ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ – ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΠΜΣ Κυβερνοασφάλεια και Επιστήμη Δεδομένων»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Ενίσχυση Ασφάλειας Δικτύου μέσω Πολυεπίπεδης Άμυνας: Μελέτη Ολοκληρωμένων Τεχνολογιών Ασφάλειας και Ανάλυσης Επιθέσεων** **Enhancing Network Security through Multi-Layered Defense: A Study of Integrated Security Technologies and Attack Analysis**
Ονοματεπώνυμο Φοιτητή	**Φιλιππαίος Γεώργιος**
Πατρώνυμο	**Δημήτριος**
Αριθμός Μητρώου	**ΜΠΚΕΔ2348**
Επιβλέπων	**Παναγιώτης Κοτζανικολάου, Καθηγητής**

Ημερομηνία Παράδοσης **Απρίλιος 2025**

Τριμελής Εξεταστική Επιτροπή

Κοτζανικολάου Παναγιώτης Καθηγητής	Κωνσταντίνος Πατσάκης Καθηγητής	Μιχαήλ Ψαράκης Αναπληρωτής Καθηγητής

Επιτελική Σύνοψη

Η παρούσα διπλωματική εργασία έχει ως βασικό στόχο τη διερεύνηση της αλληλεπίδρασης και της ενοποίησης κρίσιμων τεχνολογιών κυβερνοασφάλειας σε ένα εργαστηριακό περιβάλλον προσομοίωσης. Οι κύριες τεχνολογίες που αξιοποιούνται περιλαμβάνουν την πλατφόρμα ανταλλαγής πληροφοριών απειλών MISP (Malware Information Sharing Platform & Threat Sharing), το σύστημα διαχείρισης συμβάντων ασφαλείας IBM QRadar SIEM, καθώς και το pfSense ως firewall και πύλη ασφαλείας δικτύου. Πλαισιωτικά, χρησιμοποιούνται επίσης το Snort για ανίχνευση εισβολών (IDS) και το Squid Proxy για τον έλεγχο της εξερχόμενης διαδικτυακής κίνησης.

Το εργαστηριακό περιβάλλον έχει αναπτυχθεί σε πλατφόρμα VirtualBox, με τη χρήση εικονικών μηχανών που εκπροσωπούν πολλαπλές ζώνες ασφαλείας (DMZ, εσωτερικό δίκτυο, εξωτερικοί χρήστες). Κάθε ζώνη περιέχει συγκεκριμένους ρόλους και τεχνολογίες, προσομοιώνοντας ένα πραγματικό επιχειρησιακό σενάριο. Μέσα από τη διασύνδεση αυτών των εργαλείων, εξετάζεται πώς επιτυγχάνεται ενιαία ορατότητα σε συμβάντα ασφάλειας, συσχετισμός πληροφοριών από πολλαπλές πηγές και άμεση ανταπόκριση σε εξελιγμένες κυβερνοαπειλές.

Η τεχνολογία MISP αξιοποιείται για τη συλλογή και ανταλλαγή δεικτών συμβιβασμού (IoCs), ενισχύοντας τη γνώση του συστήματος απέναντι σε εξωτερικές απειλές. Το QRadar συλλέγει logs και flows από όλα τα σημεία του δικτύου, εντοπίζει ανωμαλίες και ενεργοποιεί ειδοποιήσεις μέσω προκαθορισμένων κανόνων. Το pfSense λειτουργεί ως η πρώτη γραμμή άμυνας, φιλτράροντας την εισερχόμενη και εξερχόμενη κίνηση με granular πολιτικές, ενώ το Snort εντοπίζει πιθανές απόπειρες εκμετάλλευσης αδυναμιών.

Συνολικά, η εργασία αποσκοπεί στο να αποδείξει ότι η ολιστική ενσωμάτωση των παραπάνω τεχνολογιών, ακόμα και σε ένα περιβάλλον με περιορισμένους πόρους, μπορεί να προσφέρει πραγματική επίγνωση κινδύνων, συνεργατική ανταλλαγή πληροφοριών και έγκαιρη αντίδραση σε απειλές, λειτουργώντας ως πρότυπο για μικρούς και μεσαίους οργανισμούς που επιθυμούν να ενισχύσουν την κυβερνοασφάλειά τους με πρακτικές λύσεις.

Abstract

The primary goal of this thesis is to explore the interaction and integration of key cybersecurity technologies within a simulated lab environment. The core technologies utilized include the MISP (Malware Information Sharing Platform & Threat Sharing) for threat intelligence sharing, the IBM QRadar SIEM for event and flow correlation, and pfSense as a network firewall and security gateway. Additional tools such as Snort (Intrusion Detection System) and Squid Proxy are employed to enhance traffic control and detection capabilities.

The lab environment has been built using VirtualBox, leveraging virtual machines to represent different security zones (DMZ, internal network, external users), each assigned distinct roles and technologies. The aim is to simulate a realistic enterprise setup where tool interoperability enables centralized visibility, correlation of threat data, and timely incident response.

MISP is used to collect and distribute Indicators of Compromise (IoCs), enriching threat context from external sources. QRadar aggregates logs and network flows, detects anomalies, and triggers alerts based on predefined rules. pfSense acts as the first layer of defense by filtering traffic through granular firewall rules, while Snort detects potential exploit attempts across the network.

Ultimately, this work aims to demonstrate that the holistic integration of these technologies — even in resource-constrained environments — can deliver actionable threat awareness, collaborative intelligence

sharing, and effective response to cyber threats. The architecture proposed could serve as a model for small and mid-sized organizations seeking to enhance their cybersecurity posture with practical, open-source, and commercial tools.

Ευχαριστίες

Θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες σε πολλά άτομα και φορείς που συνέβαλαν σημαντικά στην ολοκλήρωση αυτής της εργασίας και της ακαδημαϊκής μου διαδρομής.

Πρώτον, εκφράζω τις ειλικρινείς ευχαριστίες μου στην εταιρεία μου για τη συνεχή υποστήριξή και την ενθάρρυνση καθ' όλη τη διάρκεια αυτής της έρευνας. Ως Αναλυτής Ασφάλειας Πληροφοριών, η καθοδήγηση και οι πόροι τους ήταν πολύτιμες στη διαμόρφωση της κατεύθυνσης αυτής της διατριβής και στην επέκταση των γνώσεων μου στον τομέα της ασφάλειας δικτύων.

Θα ήθελα επίσης να εκφράσω την εκτίμησή μου στους συμφοιτητές με τους οποίους συνεργάστηκα κατά την διάρκεια του Μεταπτυχιακού Προγράμματός. Οι συλλογικές προσπάθειές μας η συνεργασία σε διάφορα ακαδημαϊκά μαθήματα συνέβαλαν καθοριστικά στην ανάπτυξή μου ως φοιτητής. Η αφοσίωση και ο ενθουσιασμός τους ήταν μια συνεχής πηγή κινήτρων και είμαι ευγνώμων για τη συντροφικότητα και την ακλόνητη υποστήριξή τους.

Απρίλιος 2025

Φιλιππαίος Γεώργιος

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΠΙΝΑΚΑΣ ΕΙΚΟΝΩΝ

1. Εισαγωγή

Στη σημερινή εποχή της πληροφορίας, τα ψηφιακά συστήματα και τα δίκτυα επικοινωνιών αποτελούν το θεμέλιο πάνω στο οποίο βασίζεται η λειτουργία των επιχειρήσεων, των κρατικών οργανισμών αλλά και οι καθημερινές δραστηριότητες των πολιτών. Η αυξανόμενη εξάρτηση από την τεχνολογία έχει επιφέρει σημαντικά οφέλη στην αποδοτικότητα και την ευκολία πρόσβασης στην πληροφορία. Ωστόσο, αυτή η τεχνολογική πρόοδος συνοδεύεται και από νέους κινδύνους, καθώς οι κυβερνοαπειλές εξελίσσονται με ταχείς ρυθμούς και γίνονται όλο και πιο πολύπλοκες και στοχευμένες.

Οι σύγχρονες επιθέσεις δεν βασίζονται πλέον μόνο σε τεχνικά τρωτά σημεία, αλλά αξιοποιούν συνδυασμούς τεχνικών κοινωνικής μηχανικής, κακόβουλου λογισμικού, και μη εξουσιοδοτημένης πρόσβασης. Τα περιστατικά παραβίασης δεδομένων, οι επιθέσεις ransomware και οι παραβιάσεις κρίσιμων υποδομών έχουν πλέον καθημερινή παρουσία στις ειδήσεις. Σε αυτό το πλαίσιο, η ανάγκη για αξιόπιστα και αποδοτικά μέτρα κυβερνοασφάλειας καθίσταται πιο επιτακτική από ποτέ.

Η παρούσα διπλωματική εργασία επικεντρώνεται στη μελέτη, ανάπτυξη και αξιολόγηση ενός εικονικού περιβάλλοντος κυβερνοασφάλειας, το οποίο περιλαμβάνει τη χρήση σύγχρονων εργαλείων όπως το SIEM QRadar, η πλατφόρμα ανταλλαγής πληροφοριών MISP, το firewall pfSense, το Snort για ανίχνευση εισβολών και το Squid για έλεγχο πρόσβασης στο διαδίκτυο. Στόχος είναι να προσομοιωθούν πραγματικές συνθήκες απειλών και να αναδειχθεί η αξία της συνδυασμένης χρήσης αυτών των τεχνολογιών για την πρόληψη, ανίχνευση και απόκριση σε περιστατικά ασφαλείας.

Μέσα από αυτή τη μελέτη, επιχειρείται η κατανόηση της πρακτικής λειτουργίας ενός σύγχρονου Security Operations Center (SOC) σε εργαστηριακό επίπεδο, ενώ παράλληλα αξιολογείται η αποτελεσματικότητα και διαλειτουργικότητα των επιμέρους εργαλείων. Το τελικό αποτέλεσμα μπορεί να αποτελέσει οδηγό για μικρομεσαίους οργανισμούς που επιθυμούν να ενισχύσουν την ασφάλειά τους αξιοποιώντας τόσο εμπορικές όσο και ανοιχτού κώδικα λύσεις.

1.1 Αντιμετωπίζοντας τις Σύγχρονες Απειλές με Συνδυαστικά Εργαλεία Κυβερνοασφάλεια

Στον σημερινό ψηφιακό κόσμο, όπου κάθε επιχείρηση και οργανισμός εξαρτάται από υπολογιστικά συστήματα και δικτυακές υποδομές, η προστασία των δεδομένων αποτελεί προτεραιότητα. Οι επιθέσεις στον κυβερνοχώρο είναι πλέον καθημερινό φαινόμενο και παρουσιάζουν διαρκώς αυξανόμενη πολυπλοκότητα και ένταση. Από τη διαρροή προσωπικών δεδομένων μέχρι στοχευμένες επιθέσεις σε κρίσιμες υποδομές, οι απειλές μπορούν να έχουν σοβαρές οικονομικές και επιχειρησιακές συνέπειες.

Οι παραδοσιακές μέθοδοι ασφάλειας, όπως η χρήση μόνο ενός firewall ή απλής antivirus προστασίας, αποδεικνύονται ανεπαρκείς. Οι σύγχρονες επιθέσεις είναι συχνά συνδυασμένες, δηλαδή εκμεταλλεύονται πολλαπλές αδυναμίες σε διαφορετικά επίπεδα του συστήματος. Έτσι, προκύπτει η ανάγκη για μια πολυεπίπεδη και ενοποιημένη προσέγγιση στην κυβερνοασφάλεια.

Η παρούσα εργασία εστιάζει στη διερεύνηση αυτής ακριβώς της ανάγκης: τη δημιουργία και αξιολόγηση ενός ολοκληρωμένου μοντέλου ασφάλειας με τη συνεργασία πολλαπλών εργαλείων και τεχνολογιών. Πιο συγκεκριμένα, το εικονικό περιβάλλον που υλοποιήθηκε περιλαμβάνει:

- Το **MISP**, μια πλατφόρμα ανταλλαγής πληροφοριών για κυβερνοαπειλές (Threat Intelligence Sharing),
- Το **SIEM QRadar**, ένα σύστημα διαχείρισης και συσχέτισης συμβάντων ασφαλείας, που συλλέγει και αναλύει δεδομένα από το δίκτυο,
- Το **pfSense**, ένα firewall που ελέγχει την κίνηση στο δίκτυο και εφαρμόζει πολιτικές πρόσβασης,
- Το **Snort IDS**, για την ανίχνευση εισβολών και κακόβουλων δραστηριοτήτων,
- Το **Squid**, για τον έλεγχο και φιλτράρισμα της πρόσβασης στο διαδίκτυο,
- Και ένα **Web Application Firewall (WAF)** μπροστά από έναν **Nginx web server**, που παρέχει επιπλέον προστασία στις διαδικτυακές εφαρμογές από επιθέσεις όπως SQL Injection, XSS, και άλλες.

Η υλοποίηση μιας τέτοιας συνδυαστικής λύσης δεν αποτελεί μόνο τεχνική επιλογή, αλλά ανταποκρίνεται και σε μια αυξανόμενη ανάγκη των οργανισμών για άμεση, αποτελεσματική και προσαρμοστική απόκριση σε κυβερνοεπιθέσεις. Το κίνητρο για τη συγκεκριμένη μελέτη προκύπτει από την επιθυμία κατανόησης του τρόπου με τον οποίο διαφορετικά εργαλεία – που συνήθως αναπτύσσονται και εφαρμόζονται ξεχωριστά – μπορούν να συνεργαστούν προς όφελος μιας ενιαίας στρατηγικής ασφάλειας.

Ωστόσο, η ενσωμάτωση ετερογενών τεχνολογιών δεν είναι απαλλαγμένη προκλήσεων. Κάθε εργαλείο έχει διαφορετική αρχιτεκτονική, απαιτήσεις και τρόπους διαχείρισης των δεδομένων. Η ρύθμιση κατάλληλων διασυνδέσεων, η διασφάλιση της συμβατότητας μεταξύ των συστημάτων, η κατανόηση των ροών πληροφορίας και η διαχείριση ψευδών θετικών είναι μερικές μόνο από τις τεχνικές και επιχειρησιακές προκλήσεις που αντιμετωπίζονται.

Παράλληλα, οι οργανισμοί καλούνται να ισορροπήσουν ανάμεσα στη συνοχή των εργαλείων, την επάρκεια πόρων (όπως υπολογιστική ισχύς, ανθρώπινο δυναμικό και τεχνογνωσία), και τη συνεχή ενημέρωση των εργαλείων ασφαλείας ώστε να ανταποκρίνονται στις ταχέως μεταβαλλόμενες απειλές.

Η διερεύνηση αυτών των θεμάτων μέσα σε ένα ελεγχόμενο, εικονικό εργαστηριακό περιβάλλον δίνει τη δυνατότητα εξαγωγής χρήσιμων συμπερασμάτων για την πρακτική υλοποίηση αντίστοιχων λύσεων σε πραγματικές συνθήκες.

1.2 Σκοπός και στόχοι της εργασίας

Ο σκοπός αυτής της διπλωματικής εργασίας είναι η δημιουργία και αξιολόγηση μιας ενοποιημένης και ασφαλούς δικτυακής υποδομής, ικανής να ανταποκριθεί στις σύγχρονες κυβερνοαπειλές μέσω της διασύνδεσης πολλαπλών προηγμένων τεχνολογιών ασφάλειας. Η εργασία επικεντρώνεται όχι μόνο στην επιτυχή υλοποίηση των επιμέρους συστημάτων αλλά κυρίως στην **ενοποίηση (integration)** τους σε ένα ενιαίο λειτουργικό σχήμα ασφάλειας.

Η εγκατάσταση του εργαστηριακού περιβάλλοντος και η διαμόρφωση των βασικών τεχνολογιών (MISP, QRadar, pfSense, Snort, WAF) αποτελεί **προαπαιτούμενο βήμα**, προκειμένου να είναι δυνατή η μελέτη της συνεργασίας τους. Το βασικό **use case** της εργασίας είναι η διερεύνηση των ωφελειών που προκύπτουν από τον συνδυασμό αυτών των τεχνολογιών και η αξιολόγηση της αποτελεσματικότητάς τους ως ένα ενιαίο σύστημα άμυνας.

Μετά την ολοκλήρωση της υλοποίησης και ενσωμάτωσης των επιμέρους λύσεων, ακολουθεί το στάδιο της **επαλήθευσης (validation)** της λειτουργικότητας και της αποτελεσματικότητας του συνόλου, με σενάρια που προσομοιώνουν ρεαλιστικές απειλές.

Οι κύριοι στόχοι της εργασίας περιλαμβάνουν:

1. **Ενσωμάτωση και παραμετροποίηση της πλατφόρμας MISP**
   Εγκατάσταση και διαμόρφωση του MISP σε εικονικό περιβάλλον, με στόχο τη συλλογή και ανταλλαγή δεικτών συμβιβασμού (IOCs). Εξετάζεται η συνδεσιμότητα με το QRadar και το pfSense ώστε να ενισχυθεί η ευαισθητοποίηση και η αντίδραση σε απειλές.
2. **Σχεδιασμός και ανάπτυξη ασφαλούς τοπολογίας δικτύου**
   Δημιουργία μιας τοπολογίας με ζώνες ασφαλείας (WAN, LAN, DMZ, MISP zone), ρυθμισμένη με το pfSense ώστε να παρέχει απομόνωση, ελεγχόμενη επικοινωνία και πολιτικές ασφάλειας ανά ζώνη.
3. **Εγκατάσταση και παραμετροποίηση του SIEM QRadar**
   Διασύνδεση του QRadar με MISP, pfSense και άλλα συστήματα για τη συλλογή, συσχέτιση και ανάλυση αρχείων καταγραφής (logs), με στόχο την ανίχνευση επιθέσεων και τη δημιουργία ειδοποιήσεων.
4. **Χρήση Web Application Firewall (WAF) για την προστασία εφαρμογών ιστού**
   Παραμετροποίηση του ModSecurity μπροστά από Nginx Web Server, για την προστασία από επιθέσεις όπως SQL Injection, XSS, και άλλες επιθέσεις σε επίπεδο εφαρμογής.
5. **Επαλήθευση της συνολικής λειτουργικότητας και αποδοτικότητας της λύσης**
   Υλοποίηση σεναρίων επίθεσης και παρακολούθηση της απόκρισης του συστήματος, με στόχο τη μέτρηση της αποτελεσματικότητας της ενοποιημένης υποδομής ασφαλείας.

1.3 Δομή της εργασίας

Η εργασία δομείται σε επτά κύρια κεφάλαια, καθένα από τα οποία εξυπηρετεί συγκεκριμένο στόχο ως προς την κατανόηση και την ανάλυση της προτεινόμενης λύσης:

1. **Εισαγωγή**: Παρουσιάζονται οι σύγχρονες προκλήσεις στην κυβερνοασφάλεια και η ανάγκη για συνεργατική χρήση πολλαπλών εργαλείων. Καθορίζονται ο σκοπός και οι στόχοι της εργασίας.
2. **Αρχιτεκτονικές και Τεχνολογίες Κυβερνοασφάλειας**: Αναλύονται οι βασικές αρχιτεκτονικές (όπως SOC και MISP με TAXII/STIX) και περιγράφονται τα εργαλεία που χρησιμοποιούνται, όπως το MISP, το pfSense, το Snort, το WAF ModSecurity, το QRadar, και άλλες σχετικές τεχνολογίες.
3. **Εγκατάσταση εργαστηριακού περιβάλλοντος**: Περιγράφεται βήμα-βήμα η δημιουργία του εργαστηριακού δικτύου, η εγκατάσταση και διαμόρφωση όλων των απαραίτητων συστημάτων, καθώς και η διασύνδεση μεταξύ τους.
4. **Ανάπτυξη Διασύνδεσης MISP, QRadar και pfSense**: Παρουσιάζονται τα bash scripts που δημιουργήθηκαν για την αυτοματοποιημένη ανταλλαγή δεδομένων απειλών και συμβάντων μεταξύ των εργαλείων.
5. **Επιγραμματική Δοκιμή**: Εκτελούνται και αξιολογούνται πρακτικές δοκιμές για τη λειτουργικότητα των διασυνδέσεων και την απόκριση του συστήματος στις απειλές.
6. **Συμπεράσματα και Μελλοντικές Επεκτάσεις**: Παρουσιάζονται τα κύρια συμπεράσματα που προκύπτουν από την εργασία, καθώς και προτάσεις για μελλοντική επέκταση, όπως η ενσωμάτωση EDR, DLP και η συνεργασία SOC μέσω TAXII.
7. **Βιβλιογραφικές Πηγές**: Παρατίθενται όλες οι επιστημονικές και τεχνικές πηγές που αξιοποιήθηκαν για την ανάπτυξη της εργασίας.

2. Αρχιτεκτονικές και Τεχνολογίες Κυβερνοασφάλειας

Η κυβερνοασφάλεια αποτελεί κρίσιμο παράγοντα για τη διατήρηση της ακεραιότητας, της διαθεσιμότητας και της εμπιστευτικότητας των δεδομένων σε έναν οργανισμό. Υπάρχουν διάφορες αρχιτεκτονικές που μπορούν να εφαρμοστούν, ανάλογα με τις ανάγκες και τις απαιτήσεις ασφαλείας ενός περιβάλλοντος. Στο παρόν κεφάλαιο, εξετάζουμε τις βασικές προσεγγίσεις στην αρχιτεκτονική κυβερνοασφάλειας και περιγράφουμε το ρόλο των SOC (Security Operations Centers).

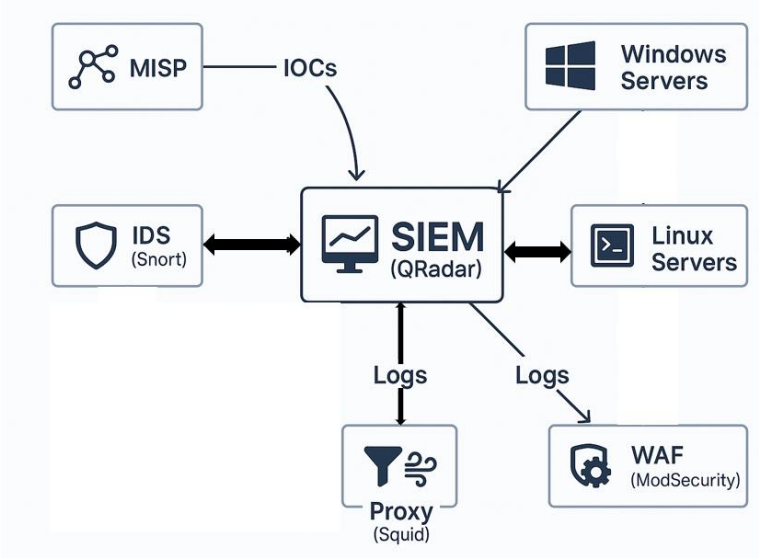
2.1 Αρχιτεκτονικές

Η παρούσα ενότητα περιγράφει βασικές **αρχιτεκτονικές υποδομές** στον τομέα της κυβερνοασφάλειας. Εξετάζονται η δομή και ο ρόλος ενός **Security Operations Center (SOC)** καθώς και οι μηχανισμοί **συνεργατικής ανταλλαγής πληροφοριών απειλών**, αξιοποιώντας πρότυπα όπως τα **TAXII, MISP και STIX**.

2.1.1 Security Operations Center (SOC)

Το Security Operations Center (SOC) είναι μια κεντρική υποδομή όπου συγκεντρώνονται και αναλύονται δεδομένα ασφαλείας ενός οργανισμού. Στο SOC, μια ομάδα αναλυτών ασφαλείας χρησιμοποιεί προηγμένα εργαλεία για την ανίχνευση, ανάλυση και απόκριση σε κυβερνοαπειλές σε πραγματικό χρόνο. Το SOC περιλαμβάνει συστήματα SIEM (όπως το QRadar), αλλά και άλλες τεχνολογίες όπως IDS/IPS, Web Application Firewalls (WAF), Network Firewalls και εργαλεία Threat Intelligence όπως το MISP.

Η παρακολούθηση δεν περιορίζεται μόνο στο QRadar, αλλά επεκτείνεται σε όλα τα εργαλεία ασφαλείας που έχουμε στο εργαστηριακό μας περιβάλλον. Αυτό περιλαμβάνει το pfSense ως firewall, το Snort για ανίχνευση εισβολών, το ModSecurity ως WAF μπροστά από τον Nginx web server και το MISP για ανταλλαγή πληροφοριών απειλών.



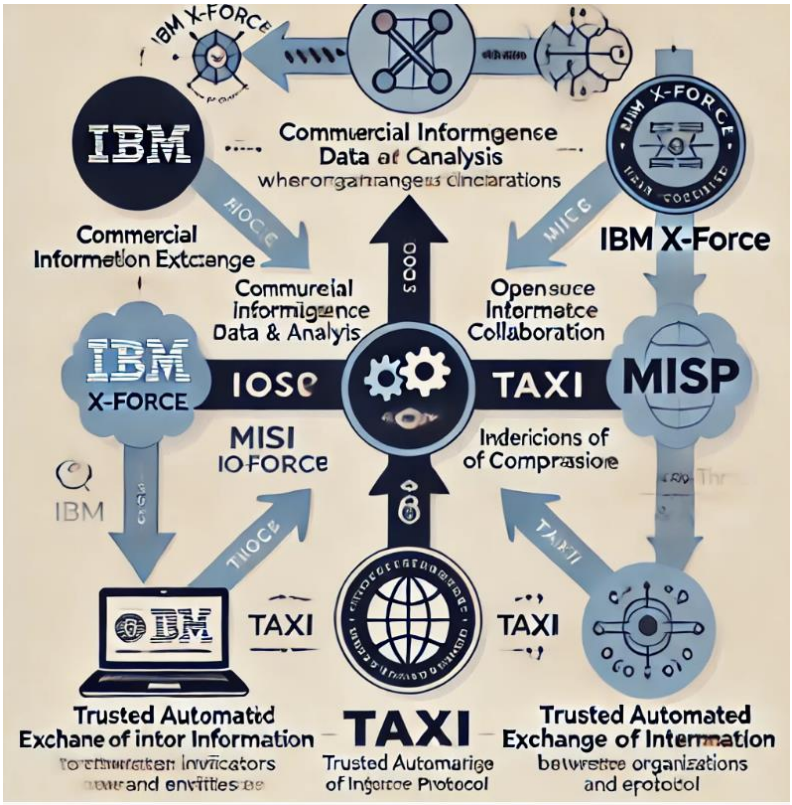
Εικόνα 1 Security Solutions Integrations

2.1.2 Συνεργατική Ανταλλαγή Πληροφοριών μέσω TAXII/MISP/STIX

Σήμερα, η διαχείριση απειλών βασίζεται σε SIEM συστήματα και πλατφόρμες Threat Intelligence, με το MISP και το IBM X-Force να είναι δύο από τα πιο γνωστά εργαλεία. Το IBM X-Force προσφέρει εμπορικά δεδομένα και αναλύσεις απειλών με μια εκτενή βάση δεδομένων, ενώ το MISP αποτελεί μια ανοιχτού κώδικα πλατφόρμα που στηρίζεται στη συνεργασία της κοινότητας. Μέσω του MISP, οργανισμοί μπορούν να ανταλλάσσουν IoCs (Indicators of Compromise), ενώ το X-Force παρέχει προγνωστική ανάλυση απειλών βασισμένη σε δεδομένα που συλλέγονται παγκοσμίως από την IBM.

Μια ακόμα σημαντική προσέγγιση στην κυβερνοασφάλεια είναι η ανταλλαγή πληροφοριών μέσω πρωτοκόλλων όπως το TAXII (Trusted Automated Exchange of Indicator Information), το οποίο επιτρέπει τη διαλειτουργική και αυτοματοποιημένη μεταφορά πληροφοριών μεταξύ διαφορετικών πλατφορμών και οργανισμών. Το TAXII συνήθως χρησιμοποιείται σε συνδυασμό με τη μορφή δεδομένων STIX (Structured Threat Information Expression), η οποία παρέχει ένα τυποποιημένο σχήμα για την αναπαράσταση πληροφοριών σχετικών με απειλές, όπως τακτικές, τεχνικές, στόχοι, καμπάνιες και IoCs.

Η υιοθέτηση του STIX και του TAXII επιτρέπει τη δημιουργία ενός παγκόσμιου, συνεργατικού οικοσυστήματος ανταλλαγής πληροφοριών, στο οποίο εργαλεία όπως το MISP και εμπορικές πλατφόρμες όπως το X-Force μπορούν να ενσωματωθούν, αυξάνοντας τη συλλογική ικανότητα ανίχνευσης, απόκρισης και πρόληψης κυβερνοεπιθέσεων.



Εικόνα 2 Xforce - MISP - TAXI Protocol

2.2 Τεχνολογίες Κυβερνοασφάλειας

Εξετάσαμε τις βασικές αρχιτεκτονικές και στρατηγικές για την παρακολούθηση και ανίχνευση κυβερνοαπειλών, όπως τα SOC και η συνεργατική ανταλλαγή πληροφοριών μέσω εργαλείων όπως το MISP και το TAXII. Αυτές οι προσεγγίσεις προσφέρουν ένα γενικό πλαίσιο για την ασφαλή διαχείριση των δεδομένων και την ανίχνευση επιθέσεων σε ευρύ επίπεδο.

Θα επικεντρωθούμε στα συγκεκριμένα δομικά στοιχεία που έχουν ενσωματωθεί και χρησιμοποιηθεί στην παρούσα εργασία, με σκοπό να αναπτύξουμε μια ολοκληρωμένη λύση κυβερνοασφάλειας.

Η αρχιτεκτονική του συστήματος μας περιλαμβάνει:

- **Συστήματα καταγραφής και ανάλυσης απειλών** (QRadar, MISP)
- **Τείχη προστασίας (Firewalls)** (pfSense, WAF , Squid Proxy)
- **Συστήματα Ανίχνευσης και Πρόληψης Εισβολών (IDS/IPS)** (Snort)
- **Web Server με Μηχανισμούς Προστασίας** (Nginx με WAF και πιστοποιητικά TLS/SSL)

2.2.1 MISP (Malware Information Sharing Platform & Threat Sharing)

Η τεχνολογία MISP (Malware Information Sharing Platform & Threat Sharing) είναι μια ανοιχτού κώδικα πλατφόρμα που έχει σχεδιαστεί για να διευκολύνει την ανταλλαγή πληροφοριών σχετικά με κυβερνοαπειλές μεταξύ οργανισμών, κυβερνητικών φορέων και κοινοτήτων. Η πλατφόρμα επιτρέπει την αποθήκευση, ανάλυση και διαμοιρασμό δεικτών συμβιβασμού (IOCs) και άλλων σχετικών πληροφοριών, επιτρέποντας στους χρήστες να αντιδράσουν γρήγορα σε νέες απειλές και να προστατεύσουν τα συστήματά τους από ενδεχόμενες επιθέσεις.

Ιστορική εξέλιξη του MISP

Αυτό το έργο ξεκίνησε γύρω στον Ιούνιο του 2011, όταν ο Christophe Vandeplas είχε μια απογοήτευση, καθώς πάρα πολλοί Δείκτες Συμβιβασμού (IOC) κοινοποιήθηκαν μέσω email ή σε έγγραφα pdf και δεν ήταν αναλύσιμοι από αυτόματα μηχανήματα. Έτσι, στο σπίτι άρχισε να παίζει με το CakePHP και έκανε μια απόδειξη της ιδέας του. Το ονόμασε CyDefSIG: Cyber Defense Signatures.

Στα μέσα Ιουλίου 2011 παρουσίασε το προσωπικό του έργο στη δουλειά (Belgian Defense), όπου τα σχόλια ήταν μάλλον θετικά. Αφού έδωσε πρόσβαση στον CyDefSIG που εκτελείται στον προσωπικό του διακομιστή, η Βελγική Άμυνα άρχισε να χρησιμοποιεί επίσημα το CyDefSIG από τα μέσα Αυγούστου 2011. Στη συνέχεια, στον Christophe επιτράπηκε να αφιερώσει λίγο χρόνο στο CyDefSIG κατά τις ώρες εργασίας του, ενώ εξακολουθούσε να εργάζεται σε αυτό στο σπίτι.

Κάποια στιγμή το NATO άκουσε για αυτό το έργο. Τον Ιανουάριο του 2012 έγινε μια πρώτη παρουσίαση για να εισαχθούν σε βάθος στο έργο. Εξέτασαν άλλα προϊόντα που προσέφερε η αγορά, αλλά φάνηκε ότι θεώρησαν ότι το άνοιγμα του CyDefSIG ήταν μεγάλο πλεονέκτημα. Ο Andrzej Dereszowski ήταν ο πρώτος προγραμματιστής μερικής απασχόλησης από την πλευρά του NATO.

Το ένα οδήγησε στο άλλο και μερικούς μήνες αργότερα το NATO προσέλαβε έναν προγραμματιστή πλήρους απασχόλησης για να βελτιώσει τον κώδικα και να προσθέσει περισσότερες δυνατότητες. Από εκείνη την ημερομηνία ξεκίνησε μια συλλογική ανάπτυξη. Όπως σε πολλά προσωπικά έργα, η άδεια δεν είχε γραφτεί ακόμη ρητά, αποφασίστηκε από κοινού ότι το έργο θα κυκλοφορούσε δημόσια με την άδεια Affero GPL. Αυτό για να μοιραστείτε τον κωδικό με όσο το δυνατόν περισσότερα άτομα και να τον προστατέψετε από οποιαδήποτε βλάβη.

Στη συνέχεια, το έργο μετονομάστηκε σε MISP: Malware Information Sharing Project, ένα όνομα που επινοήθηκε από τον Alex Vandurme από το NATO.

Τον Ιανουάριο του 2013, ο Andras Iklody έγινε ο κύριος προγραμματιστής πλήρους απασχόλησης του MISP, κατά τη διάρκεια της ημέρας που αρχικά προσλήφθηκε από το NATO και κατά τη διάρκεια της βραδιάς και του Σαββατοκύριακου συνεργάτης σε ένα έργο ανοιχτού κώδικα.

Εν τω μεταξύ άλλοι οργανισμοί άρχισαν να υιοθετούν το λογισμικό και να το προωθούν σε όλο τον κόσμο του CERT (CERT-EU, CIRCL και πολλοί άλλοι).

Σήμερα, ο Andras Iklody είναι ο κύριος προγραμματιστής του έργου MISP και εργάζεται για την CIRCL.

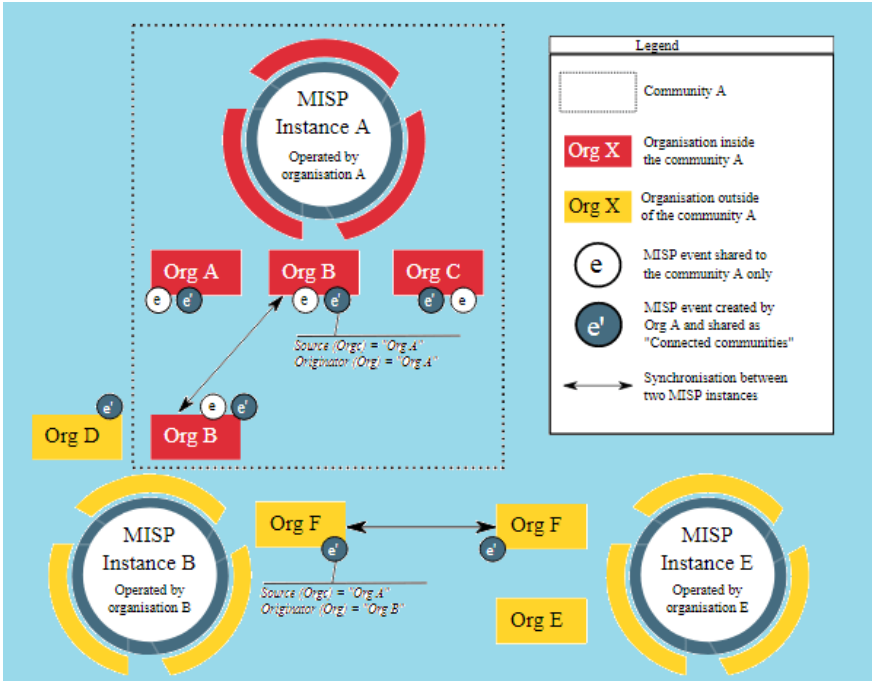
Καθώς το έργο MISP επεκτάθηκε, το MISP δεν καλύπτει μόνο τους δείκτες κακόβουλου λογισμικού αλλά και πληροφορίες απάτης ή ευπάθειας. Το όνομα είναι πλέον MISP Threat Sharing, το οποίο περιλαμβάνει το βασικό λογισμικό MISP και μια μυριάδα εργαλείων (PyMISP) και μορφή (μορφή πυρήνα, ταξινομίες MISP, λίστες προειδοποίησης) για την υποστήριξη MISP. Το MISP είναι πλέον ένα κοινοτικό έργο με επικεφαλής μια ομάδα εθελοντών.

Σημασία και χρήση του MISP

Το MISP διαδραματίζει σημαντικό ρόλο στην κυβερνοασφάλεια, καθώς παρέχει μια οργανωμένη και ασφαλή πλατφόρμα για την ανταλλαγή πληροφοριών σχετικά με τις απειλές. Η δυνατότητα να διαμοιράζονται οι οργανισμοί πληροφορίες για νέες επιθέσεις και τρωτά σημεία, τους επιτρέπει να προσαρμόζονται γρήγορα σε νέες απειλές και να λαμβάνουν προληπτικά μέτρα για την προστασία των δικτύων και των δεδομένων τους.

Επιπλέον, η χρήση του MISP επιτρέπει στους οργανισμούς να αναγνωρίζουν και να ανταποκρίνονται πιο γρήγορα σε επιθέσεις, μέσω της ανταλλαγής δεδομένων σε πραγματικό χρόνο με άλλους οργανισμούς και κοινότητες. Αυτό μειώνει τον χρόνο απόκρισης και αυξάνει την αποτελεσματικότητα των αμυντικών στρατηγικών, καθώς οι οργανισμοί μπορούν να χρησιμοποιούν τις πληροφορίες για να αναγνωρίζουν και να αναλύουν τακτικές, τεχνικές και διαδικασίες (TTPs) που χρησιμοποιούν οι επιτιθέμενοι.

Πως χρησιμοποιούν οι οργανισμοί το MISP



Εικόνα 3 Το MISP στους Οργανισμούς (Πηγή: circl.lu)

Οι οργανισμοί χρησιμοποιούν το MISP με διάφορους τρόπους για να βελτιώσουν την ασφάλεια του δικτύου τους και να ανταποκριθούν σε κυβερνοαπειλές. Μερικοί από τους κύριους τρόπους χρήσης περιλαμβάνουν:

- **Συλλογή και Ανάλυση Πληροφοριών Απειλών:** Οι οργανισμοί χρησιμοποιούν το MISP για να συλλέγουν δεδομένα από διάφορες πηγές, όπως άλλοι οργανισμοί ή ανοιχτές πηγές, και να τα αναλύουν για να αναγνωρίζουν πρότυπα επιθέσεων και πιθανές απειλές.
- **Διαμοιρασμός Δεικτών Συμβιβασμού (IOCs):** Οι οργανισμοί μπορούν να μοιράζονται IOCs μέσω του MISP, επιτρέποντας σε άλλους να ενημερώσουν τα συστήματά τους για πιθανές επιθέσεις ή κακόβουλες δραστηριότητες.
- **Συνεργασία για την Ανάπτυξη Αντιμετρήσεων:** Το MISP επιτρέπει στους οργανισμούς να συνεργάζονται για την ανάπτυξη νέων μέτρων ασφαλείας και αντιμετρήσεων, βασισμένων στις πληροφορίες που έχουν μοιραστεί.
- **Εκπαίδευση και Ευαισθητοποίηση:** Η πλατφόρμα μπορεί να χρησιμοποιηθεί για την εκπαίδευση και την ευαισθητοποίηση των υπαλλήλων σε θέματα ασφάλειας, βοηθώντας τους να αναγνωρίζουν και να αντιδρούν σε απειλές πιο αποτελεσματικά.

Εφαρμογές και οφέλη της πλατφόρμας

Η πλατφόρμα MISP προσφέρει πολλές εφαρμογές και οφέλη για τους οργανισμούς που την υιοθετούν:

- **Αυτόματη Ανίχνευση και Αντιμετώπιση Απειλών:** Το MISP μπορεί να ενσωματωθεί με άλλα συστήματα ασφαλείας για να επιτρέψει την αυτόματη ανίχνευση και αντιμετώπιση απειλών. Για παράδειγμα, τα IOCs που συλλέγονται μέσω του MISP μπορούν να αποστέλλονται αυτόματα σε συστήματα SIEM όπως το QRadar για ανάλυση και συσχέτιση.
- **Κεντρικοποίηση Δεδομένων Απειλών:** Το MISP λειτουργεί ως ένα κεντρικό αποθετήριο για όλα τα δεδομένα απειλών, επιτρέποντας στους οργανισμούς να έχουν μια ενοποιημένη εικόνα των απειλών που αντιμετωπίζουν.
- **Ενίσχυση του Οικοσυστήματος Ασφαλείας:** Με την ενσωμάτωση του MISP με άλλα εργαλεία, όπως το pfSense και το SIEM QRadar, οι οργανισμοί μπορούν να δημιουργήσουν ένα πιο ισχυρό οικοσύστημα ασφαλείας που μπορεί να αντιδράσει γρήγορα σε νέες απειλές.
- **Αυξημένη Διαφάνεια και Κατανόηση Απειλών:** Μέσω της χρήσης του MISP, οι οργανισμοί μπορούν να αποκτήσουν βαθύτερη κατανόηση των απειλών που αντιμετωπίζουν, επιτρέποντάς τους να αναπτύξουν πιο στοχευμένες στρατηγικές άμυνας.

Παραδείγματα χρήσης σε πραγματικά σενάρια

Οι πραγματικές χρήσεις του MISP καλύπτουν ένα ευρύ φάσμα σεναρίων στον τομέα της κυβερνοασφάλειας:

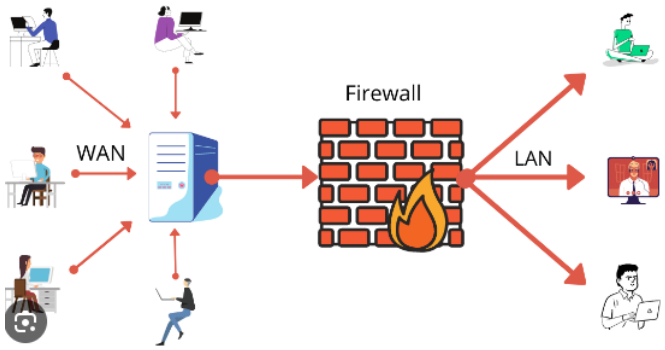
- **Ανίχνευση Κακόβουλου Λογισμικού:** Ένας οργανισμός μπορεί να χρησιμοποιήσει το MISP για να λάβει πληροφορίες σχετικά με ένα νέο είδος κακόβουλου λογισμικού που κυκλοφορεί. Οι πληροφορίες αυτές μπορούν να χρησιμοποιηθούν για την ενημέρωση των συστημάτων ασφαλείας και την πρόληψη μολύνσεων.
- **Αντιμετώπιση DDoS Επιθέσεων:** Σε περίπτωση μιας DDoS επίθεσης, ένας οργανισμός μπορεί να μοιραστεί τις πληροφορίες με άλλους μέσω του MISP για να βοηθήσει στην ταυτοποίηση και τον αποκλεισμό των πηγών της επίθεσης.

- **Ανίχνευση Σάρωσης Θυρών:** Ένας οργανισμός που ανακαλύπτει ασυνήθιστη δραστηριότητα σάρωσης θυρών μπορεί να χρησιμοποιήσει το MISP για να διασταυρώσει αν άλλοι οργανισμοί έχουν δει παρόμοιες δραστηριότητες, βοηθώντας στην αναγνώριση πιθανών επιθέσεων.
- **Πρόληψη και Αντιμετώπιση Επιθέσεων Phishing:** Οργανισμοί μπορούν να χρησιμοποιούν το MISP για να μοιράζονται πληροφορίες σχετικά με καμπάνιες phishing, βοηθώντας άλλους οργανισμούς να αναγνωρίσουν και να αποκλείσουν τέτοιες απειλές πριν προκαλέσουν ζημιές.

2.2.2 Δικτυακά τείχη προστασίας (Network Firewalls)

Τα τείχη προστασίας είναι μία από τις πιο βασικές και διαδεδομένες τεχνολογίες ασφάλειας. Χρησιμοποιούνται για την παρακολούθηση και τον έλεγχο της εισερχόμενης και εξερχόμενης κίνησης σε ένα δίκτυο βάσει προκαθορισμένων κανόνων ασφαλείας. Τα τείχη προστασίας μπορούν να είναι υλικού ή λογισμικού και συνήθως ενσωματώνουν τεχνολογίες ανίχνευσης και πρόληψης εισβολών (IDS/IPS).

- **pfSense:** Το pfSense είναι ένα ανοικτού κώδικα τείχος προστασίας που χρησιμοποιείται ευρέως για τη διαχείριση και την προστασία δικτύων. Υποστηρίζει προηγμένες λειτουργίες, όπως φιλτράρισμα πακέτων, δημιουργία VPN, διαχείριση εύρους ζώνης, και δυνατότητες IDS/IPS μέσω ενσωμάτωσης με το Snort.



Εικόνα 4Παράδειγμα Τοπολογίας με Firewall (Πηγή: geekflare.com)

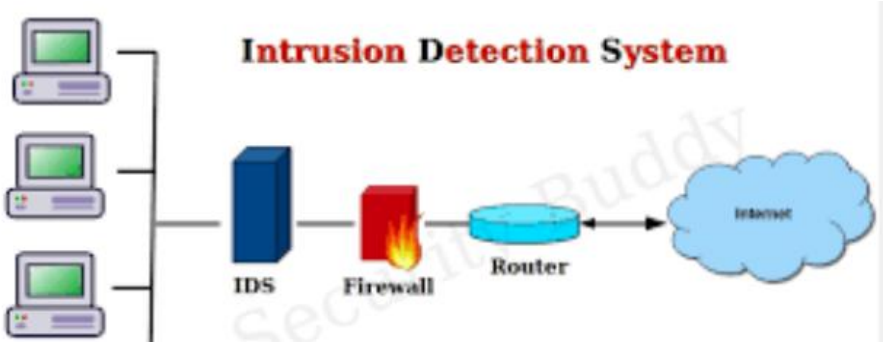
2.2.3 Συστήματα ανίχνευσης και πρόληψης εισβολών (IDS/IPS)

Τα **IDS/IPS** αποτελούν κρίσιμα συστήματα ασφαλείας, σχεδιασμένα να εντοπίζουν και να αποτρέπουν κακόβουλες δραστηριότητες στο δίκτυο.

Snort ως IDS/IPS

Το **Snort** είναι ένα από τα πιο διαδεδομένα **ανοικτού κώδικα** IDS/IPS, που αναλύει την κίνηση σε πραγματικό χρόνο και εφαρμόζει κανόνες για την ανίχνευση κακόβουλων δραστηριοτήτων. Χρησιμοποιείται ευρέως, καθώς:

- Υποστηρίζει **ευέλικτους και προσαρμόσιμους κανόνες ασφαλείας**.
- Μπορεί να λειτουργήσει τόσο ως **παθητικό IDS** όσο και ως **ενεργό IPS**.
- Ενσωματώνεται με **pfSense** για την προστασία των δικτύων από κυβερνοεπιθέσεις.

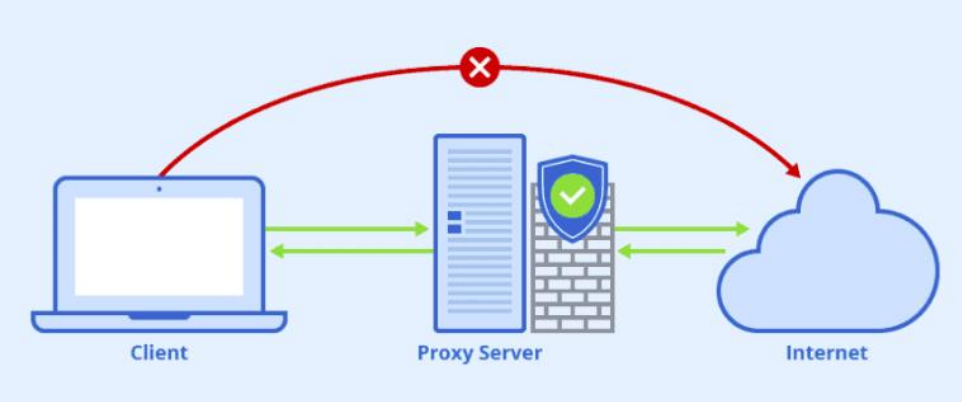


Εικόνα 5Παράδειγμα Τοπολογίας με IDS (Πηγή: thesecuritybuddy.com)

2.2.4 Proxy Servers

Οι proxy servers λειτουργούν ως ενδιάμεσοι μεταξύ των χρηστών και του διαδικτύου, προσφέροντας βελτιωμένη ασφάλεια, ανωνυμία και έλεγχο της διαδικτυακής κυκλοφορίας. Επιπλέον, τα εργαλεία φιλτραρίσματος περιεχομένου επιτρέπουν τον έλεγχο και την περιορισμό της πρόσβασης σε ανεπιθύμητο ή κακόβουλο περιεχόμενο.

- **Squid:** Το Squid είναι ένας ανοικτού κώδικα proxy server και cache εργαλείο που χρησιμοποιείται για τη βελτιστοποίηση της διαδικτυακής κυκλοφορίας και την εφαρμογή πολιτικών φιλτραρίσματος περιεχομένου. Στο περιβάλλον του δικτύου μας, το Squid συνδυάζεται με άλλες τεχνολογίες για να βελτιώσει την απόδοση και να ενισχύσει την ασφάλεια, προστατεύοντας τους χρήστες από κακόβουλες ιστοσελίδες και μη επιτρεπτές δραστηριότητες.



Εικόνα 6 Παράδειγμα Τοπολογίας με Proxy (Πηγή: seobility.net)

2.2.5 SIEM Qradar

Το **IBM QRadar** είναι ένα από τα κορυφαία συστήματα SIEM (Security Information and Event Management) που χρησιμοποιούνται παγκοσμίως για την ενίσχυση της ασφάλειας των πληροφοριακών συστημάτων και την αντιμετώπιση κυβερνοαπειλών. Το QRadar παρέχει μια ολοκληρωμένη πλατφόρμα για την ανάλυση, την παρακολούθηση και τη διαχείριση των συμβάντων ασφαλείας σε πραγματικό χρόνο, επιτρέποντας στους οργανισμούς να εντοπίζουν και να αντιδρούν άμεσα σε ύποπτες ή κακόβουλες δραστηριότητες.

- **Συγκέντρωση Δεδομένων και Καταγραφή Αρχείων (Log Management):**
  - Το QRadar μπορεί να συγκεντρώνει αρχεία καταγραφής (logs) από διάφορες πηγές όπως δικτυακά τείχη προστασίας, συστήματα ανίχνευσης εισβολών (IDS/IPS), διακομιστές, εφαρμογές και άλλα συστήματα πληροφορικής.
  - Υποστηρίζει την καταγραφή σε πραγματικό χρόνο και τη μακροχρόνια αποθήκευση αρχείων καταγραφής, διευκολύνοντας την ανάλυση και τον εντοπισμό ανωμαλιών ή ενδείξεων συμβιβασμού (Indicators of Compromise - IOCs).
- **Ανάλυση Συμβάντων και Ανίχνευση Απειλών (Event Analysis and Threat Detection):**
  - Χρησιμοποιεί προηγμένους αλγορίθμους ανάλυσης για να εντοπίζει ανωμαλίες και ύποπτες δραστηριότητες, όπως μη εξουσιοδοτημένη πρόσβαση, επιθέσεις DDoS, και παραβιάσεις πολιτικών ασφαλείας.
  - Εφαρμόζει τεχνικές μηχανικής μάθησης και ανάλυσης συμπεριφοράς για να κατανοεί το φυσιολογικό μοτίβο δραστηριότητας και να εντοπίζει αποκλίσεις που μπορεί να υποδηλώνουν κακόβουλη δραστηριότητα.
- **Συσχέτιση Δεδομένων (Correlation of Data):**
  - Το QRadar χρησιμοποιεί μηχανισμούς συσχέτισης για να συνδυάζει δεδομένα από πολλαπλές πηγές και να προσδιορίζει σύνθετα πρότυπα επιθέσεων που μπορεί να μη φαίνονται εμφανή σε ένα μόνο σύνολο δεδομένων.
  - Αυτή η συσχέτιση επιτρέπει την ανίχνευση προηγμένων επίμονων απειλών (Advanced Persistent Threats - APTs) που συχνά συνδυάζουν πολλές τεχνικές και μεθόδους για να παρακάμψουν τις συμβατικές άμυνες.

- **Ενοποίηση με Άλλα Συστήματα (Integration with Other Systems):**
    - Το QRadar μπορεί να ενσωματωθεί με πληθώρα εργαλείων ασφαλείας και πληροφορικής, όπως το MISP για ανταλλαγή πληροφοριών σχετικά με απειλές, το pfSense για ανάλυση δικτυακών επιθέσεων, και το Snort για ανίχνευση εισβολών.
    - Επιτρέπει την αυτοματοποίηση της ανταπόκρισης σε συμβάντα μέσω της ενοποίησης με συστήματα SOAR (Security Orchestration, Automation, and Response).
- **Οπτικοποίηση Δεδομένων και Αναφορές (Data Visualization and Reporting):**
    - Το QRadar παρέχει δυνατότητες οπτικοποίησης δεδομένων μέσω προσαρμόσιμων πίνακων ελέγχου και γραφημάτων που βοηθούν τους αναλυτές ασφαλείας να κατανοούν την κατάσταση του δικτύου και να εντοπίζουν γρήγορα πιθανά προβλήματα.
    - Προσφέρει αναλυτικές αναφορές και συμμόρφωση με πρότυπα, όπως PCI DSS, HIPAA, και GDPR, διευκολύνοντας τους οργανισμούς να παρακολουθούν και να αναφέρουν τη συμμόρφωση με τις κανονιστικές απαιτήσεις.
- **Κλιμακωσιμότητα και Απόδοση (Scalability and Performance):**
    - Σχεδιασμένο να υποστηρίζει τόσο μικρά όσο και μεγάλα δίκτυα, το QRadar μπορεί να κλιμακωθεί ανάλογα με τις ανάγκες του οργανισμού, από μικρές εγκαταστάσεις μέχρι μεγάλα κέντρα δεδομένων με χιλιάδες πηγές δεδομένων.
    - Η υψηλή απόδοση του QRadar εξασφαλίζει την επεξεργασία μεγάλων όγκων δεδομένων σε πραγματικό χρόνο, επιτρέποντας την άμεση ανίχνευση και ανταπόκριση σε απειλές.

Δυνατότητες του QRadar

- **Αυτοματοποιημένη Ανίχνευση και Αντιμετώπιση Απειλών (Automated Threat Detection and Response):**
    - Το QRadar επιτρέπει την αυτοματοποίηση της ανίχνευσης και της ανταπόκρισης σε απειλές, μειώνοντας το χρόνο απόκρισης και την επιβάρυνση των αναλυτών ασφαλείας.
    - Μπορεί να διαμορφωθεί για να εκτελεί αυτόματα ενέργειες, όπως αποκλεισμός IP, καραντίνα συστημάτων, και ενημέρωση κανόνων ασφαλείας, με βάση προκαθορισμένες πολιτικές και προφίλ απειλών.
- **Προηγμένη Ανάλυση Συμπεριφοράς Χρηστών και Οντοτήτων (User and Entity Behavior Analytics - UEBA):**
    - Η δυνατότητα UEBA του QRadar χρησιμοποιεί μηχανική μάθηση για να αναλύει τη συμπεριφορά χρηστών και οντοτήτων, εντοπίζοντας ασυνήθιστες ενέργειες που μπορεί να υποδηλώνουν εσωτερικές απειλές ή παραβιάσεις ασφάλειας.
    - Προσφέρει οπτικοποίηση της δραστηριότητας των χρηστών και των συσκευών, επιτρέποντας στους αναλυτές να παρακολουθούν τη δραστηριότητα σε πραγματικό χρόνο και να εντοπίζουν ύποπτες συμπεριφορές.
- **Ενσωμάτωση με Πλατφόρμες Ανταλλαγής Πληροφοριών Απειλών (Threat Intelligence Integration):**
    - Το QRadar μπορεί να ενσωματωθεί με πλατφόρμες ανταλλαγής πληροφοριών απειλών, όπως το MISP, για να εισάγει αυτόματα πληροφορίες σχετικά με νέες απειλές και δείκτες συμβιβασμού (IOCs).
    - Αυτή η δυνατότητα ενισχύει την ικανότητα του οργανισμού να προσαρμόζεται και να αντιδρά σε νέες και εξελισσόμενες απειλές.

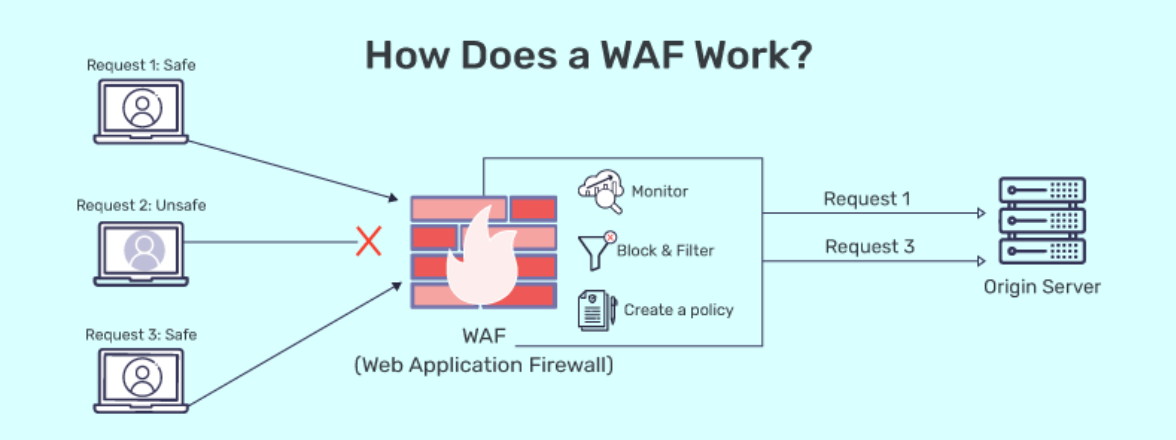
- **Διαχείριση Συμμόρφωσης και Αξιολόγηση Κινδύνου (Compliance Management and Risk Assessment):**
    - Το QRadar υποστηρίζει την παρακολούθηση και την αναφορά συμμόρφωσης με διάφορα κανονιστικά πρότυπα και απαιτήσεις, διευκολύνοντας την αξιολόγηση και τη διαχείριση του κινδύνου.
    - Παρέχει πρότυπες αναφορές και εργαλεία που βοηθούν τους οργανισμούς να εντοπίζουν κενά ασφάλειας και να εφαρμόζουν διορθωτικά μέτρα.

Εικόνα 7 Χαρακτηριστικά Λογισμικού SIEM (Πηγή: manageengine.com)

2.2.6 Web Application Firewalls (WAF)

Τα WAF είναι εξειδικευμένα τείχη προστασίας που προστατεύουν εφαρμογές ιστού από κοινές επιθέσεις, όπως SQL injection, cross-site scripting (XSS) και άλλες κακόβουλες δραστηριότητες.

Το **ModSecurity** είναι ένα ανοιχτού κώδικα Web Application Firewall (WAF) που χρησιμοποιείται για την προστασία των διαδικτυακών εφαρμογών από ποικιλία επιθέσεων. Όταν ενσωματώνεται με τον **Nginx web server**, προσφέρει ένα ισχυρό επίπεδο άμυνας που μπορεί να αποτρέψει κοινές και προηγμένες απειλές, όπως SQL injections, cross-site scripting (XSS), και επιθέσεις DDoS.



Εικόνα 8 Πως Λειτουργεί το WAF (Πηγή indusface.com)

Χαρακτηριστικά του ModSecurity

- **Ανίχνευση και Πρόληψη Απειλών:**
  - Το ModSecurity λειτουργεί σαν ένα φίλτρο μεταξύ του χρήστη και της εφαρμογής web. Αναλύει την εισερχόμενη και εξερχόμενη κίνηση για να εντοπίσει και να μπλοκάρει κακόβουλες αιτήσεις, χρησιμοποιώντας προκαθορισμένους κανόνες ασφαλείας.
  - Διαθέτει μια μεγάλη βάση δεδομένων από προκαθορισμένους κανόνες (OWASP Core Rule Set), που καλύπτουν τις πιο κοινές απειλές κατά των διαδικτυακών εφαρμογών.
- **Ευέλικτη Διαμόρφωση:**
  - Οι κανόνες του ModSecurity μπορούν να προσαρμοστούν ώστε να ανταποκρίνονται στις συγκεκριμένες ανάγκες ασφαλείας μιας εφαρμογής ή ενός οργανισμού.
  - Υποστηρίζει τον ορισμό custom κανόνων για την ανίχνευση συγκεκριμένων μοτίβων επιθέσεων ή την προσαρμογή στις απαιτήσεις της εφαρμογής.
- **Καταγραφή και Αναφορά:**
  - Προσφέρει λεπτομερή αρχεία καταγραφής των συμβάντων ασφαλείας, βοηθώντας τους διαχειριστές να κατανοήσουν τη φύση των επιθέσεων και να βελτιώσουν τη διαμόρφωση της ασφάλειας.
  - Υποστηρίζει τη δημιουργία αναφορών που βοηθούν στην ανάλυση της απόδοσης του WAF και την αναγνώριση των τάσεων των απειλών.
- **Προστασία σε Πραγματικό Χρόνο:**
  - Το ModSecurity μπορεί να ανιχνεύσει και να αποκλείσει απειλές σε πραγματικό χρόνο, προλαμβάνοντας την εκμετάλλευση τρωτών σημείων στις διαδικτυακές εφαρμογές.
  - Υποστηρίζει δυνατότητες που βοηθούν στον περιορισμό των κακόβουλων επιθέσεων, όπως το rate limiting για την αποφυγή DDoS επιθέσεων.

Nginx Web Server και ενσωμάτωση με ModSecurity

Ο **Nginx** είναι ένας δημοφιλής web server γνωστός για την υψηλή απόδοση και την ευελιξία του. Η ενσωμάτωση του Nginx με το ModSecurity προσφέρει ισχυρή προστασία από διαδικτυακές απειλές, χωρίς να μειώνει την απόδοση του διακομιστή.

- **Αρχιτεκτονική και Απόδοση:**

- Ο Nginx σχεδιάστηκε για να διαχειρίζεται μεγάλο όγκο αιτήσεων ταυτόχρονα, κάτι που τον καθιστά ιδανικό για τη διαχείριση μεγάλων ιστοσελίδων και εφαρμογών.
- Η ενσωμάτωση με το ModSecurity εκμεταλλεύεται αυτή την απόδοση, προσφέροντας προστασία χωρίς σημαντική επιβάρυνση στη λειτουργικότητα του server.

- **Υποστήριξη Αντίστροφου Διακομιστή Μεσολάβησης (Reverse Proxy):**
  - Ο Nginx συχνά χρησιμοποιείται ως αντίστροφος διακομιστής μεσολάβησης, επιτρέποντας τη διανομή του φορτίου μεταξύ πολλαπλών backend servers. Αυτή η δυνατότητα βοηθά στη βελτιστοποίηση της απόδοσης και της ασφάλειας.
  - Σε συνδυασμό με το ModSecurity, ο Nginx μπορεί να φιλτράρει την κακόβουλη κίνηση προτού φτάσει στους backend servers, προσθέτοντας ένα επιπλέον επίπεδο προστασίας.
- **Προστασία Εφαρμογών:**
  - Με το ModSecurity, ο Nginx προστατεύει τις εφαρμογές από απειλές σε επίπεδο εφαρμογής, όπως επιθέσεις injection, XSS, και CSRF (Cross-Site Request Forgery).
  - Αυτή η προστασία βοηθά να διασφαλιστεί η ακεραιότητα και η ασφάλεια των δεδομένων που διαχειρίζονται οι εφαρμογές web.
- **Ασφάλεια Βάσει Περιβάλλοντος:**
  - Το ModSecurity επιτρέπει την εφαρμογή κανόνων ασφαλείας βάσει του περιβάλλοντος του χρήστη, όπως η διεύθυνση IP, ο τύπος του προγράμματος περιήγησης, και άλλοι παράγοντες, βελτιώνοντας την ακρίβεια των πολιτικών ασφαλείας.

Πιστοποιητικό στον Nginx Web Server

Τα ψηφιακά πιστοποιητικά SSL/TLS είναι ζωτικής σημασίας για την ασφάλεια των διαδικτυακών επικοινωνιών. Στον **Nginx web server**, τα πιστοποιητικά SSL/TLS παίζουν έναν κρίσιμο ρόλο στην προστασία των δεδομένων και στην οικοδόμηση εμπιστοσύνης με τους χρήστες.

Σημασία των πιστοποιητικών SSL/TLS

- **Κρυπτογράφηση Δεδομένων:**
  - Τα πιστοποιητικά SSL/TLS εξασφαλίζουν ότι η επικοινωνία μεταξύ του web server και του client (όπως ένας περιηγητής ιστού) είναι κρυπτογραφημένη. Αυτό σημαίνει ότι τα δεδομένα που μεταφέρονται δεν μπορούν να διαβαστούν ή να αλλοιωθούν από κακόβουλους τρίτους.
  - Η κρυπτογράφηση είναι απαραίτητη για την προστασία ευαίσθητων πληροφοριών, όπως προσωπικά δεδομένα και στοιχεία πιστωτικών καρτών.
- **Αυθεντικοποίηση και Αξιοπιστία:**
  - Ένα έγκυρο πιστοποιητικό SSL/TLS επιβεβαιώνει την ταυτότητα του διακομιστή, διασφαλίζοντας στους χρήστες ότι επικοινωνούν με τον σωστό ιστότοπο και όχι με έναν κακόβουλο διακομιστή.
  - Αυτή η αυθεντικοποίηση αποτρέπει επιθέσεις phishing και man-in-the-middle (MITM), όπου ένας επιτιθέμενος προσπαθεί να υποδυθεί έναν αξιόπιστο ιστότοπο.
- **Βελτίωση SEO και Εμπιστοσύνης Χρήστη:**
  - Οι μηχανές αναζήτησης, όπως η Google, δίνουν προτεραιότητα στους ασφαλείς ιστότοπους που χρησιμοποιούν HTTPS αντί του HTTP. Αυτό σημαίνει ότι η χρήση πιστοποιητικών SSL/TLS μπορεί να βελτιώσει τη θέση ενός ιστότοπου στα αποτελέσματα αναζήτησης.

- Οι χρήστες είναι πιο πιθανό να εμπιστευτούν και να αλληλεπιδράσουν με έναν ιστότοπο που χρησιμοποιεί HTTPS, καθώς η ασφάλεια και η προστασία της ιδιωτικότητας των δεδομένων τους είναι διασφαλισμένη.

2.2.7 Διασύνδεση Με Bash Scripting (MISP, QRadar και pfSense)

Bash scripts μπορούν να χρησιμοποιηθούν για την αυτοματοποίηση της διασύνδεσης μεταξύ του MISP, του QRadar και του pfSense. Αυτή η μέθοδος παρέχει μεγάλη ευελιξία, καθώς τα scripts μπορούν να προσαρμοστούν για να ταιριάζουν με τις συγκεκριμένες ανάγκες του περιβάλλοντος ασφαλείας.

Τα scripts μπορούν να ανακτούν IOCs από το MISP και να τα προωθούν στο QRadar για ανάλυση ή στο pfSense για την ενημέρωση των κανόνων firewall.

Ένα παράδειγμα bash script θα μπορούσε να περιλαμβάνει τα εξής βήματα:

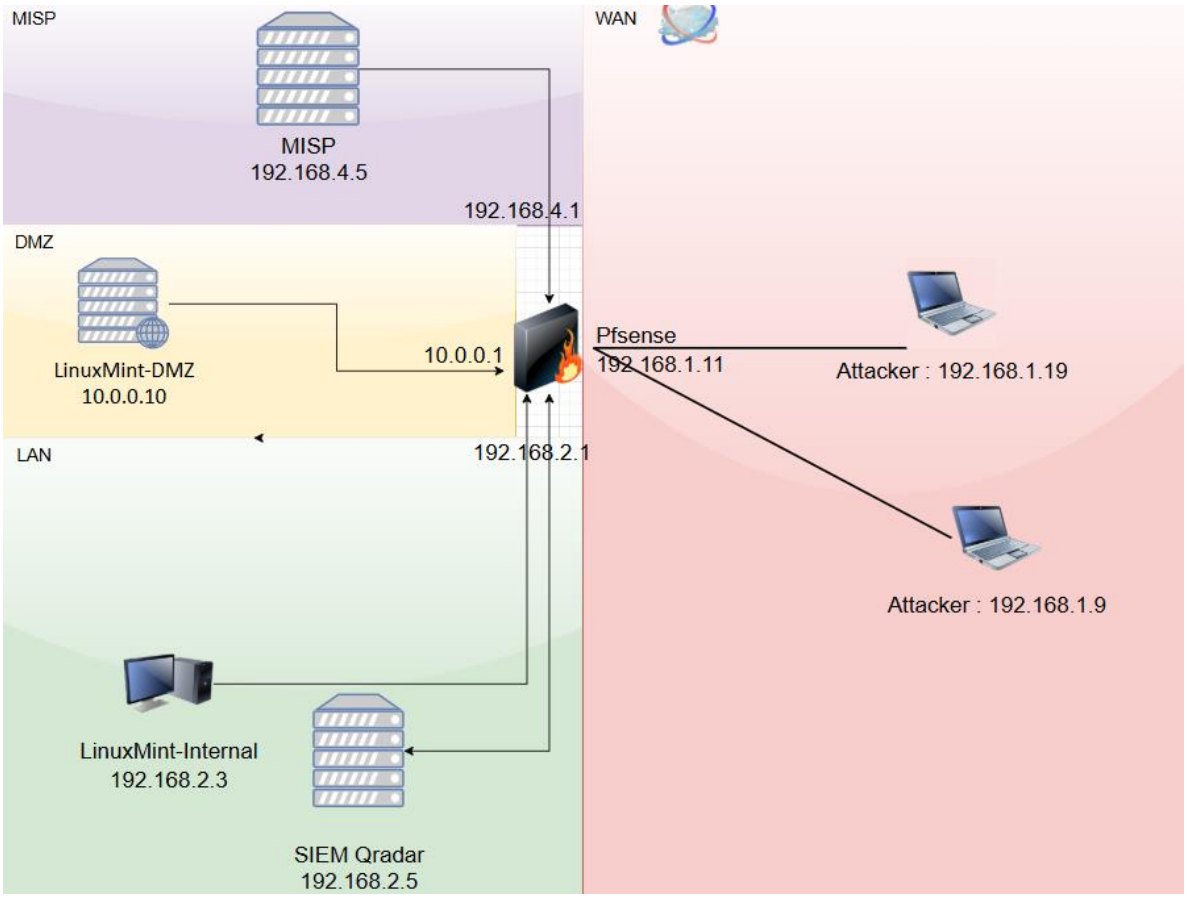
- Ανάκτηση των IOCs από το MISP μέσω των API.
- Διαμόρφωση των IOCs σε κατάλληλη μορφή για το QRadar.
- Αποστολή των IOCs στο QRadar μέσω API ή αρχείων καταγραφής.
- Ενημέρωση των κανόνων του pfSense με τους IOCs για την άμεση απόκρισή τους σε νέες απειλές.

3. Εγκατάσταση εργαστηριακού περιβάλλοντος

Σε αυτό το κεφάλαιο, περιγράφουμε τη μεθοδολογία που χρησιμοποιήθηκε για τη δημιουργία του εργαστηριακού περιβάλλοντος για τη συνολική αξιολόγηση των τεχνολογιών ασφάλειας δικτύου. Το εργαστηριακό περιβάλλον σχεδιάστηκε για να προσομοιώνει ένα πραγματικό δίκτυο με διαφορετικά στοιχεία όπως ένα σύστημα με δικτυακές ζώνες WAN, LAN, DMZ και SIEM Monitor και MISP.

3.1 Προεπισκόπηση Δικτύου

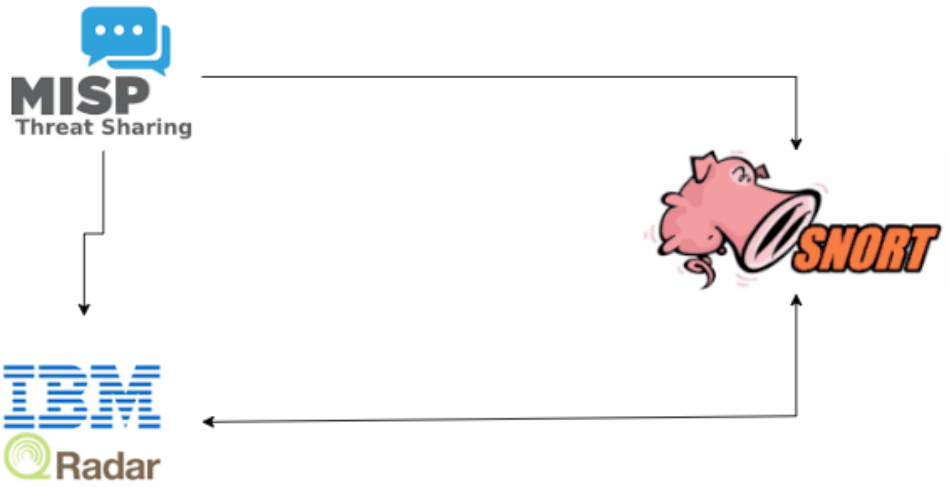
Είναι σημαντικό να παρουσιάσουμε μια επισκόπηση της τοπολογίας του δικτύου και του περιβάλλοντος που δημιουργήθηκε για την πειραματική εγκατάσταση. Ο σχεδιασμός του δικτύου ενσωματώνει μια ολοκληρωμένη σειρά τεχνολογιών ασφαλείας που στοχεύουν στην προστασία του δικτύου από πιθανές απειλές και επιθέσεις.



Εικόνα 9 Προεπίσκοπηση Δικτύου

3.2 Προεπισκόπηση διασυνδέσεων

Στην παράγραφο παρουσιάζεται μία γραφική απεικόνιση των διασυνδέσεων μεταξύ των συστημάτων MISP, QRadar και Snort. Η ροή των δεδομένων ξεκινά από το MISP, όπου οι δείκτες απειλής (IOCs) αποστέλλονται στο QRadar για ανάλυση και παρακολούθηση. Παράλληλα, οι ίδιες πληροφορίες αποστέλλονται στο Snort για ενεργό αποκλεισμό των IPs. Η σύνδεση μεταξύ QRadar και Snort διασφαλίζει ότι οι κακόβουλες δραστηριότητες που αναγνωρίζονται από το QRadar, μπορούν επίσης να φιλτραριστούν και να αποκλειστούν από το Snort.



Εικόνα 10 Προεπισκόπηση Διασυνδέσεων

3.3 Virtualization και διαμόρφωση δικτύου

Το εργαστηριακό περιβάλλον δημιουργήθηκε χρησιμοποιώντας τεχνολογίες Virtualization, επιτρέποντας ευέλικτες και επεκτάσιμες διαμορφώσεις δικτύου. Χρησιμοποιήθηκαν εικονικές μηχανές για την προσομοίωση διαφόρων συσκευών δικτύου, όπως το pfSense ως τείχος προστασίας και δρομολογητής, το Nginx ως διακομιστής ιστού στο DMZ, το Snort ως IDS, το Squid ως διακομιστής μεσολάβησης , ένα SIEM Qradar και ένα περιβάλλον MISP.

3.4 Διευθύνσεις δικτύου

Η τοπολογία δικτύου σχεδιάστηκε προσεκτικά ώστε να αντιπροσωπεύει την αρχιτεκτονική δικτύου ενός τυπικού οργανισμού. Στη διεπαφή WAN του pfSense εκχωρήθηκε η διεύθυνση IP 192.168.1.11 και το LAN χωρίστηκε σε τρεις εσωτερικές διεπαφές με διευθύνσεις IP 192.168.2.1, 10.0.0.1 και 192.168.4.1.

3.5 Αποστολή Logs σε SIEM Qradar

Για να συγκεντρωθεί η παρακολούθηση και η ανάλυση αρχείων καταγραφής, ένα σύστημα IBM QRadar SIEM ενσωματώθηκε στο δίκτυο. Όλες οι συσκευές εντός του εργαστηριακού περιβάλλοντος, συμπεριλαμβανομένου του τείχους προστασίας, των LINUX συσκευών, του IDS, του Proxy Server και του WAF, διαμορφώθηκαν ώστε να στέλνουν τα αρχεία καταγραφής τους στο σύστημα QRadar SIEM στη διεύθυνση IP 192.168.2.5. Σε συνέχεια το MISP εκτός από τα αρχεία καταγραφής ρυθμίστηκε να στέλνει με την σειρά του και IOCs. Αυτό επέτρεψε την ολοκληρωμένη παρακολούθηση συμβάντων και ανάλυση σε πραγματικό χρόνο των συμβάντων ασφαλείας.

3.6 Σχεδιασμός τοπολογίας δικτύου

Σε αυτή την ενότητα, θα περιγράψουμε τον σχεδιασμό τοπολογίας δικτύου που χρησιμοποιείται στο εργαστηριακό περιβάλλον. Η τοπολογία του δικτύου σχεδιάστηκε προσεκτικά για να αντιγράψει ένα

πραγματικό δίκτυο με διακριτά τμήματα, συμπεριλαμβανομένων των WAN, LAN και DMZ και MISP. Για να το πετύχουμε αυτό, χρησιμοποιήσαμε εικονικές μηχανές για την προσομοίωση διαφόρων συσκευών δικτύου και χρησιμοποιήσαμε το pfSense ως κεντρικό τείχος προστασίας και δρομολογητή.

3.6.1 Διαμόρφωση pfSense

Λήψη του pfSense ISO

1. Μεταβείτε στον ιστότοπο του pfSense (https://www.pfsense.org/) και κατεβάστε την εικόνα ISO του pfSense που είναι κατάλληλη για την αρχιτεκτονική του συστήματός σας (π.χ. 64-bit ή 32-bit).
2. Δημιουργήστε μια νέα εικονική μηχανή στο VirtualBox

2.1. Ανοίξτε το VirtualBox και κάντε κλικ στο " New" για να δημιουργήσετε μια νέα εικονική μηχανή.

2.2. Εισαγάγετε ένα όνομα για την εικονική μηχανή (π.χ. pfSense) και επιλέξτε τον τύπο ως "BSD".

2.3. Επιλέξτε την έκδοση ως "FreeBSD (64-bit)" εάν κατεβάσατε την έκδοση 64-bit του pfSense. Διαφορετικά, επιλέξτε "FreeBSD (32-bit)."

2.4. Εκχωρήστε μνήμη (RAM) στην εικονική μηχανή. Συνιστάται τουλάχιστον 1 GB για το pfSense.

2.5. Επιλέξτε " Create a virtual hard disk now" και κάντε κλικ στο " Create".

3. Δημιουργήστε έναν εικονικό σκληρό δίσκο

3.1. Επιλέξτε την επιλογή "VDI (VirtualBox Disk Image)" για τον τύπο αρχείου του σκληρού δίσκου.

3.2. Επιλέξτε " Dynamic allocation" για τον τύπο αποθήκευσης.

3.3. Επιλέξτε το μέγεθος του εικονικού σκληρού δίσκου. Συνιστώνται 8 GB ή περισσότερα για το pfSense.

Κάντε κλικ στο " Create" για να δημιουργήσετε τον εικονικό σκληρό δίσκο.

4. Διαμορφώστε τις ρυθμίσεις εικονικής μηχανής

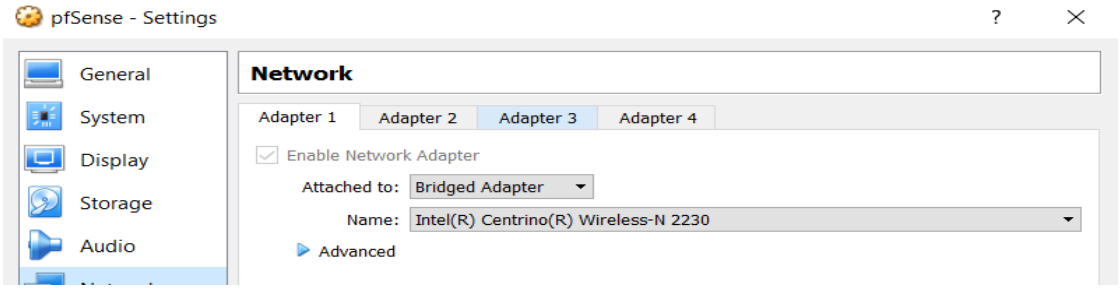
4.1. Επιλέξτε τη νέα εικονική μηχανή που δημιουργήθηκε στο VirtualBox και κάντε κλικ στο " Settings".

4.2. Μεταβείτε στην καρτέλα "Storage" και προσθέστε την εικόνα ISO του pfSense στην εικονική μονάδα CD/DVD.

4.3. Μεταβείτε στην καρτέλα " Network":

○ Διεπαφή WAN (1):

Στη διεπαφή WAN του pfSense εκχωρήθηκε Bridged Adapter με όνομα αυτό της κάρτας δικτύου.



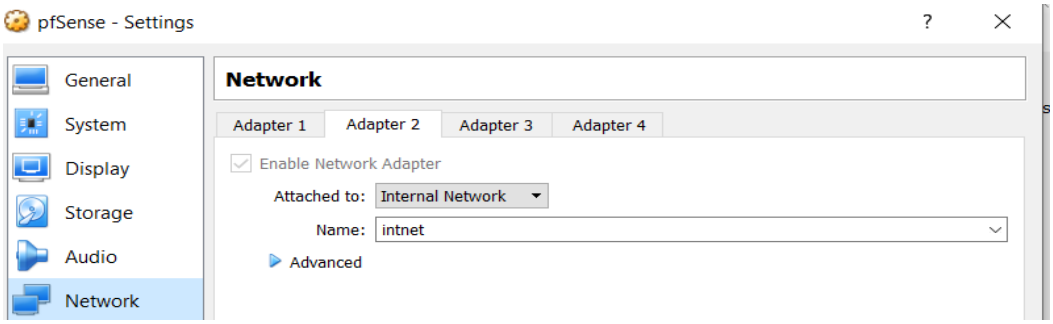
Εικόνα 11 Ρύθμιση WAN Διεπαφής στο Virtual Box

- Διεπαφές LAN (2,3,4):

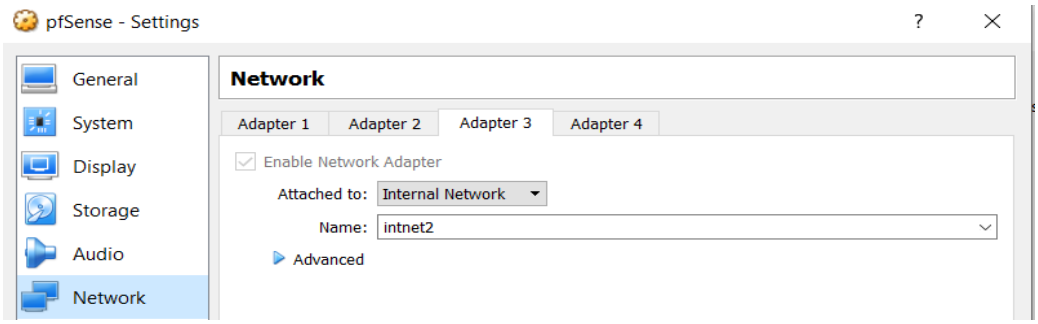
Διεπαφή 2 ,για το δίκτυο Internal Network με όνομα intnet.

Διεπαφή 3 ,για το δίκτυο Internal Network με όνομα intnet2.

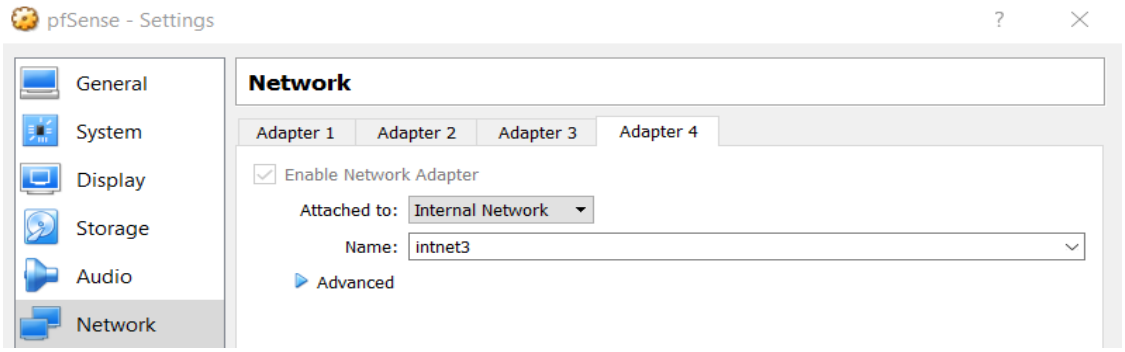
Διεπαφή 4 ,για το δίκτυο Internal Network με όνομα intnet3.



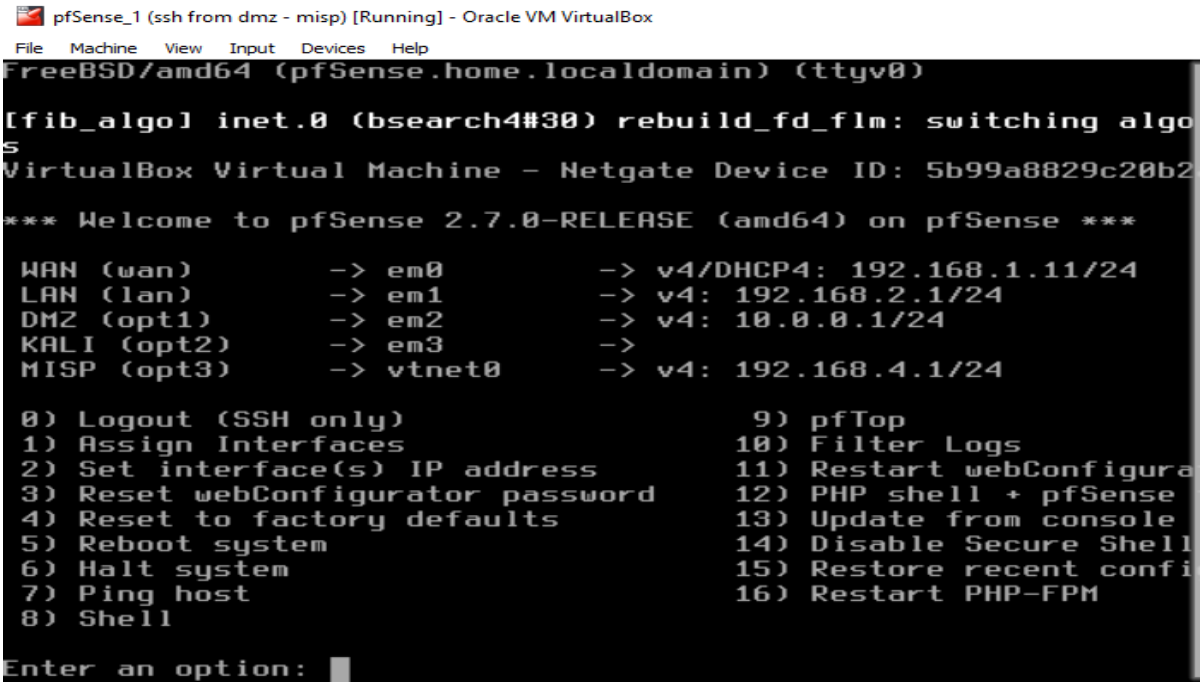
Εικόνα 12 Ρύθμιση LAN interface στο Virtual Box



Εικόνα 13 Ρύθμιση DMZ interface στο Virtual Box



Εικόνα 14 Ρύθμιση MISP interface στο Virtual Box



Εικόνα 15 Pfsense CLI Enter Menu

Εγκατάσταση pfSense

1. Εκκινήστε την εικονική μηχανή. Θα εκκινήσει από την εικόνα ISO του pfSense.
2. Στο μενού εκκίνησης, επιλέξτε " Install".
3. Ακολουθήστε τις οδηγίες που εμφανίζονται στην οθόνη για να εγκαταστήσετε το pfSense
4. Επιλέξτε " Accept these settings" όταν σας ζητηθεί.
5. Επιλέξτε τον " Standard Kernel" όταν σας ζητηθεί.
6. Διαχωρίστε το δίσκο (Χρησιμοποιήστε ολόκληρο τον δίσκο εάν έχετε διαθέσει αρκετό χώρο).
7. Αφού ολοκληρωθεί η εγκατάσταση, αφαιρέστε το pfSense ISO από την εικονική μονάδα CD/DVD και επανεκκινήστε το VM.

Αρχική Διαμόρφωση pfSense

1. Μετά την επανεκκίνηση του VM, θα δείτε ένα μενού στο οποίο θα δείχνει τις IP που εχουν εκχωρηθεί στις διεπαφές.
2. Από τον υπολογιστή που κάνατε εγκατάσταση το pfsense πληκτρολογήστε σε έναν web browser την διεύθυνση WAN του pfsense προκειμένου να εισέλθετε στο GUI του τείχου προστασίας. Στην δική μας περίπτωση http://192.168.1.11.
3. Κάντε σύνδεση με username Admin και κωδικό pfsense
4. Στην συνέχεια ακολουθούν μερικά βήματα διαμόρφωση του pfsense.
5. Εκχωρήστε ως Primary DNS Server 8.8.8.8.

6. Ορισμός διεύθυνσης IP WAN: Εάν χρησιμοποιείτε DHCP, το pfSense θα λάβει αυτόματα μια διεύθυνση IP από το δίκτυό σας. Διαφορετικά, ορίστε μια στατική διεύθυνση IP για τη διεπαφή WAN.
7. Ορισμός διεύθυνσης IP LAN: Εκχωρήστε τη διεύθυνση IP 192.168.2.1 για τη διεπαφή LAN.
8. Ολοκληρώστε την υπόλοιπη αρχική ρύθμιση, συμπεριλαμβανομένης της ρύθμισης του κωδικού πρόσβασης διαχειριστή και της επιλογής άλλων προαιρετικών διαμορφώσεων, όπως απαιτείται.

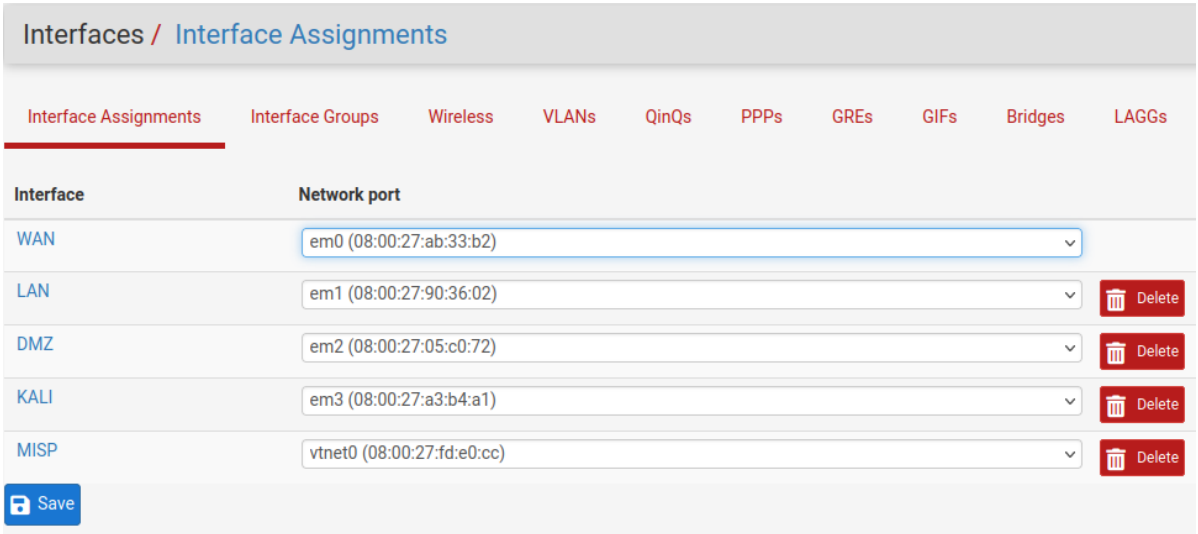
Εκχώρηση Διεπαφών στο pfSense

Στο βήμα "Εκχώρηση διεπαφών", θα δείτε τις διαθέσιμες διεπαφές δικτύου που εντοπίζονται από το pfSense. Μετεβείτε στην καρτέλα Interfaces και κάντε κλικ στην επιλογή Interface Assignment.

Αντιστοιχίστε κάθε διεπαφή στο κατάλληλο τμήμα δικτύου:

- WAN: Εκχωρήστε τον κατάλληλο προσαρμογέα δικτύου ως διεπαφή WAN και διαμορφώστε τον με τη διεύθυνση IP που παρέχεται από τον ISP σας (π.χ. 192.168.1.11).
- LAN: Αντιστοιχίστε έναν άλλο προσαρμογέα δικτύου ως διεπαφή LAN και διαμορφώστε τον με τη διεύθυνση IP 192.168.2.1 και τη μάσκα υποδικτύου (π.χ. 255.255.255.0).
- DMZ: Εκχωρήστε έναν τρίτο προσαρμογέα δικτύου ως διεπαφή DMZ και διαμορφώστε τον με τη διεύθυνση IP 10.0.0.1 και τη μάσκα υποδικτύου (π.χ. 255.255.255.0).
- MISP: Αντιστοιχίστε έναν άλλο προσαρμογέα δικτύου ως διεπαφή MISP και διαμορφώστε τον με τη διεύθυνση IP 192.168.4.1 και τη μάσκα υποδικτύου (π.χ. 255.255.255.0).

Αποθηκεύστε τις αναθέσεις και προχωρήστε με την αρχική ρύθμιση του pfSense.

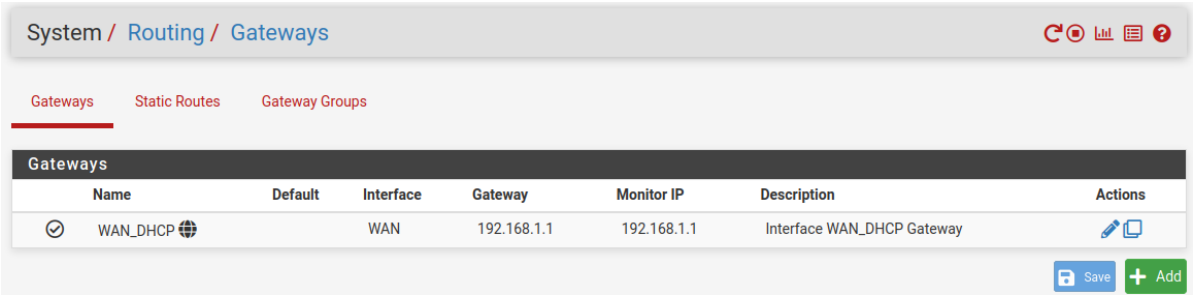


Εικόνα 16 Εκχώρηση Διεπαφών στο pfsense

Διαμορφώστε την Προεπιλεγμένη Πύλη για τη Διεπαφή WAN

1. Μεταβείτε στο "System" > "Routing" > "Gateways".
2. Δημιουργήστε μια νέα πύλη και ορίστε τη διεύθυνση πύλης στη διεύθυνση IP που παρέχεται από τον ISP σας για τη διεπαφή WAN.

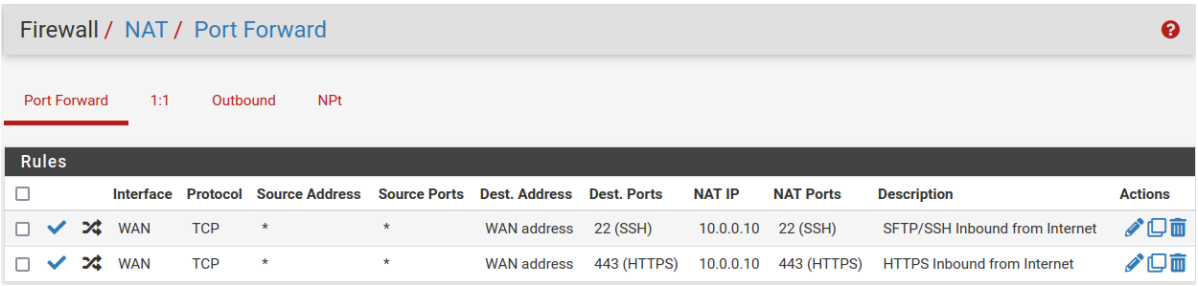
Αποθηκεύστε τις ρυθμίσεις της πύλης.



Εικόνα 17 Διαμόρφωση προεπιλεγμένης πύλης για τη διεπαφή WAN

Ενεργοποίηση Κανόνων NAT

1. Μεταβείτε στο "Firewall" > "NAT" > "Outbound" .
2. Επιλέξτε "Automatic Outbound NAT" και αποθηκεύστε τις ρυθμίσεις.
3. Μεταβείτε στο "Firewall" > "NAT" > "Port Forward"
4. Προσθέστε τους 3 κανόνες
   - Όλες οι συνδέσεις στην πόρτα 443 του WAN interface να γίνονται redirect στο Nginx web service του 10.0.0.10
   - Όλες οι συνδέσεις στην πόρτα 22 του LAN interface να γίνονται redirect στο Linux Mint device10.0.0.10



Εικόνα 18 Διαμόρφωση NAT Port Forward

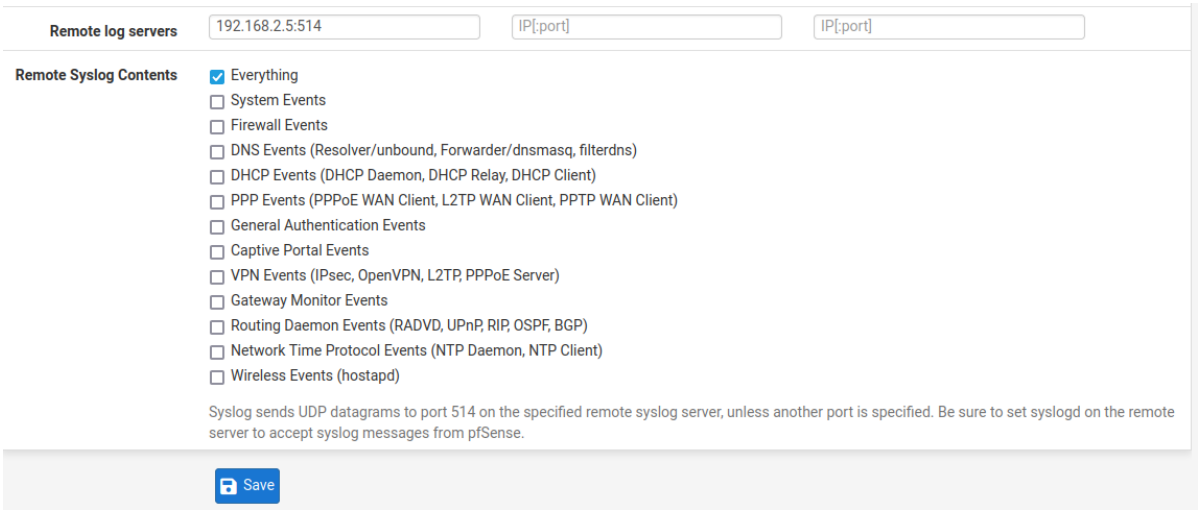
Προσθήκη DNS 8.8.8.8

1. Στη διεπαφή ιστού pfSense, κάντε κλικ στο «System» στο επάνω μενού και, στη συνέχεια, επιλέξτε «General Setup» από το αναπτυσσόμενο μενού.
2. Στη σελίδα " General Setup ", κάντε κύλιση προς τα κάτω στην ενότητα "Settings Server DNS".
3. Στο πεδίο "Server DNS", προσθέστε τη διεύθυνση IP 8.8.8.8 στη λίστα των διακομιστών DNS. Μπορείτε επίσης να προσθέσετε πολλούς διακομιστές DNS διαχωρίζοντάς τους με κόμμα (π.χ., 8.8.8.8, 8.8.4.4).
4. Κάντε κύλιση προς τα κάτω στο κάτω μέρος της σελίδας και κάντε κλικ στο κουμπί "Save" για να εφαρμόσετε τις αλλαγές.

Μετά την αποθήκευση των ρυθμίσεων, ο διακομιστής DNS 8.8.8.8 θα προστεθεί στη διαμόρφωση DNS του pfSense και θα χρησιμοποιηθεί για ανάλυση DNS στο δίκτυο.

Ρύθμιση Αποστολής Logs σε SIEM Qradar

1. Κάντε κλικ στην " Status" στο επάνω μενού και, στη συνέχεια, επιλέξτε "System Logs" από το αναπτυσσόμενο μενού.
2. Στη σελίδα "System Logs", κάντε κλικ στην καρτέλα "Settings".
3. Κάντε κύλιση προς τα κάτω στην ενότητα "Remote Logging Options".
4. Επιλέξτε το πλαίσιο "Enable Remote Logging" για να ενεργοποιήσετε την αποστολή αρχείων καταγραφής σε έναν απομακρυσμένο διακομιστή.
5. Στο πεδίο "Remote log servers", εισαγάγετε τη διεύθυνση IP ή το όνομα κεντρικού υπολογιστή του διακομιστή απομακρυσμένης καταγραφής. Χρησιμοποιήστε τη διεύθυνση IP εάν η ανάλυση DNS δεν έχει ρυθμιστεί ή είναι αναξιόπιστη.
6. Επιλέξτε το "Remote log protocol" ως "UDP" ή "TCP" με βάση τις προτιμήσεις σας και τη διαμόρφωση δικτύου. Το UDP είναι γενικά ταχύτερο, αλλά δεν παρέχει επιβεβαίωση λήψης μηνύματος, ενώ το TCP είναι αξιόπιστο, αλλά μπορεί να εισάγει κάποια καθυστέρηση.
7. Ρυθμίστε τη "Remote log port" στον κατάλληλο αριθμό θύρας για τον διακομιστή syslog στον απομακρυσμένο διακομιστή. Η προεπιλεγμένη θύρα για το syslog είναι 514.
8. Κάντε κλικ στο κουμπί "Save" για να εφαρμόσετε τις αλλαγές.



Εικόνα 19 Ρύθμιση Αποστολής Logs σε SIEM

Τρόπος Δημιουργίας Κανόνων στο pfSense

1. Κάντε κλικ στο "Firewall" στο επάνω μενού και επιλέξτε "Rules" από το αναπτυσσόμενο μενού.
2. Επιλέξτε την καρτέλα διεπαφής WAN.
3. Κάντε κλικ στο κουμπί "Add" για να δημιουργήσετε έναν νέο κανόνα.
4. Διαμορφώστε τις ρυθμίσεις κανόνων με βάση τις παρεχόμενες πληροφορίες, συμπεριλαμβανομένων της πηγής, του προορισμού, του πρωτοκόλλου και των θυρών.
5. Επιλέξτε την κατάλληλη ενέργεια για τον κανόνα (Block, Pass, Reject, κ.λπ.).
6. Κάντε κλικ στο κουμπί "Save" για να εφαρμόσετε τον κανόνα.

3.6.2 Εγκατάσταση/Διαμόρφωση συστήματος ανίχνευσης εισβολής (IDS) Snort

Εγκαταστήστε το πακέτο Snort στο pfSense

1. Μεταβείτε στο "System" > "Package Manager".
2. Στην καρτέλα "Available Packages", αναζητήστε το "snort" στη γραμμή αναζήτησης.
3. Κάντε κλικ στο κουμπί "Install" δίπλα στο "Snort" για να εγκαταστήσετε το πακέτο Snort.

Διαμόρφωση Διεπαφών Snort

1. Μετά την εγκατάσταση του Snort, μεταβείτε στις " Services" > "Snort" από το επάνω μενού.
2. Στην καρτέλα " Global Settings", επιλέξτε τις διεπαφές Snort (π.χ. WAN, LAN, DMZ) όπου θέλετε να ενεργοποιήσετε τον εντοπισμό εισβολής. Κάντε κλικ στο "Save".

Λήψη Κανόνων Snort

1. Στη σελίδα ρυθμίσεων Snort, μεταβείτε στην καρτέλα " Updates".
2. Κάντε κλικ στο κουμπί "Download Rules" για να πραγματοποιήσετε λήψη των πιο πρόσφατων κανόνων Snort που θα χρησιμοποιηθούν για τον εντοπισμό εισβολής.

Ενεργοποιήστε το Snort στις επιλεγμένες διεπαφές

1. Στην καρτέλα " Interface Settings", κάντε κύλιση προς τα κάτω στις διεπαφές Snort που επιλέξατε νωρίτερα.
2. Επιλέξτε το πλαίσιο " Enable" για κάθε διεπαφή όπου θέλετε το Snort να παρακολουθεί την κυκλοφορία.
3. Κάντε κλικ στο " Save".

Διαμόρφωση καταγραφής στα αρχεία καταγραφής συστήματος

1. Στην καρτέλα " Logging Settings", κάντε κύλιση προς τα κάτω στην ενότητα " Alert System Log Settings".
2. Επιλέξτε το πλαίσιο " Log alerts to the system log" για να ενεργοποιήσετε το Snort να στέλνει ειδοποιήσεις στο αρχείο καταγραφής συστήματος pfSense.
3. Προαιρετικά, μπορείτε να επιλέξετε το επίπεδο σοβαρότητας για τις ειδοποιήσεις Snort (π.χ. Alert, Critical, Error).
4. Κάντε κλικ στο " Save".

Ξεκινήστε το Snort

1. Αφού ολοκληρώσετε τη διαμόρφωση, επιστρέψτε στην καρτέλα " General Settings".
2. Κάντε κλικ στο κουμπί " Start" δίπλα στο "Snort".
3. Το Snort θα ξεκινήσει να εκτελείται και να παρακολουθεί τις επιλεγμένες διεπαφές για πιθανές εισβολές.

Προβολή Ειδοποιήσεων Snort στα Αρχεία Καταγραφής Συστήματος pfSense

1. Για να προβάλετε ειδοποιήσεις Snort, μεταβείτε στο "Status" > "System Logs".
2. Επιλέξτε την καρτέλα "Snort" για να φιλτράρετε τα αρχεία καταγραφής ειδικά για ειδοποιήσεις Snort.
3. Εδώ, μπορείτε να δείτε τις καταγεγραμμένες ειδοποιήσεις και το επίπεδο σοβαρότητάς τους.

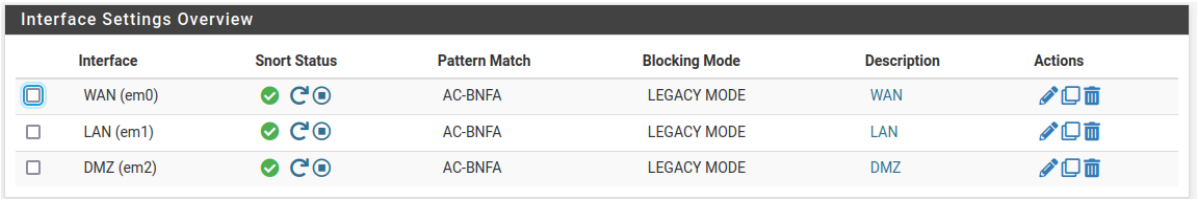
Δημιουργία Custom Rule

1. Μεταβείτε " Services" και, στη συνέχεια, επιλέξτε "Snort".

2. Κάντε κλικ στην καρτέλα " Interfaces".
3. Κάντε κλικ στο κουμπι ‘’Edit" του WAN interface.
4. Κάντε κλικ στο ‘’WAN Rules’’ και από το ‘’Category Selection’’ επιλέξτε το το **custom_rules**
5. Στο πεδίο ‘’Defines Custom Rules πληκτρολογήστε τους κανόνες

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (msg:"External HTTP Flood Attack Detected"; flow: stateless; content:"GET"; http_method; detection_filter: track by_src, count 15, seconds 30; sid: 1000003; rev:1;)


alert tcp $EXTERNAL_NET any -> $HOME_NET 22 (msg:"SSH Brute Force Attack Detected"; flow: stateless; content:"SSH-"; depth: 4; detection_filter: track by_src, count 5, seconds 60; sid: 1000002; rev:1;)
```

6. Κάντε κλικ ‘’Save’’



Εικόνα 20 Διεπαφές με Snort

Δημιουργία Custom Rule

Για να αποστείλει το **Snort** τα alerts στο **QRadar** μέσω του **pfSense**, πρέπει να ενεργοποιηθεί η αποστολή ειδοποιήσεων στο σύστημα καταγραφής του firewall.

1. **Μετάβαση στο pfSense Web Interface** και άνοιγμα της καρτέλας **Snort Interfaces**.
2. Επιλογή του **WAN Interface** (ή του interface όπου είναι ενεργό το Snort).
3. Ενεργοποίηση της επιλογής **"Snort will send alerts to the firewall’s system log"**.
4. Επιβεβαίωση ότι το pfSense αποστέλλει τα logs μέσω **Remote Syslog** στο QRadar.

Log Source	Payload
Snort @ pfSense....	<161>1 2024-09-23T22:42:32.881416+03:00 pfSense.home.localdomain snort 72848 - - [128:1:2] (spp_ssh) Challenge-Response Overflow exploit [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 10.0.0.10:51244 -> 192.168.2.5:22
Snort @ pfSense....	<161>1 2024-09-23T22:42:18.108928+03:00 pfSense.home.localdomain snort 72848 - - [128:1:2] (spp_ssh) Challenge-Response Overflow exploit [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 10.0.0.10:58736 -> 192.168.2.5:22
Snort @ pfSense....	<161>1 2024-09-23T22:42:18.109168+03:00 pfSense.home.localdomain snort 72848 - - [128:1:2] (spp_ssh) Challenge-Response Overflow exploit [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 10.0.0.10:58736 -> 192.168.2.5:22
Snort @ pfSense....	<161>1 2024-09-23T22:42:18.108668+03:00 pfSense.home.localdomain snort 72848 - - [128:1:2] (spp_ssh) Challenge-Response Overflow exploit [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 10.0.0.10:58736 -> 192.168.2.5:22
Snort @ pfSense....	<161>1 2024-09-23T22:30:31.050941+03:00 pfSense.home.localdomain snort 72848 - - [128:1:2] (spp_ssh) Challenge-Response Overflow exploit [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 10.0.0.10:34250 -> 192.168.2.5:22
Snort @ pfSense....	<161>1 2024-09-23T22:30:31.049684+03:00 pfSense.home.localdomain snort 72848 - - [128:1:2] (spp_ssh) Challenge-Response Overflow exploit [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 10.0.0.10:34250 -> 192.168.2.5:22
Snort @ pfSense....	<161>1 2024-09-23T22:30:31.050663+03:00 pfSense.home.localdomain snort 72848 - - [128:1:2] (spp_ssh) Challenge-Response Overflow exploit [Classification: Attempted Administrator Privilege Gain] [Priority: 1] {TCP} 10.0.0.10:34250 -> 192.168.2.5:22

Εικόνα 21 Snort Logs στο Qradar

3.6.3 Εγκατάσταση/Διαμόρφωση Proxy Server – Squid.

Εγκαταστήστε το Squid Package στο pfSense

1. Μεταβείτε στο "System" > "Package Manager".
2. Στην καρτέλα " Available Packages", αναζητήστε το "squid" στη γραμμή αναζήτησης.
3. Κάντε κλικ στο κουμπί " Install" δίπλα στο "Squid" για να εγκαταστήσετε το πακέτο Squid.

Διαμόρφωση του Squid Proxy

1. Μετά την εγκατάσταση του Squid, μεταβείτε στις " Services" > "Squid Proxy" από το επάνω μενού.
2. Στην καρτέλα "General Settings", επιλέξτε το πλαίσιο "Enable Squid Proxy" για να ενεργοποιήσετε την υπηρεσία Squid.
3. Ορίστε την κατάλληλη διεπαφή για το Squid (π.χ. LAN, DMZ) από το αναπτυσσόμενο μενού " Interface (s) Proxy Server".
4. Κάντε κλικ στο " Save" για να εφαρμόσετε τις αλλαγές.

Διαμόρφωση Λιστών Ελέγχου Πρόσβασης (ACL)

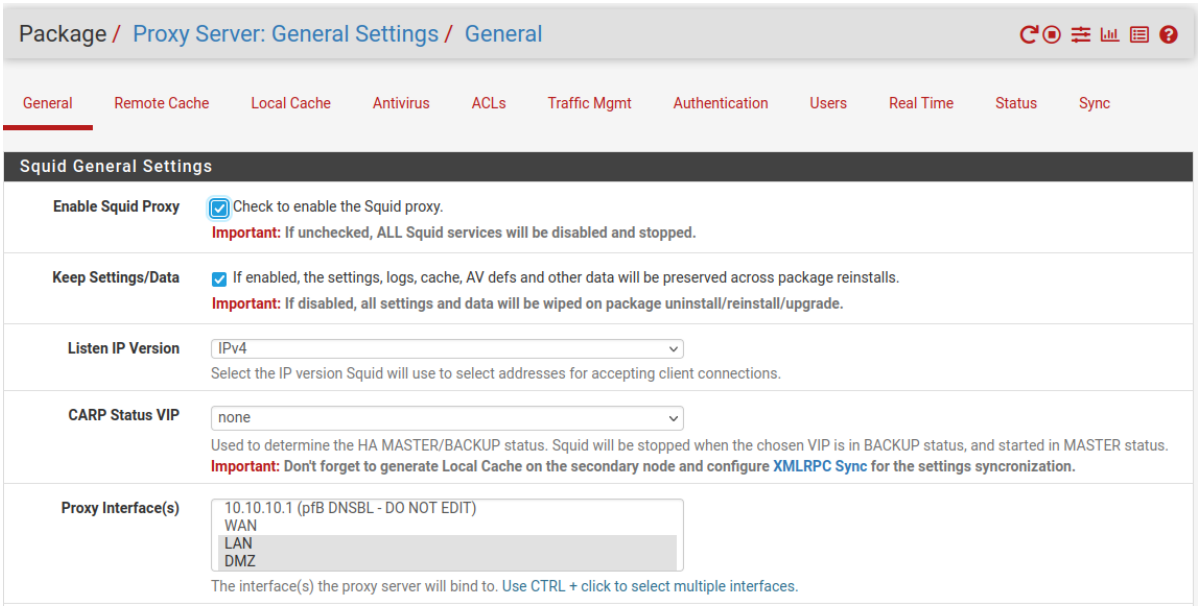
1. Στις ρυθμίσεις του Squid Proxy, μεταβείτε στην καρτέλα "ACLs".
2. Εδώ, μπορείτε να ορίσετε Λίστες ελέγχου πρόσβασης για να ελέγξετε σε ποιους πελάτες ή δίκτυα επιτρέπεται η πρόσβαση σε συγκεκριμένους πόρους Ιστού. Για παράδειγμα, μπορείτε να δημιουργήσετε ένα ACL για να επιτρέψετε ή να αρνηθείτε την πρόσβαση σε συγκεκριμένους ιστότοπους ή διευθύνσεις URL.
3. Κάντε κλικ στο "Save" για να αποθηκεύσετε τις διαμορφώσεις ACL.

Διαμόρφωση Καταγραφής στα Αρχεία Καταγραφής Συστήματος

1. Στις ρυθμίσεις του Squid Proxy, μεταβείτε στην καρτέλα "General Settings".
2. Κάντε κύλιση προς τα κάτω στην ενότητα "Logging Settings".
3. Επιλέξτε το πλαίσιο "Enable Access Logging" για να ενεργοποιήσετε την καταγραφή των αιτημάτων πρόσβασης Squid.
4. Επιλέξτε το πλαίσιο "Enable Reverse DNS Lookups in Access Logs" για να επιλύσετε τις διευθύνσεις IP σε ονόματα κεντρικών υπολογιστών στα αρχεία καταγραφής.
5. Κάντε κλικ στο " Save" για να εφαρμόσετε τις ρυθμίσεις καταγραφής.

Εκκίνηση του Squid Proxy

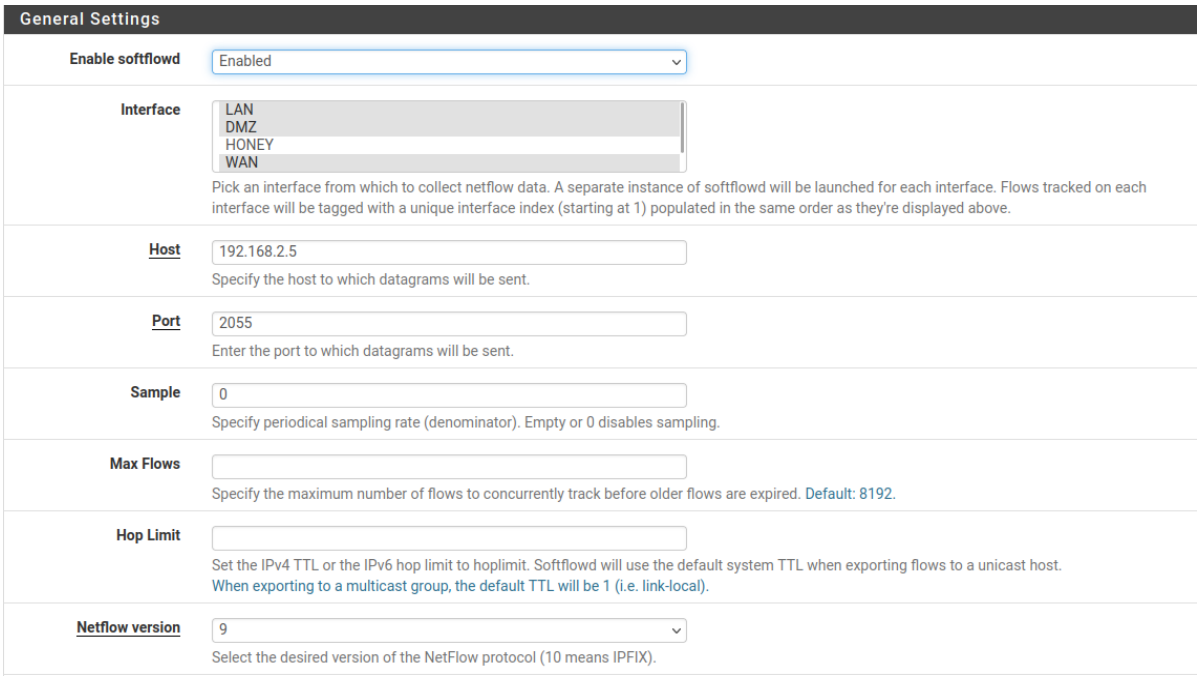
1. Αφού ολοκληρώσετε τη διαμόρφωση, επιστρέψτε στην καρτέλα "General Settings".
2. Κάντε κλικ στο κουμπί "Start" δίπλα στο "Squid" για να ξεκινήσει η υπηρεσία διακομιστή μεσολάβησης Squid.



Εικόνα 22 Ενεργοποίηση Squid Proxy

3.6.4 Εγκατάσταση/Διαμόρφωση Softflowd

1. Μεταβείτε στο "System" > "Package Manager".
2. Στην καρτέλα " Available Packages ", αναζητήστε το " Softflowd " και κάντε κλικ στο κουμπί " Install " δίπλα στο πακέτο ntopng.
3. Μετά την εγκατάσταση, μεταβείτε στις " Services " > " Softflowd ".
4. Επιλέξτε το πλαίσιο " Enable Softflowd " για να ενεργοποιήσετε την υπηρεσία.
5. Στο αναπτυσσόμενο μενού " Interface ", επιλέξτε τη διεπαφή από την οποία θέλετε να καταγράψετε δεδομένα ροής (π.χ. WAN ή LAN)
6. Ρυθμίστε τον " NetFlow Server " στη διεύθυνση IP του διακομιστή QRadar.
7. Δώστε την επιθυμητή " Port NetFlow" (συνήθως 2055 για UDP).
8. Κάντε κλικ στο "Save" για να εφαρμόσετε τις αλλαγές.



Εικόνα 23 Προεπισκόπηση Softflowd

3.6.5 Εγκατάσταση/Διαμόρφωση LinuxMint-Internal

Ρύθμιση Linux Mint

1. Κατεβάστε το ISO του Linux Mint από τον επίσημο ιστότοπο (https://linuxmint.com/download.php) και δημιουργήστε μια μονάδα USB ή DVD με δυνατότητα εκκίνησης.
2. Εισάγετε έναν Network Adapter Attached to Internal Network , **intnet**
3. Εκκινήστε τον υπολογιστή σας από το μέσο εγκατάστασης Linux Mint.
4. Ακολουθήστε τις οδηγίες που εμφανίζονται στην οθόνη για να εγκαταστήσετε το Linux Mint στον υπολογιστή σας.

Διαμόρφωση της Προώθησης Αρχείων Καταγραφής στο SIEM Qradar

1. Εντοπίστε το αρχείο διαμόρφωσης προώθησης αρχείων καταγραφής (π.χ. /etc/rsyslog.d/50-default.conf.
2. Επεξεργαστείτε το αρχείο χρησιμοποιώντας ένα πρόγραμμα επεξεργασίας κειμένου.
3. Προσθέστε την ακόλουθη γραμμή για να προωθήσετε τα αρχεία καταγραφής Kippo στο SIEM Qradar ***.* @192.168.2.5:514**
4. Αποθηκεύστε τις αλλαγές και βγείτε από το πρόγραμμα επεξεργασίας κειμένου.
5. Επανεκκινήστε την υπηρεσία Rsyslog για να εφαρμόσετε τις αλλαγές στη διαμόρφωση προώθησης αρχείων καταγραφής **sudo service rsyslog restart.**

Διαμόρφωση της Προώθησης Εκτελέσιμων Εντολών στο SIEM Qradar

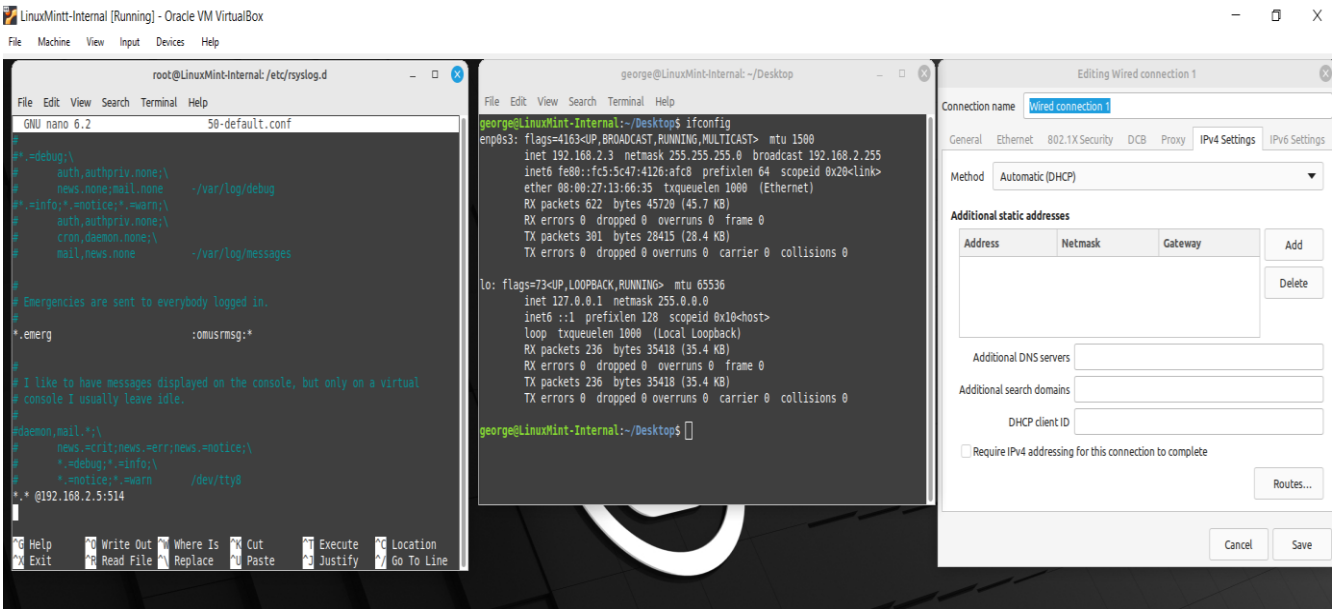
1. Εντοπίστε το αρχείο διαμόρφωσης προώθησης αρχείων καταγραφής (π.χ. /etc/rsyslog.d/50-default.conf.

2. Επεξεργαστείτε το αρχείο χρησιμοποιώντας ένα πρόγραμμα επεξεργασίας κειμένου.
3. Προσθέστε την ακόλουθη γραμμή “local6.* /var/log/syslog”
4. Αποθηκεύστε τις αλλαγές και βγείτε από το πρόγραμμα επεξεργασίας κειμένου.
5. Εντοπίστε το αρχείο /etc/bash.bashrc .
6. Επεξεργαστείτε το αρχείο χρησιμοποιώντας ένα πρόγραμμα επεξεργασίας κειμένου.
7. Προσθέστε την ακόλουθη συνάρτηση.

```
function log2syslog
{
    declare command
    command=$(fc -ln -1)

    logger -p local6.notice -t bash -i -- $USER : $SUDO_USER : $command

}

trap log2syslog DEBUG
```

Εικόνα 24 Log2syslog Συνάρτηση

8. Επανεκκινήστε την υπηρεσία Rsyslog για να εφαρμόσετε τις αλλαγές στη διαμόρφωση προώθησης αρχείων καταγραφής sudo service rsyslog restart.



Εικόνα 25 Προεπισκόπηση LinuxMint-Internal

3.6.6 Εγκατάσταση/Διαμόρφωση LinuxMint-DMZ

Ρύθμιση Linux Mint

1. Κατεβάστε το ISO του Linux Mint από τον επίσημο ιστότοπο (https://linuxmint.com/download.php) και δημιουργήστε μια μονάδα USB ή DVD με δυνατότητα εκκίνησης.
2. Εισάγετε έναν Network Adapter Attached to Internal Network , **intnet2**

3. Εκκινήστε τον υπολογιστή σας από το μέσο εγκατάστασης Linux Mint.
4. Ακολουθήστε τις οδηγίες που εμφανίζονται στην οθόνη για να εγκαταστήσετε το Linux Mint στον υπολογιστή σας.

Διαμόρφωση Διεπαφών Δικτύου

1. Μετά την εγκατάσταση του Linux Mint, συνδεθείτε στο περιβάλλον επιφάνειας εργασίας.
2. Κάντε κλικ στο εικονίδιο δικτύου στο δίσκο συστήματος και επιλέξτε “Edit Connections ".
3. Στο παράθυρο " Network Connections ", επιλέξτε την ενσύρματη ή ασύρματη σύνδεσή σας και κάντε κλικ στο κουμπί " Edit ".
4. Στην καρτέλα " Settings IPv4", επιλέξτε "Manual " από το αναπτυσσόμενο μενού Method.
5. Κάντε κλικ στο κουμπί "Add " για να προσθέσετε μια νέα διεύθυνση IP και εισαγάγετε τα ακόλουθα στοιχεία:

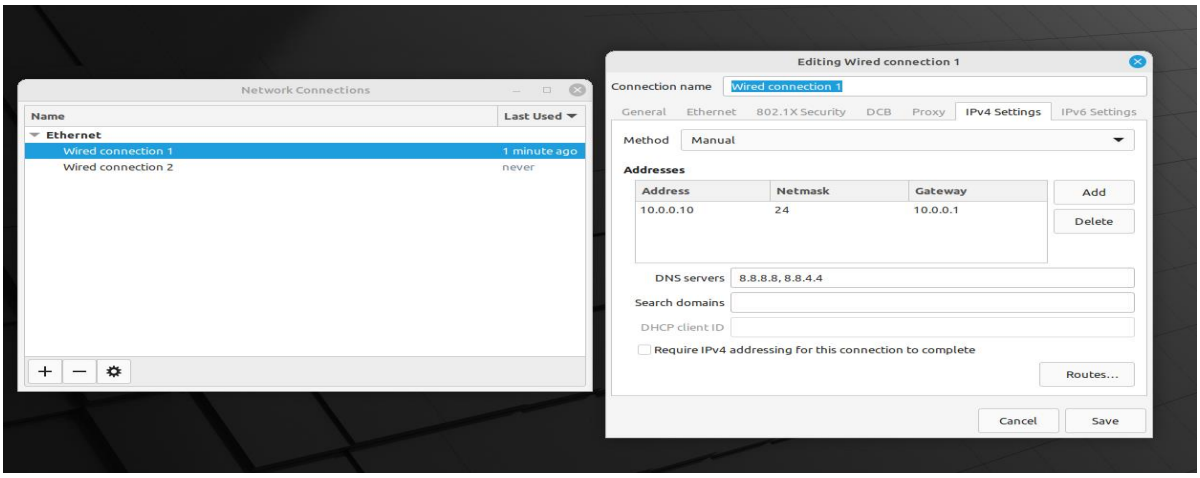
Διεύθυνση: 10.0.0.10

Μάσκα δικτύου: 255.255.255.0 (ή /24)

Πύλη: 10.0.0.1

Διακομιστές DNS: 8.8.8.8 (Google Public DNS) ή οι προτιμώμενοι διακομιστές DNS σας

Κάντε κλικ στο "Αποθήκευση" για να εφαρμόσετε τις ρυθμίσεις.



Εικόνα 26 Διαμόρφωση Διεπαφών DMZ

Διαμόρφωση της Προώθησης Αρχείων Καταγραφής στο SIEM Qradar

1. Εντοπίστε το αρχείο διαμόρφωσης προώθησης αρχείων καταγραφής (π.χ. /etc/rsyslog.d/30-rsyslog.conf).
2. Επεξεργαστείτε το αρχείο χρησιμοποιώντας ένα πρόγραμμα επεξεργασίας κειμένου.
3. Προσθέστε την ακόλουθη γραμμή για να προωθήσετε τα αρχεία καταγραφής Kippo στο SIEM Qradar ***.* @192.168.2.5:514**
4. Αποθηκεύστε τις αλλαγές και βγείτε από το πρόγραμμα επεξεργασίας κειμένου.
5. Επανεκκινήστε την υπηρεσία Rsyslog για να εφαρμόσετε τις αλλαγές στη διαμόρφωση προώθησης αρχείων καταγραφής **sudo service rsyslog restart.**

Ρύθμιση Web Server Nginx

1. Εγκατάσταση Nginx on Linux Mint:

sudo apt-get update

sudo apt-get install Nginx

2. Ξεκινήστε την υπηρεσία Nginx

sudo systemctl start Nginx

3. Ενεργοποιήστε το Nginx για εκκίνηση κατά την εκκίνηση

sudo systemctl enable Nginx

Διαμόρφωση της Προώθησης Αρχείων Καταγραφής NGIN στο SIEM Qradar

1. Επεξεργαστείτε το αρχείο διαμόρφωσης Nginx χρησιμοποιώντας ένα πρόγραμμα επεξεργασίας κειμένου (π.χ. Nano ή Vim)

sudo nano /etc/Nginx/Nginx.conf

2. Μέσα στο μπλοκ http, προσθέστε τις ακόλουθες γραμμές για να ρυθμίσετε τη μορφή αρχείου καταγραφής και να προωθήσετε τα αρχεία καταγραφής στο SIEM Qradar (αντικαταστήστε το 192.168.2.5 με την πραγματική διεύθυνση IP του SIEM σας)

access_log syslog:server=192.168.2.5:514 combined;

error_log syslog:server=192.168.2.5:514 error;

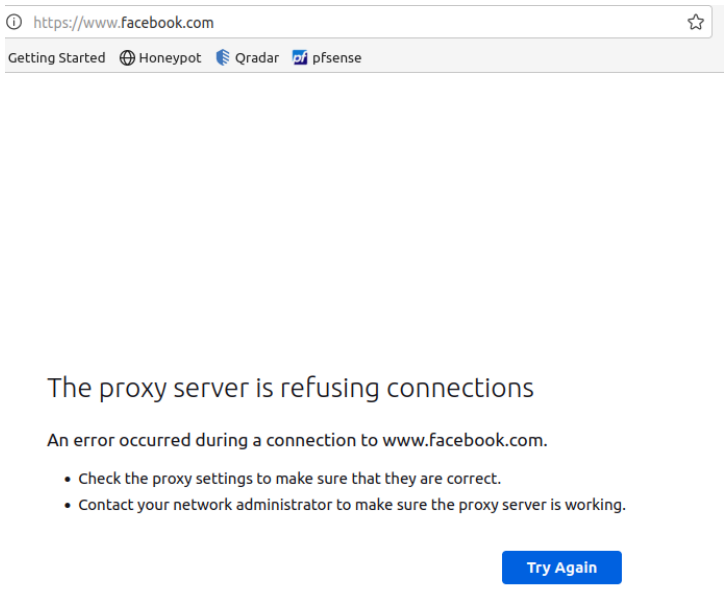
3. Αποθηκεύστε τις αλλαγές και βγείτε από το πρόγραμμα επεξεργασίας κειμένου.
4. Επαναλάβετε τη φόρτωση του Nginx για να εφαρμόσετε τις αλλαγές:

sudo systemctl reload Nginx

Ενεργοποίηση Squid Proxy στο Mozzila Firefox του LinuxMint-DMZ

Αποτέλεσμα αυτού θα είναι μη επιτυχή πρόσβαση στις ιστοσελίδες που έχουν καθοριστεί μέσω των ACL στο squid proxy που έχει εγκατασταθεί στο pfsense.

1. Ανοίξτε τον Mozilla Firefox στον υπολογιστή σας.
2. Κάντε κλικ στις τρεις οριζόντιες γραμμές στην επάνω δεξιά γωνία του προγράμματος περιήγησης για να ανοίξετε το μενού.
3. Επιλέξτε "Options" από το αναπτυσσόμενο μενού. Αυτό θα ανοίξει τη σελίδα Επιλογές Firefox.
4. Στην αριστερή πλαϊνή γραμμή, κάντε κλικ στο "General" για πρόσβαση στις Γενικές ρυθμίσεις.
5. Κάντε κύλιση προς τα κάτω στην ενότητα " Network Settings" και κάντε κλικ στο κουμπί " Settings ". Αυτό θα ανοίξει το παράθυρο διαλόγου Ρυθμίσεις σύνδεσης.
6. Στο παράθυρο διαλόγου Ρυθμίσεις σύνδεσης, επιλέξτε την επιλογή " Manually proxy configuration ".
7. Στο πεδίο "HTTP Proxy", πληκτρολογήστε τη διεύθυνση IP "192.168.2.1" και στο πεδίο "Port", πληκτρολογήστε "3128".
8. Επιλέξτε το πλαίσιο δίπλα στο "Also Use this proxy for HTTPS", εάν θέλετε να χρησιμοποιήσετε τον ίδιο διακομιστή μεσολάβησης και για πρωτόκολλο HTTPS.
9. Κάντε κλικ στο κουμπί "OK" για να αποθηκεύσετε τις ρυθμίσεις διακομιστή μεσολάβησης.



Εικόνα 27 Αποτέλεσμα ACL Blocklist Squid Proxy

Δημιουργία και Καταχώρηση Πιστοποιητικών στον Nginx Web Server

1. Χρησιμοποιούμε την εντολή «**sudo mkdir -p /etc/Nginx/ssl».** Αυτό δημιουργεί τον κατάλογο /etc/Nginx/ssl όπου θα αποθηκευτούν το κλειδί και το πιστοποιητικό.
2. Η παρακάτω εντολή χρησιμοποιείται για τη δημιουργία ενός ιδιωτικού κλειδιού. Χρησιμοποιεί τον αλγόριθμο RSA για τη δημιουργία του κλειδιού, ενώ το -aes256 εφαρμόζει κρυπτογράφηση στο ιδιωτικό κλειδί.

sudo openssl genpkey -algorithm RSA -out /etc/Nginx/ssl/selfsigned.key -aes256

3. Στην συνέχεια σημιουργουμε το CSR (Certificate Signing Request) το οποίο είναι απαραίτητο για τη δημιουργία του πιστοποιητικού και περιέχει τις πληροφορίες που χρειάζονται για το πιστοποιητικό.

sudo openssl req -new -key /etc/Nginx/ssl/selfsigned.key -out /etc/Nginx/ssl/selfsigned.csr

4. Η παρακάτω εντολή υπογράφει την αίτηση με το ιδιωτικό κλειδί που δημιουργήθηκε προηγουμένως και παράγει το πιστοποιητικό που ισχύει για 365 ημέρες.

sudo openssl x509 -req -days 365 -in /etc/Nginx/ssl/selfsigned.csr -signkey /etc/Nginx/ssl/selfsigned.key -out /etc/Nginx/ssl/selfsigned.crt

5. Κατά τη δημιουργία του CSR και την υπογραφή του πιστοποιητικού, ζητούνται διάφορες πληροφορίες, όπως:

Country Name (GR)

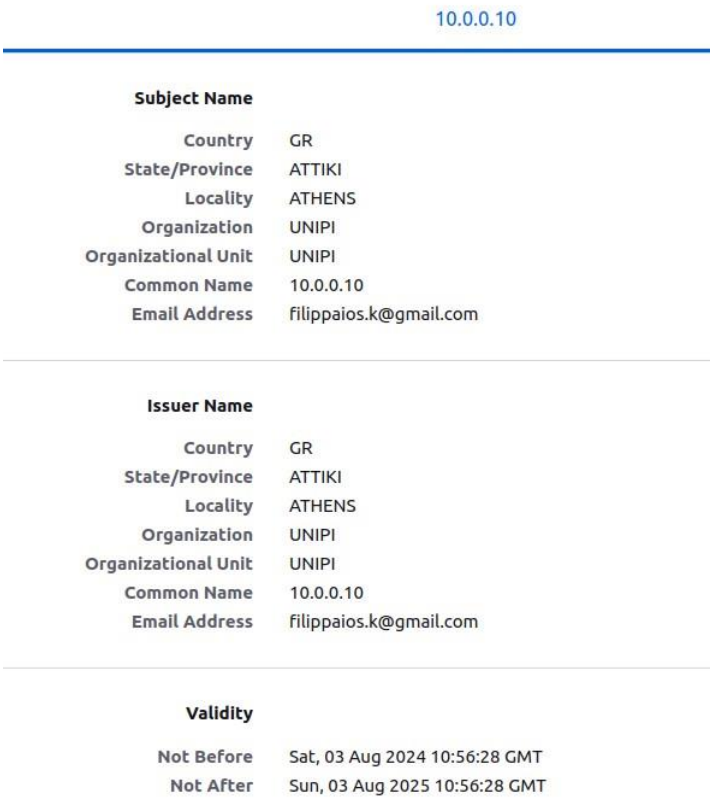
State (ATTIKI)

Locality Name (ATHENS)

Organization Name (UNIPI)

Common Name (10.0.0.10): Εδώ ορίζεται η διεύθυνση IP του server.

Email Address



Εικόνα 28 Πιστοποιητικό NGINX Server

Ασφαλή Διαμόρφωση Nginx Web Server (Security Headers)

1. Πρώτα, πηγαίνετε στο αρχείο ρυθμίσεων του Nginx που βρίσκεται στη διαδρομή **/etc/Nginx/sites-available/default**
2. Για να διασφαλίσετε ότι όλες οι αιτήσεις HTTP θα ανακατευθύνονται αυτόματα στο HTTPS, μπορείτε να προσθέσετε τις παρακάτω οδηγίες:

```
server {
  listen 80;
  server_name example.com www.example.com;
  return 301 https://$host$request_uri;
}
```

3. Ενεργοποιήστε την SSL σύνδεση στο server σας στη θύρα 443 (HTTPS). Αυτές οι οδηγίες δηλώνουν τη χρήση του αυτο-υπογεγραμμένου πιστοποιητικού και του ιδιωτικού κλειδιού που δημιουργήθηκαν στο προηγούμενο βήμα.

```
server {
```

```
    listen 443 ssl;
    server_name example.com www.example.com;
    ssl_certificate /etc/Nginx/ssl/selfsigned.crt;
    ssl_certificate_key /etc/Nginx/ssl/selfsigned.key;
}
```

4. Για να βελτιώσετε την ασφάλεια, προσθέστε πρόσθετες ρυθμίσεις SSL:

```
ssl_protocols TLSv1.2 TLSv1.3;
ssl_prefer_server_ciphers on;
ssl_ciphers "ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305";
ssl_session_cache shared:SSL:10m;
ssl_session_timeout 10m;
```

ssl_protocols: Ορίζει ποια πρωτόκολλα SSL/TLS θα υποστηρίζονται. Συνιστάται η χρήση TLS 1.2 και TLS 1.3.

ssl_prefer_server_ciphers: Προτιμά τις κρυπτογραφήσεις που επιλέγονται από τον διακομιστή.

ssl_ciphers: Ορίζει ασφαλείς αλγόριθμους κρυπτογράφησης.

ssl_session_cache: Ορίζει το μέγεθος της προσωρινής μνήμης των συνεδριών SSL.

ssl_session_timeout: Ορίζει το χρόνο λήξης των συνεδριών SSL.

5. Για να προσθέσετε ασφαλείς κεφαλίδες HTTP, μπορείτε να χρησιμοποιήσετε τις ακόλουθες οδηγίες:

```
add_header X-Frame-Options "SAMEORIGIN" always;
add_header X-XSS-Protection "1; mode=block" always;
add_header X-Content-Type-Options "nosniff" always;
add_header Referrer-Policy "no-referrer-when-downgrade" always;
add_header Content-Security-Policy "default-src 'self'; script-src 'self'; object-src 'none';" always;
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;
```

X-Frame-Options: Προστατεύει από επιθέσεις clickjacking, επιτρέποντας την ενσωμάτωση της σελίδας μόνο από την ίδια προέλευση.

X-XSS-Protection: Ενεργοποιεί την προστασία κατά των επιθέσεων Cross-Site Scripting (XSS).

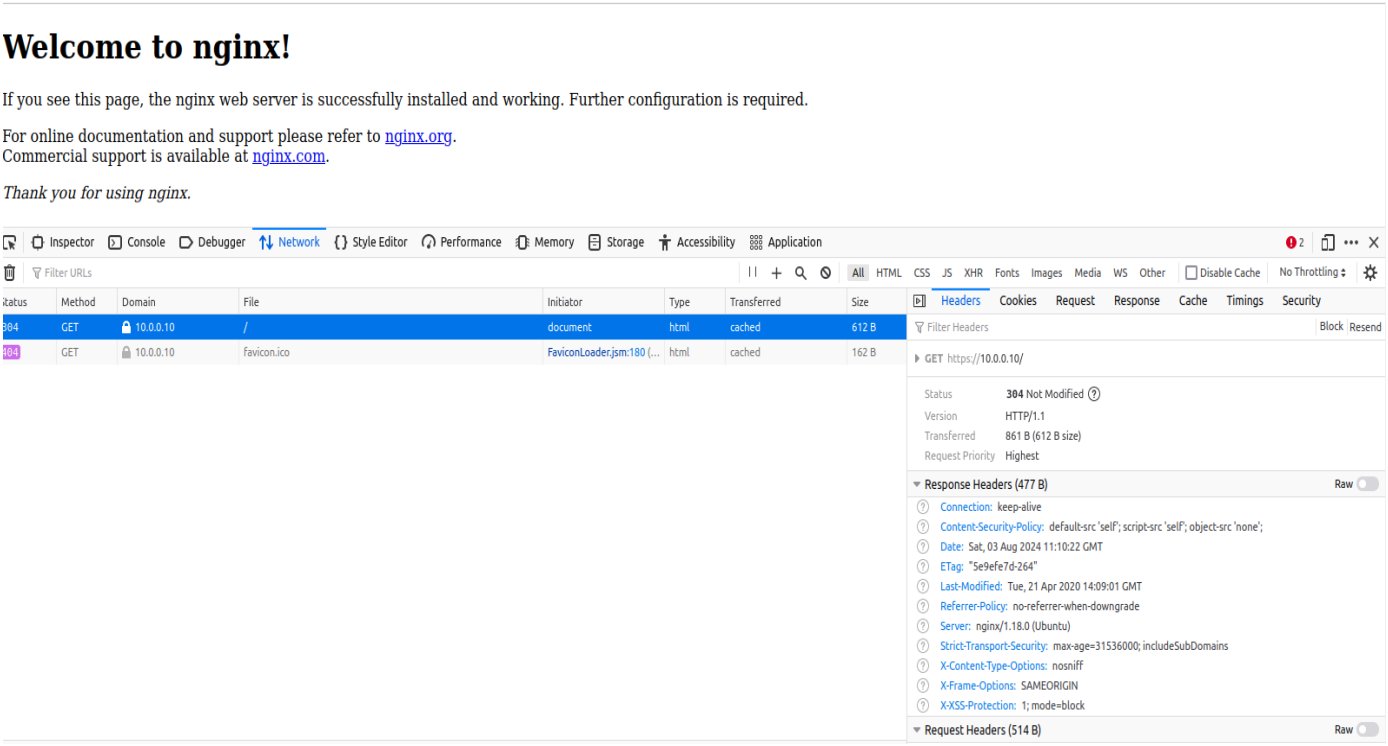
X-Content-Type-Options: Αποτρέπει την ανίχνευση τύπων περιεχομένου, βοηθώντας στην αποτροπή ορισμένων τύπων επιθέσεων.

Referrer-Policy: Ορίζει την πολιτική για την αποστολή πληροφοριών παραπομπής.

Content-Security-Policy: Περιορίζει τους επιτρεπόμενους πόρους για σενάρια, αντικείμενα, κ.λπ.

Strict-Transport-Security (HSTS): Υποχρεώνει τους πελάτες να χρησιμοποιούν μόνο ασφαλείς συνδέσεις (HTTPS).

Με τα παραπάνω βήματα, ο Nginx Web Server σας θα είναι σωστά ρυθμισμένος και ασφαλής για να υποστηρίζει ασφαλείς συνδέσεις HTTPS και να προστατεύεται από κοινές απειλές στο διαδίκτυο.



Εικόνα 29 Nginx Security Headers

3.7 Ανάπτυξη και Διαμόρφωση WAF (Web Application Firewall)

Η προστασία του ιστότοπού σας από κακόβουλες επιθέσεις είναι ζωτικής σημασίας για τη διατήρηση της ακεραιότητάς του και τη διασφάλιση της ασφάλειας των δεδομένων των επισκεπτών σας. Το ModSecurity, όταν ενσωματώνεται με το Nginx, παρέχει μια αποτελεσματική λύση φιλτράροντας και αποκλείοντας την δυνητικά επιβλαβή κίνηση HTTP.

3.7.1 Λήψη και εγκατάσταση του ModSecurity

1. Προσθέστε τις ακόλουθες γραμμές στο αρχείο **/etc/apt/sources.list** και στην συνέχεια εκτελέστε

Sudo apt Update.

deb-src http://deb.debian.org/debian/ bullseye main

deb-src http://security.debian.org/debian-security bullseye/updates main

deb-src http://archive.ubuntu.com/ubuntu/ hirsute main restricted universe multiverse

deb-src http://archive.ubuntu.com/ubuntu/ hirsute-updates main restricted universe multiverse

deb-src http://archive.ubuntu.com/ubuntu/ hirsute-backports main restricted universe multiverse

deb-src http://security.ubuntu.com/ubuntu/ hirsute-security main restricted universe multiverse

2. Δημιουργήστε έναν κατάλογο για τον πηγαίο κώδικα Nginx που κατεβάσατε. Πρέπει να βεβαιωθούμε ότι η έκδοση του πηγαίου κώδικα ταιριάζει με τη δυαδική έκδοση Nginx.

```
sudo apt install dpkg-dev
mkdir -p /usr/local/src/Nginx
cd /usr/local/src/Nginx/
apt source Nginx
```

```
george@LinuxMint-DMZ:/usr/local/src/nginx$ nginx -v
nginx version: nginx/1.18.0 (Ubuntu)
```

Εικόνα 30 Nginx Version

3. Εγκατάσταση του Libmodsecurity3 που είναι η βιβλιοθήκη ModSecurity που είναι υπεύθυνη για το φιλτράρισμα HTTP. Συνιστάται η μεταγλώττιση της πιο πρόσφατης σταθερής έκδοσης.

```
sudo apt install git
git clone --depth 1 -b v3/master --single-branch https://github.com/SpiderLabs/ModSecurity /usr/local/src/ModSecurity/
cd /usr/local/src/ModSecurity/
```

```
george@LinuxMint-DMZ:/usr/local/src/ModSecurity$ ls
aclocal.m4     config.status  libtool                     others
ar-lib         config.sub     LICENSE                     README.md
AUTHORS        configure      ltmain.sh                   SECURITY.md
bindings       configure~     Makefile                    src
build          configure.ac   Makefile.am                 test
build.sh       depcomp        Makefile.in                 test-driver
CHANGES        doc            missing                     tools
compile        examples       modsecurity.conf-recommended unicode.mapping
config.guess   headers        modsecurity.pc              ylwrap
config.log     install-sh     modsecurity.pc.in
```

Εικόνα 31 Libmodsecurity3 Install

4. Εγκατάσταση Build Dependencies για το libmodssecurity

```
sudo apt install gcc make build-essential autoconf automake libtool libcurl4-openssl-dev liblua5.3-dev libpcre2-dev libfuzzy-dev ssdeep gettext pkg-config libpcre3 libpcre3-dev libxml2 libxml2-dev libcurl4 libgeoip-dev libyajl-dev doxygen
git submodule init
git submodule update
./build.sh
./configure
make -j4
sudo make install
```

3.7.2 Διαμόρφωση του Nginx για χρήση του ModSecurity

1. Σε αυτό το βήμα, κατεβάστε και μεταγλωττίστε το ModSecurity Nginx Connector, το οποίο συνδέει το libmodsecurity με τον διακομιστή ιστού Nginx.

```
git clone --depth 1 https://github.com/SpiderLabs/ModSecurity-Nginx.git  /usr/local/src/ModSecurity-Nginx/
cd /usr/local/src/Nginx/Nginx-1.19.5/
sudo apt build-dep Nginx
sudo apt install uuid-dev
sudo ./configure --with-compat --with-openssl=/usr/include/openssl/ --add-dynamic-module=/usr/local/src/ModSecurity-Nginx
sudo make modules
sudo cp objs/ngx_http_modsecurity_module.so /usr/share/Nginx/modules/
```

Ακολουθώντας αυτά τα βήματα, κατεβάσαμε με επιτυχία και μεταγλωττίσαμε το ModSecurity v3 Nginx Connector, επιτρέποντάς μας να ενσωματώσουμε το ModSecurity με τον διακομιστή ιστού Nginx.

```
root@LinuxMint-DMZ:/usr/lib/nginx/modules# ls
ngx_http_geoip2_module.so         ngx_mail_module.so
ngx_http_image_filter_module.so   ngx_stream_geoip2_module.so
ngx_http_modsecurity_module.so    ngx_stream_module.so
ngx_http_xslt_filter_module.so
```

Εικόνα 32 Modsecurity Nginx Connector

2. Σε αυτό το βήμα, φορτώστε τον Αντάπτορα ModSecurity v3 Nginx Connector στη ρύθμιση του Nginx για να ενεργοποιήσετε το ModSecurity για τον ιστοτόπο. Πιο συγκεκριμένα:
   - **sudo nano /etc/Nginx/Nginx.conf**
   - Στην αρχή του αρχείου, προσθέστε την παρακάτω γραμμή για να φορτώσουμε τον αντάπτορα ModSecurity:

     load_module modules/ngx_http_modsecurity_module.so;
   - Εντός του http {...} τμήματος του αρχείου ρυθμίσεων, προσθέστε τις παρακάτω δύο γραμμές για να ενεργοποιήσουμε το ModSecurity για όλες τις εικονικές σελίδες φιλοξενίας του Nginx:

     modsecurity on;

     modsecurity_rules_file /etc/Nginx/modsec/main.conf;
   - Δημιουργήστε τον κατάλογο **/etc/Nginx/modsec/** για να αποθηκεύσετε τις ρυθμίσεις του ModSecurity: **sudo mkdir /etc/Nginx/modsec/**
   - Αντιγράψτε το αρχείο ρυθμίσεων του ModSecurity από την πηγή του στον κατάλογο ρυθμίσεων:

     sudo cp /usr/local/src/ModSecurity/modsecurity.conf-recommended /etc/Nginx/modsec/modsecurity.conf
   - Επεξεργαστήτε το αρχείο ρυθμίσεων του ModSecurity για να προσαρμόσετε τις ρυθμίσεις του:

     sudo nano /etc/Nginx/modsec/modsecurity.conf

Άλλαξτε την οδηγία **SecRuleEngine** σε **On** για να ενεργοποιήσουμε το ModSecurity για την ανίχνευση και αποκλεισμό των επιθέσεων στον ιστό.

- Δημιουργήστε το αρχείο **/etc/Nginx/modsec/main.conf** και συμπεριλάβαμε τις ρυθμίσεις του ModSecurity:

  sudo nano /etc/Nginx/modsec/main.conf

  Προσθέσαμε τη γραμμή:

  Include /etc/Nginx/modsec/modsecurity.conf

3. Αντιγράψαμε το αρχείο κατανομής Unicode στον κατάλογο ρυθμίσεων του ModSecurity:

   sudo cp /usr/local/src/ModSecurity/unicode.mapping /etc/Nginx/modsec/

Τέλος, αν η δοκιμή της ρύθμισης ήταν επιτυχής, επανεκκινήσαμε το Nginx για να εφαρμόσουμε τις αλλαγές:

sudo systemctl restart Nginx

```
root@LinuxMint-DMZ:/etc/nginx/modsec# sudo systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
     Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset:
     Active: active (running) since Tue 2024-02-20 19:47:29 EET; 23min ago
       Docs: man:nginx(8)
```

Εικόνα 33 Nginx Active

3.7.3 Διαμόρφωση και εισαγωγή κανόνων ασφάλειας

Για να καταστήσουμε το ModSecurity ικανό να προστατεύει τις ιστοσελίδες μας, χρειαζόμαστε κανόνες που να ανιχνεύουν και να μπλοκάρουν κακόβουλες ενέργειες. Υπάρχουν πολλά δωρεάν σύνολα κανόνων για το ModSecurity, μεταξύ αυτών και το OWASP Core Rule Set (CRS), το οποίο είναι το προτεινόμενο σύνολο κανόνων.

1. Κατεβάστε το Τελευταίο OWASP CRS από το GitHub:

   wget https://github.com/coreruleset/coreruleset/archive/v3.3.4.tar.gz

2. Εκτελέστε τις ακόλουθες εντολές.

   tar xvf **v3.3.4.tar.gz**

   sudo mv coreruleset-3.3.4/ /etc/nginx/modsec/

   sudo mv /etc/nginx/modsec/coreruleset-3.3.4/crs-setup.conf.example /etc/nginx/modsec/coreruleset-3.3.4/crs-setup.conf

```
root@LinuxMint-DMZ:/etc/nginx/modsec/coreruleset-3.3.4# ls
CHANGES           crs-setup.conf  KNOWN_BUGS  rules        tests
CONTRIBUTING.md   docs            LICENSE     SECURITY.md  util
CONTRIBUTORS.md   INSTALL         README.md   SPONSORS.md
```

Εικόνα 34 OWASP CRS Rules

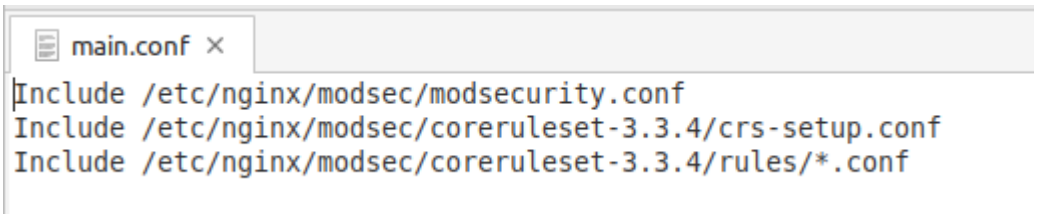
3. Επεξεργαστείτε το Κύριο Αρχείο Ρυθμίσεων:

   sudo nano /etc/nginx/modsec/main.conf

   Προσθέστε τις παρακάτω δύο γραμμές για να συμπεριληφθεί το αρχείο ρυθμίσεων του CRS και οι μεμονωμένοι κανόνες:

Include /etc/nginx/modsec/coreruleset-3.3.4/crs-setup.conf

Include /etc/nginx/modsec/coreruleset-3.3.4/rules/*.conf



Εικόνα 35 Import CRS Rules

4. sudo systemctl restart nginx

3.7.4 Προσαρμογή και δημιουργία προσαρμοσμένων κανόνων

Η δημιουργία και προσαρμογή κανόνων στο ModSecurity για τον Nginx μπορεί να ενισχύσει σημαντικά την ασφάλεια της web εφαρμογής σας. Παρακάτω περιγράφονται αναλυτικά τα βήματα που πρέπει να ακολουθήσετε για να δημιουργήσετε και να προσαρμόσετε προσαρμοσμένους κανόνες χρησιμοποιώντας το path **/etc/nginx/modsec/coreruleset-3.3.4/rules**.

3.7.5 Επεξεργασία του αρχείου κανόνων

Για να δημιουργήσετε προσαρμοσμένους κανόνες, θα πρέπει να επεξεργαστείτε ένα αρχείο ρυθμίσεων κανόνων. Μπορείτε να δημιουργήσετε ένα νέο αρχείο ή να επεξεργαστείτε ένα υπάρχον. Ακολουθήστε τα παρακάτω βήματα:

1. Στον φάκελο **/etc/nginx/modsec/coreruleset-3.3.4/rules**, δημιουργήστε ένα νέο αρχείο κανόνων. Για παράδειγμα

   sudo touch /etc/nginx/modsec/coreruleset-3.3.4/rules/custom_rules.conf
2. Στο αρχείο custom_rules.conf, μπορείτε να ξεκινήσετε να προσθέτετε προσαρμοσμένους κανόνες. Παρακάτω παρατίθενται παραδείγματα κανόνων που μπορείτε να χρησιμοποιήσετε.

3.7.6 Δημιουργία απλών προσαρμοσμένων κανόνων

- **Παράδειγμα 1: Μπλοκάρισμα Αιτημάτων με Ειδικό Όρο**

Αυτός ο κανόνας ελέγχει όλες τις παραμέτρους των αιτημάτων (ARGS) για την ύπαρξη του όρου "malicious" και απορρίπτει το αίτημα με κατάσταση 403 αν τον βρει.

```
SecRule ARGS "malicious" "id:1001,phase:2,deny,status:403,log,msg:'Blocked malicious request' "
```

id: Κάθε κανόνας πρέπει να έχει μοναδικό ID.

phase: Καθορίζει τη φάση που εκτελείται ο κανόνας. Η φάση 2 εκτελείται όταν το αίτημα έχει διαβιβαστεί στον server.

deny: Απορρίπτει το αίτημα αν εντοπιστεί η παράβαση.

log: Καταγράφει το συμβάν.

msg: Προσαρμοσμένο μήνυμα καταγραφής.

- **Παράδειγμα 2: Μπλοκάρισμα Αιτημάτων προς Συγκεκριμένο URL**

Για να μπλοκάρετε πρόσβαση σε ένα συγκεκριμένο endpoint, όπως το /admin, προσθέστε τον ακόλουθο κανόνα:

```
SecRule REQUEST_URI "^/admin" "id:1002,phase:1,deny,status:403,log,msg:'Admin access denied' "
```

REQUEST_URI: Αναφέρεται στο URI που ζητάει ο πελάτης.

^/admin: Ο κανόνας εφαρμόζεται σε οποιοδήποτε URL ξεκινά με /admin.

status: Ορίζει την κατάσταση HTTP που θα επιστρέψει ο server.

- **Παράδειγμα 3: Επιτρεπτή Ανοχή σε Συγκεκριμένα Headers**

Για παράδειγμα, αν δεν θέλετε να αποκλείσετε αιτήματα με ειδικούς χαρακτήρες, αλλά θέλετε να καταγράψετε τα περιστατικά για ανάλυση, προσθέστε τον ακόλουθο κανόνα:

```
SecRule REQUEST_HEADERS:Content-Type "application/json" "id:1005,phase:2,log,pass,status:200,msg:'Allowed JSON request with header check' "
```

pass: Ορίζει ότι το αίτημα περνά κανονικά (δεν απορρίπτεται), αλλά καταγράφεται.

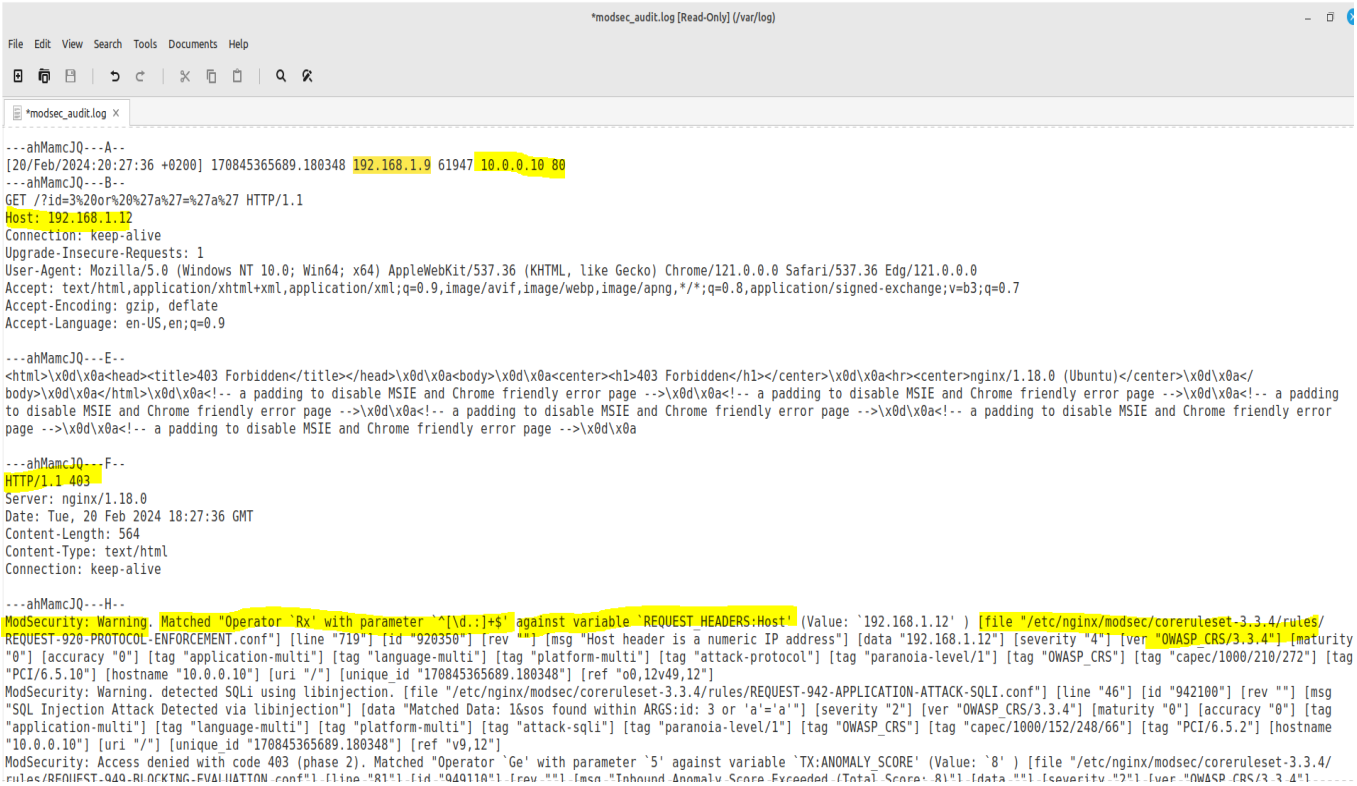
status: Ορίζει ότι επιστρέφεται η κανονική κατάσταση 200.

3.7.7 Παρακολούθηση και καταγραφή συμβάντων

Για να ελέγξετε αν οι κανόνες λειτουργούν σωστά και καταγράφονται τα συμβάντα, μπορείτε να παρακολουθείτε τα αρχεία καταγραφής του ModSecurity:

sudo tail -f /var/log/modsec_audit.log

Μετά την εγκατάσταση του WAF, διενεργήσαμε μια δοκιμή εισβολής SQL από τη διεύθυνση IP 192.168.1.9. Στα αρχεία καταγραφής ModSecurity, εντοπίσαμε την παρακάτω εγγραφή:



Εικόνα 36 WAF Rule Triggered

1. HTTP Αίτημα (Request):
    - Ο τύπος του HTTP αιτήματος είναι GET.
    - Το URL που ζητείται είναι /?id=3%20or%20%27a%27=%27a%27, το οποίο φαίνεται να είναι μια προσπάθεια εισβολής SQL.
    - Υπάρχουν πολλές κεφαλίδες HTTP συμπεριλαμβανομένων της Host, Connection, User-Agent, Accept, Accept-Encoding, Accept-Language.
2. HTTP Απόκριση (Response):
    - Η απόκριση HTTP έχει κωδικό 403 Forbidden, υποδηλώνοντας ότι η πρόσβαση απορρίφθηκε από τον διακομιστή.
    - Η σελίδα που επιστρέφεται περιλαμβάνει ένα κείμενο "403 Forbidden" και αναφέρει την έκδοση του Nginx που χρησιμοποιείται.
    - Η απόκριση περιλαμβάνει επίσης μια προειδοποίηση ModSecurity που αναφέρει αντιστοίχηση σε έναν κανόνα του OWASP CRS που ανιχνεύει προσπάθειες εισβολής SQL.

3.7.8 Ενσωμάτωση των Logs του ModSecurity στο QRadar

Η ενσωμάτωση των αρχείων καταγραφής (logs) του **ModSecurity** στο **QRadar** είναι μια κρίσιμη διαδικασία για την κεντρική παρακολούθηση των γεγονότων ασφαλείας. Με την ενσωμάτωση αυτή, μπορείτε να αναλύετε τα συμβάντα ασφαλείας και να αντιδράτε γρήγορα σε πιθανές απειλές. Παρακάτω

παρουσιάζονται τα βήματα που ακολουθήθηκαν για τη ρύθμιση της αποστολής των logs του **ModSecurity** στο **QRadar**.

1. Ανοίξτε το **/etc/rsyslog.d/** και δημιουργήστε ένα νέο αρχείο ρύθμισης με όνομα mod.conf για να καθορίσετε την αποστολή των logs του ModSecurity.

   sudo nano /etc/rsyslog.d/mod.conf

2. Προσθέστε την παρακάτω ρύθμιση στο αρχείο:

```
module(load="imfile")
$InputFileName /var/log/modsec_audit.log
$InputFileTag modsecurity
$InputFileStateFile stat-modsec
$InputFileSeverity info
$InputFileFacility local1
$InputRunFileMonitor
if $programname == 'modsecurity' then @@192.168.2.5:514
```

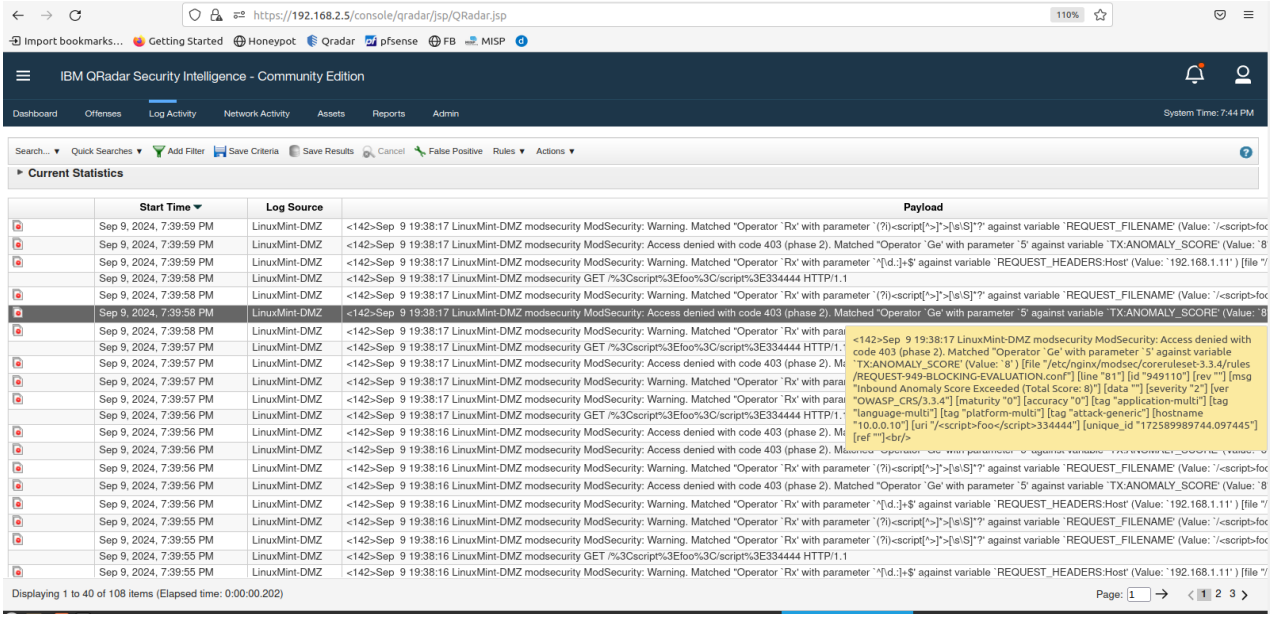
3. Για να διασφαλίσετε ότι τα logs του ModSecurity καταγράφονται σωστά, επεξεργαστείτε το αρχείο ρυθμίσεων 50-default.conf. Προσθέστε την ακόλουθη γραμμή:

   local1.* -/var/log/syslog

4. Για να εφαρμοστούν οι αλλαγές, επανεκκινήστε την υπηρεσία rsyslog.

   sudo systemctl restart rsyslog

5. Μεταβείτε στον διακομιστή QRadar και ελέγξτε αν τα logs λαμβάνονται σωστά.



Εικόνα 37 Modsecurity Logs in Qradar

3.7.9 Παρακολούθηση ενημερώσεων κανόνων (OWASP Core Rule Set - CRS)

Οι κανόνες που εφαρμόζει το ModSecurity βασίζονται συνήθως στο OWASP Core Rule Set (CRS). Το CRS ανανεώνεται τακτικά με νέους κανόνες που προστατεύουν από αναδυόμενες απειλές. Είναι σημαντικό να παρακολουθείτε για νέες εκδόσεις του CRS και να το ενημερώνετε τακτικά.

1. Επισκεφθείτε το GitHub αποθετήριο του OWASP Core Rule Set για να ελέγξετε αν υπάρχει νέα έκδοση.
2. Αναβάθμιση του CRS

```
cd /etc/nginx/modsec/
sudo wget https://github.com/coreruleset/coreruleset/archive/refs/tags/v3.3.5.tar.gz
sudo tar -xzvf v3.3.5.tar.gz
sudo mv coreruleset-3.3.5 coreruleset
```

3.7.10 Αναβάθμιση του ModSecurity

Η ίδια η μηχανή του ModSecurity αναβαθμίζεται με ενημερώσεις που επιλύουν ευπάθειες ή βελτιώνουν την απόδοση του WAF. Πρέπει να ελέγχετε τακτικά για νέες εκδόσεις του ModSecurity.

1. Έλεγχος της έκδοσης του ModSecurity:
   sudo nginx -V 2>&1 | grep -o with-modsecurity
2. Ενημέρωση του ModSecurity
   sudo apt update
   sudo apt install libmodsecurity-dev

3.8 Ανάπτυξη και Διαμόρφωση MISP

Σε αυτή την ενότητα παρουσιάζεται η **εγκατάσταση** και **παραμετροποίηση** της πλατφόρμας **MISP (Malware Information Sharing Platform)**. Περιγράφονται αναλυτικά τα βήματα για τη λήψη, εγκατάσταση, ενεργοποίηση feeds και δημιουργία χρηστών, καθώς και η σύνδεση με **TAXII servers**. Στόχος είναι η δημιουργία ενός λειτουργικού περιβάλλοντος ανταλλαγής πληροφοριών απειλών.

3.8.1 Προαπαιτούμενα εγκατάστασης MISP

1. Μικροί κόμβοι ή τοπικά MISP hubs μπορούν να λειτουργήσουν άνετα με **16GB μνήμης** και **2 vCPUs**.
2. Μεγάλες κοινότητες όπως η **CIRCL private sector community** χρησιμοποιούν **128GB μνήμης** και **32 πυρήνες CPU** σε σύγχρονους επεξεργαστές Xeon.
3. Για εκπαιδευτικούς σκοπούς, οι εικονικές μηχανές που χρησιμοποιούμε μπορούν να λειτουργήσουν με μόλις **2GB μνήμης** και **1 vCPU** (δεν προτείνεται για παραγωγική χρήση).
4. Η χρήση SSD προσφέρει χαμηλότερη **καθυστέρηση I/O** και καλύτερη απόκριση της βάσης δεδομένων.
5. Το MISP χρησιμοποιεί τη μνήμη RAM για την προσωρινή αποθήκευση δεδομένων από τα ενεργοποιημένα feeds. Παραδείγματος χάριν, με ενεργοποιημένες τις προεπιλεγμένες τροφοδοσίες (feeds), μπορεί να χρησιμοποιηθούν έως και **1.2GB μνήμης**.

3.8.2 Λήψη και εγκατάσταση του MISP σε Ubuntu Server 20.04

1. Αρχικά, θα κατεβάσετε το **Ubuntu Server 20.04** από την επίσημη ιστοσελίδα.
2. Στη συνέχεια, θα δημιουργήσετε μια νέα εικονική μηχανή στο **VirtualBox** για την εγκατάσταση του Ubuntu Server.
3. Κατά τη διαμόρφωση της εικονικής μηχανής, ορίστε τον τύπο δικτύου σε **Internal Network** με όνομα προσαρμογέα **"intnet3"**.
4. Εγκαταστήστε το **Ubuntu Server** στην εικονική μηχανή.

Αφού εγκατασταθεί και προετοιμαστεί ο **Ubuntu Server 20.04**, θα χρειαστεί να εγκαταστήσετε το **MISP**. Για την εγκατάσταση του MISP, θα χρησιμοποιήσετε ένα έτοιμο script που αυτοματοποιεί τη διαδικασία εγκατάστασης

1. Εκτελέστε τις παρακάτω εντολές για να κατεβάσετε και να εκτελέσετε το script:

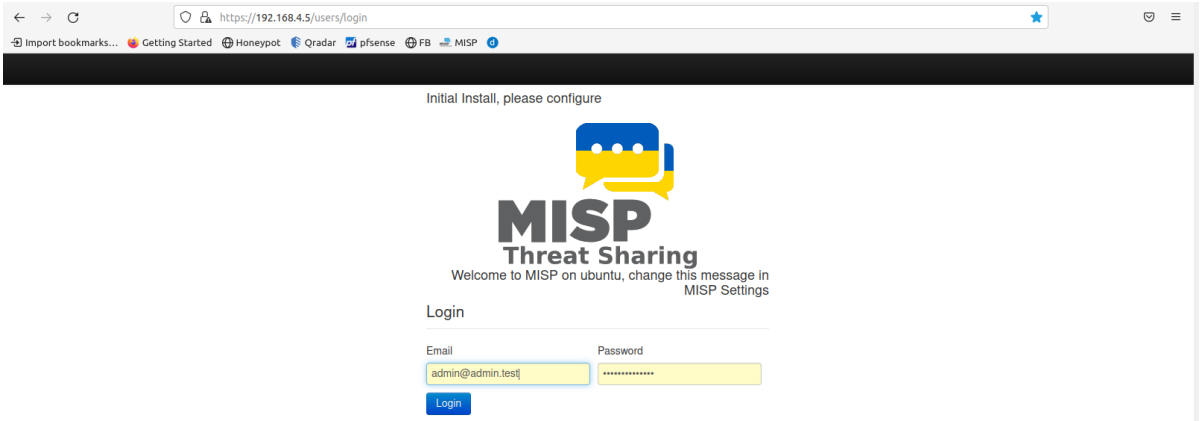
   wget https://raw.githubusercontent.com/MISP/MISP/master/INSTALL/INSTALL.sh
2. Αφού κατεβάσετε το **INSTALL.sh**, εκτελέστε το για να ξεκινήσετε την εγκατάσταση:

   sudo bash INSTALL.sh

```
george@ubuntu:~$ curl -o /tmp/INSTALL.sh -L -C - https://raw.githubusercontent.com/MISP/MISP/2.4/INS
TALL/INSTALL.sh^C
george@ubuntu:~$ bash /tmp/INSTALL.sh -A_
```

Εικόνα 38 MISP Download-Install Commands

3. Μετά την ολοκλήρωση της εγκατάστασης, χρησιμοποιήστε την εντολή **ifconfig** για να βρείτε τη διεύθυνση IP του συστήματός σας.
4. Αφού βρείτε τη διεύθυνση IP, ανοίξτε έναν browser και μεταβείτε στο MISP χρησιμοποιώντας την IP.

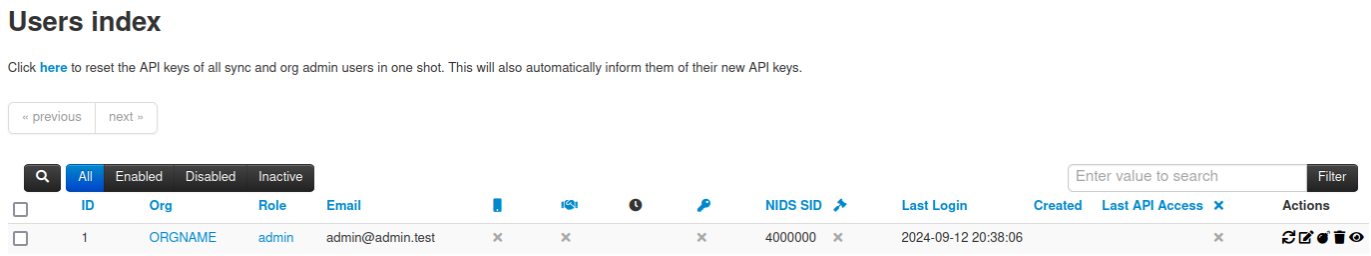


Εικόνα 39 MISP Login Page

5. Στη σελίδα του MISP, κάντε login χρησιμοποιώντας τα εξής διαπιστευτήρια:
   a. Email: admin@admin.test
   b. Password: admin

3.8.3 Δημιουργία χρηστών

1. Συνδεθείτε στο περιβάλλον διαχείρισης του MISP μέσω του web GUI.
2. Πηγαίνετε στο **Administration** > **List Users**.
3. Πατήστε **Add User** για να δημιουργήσετε έναν νέο χρήστη.
4. Συμπληρώστε τα πεδία που απαιτούνται (όνομα, email, ρόλος κλπ.).
5. Καθορίστε τον ρόλο του χρήστη (π.χ., user, admin) και τυχόν επιπλέον δικαιώματα ανάλογα με τις ανάγκες σας.



Εικόνα 40 MISP Users

3.8.4 Δημιουργία Authentication Keys (API Keys)

Τα **API Keys** επιτρέπουν στους χρήστες να αλληλεπιδρούν με το **MISP** χρησιμοποιώντας scripts ή άλλες εφαρμογές μέσω του API.

1. Από το **My Profile** στο μενού πάνω δεξιά, πηγαίνετε στο **Auth Keys**.
2. Πατήστε **Add Authentication Key**.
3. Δώστε ένα όνομα για το key και επιλέξτε την ημερομηνία λήξης του.
4. Πατήστε **Submit** για να δημιουργήσετε το key, το οποίο μπορείτε να χρησιμοποιήσετε για εξωτερικές εφαρμογές που χρειάζονται πρόσβαση στο MISP.

Προβήκαμε στη δημιουργία ενός νέου API Key (κλειδιού αυθεντικοποίησης) με το σχόλιο "**Auth Key for QRadar**", ώστε αυτό να χρησιμοποιηθεί στη διασύνδεση μεταξύ MISP και QRadar.

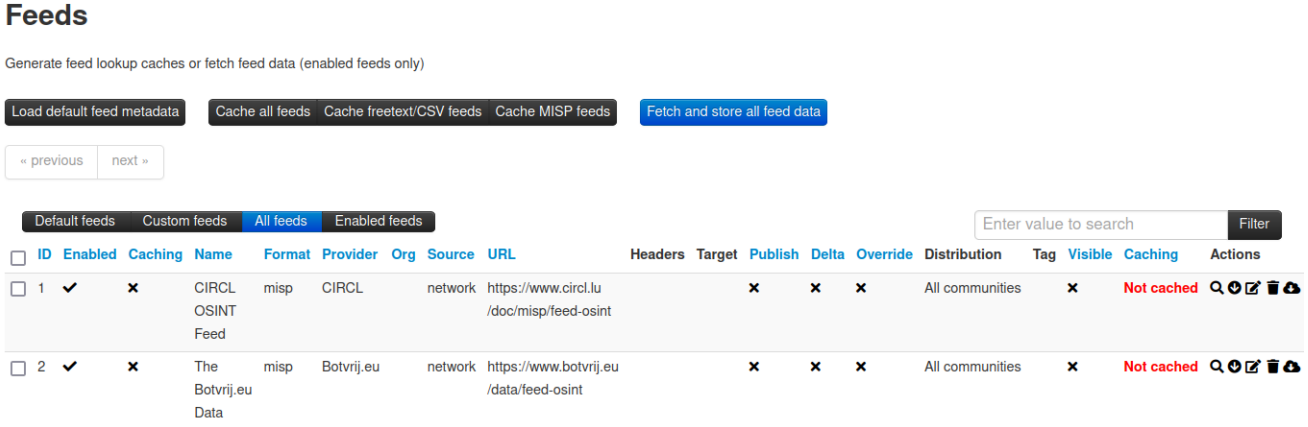
Το API Key είναι απαραίτητο για την ασφαλή και αυθεντικοποιημένη πρόσβαση στις λειτουργίες του MISP μέσω άλλων εργαλείων, όπως το QRadar, επιτρέποντας την αυτόματη ανταλλαγή πληροφοριών (IOCs).

Εικόνα 41 MISP Auth Keys

3.8.5 Ενεργοποίηση Feeds

Τα **feeds** στο **MISP** είναι πηγές δεδομένων που σας επιτρέπουν να εισάγετε αυτόματα δεδομένα πληροφοριών απειλών (threat intelligence).

1. Μεταβείτε στο **Sync Actions** > **List Feeds**.
2. Θα δείτε μια λίστα με προεπιλεγμένα διαθέσιμα feeds.
3. Επιλέξτε τα feeds που θέλετε να ενεργοποιήσετε και πατήστε **Enable**.
4. Για να πραγματοποιηθεί άμεση λήψη δεδομένων, πατήστε το κουμπί **Fetch all** για να κατεβάσετε τα δεδομένα των ενεργών feeds.

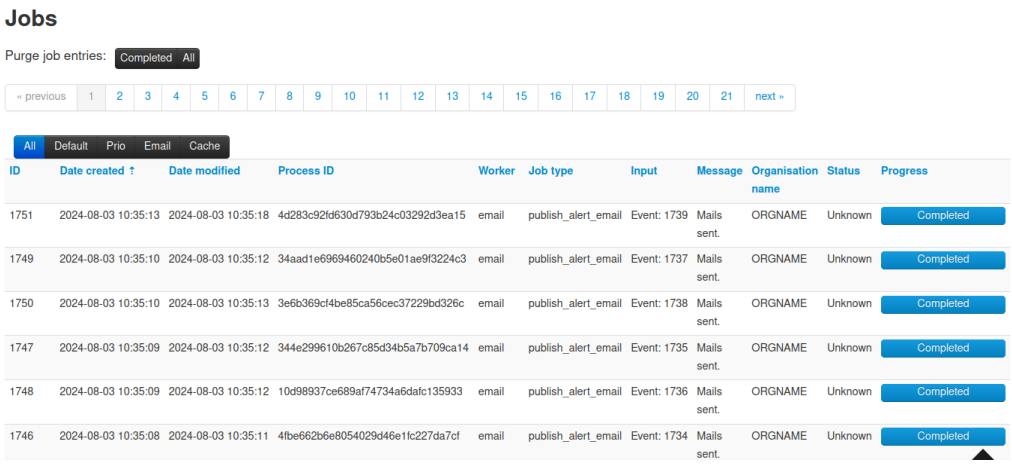


Εικόνα 42 MISP Feeds

3.8.6 Παρακολούθηση Jobs (Εργασιών)

Το **MISP** εκτελεί διάφορες εργασίες στο παρασκήνιο (jobs), όπως το κατέβασμα feeds, τη δημιουργία events, κ.ά. Μπορείτε να παρακολουθείτε την κατάσταση αυτών των εργασιών μέσω του GUI.

1. Πηγαίνετε στο **Diagnostics** > **List Jobs**.
2. Θα δείτε μια λίστα με όλα τα ενεργά jobs, την κατάστασή τους και τυχόν σφάλματα που μπορεί να έχουν προκύψει.

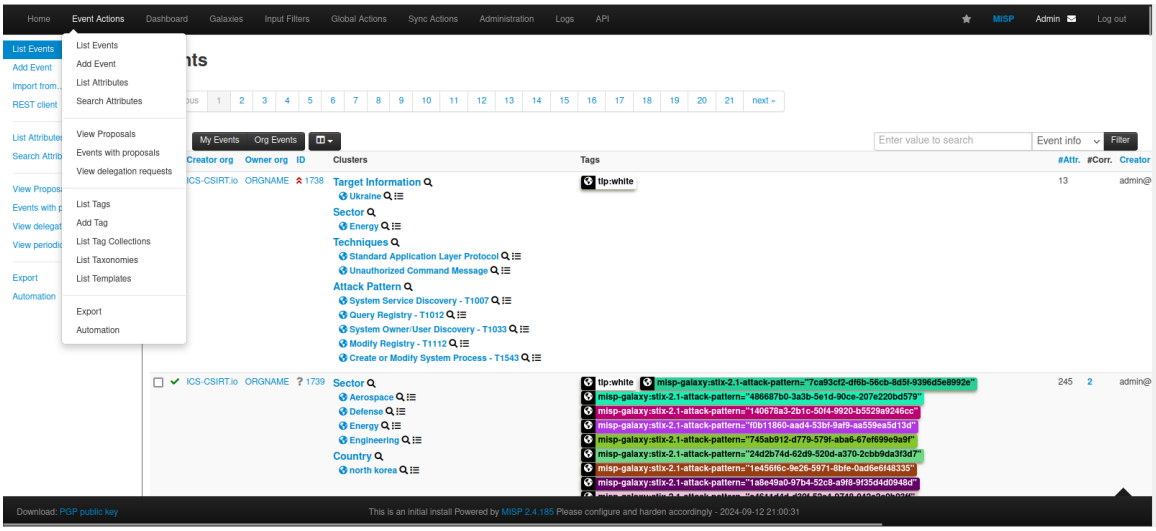


Εικόνα 43 MISP Jobs

3.8.7 Παρακολούθηση Events που κατεβαίνουν από Feeds

Αφού ενεργοποιήσετε τα feeds και κατεβάσετε δεδομένα, τα events αυτά θα εμφανιστούν στο **Events** tab.

1. Μεταβείτε στο **Event Actions** > **List Events**.
2. Εδώ μπορείτε να δείτε όλα τα events που έχουν εισαχθεί από τα feeds ή άλλα εξωτερικά συστήματα.
3. Μπορείτε να τα φιλτράρετε, να τα επεξεργαστείτε, ή να τα διαγράψετε ανάλογα με τις ανάγκες σας.

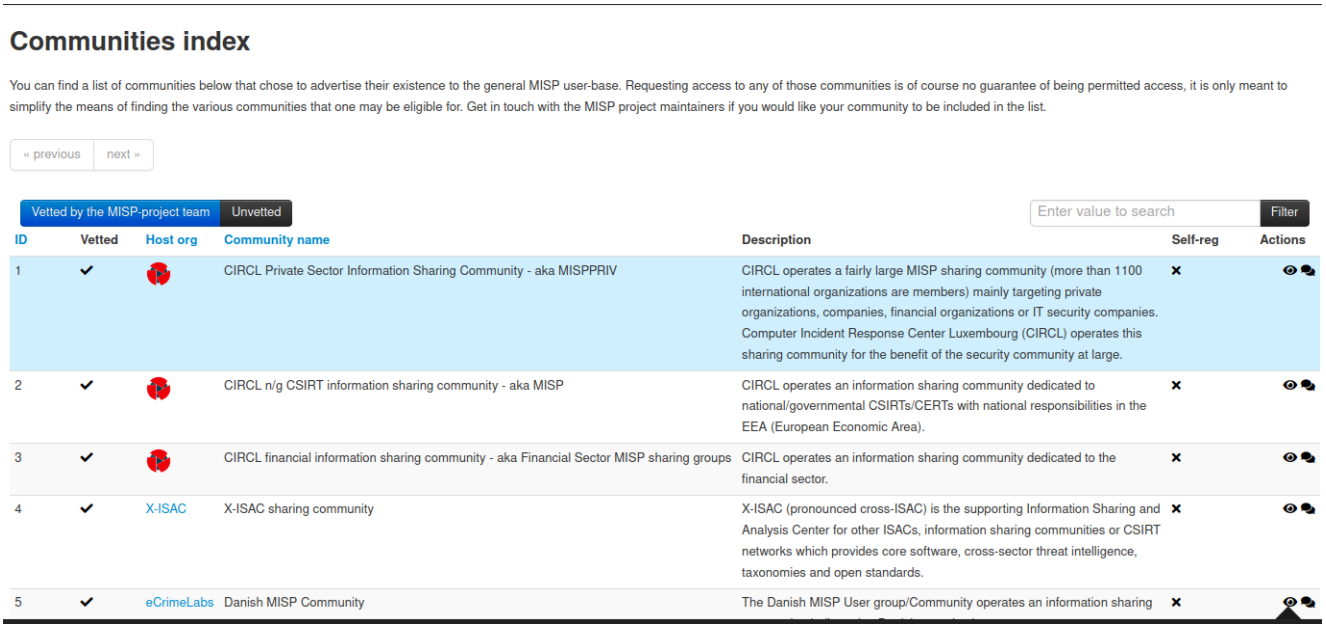


Εικόνα 44 MISP List Events

3.8.8 Communities στο MISP

Το **MISP** υποστηρίζει τη δημιουργία ή την ένταξη σε κοινότητες (communities) για κοινή χρήση πληροφοριών σχετικά με απειλές. Κάθε κοινότητα μπορεί να μοιράζεται events, indicators of compromise (IoCs), και άλλα δεδομένα σε ασφαλές και ελεγχόμενο περιβάλλον.

- Οι κοινότητες είναι ομάδες ή οργανισμοί που συνδέονται μεταξύ τους για να ανταλλάσσουν πληροφορίες απειλών με ασφαλή και αξιόπιστο τρόπο.
- Κάθε χρήστης μπορεί να δημιουργήσει ή να ενταχθεί σε μια κοινότητα μέσω του **Sync Actions** > **List Communities**.



Εικόνα 45 MISP Communities

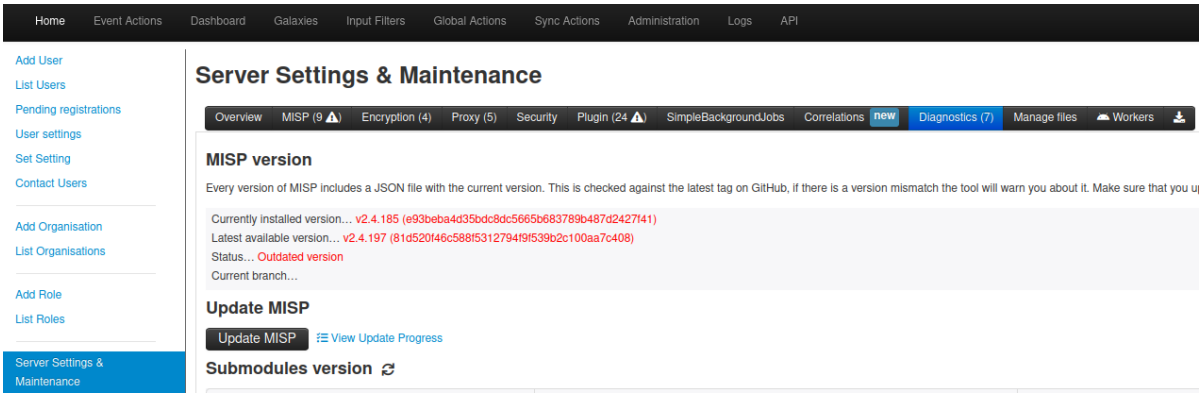
3.8.9 TAXII Servers

Οι **TAXII servers** (Trusted Automated eXchange of Indicator Information) είναι servers που επιτρέπουν την αυτόματη ανταλλαγή δεδομένων απειλών μεταξύ οργανισμών χρησιμοποιώντας το πρότυπο **STIX**.

1. Στο **Sync Actions** > **TAXII Servers**, μπορείτε να προσθέσετε **TAXII servers** για αυτόματη εισαγωγή και εξαγωγή δεδομένων απειλών.
2. Συμπληρώστε τα στοιχεία του **TAXII server** που θέλετε να χρησιμοποιήσετε.
3. Ο **TAXII server** επιτρέπει την ανταλλαγή IoCs και events με άλλες πλατφόρμες που υποστηρίζουν **STIX/TAXII**.

3.8.10 Ενημέρωση του MISP

Η διαδικασία ενημέρωσης του MISP μπορεί να πραγματοποιηθεί είτε χειροκίνητα είτε μέσω αυτοματοποιημένων scripts που παρέχονται από την κοινότητα του MISP. Για να ελέγξουμε αν υπάρχει νέα έκδοση, μπορούμε να μεταβούμε στη διαχείριση του συστήματος μέσω του MISP GUI, όπου εμφανίζεται μια ειδοποίηση εάν υπάρχει διαθέσιμη ενημέρωση.



Εικόνα 46 MISP Server Maintenance

3.9 Ανάπτυξη και Διαμόρφωση SIEM QRadar

Η ενότητα αυτή εστιάζει στην **εγκατάσταση**, **παραμετροποίηση** και **ενσωμάτωση** του **SIEM QRadar** στο εργαστηριακό περιβάλλον. Περιγράφονται τα βήματα για τη δημιουργία **Log Sources**, η χρήση εργαλείων όπως το **Log Source Management App** και οι **κανόνες ανάλυσης συμβάντων**. Επιπλέον, παρουσιάζεται η διαχείριση της **δικτυακής ιεραρχίας**, των **reference sets** και η συσχέτιση των logs με **εισερχόμενη δικτυακή κυκλοφορία**.

3.9.1 Προετοιμασία περιβάλλοντος

1. Πριν συνεχίσετε, βεβαιωθείτε ότι το σύστημά σας πληροί τις ελάχιστες απαιτήσεις υλικού και λογισμικού για την εκτέλεση του QRadar Community Edition.

   Απαιτήσεις υλικού:

   CPU: Τετραπύρηνος 2,0 GHz ή υψηλότερος

   RAM: 8 GB ή υψηλότερη

   Αποθήκευση: Ελάχιστο 250 GB χώρου στο δίσκο (SAS/SATA HDD ή SSD)

2. Επισκεφτείτε τον ιστότοπο του IBM QRadar Community Edition και εγγραφείτε για έναν δωρεάν λογαριασμό. Μετά την εγγραφή, θα πρέπει να μπορείτε να κάνετε λήψη της εικόνας εγκατάστασης του QRadar Community Edition.

   https://www.ibm.com/community/qradar/ce/

3. Ρυθμίστε μια εικονική μηχανή για να φιλοξενήσει το QRadar Community Edition. Βεβαιωθείτε ότι η συνδεσιμότητα δικτύου είναι διαθέσιμη, ότι ο network adapter ανήκει στο Internal Network “intent”, και ότι το σύστημα πληροί τις προϋποθέσεις.

3.9.2 Εγκατάσταση

1. Εκκινήστε την εικονική μηχανή και επιλέξτε στο πρώτο παράθυρο που εμφανίζεται την επιλογή “**CentOS Linux (3.10.0-1062.4.1.el7.x86_64) 7 (core)”**
2. Στην συνέχει θα σας ζητηθεί να κάνετε σύνδεση. Πληκτρολογήστε

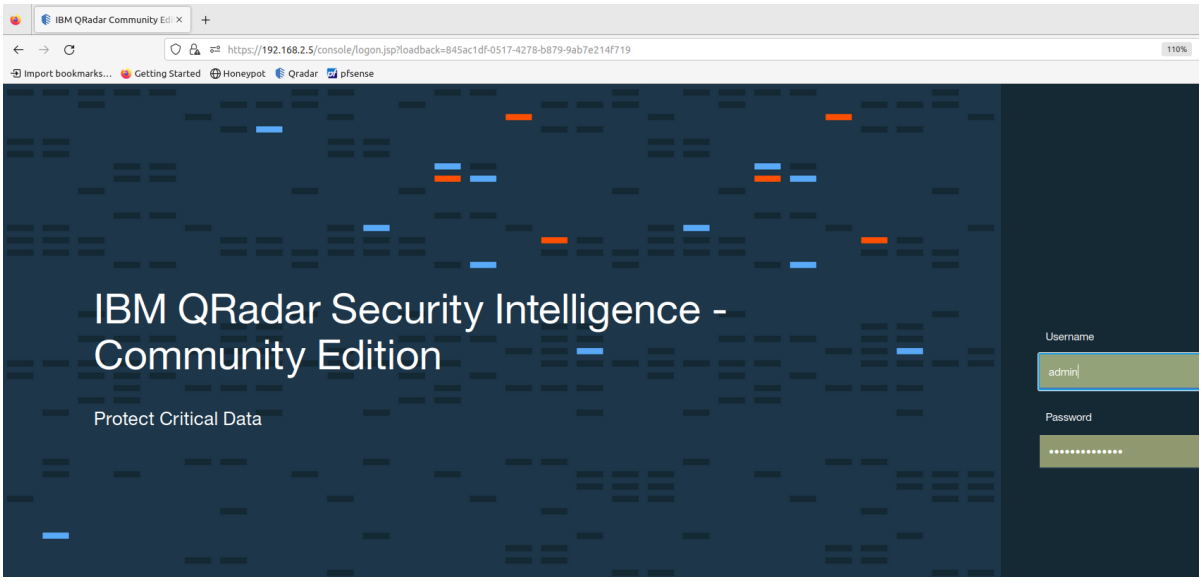
   Usernale: root.

Έπειτα σας ζητάει να εισάγετε νέο κωδικό για το username:root.

3. Τρέξτε την εντολή **" ./setup"** στην γραμμή εντολών.
4. Μετά το τέλος της εγκατάστασης θα σας ζητηθεί νέος κωδικός για το **username:admin**. Το συγκεκριμένο account θα χρησιμοποιηθεί στο GUI του qradar , σε αντίθεση με το account:root που χρησιμοποιείται για την γραμμή εντολών.
5. Τέλος, θα μπορείτε να εισέλθετε στο περιβάλλον του Qradar μέσω της διεύθυνσης https://192.168.2.5

```
Enter a password for the admin user. This is used to log in to QRadar user interface.


Please enter the new admin password.
Password:
Confirm password:
The admin password has been changed.

[root@localhost ~]# systemctl status tomcat
● tomcat.service - Apache Tomcat
   Loaded: loaded (/usr/lib/systemd/system/tomcat.service; enabled; vendor preset: disabled)
  Drop-In: /etc/systemd/system/tomcat.service.d
           └─ulimit.conf
   Active: active (running) since Mon 2020-04-13 14:43:38 UTC; 12min ago
 Main PID: 19645 (java)
    Tasks: 262
   Memory: 1.5G
   CGroup: /system.slice/tomcat.service
           └─19645 /bin/java -Dcatalina.base=/opt/tomcat -Dcatalina.home=/opt/tomcat -Djava.security
```

Εικόνα 47 Τελευταίο βήμα κατά την εγκατάσταση του Qradar



Εικόνα 48 Αρχική σελίδα SIEM Qradar

3.9.3 Log Sources

Στο IBM QRadar, ένα Log Source αναφέρεται σε οποιαδήποτε συσκευή, σύστημα ή εφαρμογή που δημιουργεί δεδομένα καταγραφής ή συμβάντα ασφαλείας. Τα Log Sources είναι κρίσιμα για τη συλλογή και τη συγκέντρωση δεδομένων στην πλατφόρμα QRadar SIEM, επιτρέποντας στους αναλυτές ασφαλείας να παρακολουθούν και να αναλύουν δραστηριότητες εντός του δικτύου για πιθανές απειλές ή συμβάντα ασφαλείας.

3.9.4 Log Source Management App

Αυτή οι εφαρμογή έχει σχεδιαστεί για να απλοποιεί τη διαδικασία Log Source και να διασφαλίζουν ότι τα δεδομένα που συλλέγονται αναλύονται σωστά για ουσιαστική ανάλυση.

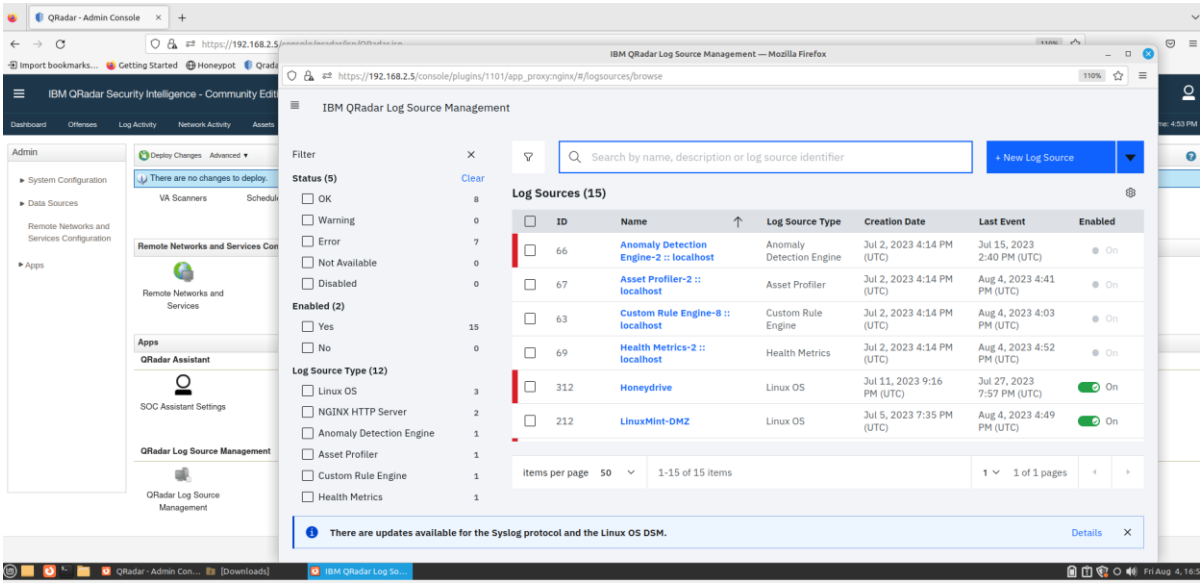
Πλεονεκτήματα Log Source App:

- Εξαλείφει την ανάγκη για μη αυτόματη διαμόρφωση της πηγής καταγραφής. Με την εγκατάσταση της σχετικής εφαρμογής, το QRadar μπορεί αυτόματα να εντοπίσει και να συλλέξει αρχεία καταγραφής από υποστηριζόμενες συσκευές, καθιστώντας τη διαδικασία ενσωμάτωσης ταχύτερη και πιο αποτελεσματική.
- Κάθε εφαρμογή Log Source περιλαμβάνει κανόνες ανάλυσης προσαρμοσμένους στη συγκεκριμένη μορφή αρχείου καταγραφής της υποστηριζόμενης συσκευής ή εφαρμογής. Αυτή η τυποποίηση διασφαλίζει ότι τα δεδομένα καταγραφής αναλύονται σωστά και κανονικοποιούνται, επιτρέποντας συνεπή και ακριβή ανάλυση.

Εγκατάσταση Log Source Management App

1. Κατεβάστε το αρχείο της εφαρμογής Log Source Management QRadar από το IBM Security App Exchange (https://apps.xforce.ibmcloud.com/) στον τοπικό σας υπολογιστή. Πρέπει να έχετε αναγνωριστικό IBM για να αποκτήσετε πρόσβαση στο App Exchange.
2. Στην Κονσόλα QRadar, κάντε κλικ στην επιλογή Admin > Extensions Management.

3. Στη σελίδα Extension Management, κάντε κλικ στην Add και επιλέξτε το αρχείο εφαρμογής που θέλετε να ανεβάσετε στην κονσόλα.
4. Επιλέξτε το πλαίσιο ελέγχου Install immediately.



Εικόνα 49 Εγκατάσταση Log Source Management App

3.9.5 DSM Editors

Στο IBM QRadar, οι Editors DSM (Device Support Module) είναι εργαλεία που επιτρέπουν στους χρήστες να προσαρμόζουν και να τελειοποιούν την ανάλυση και την επεξεργασία δεδομένων αρχείων καταγραφής από διάφορες συσκευές και εφαρμογές. Τα προγράμματα Editors DSM είναι απαραίτητα για τη δημιουργία ή την τροποποίηση αρχείων διαμόρφωσης DSM, τα οποία καθορίζουν τον τρόπο με τον οποίο το QRadar ερμηνεύει και αναλύει συμβάντα καταγραφής που λαμβάνονται από πηγές καταγραφής.

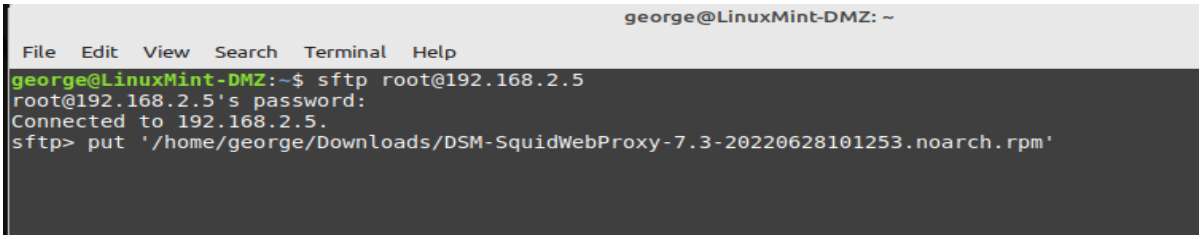
Βασικές λειτουργίες των DSM Editors:

- Οι DSM Editors παρέχουν επιλογές για την κανονικοποίηση των αναλυμένων δεδομένων καταγραφής, διασφαλίζοντας ότι τα συμβάντα καταγραφής από διαφορετικές πηγές αντιπροσωπεύονται σε τυποποιημένη μορφή. Αυτή η διαδικασία κανονικοποίησης ενισχύει τη συνοχή και διευκολύνει τον συσχετισμό και την ανάλυση δεδομένων σε διάφορες πηγές καταγραφής.
- Οι ομάδες ασφαλείας μπορούν να αντιστοιχίσουν συγκεκριμένα πεδία στα δεδομένα καταγραφής σε αντίστοιχα χαρακτηριστικά συμβάντων QRadar. Αυτό το βήμα βοηθά στην οργάνωση και την κατηγοριοποίηση συμβάντων καταγραφής σωστά στο σύστημα QRadar, καθιστώντας το πιο διαχειρίσιμο για τους αναλυτές ασφαλείας να αναζητούν, να φιλτράρουν και να διερευνούν συμβάντα.
- Παρέχουν συνήθως εργαλεία δοκιμών και επικύρωσης που επιτρέπουν στους χρήστες να ελέγχουν την αποτελεσματικότητα των κανόνων ανάλυσης και να επαληθεύουν ότι τα δεδομένα καταγραφής υποβάλλονται σε σωστή επεξεργασία. Αυτό βοηθά στον εντοπισμό και την επίλυση τυχόν προβλημάτων με τις διαμορφώσεις DSM.

Εγκατάσταση DSM Editors

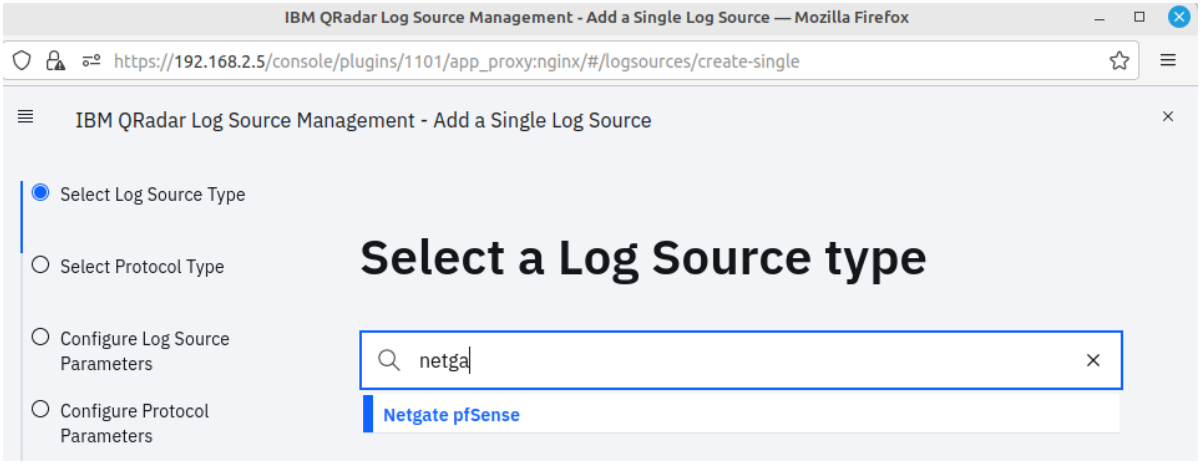
Στο εργαστηριακό μας περιβάλλον έχουμε αρχεία καταγραφής από Pfsense , Nginx , Squid, και συσκευές Linux. Αυτά είναι τα 4 είδη αρχείων καταγραφής που θα προβάλλονται από το SIEM Qradar. Δεν προσφέρει όμως συγκεκριμένα προγράμματα DSM Editors για pfSense, Nginx ή Squid. Γιαυτό τον λόγο χρειάζεται να εγκατασταθούν manual.

1. Κάντε λήψη του αρχείου DSM RPM από τον ιστότοπο υποστήριξης της IBM® (http://www.ibm.com/support).
2. Συνδεθείτε στο Qradar με sftp. Από την συσκευή που είστε συνδεμένοι στο Qradar πληκτρολογήστε στην γραμμή εντολών την εντολή “put” ακολουθούμενη από την διαδρομή και το αρχείο .rpm που κάνατε download στο βήμα 1.



Εικόνα 50 Sftp σύνδεση με Qradar

3. Τρέχοντας την παραπάνω εντολή μεταφέρουμε τα επιθυμητά .rpm αρχεία στο Qradar.
4. Επαναλαμβάνουμε την ίδια εντολή και για τα υπόλοιπα .rpm αρχεία (pfsense, Nginx)
5. Χρησιμοποιώντας SSH (εντολή ssh root@192.168.2.5) , συνδεθείτε στον κεντρικό υπολογιστή QRadar.
6. Μεταβείτε στον κατάλογο που περιλαμβάνει το ληφθέν αρχείο.
7. Πληκτρολογήστε την ακόλουθη εντολή:
8. yum -y εγκατάσταση <rpm_filename>
9. Συνδεθείτε στην κονσόλα του QRadar.
10. Στην καρτέλα Admin, κάντε κλικ στην επιλογή Deploy Changes



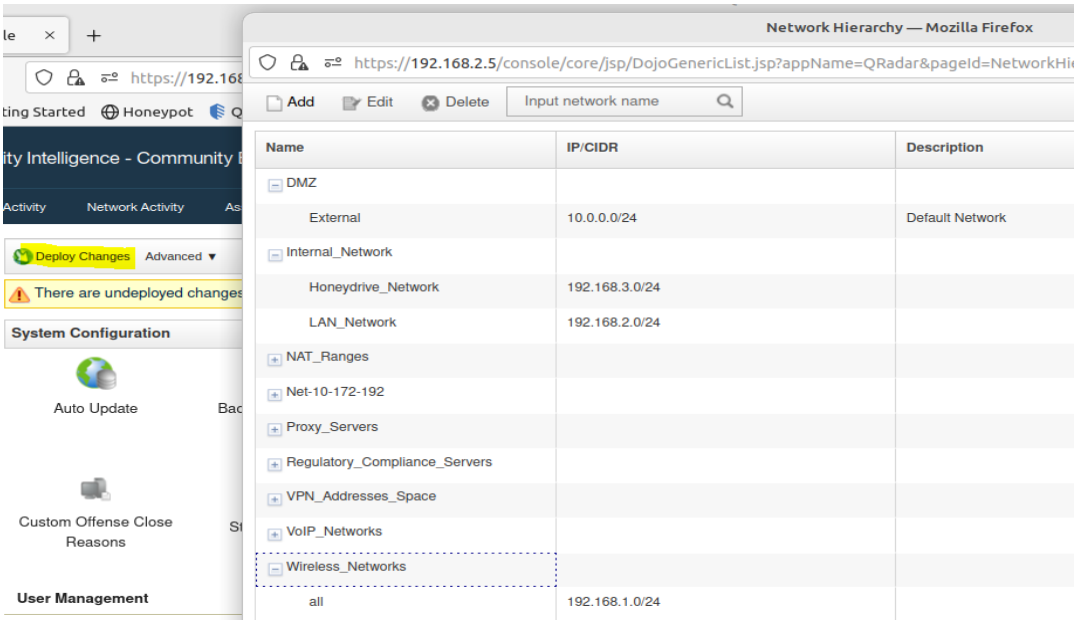
Εικόνα 51 Προβολή Εγκατεστημένου DSM για Pfsense Firewall

3.9.6 Ιεραρχία δικτύου (Network Hierarchy)

Η Ιεραρχία Δικτύου είναι μια δυνατότητα στο IBM QRadar που επιτρέπει στους χρήστες να οργανώνουν και να διαχειρίζονται τα στοιχεία του δικτύου τους σε μια ιεραρχική δομή. Παρέχει μια οπτική αναπαράσταση της τοπολογίας του δικτύου, καθιστώντας ευκολότερη την κατανόηση των σχέσεων μεταξύ διαφορετικών στοιχείων δικτύου, όπως υποδίκτυα, περιοχές IP και μεμονωμένες συσκευές.

Προσθήκη δικτύου στην ιεραρχία δικτύου:

1. Στο QRadar, μεταβείτε στην καρτέλα "Admin" και επιλέξτε " Network Hierarchy ".
2. Δημιουργήστε μια νέα ομάδα εντός της ιεραρχίας για να αντιπροσωπεύσετε το τμήμα δικτύου που θέλετε να προσθέσετε. Δώστε στην ομάδα ένα ουσιαστικό όνομα και περιγραφή.
3. Στην ομάδα που δημιουργήθηκε πρόσφατα, μπορείτε να προσθέσετε μεμονωμένα δίκτυα, υποδίκτυα ή περιοχές IP που ανήκουν στο ίδιο τμήμα.
4. Στην καρτέλα Admin, κάντε κλικ στην επιλογή Deploy Changes.



Εικόνα 52Network Hierarchy Qradar

3.9.7 Log Activity και δημιουργία Log Sources

Κατά την πρόσβαση στην καρτέλα "Log Activity" στο IBM QRadar, τα αρχεία καταγραφής παρουσιάζονται όπως παρακάτω. Αυτό συμβαίνει διότι χρειάζεται κανονικοποιηθούν σύμφωνα με τον DSM editor που έχουμε εγκαταστήσει προηγουμένως.

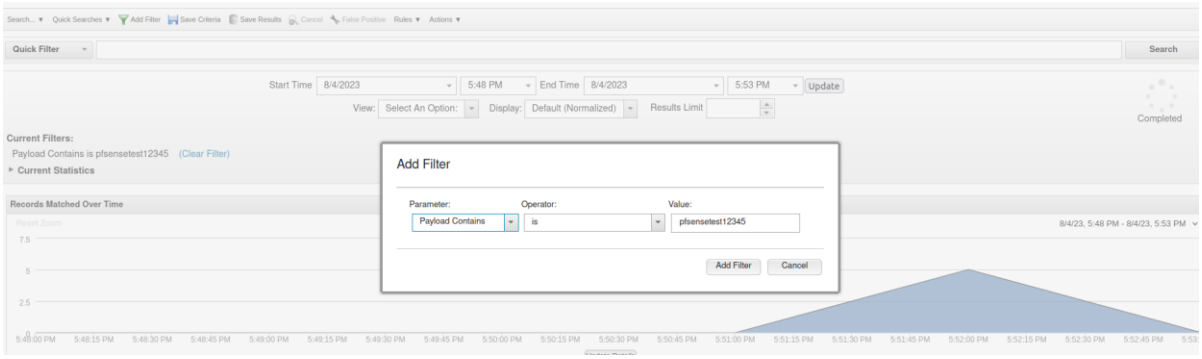
Event Name	Log Source
Unknown log event	SIM Generic Log DSM-7 :: csd35
Unknown log event	SIM Generic Log DSM-7 :: csd35
Unknown log event	SIM Generic Log DSM-7 :: csd35
Unknown log event	SIM Generic Log DSM-7 :: csd35

Εικόνα 53 Αρχική Μορφή Logs

Για να προβείτε σε αυτή την διαδικασία χρειάζεται αρχικά να αναγνωρίσετε ποιο log είναι , ποιας συσκευής. Στην συνέχεια για το εκάστοτε log που θα αναγνωρίζεται θα δημιουργείται και το αντίστοιχο Log Source.

3.9.8 Pfsense Log Source

1. Μεταβείτε γραμμή εντολών του pfsense και τρέξτε την εντολή
2. Logger pfsensetest12345
3. Μεταβείτε στο Log Activity του Qradar και κάντε αναζήτηση “Paylod Contains is pfsensetest12345”



Εικόνα 54 Αναζήτηση Payload Contains

4. Εμφανίζονται τα logs που ήρθαν στο Qradar και στο payload έχουν το συγκεκριμένο κείμενο.

Source and Destination Information

Source IP	192.168.2.1	**Destination IP**	192.168.2.1
Source Asset Name	192.168.2.1	**Destination Asset Name**	192.168.2.1
Source Port	0	**Destination Port**	0
Pre NAT Source IP		**Pre NAT Destination IP**	
Pre NAT Source Port	0	**Pre NAT Destination Port**	0
Post NAT Source IP		**Post NAT Destination IP**	
Post NAT Source Port	0	**Post NAT Destination Port**	0
Source IPv6	0:0:0:0:0:0:0:0	**Destination IPv6**	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	**Destination MAC**	00:00:00:00:00:00

Payload Information

utf hex base64

Wrap Text

<13>1 2023-08-04T17:52:14.038815+03:00 pfSense.home.localdomain root 89463 - - pfsensetest12345

Εικόνα 55 Log με το Κείμενο pfsensetest12345

5. Μέσω του Payload έρχεται και το αναγνωριστικό της συσκευής , το οποίο έστειλε το αρχείο καταγραφής. Όπως βλέπετε παραπάνω αυτό είναι pfsense.home.localdomain
6. Μεταβείτε στην καρτέλα "Admin". Από εκεί, κάντε κλικ στην εφαρμογή " Log Source Management".
7. Στην εφαρμογή Log Source Managemen, κάντε κλικ στο κουμπί " Add" για να ξεκινήσει η διαδικασία προσθήκης μιας νέας πηγής καταγραφής.
8. Επιλέξτε τον τύπο της πηγής καταγραφής που θέλετε να προσθέσετε. Στην προκειμένη περίπτωση Netgate Pfsense
9. Συμπληρώστε τις απαιτούμενες πληροφορίες για την πηγή καταγραφής, όπως τη διεύθυνση IP, το όνομα κεντρικού υπολογιστή, το αναγνωριστικό πηγής καταγραφής και άλλες συγκεκριμένες λεπτομέρειες ανάλογα με τον επιλεγμένο τύπο πηγής καταγραφής. Σαν Log Source identifier θα εισάγουμε pfsense.home.localdomain.
10. Μπορείτε να επιλέξετε να δοκιμάσετε τη σύνδεση με την πηγή καταγραφής για να διασφαλίσετε ότι το QRadar μπορεί να επικοινωνήσει με επιτυχία με τη συσκευή και να συλλέξει δεδομένα καταγραφής.
11. Τέλος, στην καρτέλα Admin, κάντε κλικ στην επιλογή Deploy Changes
12. Στην συνέχεια τα Logs θα είναι όπως στην παρακάτω εικόνα.

Event Name	Log Source	Event Count	Time ▼	Low Level Category	Source IP	Source Port	Destination IP	Destinati Port	Username	Magnitude
Firewall - Permit	Pfsense	15	Aug 4, 2023, 6:22:49 PM	Firewall Permit	192.168.2.5	56688	8.8.8.8	53	N/A	
Firewall - Permit	Pfsense	16	Aug 4, 2023, 6:22:39 PM	Firewall Permit	192.168.2.5	41287	8.8.8.8	53	N/A	
Firewall - Permit	Pfsense	16	Aug 4, 2023, 6:22:29 PM	Firewall Permit	192.168.2.5	57116	8.8.8.8	53	N/A	
Firewall - Deny	Pfsense	1	Aug 4, 2023, 6:22:25 PM	Firewall Deny	192.168.1.3	9487	192.168.2.1	9478	N/A	
Firewall - Permit	Pfsense	19	Aug 4, 2023, 6:22:19 PM	Firewall Permit	192.168.2.5	47401	8.8.8.8	53	N/A	
Firewall - Permit	Pfsense	7	Aug 4, 2023, 6:22:18 PM	Firewall Permit	10.0.0.10	49305	8.8.8.8	53	N/A	
Firewall - Permit	Pfsense	21	Aug 4, 2023, 6:22:05 PM	Firewall Permit	192.168.2.5	50640	8.8.8.8	53	N/A	
Firewall - Deny	Pfsense	5	Aug 4, 2023, 6:22:03 PM	Firewall Deny	192.168.2.1	5353	192.168.2.1	5353	N/A	
Firewall - Deny	Pfsense	5	Aug 4, 2023, 6:22:03 PM	Firewall Deny	192.168.1.3	5353	224.0.0.251	5353	N/A	
Firewall - Permit	Pfsense	33	Aug 4, 2023, 6:21:54 PM	Firewall Permit	192.168.2.5	55885	8.8.8.8	53	N/A	
Firewall - Deny	Pfsense	1	Aug 4, 2023, 6:21:48 PM	Firewall Deny	192.168.1.9	50576	224.0.0.253	3544	N/A	
Firewall - Permit	Pfsense	29	Aug 4, 2023, 6:21:39 PM	Firewall Permit	192.168.2.5	53151	8.8.8.8	53	N/A	
Firewall - Permit	Pfsense	7	Aug 4, 2023, 6:21:33 PM	Firewall Permit	10.0.0.10	45671	8.8.8.8	53	N/A	
Firewall - Deny	Pfsense	1	Aug 4, 2023, 6:21:32 PM	Firewall Deny	192.168.1.3	9999	192.168.2.1	9999	N/A	
Firewall - Permit	Pfsense	34	Aug 4, 2023, 6:21:29 PM	Firewall Permit	192.168.2.5	59879	8.8.8.8	53	N/A	
Firewall - Deny	Pfsense	1	Aug 4, 2023, 6:21:27 PM	Firewall Deny	192.168.1.3	9487	192.168.2.1	9478	N/A	
Firewall - Deny	Pfsense	8	Aug 4, 2023, 6:21:22 PM	Firewall Deny	192.168.1.9	60845	239.255.255.250	1900	N/A	
Firewall - Permit	Pfsense	28	Aug 4, 2023, 6:21:19 PM	Firewall Permit	192.168.2.5	37650	8.8.8.8	53	N/A	
Firewall - Deny	Pfsense	11	Aug 4, 2023, 6:21:09 PM	Firewall Deny	192.168.1.1	32916	239.255.255.250	1900	N/A	
Firewall - Permit	Pfsense	31	Aug 4, 2023, 6:21:09 PM	Firewall Permit	192.168.2.5	50193	8.8.8.8	53	N/A	

Εικόνα 56 Pfsense Logs in Qradar

3.9.9 Log Source Auto Discovered

Η εφαρμογή Log Source Management στο QRadar προσφέρει μια ισχυρή και βολική λειτουργία γνωστή ως "auto-discovery", η οποία απλοποιεί τη διαδικασία προσθήκης Log Source στο Qradar. Με την αυτόματη ανακάλυψη, το QRadar μπορεί αυτόματα να εντοπίσει και να αναγνωρίσει Log Source που υπάρχουν στο δίκτυο, απλοποιώντας τη διαδικασία διαμόρφωσης και ρύθμισης για τους διαχειριστές.

Αξιοποιώντας αυτή τη δυνατότητα, το QRadar εντοπίζει και συσχετίζει αβίαστα μια βασική πηγή καταγραφής: "Nginx HTTP Server@ pfsense.home.localdomain." η οποία έχει το ίδιο Log Source identifier με το Log source Pfsense που δημιουργήθηκε προηγουμένως.

Μέσω αυτής της απρόσκοπτης ενσωμάτωσης, το QRadar επεκτείνει το πεδίο εφαρμογής του για να συμπεριλάβει τα αρχεία καταγραφής HTTP που δημιουργούνται από διακομιστή HTTP Nginx. Αυτή η

συνεργασία εμπλουτίζει την ανάλυση του αρχείου καταγραφής μας με μια ολοκληρωμένη προβολή τόσο των δραστηριοτήτων του τείχους προστασίας όσο και των αλληλεπιδράσεων της κυκλοφορίας στον ιστό, ενισχύοντας την ικανότητά μας να εντοπίζουμε πιθανές απειλές και να ανταποκρινόμαστε προληπτικά σε τυχόν ανωμαλίες.

Name	Log Source Type	Creation Date	Last Event	Enabled	Groups	Auto Discovered	Log Source Identifier
NGINX HTTP Server @ pfSense.home.localdomain	NGINX HTTP Server	Aug 2, 2023 6:49 PM (UTC)	Aug 4, 2023 6:32 PM (UTC)	On	IIS/Apache2 Services	Yes	pfSense.home.localdomain
NGINX @LinuxMint	NGINX HTTP Server	Jul 5, 2023 11:39 PM (UTC)	Aug 4, 2023 5:09 PM (UTC)	On	IIS/Apache2 Services	No	linuxmint-dmz
Pfsense	Netgate pfSense	Jul 5, 2023 3:07 PM (UTC)	Aug 4, 2023 6:41 PM (UTC)	On	Firewall	No	pfSense.home.localdomain

Εικόνα 57 Log Source Auto Discovered

3.9.10 LinuxMint-Internal , LinuxMint-DMZ Log Sources

Τα βήματα προκειμένου να αναγνωρίσετε και να δημιουργήσετε τις 2 συσκευές Linux είναι ίδια με αυτά του pfsense. Με την διαφορά ότι μπορείτε

1. Σε κάθε συσκευή να χρησιμοποιήστε διαφορετικό κείμενο στην εντολή “Logger xxx” .
2. Στην συνέχεια θα κάνετε αναζήτηση στο Log Activity του Qaradar με το κείμενο στην εντολή Logger που θα έχετε εισάγει. Για παράδειγμα Payload Contains is xxx.
3. Κατά την δημιουργία του Log source , το αναγνωριστικό πηγής θα είναι ξεχωριστό για κάθε συσκευή.

Source and Destination Information

Source IP	10.0.0.10	Destination IP	10.0.0.10
Source Asset Name	10.0.0.10	Destination Asset Name	10.0.0.10
Source Port	0	Destination Port	0
Pre NAT Source IP		Pre NAT Destination IP	
Pre NAT Source Port	0	Pre NAT Destination Port	0
Post NAT Source IP		Post NAT Destination IP	
Post NAT Source Port	0	Post NAT Destination Port	0
Source IPv6	0:0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00

Payload Information

utf hex base64

Wrap Text

```
<85>Aug  4 18:03:21 LinuxMint-DMZ sudo:   george : PWD=/home/george ; USER=root ; COMMAND=/usr/lib/linuxmint/mintUpdate/dpkg_lock_check.sh
```

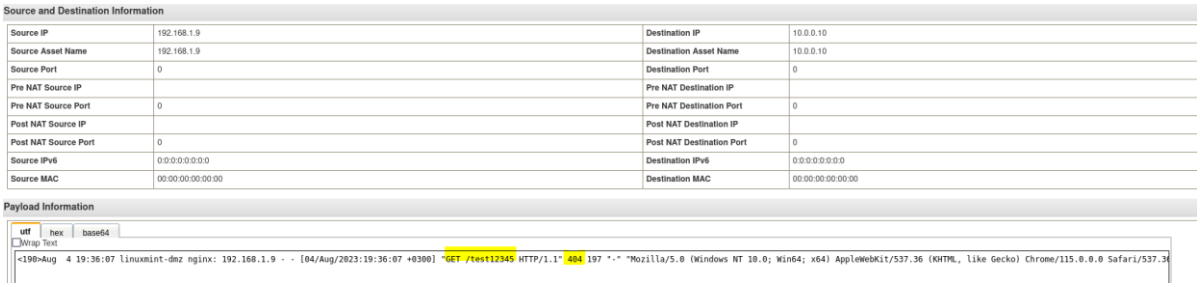
Εικόνα 58 Payload απο LinuxMint-DMZ

3.9.11 NGINX@ LinuxMint-DMZ Log Source

Το συγκεκριμένο Log Source προέρχεται από την ίδια συσκευή με το LinuxMint-DMZ. Με διαφορετικό Log Source identifier. Επιπλέον το παρών Log Source παρέχει HTTP logs που αφορούν το web service Nginx. Για να δίνει η κανονικοποίηση μπορείτε να ακολουθήσετε τα εξής βήματα.

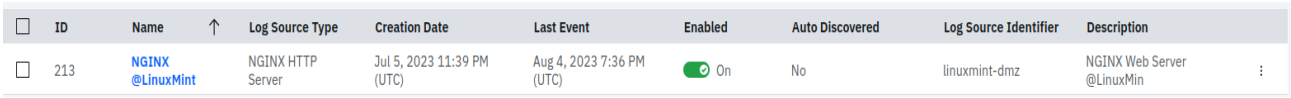
1. Μεταβείτε στην ιστοσελίδα του Nginx web server Πληκτρολογώντας την WAN διεύθυνση του pfsense από μια οποιαδήποτε συσκευή του δικτύου. http://192.168.1.11

2. Συμπληρώστε στο URL του web browser την διεύθυνση /test12345. Δηλαδή http://192.168.1.11/test12345
3. Μεταβείτε στο Log Activity του Qradar και κάντε αναζήτηση “Paylod Contains is test12345”
4. Εμφανίζονται τα logs που ήρθαν στο Qradar και στο payload έχουν το συγκεκριμένο κείμενο.



Εικόνα 59 Log με το Κείμενο test12345

5. Παρατηρείται ότι ως Log Source Identifier είναι Linuxmint-dmz
6. Μεταβείτε στην καρτέλα "Admin". Από εκεί, κάντε κλικ στην εφαρμογή " Log Source Management".
7. Στην εφαρμογή Log Source Managemen, κάντε κλικ στο κουμπί " Add" για να ξεκινήσει η διαδικασία προσθήκης μιας νέας πηγής καταγραφής.
8. Επιλέξτε τον τύπο της πηγής καταγραφής που θέλετε να προσθέσετε. Στην προκειμένη περίπτωση NGINX HTTP Server
9. Συμπληρώστε τις απαιτούμενες πληροφορίες για την πηγή καταγραφής, όπως τη διεύθυνση IP, το όνομα κεντρικού υπολογιστή, το αναγνωριστικό πηγής καταγραφής και άλλες συγκεκριμένες λεπτομέρειες ανάλογα με τον επιλεγμένο τύπο πηγής καταγραφής. Σαν αναγνωριστικό πηγής θα εισάγουμε Linuxmint-dmz.
10. Τέλος, στην καρτέλα Admin, κάντε κλικ στην επιλογή Deploy Changes



Εικόνα 60 NGINX@ LinuxMint-DMZ Log Source

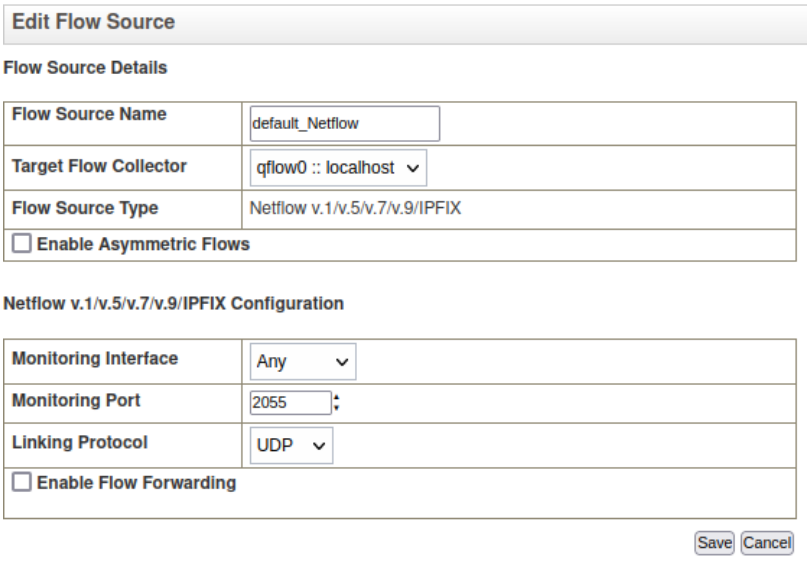
3.9.12 Ανάλυση κυκλοφορίας δικτύου στο Qradar

Η ανάλυση Κυκλοφορίας Δικτύου στο QRadar περιλαμβάνει τη συλλογή και ανάλυση δεδομένων ροής δικτύου για την απόκτηση γνώσεων σχετικά με τις επικοινωνίες δικτύου και τον εντοπισμό πιθανών απειλών ασφαλείας.

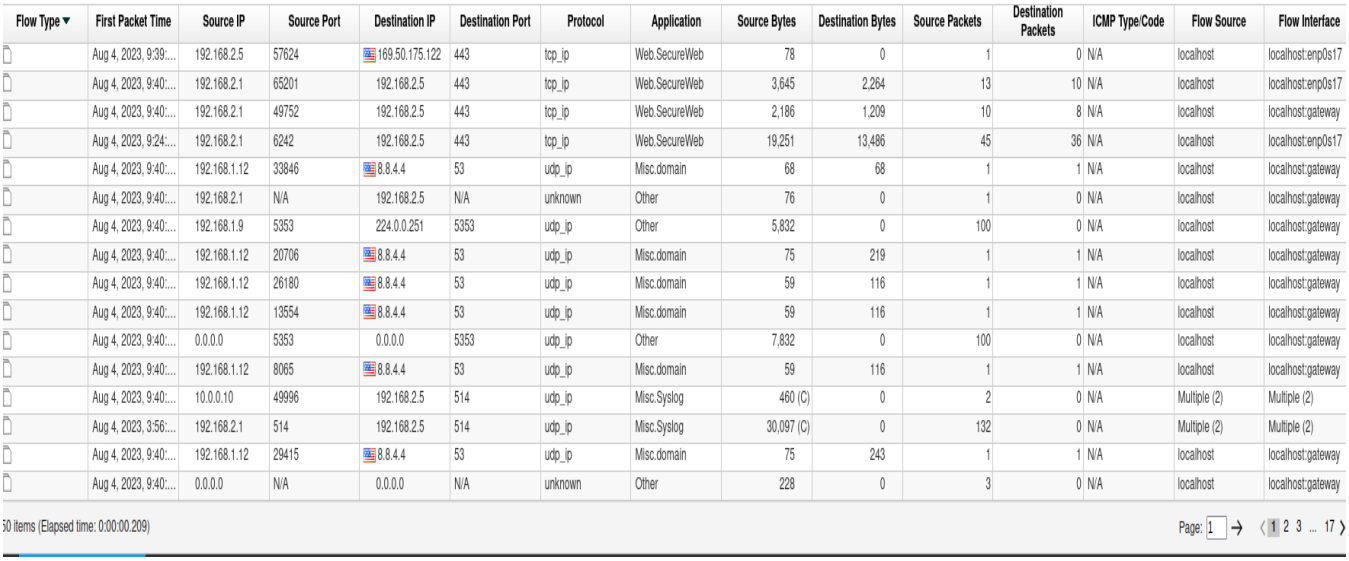
Για να ενεργοποιήσετε τις ροές δικτύου στο QRadar, ακολουθήστε τα εξής βήματα:

1. Μεταβείτε στην καρτέλα Admin στο επάνω μενού πλοήγησης και επιλέξτε " Flow Sources " .
2. Κάντε κλικ στο κουμπί " Add " για να προσθέσετε μια νέα πηγή ροής.
3. Επιλέξτε το κατάλληλο πρωτόκολλο ροής που θέλετε να ενεργοποιήσετε (NetFlow, J-Flow, sFlow ή IPFIX) με βάση τις δυνατότητες των συσκευών δικτύου σας.
4. Παρέχετε τις απαραίτητες λεπτομέρειες διαμόρφωσης για την πηγή ροής, όπως τη διεύθυνση IP της πηγής, τη θύρα ακρόασης και το πρότυπο ροής.

5. Αποθηκεύστε τη διαμόρφωση της πηγής ροής.



Εικόνα 61 Ενεργοποίηση των Ροών Δικτύου



Flow Type	First Packet Time	Source IP	Source Port	Destination IP	Destination Port	Protocol	Application	Source Bytes	Destination Bytes	Source Packets	Destination Packets	ICMP Type/Code	Flow Source	Flow Interface
	Aug 4, 2023, 9:39:...	192.168.2.5	57624	169.50.175.122	443	tcp_ip	Web.SecureWeb	78	0	1	0	N/A	localhost	localhost:enp0s17
	Aug 4, 2023, 9:40:...	192.168.2.1	65201	192.168.2.5	443	tcp_ip	Web.SecureWeb	3,645	2,264	13	10	N/A	localhost	localhost:enp0s17
	Aug 4, 2023, 9:40:...	192.168.2.1	49752	192.168.2.5	443	tcp_ip	Web.SecureWeb	2,186	1,209	10	8	N/A	localhost	localhost:gateway
	Aug 4, 2023, 9:24:...	192.168.2.1	6242	192.168.2.5	443	tcp_ip	Web.SecureWeb	19,251	13,486	45	36	N/A	localhost	localhost:enp0s17
	Aug 4, 2023, 9:40:...	192.168.1.12	33846	8.8.4.4	53	udp_ip	Misc.domain	68	68	1	1	N/A	localhost	localhost:gateway
	Aug 4, 2023, 9:40:...	192.168.2.1	N/A	192.168.2.5	N/A	unknown	Other	76	0	1	0	N/A	localhost	localhost:gateway
	Aug 4, 2023, 9:40:...	192.168.1.9	5353	224.0.0.251	5353	udp_ip	Other	5,832	0	100	0	N/A	localhost	localhost:gateway
	Aug 4, 2023, 9:40:...	192.168.1.12	20706	8.8.4.4	53	udp_ip	Misc.domain	75	219	1	1	N/A	localhost	localhost:gateway
	Aug 4, 2023, 9:40:...	192.168.1.12	26180	8.8.4.4	53	udp_ip	Misc.domain	59	116	1	1	N/A	localhost	localhost:gateway
	Aug 4, 2023, 9:40:...	192.168.1.12	13554	8.8.4.4	53	udp_ip	Misc.domain	59	116	1	1	N/A	localhost	localhost:gateway
	Aug 4, 2023, 9:40:...	0.0.0.0	5353	0.0.0.0	5353	udp_ip	Other	7,832	0	100	0	N/A	localhost	localhost:gateway
	Aug 4, 2023, 9:40:...	192.168.1.12	8065	8.8.4.4	53	udp_ip	Misc.domain	59	116	1	1	N/A	localhost	localhost:gateway
	Aug 4, 2023, 9:40:...	10.0.0.10	49996	192.168.2.5	514	udp_ip	Misc.Syslog	460 (C)	0	2	0	N/A	Multiple (2)	Multiple (2)
	Aug 4, 2023, 3:56:...	192.168.2.1	514	192.168.2.5	514	udp_ip	Misc.Syslog	30,097 (C)	0	132	0	N/A	Multiple (2)	Multiple (2)
	Aug 4, 2023, 9:40:...	192.168.1.12	29415	8.8.4.4	53	udp_ip	Misc.domain	75	243	1	1	N/A	localhost	localhost:gateway
	Aug 4, 2023, 9:40:...	0.0.0.0	N/A	0.0.0.0	N/A	unknown	Other	228	0	3	0	N/A	localhost	localhost:gateway

50 items (Elapsed time: 0:00:00.209) Page: 1 → 〈 1 2 3 ... 17 〉

Εικόνα 62 Προεπισκόπηση Ροών Δικτύου

3.9.13 Reference Sets στο Qradar

Τα **Reference Sets** στο QRadar είναι συλλογές δεδομένων που χρησιμοποιούνται για να αποθηκεύουν και να συγκρίνουν δυναμικά σύνολα τιμών όπως διευθύνσεις IP, ονόματα τομέων, URLs, hashes και άλλα. Οι τιμές αυτές χρησιμοποιούνται στις λογικές των κανόνων του QRadar για τη συσχέτιση και τον εντοπισμό απειλών.

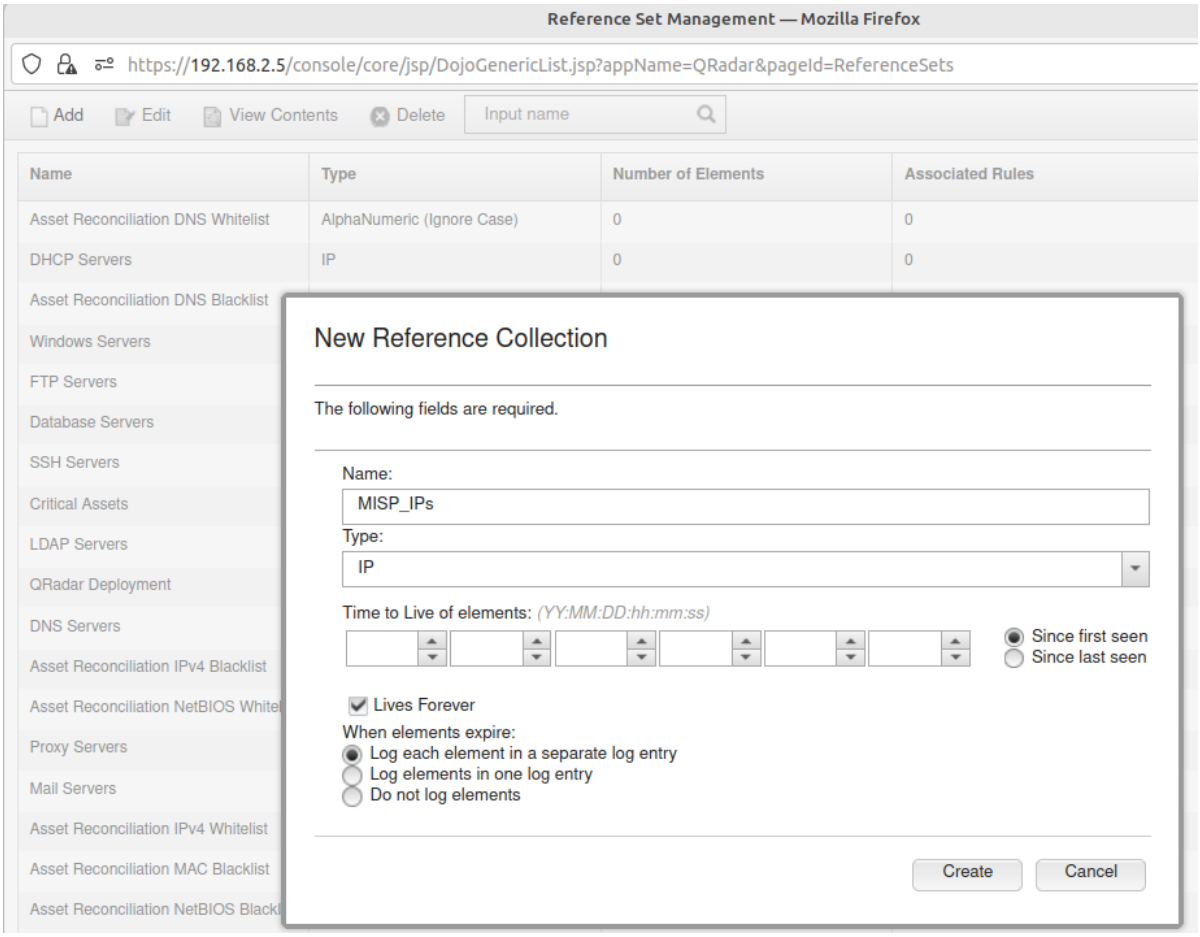
Τα **Reference Sets** είναι ιδιαίτερα χρήσιμα όταν θέλουμε να διατηρούμε λίστες με δυναμικά ενημερούμενες τιμές, όπως κακόβουλες διευθύνσεις IP από το MISP, οι οποίες μπορούν να ενημερώνονται τακτικά χωρίς την ανάγκη να τροποποιούνται χειροκίνητα οι κανόνες ή τα logs του συστήματος.

Ακολουθούν τα βήματα για τη δημιουργία του **Reference Set "MISP_IPs"** στο QRadar, το οποίο θα χρησιμοποιηθεί για να αποθηκεύει και να ενημερώνει δυναμικά διευθύνσεις IP από το MISP:

1. Από το βασικό μενού του QRadar, επιλέξτε **"Admin"**.
2. Στην ενότητα **"Reference Data"**, επιλέξτε την επιλογή **"Reference Sets"** για να δείτε και να διαχειριστείτε τα reference sets του συστήματος.
3. Πατήστε το κουμπί **"Add"** για να δημιουργήσετε ένα νέο reference set.
4. Στο πεδίο **"Name"**, δώστε το όνομα **"MISP_IPs"**.
5. Στο πεδίο **"Element Type"**, επιλέξτε **"IP"** καθώς πρόκειται για συλλογή διευθύνσεων IP που θα λαμβάνουμε από το MISP.
6. Στο πεδίο **"Time to Live (TTL)"**, καθορίστε τη διάρκεια για την οποία θέλετε να παραμείνουν οι τιμές στο reference set, εάν το επιθυμείτε (π.χ., 30 days). Αν δεν επιθυμείτε συγκεκριμένο χρόνο λήξης, αφήστε το κενό.
7. Πατήστε **"Create"** για να αποθηκεύσετε το reference set **"MISP_IPs"**. Τώρα το reference set έχει δημιουργηθεί και είναι έτοιμο να δεχτεί δεδομένα.

Αφού δημιουργηθεί το reference set **"MISP_IPs"** και εισαχθούν οι κακόβουλες IPs, μπορείτε να χρησιμοποιήσετε αυτό το set σε κανόνες συσχέτισης του QRadar.

Για παράδειγμα, μπορείτε να δημιουργήσετε έναν κανόνα που ανιχνεύει traffic από ή προς τις IPs του **MISP_IPs**, επιτρέποντας τον γρήγορο εντοπισμό απειλών με βάση τα δεδομένα που λαμβάνουμε από το MISP.



Εικόνα 63 Ref. Set "MISP_IPs"

3.9.14 Κανόνες στο Qradar

Στο QRadar, οι κανόνες είναι τα θεμελιώδη στοιχεία του συστήματος που επιτρέπουν τον εντοπισμό και την ανάλυση συμβάντων ασφαλείας. Αποτελούνται από συνθήκες ή κριτήρια που αξιολογούν τα εισερχόμενα δεδομένα καταγραφής και συμβάντων δικτύου για τον εντοπισμό συγκεκριμένων μοτίβων ή συμπεριφορών ενδεικτικών απειλών ασφαλείας ή παραβιάσεων πολιτικής. Οι κανόνες λειτουργούν ως η ραχοκοκαλιά των πληροφοριών ασφαλείας στο QRadar, βοηθώντας στην αυτοματοποίηση της διαδικασίας εντοπισμού και απόκρισης.

Τα Building blocksστο QRadar είναι προκαθορισμένα σύνολα συνθηκών ή κριτηρίων που μπορούν να χρησιμοποιηθούν ως επαναχρησιμοποιήσιμα στοιχεία εντός κανόνων. Λειτουργούν ως δομικά στοιχεία επειδή ενσωματώνουν συγκεκριμένη λογική ή συμπεριφορά που μπορεί να εφαρμοστεί σε πολλούς κανόνες, προωθώντας τη συνέπεια και την αποτελεσματικότητα στη δημιουργία κανόνων. Αξιοποιώντας Building blocks, οι αναλυτές ασφαλείας μπορούν να απλοποιήσουν τη διαδικασία δημιουργίας κανόνων και να εξασφαλίσουν συνεπή κριτήρια σε όλο το σύστημα.

Οι κανόνες στο QRadar μπορούν να σχεδιαστούν για να εκτελούν διάφορες ενέργειες εφόσον πληρούνται οι καθορισμένες συνθήκες. Αυτές οι ενέργειες περιλαμβάνουν:

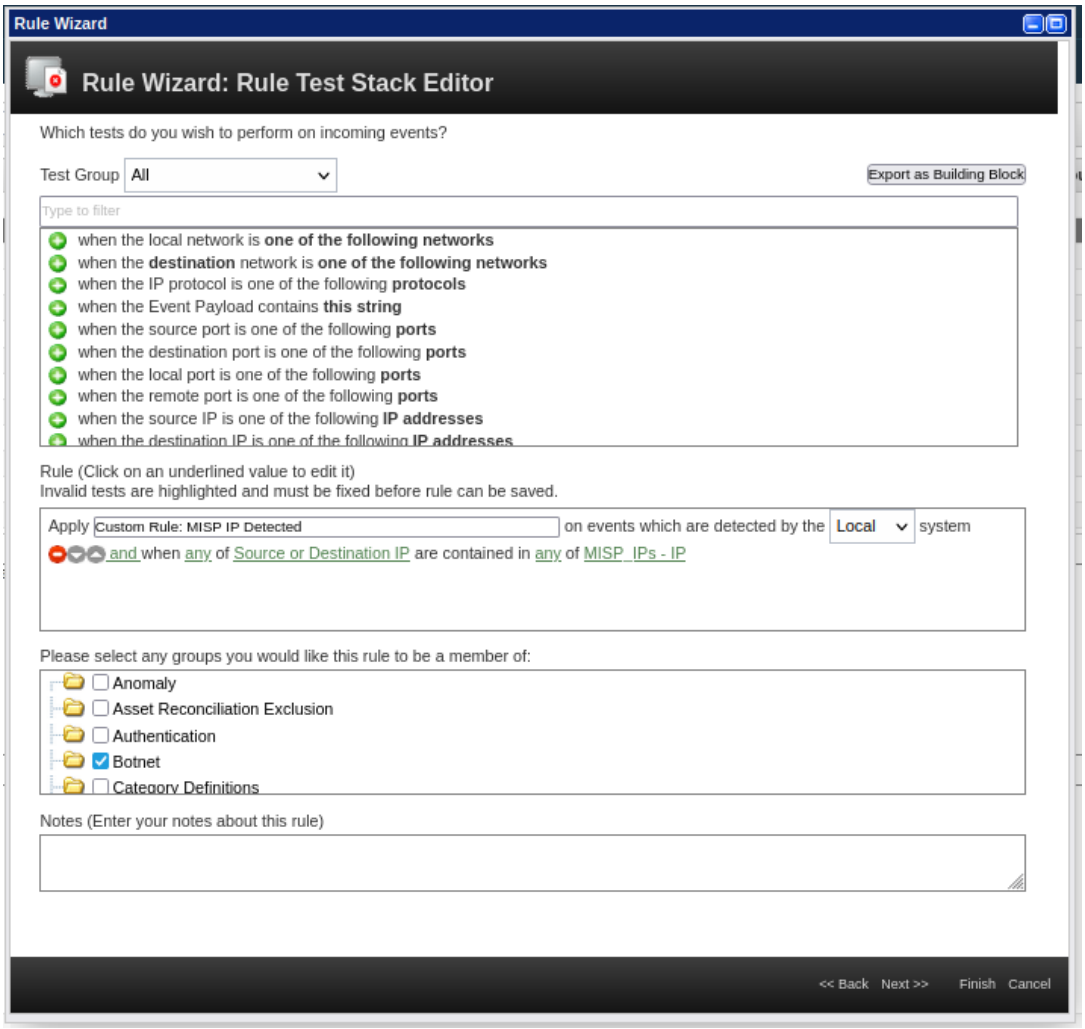
- Δημιουργία offenses, τα οποία είναι συγκεντρωτικά συμβάντα ασφαλείας που αντιπροσωπεύουν πιθανές απειλές.
- Επιπλέον, οι κανόνες μπορούν να αποστέλλουν ειδοποιήσεις μέσω email.
- Να δημιουργούν νέα συμβάντα ή να επικαλούνται ενέργειες απόκρισης, όπως ο αποκλεισμός μιας ύποπτης διεύθυνσης IP ή η απομόνωση ενός παραβιασμένου κεντρικού υπολογιστή.

3.9.15 Δημιουργία κανόνων

Οι **κανόνες** στο QRadar είναι λογικές δηλώσεις που χρησιμοποιούνται για την ανάλυση και τη συσχέτιση δεδομένων από τα logs και τα δίκτυα. Οι κανόνες βοηθούν στο να εντοπίζονται ύποπτες ή κακόβουλες δραστηριότητες, να παράγονται alerts και να δημιουργούνται αναφορές. Ένας κανόνας μπορεί να ανιχνεύει δραστηριότητα που πληροί συγκεκριμένα κριτήρια, όπως ύποπτες διευθύνσεις IP, κακόβουλα αρχεία, ή ασυνήθιστη κίνηση δικτύου.

Ακολουθούν τα βήματα για να δημιουργήσετε έναν κανόνα που θα στέλνει ένα email alert όταν η **source IP** ανήκει στο reference set **MISP_IPs**:

1. Από το κύριο μενού, επιλέξτε την καρτέλα **"Offenses"** και στη συνέχεια πατήστε στο **"Rules"**.
2. Πατήστε το κουμπί **"Actions"** και στη συνέχεια επιλέξτε **"New Rule"**.
3. Επιλέξτε την κατηγορία του κανόνα, π.χ., **"Events"**
4. Στο παράθυρο του κανόνα, καθορίστε το λογικό κριτήριο που θέλετε να ισχύει. Για αυτόν τον κανόνα, πρέπει να προσθέσουμε έναν όρο που λέει ότι η **Source IP** πρέπει να ανήκει στο reference set **MISP_IPs**.
5. Μετά την προσθήκη των κριτηρίων, πρέπει να ορίσετε τη δράση που θα εκτελεστεί όταν ο κανόνας ενεργοποιηθεί.
6. Πατήστε το κουμπί **"Add Response"** και επιλέξτε **"Send Email"**.
7. Στη φόρμα, συμπληρώστε τις λεπτομέρειες του email
8. Αφού προσθέσετε όλα τα κριτήρια και τις δράσεις, δώστε ένα όνομα στον κανόνα σας (π.χ., **"Custom Rule:MISP IP Detected"**) και πατήστε **"Save"**.



Εικόνα 64 Custom Rule: MISP IP Detected

4. Ανάπτυξη Διασύνδεσης MISP,Qradar και PfSense

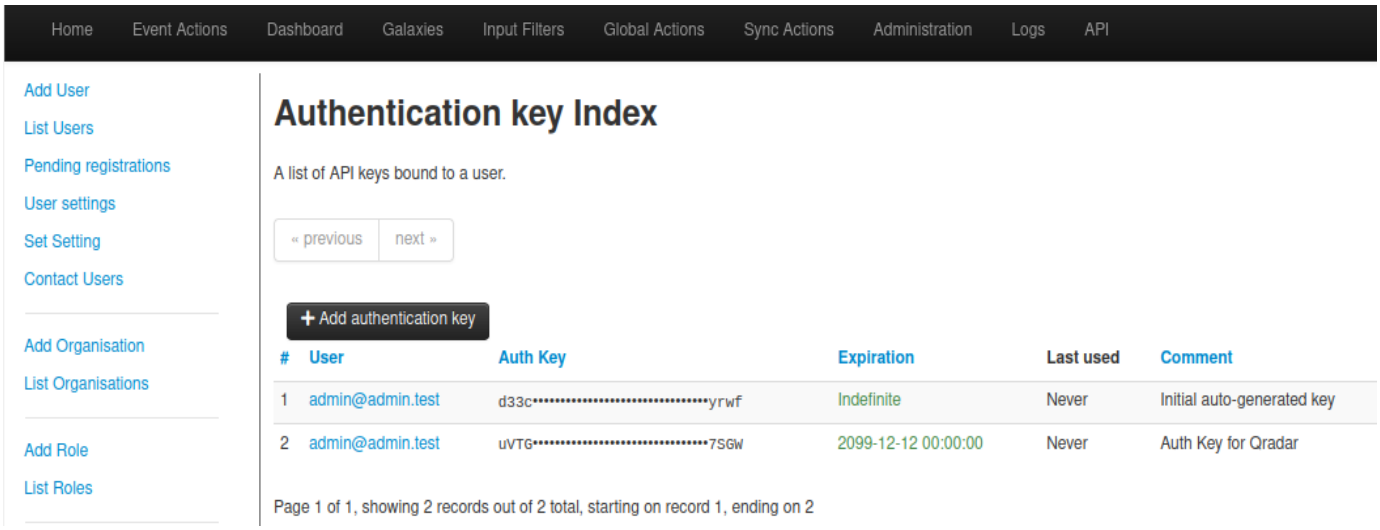
Το κεφάλαιο αυτό περιγράφει την υλοποίηση της διασύνδεσης μεταξύ των MISP, Qradar και pfSense μέσω Bash scripts. Παρουσιάζονται τα βήματα για την αποστολή και επεξεργασία πληροφοριών απειλών μεταξύ των συστημάτων. Η διασύνδεση επιτρέπει την αυτοματοποίηση και την αποτελεσματικότερη ανταπόκριση σε απειλές.

4.1 Διασύνδεση Με Bash Scripting (MISP -> Qradar)

1. **Δημιουργία Authentication Key στο MISP**

Αρχικά, συνδεθήκαμε στο περιβάλλον του MISP και δημιουργήσαμε ένα **Auth Key** για να το χρησιμοποιήσουμε στο script. Το κλειδί αυτό μας επιτρέπει να έχουμε πρόσβαση στα δεδομένα του MISP μέσω του API του.

Κατά τη δημιουργία του κλειδιού, προσθέσαμε το comment **"Auth Key for QRadar"**, έτσι ώστε να γνωρίζουμε ότι αυτό το κλειδί θα χρησιμοποιηθεί στη διασύνδεση με το QRadar.

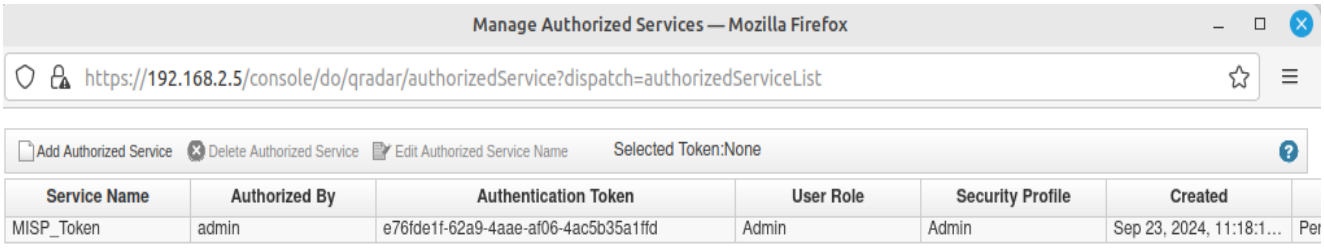


Εικόνα 65 MISP API KEY

2. **Δημιουργία Authentication Token στο QRadar**

Στη συνέχεια, συνδεθήκαμε στο QRadar και δημιουργήσαμε ένα **Auth Token**. Αυτό το token παρέχει την απαραίτητη ασφάλεια για τη διασύνδεση και επιτρέπει στο script να εισάγει δεδομένα στο QRadar μέσω του API.

Το token αυτό χρησιμοποιείται για την εισαγωγή των IOCs στο reference set που έχουμε δημιουργήσει (π.χ. **MISP_IPs**).



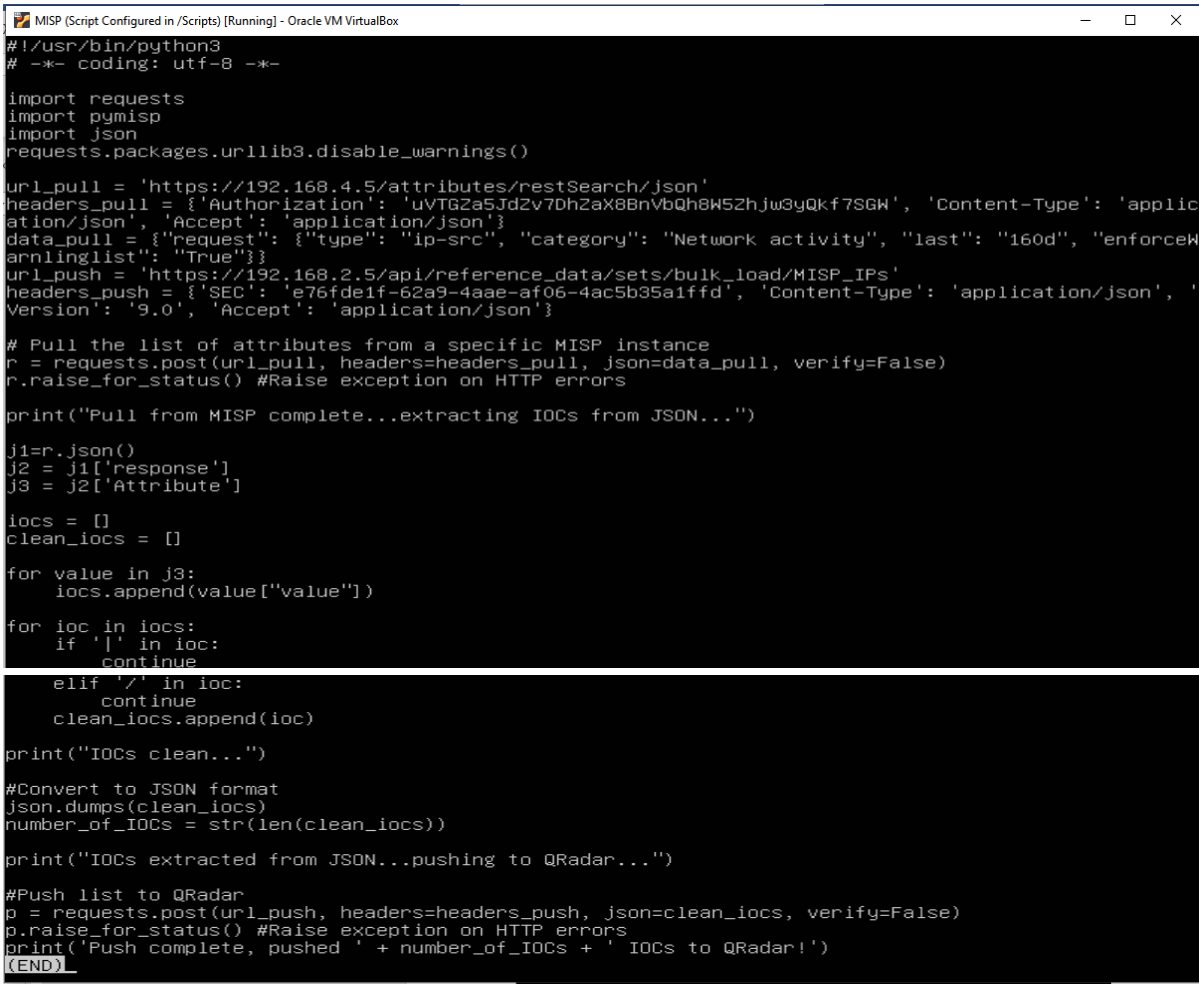
Εικόνα 66 Auth. Token Qradar

3. **Τοποθέτηση και Ρύθμιση του Script στο MISP Device**

Μεταβήκαμε στον server του MISP (IP: **192.168.4.5**) και τοποθετήσαμε το αρχείο **master_qradar_misp_ipsrc.py**.

Το script αυτό είναι υπεύθυνο για την ανάκτηση των IOCs από το MISP και την εισαγωγή τους στο QRadar.

Ανοίξαμε το script και συμπληρώσαμε τα απαραίτητα στοιχεία:



Εικόνα 67 Script MISP-Qradar Integration

4. **Δημιουργία Cron Job για Αυτόματη Εκτέλεση του Script**

Για να αυτοματοποιήσουμε τη διαδικασία και να ενημερώνουμε το reference set με νέες IPs, δημιουργήσαμε ένα cron job που εκτελεί το script κάθε 5 ημέρες.

Ανοίξαμε τον crontab με την εντολή: **crontab -e**

Προσθέσαμε την παρακάτω γραμμή στο αρχείο crontab:

0 0 */5 * * /usr/bin/python3 /path/to/master_qradar_misp_ipsrc.py

5. **Χρήση του Reference Set σε Κανόνες QRadar**

Το reference set **MISP_IPs** χρησιμοποιείται στον κανόνα **Custom Rule:MISP IP Detected (7.8.1)** του QRadar που παρακολουθεί τις IPs για πιθανές απειλές.

Όταν εντοπίζεται traffic από μια IP που υπάρχει στο **MISP_IPs**, το QRadar ενεργοποιεί τον κανόνα και δημιουργεί alerts, διευκολύνοντας την ταχεία αντίδραση των αναλυτών.

Με τον ίδιο τρόπο και με παρόμοια scripts που υπάρχουν εδώ: https://github.com/syloktools/MISP-QRADAR-REFERENCE-SET-BUILDER, μπορούμε να υλοποιήσουμε την αποστολή και για άλλα IOCs όπως

Hashes, **Destination IPs**, και **Domains**, επιτρέποντας έτσι την ενσωμάτωση ποικίλων τύπων δεικτών απειλών στο QRadar για πιο ολοκληρωμένη ανάλυση και προστασία του δικτύου.

4.2 Διασύνδεση Με Bash Scripting (MISP -> Snort)

1. **Δημιουργία του Python Script για την Ανάκτηση των IOCs από το MISP**

Γράψαμε ένα Python script το οποίο εκτελεί τα παρακάτω:

root@ubuntu: /Scripts

File Edit View Search Terminal Help

```
import json
requests.packages.urllib3.disable_warnings()

url_pull = 'https://192.168.4.5/attributes/restSearch/json'
headers_pull = {
    'Authorization': 'uVTGZa5JdZv7DhZaX8BnVbQh8W5Zhjw3yQkf7SGW',
    'Content-Type': 'application/json',
    'Accept': 'application/json'
}
data_pull = {
    "request": {
        "type": "ip-src",
        "category": "Network activity",
        "last": "160d",
        "enforceWarnlinglist": "True"
    }
}

# Pull the list of attributes from a specific MISP instance
r = requests.post(url_pull, headers=headers_pull, json=data_pull, verify=False)
r.raise_for_status()  # Raise exception on HTTP errors

print("Pull from MISP complete...extracting IOCs from JSON...")

j1 = r.json()
j2 = j1['response']
j3 = j2['Attribute']

iocs = []
clean_iocs = []

for value in j3:
    iocs.append(value["value"])

for ioc in iocs:
    if '|' in ioc or '/' in ioc:
        continue
    clean_iocs.append(ioc)

print("IOCs clean...")

# Save the IOCs to a text file on the MISP server
output_file = 'pfsense_iocs.txt'  # Change this to your desired output path
with open(output_file, 'w') as f:
    for ioc in clean_iocs:
        f.write(ioc + '\n')

print(f"IOCs saved to {output_file}. Total IOCs: {len(clean_iocs)}")
```

Εικόνα 68 pfsense__misp_ipsrc.py

2. **Εξαγωγή των IOCs σε Αρχείο Κειμένου**

Το script δημιουργεί ένα αρχείο με τα καθαρισμένα IOCs, το οποίο αποθηκεύεται στον MISP server με όνομα pfsense_iocs.txt

3. **Διαμόρφωση SSH για Ασφαλή Μεταφορά χωρίς Κωδικό**

Για να αποφύγουμε την εισαγωγή κωδικού κάθε φορά που στέλνουμε το αρχείο στο pfSense, δημιουργήσαμε ένα ζεύγος SSH κλειδιών

Εκτελέσαμε την εντολή: ssh-keygen -t rsa -b 4096

Αντιγράψαμε το public key στο pfSense: ssh-copy-id admin@192.168.4.1

Ενεργοποιήσαμε τον SSH agent και προσθέσαμε το private key:

eval "$(ssh-agent -s)"

ssh-add ~/.ssh/id_rsa

4. **Δημιουργία Cron Job για Αυτόματη Εκτέλεση του Script κάθε 5 Μέρες**

Για να εκτελείται το script που τραβάει τα IOCs από το MISP και τα αποστέλλει στο Pfsense κάθε 5 μέρες, προσθέσαμε το παρακάτω cron job:

0 0 */5 * * /Scripts/pfsense_misp_ipsrc.py

Για να γίνονται προσθήκη στο αρχείο των IOCs στο pfSense κάθε 6 μέρες, προσθέσαμε το εξής cron job:

0 0 */6 * * cat /path/to/local/pfsense_iocs.txt | ssh admin@192.168.4.1 "cat >> /var/db/snort/iprep/pfsense_iocs.txt" >> /path/to/logfile.log 2>&1

4.3 Διασύνδεση Με Bash Scripting (Qradar -> Snort)

Στην παρούσα διαδικασία, περιγράφουμε τα βήματα που ακολουθήσαμε για τη διασύνδεση του QRadar με το PfSense, χρησιμοποιώντας Bash scripting. Στόχος είναι η αυτόματη συλλογή κακόβουλων IPs από το QRadar και η αποστολή τους στο Snort του PfSense για ενίσχυση της προστασίας του δικτύου. Μέσω αυτής της μεθόδου, θα εξασφαλίσουμε ότι οι κακόβουλες IPs που ανιχνεύονται από το QRadar θα ενημερώνονται συνεχώς στο PfSense, ενισχύοντας την αποτελεσματικότητα του συστήματος ασφαλείας μας.

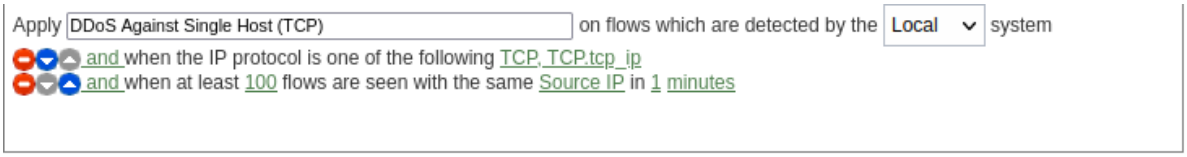
1. **Δημιουργία κανόνα στο QRadar:**

Αρχικά, δημιουργούμε έναν κανόνα στο QRadar ο οποίος ανιχνεύει επιθέσεις DDoS.

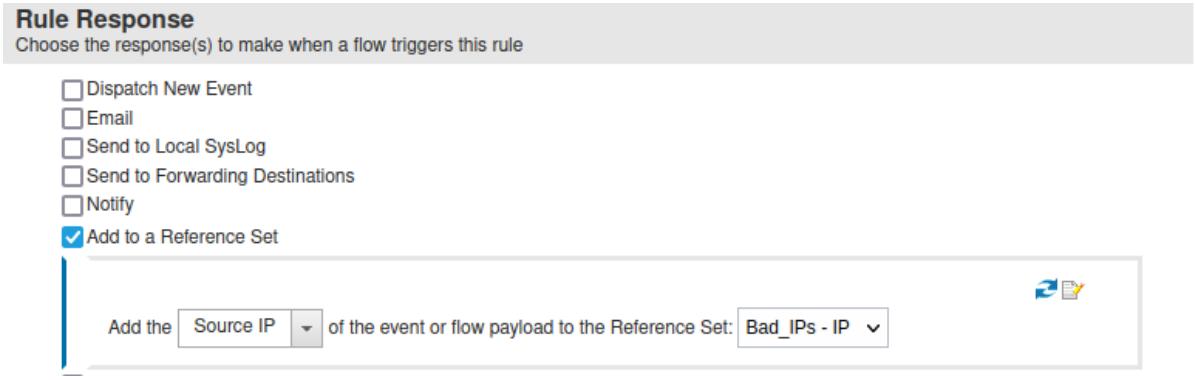
Ο κανόνας ενεργοποιείται όταν παρατηρείται traffic από την ίδια IP, με:

- Πρωτόκολλο TCP.
- Τουλάχιστον 100 ροές (flows) από τον ίδιο source σε 1 λεπτό.

Όταν ο κανόνας ενεργοποιηθεί, αποθηκεύει την κακόβουλη IP στο reference set "**Bad_IPs**."



Εικόνα 69 DDoS Against Single Host (TCP)



Εικόνα 70 DDoS Against Single Host (TCP)- Response

2. **Δημιουργία Bash Script για αποστολή IPs στο Snort του PfSense:**

Το παρακάτω script δημιουργείται για να εξάγει τις IPs από το reference set του QRadar και να τις στέλνει στο Snort του PfSense:

```
[root@localhost bin]# cat export_qradar_bad_ips.sh
#!/bin/bash
#navigate to the QRadar bin directory
cd /opt/qradar/bin/

# List the reference set "Bad_IPs" and grep for "Data=" to extract the content
./ReferenceDataUtil.sh list "Bad_IPs" [displayContents] | grep "Data=" > temp_qradar_bad_IPs.txt

# Use awk to extract only the IPs from the output and save to a new file
awk -F'=' '{print $2}' temp_qradar_bad_IPs.txt > qradar_bad_ips.txt

# Transfer the extracted IPs to the remote server (adjust the path and user accordingly)
scp qradar_bad_ips.txt admin@192.168.2.1:/var/db/snort/iprep

# Cleanup temporary file
rm temp_qradar_bad_IPs.txt
```

Εικόνα 71 export_qradar_bad_ips.sh

3. **Διαμόρφωση SSH για Ασφαλή Μεταφορά χωρίς Κωδικό**

Για να αποφύγουμε την εισαγωγή κωδικού κάθε φορά που στέλνουμε το αρχείο στο pfSense, δημιουργήσαμε ένα ζεύγος SSH κλειδιών

Εκτελέσαμε την εντολή: ssh-keygen -t rsa -b 4096

Αντιγράψαμε το public key στο pfSense: ssh-copy-id admin@192.168.4.1

Ενεργοποιήσαμε τον SSH agent και προσθέσαμε το private key:

eval "$(ssh-agent -s)"

ssh-add ~/.ssh/id_rsa

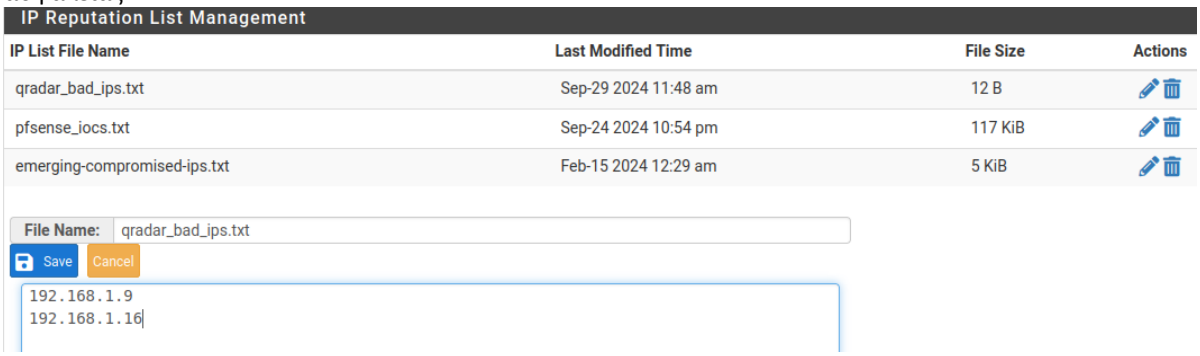
4. **Χρονοπρογραμματισμός της αυτόματης εκτέλεσης του script:**

Για να εξασφαλιστεί η περιοδική αποστολή των κακόβουλων IPs στο PfSense, προσθέτουμε το script στο crontab για να εκτελείται κάθε 6 μέρες.

0 0 */6 * * /path/to/export_qradar_bad_ips.sh

5. **Αναγνώριση των IOCs από το Snort**

Κάθε φορά που προσθέτουμε αρχεία με IPs στο directory **/var/db/snort/iprep**, το Snort του pfSense τις αναγνωρίζει και μπορεί αυτόματα να τις μπλοκάρει ως IPs που σχετίζονται με κακόβουλες δραστηριότητες. Οι λίστες με τις IPs μπορούν να χρησιμοποιηθούν στα interfaces του Snort, ώστε να ορίζονται είτε για block είτε για whitelist ανάλογα με τις ανάγκες ασφάλειας.



Εικόνα 72 Snort qradar_bad_ips.txt

5. Πειραματική Δοκιμή

Σε αυτό το κεφάλαιο πραγματοποιούνται βασικές δοκιμές για να επαληθευτεί η σωστή λειτουργία της διασύνδεσης μεταξύ των εργαλείων. Παρουσιάζονται σενάρια επικοινωνίας από το MISP προς το Qradar και το Snort, καθώς και μεταξύ Qradar και Snort. Οι δοκιμές επιβεβαιώνουν την επιτυχία της υλοποίησης.

5.1 Δοκιμή Διασύνδεσης MISP -> Qradar -> Snort

Πριν την εκτέλεση του script, πραγματοποιήσαμε σύνδεση στο MISP μέσω της διεύθυνσης IP 192.168.4.5.

Εκτέλεση του Script

Τρέξαμε το script στον server του MISP χρησιμοποιώντας την παρακάτω εντολή:

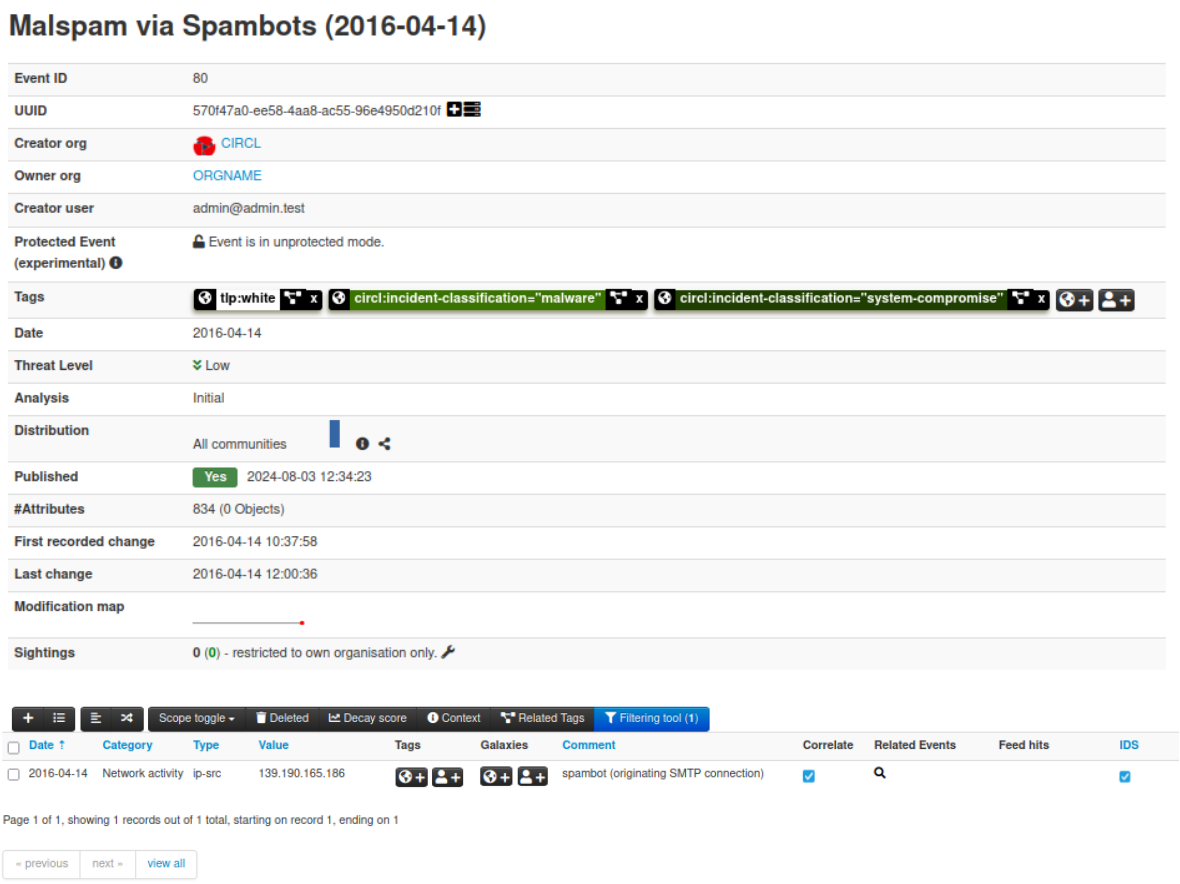
python3 master_qradar_misp_ipsrc.py

Το script ξεκίνησε να αντλεί τα IOCs (IP sources) από το MISP και να τα εισάγει στο **QRadar**.

Η διαδικασία ολοκληρώθηκε επιτυχώς, και το reference set **MISP_IPs** ενημερώθηκε με **8518 IOCs**.

```
root@ubuntu:/Scripts# python3 master_qradar_misp_ipsrc.py
master_qradar_misp_ipsrc.py:5: DeprecationWarning:
As our baseline system is the latest Ubuntu LTS, and Ubuntu LTS 22.04 has Python 3.10 available,
we will officially deprecate python versions below 3.10 on January 1st 2024.
**Please update your codebase.**
  import pymisp
Pull from MISP complete...extracting IOCs from JSON...
IOCs clean...
IOCs extracted from JSON...pushing to QRadar...
Push complete, pushed 8518 IOCs to QRadar!
root@ubuntu:/Scripts# _
```

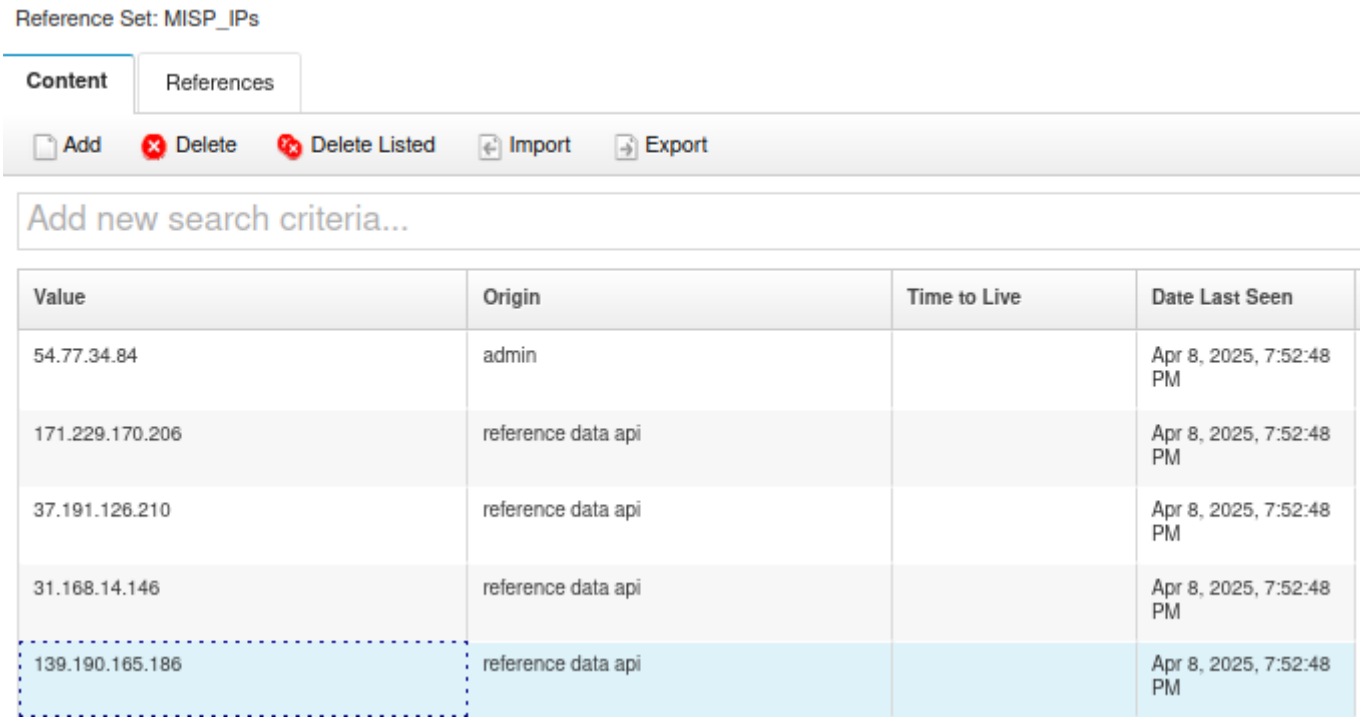
Εικόνα 73 master_qradar_misp_ipsrc.py



Εικόνα 74 Bad IP (139.190.165.186) σε MISP

Έλεγχος των IPs στο Reference Set του QRadar

Αφού ολοκληρώθηκε η εκτέλεση του script, μεταβήκαμε στο QRadar για να επιβεβαιώσουμε ότι τα IOCs εισήχθησαν.



Εικόνα 75 MISP_IPs με IOCs

Δημιουργία Cron Job για Αυτόματη Εκτέλεση του Script

Για να αυτοματοποιήσουμε τη διαδικασία και να διασφαλίσουμε ότι το reference set παραμένει ενημερωμένο με τις τελευταίες απειλές από το MISP, ρυθμίσαμε την εκτέλεση του script μέσω ενός **cron job** όπως αναφέρθηκε στην παράγραφο 4.1.

Συσχέτιση με Custom Rule στο QRadar και Αντίδραση (Παράδειγμα με IP 139.190.165.186)

Το reference set MISP_IPs χρησιμοποιείται ενεργά στον κανόνα **Custom Rule: MISP IP Detected** στο QRadar. Ο κανόνας αυτός παρακολουθεί την εισερχόμενη και εξερχόμενη κυκλοφορία, και ενεργοποιείται όταν εντοπιστεί δραστηριότητα από ή προς μια IP που περιλαμβάνεται στο **MISP_IPs** reference set. Η ενεργοποίηση του κανόνα δημιουργεί alert, επιτρέποντας στους αναλυτές να εντοπίζουν και να ανταποκρίνονται ταχύτερα σε ενδεχόμενες απειλές.

Offense 53

Magnitude		**Status**	**Relevance** 5
Description	Potentially Bad Traffic preceded by Firewall - Permit	**Offense Type**	Destination IP
		Event/Flow count	9 events and 0 flows in 2 categories
Source IP(s)	192.168.1.11 (192.168.1.11)	**Start**	Apr 8, 2025, 8:55:56 PM
Destination IP(s)	139.190.165.186	**Duration**	8s
Network(s)	other	**Assigned to**	Unassigned

Offense Source Summary

IP	139.190.165.186

Εικόνα 76 MISP IP Detected Offense

Event Name	Log Source	Event Count	Time	Low Level Category	Source IP	Source Port	Destination IP
Potentially Bad Traffic	Snort @ pfSense.home.localdomain	1	Apr 8, 2025, 8:55:59 PM	Misc Suspicious Event	192.168.1.11	N/A	139.190.165.186
Potentially Bad Traffic	Snort @ pfSense.home.localdomain	1	Apr 8, 2025, 8:55:58 PM	Misc Suspicious Event	192.168.1.11	N/A	139.190.165.186
Potentially Bad Traffic	Snort @ pfSense.home.localdomain	1	Apr 8, 2025, 8:55:57 PM	Misc Suspicious Event	192.168.1.11	N/A	139.190.165.186

Start Time	Log Source	Payload
Apr 8, 2025, 8:56:05 PM	Snort @ pfSense....	<35>1 2025-04-08T20:56:06.195367+03:00 pfSense.home.localdomain snort 81791 - - [136:1:1] (spp_reputation) packets block-list [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 192.168.1.11:14072 -> 139.190.165.186:443
Apr 8, 2025, 8:56:00 PM	Snort @ pfSense....	<35>1 2025-04-08T20:56:03.179642+03:00 pfSense.home.localdomain snort 81791 - - [136:1:1] (spp_reputation) packets block-list [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 192.168.1.11 -> 139.190.165.186
Apr 8, 2025, 8:55:59 PM	Snort @ pfSense....	<35>1 2025-04-08T20:56:00.187390+03:00 pfSense.home.localdomain snort 81791 - - [136:1:1] (spp_reputation) packets block-list [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 192.168.1.11 -> 139.190.165.186
Apr 8, 2025, 8:55:58 PM	Snort @ pfSense....	<35>1 2025-04-08T20:55:59.187494+03:00 pfSense.home.localdomain snort 81791 - - [136:1:1] (spp_reputation) packets block-list [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 192.168.1.11 -> 139.190.165.186
Apr 8, 2025, 8:55:57 PM	Snort @ pfSense....	<35>1 2025-04-08T20:55:58.172928+03:00 pfSense.home.localdomain snort 81791 - - [136:1:1] (spp_reputation) packets block-list [Classification: Potentially Bad Traffic] [Priority: 2] {ICMP} 192.168.1.11 -> 139.190.165.186

Εικόνα 77 Requests προς Bad IP (Logs)

Αξιοποιώντας το παραπάνω alert, οι αναλυτές μπορούν μεμονωμένα να αξιολογήσουν την κάθε ύποπτη IP και, εφόσον κριθεί απαραίτητο, να την προσθέσουν στο reference set **Bad_IPs**. Στη συνέχεια, μέσω του script **export_qradar_bad_ips.sh**, οι κακόβουλες IPs που βρίσκονται στο Bad_IPs εξάγονται και αποστέλλονται στο σύστημα Snort IDS, το οποίο και αναλαμβάνει τον αποκλεισμό τους μέσω κατάλληλου κανόνα.

Services / Snort / IP Reputation Lists

Snort Interfaces | Global Settings | Updates | Alerts | Blocked | Pass Lists | Suppress | IP Lists | SID Mgmt | Log Mgmt | Sync

IP Reputation List Management

IP List File Name	Last Modified Time	File Size	Actions
qradar_bad_ips.txt	Apr-08 2025 8:29 pm	29 B	
pfsense_iocs.txt	Apr-08 2025 8:26 pm	117 KiB	
emerging-compromised-ips.txt	Apr-08 2025 8:26 pm	5 KiB	

File Name: pfsense_iocs.txt

Save Cancel

```
182.65.96.201
139.190.165.186
115.250.105.20
5.101.140.71
```

Εικόνα 78 Bad IP σε Snort

5.2 Δοκιμή Διασύνδεσης MISP -> Snort

Πριν την εκτέλεση του script, πραγματοποιήσαμε σύνδεση στο MISP μέσω της διεύθυνσης IP 192.168.4.5.

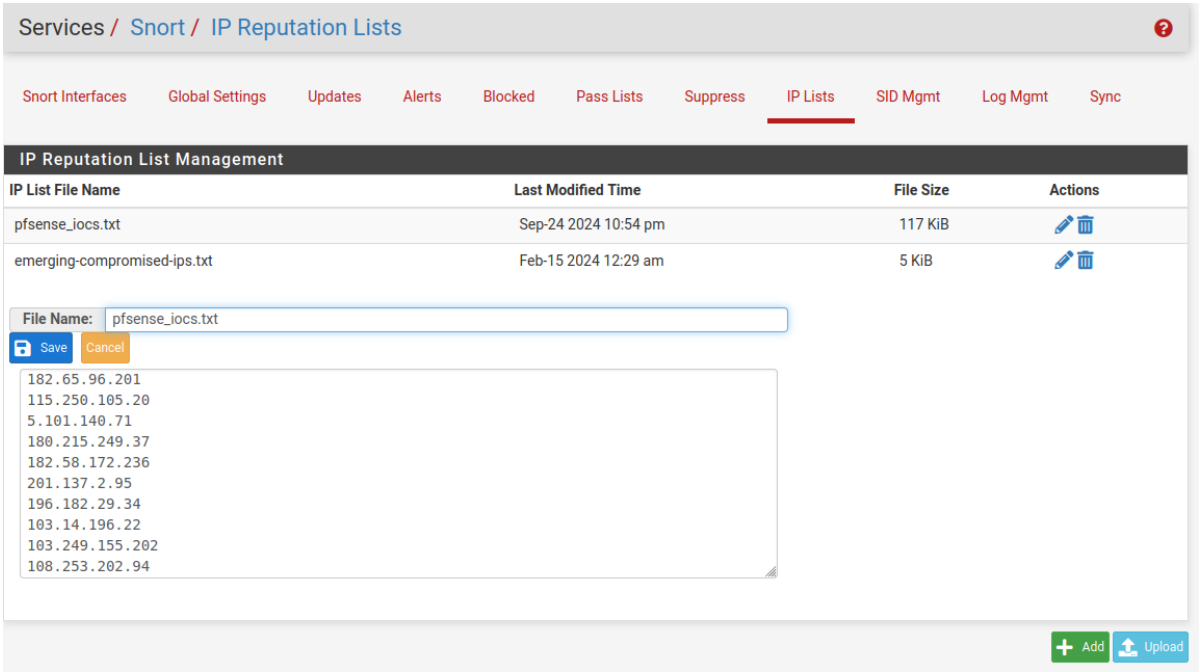
Μεταφορά του Αρχείου στο pfSense μέσω SCP

Χρησιμοποιώντας το SCP (Secure Copy), μεταφέραμε το αρχείο pfsense_iocs.txt στο Snort του pfSense:

scp pfsense_iocs.txt admin@192.168.4.1:/var/db/snort/iprep

Αναγνώριση των IOCs από το Snort

Κάθε φορά που προσθέτουμε αρχεία με IPs στο directory **/var/db/snort/iprep**, το Snort του pfSense τις αναγνωρίζει και μπορεί αυτόματα να τις μπλοκάρει ως IPs που σχετίζονται με κακόβουλες δραστηριότητες. Οι λίστες με τις IPs μπορούν να χρησιμοποιηθούν στα interfaces του Snort, ώστε να ορίζονται είτε για block είτε για whitelist ανάλογα με τις ανάγκες ασφάλειας.



Εικόνα 79 Snort pfsense_iocs.txt

Δημιουργία Cron Job για Αυτόματη Εκτέλεση του Script κάθε 5 Μέρες

Για να αυτοματοποιήσουμε τη διαδικασία και να διασφαλίσουμε ότι τα IOCs από το MISP μεταφέρονται στο Snort που είναι εγκατεστημένο στον pfSense, ρυθμίσαμε την εκτέλεση του script μέσω ενός cron job, όπως αναφέρθηκε στην παράγραφο 4.2.

5.3 Δοκιμή Διασύνδεσης Qradar -> Snort

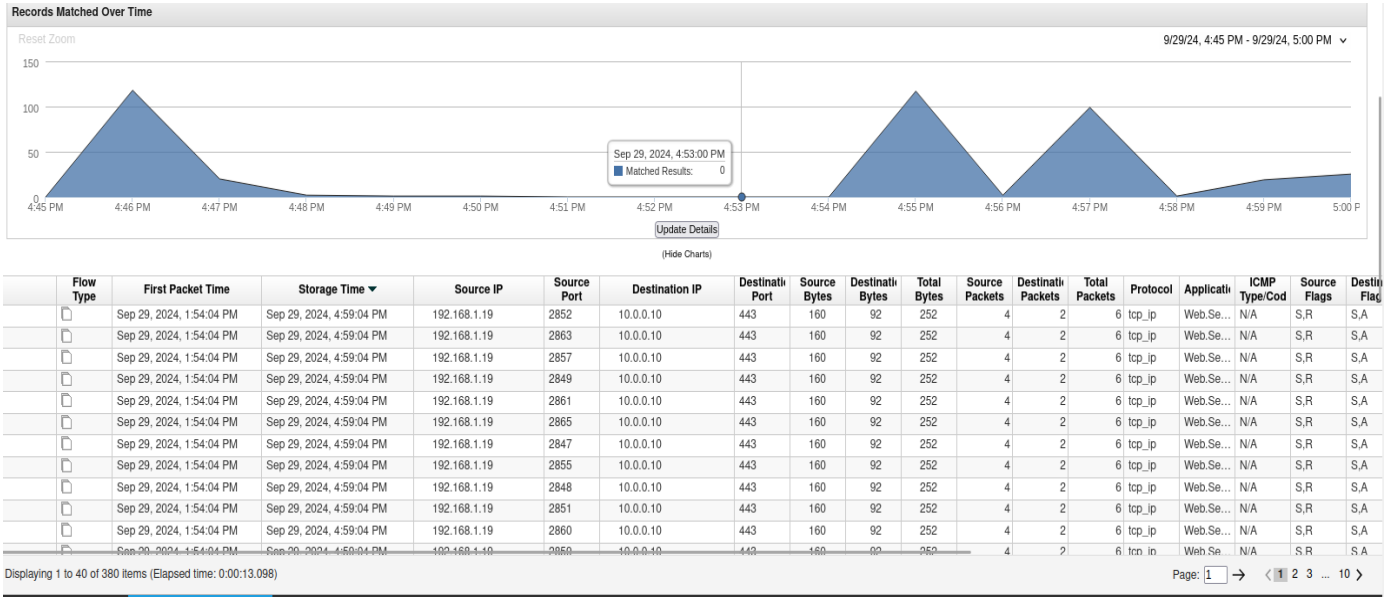
Σε αυτό το βήμα, υλοποιήσαμε ένα σενάριο προσομοίωσης επίθεσης DoS (Denial of Service) με σκοπό να ελέγξουμε την αλληλεπίδραση μεταξύ του QRadar και του pfSense, και τον τρόπο με τον οποίο ανιχνεύονται και αντιμετωπίζονται τέτοιες επιθέσεις. Χρησιμοποιήσαμε μια επίθεση DDoS με κακόβουλη συσκευή που στοχεύει σε ένα συγκεκριμένο host στο δίκτυο. Στη συνέχεια, παρατηρήσαμε πώς το QRadar

ενεργοποιεί έναν κανόνα που προσθέτει την IP της πηγής στο reference set Bad_IPs, και πώς μέσω scripting η διεύθυνση IP αποστέλλεται στο pfSense για αποκλεισμό από το Snort.

1. **Προσομοίωση επίθεσης DoS:**

Ξεκινήσαμε την προσομοίωση επίθεσης DoS από το malicious device με IP 192.168.1.19, χρησιμοποιώντας την ακόλουθη εντολή: **ping3 -i u100 -S -p 443 192.168.1.11**

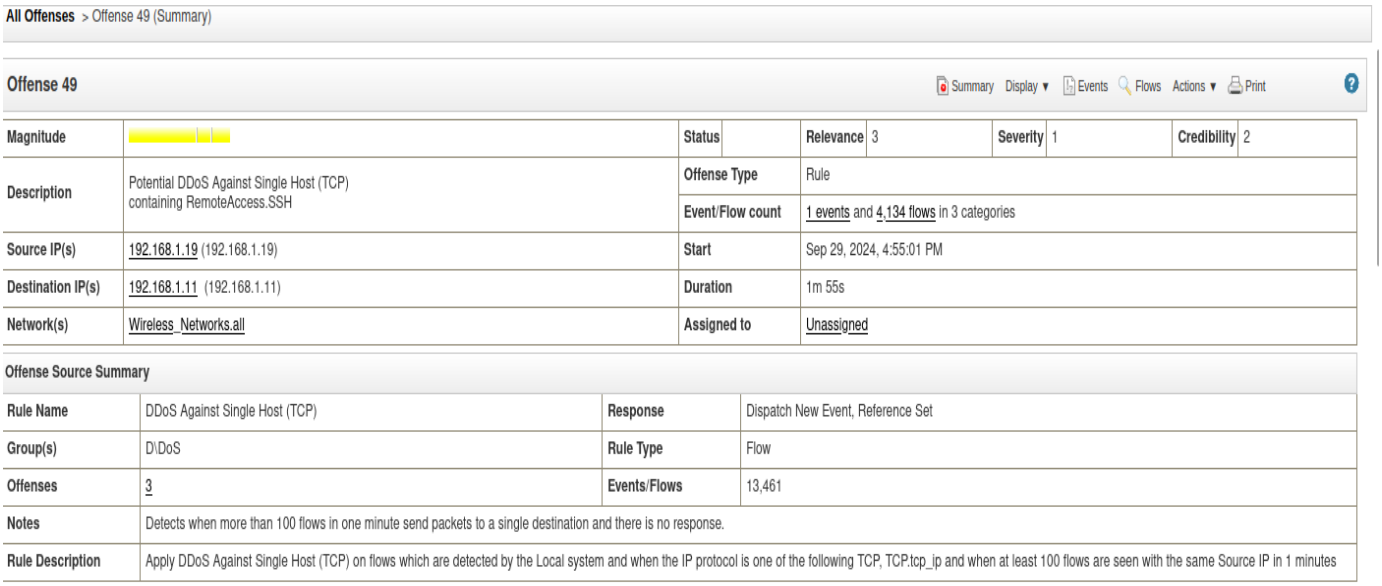
2. **Προεπισκόπηση των Flows στο Qradar:**



Εικόνα 80 Flows απο DDoS στο Qradar

3. **Trigger του κανόνα στο QRadar:**

Κατά τη διάρκεια της επίθεσης, το QRadar ενεργοποίησε τον κανόνα **DDoS Against Single Host (TCP)**, ο οποίος παρακολουθεί τη συνεχή ροή πακέτων σε έναν μόνο host και ανιχνεύει καταστάσεις υπερφόρτωσης.



All Offenses > Offense 49 (Summary)

Offense 49

Summary Display ▾ Events Flows Actions ▾ Print

Magnitude		Status		Relevance	3	Severity	1	Credibility	2
Description	Potential DDoS Against Single Host (TCP) containing RemoteAccess.SSH	Offense Type	Rule				
		Event/Flow count	1 events and 4,134 flows in 3 categories				
Source IP(s)	192.168.1.19 (192.168.1.19)	Start	Sep 29, 2024, 4:55:01 PM				
Destination IP(s)	192.168.1.11 (192.168.1.11)	Duration	1m 55s				
Network(s)	Wireless_Networks.all	Assigned to	Unassigned				

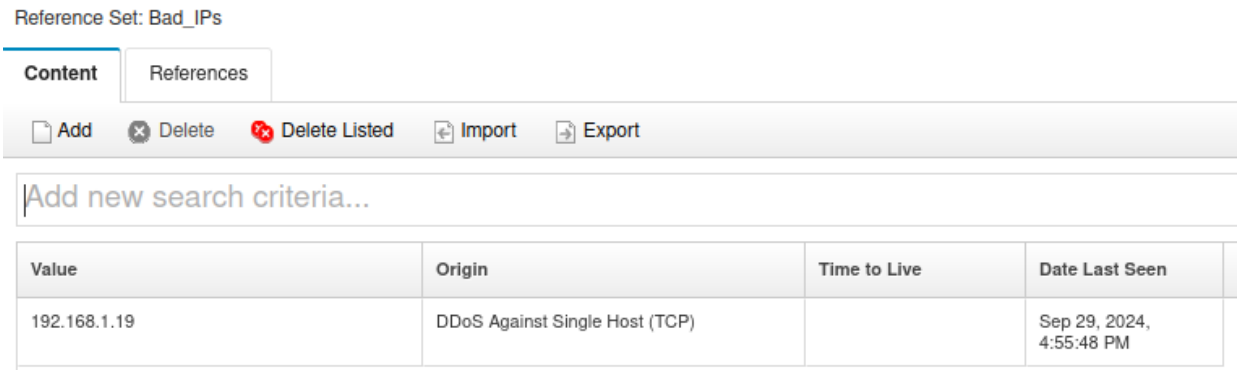
Offense Source Summary

Rule Name	DDoS Against Single Host (TCP)	Response	Dispatch New Event, Reference Set
Group(s)	D\DoS	Rule Type	Flow
Offenses	3	Events/Flows	13,461
Notes	Detects when more than 100 flows in one minute send packets to a single destination and there is no response.		
Rule Description	Apply DDoS Against Single Host (TCP) on flows which are detected by the Local system and when the IP protocol is one of the following TCP, TCP.tcp_ip and when at least 100 flows are seen with the same Source IP in 1 minutes		

Εικόνα 81 Offence Triggered μετά την DDoS

4. **Προσθήκη στο Reference Set:**

Μετά την ενεργοποίηση του κανόνα, η IP της κακόβουλης συσκευής (192.168.1.19) προστέθηκε αυτόματα στο reference set **Bad_IPs**, το οποίο χρησιμοποιείται για την αναγνώριση και καταγραφή επικίνδυνων IPs.



Reference Set: Bad_IPs

Content References

Add Delete Delete Listed Import Export

Add new search criteria...

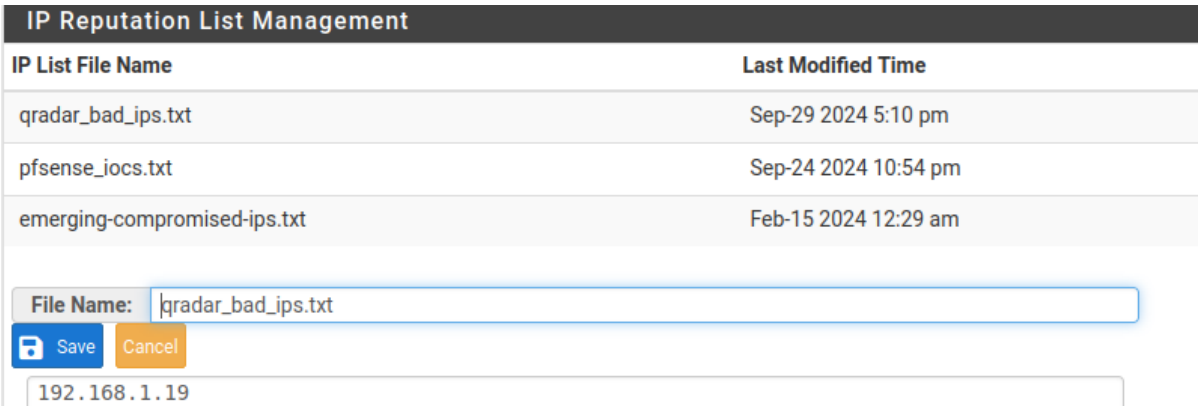
Value	Origin	Time to Live	Date Last Seen
192.168.1.19	DDoS Against Single Host (TCP)		Sep 29, 2024, 4:55:48 PM

Εικόνα 82 IP Σε Reference Set Μετά την DDoS

5. **Εκτέλεση του script export_qradar_bad_ips.sh:**

Εκτελέσαμε το script **export_qradar_bad_ips.sh**, το οποίο αναλαμβάνει την εξαγωγή των IPs από το reference set **Bad_IPs** και την αποστολή τους στο Snort του pfSense.

Η IP του κακόβουλου device αποστάλθηκε επιτυχώς στο Snort μέσω του script και προστέθηκε στους κανόνες του pfSense, διασφαλίζοντας ότι η συγκεκριμένη διεύθυνση IP θα αποκλειστεί από το firewall και το IDS (Intrusion Detection System).



Εικόνα 83 qradar_bad_ips.txt Μετά την DDoS

6. Συμπεράσματα και Μελλοντικές Επεκτάσεις

Το κεφάλαιο αυτό συνοψίζει τα συμπεράσματα της εργασίας και προτείνει πιθανές επεκτάσεις. Εξετάζεται η αξία της ολοκληρωμένης πλατφόρμας κυβερνοασφάλειας, ενώ προτείνονται επεκτάσεις με εργαλεία όπως EDR, DLP και εκπαιδευτικά modules. Τονίζεται η σημασία της συνεχούς βελτίωσης και αυτοματοποίησης.

6.1 Επαλήθευση Λειτουργικότητας και Ενίσχυση Άμυνας μέσω Ενοποίησης Εργαλείων

Στη διάρκεια της υλοποίησης πραγματοποιήθηκαν **επιγραμματικές δοκιμές** που επιβεβαίωσαν την ορθή λειτουργία των **διασυνδέσεων** μεταξύ των επιμέρους εργαλείων. Ειδικότερα, η **ροή δεδομένων** από το **MISP** προς το **QRadar** και η **αυτόματη ενημέρωση** του reference set **MISP_IPs** διασφαλίζουν την έγκαιρη ενσωμάτωση **κακόβουλων IP διευθύνσεων** στην **ανάλυση συμβάντων**.

Μέσω της δημιουργίας **custom κανόνων** στο **QRadar**, τα **IOCs** που εντοπίζονται ενεργοποιούν **αυτοματοποιημένες ειδοποιήσεις**, επιτρέποντας την άμεση αντίδραση των αναλυτών. Ταυτόχρονα, η προώθηση των επικίνδυνων **IP διευθύνσεων** στο **pfSense** και στο **Snort IDS** ενισχύει την προστασία του **perimeter**, μέσω **άμεσου αποκλεισμού** των απειλών.

Η ενσωμάτωση εργαλείων όπως το **ModSecurity WAF** (σε συνδυασμό με τον **Nginx Web Server**), το **MISP** και το **pfSense** στο **QRadar** συνέβαλε καθοριστικά στη βελτίωση της **απόκρισης** απέναντι σε επιθέσεις. Το **WAF** προστατεύει τις **web εφαρμογές** από **SQL injection** και **XSS**, με τα σχετικά **συμβάντα** να καταγράφονται στο **SIEM**. Παράλληλα, το **MISP** προσφέρει δυνατότητα **ανταλλαγής πληροφοριών απειλών**, διευκολύνοντας την **πρόληψη επιθέσεων**. Το **pfSense** λειτουργεί ως πρόσθετο **firewall επιθεώρησης και φιλτραρίσματος**, προσφέροντας **προστασία σε πρώιμο στάδιο**.

Η **προσομοίωση επίθεσης τύπου DDoS** ανέδειξε τη δυνατότητα του **QRadar** να ενεργοποιεί άμεσα κανόνες και να διανέμει τις σχετικές εντολές προς το **IDS**, αξιοποιώντας **scripts** και **cron jobs** για **αυτοματοποιημένη** και **συνεπή ροή ενεργειών**.

6.2 Επέκταση με Προστασίας από ιούς (EDR)

Η ενσωμάτωση ισχυρού λογισμικού προστασίας από ιούς, όπως το Trend Micro, στην υποδομή δικτύου μπορεί να είναι ένας αποτελεσματικός τρόπος για την καταπολέμηση κακόβουλου λογισμικού και άλλου κακόβουλου λογισμικού. Το λογισμικό προστασίας από ιούς σαρώνει συνεχώς αρχεία και εφαρμογές για γνωστά μοτίβα και υπογραφές κακόβουλου λογισμικού. Βοηθά στον εντοπισμό και την καραντίνα ή την αφαίρεση απειλών προτού προκαλέσουν βλάβη στο δίκτυο ή σε κίνδυνο ευαίσθητων δεδομένων. Οι τακτικές ενημερώσεις στους ορισμούς προστασίας από ιούς διασφαλίζουν ότι το σύστημα παραμένει ενημερωμένο με τις πιο πρόσφατες απειλές, παρέχοντας μια προληπτική άμυνα έναντι των αναδυόμενων κακόβουλων προγραμμάτων.

6.3 Επέκταση με πρόληψη απώλειας δεδομένων (DLP)

Η εφαρμογή μιας λύσης DLP (Data Loss Prevention) είναι κρίσιμη για την προστασία των ευαίσθητων πληροφοριών από μη εξουσιοδοτημένη πρόσβαση και διαρροή. Το DLP παρακολουθεί και ελέγχει τη ροή των δεδομένων εντός και εκτός του δικτύου, διασφαλίζοντας ότι οι πολιτικές ασφαλείας τηρούνται. Μπορεί να αποτρέψει τη μεταφορά ευαίσθητων δεδομένων, όπως προσωπικές πληροφορίες, οικονομικά δεδομένα ή πνευματική ιδιοκτησία, εκτός του οργανισμού χωρίς την κατάλληλη άδεια. Επιπλέον, ένα καλά ρυθμισμένο DLP μπορεί να εντοπίσει τυχόν κακόβουλη δραστηριότητα ή ανθρώπινα λάθη που ενδέχεται να οδηγήσουν σε απώλεια δεδομένων, παρέχοντας μεγαλύτερη ορατότητα και έλεγχο πάνω στην πληροφοριακή ροή.

6.4 Επέκταση με συνεχή εκπαίδευση μηχανικών και αναλυτών ασφαλείας

Η αποτελεσματική λειτουργία και εξέλιξη της υποδομής ασφαλείας ενός οργανισμού εξαρτάται όχι μόνο από την τεχνολογία, αλλά και από τη συνεχή εκπαίδευση του ανθρώπινου δυναμικού. Οι μηχανικοί και αναλυτές ασφαλείας πρέπει να είναι διαρκώς ενημερωμένοι για τις τελευταίες εξελίξεις σε απειλές, επιθέσεις και νέες μεθοδολογίες ανίχνευσης και απόκρισης.

Για να επιτευχθεί αυτό, είναι απαραίτητο να υιοθετηθούν πρακτικές όπως:

- **Εκπαίδευση σε νέες τεχνολογίες και εργαλεία**: Τα συστήματα SIEM (όπως το QRadar), πλατφόρμες threat intelligence (όπως το MISP) και τεχνολογίες ανίχνευσης εισβολών (όπως το Snort) εξελίσσονται συνεχώς. Οι μηχανικοί πρέπει να γνωρίζουν πώς να αξιοποιούν τις δυνατότητές τους στο έπακρο.
- **Simulations και Red Team/Blue Team ασκήσεις**: Η προσομοίωση πραγματικών επιθέσεων επιτρέπει στους αναλυτές να δοκιμάσουν την αντίδρασή τους σε πραγματικά σενάρια, βελτιώνοντας την ικανότητα ανίχνευσης και αντιμετώπισης περιστατικών.
- **Διαρκής ενημέρωση μέσω Threat Intelligence Feeds**: Οι μηχανικοί πρέπει να έχουν πρόσβαση σε ενημερωμένες βάσεις δεδομένων απειλών, ώστε να προσαρμόζουν τις πολιτικές ασφαλείας ανάλογα με τις νέες μορφές επιθέσεων.
- **Συμμετοχή σε κοινότητες κυβερνοασφάλειας**: Πλατφόρμες όπως το FIRST, MITRE ATT&CK, και forums κυβερνοασφάλειας παρέχουν πολύτιμη γνώση σχετικά με βέλτιστες πρακτικές και emerging threats.
- **Πιστοποιήσεις και σεμινάρια**: Η παρακολούθηση πιστοποιημένων εκπαιδεύσεων όπως CISSP, CEH, CISM και εξειδικευμένων σεμιναρίων σε εργαλεία όπως QRadar, Fortinet, και Snort ενισχύει την τεχνογνωσία και την αυτοπεποίθηση των μηχανικών ασφαλείας.

6.5 Επέκταση με ανταλλαγή πληροφοριών μεταξύ SOC μέσω TAXII

Η διασύνδεση και ανταλλαγή πληροφοριών απειλών (Threat Intelligence Sharing) μεταξύ Κέντρων Επιχειρήσεων Ασφαλείας (SOC) αποτελεί κρίσιμο στοιχείο για την ενίσχυση της κυβερνοάμυνας ενός οργανισμού. Η χρήση του **TAXII (Trusted Automated Exchange of Indicator Information)** επιτρέπει τη δομημένη και αυτοματοποιημένη ανταλλαγή δεδομένων απειλών, διευκολύνοντας τη συνεργασία μεταξύ διαφορετικών SOC και οργανισμών.

7. Βιβλιογραφικές Πηγές

Udemy. (n.d.). The Complete Cyber Security Course : Network Security! URL: https://www.udemy.com/course/network-security-course/

PfSense Documentation. (n.d.). URL:https://docs.netgate.com/pfsense/en/latest/index.html

Snort Documentation. (n.d.). URL:https://www.snort.org/documentation

Ntop Documentation. (n.d.). URL:https://www.ntop.org/documentation/

SoftFlow Documentation. (n.d.). URL: https://docs.netgate.com/pfsense/en/latest/recipes/netflow-with-softflowd.html

Open Web Application Security Project. (n.d.). URL:https://www.owasp.org/

QRadar Documentation. (n.d.). URL:https://www.ibm.com/support/knowledgecenter/SSKMKU/welcome.html

Udemy. (n.d.). pfSense Fundamentals - Secure Networks With pfSense Firewall. URL:https://www.udemy.com/course/pfsense-fundamentals-secure-your-network-with-pfsense/

Cisco - Cisco offers extensive documentation, white papers, and resources on network security, including topics like firewalls, intrusion detection, and access control. URL: https://www.cisco.com/c/en/us/solutions/enterprise-networks/index.html

Symantec - Symantec is a well-known cybersecurity company that offers insights into the latest security threats and solutions. Their website contains informative articles and reports on various security topics. URL: https://www.symantec.com/

NIST (National Institute of Standards and Technology) - NIST provides cybersecurity frameworks, guidelines, and standards that can be used as references for network security best practices. URL: https://www.nist.gov/cyberframework

National Institute of Standards and Technology (NIST) - Οδηγός για μια Ασφαλή Επιχειρησιακή Δικτυακή Υποδομή (SP 800-215) URL: https://csrc.nist.gov/News/2022/sp-800-215-secure-enterprise-network-landscape

ThreatConnect - Πλατφόρμα Πληροφοριών Απειλών και Ποσοτικοποίηση Κινδύνου: URL: https://threatconnect.com/

MISP Project Website URL: https://www.misp-project.org/ - https://misp.github.io/MISP/xINSTALL.ubuntu2204

IBM Developer Article "Import IOCs from MISP to IBM Security QRadar". (n.d.). URL: https://developer.ibm.com/articles/awb-import-iocs-from-misp-to-qradar/

AlienVault Open Threat Exchange (OTX) Πηγή ανταλλαγής πληροφοριών απειλών που συνεργάζεται και με το MISP. URL: https://otx.alienvault.com

IBM Security Learning Academy. URL: https://www.securitylearningacademy.com

OWASP ModSecurity Core Rule Set (CRS) Επίσημη σελίδα του βασικού σετ κανόνων για το ModSecurity. URL: https://coreruleset.org