνατότητα να έχουμε πάντα διαθέσιμα τα πιο πρόσφατα δεδομένα 24 ωρών.

Με την εντολή *rita-show-databases* μπορούμε να δούμε τις βάσεις που έχουν δημιουργηθεί. Φυσικά το dataset σαν όνομα δεν είναι δεσμευτικό και μπορεί να είναι οτιδήποτε εκτός από ειδικούς χαρακτήρες και χρονική περίοδο.

Εικόνα 138 - RITA Show Databases

Οι παρακάτω εντολές μας επιτρέπουν να δούμε από μια βάση δεδομένων τις μεγάλες συνδέσεις καθώς και τα beacons που μπορεί να σχετίζονται με μια ενέργεια τύπου C2. Η παράμετρος -H εμφανίζει τα αποτελέσματα σε μορφή που μπορούν να διαβαστούν. [3][9]

```
rita show-beacons dataset_name -H | less -S
```

```
[chrisgourz@securityonion ~]$ rita show-beacons dataset2 -H | less -S
+-------+----------------+-----------------+-------------+-------------+-------------+------------+
| SCORE |   SOURCE IP    | DESTINATION IP  | CONNECTIONS | AVG  BYTES  | INTVL RANGE | SIZE RANGE |
+-------+----------------+-----------------+-------------+-------------+-------------+------------+
| 0.878 | 192.168.50.190 | 8.8.8.8         |       12870 |          88 |          35 |         68 |
| 0.837 | 172.17.0.6     | 8.8.8.8         |         386 |         108 |         599 |          0 |
| 0.836 | 192.168.50.190 | 34.120.177.193  |         192 |        2021 |         600 |         52 |
| 0.836 | 172.17.0.6     | 34.120.177.193  |         192 |        2021 |         600 |         52 |
| 0.835 | 192.168.50.199 | 204.16.253.153  |         192 |         112 |           0 |          0 |
|  0.83 | 192.168.50.199 | 40.126.31.9     |         115 |        6447 |       16588 |       4565 |
|  0.83 | 192.168.50.199 | 92.42.151.220   |          32 |        6314 |           0 |         40 |
| 0.829 | 192.168.50.199 | 65.55.252.93    |          51 |          86 |        1425 |        104 |
| 0.809 | 192.168.50.199 | 40.126.31.140   |          95 |        6329 |       15277 |       3506 |
| 0.794 | 192.168.50.190 | 193.239.214.226 |          57 |          73 |         522 |          0 |
| 0.788 | 192.168.50.190 | 176.119.210.243 |          61 |          76 |         532 |          0 |
| 0.773 | 192.168.50.190 | 50.205.244.113  |          55 |          76 |          20 |          0 |
| 0.766 | 192.168.6.52   | 209.197.3.8     |          51 |       94025 |         230 |       3942 |
| 0.724 | 192.168.6.59   | 20.73.128.142   |          24 |       10485 |           7 |        256 |
```

Εικόνα 139 - RITA Show Beacons

```
rita show-long-connections dataset_name -H | less -S
```

```
[chrisgourz@securityonion ~]$ rita show-long-connections dataset2 -H | less -S
+----------------+-----------------+-------------------------------+------------------+--------+
|   SOURCE IP    | DESTINATION IP  |     PORT:PROTOCOL:SERVICE     |     DURATION     | STATE  |
+----------------+-----------------+-------------------------------+------------------+--------+
| 192.168.50.199 | 35.190.242.135  | 4070:tcp:-                    | 1d21h30m11.9169s | closed |
| 192.168.50.199 | 35.186.224.45   | 443:tcp:ssl                   | 1d21h30m10.5879s | closed |
| 192.168.50.199 | 35.186.224.47   | 443:tcp:ssl                   | 1d17h22m50.562s  | closed |
| 192.168.50.199 | 34.76.0.142     | 443:tcp:ssl                   | 11h25m39.5329s   | closed |
| 192.168.50.199 | 35.236.238.213  | 443:tcp:ssl                   | 6h49m43.4478s    | closed |
| 192.168.50.199 | 44.233.180.72   | 443:tcp:ssl                   | 3h18m51.1628s    | closed |
| 192.168.6.51   | 44.233.180.72   | 443:tcp:- 443:tcp:ssl         | 3h5m9.5439s      | closed |
| 192.168.50.199 | 35.186.224.25   | 443:tcp:ssl                   | 1h4m0.0276s      | closed |
| 192.168.50.199 | 8.8.8.8         | 53:udp:dns 443:tcp:ssl        | 1h2m18.8599s     | closed |
|                |                 | 443:udp:-                     |                  |        |
```

Εικόνα 140 - RITA Show Long Connections

Η εντολή *rita-html-report* μας δημιουργεί τα αρχεία καταγραφής σε μορφή html για τις βάσεις δεδομένων που έχουμε.

```
[chrisgourz@securityonion ~]$ rita html-report
[-] Writing: /home/chrisgourz/rita-html-report1/dataset1
[-] Writing: /home/chrisgourz/rita-html-report1/dataset2
```

Εικόνα 141 - RITA HTML Report

Σε μορφή HTML, παίρνουμε όλα τα αποτελέσματα της βάσης και φαίνονται όπως παρακάτω:

RITA | Viewing: dataset2 | Beacons | Beacons FQDN | Beacons Proxy | Strobes | DNS | BL Source IPs | BL Dest. IPs

BL Hostnames | Long Connections | User Agents | RITA on

Source	Destination	DstPort:Protocol:Service	Duration
192.168.50.199	35.190.242.135	4070:tcp:-	163811.9169
192.168.50.199	35.186.224.45	443:tcp:ssl	163810.5879
192.168.50.199	35.186.224.47	443:tcp:ssl	148970.562
192.168.50.199	34.76.0.142	443:tcp:ssl	41139.5329
192.168.50.199	35.236.238.213	443:tcp:ssl	24583.4478
192.168.50.199	44.233.180.72	443:tcp:ssl	11931.1628
192.168.6.51	44.233.180.72	443:tcp:ssl, 443:tcp:-	11109.5439
192.168.50.199	35.186.224.25	443:tcp:ssl	3840.0276
192.168.50.199	8.8.8.8	443:tcp:ssl, 443:udp:-, 53:udp:dns	3738.8599

Εικόνα 142 - RITA HTML Report (2)

Σε ένα ειδικά διαμορφωμένο μηχάνημα για την αναζήτηση της απειλής, θα δούμε την συμπεριφορά από μια συγκεκριμένη διεύθυνση IP, που ανήκει σε ένα Windows μηχάνημα του δικτύου μας. [4]

```
thunt@thunt:~/chrisgourzlab$ cat conn.log | zeek-cut id.orig_h id.resp_h duration | sort -k 3 -nr |
head
192.168.6.59    167.71.97.235   86389.659357
192.168.6.59    104.248.234.238 243.768999
192.168.6.59    104.118.9.117   166.139547
192.168.6.59    72.21.91.29     134.888177
192.168.6.59    52.184.216.246  129.075227
192.168.6.59    52.167.249.196  128.957107
192.168.6.59    52.184.216.246  128.481757
192.168.6.59    13.107.5.88     128.346889
192.168.6.59    52.179.219.14   128.116421
192.168.6.59    13.107.5.88     128.042647
```

Εικόνα 143 - RITA Analysis (1)

Το *id.orig_h* αντιστοιχεί στην διεύθυνση Source IP, το *id.resp_h* στην Destination IP και το duration, το χρονικό διάστημα που πέρασε μεταξύ του πρώτου και του τελευταίου πακέτου σε μια περίοδο λειτουργίας. Στόχος είναι να προσδιορίσουμε ποια από τα εσωτερικά μας συστήματα επικοινωνούν περισσότερο με εξωτερικές διευθύνσεις IP. Το πεδίο "duration" θα μας βοηθήσει να αναγνωρίσουμε αυτές τις περιόδους σύνδεσης. Επειδή όμως μπορεί να υπάρχουν πολλά δεδομένα, είναι δύσκολο να γίνει άμεσα. Με την παράμετρο zeek-cut μπορούμε να προσδιορίσουμε μόνο τα συγκεκριμένα πεδία με τα οποία θέλουμε να εργαστούμε. [3]

Το αποτέλεσμα της zeek-cut είναι σχεδόν αυτό που χρειαζόμαστε, όμως μας λείπει κάποια ταξινόμηση σε αυτά. Θα ήταν ιδιαίτερα χρήσιμο, αν είχαμε τις μεγαλύτερες συνδέσεις πάνω ώστε να μπορούμε να επικεντρωθούμε ακριβώς σε αυτές. Αυτό μπορεί να πραγματοποιηθεί με την παρακάτω εντολή: [4]

```
thunt@thunt:~/chrisgourzlab$ cat conn.log | zeek-cut id.orig_h id.resp_h duration | sort | grep -v -
e '^$' | grep -v '-' | datamash -g 1,2 sum 3 | sort -k 3 -rn | head
192.168.6.59    167.71.97.235   86389.659357
192.168.6.59    52.179.219.14   4067.394413
192.168.6.59    52.184.217.56   2936.172839
192.168.6.59    52.184.216.246  2825.858
```

Εικόνα 144 - RITA Analysis (2)

Η παράμετρος *-k 3* μας βοηθά ώστε να εμφανιστούν τα αποτελέσματα με βάση την τρίτη στήλη που είναι και το χρονικό διάστημα, η παράμετρος *-r* σημαίνει να ταξινομηθούν με αντίστροφη σειρά (από το μεγαλύτερο προς το μικρότερο) και η παράμετρος *-n* σημαίνει ότι τα περιεχόμενα της στήλης αυτής είναι αριθμητικές τιμές. Τέλος, η παράμετρος *datamash -g* αφορά ένα εργαλείο το οποίο μας βοηθά να αθροίσουμε το συνολικό χρονικό διάστημα σε περίπτωση που υπάρχει ίδια σύνδεση μεταξύ Source και Destination IP σε παραπάνω από 1 γραμμές. Το datamash είναι ένα αρκετά βοηθητικό εργαλείο το οποίο δεν υπάρχει προεγκατεστημένο στο Linux και μας βοηθά αν θέλουμε να ανιχνεύσουμε για παράδειγμα επιθέσεις τύπου RAT (Remote Access Trojan), που σκοπός του είναι να κρατά την σύνδεση ανοιχτή για 1 ώρα, να τερματίζει την σύνδεση και να ανοίγει μια νέα. [4]

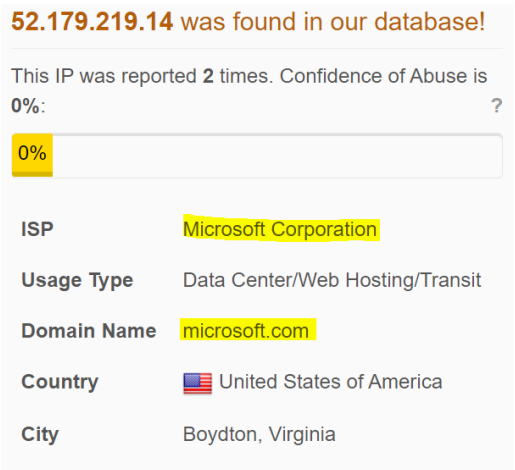
Παρακάτω, θα δούμε περισσότερες πληροφορίες σχετικά με τις 2 διευθύνσεις IP που έχουν την μεγαλύτερη χρονική διάρκεια σε δευτερόλεπτα.

```
thunt@thunt:~/chrisgourzlab$ host 167.71.97.235
235.97.71.167.in-addr.arpa domain name pointer demo1.aihhosted.com.
thunt@thunt:~/chrisgourzlab$ host 52.179.219.14
Host 14.219.179.52.in-addr.arpa. not found: 3(NXDOMAIN)
```

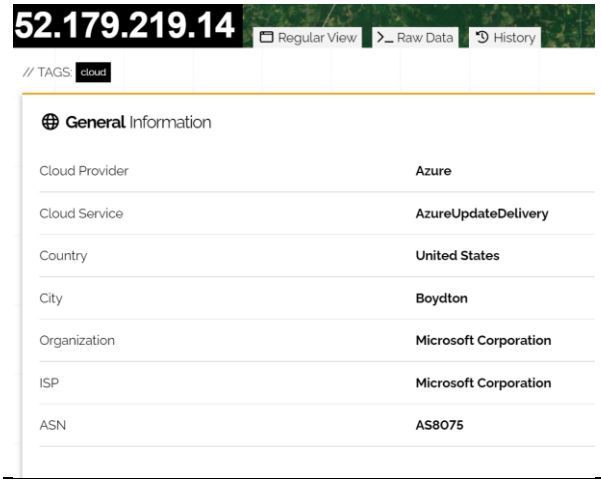
Εικόνα 145 - RITA Analysis (3)

Η διεύθυνση *167.71.97.235* που πραγματοποιήθηκε από το Windows μηχάνημα μας με *Source IP: 192.168.6.59* απαντάει στο demo1.aihhosted.com και έχει διάρκεια 86389.65 δευτερόλεπτα, πράγμα που σημαίνει πως η σύνδεση έγινε για σχεδόν 1 ημέρα (86400 δευτερόλεπτα). Θα πρέπει να εξετάσουμε αν υπάρχει πράγματι η ανάγκη αυτή, αν όχι, θα πρέπει να το εξετάσουμε περεταίρω.

Η διεύθυνση *52.179.219.14* δεν μας δίνει αποτελέσματα, άρα θα πρέπει να την εξετάσουμε περεταίρω.



Εικόνα 146 - IP Check (1)



Εικόνα 147 - IP Check (2)

Βλέπουμε πως η συγκεκριμένη διεύθυνση IP ανήκει στην Microsoft, όμως χρειαζόμαστε περισσότερες πληροφορίες.

IP WHOIS

Property	Value
Location	Wilmington, United States
Country	United States

REVERSE DNS

Domain	Date
array503.prod.do.dsp.mp.microsoft.com	2021-11-29
52.179.219.14	2021-10-12
array503-prod.do.dsp.mp.microsoft.com	2021-08-28
geo-prod.do.dsp.mp.microsoft.com	2021-03-16
dbk2gusuwcoxoqjmsyhz2m3zfacameap.qw776iawpez267udlbikkahi5yivxqkc.1.0.od6u6m3cwr	2021-02-05
etclpbjw6fdjpulrfarjm4vxsjkpxr46.kzfhjer7xzp7voaycava.1.0.ozlnabtsgij2f5y455ywbx	2020-12-18
geo.prod.do.dsp.mp.microsoft.com	2020-12-18
orgeover-prod.do.dsp.mp.microsoft.com	2020-12-12
geo-prod.dodsp.mp.microsoft.com.nsatc.net	2020-09-23
sbzurncdc4clwz5.eastus2.atlas.cloudapp.azure.com	2020-05-29
runnercitus-eastus2-a149423e-0.postgres.database.azure.com	2020-05-16

Εικόνα 148 - IP Check (3)

Πράγματι, σε περεταίρω έλεγχο της συγκεκριμένης IP, φαίνεται πως ανήκει στην Microsoft και μάλιστα η πρώτη φορά που βρέθηκε είναι στις 16-05-2020.

Μπορούμε επίσης να τρέξουμε τις παρακάτω εντολές, χρήσιμες για μια συγκεκριμένη διεύθυνση IP για να δούμε περισσότερες πληροφορίες:

```
thunt@thunt:~/chrisgourzlab$ cat dns.log | zeek-cut query answers | grep 52.179.219.14 | sort | uniq
 -c
     26 array503.prod.do.dsp.mp.microsoft.com   52.179.219.14
thunt@thunt:~/chrisgourzlab$ cat conn.log | zeek-cut id.orig_h id.resp_h service | grep 52.179.219.1
4 | sort | uniq -c
     38 192.168.6.59    52.179.219.14   ssl
thunt@thunt:~/chrisgourzlab$ cat ssl.log | zeek-cut id.resp_h server_name subject | grep 52.179.219.
14 | sort | uniq -c
     38 52.179.219.14   array503.prod.do.dsp.mp.microsoft.com   CN=*.prod.do.dsp.mp.microsoft.com,OU
=DSP,O=Microsoft,L=Redmond,ST=WA,C=US
```

Εικόνα 149 - IP Check with Zeek (1)

Δεδομένου πως και οι 2 διευθύνσεις IP που ελέγξαμε είναι ασφαλής, θα πρέπει να τις ορίσουμε σε μια whitelist ώστε να εξαιρεθούν από μελλοντικές αναζητήσεις κυβερνοαπειλών.

```
thunt@thunt:~/chrisgourzlab$ cat > excludeips.txt << EOF
> 167.71.97.235
> 52.179.219.14
> EOF
thunt@thunt:~/chrisgourzlab$ cat excludeips.txt
167.71.97.235
52.179.219.14
```

Εικόνα 150 - RITA exclude IPs from analysis (1)

Και άρα σε επόμενο έλεγχο για beacons μπορούμε να ορίσουμε αυτό το αρχείο, ώστε να εξαιρέσει αυτές τις IP με την εντολή:

```
 rita show-beacons database_name | grep -v -w -F -f filewithIPs.txt
thunt@thunt:~$ rita show-beacons chrisgourzlab | grep -v -w -F -f excludeips.txt
```

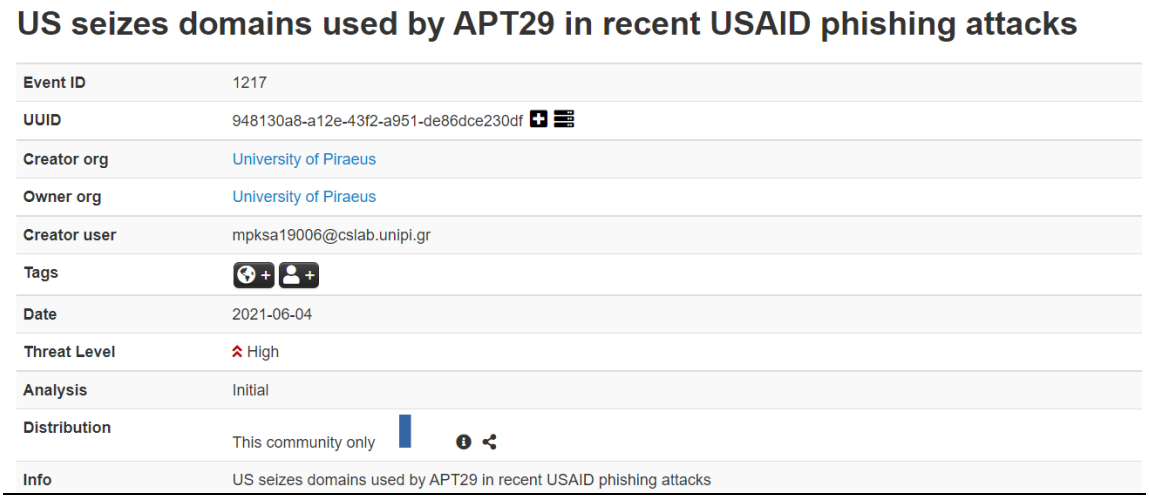
Εικόνα 151 - RITA exclude IPs from analysis (2)

Οι συνδέσεις που παραμένουν ανοιχτές για παρατεταμένες χρονικές περιόδους μπορεί να είναι ενδιαφέρουσες από την πλευρά της ασφάλειας λόγω του ότι μπορεί να αποτελούν ένδειξη δραστηριότητας τύπου C2. Ο συνδυασμός του RITA μαζί με το Zeek και άλλα εργαλεία όπως το Security Onion, μπορεί να βελτιώσει σημαντικά την ικανότητα της ανάλυσης του αριθμού των συνδέσεων, το μήκος καθώς και την διάρκεια τους. Παρόλο που το πεδίο της κυβερνοασφάλειας αλλάζει συνεχώς, είναι σημαντικά στοιχεία που θα μας βοηθήσουν στην προληπτική αναζήτηση της απειλής, τόσο στο παρόν όσο και στο μέλλον.

Κεφάλαιο 6 – Ανάλυση Αποτελεσμάτων - Δοκιμών

Στο κεφάλαιο αυτό θα δούμε τα αποτελέσματα από τις δοκιμές που έγιναν στα συστήματα της υποδομής, χρησιμοποιώντας τις πληροφορίες που έχουμε συνδυαστικά από τα εργαλεία συλλογής πληροφοριών και παρακολούθησης αυτών μέσα από τις πλατφόρμες MISP, Minemeld και Security Onion.

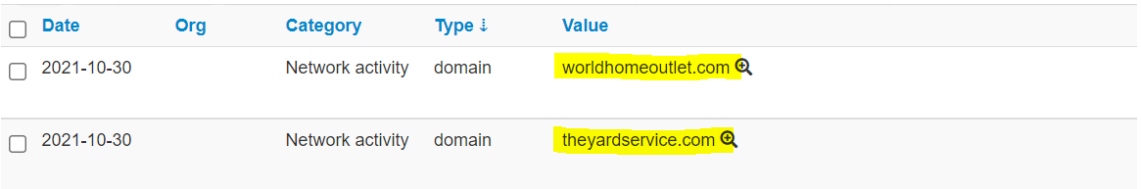
Υπόθεση - Ανάλυση της επίθεσης μέσω phishing email – **MISP ID #1217**



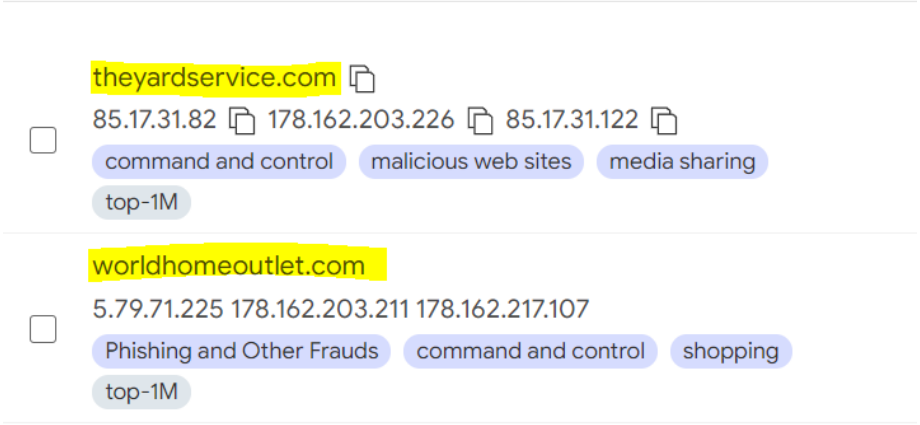
Εικόνα 152 - USAID Analysis #1

Η συγκεκριμένη επίθεση αφορά καμπάνια phishing που υποδύεται τον Οργανισμό Διεθνούς Ανάπτυξης των ΗΠΑ (USAID) για τη διανομή κακόβουλου λογισμικού και την πρόσβαση σε εσωτερικά δίκτυα.

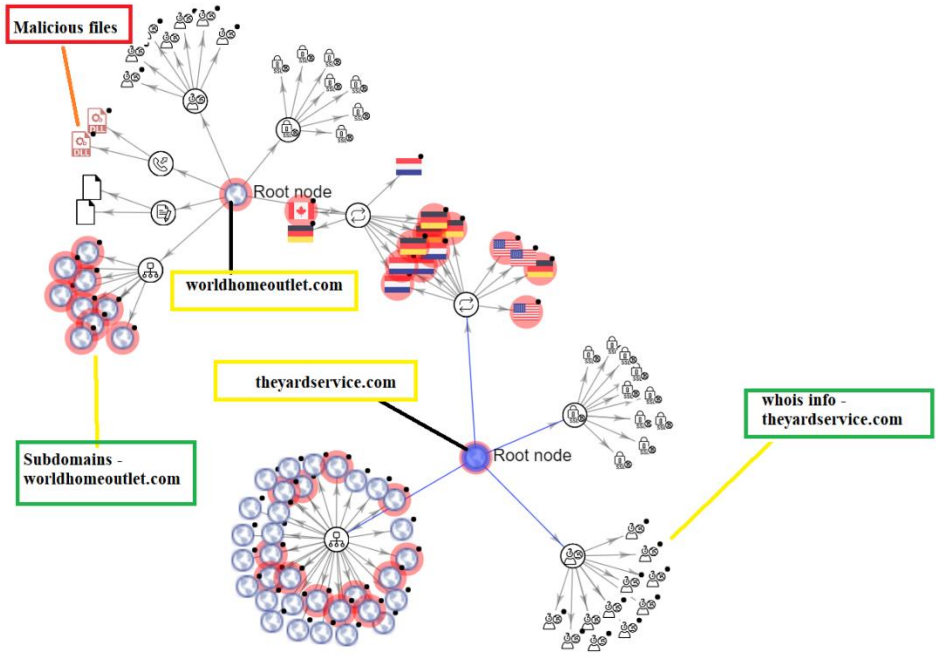
Οι δύο τομείς που κατασχέθηκαν από το Υπουργείο Δικαιοσύνης είναι τα *theyardservice.com* και *worldhomeoutlet.com* και χρησιμοποιήθηκαν για τη λήψη δεδομένων που προέρχονται από τα θύματα των στοχευμένων επιθέσεων phishing και την αποστολή περαιτέρω εντολών κακόβουλου λογισμικού για εκτέλεση σε παραβιασμένα μηχανήματα.



Εικόνα 153 - USAID Analysis #2



Περισσότερες πληροφορίες, μπορούμε να πάρουμε με την βοήθεια γραφήματος, που χωρίζονται όλα τα σημαντικά στοιχεία που έχουν να κάνουν με τα 2 domains αυτά.



Σε περαιτέρω αναζήτηση της συγκεκριμένης επίθεσης, η Microsoft αποκάλυψε ότι διεξήχθησαν από μια ομάδα hacking που συνδέεται με το ρωσικό κράτος, γνωστή ως NOBELIUM (APT29, Cozy Bear και The Dukes).

Με την βοήθεια του MITRE ATT&CK που είδαμε σε προηγούμενο κεφάλαιο, μπορούμε να δούμε περισσότερες πληροφορίες για την ομάδα αυτή. Αυτή η ομάδα πιστεύεται ότι συνδέεται με τη Ρωσική Υπηρεσία Εξωτερικών Πληροφοριών.

Home > Groups > APT29

APT29

APT29 is threat group that has been attributed to Russia's Foreign Intelligence Service (SVR).[1][2] They have operated since at least 2008, often targeting government networks in Europe and NATO member countries, research institutes, and think tanks. APT29 reportedly compromised the Democratic National Committee starting in the summer of 2015.[3][4][5][6]

In April 2021, the US and UK governments attributed the SolarWinds supply chain compromise cyber operation to the SVR; public statements included citations to APT29, Cozy Bear, and The Dukes.[7][8] Victims of this campaign included government, consulting, technology, telecom, and other organizations in North America, Europe, Asia, and the Middle East. Industry reporting referred to the actors involved in this campaign as UNC2452, NOBELIUM, StellarParticle, and Dark Halo.[9][10][11][12][13]

Εικόνα 154 - APT29 - MITRE ATT&CK

ID: G0016

Associated Groups: NobleBaron, Dark Halo, StellarParticle, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear, CozyDuke

Contributors: Daniyal Naeem, BT Security; Matt Brenton, Zurich Insurance Group; Katie Nickels, Red Canary

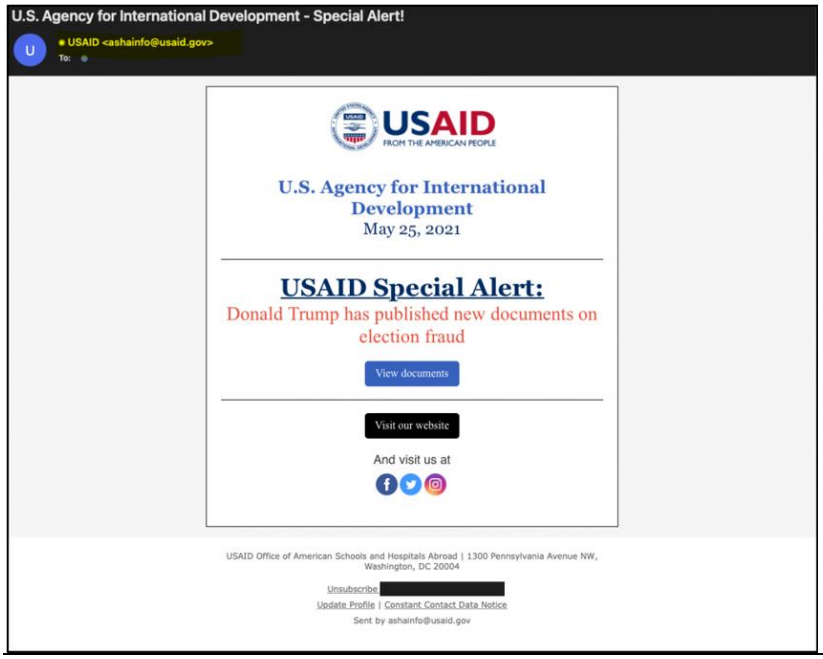
Version: 2.1

Created: 31 May 2017

Last Modified: 16 October 2021

Εικόνα 155 - APT29 - MITRE ATT&CK (2)

Το e-mail που είχε σταλεί φαίνεται στην παρακάτω εικόνα:



Εικόνα 156 - USAID Phishing email

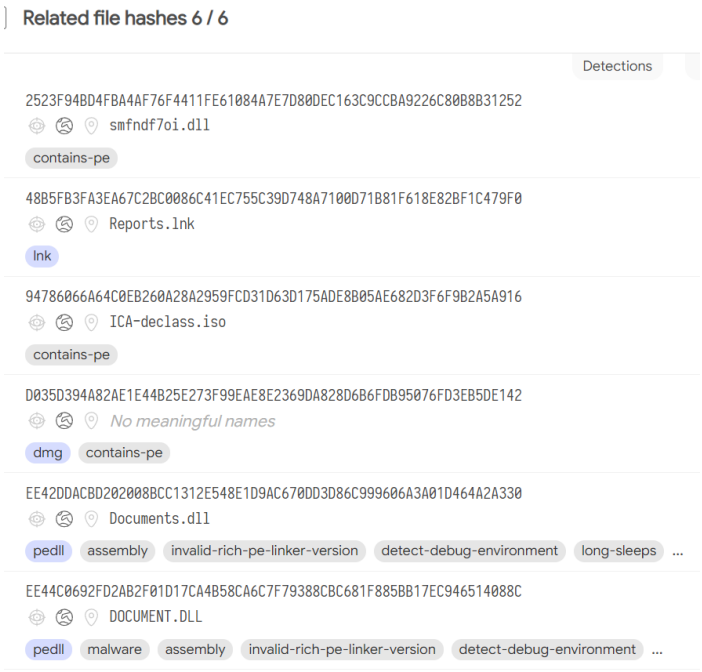
Πράγματι, αν παρατηρήσουμε στην πλατφόρμα του MISP βλέπουμε πως το e-mail αυτό αποστέλλεται από την διεύθυνση που αναφέρεται.

Εικόνα 157 - USAID Phishing email sender

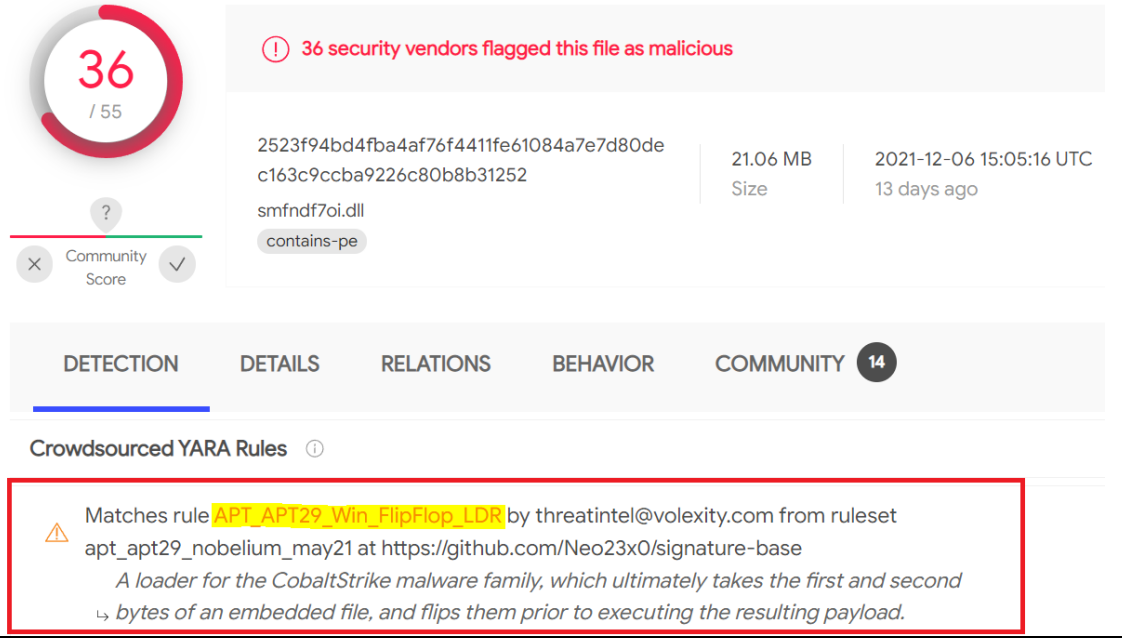
Με τις πληροφορίες που έχουμε στο MISP και τα IOCs τα οποία αναρτήθηκαν στο διαδίκτυο, μπορούμε να δούμε και την συσχέτιση που έχει με άλλα λογισμικά ή αρχεία.

Category	Type	Value
Payload Delivery	sha256	2523f94bd4fba4af76f4411fe61084a7e7d80dec163c9ccba9226c80b8b31252
Payload Delivery	sha256	d035d394a82ae1e44b25e273f99eae8e2369da828d6b6fdb95076fd3eb5de142
Payload Delivery	sha256	94786066a64c0eb260a28a2959fcd31d63d175ade8b05ae682d3f6f9b2a5a916
Payload Delivery	sha256	48b5fb3fa3ea67c2bc0086c41ec755c39d748a7100d71b81f618e82bf1c479f0
Payload Delivery	sha256	ee44c0692fd2ab2f01d17ca4b58ca6c7f79388cbc681f885bb17ec946514088c
Payload Delivery	sha256	ee42ddacbd202008bcc1312e548e1d9ac670dd3d86c999606a3a01d464a2a330

Με την βοήθεια του virustotal, μπορούμε να αναλύσουμε τις τιμές κατακερματισμού (hash values) ώστε να δούμε περισσότερες πληροφορίες.



Εικόνα 158 - VirusTotal Related Hashes



Εικόνα 159 - VirusTotal APT29 Detection

Ο κανόνας που συσχέτισε το αρχείο αυτό με την επίθεση της ομάδας αυτής:

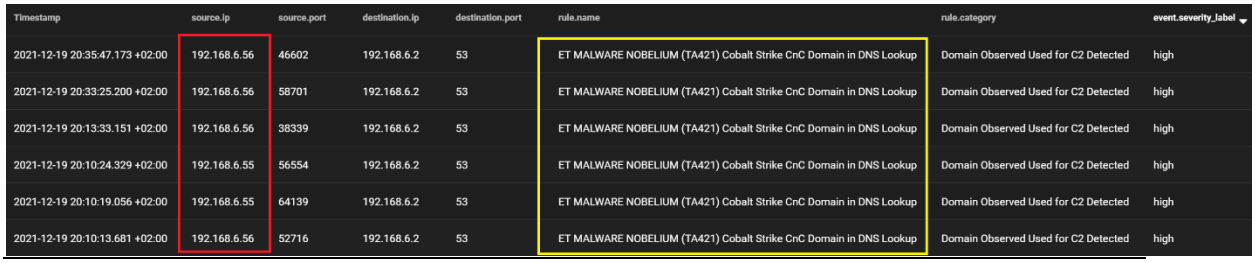
```
rule APT_APT29_NOBELIUM_Stageless_Loader_May21_2 {
  meta:
    description = "Detects stageless loader as used by APT29 / NOBELIUM"
    author = "Florian Roth"
    reference = "https://www.microsoft.com/security/blog/2021/05/28/breaking-down-
nobeliums-latest-early-stage-toolset/"
    date = "2021-05-29"
    hash1 = "a4f1f09a2b9bc87de90891da6c0fca28e2f88fd67034648060cef9862af9a3bf"
    hash2 = "c4ff632696ec6e406388e1d42421b3cd3b5f79dcb2df67e2022d961d5f5a9e78"
  strings:
    $x1 = "DLL_stageless.dll" ascii fullword

    $s1 = "c:\\users\\devuser\\documents" ascii fullword nocase
    $s2 = "VisualServiceComponent" ascii fullword
    $s3 = "CheckUpdteFrameJavaCurrentVersion" ascii fullword

    $op1 = { a3 d? 6? 04 10 ff d6 33 05 00 ?0 0? 10 68 d8 d4 00 10 57 a3 d? 6? 04 10 ff d6 33
05 00 ?0 0? 10 }
    $op2 = { ff d6 33 05 00 ?0 0? 10 68 d8 d4 00 10 57 a3 d? 6? 04 10 ff d6 33 05 00 ?0 0? 10
68 e8 d4 00 10 }
  condition:
    uint16(0) == 0x5a4d and
    filesize < 900KB and
    2 of them or 3 of them
}
```

Εντοπισμός σχετικής κίνησης μέσα από το SecurityOnion:

Εικόνα 160 - Security Onion - NOBELIUM Detection (1)

Οι πληροφορίες που μας δίνονται αρχικά είναι ότι πρόκειται για κακόβουλο λογισμικό, αναγνωρισμένο από το APT GROUP Nobelium. Επιπλέον, μας δίνεται η πληροφορία ότι πρόκειται για το framework Cobalt Strike το οποίο χρησιμοποιούν οι κακόβουλοι για τις διάφορες ενέργειες τους.

Με όλα τα στοιχεία τα οποία έχουμε συλλέξει και βλέποντας ένα τέτοιο alert, το μόνο σίγουρο είναι ότι θα πρέπει να το εξετάσουμε παραπάνω. Η συγκεκριμένη επίθεση αφορά όπως είπαμε phishing attack, που σημαίνει ότι θα ψάξουμε για αρχεία/URLS τα οποία μπορεί να σχετίζονται με την επίθεση αυτή.



Timestamp	source.ip	source.port	destination.ip	destination.port	rule.name	rule.category	event.severity_label
2021-12-19 20:35:47.173 +02:00	192.168.6.56	46602	192.168.6.2	53	ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup	Domain Observed Used for C2 Detected	high
2021-12-19 20:33:25.200 +02:00	192.168.6.56	58701	192.168.6.2	53	ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup	Domain Observed Used for C2 Detected	high
2021-12-19 20:13:33.151 +02:00	192.168.6.56	38339	192.168.6.2	53	ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup	Domain Observed Used for C2 Detected	high
2021-12-19 20:10:24.329 +02:00	192.168.6.55	56554	192.168.6.2	53	ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup	Domain Observed Used for C2 Detected	high
2021-12-19 20:10:19.056 +02:00	192.168.6.55	64139	192.168.6.2	53	ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup	Domain Observed Used for C2 Detected	high
2021-12-19 20:10:13.681 +02:00	192.168.6.56	52716	192.168.6.2	53	ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup	Domain Observed Used for C2 Detected	high

Εικόνα 161 - Security Onion - NOBELIUM Detection (2)

Το μήνυμα που παίρνουμε για το συγκεκριμένο alert φαίνεται παρακάτω:

{"timestamp":"2021-12-19T18:35:47.173846+0000","flow_id":1690451807807254,"in_iface":"bond0","event_type":"alert","src_ip":"192.168.6.56","src_port":46602,"dest_ip":"192.168.6.2","dest_port":53,"proto":"UDP","community_id":"1:BTLOz7TOtoFTQ7C4tRfJFd88N08=","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":2033051,"rev":1,"signature":"ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup","category":"Domain Observed Used for C2 Detected","severity":1,"metadata":{"affected_product":["Windows_XP_Vista_7_8_10_Server_32_64_Bit"],"attack_target":["Client_Endpoint"],"created_at":["2021_05_28"],"deployment":["Perimeter"],"former_category":["MALWARE"],"malware_family":["Cobalt_Strike"],"performance_impact":["Low"],"signature_severity":["Major"],"updated_at":["2021_05_28"]},"rule":"alert dns $HOME_NET any -> any any (msg:\"ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup\"; dns.query; dotprefix; content:\".worldhomeoutlet.com\"; nocase; endswith; reference:url,www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/; classtype:domain-c2; sid:2033051; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2021_05_28, deployment Perimeter, former_category MALWARE, malware_family Cobalt_Strike, performance_impact Low, signature_severity Major, updated_at 2021_05_28;)"},"app_proto":"dns","payload_printable":"d.....worldhomeoutlet.com.....","stream":0,"packet":"AFBW8o9mAAwpvHI+CABFAABBhfVAAEARJyzAqAY4wKgGArYKADUALdalZNkBAAABAAAAAAAAD3dvcmxkaG9tZW91dGxldANjb20AAAEAAQ==","packet_info":{"linktype":1}}

{"timestamp":"2021-12-19T18:33:25.200908+0000","flow_id":1895564404134092,"in_iface":"bond0","event_type":"alert","src_ip":"192.168.6.56","src_port":58701,"dest_ip":"192.168.6.2","dest_port":53,"proto":"UDP","community_id":"1:oxvUAv6pknmd3U1qnMwJgSA3IWk=","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":2033050,"rev":1,"signature":"ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup","category":"Domain Observed Used for C2 Detected","severity":1,"metadata":{"affected_product":["Windows_XP_Vista_7_8_10_Server_32_64_Bit"],"attack_target":["Client_Endpoint"],"created_at":["2021_05_28"],"deploym

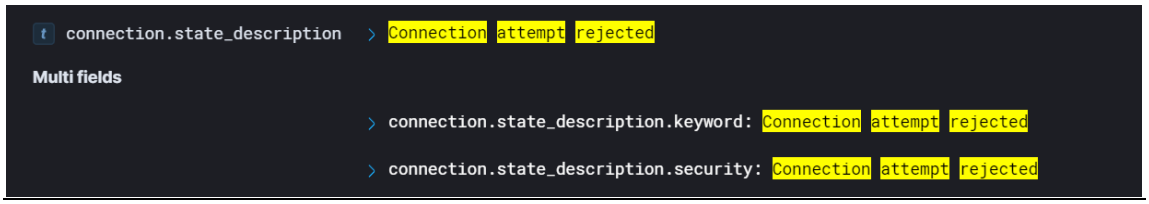
ent":["Perimeter"],"former_category":["MALWARE"],"malware_family":["Cobalt_Strike"],"performance_impact":["Low"],"signature_severity":["Major"],"updated_at":["2021_05_28"]},"rule":"alert dns $HOME_NET any -> any any (msg:\"ET MALWARE NOBELIUM (TA421) Cobalt Strike CnC Domain in DNS Lookup\"; dns.query; dotprefix; content:\".theyardservice.com\"; nocase; endswith; reference:url,www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/; classtype:domain-c2; sid:2033050; rev:1; metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, created_at 2021_05_28, deployment Perimeter, former_category MALWARE, malware_family Cobalt_Strike, performance_impact Low, signature_severity Major, updated_at 2021_05_28;)"},"app_proto":"dns","payload_printable":"{.....theyardservice.com.....","stream":0,"packet":"AFBW8o9mAAwpvHI+CABFAABARAlAAEARaRnAqAY4wKgGAuVNADUALCive4QBAAABAAAAAAAADnRoZXlhcmRzZXJ2aWNlA2NvbQAAAQAB","packet_info":{"linktype":1}}

Οι πληροφορίες που παίρνουμε από τα παραπάνω alerts είναι ότι πρόκειται για DNS query σε ένα από τα domains που ανιχνεύθηκαν στην επίθεση αυτή. Φυσικά και αυτό δεν μας αρκεί καθώς θα πρέπει να αναλύσουμε περεταίρω την συγκεκριμένη κίνηση, για να δούμε αν πράγματι πρόκειται για επιτυχημένη επίθεση ή κάποια προσπάθεια.

Κοιτώντας στην δικτυακή κίνηση και φιλτράροντας βάση των στοιχείων που έχουμε, βλέπουμε πως στο διάστημα μεταξύ 18:00 – 21:00 πραγματοποιήθηκαν αυτά τα αιτήματα.

Εικόνα 162 - Security Onion - Connections over time

Με την βοήθεια του MISP και του Minemeld για την ανίχνευση και την παρακολούθηση της συγκεκριμένης επίθεσης, είχαμε ορίσει τις IP και τα αντίστοιχα hostnames στην λίστα των blacklisted IPs. Αυτό είχε ως αποτέλεσμα το αίτημα να απορριφθεί, πράγμα που σημαίνει ότι η επικοινωνία δεν έγινε και δεν χρειάζεται κάποια περεταίρω ενέργεια.



Εικόνα 163 - Security Onion - Connection attempt rejected

Έχουμε αναφέρει σε προηγούμενα κεφάλαια το γεγονός ότι το έργο μας θα είναι αρκετά δύσκολο όταν πρόκειται να αναζητήσουμε την απειλή, ειδικότερα την πρώτη φορά. Χρειάζεται εξειδικευμένη εμπειρία στην διαχείριση αυτών των εργαλείων, ωστόσο δεν είναι κάτι το οποίο δεν είναι εφικτό. Αυτό διότι ο όγκος των alerts που θα παίρνουμε, ειδικότερα σε έναν μεγάλο οργανισμό, θα είναι μεγάλος. Χρειάζεται ειδική διαχείριση και φιλτράρισμα ώστε να εντοπίσουμε μια ενδεχόμενη απειλή, καθώς ο όγκος των δεδομένων που θα λαμβάνουμε δεν αναιρεί και την πιθανότητα να παίρνουμε και false positives.

Όλα τα παραπάνω εργαλεία που χρησιμοποιήθηκαν στην εργαστηριακή υποδομή, αφορούν εργαλεία ανοιχτών πηγών. Αυτό φυσικά έχει τα πλεονεκτήματα αλλά και τα μειονεκτήματα του. Από την μια πλευρά, μπορεί ο οργανισμός να επωφεληθεί και να αυξήσει κατά πολύ το επίπεδο ασφάλειας του αλλά από την άλλη χρειάζεται γνώση, εμπειρία και επαγγελματίες στο αντικείμενο αυτό. Για παράδειγμα, όπως είδαμε, το Security Onion είναι πολύ περισσότερο από ένα εργαλείο δικτυακής ανάλυσης, ειδικότερα αν συνδυαστεί μελλοντικά και με άλλα εργαλεία ασφάλειας.

Κεφάλαιο 7 - Συμπεράσματα και Μελλοντικές Επεκτάσεις

Η ανθεκτικότητα στον κυβερνοχώρο είναι μια εξελισσόμενη προοπτική που ειδικότερα τα τελευταία χρόνια κερδίζει μεγάλη αναγνώριση. Η ιδέα ουσιαστικά συνδυάζει τους τομείς της ασφάλειας των πληροφοριών, της επιχειρηματικής συνέχειας και της οργάνωσης στα θέματα της κυβερνοασφάλειας.

Η συλλογή πληροφορίων για νέες κυβερνοαπειλές, η προληπτική αναζήτηση απειλών καθώς και η παρακολούθηση και αντιμετώπιση των απειλών μέσα από ένα SOC, παρέχει μια ολοκληρωμένη και σύνθετη δομή ασφαλείας για έναν οργανισμό.

Η προετοιμασία είναι το κλειδί σε κάθε στρατηγική πρόληψης και η βέλτιστη ασφάλεια ξεκινά πάντα από τον άνθρωπο, ειδικότερα για την ασφάλεια στον κυβερνοχώρο. Οι βέλτιστες πρακτικές κυβερνοασφάλειας είναι ακριβώς οι πρακτικές που ακολουθούμε. Τα μέτρα κυβερνοασφάλειας θα είναι πάντα ένα έργο σε εξέλιξη και αντικατοπτρίζουν τη συνεχή ροή της τεχνολογίας. Χρειάζεται χρόνος για να ανακαλύψουμε, να μάθουμε και να εφαρμόσουμε τις καλύτερες μεθόδους. Η συνεχής εκπαίδευση σε αυτήν την «κουλτούρα ασφάλειας» είναι επιτακτική ανάγκη στην προσπάθεια εφαρμογής των καλύτερων δυνατών διαδικασιών και η πραγματική δύναμη για την εφαρμογή αυτή, είναι η γνώση.

Θα ήταν ωφέλιμο να ενημερώνεται συχνά το πλαίσιο και η επεξεργασία των νέων πληροφοριών, ως μια ευκολότερη λύση για την εφαρμογή της προληπτικής κυβερνοάμυνας και της διεξαγωγής συχνών αναζητήσεων για νέες κυβερνοαπειλές. Υπάρχουν τεράστιες δυνατότητες, ειδικότερα με την χρήση της τεχνητής νοημοσύνης (AI) και της μηχανικής μάθησης (Machine Learning), για την βελτίωση και αυτοματοποίηση της προληπτικής αναζήτησης κυβερνοαπειλών, την αναζήτηση διαφορετικών μοτίβων για λήψη αυτοματισμών με σκοπό να ανταποκρίνονται όπως η ανθρώπινη συμπεριφορά. Μια ενδεχόμενη εφαρμογή του κύκλου OODA (Παρατηρώ-Προσανατολίζω-Αποφασίζω-Πράττω) θα μπορούσε να ωφελήσει στην ευκολότερη εφαρμογή της κυβερνοάμυνας με την πάροδο του χρόνου, καθώς ολοένα και περισσότερα στοιχεία θα συλλέγονται και η προληπτική αναζήτηση των απειλών θα είναι ευκολότερο να μελετηθεί.

Βιβλιογραφία

[1] Ahlberg, C., *The Threat Intelligence Handbook.* 2nd ed. s.l.:CyberEdge Group.

[2] Bianco, D., *Pyramid of Pain.*
Available at: http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

[3] Active Countermeasures, *Network Threat Hunting.*
Available at: https://www.activecountermeasures.com/

[4] Active Countermeasures, *Identifying long connections with bro-zeek.*
Available at: https://activecountermeasures.com

[5] Active Countermeasures, *RITA (Real Intelligence Threat Analytics).*
Available at: https://github.com/activecm/rita

[6] Digital, D. &. T., *Detecting the Unknown: A Guide to Threat Hunting.*
Available at: https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Detecting-the-Unknown-A-Guide-to-Threat-Hunting-v2.0.pdf

[7] Dr Goundar, S. & Dr Akashdeep, B., *A framework for effective threat hunting*.

[8] Eoannidis, N., *How To Setup Palo Alto Minemeld on Ubuntu 18.04.*
Available at: https://www.insecurewi.re/

[9] Haselhorst, D., *Onion-Zeek-RITA: Improving Network Visibility and Detecting C2 Activity,* SANS Institute.

[10] Hickman, A., *Gaining Visibility on the Network with Security Onion: A Cyber Threat Intelligence Based Approach.*
Available at: https://www.sans.org/white-papers/38740/

[11] Imam, F., *Threat Hunting Maturity Model - Infosec Institute.*
Available at: https://resources.infosecinstitute.com/topic/threat-hunting-maturity-model

[12] Johansen, G., *Digital Forensics and Incident Response.* Second ed. s.l.:Packt Publishing Ltd.

[13] Martin, J., *Cyber Threat Hunting: Identify and Hunt Down Intruders.*
Available at: https://www.infosecinstitute.com/podcast/cyber-threat-hunting-identify-and-hunt-down-intruders/

[14] Martin, L., *The Cyber Kill Chain.*
Available at: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

[15]MISP Project
Available at: https://www.misp-project.org/

[16]MITRE, *MITRE ATT&CK*
Available at: https://attack.mitre.org

[17]Oktavianto, D., *ITU - Cyber Threat Hunting Workshop.*
Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/CyberDrill-2020/Cyber%20Threat%20Hunting%20Workshop%20-%20ITU%2019112020.pdf

[18]Palo Alto, *Minemeld*
Available at: https://www.paloaltonetworks.com/products/secure-the-network/subscriptions/minemeld

[19]Scutt, M., *Threat Hunting Landscape.*
Available at: https://www.bluevoyant.com

[20]Security Onion Solutions, LLC, *Security Onion.*
Available at: https://securityonionsolutions.com/

[21]Sqrrl, *A Framework for Cyber Threat Hunting.*
Available at: www.sqrrl.com

[22]Sqrrl, *Hunt Evil: Your Practical Guide to Threat Hunting.*
Available at: www.sqrrl.com

[23]Varonis, *What is C2? Command and Control Infrastructure Explained.*
Available at: https://www.varonis.com/

[24]Splunk, *What Is a Security Operations Center (SOC)?*
Available at: https://www.splunk.com/en_us/data-insider/what-is-a-security-operations-center.html