ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ

ΕΥΦΥΕΙΣ ΤΕΧΝΟΛΟΓΙΕΣ ΔΙΑΔΙΚΤΥΟΥ - WEBINTELLIGENCE

NIS οδηγία σε μεγάλους Δημόσιους οργανισμούς και ενίσχυση αυτής με την εφαρμογή συστήματος προσδιορισμού συμβάντων και επιθέσεων ασφάλειας (SIEM)

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΙΩΑΝΝΗ ΚΑΠΟΥΛΑ

Επιβλέπων : Χρήστος Ηλιούδης
Καθηγητής ΔΙ.ΠΑ.Ε.

Θεσσαλονίκη, Φεβρουάριος 2023

Η σελίδα αυτή είναι σκόπιμα λευκή.

Υπόδειγμα φύλλου τίτλου (μπροστινή σελίδα) του αντιτύπου ΜΔΕ

ΔΙΕΘΝΕΣ ΠΑΝΕΠΙΣΤΗΜΙΟ ΤΗΣ ΕΛΛΑΔΟΣ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΕΥΦΥΕΙΣ ΤΕΧΝΟΛΟΓΙΕΣ ΔΙΑΔΙΚΤΥΟΥ – WEB INTELLIGENCE

NIS οδηγία σε μεγάλους Δημόσιους οργανισμούς και ενίσχυση αυτής με την εφαρμογή συστήματος προσδιορισμού συμβάντων και επιθέσεων ασφάλειας (SIEM)

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

ΙΩΑΝΝΗ ΚΑΠΟΥΛΑ

Επιβλέπων : Χρήστος Ηλιούδης
Καθηγητής ΔΙ.ΠΑ.Ε.

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή στις Choose a date.

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Όνομα Επώνυμο	Όνομα Επώνυμο	'Ονομα Επώνυμο
Choose an item. ΔΙ.ΠΑ.Ε.	Choose an item. ΔΙ.ΠΑ.Ε.	Choose an item. ΔΙ.ΠΑ.Ε.

Θεσσαλονίκη, Φεβρουάριος 2023

(Υπογραφή)

.....

Click here to enter text.

Click here to enter text.

Περίληψη

Υπό το πρίσμα της διαφύλαξης υψηλού επιπέδου κυβερνοασφάλειας και μιας ολιστικής στρατηγικής προσέγγισης η ΕΕ το 2016 εξέδωσε την NIS οδηγία η οποία αποτέλεσε την πρώτη συγκροτημένη ευρωπαϊκή προσπάθεια θεσμοθέτησης κανόνων για την κυβερνοασφάλεια, με ρητές υποχρεώσεις για τα κράτη μέλη. Η οδηγία, τόσο στην πρώτη της μορφή, όσο και στην μεταγενέστερη επιχειρούμενη αναθεώρησή της (NIS2), έχει ως απώτερο σκοπό τη συνεχή βελτίωση της ανθεκτικότητας των δημόσιων και ιδιωτικών φορέων, των καθορισμένων αρχών, και της Ευρωπαϊκής Ένωσης συνολικά στο πλαίσιο της κυβερνοασφάλειας και της προστασίας των υποδομών ζωτικής σημασίας, αλλά και την ανάπτυξη της ικανότητάς τους να ανταποκρίνονται σε περιστατικά επιθέσεων στον κυβερνοχώρο.

Η παρούσα διπλωματική εργασία έχει ως σκοπό να αναλύσει εις βάθος την νέα αναθεωρημένη οδηγία «NIS2» και να ορίσει το πλαίσιο υποχρεώσεων που έχουν οι οργανισμοί του Δημοσίου στα πλαίσια της νέας αναθεωρημένης οδηγίας. Μια σημαντική παράμετρος εφαρμογής που μπορεί να συμβάλει στην επίτευξη συμμόρφωσης με όλες τις τεχνικές πτυχές την νέας οδηγίας NIS 2 είναι τα Συστήματα Πληροφοριών Ασφάλειας και Διαχείρισης Περιστατικών (Security Information and Event Management - SIEM). Στο πλαίσιο αυτό θα αναπτυχθεί μία μελέτη εφαρμογής σε έναν δημόσιο φορέα κάνοντας εγκατάσταση στους διακομιστές του φορέα ένα από τα πιο δημοφιλής εργαλεία SIEM ανοιχτού κώδικα, το OSSIM της AlienVault.

Λέξεις Κλειδιά: NIS, NIS2, SIEM, OSSIM, OSSEC

Η σελίδα αυτή είναι σκόπιμα λευκή.

Abstract

In the light of a high level of cyber security and a holistic strategic approach, EU in 2016 issued the NIS directive which was the first organized European effort to establish cyber security rules, with explicit obligations for member states. The directive, both in its first form and in its later attempted revision (NIS2), has as its specific aim to achieve a high common level of cybersecurity across the Member States. The Directive sets strict incident reporting requirements, which are difficult to comply with for an organization without mature incident management processes and SIEM solutions.

The purpose of this thesis is to analyze in depth the new revised directive "NIS2" and to define the framework of obligations that public organizations have. An important application parameter that can help achieve compliance with all technical aspects of the new NIS 2 directive is Security Information and Event Management (SIEM) systems. In this context, a case study will be developed in a public sector by deploying one of the most popular open source SIEM tool, AlienVault's OSSIM.

Keywords: NIS, NIS2, SIEM, OSSIM, OSSEC

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πίνακας περιεχομένων

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

Συντομογραφίες

Δ.Ε.	Διπλωματική Εργασία
ΔΙΠΑΕ	Διεθνές Πανεπιστήμιο Ελλάδος
SIEM	Security Information and Event Management
OSSIM	Open Source Security Information Management
OSSEC	Open-Source Host-based Intrusion Detection System
ΤΠΕ	Τεχνολογία Πληροφοριών και Τεχνολογιών
NIS	Network and Information Systems
ΕΕ	Ευρωπαϊκή Ένωση
DDos	Df-service attack, DoS attack
IP	Protocol Address
URL	Uniform Resource Locator
CPU	Central Processing Unit
ΤΝ	Τεχνητή Νοημοσύνη
CSIRT	Ομάδες αντιμετώπισης περιστατικών ασφαλείας
SOC	Security Operation Center
ENISA	Οργανισμού της Ευρωπαϊκής Ένωσης για την Κυβερνοασφάλεια

1

Εισαγωγή

Οι αυξανόμενες επενδύσεις σε ψηφιακές τεχνολογίες επηρεάζουν όλους τους τομείς δραστηριότητας μιας τεχνολογικά αναπτυσσόμενης κοινωνίας. Πλέον βαδίζουμε στην εποχή που όλοι μας έχουμε άμεση πρόσβαση στα δεδομένα μας αν πάσα στιγμή με οποιαδήποτε ψηφιακή συσκευή. Αυτό όμως δημιουργεί μια σειρά από απαιτήσεις ασφάλειας (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα) για τις παρεχόμενες υπηρεσίες και τα εμπλεκόμενα ψηφιακά μέσα.

Η υιοθέτηση μίας γενικότερης κουλτούρα ασφάλειας είναι ένα ουσιαστικό βήμα εδραίωσης του αισθήματος ασφάλειας των πολιτών για να μπορέσουν να αντιμετωπίσουν αποτελεσματικά και αποδοτικά τα ολοένα και περισσότερα περιστατικά επιθέσεων που μπορούν να υπονομεύσουν την ακεραιότητα υποδομών ζωτικής σημασίας και να θέσουν σε κίνδυνο την ασφάλεια των κρατών και των πολιτών. [1]

Υπό το πρίσμα της διαφύλαξης υψηλού επιπέδου κυβερνοασφάλειας και μιας ολιστικής στρατηγικής προσέγγισης, η ΕΕ το 2016 εξέδωσε την οδηγία 2016/1148/ΕΚ ευρέως γνωστή ως NIS (από τα αρχικά «Network and Information Systems») η οποία αποτέλεσε την πρώτη συγκροτημένη ευρωπαϊκή προσπάθεια θεσμοθέτησης κανόνων για την κυβερνοασφάλεια, με ρητές υποχρεώσεις για τα μέλη της ΕΕ. Το επίκεντρο προσπάθειας της οδηγίας, τόσο στην πρώτη της μορφή (NIS), όσο και στην μεταγενέστερη επιχειρούμενη αναθεώρησή της (NIS2), είναι η διαρκή βελτίωση της ανθεκτικότητας των δημοσίων οργανισμών και των οργανισμών του ιδιωτικού τομέα, τις αρμόδιες αρχές και την Ευρωπαϊκή Ένωση στο σύνολό της, στον τομέα της ασφάλειας στον κυβερνοχώρο και της προστασίας των υποδομών ζωτικής σημασίας,

αλλά και την ανάπτυξη των ικανοτήτων αυτών στην αντιμετώπισης περιστατικών κυβερνοεπιθέσεων.

1.1 Αντικείμενο διπλωματικής

Η παρούσα διπλωματική εργασία έχει ως σκοπό να ερευνήσει και να παρουσιάσει σε βάθος την νέα αναθεωρημένη οδηγία «NIS2» και να ορίσει το πλαίσιο υποχρεώσεων που έχουν οι οργανισμοί του Δημοσίου στα πλαίσια της νέας αναθεωρημένης οδηγίας. Ένα κλασικό πληροφοριακό σύστημα ασφάλειας θα πρέπει να καλύπτει τις τρείς «παραδοσιακές» απαιτήσεις ασφάλειας: την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα των πόρων και των πληροφοριών. Η διασφάλιση των «ευαίσθητων» υποδομών σε δημόσιους οργανισμούς οι οποίοι έχουν προσδιοριστεί ως φορείς εκμετάλλευσης βασικών υπηρεσιών, άπτεται στη δυνατότητα βελτίωσης της ανθεκτικότητας και των δυνατοτήτων αντιμετώπισης κακόβουλων ενεργειών σύμφωνα με τις τελευταίες απαιτήσεις ασφάλειας. Η κοινοτική οδηγία NIS 2 θα συμβάλει στον καθορισμό μέτρων που πρέπει να παρθούν για την ορθολογιστική διαχείριση των κινδύνων στον κυβερνοχώρο και των υποχρεώσεων αναφοράς περιστατικών σε όλους τους φορείς τους οποίους καλείται να καλύψει.

Μια σημαντική παράμετρος εφαρμογής που μπορεί να συμβάλει στην επίτευξη συμμόρφωσης με όλες τις τεχνικές πτυχές την νέας οδηγίας NIS 2 είναι τα Συστήματα Πληροφοριών Ασφάλειας και Διαχείρισης Περιστατικών (Security Information and Event Management - SIEM). Οι λύσεις SIEM αποτελούν ένα αδιαμφισβήτητο όπλο της κυβερνοασφάλειας καθώς παρέχουν τη δυνατότητα ορθολογιστικής διαχείρισης των απειλών και τα περιστατικών ασφάλειας συλλέγοντας και αναλύοντας συμβάντα από μια ευρύτερη ποικιλία περιστατικών και δεδομένων σε πραγματικό χρόνο. Επιπλέον συμβάλουν, στην καλύτερη δυνατή έρευνα των περιστατικών και την ικανοποίηση συγκεκριμένων κανονιστικών απαιτήσεων συμμόρφωσης μέσω της ανάλυσης και της αναφοράς ιστορικών στοιχείων από αυτές τις πηγές.

Στο πλαίσιο αυτό θα αναπτυχθεί μία μελέτη εφαρμογής σε έναν δημόσιο φορέα κάνοντας εγκατάσταση στους διακομιστές του φορέα ένα από τα πιο δημοφιλής εργαλεία SIEM ανοιχτού κώδικα, το OSSIM της AlienVault. Στόχος της μελέτης αυτής είναι να παρουσιάσει μια λύση που μπορεί να συμβάλει στην ψηφιακή θωράκιση του Δημοσίου και την διασφάλιση των τριών βασικών αρχών της ασφάλειας: της ακεραιότητα, της εμπιστευτικότητας και της διαθεσιμότητας των πληροφοριών. Σε εθνικό επίπεδο, ιδιαίτερα οι φορείς Δημόσιας Διοίκησης θα πρέπει να «οχυρώσουν» την δικτυακή υποδομή των πληροφοριακών τους συστημάτων, με την χρήση SIEM εργαλείων, για εδραίωση ενός ασφαλούς ηλεκτρονικού περιβάλλοντος και την λήψη μέτρων «επιθετικής» άμυνας για την πρόληψη και την αντιμετώπιση μελλοντικών κινδύνων, λειτουργώντας πάντα βάσει των κεντρικών οδηγιών του Υπουργείου Ψηφιακής

Διακυβέρνησης και των θεσμοθετημένων κανόνων της κοινοτικής οδηγίας NIS2 για την κυβερνοασφάλεια.

1.2 Δομή της διπλωματικής

Η παρούσα διπλωματική εργασία αποτελείται από οκτώ κεφάλαια.

Το πρώτο κεφάλαιο είναι το εισαγωγικό στο οποίο αναλύεται το αντικείμενο της συγκεκριμένης διπλωματικής αλλά και η δομής της.

Το δεύτερο κεφάλαιο αναλύει τον ορισμό και τη σημασία της ασφάλειας στον κυβερνοχώρο.

Στο τρίτο κεφάλαιο παρουσιάζεται η στρατηγική της ΕΕ για την Κυβερνοασφάλεια

Στο τέταρτο κεφάλαιο παρουσιάζεται η Εθνική Στρατηγική Κυβερνοασφάλειας για Δημόσια Διοίκηση και ΟΤΑ

Στο πέμπτο κεφάλαιο παρουσιάζονται η κοινοτική οδηγία NIS και αναλύεται εις βάθος η νέα αναθεωρημένη οδηγία «NIS2», καθώς και το πλαίσιο υποχρεώσεων που έχουν οι οργανισμοί του Δημοσίου στα πλαίσια της νέας αναθεωρημένης οδηγίας.

Στο έκτο κεφάλαιο παρουσιάζεται η λύση των SIEM εργαλείων και πως αυτά συμβάλουν στην επίτευξη συμμόρφωσης με όλες τις τεχνικές πτυχές της νέας οδηγίας NIS 2.

Στο έβδομο κεφάλαιο θα επικεντρωθούμε σε ένα συγκεκριμένο SIEM εργαλείο το OSSIM της AlienVault. Θα παρουσιαστούν τα βήματα εγκατάστασης στο Πληροφοριακό Σύστημα ενός δημόσιου οργανισμού.

Στο όγδοο κεφάλαιο θα γίνει η παρουσίαση του AlienVault OSSIM στην μελέτη εφαρμογής που πραγματοποιήθηκε σε έναν δημόσιο φορέα.

Στο τελευταίο και ένατο κεφάλαιο θα γίνει η σύνοψη της υλοποίησής και θα εξαχθούν τα συμπεράσματα για τη χρήση τους σε μελλοντικές επεκτάσεις.

2

Κυβερνοασφάλεια

2.1 Η έννοια της κυβερνοασφάλειας

Αν και δεν υπάρχει συμβατικός ορισμός της κυβερνοασφάλειας, θα μπορούσαμε να ορίσουμε ως κυβερνοασφάλεια την «τέχνη» εκείνη που έχει ως απώτερο σκοπό την προστασία δικτυακών συσκευών και δεδομένων από άνομη πρόσβαση ή εγκληματική χρήση με σκοπό την καταπάτηση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών.

Μία άλλη ποιο σύγχρονη προσέγγιση, είναι αυτή των Schatz Daniel et al.[1], κατά την οποία «Κυβερνοασφάλεια είναι η προστασία των συστημάτων και των δικτύων από παράνομη αποποίηση και παράνομη δημοσιοποίηση πληροφοριών, όπως επίσης και από την διαταραχή ή την παραπλανητική ανακατεύθυνση των υπηρεσιών που παρέχουν».

Κατά την ΕΕ, ο όρος «κυβερνοασφάλεια» καλύπτει κάθε παράνομη δραστηριότητα με τη χρήση ψηφιακών μέσων και όχι μόνο την ασφάλεια των δικτύων και των πληροφοριών. Οι κακόβουλες αυτές δραστηριότητες στον κυβερνοχώρο ισοδυναμούν με τον όρο κυβερνοέγκλημα όπως την εξαπόλυση επιθέσεων με κακόβουλα προγράμματα υπολογιστών ή την εξαπάτηση μέσω ηλεκτρονικών πληρωμών καθώς και τη διάδοση υλικού παιδεραστίας στο διαδίκτυο.

Το κυβερνοέγκλημα μπορεί να αποτελέσει ένα πολύ ισχυρό όπλο στα χέρια κυβερνοτρομοκρατών, οι οποίοι μπορούν να πάσα στιγμή να προβούν σε τρομοκρατικές επιθέσεις στον κυβερνοχώρο της υποδομής μίας χώρας. Επίσης θα μπορούσε να χρησιμοποιηθεί ως ένα επικίνδυνο όπλο σε εκστρατείες προπαγάνδας για την άσκηση επιρροής της κοινής γνώμης οι οποίες μπορεί έχουν καταστροφικές επιπτώσεις στις κοινωνίες. Επιπλέον, η Ευρωπόλ τα τελευταία χρόνια πρωτοστατεί στην πάταξη του κυβερνοεγκλήματος καθώς θεωρεί ότι υπάρχει σύγκλιση με τα εγκλήματα της τρομοκρατίας. [2]

Τον Σεπτέμβριο του έτους 2020 καταγράφηκε επίσημα ο πρώτος θάνατος πολίτη που οφείλεται σε κυβερνοεπίθεση σε βάρος κρίσιμης υποδομής. Συγκεκριμένα, η επίθεση τύπου ransomware που εκδηλώθηκε από άγνωστους οι οποίοι εκμεταλλεύτηκαν μία ευπάθεια των πληροφοριακών συστημάτων νοσοκομείου του Ντίσελντορφ της Γερμανίας, είχε ως αποτέλεσμα να αδρανοποιήσει τη συγκεκριμένη δομή υγείας και να προκαλέσει έμμεσα το θάνατο μίας γυναίκας, εξαιτίας της αναγκαστικής διακομιδής της σε άλλο νοσοκομείο [3]. Το συγκεκριμένο περιστατικό πρόσβαλε την ανθρώπινη ζωή, το μέγιστο αγαθό. Το σίγουρο είναι όμως ότι η με εκθετικούς ρυθμούς αυξανόμενη τεχνολογική πρόοδος είναι αλληλένδετα συνδεδεμένη με την αύξηση του κινδύνου της απειλής και αποσταθεροποίησης πολλών άλλων σημαντικών αγαθών της ζωής των πολιτών τόσο της Ευρώπης, όσο και όλου του πλανήτη.

Μία κυβερνοεπίθεση μπορεί να ταξινομηθεί είτε σύμφωνα με το είδος καταστροφής που μπορεί να προκαλέσει στις πληροφορίες – τροποποίηση, καταστροφή ή άρνηση πρόσβασης– είτε σύμφωνα με τις παραβιαζόμενες αρχές ασφάλειας που μπορεί να προκαλέσει.. Ορισμένα παραδείγματα επιθέσεων περιγράφονται στην Εικόνα 2-1.

Εικόνα 2-1 Τα είδη απειλών και οι αρχές ασφάλειας που θέτουν σε κίνδυνο [4]

Εικόνα 1 – Τα είδη απειλών και οι αρχές ασφάλειας που θέτουν σε κίνδυνο

Λουκέτο = χωρίς αντίκτυπο στην ασφάλεια. Θαυμαστικό = η ασφάλεια σε κίνδυνο. (www.eca.europa.eu)

2.2 Στόχοι Κυβερνοασφάλειας

Με βάση τα παραπάνω, μπορούν να αναλυθούν οι επτά στόχοι της ασφάλειας στον κυβερνοχώρο και να προχωρήσει η εννοιολογική διερεύνηση τους, καλύπτοντας εν συντομία τις πρακτικές που εμπίπτουν σε αυτούς τους στόχους.

2.2.1 Εμπιστευτικότητα (confidentiality)

Η εμπιστευτικότητα είναι η δυνατότητα της μη διάθεσης/αποκάλυψης των πληροφοριών σε μη εξουσιοδοτημένα άτομα, προγράμματα ή διαδικασίες. Η συσχέτιση με την ασφάλεια των πληροφοριών έγκειται στο γεγονός ότι απαιτεί έλεγχο της πρόσβασης σε προστατευμένες πληροφορίες μόνο σε εξουσιοδοτημένους χρήστες. Η εμπιστευτικότητα διασφαλίζει ότι μόνο εξουσιοδοτημένα άτομα έχουν πρόσβαση στις πληροφορίες και ενώ απαγορεύεται η πρόσβαση σε μη εξουσιοδοτημένα άτομα. Η εμπιστευτικότητα μπορεί να εξασφαλιστεί με τη βοήθεια της κρυπτογραφίας, με την οποία δημιουργούνται ψηφιακά κλειδιά.

2.2.2 Ακεραιότητα (integrity)

Ακεραιότητα αφορά την διαδικασία κατά την οποία οι πληροφορίες προστατεύονται από ακατάλληλη τροποποίηση και καταστροφή, διασφαλίζοντας ότι οι πληροφορίες δεν μπορούν να αλλάξουν χωρίς εντοπισμό και η διασφάλιση της ακεραιότητας των πληροφοριών. Η ακεραιότητα βασίζεται στην κρυπτογράφηση και τον κατακερματισμό για να διασφαλιστεί η καλύτερη δυνατή προστασία από κακόβουλες ενέργειες και απειλές στον κυβερνοχώρο, απαιτώντας όλες οι πληροφορίες να παραμένουν ασφαλής και αναλλοίωτες.

2.2.3 Αξιοπιστία (Reliability)

Η ικανότητα ενός συστήματος να λειτουργεί υπό καθορισμένες συνθήκες με απώτερο σκοπό την αξιοπιστία την ακεραιότητα και την ταυτότητα των προσωπικών πληροφοριών. Ένας χρήστης, ή ένας οργανισμός, έχει ως απαίτηση όλες οι πληροφορίες του να παραμένουν ασφαλής και αναλλοίωτες.

2.2.4 Διαθεσιμότητα (Availability)

Εξασφαλίζει ότι οι εξουσιοδοτημένοι χρήστες έχουν πρόσβαση στις υπηρεσίες του δικτύου υπολογιστών όταν τις χρειάζονται και χωρίς αδικαιολόγητη καθυστέρηση. Κύριο μέλημα είναι η αποτροπή κακόβουλων επιθέσεων που εμποδίζουν την πρόσβαση εξουσιοδοτημένων χρηστών στα συστήματα πληροφοριών.

2.2.5 Αυθεντικοποίηση

Η αυθεντικοποίηση αφορά τη διαδικασία επαλήθευσης ταυτότητας ενός ατόμου ή μίας διεργασίας. Τα συστήματα αυθεντικοποίησης είναι τα πρώτα στη γραμμή κρούσης κατά την διάρκεια μιας κυβερνοεπίθεσης, καθώς η μη εξουσιοδοτημένη πρόσβαση έχει ως αποτέλεσμα την κλοπή ή παραβίαση ψηφιακού υλικού. Τα περισσότερα πληροφοριακά συστήματα χρησιμοποιούν πλέον έλεγχο ταυτότητας πολλαπλών παραγόντων. Ο έλεγχος ταυτότητας

πολλαπλών παραγόντων είναι αδιαμφισβήτητα πιο ασφαλής επειδή, εκτός από τον κωδικό πρόσβασης, υπάρχουν πρόσθετες παράμετροι για την επαλήθευση της ταυτότητας ενός χρήστη.

2.2.6 Εξουσιοδότηση (Authorization)

Η εξουσιοδότηση είναι η διαδικασία κατά την οποία καθορίζονται τα δικαιώματα πρόσβασης σε πληροφορίες ή πόρους ενός συστήματος. Ο καθορισμός του τύπου χρήστη (διαχειριστή, απλός χρήστης ή απλός επισκέπτης), είναι κρίσιμος παράγοντας για την σωστή προσπέλαση, τροποποίηση και ρύθμιση του πόρου. Η εξουσιοδότηση συνήθως συνδυάζεται με έλεγχο ταυτότητας, ώστε να καθορίζεται με σαφήνεια για το ποιος είναι ο χρήστης που ζητά πρόσβαση.

2.2.7 Μη αποποίηση (Non-repudiation)

Η διασφάλιση της μη αποποίηση μπορεί να επιτευχθεί με την χρήση ψηφιακών υπογραφών. Με αυτόν τον τρόπο γίνεται η διαβεβαίωση ότι στον αποστολέα των πληροφοριών παρέχεται απόδειξη παράδοσης και στον παραλήπτη παρέχεται απόδειξη της ταυτότητας του αποστολέα, επομένως κανένας από τους δύο δεν μπορεί αργότερα να αρνηθεί ότι έχει επεξεργαστεί τις πληροφορίες και έτσι να αποτραπεί η αποποίηση της ευθύνης των χρηστών για ορισμένες δραστηριότητες. Η φιλοσοφία των ψηφιακών αρχών πιστοποίησης είναι να διασφαλίζουν ότι τα δημόσια κλειδιά αντιστοιχούν στη νομική οντότητα που υποτίθεται ότι είναι ο ιδιοκτήτης τους, ώστε άλλες νομικές οντότητες και χρήστες να μπορούν να εμπιστεύονται αυτά τα κλειδιά και τις υπογραφές.

2.3 Πόσο σοβαρό είναι το πρόβλημα

Σύμφωνα με την Εκθέσεις ελέγχου του Contact Committee των ανώτατων οργάνων ελέγχου της Ευρωπαϊκής Ένωσης [5], σήμερα η ελλείπει συγκέντρωση συγκρίσιμων γεγονότων, κάνει δύσκολο το έργο των αρχών να μετρήσουν τον γενικό αντίκτυπο των κακόβουλων δράσεων κατά της ασφάλειας. Οι επιθέσεις αυτές όχι μόνο κατάφεραν να «προσπεράσουν» τους ελέγχους ασφαλείας αλλά είχαν και ως αποτέλεσμα από το 2014 έως το 2018 να πενταπλασιαστεί η κυβερνοεγκληματικότητα με τεράστιο οικονομικό αντίκτυπος, πλήττοντας κυβερνήσεις και επιχειρήσεις, ανεξαρτήτως μεγέθους. Το γεγονός αυτό είχε ως αποτέλεσμα να γίνει μια τεράστια αύξηση των κυβερνοασφαλίστρων από 3 δισεκατομμύρια ευρώ το 2018 σε 8,8 δισεκατομμύρια ευρώ το 2021 [5].

Παρόλο που το ποσοστό του ιδιωτικού τομέα της ΕΕ που πλήγηκε από σοβαρά περιστατικά ασφαλείας έφτασε το 80% το 2016, η ανίχνευση ανωμαλιών παραμένει σε ανησυχητικά χαμηλά επίπεδα. Ποσοστό 69% των επιχειρήσεων της ΕΕ αγνοεί ή δεν συμμερίζεται την

σοβαρότητα των κινδύνων στους οποίους εκτίθεται στον κυβερνοχώρο, και ποσοστό 60% δεν εκτιμούν επαρκώς τον οικονομικό αντίκτυπο μιας παραβίασης ασφαλείας στον οργανισμό τους.

Σύμφωνα με την ένατη κατά σειρά ετήσια έκθεση της ENISA Threat Landscape (ETL) τα οκτώ σημαντικότερα είδη απειλών, τα οποία αποτυπώθηκαν και σχηματικά στην Εικόνα 2-2 είναι:

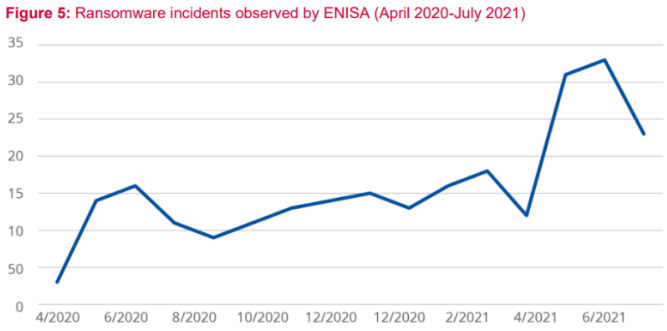
1. Ransomware
2. Malware
3. Cryptojacking
4. E-mail related threats
5. Threats against data
6. Threats against availability and integrity
7. Disinformation – Misinformation
8. Non - malicious threats

Εικόνα 2-2 ENISA Threat Landscape 2021 [6]

Στη σημερινή κυβερνοπραγματικότητα οι περισσότερες μορφές απειλών έχουν βασικό οικονομικό κίνητρο και σπανίως αφορούν περιπτώσεις κυβερνοβανδαλισμών, οι οποίες άνθιζαν παλαιότερα. Ακολούθως παρατίθεται μια πολύ σύντομη περιγραφή κάθε τέτοιας απειλής και πραγματικών περιστατικών σε βάρος κρίσιμων υποδομών:

- Ransomware

Ένας τύπος κακόβουλης επίθεσης όπου οι εισβολείς κρυπτογραφούν τα δεδομένα ενός οργανισμού και απαιτούν χρηματικά ανταλλάγματα (Bit coins, Monero, ή άλλα e-coins) ώστε να αποκαταστήσουν την πρόσβαση, ή σε κάποιες περιπτώσεις ώστε να μην αποκαλύψουν δεδομένα στο κοινό ή σε ανταγωνιστές [7]. Οι επιθέσεις αυτές, κατά το τελευταίο τρίμηνο του 2021, παρουσιάζουν σημαντική αύξηση, τόσο σε καταγεγραμμένα περιστατικά, όσο και σε οικονομική αποτίμηση (Εικόνα 2-3).

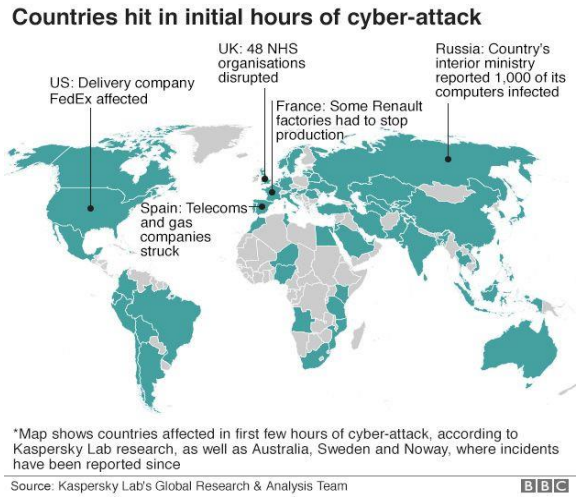


Εικόνα 2-3 Ransomware που παρατηρήθηκαν από την ENISA (Απρ 20-Ιούλ 21) [8]

Όπως είναι φυσικό, οι κρίσιμες υποδομές δεν θα μπορούσαν να απουσιάζουν από το target group των συγκεκριμένων επίδοξων κυβερνοεπιτιθέμενων. Πράγματι, την 25 Σεπτεμβρίου 2018 στόχος τέτοιας επίθεσης ήταν μία κρίσιμη υποδομή του τομέα μεταφορών και συγκεκριμένα το λιμάνι του Σαν Ντιέγκο στις Ηνωμένες Πολιτείες, περιστατικό το οποίο επηρέασε τα τρέχοντα αιτήματα αδειών πλοίων για την είσοδό τους στο λιμάνι, τα αιτήματα καταγραφής πλοίων και άλλες λειτουργίες. Μάλιστα, η υπεύθυνη Διευθύνων Σύμβουλος του λιμανιού χαρακτήρισε την επίθεση ως σοβαρό περιστατικό κυβερνοασφάλειας, το οποίο τους οδήγησε να ενεργοποιήσουν εναλλακτικά συστήματα και διαδικασίες για την ελαχιστοποίηση των επιπτώσεων στη δημόσια ασφάλεια [9].

Άλλη μια χαρακτηριστική περίπτωση επίθεσης ransomware που απασχόλησε την παγκόσμια κοινότητα ήταν αυτή του πήρε το όνομα WannaCry, η οποία στις διαφορετικές μορφές με τις οποίες εμφανίστηκε από 12 Μαΐου 2017, επηρέασε πολλούς οργανισμούς σε όλο τον κόσμο σε σύντομο χρονικό διάστημα. Οι εκτιμήσεις μιλούν για περίπου 190.000 υπολογιστές που επηρεάστηκαν σε περισσότερες από 150 χώρες. Ανάμεσα στους στόχους συγκαταλέγονται φορείς εκμετάλλευσης υποδομών ζωτικής σημασίας (υγεία, ενέργεια, μεταφορές, χρηματοδότηση και τηλεπικοινωνίες), κατασκευαστές και πάροχοι υπηρεσιών σε όλη την

Ευρώπη και τον κόσμο. Μάλιστα, σύμφωνα με τον χάρτη της Εικόνα 2-4, φαίνονται οι χώρες που χτυπήθηκαν τις πρώτες ώρες της συγκεκριμένης κυβερνοεπίθεσης.



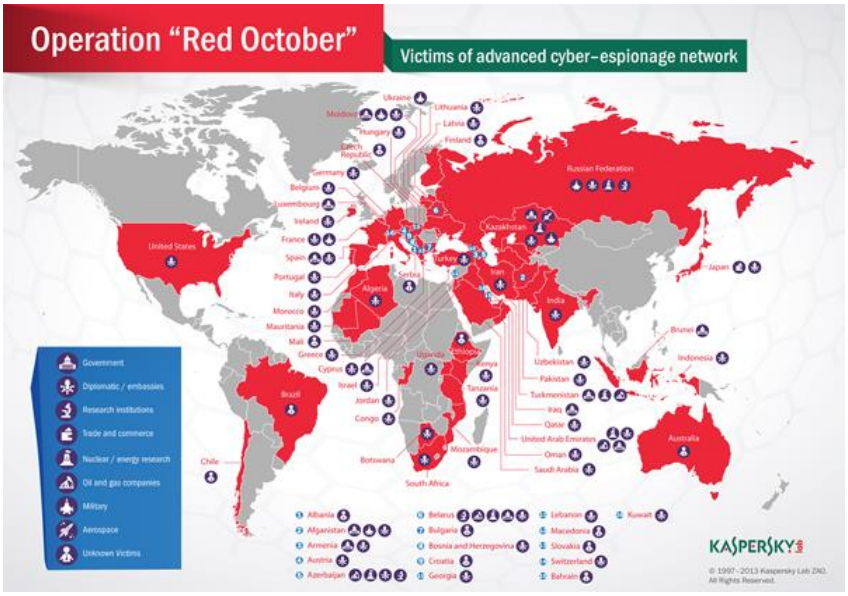
Εικόνα 2-4 Παγκόσμια Έρευνα Kaspersky Lab

Για τη συγκεκριμένη επίθεση, ο Udo HELMBRECHT, Εκτελεστικός Διευθυντής του ENISA, δήλωσε: «Ως Ευρωπαϊκός Οργανισμός Κυβερνοασφάλειας, παρακολουθούμε στενά την κατάσταση και εργαζόμαστε όλο το εικοσιτετράωρο με τα ενδιαφερόμενα μέρη μας για να διασφαλίσουμε την ασφάλεια των ευρωπαίων πολιτών και επιχειρήσεων και τη σταθερότητα της ψηφιακής ενιαίας αγοράς. Αναφέρουμε την εξέλιξη των επιθέσεων στην Ευρωπαϊκή Επιτροπή και επικοινωνούμε με τους εταίρους μας στο δίκτυο CSIRT της Ευρωπαϊκής Ένωσης».

- Malware

Στην περίπτωση αυτή βάλλεται ξεκάθαρα η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα ενός συστήματος, μέσω ενός κακόβουλου λογισμικού που προορίζεται να εκτελέσει μια μη εξουσιοδοτημένη διαδικασία. Παρά το γεγονός ότι την τελευταία πενταετία κατατάσσεται σταθερά σε υψηλό επίπεδο στη λίστα των απειλών, για το έτος 2021 παρουσιάζει πτωτικές τάσεις [10]. Η Kaspersky Lab το 2013 δημοσίευσε μία ερευνητική έκθεση [8] σύμφωνα με την οποία εντοπίστηκε μια προηγμένη εκστρατεία κυβερνοκατασκοπείας που στόχευε σε διπλωματικά και κυβερνητικά ιδρύματα παγκοσμίως, την οποία ονόμασε Red October. Οι επιτιθέμενοι δημιούργησαν μοναδικό, εξαιρετικά ευέλικτο κακόβουλο λογισμικό για την κλοπή δεδομένων από συστήματα υπολογιστών, κινητά τηλέφωνα και εξοπλισμό εταιρικού δικτύου των θυμάτων-στόχων, με ανυπολόγιστες δυσμενείς συνέπειες, καθώς οι στόχοι φέρονται να ξεπέρασαν τους 55.000, αφορούσαν πολύ μεγάλο μέρος των χωρών του

πλανήτη, όπως χαρακτηριστικά φαίνεται στην Εικόνα 5 και εκτός από κυβερνητικούς οργανισμού, έβαλαν κατά βασικών κρίσιμων υποδομών (ενέργεια, διάστημα, πυρηνικά κ.λπ.).



Εικόνα 2-5 Red October κατά βασικών κρίσιμων υποδομών [11]

- Hacking

Σύμφωνα με δημοσιεύματα τύπου [12] η McAfee, τον Φεβρουάριο του 2011, ανέφερε ότι εντόπισε κυβερνοεπιθέσεις σε εταιρίες παροχής ενέργειας (πετρέλαιο, φυσικό αέριο, πετροχημικά), χωρίς να κατονομάσει αυτές, οι οποίες είχαν ξεκινήσει από το 2009 και τις οποίες ονόμασε Night Dragon. Μάλιστα, στόχος της επίθεσης φέρεται να αποτέλεσαν οι νομικές και οικονομικές πληροφορίες, καθώς και οι πληροφορίες για τις συμφωνίες, χωρίς όμως οτιδήποτε να είναι απολύτως σαφές, με δεδομένη την ελλιπή πληροφόρηση. Σύμφωνα με το ίδιο δημοσίευμα φέρεται να επλήγησαν οι εταιρίες Exxon Mobil, Royal Dutch Shell and BP, καθώς επίσης και οι εταιρίες Marathon Oil, ConocoPhillips and Baker Hughes. Οι επιθέσεις αποδόθηκαν σε hackers που όπως προκύπτει από την έρευνα έδρασαν με έδρα την Κίνα, χωρίς όμως να συσχετίζονται αυτές με την κινεζική κυβέρνηση.

- Cryptojacking

Είναι ένας τύπος εγκλήματος στον κυβερνοχώρο όπου ένας εγκληματίας χρησιμοποιεί κρυφά την υπολογιστική ισχύ του θύματος για να δημιουργήσει κρυπτονομίσματα. Όπως είναι φυσικό, η δημοφιλία των κρυπτονομισμάτων και η διαρκώς αυξανόμενη απορρόφησή τους από το ευρύτερο κοινό, έχει παρασύρει σε αύξηση των αντίστοιχων περιστατικών κυβερνοασφάλειας. Παρά το γεγονός ότι τα περισσότερα θύματα μπορεί να μην παρατηρήσουν μόλυνση ή να μην αναγνωρίσουν τον ένοχο, η απειλή είναι πραγματική και επηρεάζει καίρια την απόδοση των συστημάτων, υποβαθμίζοντας αισθητά τις παρεχόμενες υπηρεσίες και δημιουργώντας σοβαρά προβλήματα στην εύρυθμη λειτουργία τους. Με βάση το δημοσίευμα [13], η εταιρεία ασφάλειας κρίσιμων υποδομών Radiflow ανακοίνωσε τον Δεκέμβριο του 2018

ότι ανακάλυψε κακόβουλο λογισμικό εξόρυξης κρυπτονομισμάτων στο δίκτυο επιχειρησιακής τεχνολογίας μιας εταιρείας ύδρευσης στην Ευρώπη, το οποίο ενεργούσε παρακολούθηση και έλεγχο. Με βάση την έρευνα που ακολούθησε προέκυψε ότι το κακόβουλο λογισμικό κατασκευάστηκε για να λειτουργεί αθόρυβα στο παρασκήνιο, χρησιμοποιώντας όση περισσότερη επεξεργαστική ισχύ μπορούσε για την εξόρυξη του κρυπτονομίσματος Monero χωρίς να κατακλύζει το σύστημα και να δημιουργεί προφανή προβλήματα και συνακόλουθα εύκολο εντοπισμό του.

- E-mail related threats

Οι επιθέσεις που σχετίζονται με το ηλεκτρονικό ταχυδρομείο είναι μια δέσμη απειλών που εκμεταλλεύονται αδυναμίες στις καθημερινές συνήθειες και στον ανθρώπινο παράγοντα, αντί κάποιας τεχνικής ευπάθειας στα συστήματα πληροφοριών. Παρά τις πολλές εκστρατείες ευαισθητοποίησης και εκπαίδευσης ενάντια σε αυτούς τους τύπους επιθέσεων, η απειλή παραμένει σε αξιοσημείωτο βαθμό και βασανίζει πολλούς φορείς, υπηρεσίες και επιχειρήσεις, ιδιαιτέρως μεγάλης κλίμακας. Με δεδομένο ότι καταγράφεται αύξηση αυτού του είδους των επιθέσεων, θα πρέπει να καταστεί κατανοητό ότι οι χρήστες δεν μπορούν να βασίζονται σε έναν γνωστό αξιόπιστο αποστολέα ώστε να θεωρούν ότι είναι ασφαλές να ανοίξουν συνημμένα ή συνδέσμους στην ηλεκτρονική αλληλογραφία τους. Πάμπολλα είναι τα παραδείγματα τέτοιων επιθέσεων σε οργανισμούς που εντάσσονται στις κρίσιμες υποδομές. Το 2017 χάκερ χτύπησαν τον λογαριασμό e-mail της Τράπεζας της Ιταλίας, το οποίο είχε ως αποτέλεσμα τη σημαντική διαρροή δεδομένων [3].

- Threats against data

Ως παραβίαση ή διαρροή δεδομένων περιγράφεται η αποδέσμευση ευαίσθητων, εμπιστευτικών ή προστατευμένων δεδομένων σε ένα μη αξιόπιστο περιβάλλον. Οι παραβιάσεις δεδομένων μπορεί να προκύψουν ως αποτέλεσμα μιας κυβερνοεπίθεσης, μιας εργασίας εμπιστευτικών πληροφοριών, ακούσιας απώλειας, ή έκθεσης δεδομένων. Η απειλή που σχετίζεται με την πρόσβαση στα δεδομένα δύναται να συνδυάζεται με εκβιασμούς, λύτρα, δυσφήμιση, παραπληροφόρηση. Το 2014 η Ευρωπαϊκή Κεντρική Τράπεζα έπεσε θύμα τέτοιας επίθεσης, η οποία είχε ως αποτέλεσμα να διαρρεύσουν 20.000 διευθύνσεις ηλεκτρονικού ταχυδρομείου και επαφές [3].

- Threats against availability and integrity

Η διαθεσιμότητα και η ακεραιότητα, δύο από τους τρεις συνολικά βασικούς παράγοντες της ασφάλειας, αποτελούν στόχο μιας πληθώρας απειλών και επιθέσεων, μεταξύ των οποίων ξεχωρίζουν αυτές που ονομάζονται άρνηση υπηρεσιών (Denial of Service) και κατανεμημένη άρνηση υπηρεσιών (Distribution DoS). Το DDoS είναι μια από τις πιο κρίσιμες απειλές για τα συστήματα πληροφορικής, στοχεύοντας στη διαθεσιμότητά τους, εξαντλώντας τους πόρους τους, προκαλώντας μειώσεις στην απόδοση, απώλεια δεδομένων και διακοπές λειτουργίας

[14]. Το 2007 στο πλαίσιο της Εσθονικής κυβερνοεπίθεσης καταγράφηκαν περιστατικά DDoS στις ψηφιακές υποδομές. Το 2012 μια κυβερνοεπίθεση DDoS είχε ως αποτέλεσμα να προκαλέσει πεντάωρο πρόβλημα διαθεσιμότητας του Διεθνούς Νομισματικού Ταμείου.

- Disinformation – misinformation

Η παραπληροφόρηση και οι κακόβουλες πληροφορίες αποτελούν όλο και πιο σημαντικά στοιχεία σε υβριδικές επιθέσεις που συνδυάζουν επιθέσεις στον κυβερνοχώρο και παραβιάσεις δικτύων [15]. Οι επιθέσεις αυτές εκμεταλλεύονται την ευρεία εξάπλωση των μέσων κοινωνικής δικτύωσης και των διαδικτυακών μέσων ενημέρωσης και αποκτούν αυξημένη δυναμική. Στοχεύουν στο να μειώσουν τη συνολική αντίληψη της εμπιστοσύνης, που είναι κύριος υπέρμαχος της κυβερνοασφάλειας και να δημιουργούν κλίμα δυσπιστίας, υπονομεύοντας την εμπιστοσύνη και τις δημοκρατικές διαδικασίες. Χαρακτηριστικό παράδειγμα αποτέλεσε η ραγδαία αύξηση των ανθρώπων που ενημερώνονται μέσω του διαδικτύου, ιδίως τα δύο τελευταία έτη και λόγω της πανδημίας. Η κλίμακα, η ταχύτητα και το εύρος της παραπληροφόρησης έχουν πλέον αυξηθεί σε σημείο που αποτελεί πραγματική απειλή για την ασφάλεια της ΕΕ. Χαρακτηριστικό της δυναμικής των fake news είναι ότι σύμφωνα με μελέτες, έχει αποδειχθεί ότι τα ψεύτικα νέα ταξιδεύουν έξι φορές γρηγορότερα από την αλήθεια [16].

- Non malicius threats

Στη μεγάλη αυτή κατηγορία εντάσσονται περιπτώσεις που δύνανται να αποβούν ιδιαιτέρως ζημιογόνες, ή ακόμη και καταστροφικές, χωρίς να προκύπτει ξεκάθαρη κακόβουλη πρόθεση των εμπλεκομένων. Αφορούν σε ανθρώπινα λάθη, ή ακόμη και σε λανθασμένες διαμορφώσεις πληροφοριακών συστημάτων. Η συνεχής και σταθερή ετήσια παρουσία τους στο τοπίο των καταγεγραμμένων απειλών μας οδηγεί στο συμπέρασμα ότι αποτελούν σημαντικό μέλημα για τις εκτιμήσεις κινδύνου. Η γνωστή κυβερνοεπίθεση WannaCry (12-5-2017) επηρέασε ιδιαίτερα το Εθνικό Σύστημα Υγείας της Αγγλίας, το οποίο για να καταφέρει να επανακάμψει και να διατηρήσει την υγεία και περίθαλψη των ασθενών εφάρμοσε τις ρυθμίσεις έκτακτης ανάγκης. Από την έρευνα που ακολούθησε, ανάμεσα στα άλλα, διαπιστώθηκε ότι όλοι οι οργανισμοί που μολύνθηκαν μοιράζονταν την ίδια ευπάθεια και συγκεκριμένα είχαν μη επιδιορθωμένα ή μη υποστηριζόμενα λειτουργικά συστήματα Windows, επομένως ήταν επιρρεπείς στο ransomware [17].

2.4 Έκρηξη των κυβερνοεπιθέσεων μέσα στην πανδημία

Κατά την περίοδο της πανδημίας του Covid-19 παρατηρήθηκε έκρηξη στον αριθμό των επιθέσεων στον κυβερνοχώρο σε δημόσιους οργανισμούς και ιδρύματα, ενώ πρόσφατη μελέτη της ΕΥ [18] δείχνει αύξηση 10%-20% στον αριθμό των κυβερνοεπιθέσεων εντός των τελευταίων 12μηνών του 2021, σε σύγκριση με τα προηγούμενα έτη. [19]

Στις μέρες μας νέα τρωτά σημεία εισήλθαν σε ένα ήδη ταχέως μεταβαλλόμενο περιβάλλον και συνεχίζουν να απειλούν κρίσιμες υποδομές της χώρας δυσκολεύοντας το έργο των Υπευθύνων Ασφαλείας να προστατεύσουν τον οργανισμό τους. Στην Ελλάδα σύμφωνα με επίσημα στοιχεία [19] κατά τη διάρκεια του 2020 παρουσιάστηκε μεγάλος αριθμός παραβιάσεων τύπου ransomware με κάποιες από τις πιο σημαντικές να αφορούν σε δημόσιους φορείς. Ο COVID-19 ανάγκασε τους οργανισμούς να παρακάμψουν τις διαδικασίες ασφάλειας στον κυβερνοχώρο στα πλαίσια της τηλεργασίας των υπαλλήλων με αποτέλεσμα οι περισσότερες επιθέσεις να στοχοποιούν τα εργαλεία που χρησιμοποιήθηκαν κατά την περίοδο της τηλεργασίας. [19] Πολλοί οργανισμοί δεν ενέπλεξαν την κυβερνοασφάλεια στη διαδικασία της τηλεργασίας, είτε μέσω εποπτείας είτε μέσω επείγουσας ανάγκης να κινηθούν όσο το δυνατόν γρηγορότερα. Ως αποτέλεσμα, νέα τρωτά σημεία εισήλθαν στον χώρο της τηλεργασίας και συνεχίζουν να απειλούν τους οργανισμούς μέχρι σήμερα.

Σήμερα, οι Υπεύθυνοι Ασφαλείας έχουν να αντιμετωπίσουν την αναταραχή της παγκόσμιας πανδημίας, η οποία έχει δημιουργήσει μια τέλεια «καταιγίδα» συνθηκών στις οποίες μπορούν να δράσουν άπειροι παράγοντες απειλών. Δεν είναι απλά υπεύθυνοι για τον έλεγχο και την ασφάλεια των δικτύων και των υπολογιστών του οργανισμού, αλλά και υπεύθυνοι στο να μεταλαμπαδεύουν στους εργαζόμενους πώς θα πρέπει να προστατεύουν τα αντίστοιχα «γραφεία» στο σπίτι τους, καθώς η συντριπτική πλειονότητα των επιτυχημένων παραβιάσεων είναι επακόλουθο ανθρώπινου λάθους.

Ένα παράδειγμα παραβίασης της κυβερνοασφάλειας στην απομακρυσμένη εργασία ήταν η σειρά κυβερνοεπιθέσεων σε υπηρεσίες τηλεδιάσκεψης. Μεταξύ Φεβρουαρίου 2020 και Μαΐου 2020, περισσότεροι από μισό εκατομμύριο άνθρωποι επηρεάστηκαν από παραβιάσεις κατά τις οποίες τα προσωπικά δεδομένα των χρηστών υπηρεσιών τηλεδιάσκεψης (π.χ. όνομα, κωδικοί πρόσβασης, διευθύνσεις email) κλάπηκαν και πωλήθηκαν στον σκοτεινό ιστό. Για να εκτελέσουν αυτήν την επίθεση, ορισμένοι χάκερ χρησιμοποίησαν ένα εργαλείο που ονομάζεται «OpenBullet». [20]

3

Στρατηγική της ΕΕ για την Κυβερνοασφάλεια

Με γνώμονα την μείωση των απειλών στον κυβερνοχώρο, η ΕΕ προχώρησε στην υλοποίηση σχετικών δράσεων τόσο σε εθνικό επίπεδο όσο και στο πλαίσιο μορφών συνεργασίας. Η νέα πολιτική για την κυβερνοάμυνα στοχεύει στον εντοπισμό και την αποτροπή των συνεχώς αυξανόμενων επιθέσεων διασφαλίζοντας την προστασία όλων των πολιτών καθώς και των επιχειρήσεων. Η στρατηγική της ΕΕ για την κυβερνοασφάλεια αφορά την ωφέλεια όλων, είτε πρόκειται για τα δίκτυα ενέργειας, τις υποδομές των μεταφορών, τις ένοπλες δυνάμεις, τους δημόσιους φορείς ή οτιδήποτε εξυπηρετεί τους Ευρωπαίους, εξασφαλίζοντας την προστασία τους.

Ο κύριος στόχος της νέας στρατηγικής είναι η ενίσχυση της Ευρωπαϊκής ανθεκτικότητας έναντι των κυβερνοεπιθέσεων. Εστιάζει στην πλήρη αξιοποίηση των πόρων που διαθέτει η ΕΕ έτσι ώστε να είναι κυρίαρχη τεχνολογικά καθώς επίσης επιχειρεί παγκόσμιες συνεργασίες με εταίρους κατοχυρώνοντας τον ηγετικό της ρόλο.

Μέρος της στρατηγικής της Ε.Ε. είναι η εφαρμογή της (αναθεωρημένης) οδηγίας «NIS 2» η οποία αφορά στην μείωση της αυξανόμενης έκθεσης της Ευρώπης στις κυβερνοαπειλές. Ουσιαστικά η νέα οδηγία περιλαμβάνει περισσότερους τομείς κοινωνικής και οικονομικής σημασίας, οι οποίοι είναι υπόχρεοι να τηρούν όλα τα μέτρα που έχουν ληφθεί έναντι των κινδύνων έτσι ώστε να ενισχυθεί η κυβερνοανθεκτικότητα καθώς και να διατηρηθεί σε βάθος χρόνου. Απευθύνεται σε δημόσιες υπηρεσίες αλλά και σε ιδιωτικές εταιρείες στις οποίες διενεργούνται έλεγχοι για την συμμόρφωση στις υποχρεώσεις τους περί της κυβερνοασφάλειας. Μια πιθανή επιβλαβής κυβερνοεπίθεση, μπορεί να έχει τεράστια επιρροή ακόμη και στην οικονομία ενός ή πολλών κρατών μελών της Ε.Ε. Για τον λόγο αυτό, τίθεται άμεσα σε λειτουργία και η συνεργασία των αρχών μεταξύ των Ευρωπαϊκών χωρών.

3.1 Η εμπιστοσύνη και η ασφάλεια στο επίκεντρο της ψηφιακής δεκαετίας της ΕΕ

Η νέα στρατηγική της ΕΕ για την κυβερνοασφάλεια έχει ως κύρια προτεραιότητα να προσφέρει ένα παγκόσμια ανοιχτό διαδίκτυο και να διαφυλάξει όχι μόνο την ασφάλεια, αλλά και τις αξίες και τα θεμελιώδη δικαιώματα των πολιτών της. Στηριζόμενη στην επιτυχία της προηγούμενης στρατηγικής, η νέα στρατηγική επικεντρώνεται σε επενδυτικές, ρυθμιστικές και πολιτικές πρωτοβουλίες σε τρεις τομείς δέσμευσης της ΕΕ. Ανθεκτικότητα, τεχνολογική υπεροχή και ηγεσία, ανάπτυξη επιχειρησιακής ικανότητας πρόληψης, αποτροπής και αντιμετώπισης και τέλος προώθηση ενός παγκόσμιου και ανοιχτού κυβερνοχώρου μέσω συνεργασίας.

3.2 Ανθεκτικότητα, τεχνολογική κυριαρχία και ηγετική θέση

Δεδομένων των πρόσφατων κυβερνοεπιθέσεων παγκοσμίως, λαμβάνοντας υπόψη περιστατικά στον τομέα της υγείας, όπου προσωπικά δεδομένα ασθενών εκλάπησαν, όπως επίσης δεδομένα στον τομέα των καυσίμων, προκαλώντας λογιστικά θέματα, καθώς και σε άλλες υπηρεσίες ζωτικής σημασίας, η Ευρωπαϊκή Επιτροπή επιταχύνει την πρόοδο των μέτρων έτσι ώστε να αυξήσει τα επίπεδα της ανθεκτικότητας στον κυβερνοχώρο. Τα καταγεγραμμένα περιστατικά επισημαίνουν τον μεγάλο κίνδυνο για την οικονομία και την κοινωνία γενικότερα έχοντας αντίκτυπο σε όλους, υπονομεύοντας την ασφάλειά μας. Έτσι λοιπόν επιδιώκεται μία προσέγγιση για την διασφάλιση της ανθεκτικότητας και της έγκαιρης ενημέρωσης των περιστατικών δημιουργώντας ένα δίκτυο κέντρων επιχειρήσεων ασφαλείας («SOC») ώστε η δράση να είναι άμεση και να προέχει στης βλάβης με την βοήθεια της Τεχνητής Νοημοσύνης («A.I.»). Επίσης πρόσθετα μέτρα αναλαμβάνουν υποστηρικτικό ρόλο στις μικρές και μεσαίες επιχειρήσεις αναβαθμίζοντας τα ψηφιακά μέσα και εκπαιδεύοντας το προσωπικό ώστε να επιτευχθεί η μείωση της εξάπλωσης του προβλήματος. [21]

3.3 Ανάπτυξη επιχειρησιακής ικανότητας πρόληψης, αποτροπής και αντιμετώπισης

Οι ολοένα αυξανόμενες επιθέσεις σε δίκτυα και πληροφοριακά συστήματα καθώς και η εξάρτηση από βάσεις δεδομένων ευαίσθητων πληροφοριών, οδήγησαν την Επιτροπή να

στοχεύσει στην συνεργασία των αρχών και των οργάνων των χωρών της Ε.Ε. σε ότι αφορά την πρόληψη, αποτροπή και αντιμετώπιση των κυβερνοεπιθέσεων. Βέβαια, εξαιρείται η στρατιωτική, διπλωματική και διαστημική βιομηχανία μιας και η Επιτροπή προτείνει νέο σχέδιο δράσης σε αυτούς τους τομείς. Ως εκ τούτου, είναι απαραίτητη η δημιουργία μίας Κοινής Μονάδας Κυβερνοχώρου στην οποία όλες οι κοινότητες υποχρεούνται να καταβάλουν τις προσπάθειες τους ούτως ώστε να συμβάλουν στην ανθεκτικότητα του κυβερνοχώρου παραμένοντας συνδεδεμένες σε ότι και αν προκύψει. Ο ύπατος εκπρόσωπος επικεντρώνεται στην ενίσχυση των ψηφιακών εργαλείων που τους είναι απαραίτητα με σκοπό την πρόληψη, αποτροπή και αντιμετώπιση των κυβερνοεγκλημάτων, δίνοντας ιδιαίτερη βαρύτητα στις εφοδιαστικές αλυσίδες, στην ηλεκτρονική επικοινωνία και στην καταπολέμηση της παιδικής σεξουαλικής κακοποίησης, αλλά και σε όλες τις υποδομές ζωτικής σημασίας που επηρεάζονται. [21]

3.4 Προώθηση παγκόσμιου και ανοικτού κυβερνοχώρου μέσω αυξημένης συνεργασίας

Σε μια εποχή που τα κυβερνοεγκλήματα αποτελούν μάστιγα απειλώντας τα ανθρώπινα δικαιώματα, την ελευθερία χρήσης του διαδικτύου και την διεθνή ασφάλεια, η Ε.Ε. ενδυναμώνει τις δράσεις της στον τομέα της συνεργασίας. Πιο συγκεκριμένα, προωθεί δράσεις με σκοπό την ενίσχυση της υπευθυνότητας των κρατών στον κυβερνοχώρο σε επίπεδο Ηνωμένων Εθνών. Εκτός αυτού, μεγάλη βαρύτητα δίνει στην ανάπτυξη της κυβερνο-διπλωματίας, με την δημιουργία σχέσεων με τρίτες χώρες. Διεθνείς ομάδες που θα συμμετέχουν στην κοινότητα, θα προσφέρουν την βοήθειά τους ούτως ώστε να εξαπλωθεί μία παγκόσμια ασπίδα προστασίας η οποία θα μας παρέχει έναν ανοιχτό διαδικτυακό χώρο χωρίς περιορισμούς. Επιπροσθέτως, η Ε.Ε. ορίζει ένα συμβούλιο το οποίο θα είναι υπεύθυνο για τον συντονισμό όλων των οργάνων και των οργανισμών που εμπλέκονται στα πλαίσια της συνεργασίας.

Παράλληλα, στα μέτρα για την ενίσχυση της κυβερνοασφάλειας, προστίθενται η δέσμευση για νέες επενδύσεις, εκδίδοντας έναν μακροπρόθεσμο προϋπολογισμό ο οποίος αφορά σε προγράμματα όπως «Ψηφιακή Ευρώπη» και «Ορίζων Ευρώπη». Τα κονδύλια θα απορροφηθούν στη δημιουργία φυσικής και εικονικής πλατφόρμας, στην ασφάλεια των καναλιών επικοινωνίας αλλά και στην εξέλιξη της δυνατότητας εντοπισμού των απειλών. Οι επενδύσεις τείνουν να είναι συνδυαστικές και τα κράτη μέλη οφείλουν να εκμεταλλευτούν με τον καλύτερο τρόπο τον μηχανισμό ανάκαμψης και ανθεκτικότητας, με τελικό σκοπό την ενίσχυση των μικρομεσαίων επιχειρήσεων. Η δημιουργία μιας κοινής διεθνούς φύσεως ομάδας

θα συνδράμει στην διατήρηση ενός ηγετικού ρόλου στην κυβερνοασφάλεια παρέχοντας σε όλους τον ελεύθερο, χωρίς περιορισμούς ανοιχτό κυβερνοχώρο.

4

Εθνική Στρατηγική Κυβερνοασφάλειας 2020-2025

Εντός της ευρύτερης στρατηγικής κυβερνοθωράκισης, στην οποία συμμετέχει ενεργά και η χώρα μας, αναγνωρίζοντας τη σημαντικότητα της ανταπόκρισής της επί του θέματος, έχουν αναληφθεί συγκεκριμένες θεσμικές πρωτοβουλίες, οι οποίες χαρακτηρίζουν μονοσήμαντα την Εθνική Στρατηγική Κυβερνοασφάλειας και περιλαμβάνονται στη νομοθετική αντιμετώπιση του ζητήματος, που υλοποιήθηκε με το Ν. 4577 «Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις», αλλά και την Υπουργική Απόφαση 1027/2019, δια των οποίων καθορίστηκε το πλαίσιο υποχρεώσεων για τους Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών (Φ.Ε.Β.Υ.) και τους Παρόχους Ψηφιακών Υπηρεσιών (Π.Ψ.Υ.). Μάλιστα, στην ίδια απόφαση συμπεριλήφθηκαν και προβλέφθηκαν ζητήματα απαιτήσεων ασφαλείας που οφείλουν να τηρούν οι φορείς αυτοί, ζητήματα οργάνωσης και συμμετοχής σε ασκήσεις ετοιμότητας, καθώς και το σύνολο των ζητημάτων που άπτονται των αναφερομένων ζητημάτων και υπήρξε η αναγκαιότητα ρύθμισης [22].

Η συνολική προσπάθεια κατατείνει στον ψηφιακό μετασχηματισμό της χώρας μας, που είναι βέβαιο ότι θα συνεισφέρει σημαντικά στην οικονομική και κοινωνική σταθερότητα και ανάπτυξη. Οι ψηφιακές υπηρεσίες τυγχάνουν αυξημένης ανάγκης προστασίας, καθώς η χώρα μας φιλοδοξεί να δημιουργήσει ασφαλές περιβάλλον επιχειρηματικής ανάπτυξης και να διασφαλίσει τις κατάλληλες συνθήκες προς τους πολίτες της, ώστε να εμπιστευτούν τις ψηφιακές υπηρεσίες και κατ` επέκταση τις ψηφιακές τεχνολογίες [22].

4.1 Στρατηγικός Σχεδιασμός για Δημόσια Διοίκηση και ΟΤΑ

Οι τελευταίες τεχνολογικές εξελίξεις, σε συνδυασμό με την ενεστώσα γεωπολιτική κατάσταση καθιστούν αναγκαία την αναπροσαρμογή των μέτρων κυβερνοασφάλειας, η οποία εντάσσεται

σε πλαίσιο ευρύτερου στρατηγικού σχεδιασμού, με πρωταρχικό στόχο την προάσπιση της ακεραιότητας των υφιστάμενων υποδομών, που συναρτούν άμεσα τη διασφάλιση της εύρυθμης λειτουργίας του κράτους και παρέχουν εχέγγυα ασφάλειας στους πολίτες.

Η Εθνική Στρατηγική Κυβερνοασφάλειας για την περίοδο 2020-2025 θεσμοθετήθηκε σε ένα περιβάλλον απειλών που αλλάζει δυναμικά και επηρεάζεται από το ευρύτερο πλαίσιο των απειλών στον κυβερνοχώρο. Στο πλαίσιο αυτό τέθηκε ως βασικός στόχος η προστασία των κρίσιμων υποδομών δια της θεσμοθέτησης μέτρων που επιτυγχάνουν το βέλτιστο δυνατό περιορισμό των κακόβουλων ενεργειών σε βάρος αυτών.

Υπό το πρίσμα των ανωτέρω αρχών και προτεραιοτήτων του στρατηγικού σχεδιασμού, διαμορφώνονται πέντε (5) πυλώνες παρέμβασης Εικόνα 4-1, οι οποίοι καλύπτουν όλους τους στόχους που θέτει ο ENISA για τα κράτη μέλη της Ε.Ε., ως ακολούθως:[11]

- Δημιουργία ενός λειτουργικού συστήματος διακυβέρνησης,

- Νέες τεχνολογικές λύσεις και προσεγγίσεις που επιτυγχάνουν ισχυροποίηση της προστασίας των κρίσιμων υποδομών

- Αποδοτικότερη διαχείριση των περιστατικών που απασχολούν, προς την κατεύθυνση προστασίας της ιδιωτικότητας, στο γενικότερο πλαίσιο της καταπολέμησης του κυβερνοεγκλήματος

-Δημιουργία συνθηκών ανάπτυξης και έρευνας, αλλά και περιβάλλον που θα προάγει τις σχετικές σύγχρονες επενδύσεις

- Ενεργή εμπλοκή των πολιτών και αρχών, με στόχο τη βελτίωση της ικανότητας αντίδρασης από το σύνολο των δομών, μέσα σε ένα πλαίσιο διαρκούς ενημέρωσης και συνολικής ευαισθητοποίησης.

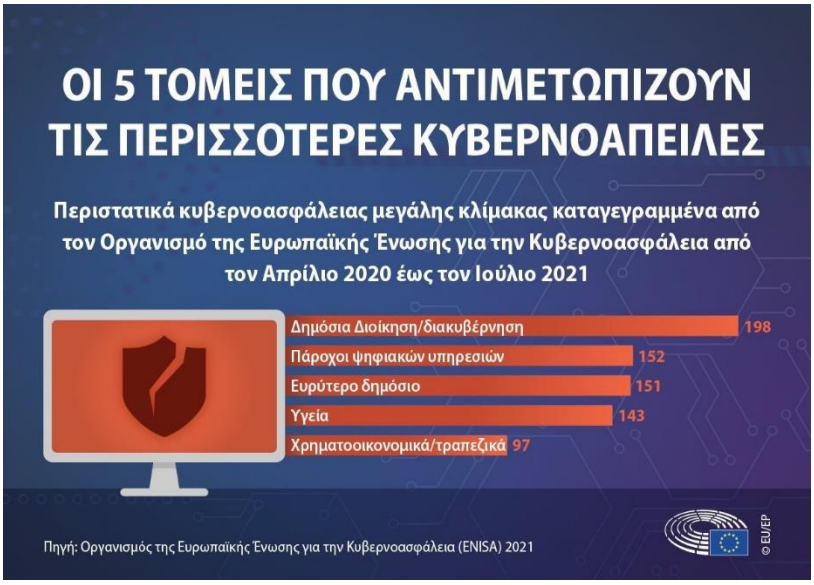
Εικόνα 4-1 Πέντε στρατηγικοί στόχοι ανάπτυξης του στρατηγικού σχεδιασμού [23]

Τους στόχους αυτούς πλαισιώνουν 15 ειδικοί στόχοι και πάνω από 50 δραστηριότητες. Αυτές περιλαμβάνουν την θωράκιση της κυβερνοασφάλειας στους δημόσιους φορείς, τα πλαίσια για την προώθηση της καλής κυβερνοασφάλειας, τα σχέδια αξιολόγησης των κινδύνων, μέτρα για τις προκλήσεις των νέων τεχνολογιών, λύσεις πρόληψης και αντιμετώπισης κακόβουλων ενεργειών, κίνητρα για επενδύσεις στην κυβερνοασφάλεια, δημιουργία δικτύου συνεργασίας σε ευρωπαϊκό και διεθνές επίπεδο, ενίσχυση των απαιτήσεων ασφαλείας, συστήματα πρόληψης και αντιμετώπισης των ουκ ολίγων πολυσύνθετων απειλών του σήμερα, ενδυνάμωση επιχειρησιακής συνεργασίας σε θέματα ασφάλειας, καθώς και ολοκληρωμένο πλαίσιο ανάπτυξης ικανοτήτων και ευαισθητοποίησης. [18]

Η πρωτοβουλία της ενίσχυσης της ψηφιακής ακολουθεί μια σειρά ενεργειών του Υπουργείου Ψηφιακής Διακυβέρνησης για την αποτροπή των πασης φύσεως διανοητικών εισβολέων. Η αναβάθμιση της Εθνικής Αρχής Κυβερνοασφάλειας σε Γενική Διεύθυνση του Υπουργείου Ψηφιακής Διακυβέρνησης, η ακριβής έννοια του όρου κρίσιμες υποδομές, το πλαίσιο υποχρεώσεών των κρίσιμων υποδομών, η έναρξη της εκπαίδευσης σε θέματα ετοιμότητας, η χρήση προηγμένων συστημάτων για την πρόληψης και την αντιμετώπισης των επιθέσεων στον κυβερνοχώρο, είναι κάποιες από τις πρωτοβουλίες που αναλαμβάνει το Εθνικού Σχέδιο. [21]

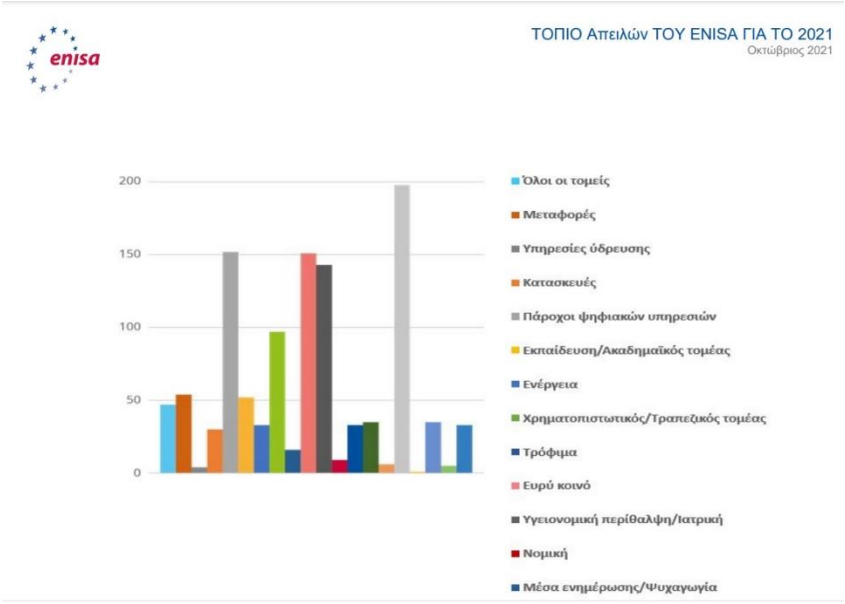
4.2 Δημόσια Διοίκηση, ο τομέας που επλήγη Περισσότερο στην ΕΕ

Η μία έρευνα που διενεργήθηκε από τον ENISA, τον Απρίλιο του 2020 έως το Ιούλιο του 2021, [8] ανέδειξε ότι την περίοδο αυτή μεγάλο αριθμό παραβιάσεων είχαν ως στόχο πέντε σημαντικούς τομείς του κράτους. Η δημόσια διοίκηση/διακυβέρνηση (198 παραβιάσεις), οι πάροχοι ψηφιακών υπηρεσιών (152 παραβιάσεις), το ευρύτερο δημόσιο (151 παραβιάσεις), η υγεία (143 παραβιάσεις) και ο χρηματοοικονομικός/τραπεζικός τομέας (97 παραβιάσεις). Για τους παρόχους ψηφιακών υπηρεσιών αυτό ήταν φυσικό επακόλουθο μιας και η φύση των υπηρεσιών που παρέχουν είναι νούμερο ένα στόχος των παραβιάσεων Εικόνα 4-2



Εικόνα 4-2 Στοχευμένοι τομείς ανά αριθμό περιστατικών (Απρίλιος 20-Ιούλιος 21) [8]

Σε μια άλλη έρευνα που πραγματοποιήθηκε από τον ENISA, (Εικόνα 4-3) παρατηρήσαμε επίσης μεγάλο αριθμό παραβιάσεων είχαν ως στόχο το ευρύ κοινό και όχι απαραίτητα κάποιον τομέα, γεγονός που αναδεικνύει το τοπίο των απειλών δεν διακρείνει τομείς και τελικούς χρήστες. Ο τομέα της υγείας είχε και αυτός να αντιμετωπίσει ένα μεγάλο αριθμό κυβερνοεπιθέσεων κατά την περίοδο της έρευνας και μάλιστα να παρουσιάζει αυξητική τάση κατά τους τελευταίους μήνες της περιόδου αναφοράς. Η αλυσίδα εφοδιασμού λογισμικού είδε επίσης αύξηση του αριθμού των περιστατικών σε αντίθεση με τον τράπεζες που αντιμετώπισαν σταθερό αριθμό περιστατικών καθ' όλη τη διάρκεια του έτους. [8]



Εικόνα 4-3 Στοχευμένοι τομείς ανά αριθμό περιστατικών (Απρίλιος 20-Ιούλιος 21) [8]

5

Η εφαρμογή της οδηγίας NIS στην Ελλάδα

5.1 Κοινοτική Οδηγία NIS για την Κυβερνοασφάλεια

Η Ευρωπαϊκή Ένωση το 2013 ενέκρινε την στρατηγική για την κυβερνοθωράκιση που είχε ως στόχο να βελτιστοποιήσει νομοθετικά την κατάσταση προγραμματίζοντας μια σειρά ενεργειών με απώτερο σκοπό να ενισχύσει την ανθεκτικότητα του κυβερνοχώρου και να κατοχυρώσει την αξιοπιστία των ψηφιακών υπηρεσιών για τους πολίτες. Ο πρωταρχικός στόχος ήταν ο ψηφιακός μετασχηματισμός της κοινωνίας εντός της ΕΕ και η ανάπτυξη της αντίληψης της ασφάλειας για το κοινό καλό όχι μόνο των πολιτών, αλλά και των καταναλωτών, των επιχειρήσεων και των δημοσίων οργανισμών της Ευρωπαϊκής Ένωσης, [25]. Ο στόχος αυτός τον Μάρτιο του 2004 γέννησε τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών (εφεξής ENISA), ο οποίος αναδείχθηκε τα επόμενα χρόνια ένα πολύτιμο εργαλείο στον τομέα της κυβερνοασφάλειας. Ακολούθησε πληθώρα ανακοινώσεων και δράσεων στο πλαίσιο της γενικής διαπίστωσης ότι οι Τ.Π.Ε. είναι ευάλωτες σε επιβουλές που δεν έχουν εθνικά σύνορα, οι οποίες οδήγησαν την 6η Ιουλίου του 2016 στην οδηγία NIS. Η οδηγία, πλέον του προφανούς στόχου για ανάπτυξη των ικανοτήτων της κυβερνοασφάλειας της Ένωσης έναντι των απειλών σε δικτυακά και πληροφοριακά συστήματα των υποδομών, έθεσε ως ζητούμενο τη συνέχεια των παρεχόμενων υπηρεσιών κυβερνοασφάλειας, ώστε να δημιουργείται ασφαλές οικονομικό και επιχειρηματικό περιβάλλον, το οποίο είναι αλληλένδετο με την οικονομική ευημερία

Υπό το πρίσμα των ανωτέρω, της διαφύλαξης υψηλού επιπέδου κυβερνοασφάλειας και μιας ολιστικής στρατηγικής προσέγγισης η ΕΕ το 2016 εξέδωσε την οδηγία 2016/1148/ΕΚ ευρέως γνωστή ως NIS (από τα αρχικά «Network and Information Systems») η οποία αποτέλεσε την πρώτη συγκροτημένη ευρωπαϊκή προσπάθεια θεσμοθέτησης κανόνων για την κυβερνοασφάλεια, με ρητές υποχρεώσεις για τα κράτη μέλη. Η οδηγία NIS, στην πενταετή πορεία της, αποδείχθηκε επιτυχημένη, καθώς υπήρξε ο οδηγός ευαισθητοποίησης των κρατών

μελών της Ευρωπαϊκής Ένωσης σε ότι αφορά την προστασία των κρίσιμων υποδομών από κυβερνοεπιθέσεις. Τα κύρια οφέλη της υλοποίησης της οδηγίας εδράζονται στην αλλαγή νοοτροπίας, στην ολοκλήρωση της υλοποίησης των εθνικών νομοθετικών πλαισίων που συνιστούν προαπαιτούμενο για το επόμενο βήμα και στην προώθηση της συνεργασίας μεταξύ των κρατών τόσο της Ευρωπαϊκής Ένωσης, όσο και εκτός αυτής. [26] Η υλοποίηση της οδηγίας δεν αποτέλεσε εύκολο στόχο, η εγχείρημα δίχως προβλήματα. Σε πολλές περιπτώσεις καταγράφηκαν δυσλειτουργίες, αδικαιολόγητες καθυστερήσεις και σημαντικές διαφοροποιήσεις αντιμετώπισης των ίδιων παραμέτρων, επειδή τούτο ήταν επιτρεπτό από το νομικό πλαίσιο που έθετε η Οδηγία NIS. Όμως η κυβερνοασφάλεια των κρίσιμων υποδομών, ως μείζον θέμα ασφάλειας δεν θα μπορούσε να ιδωθεί με στατική ματιά, ειδικότερα σε ένα ταχέως διαδικτυακά αναπτυσσόμενο περιβάλλον, όπου ο ψηφιακός μετασχηματισμός και η διασύνδεση της κοινωνίας μέσω των διασυνοριακών συναλλαγών αποτελούν καθοριστικό στοιχείο της καθημερινής ζωής [26].

Σύμφωνα με την οδηγία 2008/114/ΕΚ του Συμβουλίου της Ευρωπαϊκής Ένωσης, ως υποδομή ζωτικής σημασίας (που αναφέρεται επίσης ως κρίσιμη υποδομή) νοείται κάθε περιουσιακό στοιχείο, σύστημα ή μέρος αυτού που είναι ουσιώδες για τη διατήρηση των βασικών λειτουργιών της κοινωνίας της υγείας, της ασφάλειας, της προστασίας, της οικονομίας και της κοινωνικής ευημερίας των μελών της και του οποίου η διατάραξη ή η καταστροφή θα εμπόδιζε τη συνέχιση των λειτουργιών αυτών, με σημαντικές εθνικές συνέπειες.

Έτσι προέκυψαν δύο ξεκάθαρες ανάγκες που η Οδηγία NIS ήταν αδύνατο να καλύψει: (α)η επιβεβλημένη θέσπιση μηχανισμών που να απαγορεύουν στις μεγάλες αποκλείσεις στο χειρισμό του θέματος ανάμεσα στα κράτη μέλη και (β)η ορθή θεώρηση των τομέων που καλύπτει η οδηγία, ώστε να μην είναι παρωχημένες και να καλύπτουν ολοκληρωμένα και δίκαια τους τομείς και τις υπηρεσίες ζωτικής σημασίας.

Έχοντας ως πρωταρχικό σκοπό την προετοιμασία τη ΕΕ στην νέα ψηφιακή εποχή, η Επιτροπή πρότεινε τον Δεκέμβριο του 2020 την αναθεώρηση της οδηγίας NIS 2. Η μετάβαση από την Οδηγία NIS, η οποία έχει επιτελέσει ήδη σε ικανοποιητικό βαθμό τον σκοπό της, στην αναθεώρηση αυτής (εφεξής Οδηγία NIS2) φιλοδοξεί πλέον να διασφαλίσει ένα υψηλό επίπεδο κυβερνοασφάλειας σε ολόκληρη της Ευρωπαϊκή ζώνη και να εγκαθιδρύσει την ανθεκτικότητα των κρίσιμων υποδομών.

5.2 Αναθεωρημένη κοινοτική οδηγία NIS 2

Τον Δεκέμβριο του 2020 παρουσιάσθηκε η νέα στρατηγική της ΕΕ για την κυβερνοασφάλεια. Η μετάβαση από την Οδηγία NIS, η οποία έχει επιτελέσει ήδη σε ικανοποιητικό βαθμό τον σκοπό της, στην αναθεώρηση αυτής (εφεξής Οδηγία NIS2) φιλοδοξεί πλέον να διασφαλίσει ένα υψηλό επίπεδο κυβερνοασφάλειας σε ολόκληρη της Ευρώπη και να εγκαθιδρύσει την

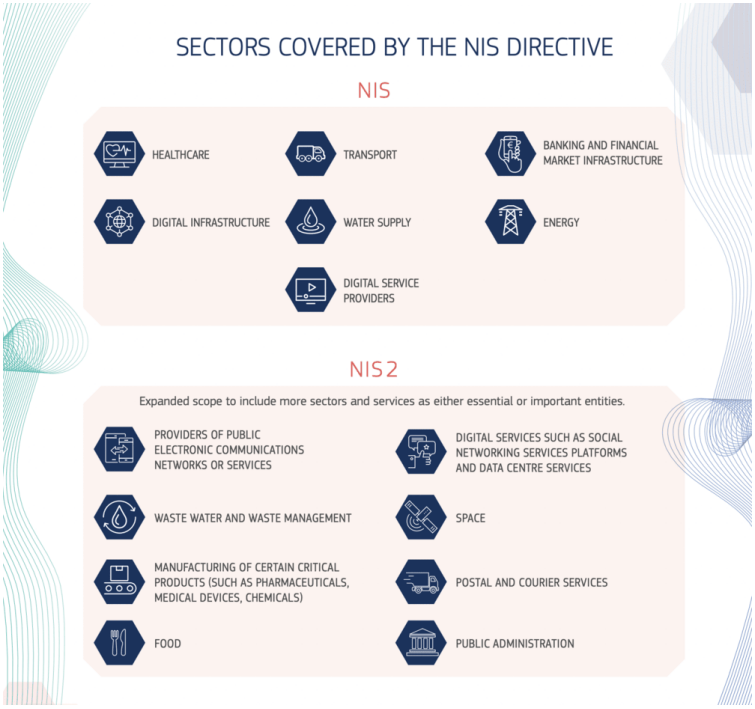
ανθεκτικότητα των κρίσιμων υποδομών. Η Οδηγία NIS2 που ισχύει από τις 16 Ιανουαρίου 2023 καλύπτει τρεις βασικούς τομείς

α) Την ανθεκτικότητα, τεχνολογική κυριαρχία και ηγετική θέση.

β) Την ανάπτυξη της επιχειρησιακής ικανότητας στην πρόληψη, αποτροπή και αντιμετώπιση κυβερνοεπιθέσεων.

γ) Την προώθηση ενός παγκόσμιου και ανοικτού κυβερνοχώρου μέσω αυξημένης συνεργασίας.

Συγκεκριμένα η οδηγία NIS, καλύπτει επτά (7) διακριτές οντότητες (Εικόνα 5-1) που έχουν χαρακτηριστεί ως κρίσιμες υποδομές:



Εικόνα 5 1 Από την επίσημη ιστοσελίδα του Ευρωπαϊκού Συμβουλίου [27]

1. Ενέργεια
2. Μέσα Μαζικής Μεταφοράς
3. Χρηματοπιστωτικά Ιδρύματα
4. Υποδομές χρηματοπιστωτικών αγορών
5. Υγειονομικός κλάδος
6. Προμήθεια και διανομή πόσιμου νερού
7. Ψηφιακή υποδομή

Παράλληλα, συμπεριλαμβάνει στην ασπίδα προστασίας και νομικής υπαγωγής στο καθεστώς κυβερνοασφάλειας και τις ακόλουθες υπηρεσίες: (α)Επιγραμμική αγορά, (β)Επιγραμμική μηχανή αναζήτησης και (γ)Υπηρεσία νεφοϋπολογιστικής.

Η αναθεωρημένη οδηγία NIS2, αναφέρεται σε δημόσιες ή ιδιωτική οντότητες είδους που διακρίνονται σε:

(Α)Βασικές,

(Β)Σημαντικές και

(Γ)Με συγκεκριμένα χαρακτηριστικά.

Συγκεκριμένα:

(Α)Βασικές Οντότητες

Α.1. Ενέργειας, στην οποία εντάσσονται η ηλεκτρική ενέργεια, υπηρεσίες τηλεθέρμανσης και τηλεψήξης, το πετρέλαιο, το αέριο και το υδρογόνο.

Α.2. Οι μεταφορές, οι οποίες εξειδικεύονται σε εναέριες, σιδηροδρομικές, πλωτές και οδικές.

Α.3. Τράπεζες

Α.4. Υποδομές χρηματοπιστωτικών αγορών

Α.5. Υγεία

Α.6. Πόσιμο νερό

Α.7. Λύματα

Α.8. Ψηφιακές υποδομές, όπου εντάσσονται πλέον οι πάροχοι σημείων ανταλλαγής κίνησης, οι πάροχοι υπηρεσιών συστήματος ονομάτων τομέα (DNS), τα μητρώα ονομάτων τομέα ανωτάτου επιπέδου (TLD), οι πάροχοι νεφοϋπολογιστικής, οι πάροχοι υπηρεσιών κέντρου δεδομένων, οι πάροχοι υπηρεσιών εμπιστοσύνης (Άρθρο 3 σημείο 19 του κανονισμού (ΕΕ) 910/2014) οι πάροχοι δημοσίων δικτύων ηλεκτρονικών επικοινωνιών (Άρθρο 2 σημείο 8 της οδηγίας (ΕΕ) 2018/1972) ή οι πάροχοι υπηρεσιών ηλεκτρονικών επικοινωνιών (Άρθρο 2 σημείο 4 της οδηγίας (ΕΕ) 2018/1972) όταν οι υπηρεσίες τους είναι δημοσίως διαθέσιμες.

Α.9. Δημόσια διοίκηση

Α.10. Διάστημα

(Β)Σημαντικές Οντότητες

Β.1. Ταχυδρομικές υπηρεσίες και υπηρεσίες ταχυμεταφορών

Β.2. Διαχείριση αποβλήτων

Β.3. Παρασκευή, παραγωγή και διανομή χημικών προϊόντων

Β.4. Παραγωγή, μεταποίηση και διανομή τροφίμων

Β.5. Κατασκευαστικός τομέας που εξειδικεύεται σε ιατροτεχνολογικά προϊόντα, διαγνωστικά ιατροτεχνολογικά διαγνωστικά ιατροτεχνολογικά προϊόντα, προϊόντα υπολογιστών, ηλεκτρονικών οπτικών προϊόντνων, προϊόντων κατασκευής ηλεκτρολογικού εξοπλισμού, μηχανημάτων και εξοπλισμού μεταφορών, μηχανοκίνητων οχημάτων, ρυμουλκούμενων και ημιρυμουλκούμενων, κ.α.λ.

Β.6. Ψηφιακοί πάροχοι, ήτοι πάροχοι επιγραμμικών αγορών, επιγραμμικών μηχανών αναζήτησης, πλατφόρμας υπηρεσιών κοινωνικής δικτύωσης.

(Γ)Οντότητες με συγκεκριμένα χαρακτηριστικά

Γ.1.Δημόσια δίκτυα ηλεκτρονικών υπηρεσιών ή διαθέσιμες στο κοινό υπηρεσίες ηλεκτρονικών επικοινωνιών

Γ.2. Παρόχους υπηρεσιών εμπιστοσύνης

Γ.3. Παρόχους μητρώων ονομάτων τομέα ανώτατου επιπέδου και παρόχους υπηρεσιών του συστήματος ονομάτων τομέα (DNS)

Γ.4. Φορείς δημόσιας διοίκησης

Γ.5. Οντότητα που αποτελεί το μοναδικό πάροχο υπηρεσίας σε κράτος μέλος.

Γ.6. Κάθε οντότητα για την οποία η διατάραξη της υπηρεσίας που προσφέρει θα μπορούσε να έχει επιπτώσεις στη δημόσια ασφάλεια, στη δημόσια προστασία, ή στη δημόσια υγεία, καθώς επίσης και τυχόν συστημικούς κινδύνους με διασυνοριακό αντίκτυπο

Γ.7. Η οντότητα χαρακτηρίζεται κρίσιμη σύμφωνα με την οδηγία του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου.

Επισημαίνεται, ότι οι πάροχοι των στοιχείων Γ.1 έως και Γ.3 εντάσσονται ακόμη και εάν αφορούν σε πολύ μικρές ή μικρές επιχειρήσεις κατά την έννοια της οδηγίας 2003/361/ΕΚ της Επιτροπής και ότι υφίσταται η υποχρέωση από τα κράτη μέλη να καταρτίσουν καταλόγους οντοτήτων μόνο για την τρίτη κατηγορία.

5.3 Όργανα υλοποίησης

Σημαντικό στοιχείο της οδηγίας είναι η υιοθέτηση λεξικού κρίσιμων όρων που αφορούν την κυβερνοασφάλεια. Έννοιες και όροι όπως: «δικτυακά πληροφοριακά συστήματα», «ασφάλεια δικτυακών και πληροφοριακών συστημάτων», «εθνική στρατηγική κυβερνοασφάλειας», «περιστατικό», «χειρισμός περιστατικού», «κυβερνοαπειλή», «τρωτό σημείο», «πρότυπο», «τεχνική προδιαγραφή», «πάροχος», «IXP, DNS, TLD», «φορείς» και «οντότητες» έχουν πλέον την ίδια σημασία για όλα τις χώρες μέλη της ΕΕ, την υποχρέωση να εντάξουν την συγκεκριμένη ορολογία στην εθνική τους νομοθεσία.

Παράλληλα, οριοθετήθηκε με σαφήνεια η εθνική στρατηγική κυβερνοασφάλειας, η οποία περιλαμβάνει συγκεκριμένες υποχρεώσεις αναφορικά με τους στόχους, τις προτεραιότητες, την ετοιμότητα και όλα τα επί μέρους θέματα με ξεχωριστό αυτό του ορισμού συγκεκριμένων αρχών και φορέων που επωμίζονται την υλοποίηση. Οι αρχές αυτές αναλαμβάνουν συγκεκριμένες δεσμεύσεις υλοποίησης και εποπτικά καθήκοντα τήρησης των υποχρεώσεων.

Το παράδειγμα της Ελλάδας είναι χαρακτηριστικό της σημασίας δημιουργίας των Οργάνων που προβλέπονται από την Οδηγία NIS2. Η Εθνική Αρχή Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης η οποία αποτελεί την επισπεύδουσα υπηρεσία, προέβη στην επικαιροποίηση του πενταετούς εθνικού σχεδιασμού της Εθνικής Στρατηγικής Κυβερνοασφάλειας 2020- 2025 για τη χώρα μας. Ξεχωρίζουν:

α) Γενική Διεύθυνση Κυβερνοασφάλειας – Εθνική Αρχή Κυβερνοασφάλειας (National Cybersecurity Authority).

β) Εθνική αρχή αντιμετώπισης ηλεκτρονικών επιθέσεων (Εθνικό CERT), η οποία εντάχθηκε στο οργανόγραμμα της Εθνικής Υπηρεσίας Πληροφοριών (Ε.Υ.Π.). Σ` αυτήν εντάσσονται:

β.1 Εθνική Αρχή INFOSEC, για τεχνικής φύσεως θέματα ασφάλειας εθνικών επικοινωνιών συστημάτων τεχνολογίας πληροφοριών

β.2 Εθνική Αρχή CRYPTO, για την αξιολόγηση και πιστοποίηση κρυπτοσυστημάτων και την υποστήριξη των Ενόπλων Δυνάμεων και των υπηρεσιών του δημοσίου σε θέματα κρυπτασφάλειας

β.3 Εθνική Αρχή TEMPEST, για την εξασφάλιση εθνικών ηλεκτρονικών συσκευών τηλεπικοινωνιών από διαρροές

γ) Δίωξη Ηλεκτρονικού Εγκλήματος της Ελληνικής Αστυνομίας, για την πρόληψη, έρευνα και καταστολή των διαδικτυακών εγκλημάτων.

δ) Αρχή προστασίας δεδομένων προσωπικού χαρακτήρα, αρμόδια για τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR),

ε) Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.), η εποπτεύουσα αρχή των ηλεκτρονικών επικοινωνιών που δραστηριοποιούνται οι εταιρείες κινητής και σταθερής τηλεφωνίας, καθώς και την ταχυδρομική αγορά

στ) Αρχή Διασφάλισης Απορρήτου Επικοινωνιών (Α.Δ.Α.Ε.), που είναι αρμόδια εκτός των άλλων για την ασφάλεια των δικτύων και πληροφοριών.

ζ) Κέντρο Παρακολούθησης Κρίσιμων Υποδομών (Security Operation Center - SOC), το οποίο έχει ως στόχο την διαρκή παρακολούθηση κρίσιμων υποδομών και φορέων, της διαδικτυακής κίνησης αυτών για την έγκαιρη αναγνώριση συμβάντων και την ορθή διαχείριση αυτών, με βασικά εργαλεία:

ζ.1 Security Information and Event Management (SIEM), για τη συγκέντρωση στοιχείων και συσχετισμό αυτών

ζ.2 Security Orchestration, Automation and Response (SOAR), για την απόκριση σε συμβάντα με εφαρμογή ή αλλαγή κανόνων

ζ.3 Case Management, για τη διαχειριστική κάλυψη ενός SOC.

ζ.4 Cyber Hotline, για τη δημιουργία των απαραίτητων διεπαφών με φορείς και αρχές.

ζ.5 Threat Intelligence, για τη δημιουργία μητρώου συμβάντων.

5.4 Οι νέες προσθήκες της πρότασης NIS2

Οι ολοένα και περισσότερες παράνομες δραστηριότητες στον κυβερνοχώρο έχουν εντείνει το τοπίο απειλών και έχουν εισαγάγει νέες προκλήσεις στο πλαίσιο του ήδη εξελισσόμενου ψηφιακού μετασχηματισμού της ευρωπαϊκής κοινωνίας. Οι διακοπές παροχής υπηρεσιών σε έναν τομέα υπηρεσιών μπορεί να προκαλέσουν διαδοχικές επιπτώσεις σε άλλους τομείς και να επηρεάσουν σημαντικά τις ευρωπαϊκές αγορές.

Στις 6 Δεκεμβρίου 2020, η Επιτροπή της ΕΕ δημοσίευσε την αναθεωρημένη πρόταση της NIS Οδηγίας για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών. Η πρόταση που είναι γνωστή ως Οδηγία NIS2 μαζί με την προκάτοχό της, αποτέλεσε ένα ζευγάρι των ρυθμιστικών πρωτοβουλιών που εισήγαγε η Στρατηγική Κυβερνοασφάλειας της ΕΕ για την Ψηφιακή Δεκαετία.

Η νέα πρόταση NIS2 επικεντρώνεται στην προσαρμογή της υφιστάμενης Οδηγίας NIS στις νέες ανάγκες που προέκυψαν με σκοπό να την καταστήσει ικανή να προσαρμοστεί στις μελλοντικές καταστάσεις των ψηφιακών κοινωνιών. Ο παρακάτω πίνακας δείχνει τις νέες προσθήκες της πρότασης NIS2 στους βασικούς τομείς της οδηγίας: [24]

Πίνακας 5-1 Νέες προσθήκες της NIS2 [24]

Οδηγία NIS	Οδηγία NIS2
ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ	
Βασικός κατάλογος κρίσιμων υποδομών	Διευρυμένο πεδίο εφαρμογής με νέους τομείς που βασίζονται στην κρισιμότητα για την οικονομία και την κοινωνία
	Συμπερίληψη καθαρού ανώτατου ορίου μεγέθους: μεσαίες και μεγάλες εταιρείες σε επιλεγμένους τομείς θα συμπεριληφθούν στο πεδίο εφαρμογής
	Τα κράτη μέλη είναι ελεύθερα να προσδιορίζουν επιπλέον μικρότερες τομείς με τοπικό προφίλ υψηλού κινδύνου ασφάλειας

ΤΑΞΙΝΟΜΗΣΗ	
Χειριστές Βασικών Υπηρεσιών & Παρόχων Ψηφιακών Υπηρεσιών	Η προηγούμενη διάκριση καταργείται. Οι οντότητες ταξινομούνται με βάση τη σημασία τους και χωρίζονται αντίστοιχα σε τρεις κατηγορίες: βασικές, σημαντικές και με συγκεκριμένα χαρακτηριστικά
ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΤΙΣ ΕΤΑΙΡΙΕΣ	
Ουσιαστικές απαιτήσεις και πρακτικές κυβερνοασφάλειας σχετικά με τη διαχείριση κινδύνου, τη διαχείριση συμβάντων και την αναφορά, τις πολιτικές, τους ρόλους και τις ευθύνες	Η προσέγγιση διαχείρισης κινδύνου παρέχει έναν ελάχιστο κατάλογο βασικών στοιχείων ασφαλείας που πρέπει να εφαρμοστούν
	Ακριβέστερες διατάξεις σχετικά με τη διαδικασία αναφοράς περιστατικών, το περιεχόμενο των αναφορών και τα χρονοδιαγράμματα
ΑΣΦΑΛΕΙΑ ΕΦΟΔΙΑΣΤΙΚΗΣ ΑΛΥΣΙΔΑΣ	
Ουσιαστική διαχείριση ασφάλειας της εφοδιαστικής αλυσίδας βασισμένη σε SLA & risk management	Μεμονωμένες εταιρείες να ορίσουν τα πλαίσια αντιμετώπισης κινδύνων κυβερνοασφάλειας στις αλυσίδες εφοδιασμού και τις σχέσεις προμηθευτών
ΕΠΟΠΤΙΚΕΣ ΕΘΝΙΚΕΣ ΑΡΧΕΣ	
Εκ των προτέρων εποπτεία σε κρίσιμους τομείς και εκ των υστέρων εποπτεία για κρίσιμους παρόχους ψηφιακών υπηρεσιών	Αυστηρότερα εποπτικά μέτρα
	Διαφορετικά εποπτικά καθεστώτα ανά ταξινόμηση
	Αυστηρότερες απαιτήσεις επιβολής
ΔΙΚΤΥΟ ΣΥΝΕΡΓΑΣΙΑΣ	
Στρατηγική καθοδήγηση για τις δραστηριότητες του δικτύου CSIRTs	Ενδυναμωμένος ρόλος στη διαμόρφωση στρατηγικών αποφάσεων πολιτικής για τις αναδυόμενες τεχνολογίες και ενισχύεται η ανταλλαγή πληροφοριών και η συνεργασία μεταξύ των αρχών των κρατών μελών
Δημοσίευση μη δεσμευτικών κατευθυντήριων γραμμών για τα κράτη μέλη της ΕΕ που επαναπροσδιορίζουν την εφαρμογή της NISD	Βασικό πλαίσιο με υπεύθυνους βασικούς παράγοντες για τη συντονισμένη αποκάλυψη τρωτών σημείων για τρωτά σημεία που ανακαλύφθηκαν πρόσφατα σε ολόκληρη την ΕΕ
	Δημιουργία μητρώου ΕΕ με βάση τις παραπάνω πληροφορίες που διαχειρίζεται ο ENISA

5.5 Ο ρόλος των CSIRTs

Ξεχωριστή θέση στους Οργανισμούς που προβλέπονται από την οδηγία κατέχουν οι Ομάδες αντιμετώπισης περιστατικών ασφαλείας σε υπολογιστές (εφεξής CSIRT). Κάθε χώρα της ΕΕ θα πρέπει να ορίσει μία ή περισσότερες CSIRT και διασφαλίζει τις προϋποθέσεις ορθής λειτουργίας τους. Ενδεικτικό της σπουδαιότητας λειτουργίας τους είναι το γεγονός ότι υφίσταται πρόβλεψη για συνδρομή από τον ENISA σε κράτη μέλη για τη δημιουργία των CSIRT`s, σε περίπτωση αδυναμίας.

Οι Ομάδες αντιμετώπισης περιστατικών ασφαλείας παρακολουθούν τις κυβερνοαπειλές, τα τρωτά σημεία και τα περιστατικά σε εθνικό επίπεδο ώστε να είναι σε θέση να παρέχουν έγκαιρα ειδοποιήσεις επαγρύπνησης και ετοιμότητας στις βασικές και στις σημαντικές οντότητες.

Παρέχει δυναμική ανάλυση απειλών και συμβάντων και προληπτική σάρωση κατόπιν αιτήματος για τα δίκτυα και τα συστήματα πληροφοριών που χρησιμοποιούν οι οντότητες για την παροχή των υπηρεσιών τους. Σε κάθε περίπτωση συμμετέχουν στο δίκτυο CSIRT για τη διασφάλιση αμοιβαίας συνδρομής και συνεργασίας με σκοπό την καλύτερη επίτευξη των στόχων της οδηγίας.

Στο πλαίσιο της ορθολογιστικής λειτουργίας τους τυποποιεί τις πρακτικές συντονισμού για: (α)τη διαδικασία χειρισμού περιστατικών, (β)τη διαχείριση κρίσεων στον τομέα της ασφάλειας στον κυβερνοχώρο και (γ)την κοινοποίησης ευπαθειών .

Στη Χώρα μας υπάρχουν συνολικά έξι τέτοιες ομάδες, μια εκ των οποίων αποτελεί τον επίσημο κρατικό φορέα που ως αναφέρθηκε εντάχθηκε στο Υπουργείο Άμυνας. [25]

5.6 Εθνικό Κέντρο Κυβερνοασφάλειας (Security Operation Center – SOC)

Υπό το πρίσμα της δημιουργίας μια αποτελεσματικής "γραμμής άμυνας" του ελληνικού Δημοσίου κατά των ψηφιακών απειλών, αναμένεται μέσα στο 2023 να δημιουργηθεί το Εθνικό Κέντρο Επιχειρήσεων Κυβερνοασφάλειας. Κύριος στόχος του έργου είναι η προστασία του ελληνικού πληθυσμού από επιθέσεις στον κυβερνοχώρο, με την αμέριστη υποστήριξη του ENISA. Μετά από πρόταση του υπουργείου Ψηφιακής Διακυβέρνησης στο Ταμείο Ανάκαμψης και Ανθεκτικότητας είναι σε εξέλιξη μια διαγωνιστική διαδικασία ύψους 35 εκατ. Ευρώ και θα αφορά όλο το ελληνικό Δημόσιο, εκτός του υπουργείου Εθνικής Άμυνας. Το έργο υπολογίζεται να δοθεί θα μεταφερθεί στα χέρια της ΕΥΠ στο τέλος του 2024.

Ο κύριος στόχος του Κέντρου Επιχειρήσεων Ασφαλείας (SOC) είναι να αποτελέσει μια εσωτερική ή εξωτερική ομάδα επαγγελματιών ασφάλειας πληροφορικής που θα παρακολουθεί ολόκληρη την υποδομή πληροφορικής επι εικοσιτετράωρου βάση, για να ανιχνεύει συμβάντα κυβερνοασφάλειας σε πραγματικό χρόνο και να τα αποτρέπει όσο το δυνατόν πιο γρήγορα και αποτελεσματικά κρατικές κυβερνοεπιθέσεις. Με αυτόν τον τρόπο θα παρακολουθεί και θα προστατεύει συνεχώς την περίμετρο των συστημάτων του δημοσίου και θα εντοπίζει εγκαίρως πιθανές απειλές και ύποπτες δραστηριότητες. Επιπλέον ένα SOC αναλύει συνεχώς τα δεδομένα απειλών ενός οργανισμού για να βρει τρόπους βελτίωσης της ασφάλειας του οργανισμού.

Παρέχει επίσης δυναμική ανάλυση κινδύνων για την προληπτική αντιμετώπιση ευπαθειών στα πληροφοριακά συστήματα τα οποία είναι υπό την επίβλεψή του.

Το εξιδεικευμένο προσωπικό των SOC θα παρέχει υπηρεσίες ανάλυσης δεδομένων για την αποτροπή κακόβουλης συμπεριφοράς και τον άμεσο εντοπισμό απειλών στον κυβερνοχώρο, ώστε να αποτραπεί η εξάπλωση κακόβουλων ενεργειών στην περίμετρο των συστημάτων του δημοσίου της χώρας.

Το κύριο όφελος από την ίδρυση των SOC θα είναι η ενοποίηση και ο συντονισμός όλων των εργαλείων ασφαλείας, των πρακτικών και την απόκριση ενός δημόσιου οργανισμού σε πιθανά συμβάντα ασφαλείας. θα παρέχονται οδηγίες για την με τον άμεσο τρόπο αντίδρασης σε απειλές και ύποπτες συμπεριφορές και θα κάνει υποδείξεις για την προστασία των πληροφοριακών συστημάτων από ενδεχόμενες κακόβουλες ενέργειες. Θα κάνει χρήση εξειδικευμένων εργαλείων για την παρακολούθηση των δικτύων και την ανίχνευση κακόβουλων συμβάντων σε αυτό.

Η εποπτεία αυτή θα υλοποιείται με την χρήση εργαλείων Συστημάτων Πληροφοριών Ασφάλειας και Διαχείρισης Περιστατικών (Security Information and Event Management - SIEM). Χρησιμοποιώντας νοημοσύνη απειλών και τεχνητή νοημοσύνη, αυτά τα εργαλεία θα βοηθούν τα SOC να ανιχνεύουν εξελισσόμενες απειλές, να επιταχύνουν την απόκριση σε περιστατικά και να παραμείνουν μπροστά από τους επιτιθέμενους.

Ένα ισχυρό SOC αποτελεί ένα αμυντικό «όπλο» των κυβερνήσεων και των οργανισμών μπροστά από ένα εξελισσόμενο τοπίο απειλών στον κυβερνοχώρο. Αυτό δεν είναι εύκολο έργο. Τόσο οι επιτιθέμενοι όσο και η αμυντική κοινότητα αναπτύσσουν συχνά νέες τεχνολογίες και στρατηγικές και χρειάζεται χρόνος και εστίαση για να ανταποκριθούν σε όλες αυτές τι αλλαγές που εξελίσσονται στην εποχή μας. Χρησιμοποιώντας την βάση γνώσεων που θα διαθέτει για το ευρύτερο περιβάλλον κυβερνοασφάλειας, ένα SOC θα βοηθήσει να αναπτυχθεί ένας οδικός χάρτης ασφάλειας που ευθυγραμμίζεται με τις μακροπρόθεσμες ανάγκες του κράτους.

5.7 Ο σκοπός των SOC

Ειδικότερα, τα SOC έχουν σχεδιαστεί για να ανιχνεύουν, να διερευνούν, να ανταποκρίνοται και να διαχειρίζονται περιστατικά ασφάλειας που συμβαίνουν στις δικτυακές υποδομές και υπηρεσίες των δημόσιων αρχών με συνεχή και έγκαιρο τρόπο 24 ώρες το 24ωρο. Μεταξύ άλλων δίνει έμφαση στις μελλοντικές απειλές, δεδομένων και των σύγχρονων γεωπολιτικών προκλήσεων στην Ευρώπη λόγο του πολέμου στην Ουκρανία.

Το Υπουργείο Ψηφιακής Διακυβέρνησης έχοντας αφουγκραστεί τις τελευταίες προκλήσεις, αποφάσισες την δημιουργία των Κυβερνητικών Κέντρων Επιχειρήσεων Κυβερνοασφάλειας (gSOC) τα οποία θα στελεχωθούν με πλήρως καταρτισμένους μηχανικούς ασφαλείας.

Επιπλέων θα δημιουργηθεί και η Εθνική αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (National Computer Emergency Response Team – nCERT) η οποία θα υποστηρίζει όλους τους φορείς Κεντρικής Κυβέρνησης δίνοντας οδηγίες και κατευθύνσεις με σκοπό την πρόληψη, την έγκαιρη προειδοποίηση σε περίπτωση κυβερνοεπιθέσεων [26]

Επίσης θα δημιουργηθούν μικρό-Κέντρα Επιχειρήσεων Κυβερνοασφάλειας (Mini-SOC) κεντρικά καθοδηγούμενα από το gSOC που θα υποστηρίζουν Κυβερνητικούς Οργανισμούς, και να επιβάλλει την πολιτική ασφάλειας του nCERT.

Τέλος, η Εθνική Ομάδα Αντιμετώπισης Επιθέσεων στον Κυβερνοχώρο (nCERT) θα διασυνδεθεί επιχειρησιακά με τις αντίστοιχες εθνικές αρχές άλλων χωρών κρατών μελών για την έγκαιρη προειδοποίηση για απειλές στον κυβερνοχώρο.

5.8 Ισχυρότερη διαχείριση κινδύνων και συμβάντων και ισχυρότερη συνεργασία

Η NIS2 είχε ως πρωταρχικό στόχο την εδραίωση της βασικής αρχής για τον καθορισμό μέτρων για την ορθολογιστική διαχείριση των κινδύνων και υποχρεώσεων αναφοράς περιστατικών σε όλους τους καλυπτόμενους τομείς, συμπεριλαμβανομένων της ενέργειας, των μεταφορών, της υγείας και των ψηφιακών υποδομών. Η αναθεωρημένη οδηγία NIS2, στοχεύει στην θωράκιση των οικονομικών δεδομένων – δεδομένων που επηρεάζουν την οικονομία και τον ψηφιακό μετασχηματισμό της κοινωνίας. Υπέρτατη αρχή της είναι ο ακριβής ορισμός, χωρίς αποκλείσεις, των απαιτήσεων ασφαλείας και στην λήψη μέτρων στην περίπτωση κυβερνοαπειλών. Έτσι με γνώμονα την ανωτέρα απαίτηση, διατυπώνει συγκεκριμένες προτάσεις σχετικά με το κανονιστικό πλαίσιο και ενισχύει τους μηχανισμούς για την ενίσχυση της συνεργασίας μεταξύ των αρμόδιων αρχών σε κάθε κράτος μέλος της ΕΕ. Καθορίζει με

ακρίβεια τους εμπλεκόμενους τομείς που έχουν υποχρεώσεις στον τομέα της ασφάλειας στον κυβερνοχώρο, προβλέπει δε λύσεις και κυρώσεις για τη διασφάλιση της συμμόρφωσης. Παράλληλα, φιλοδοξεί να δημιουργήσει προοπτική συμπερίληψης των επερχόμενων τεχνολογικών αλμάτων, θεσπίζοντας εκτός των άλλων και ένα πλαίσιο διαρκούς επικαιροποίησης. Και στην περίπτωση της οδηγίας NIS2 θα δοθεί διετής προθεσμία στα κράτη μέλη να εντάξουν τις προβλέψεις στην εθνική τους νομοθεσία. [27]

Η NIS2 θεσπίζεται επίσημα ένα ευρωπαϊκό δίκτυο διασύνδεσης σε θέματα κρίσεων στον κυβερνοχώρο, το EU-CyCLONE, για να βοηθήσει στη αντιμετώπιση μεγάλων κρίσεων στον κυβερνοχώρο σε όλη την Ευρώπη και να αυξήσει την ανταλλαγή πληροφοριών και τη συνεργασία μεταξύ των κρατών μελών.

5.9 Μέτρα και οι οδηγίες διαχείρισης κινδύνων για τους υπόχρεους της NIS 2

Η NIS2 καθιερώνει νέες απαιτήσεις για της εμπλεκόμενου φορείς. Απαιτήσεις που αφορούν την υιοθέτηση καλών πρακτικών για την εξειδίκευση και ευθύνη της διοίκησης, την δραστική διαχείριση των τρωτών σημείων των πολιτικών ασφαλείας τους, διασφαλίζοντας:

(α) τα κράτη μέλη, επιβάλλεται να είναι κατάλληλα εξοπλισμένα με μια Ομάδα Αντιμετώπισης Συμβάντων Ασφάλειας Υπολογιστών (CSIRT) και μια αρμόδια NIS εθνική αρχή,

(β) όλα τα κράτη μέλη της ΕΕ θα πρέπει να έχουν μια συνεργασία στα πλαίσια ανταλλαγή γνώσεων και εμπειριών όσον αφορά την κοινοποίηση περιστατικών.

(γ) μια κουλτούρα ασφάλειας σε όλους τους ζωτικής σημασίας τομείς για την οικονομία και την κοινωνία μας και που στηρίζονται σε μεγάλο βαθμό στις ΤΠΕ.

Όπως περιγράφεται στο άρθρο 21 «Μέτρα διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας» της ευρωπαϊκής οδηγίας 2022/2555 [28], τα μέτρα για την ενίσχυση του συνολικού επιπέδου ασφάλειας στον κυβερνοχώρο στην ΕΕ βασίζονται σε μία ολιστική προσέγγιση του κινδύνου, που αποσκοπεί στην προστασία των συστημάτων δικτύου και πληροφοριών και του φυσικού περιβάλλοντος των εν λόγω συστημάτων από περιστατικά. Τα μέτρα αυτά περιλαμβάνουν:

(α) πολιτικές ασφαλείας για την ανάλυση κινδύνου πληροφοριακών συστημάτων

(β) βελτιστοποίηση διαχείρισης περιστατικών και καταπολέμηση του κυβερνοεγκλήματος

(γ) διαχείριση αντιγράφων ασφαλείας και αποκατάσταση έπειτα από καταστροφή, και διαχείριση των κρίσεων

(δ) ασφάλεια της αλυσίδας εφοδιασμού, συμπεριλαμβανομένων των σχετικών με την ασφάλεια πτυχών που αφορούν τις σχέσεις μεταξύ κάθε οντότητας και των άμεσων προμηθευτών ή παρόχων υπηρεσιών της

(ε) ασφάλεια στην απόκτηση, ανάπτυξη και συντήρηση συστημάτων δικτύου και πληροφοριών, συμπεριλαμβανομένου του χειρισμού και της γνωστοποίησης ευπαθειών

(στ) πολιτικές και διαδικασίες για την αξιολόγηση της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας

(ζ) βασικές πρακτικές κυβερνοϋγιεινής και κατάρτιση στην κυβερνοασφάλεια

(η) πολιτικές και διαδικασίες σχετικά με τη χρήση κρυπτογραφίας και, κατά περίπτωση, κρυπτογράφησης

(θ) ασφάλεια ανθρώπινων πόρων, πολιτικές ελέγχου πρόσβασης και διαχείριση πάγιων στοιχείων

(ι) χρήση λύσεων πολυπαραγοντικής επαλήθευσης ταυτότητας ή συνεχούς επαλήθευσης ταυτότητας, ασφαλών φωνητικών επικοινωνιών, επικοινωνιών βίντεο και κειμένου και ασφαλών συστημάτων επικοινωνιών έκτακτης ανάγκης εντός της οντότητας, κατά περίπτωση. [28]

5.9.1 Ποιες είναι οι νέες υποχρεώσεις που επιβάλει η NIS2

Θεμελιώδη προτεραιότητα που επιβάλλει η NIS2 αφορά την υποχρέωση αποτελεσματικής διαχείρισης απειλών, ανάλυσης κινδύνων και της αντιμετώπισης κακόβουλων ενεργειών, καθώς και αναφορά των συμβάντων αυτών στον κυβερνοχώρο.

Σύμφωνα με το NIS2, σε περίπτωση περιστατικού ασφαλείας στο πληροφοριακό σύστημα μιας υπόχρεης οντότητας, η αρχική κοινοποίηση θα πρέπει να υποβληθεί εντός 24 ωρών και λεπτομερέστερες αναφορές για τα ύποπτα περιστατικά εντός 72 ωρών. Η ΕΕ θα ορίσει επακριβώς τον όρο «σημαντικό περιστατικό», για να αποφευχθούν διαφορετικοί ορισμοί και όρια μεταξύ των κρατών μελών.

Οι οντότητες που είναι υπόχρεοι θα πρέπει να κοινοποιούν τα «σημαντικά περιστατικά» ασφαλείας στις εθνικές τους ομάδες αντιμετώπισης περιστατικών ασφάλειας (CSIRT) ή την αρμόδια αρχή τους, για να μπορεί να επιτευχθεί μία έγκαιρη αντιμετώπισή τους. Η NIS2 εισάγει μια διαδικασία τριών σταδίων για τις προθεσμίες αναφοράς

(α) Θα δοθεί έγκαιρη προειδοποίηση εντός 24 ωρών «αφού λάβετε γνώση του συμβάντος».

(β) Αυτή η προειδοποίηση θα ακολουθείται από πλήρη ειδοποίηση εντός 72 ωρών, συμπεριλαμβανομένης μιας αρχικής αξιολόγησης του συμβάντος·

(γ) Μια τελική έκθεση συντάσσεται μέσα σε ένα μήνα μετά την υποβολή της κοινοποίησης του συμβάντος, συμπεριλαμβανομένης λεπτομερούς περιγραφής του συμβάντος, του είδους της απειλής και των διασυνοριακών επιπτώσεων. [29]

5.9.2 Οι υπόχρεοι της NIS 2

Η πρώτη οδηγία 2016/1148/ΕΚ ευρέως γνωστή NIS ως η πρώτη νομοθετική προσπάθεια για την κυβερνοασφάλεια στην ΕΕ δεν συμπεριελάμβανε κρίσιμου τομείς. Η NIS2 προβλέπει ευρύτερο πεδίο δράσης, σημαντικό για την ανάπτυξη και την οικονομία μίας χώρας. Η νέα νομοθετική προσπάθεια επηρεάζει τους "κρίσιμους τομείς", τόσο του δημοσίου όσο και του ιδιωτικού τομέα. Η ενέργεια, οι μεταφορές, οι τράπεζες, η ύδρευση και τα λύματα, μεταξύ άλλων κρίσιμων υποδομών. Επιπλέον η NIS2 προβλέπει νέες υποχρεώσεις και σε άλλους «ζωτικής σημασίας» τομείς, όπως η μεταποίηση, τα χημικά, τα τρόφιμα, τα ταχυδρομεία, η διαχείριση αποβλήτων, και τις ταχυμεταφορές.

Αυτό οφείλεται στο γεγονός ότι ο πρωταρχικός στόχος της οδηγίας NIS2 είναι η καλύτερη προστασία των οντοτήτων που είναι κρίσιμοι για την οικονομική και κοινωνική ανάπτυξη των κρατών μελών της ΕΕ. Προστατεύοντας τους εαυτούς τους από επιθέσεις στον κυβερνοχώρο, τα κράτη μέλη μπορούν να μετριάσουν τον κίνδυνο παραβίασης δεδομένων, ο οποίος μπορεί να απειλήσει την ασφάλεια, και να βλάψει την εμπιστοσύνη με τους πολίτες.

Αναλυτικότερα οι υπόχρεοι βάσει της NIS2 χωρίζονται σε τρείς κατηγορίες:

- στους significant entities (π.χ. εταιρείες τηλεπικοινωνιών, επιχειρήσεις κοινής ωφέλειας και τράπεζες),
- στους important entities (π.χ. εταιρείες τροφίμων και εταιρείες εμπορευματικών μεταφορών)
-και στους Entities with specific features (π.χ. Δημόσια δίκτυα ηλεκτρονικών υπηρεσιών, παρόχους υπηρεσιών εμπιστοσύνης, Φορείς δημόσιας διοίκησης)

Απαλλάσσονται της NIS2 συμμόρφωσης οι οργανισμοί που απασχολούν λιγότερους από 250 εργαζομένους ή έχουν ετήσιο κύκλο εργασιών μικρότερο των 50 εκατομμυρίων ευρώ.

Η NIS2 επιβάλλει νέες απαιτήσεις στα ενδιαφερόμενα μέρη, όπως επαγγελματισμό και υπευθυνότητα, αποτελεσματική διαχείριση και ανάλυση κινδύνων, αντιμετώπιση περιστατικών ασφαλείας και αναφορά και χειρισμό περιστατικών. Οι επηρεαζόμενες οντότητες είναι υπεύθυνες για τη συμμόρφωση με την οδηγία NIS 2 και ενδέχεται να θεωρηθούν υπεύθυνες για μη συμμόρφωση.

Οι ίδιες οι επιχειρήσεις και οι οργανισμοί θα πρέπει ως επί το πλείστων να εφαρμόζουν μέτρα ασφαλείας και να συμμορφώνονται με κανονίστηκες απαιτήσεις κυβερνοασφάλειας, συμπεριλαμβανομένων διεθνών προτύπων όπως το ISO 27001 και το πλαίσιο NIST.

Η μη συμμόρφωση με την κοινοτική NIS 2 μπορεί να επιφέρει πρόστιμο έως και 10 εκατ. ευρώ ή 2% του παγκόσμιου ετήσιου ακαθάριστου κύκλου εργασιών της εταιρείας.

Στις αρχές του 2023, η κοινοτική οδηγία NIS2 εγκρίθηκε και επισημοποιήθηκε από την ΕΕ. Πλέον τα κράτη μέλη έχουν μια προθεσμία της τάξεως των 21 μηνών για να μεταφέρουν την οδηγία στο εθνικό τους δίκαιο. Στο διάστημα αυτό, τα κράτη μέλη θα θεσπίσουν και θα δημοσιεύσουν τα απαιτούμενα μέτρα συμμόρφωσης με τις εν λόγω οδηγίες.

Η οδηγία NIS2 δεν παρέχει κατευθυντήριες γραμμές για την δημιουργία των κατάλληλων υποδομών και των ελάχιστων τεχνολογικών απαιτήσεων που θα πρέπει να υιοθετήσουν οι υπόχρεοι έναντι των κυβερνοεπιθέσεων.

Η NIS2 ορίζει τον όρο "επαρκής προστασία", ο οποίος μπορεί κάποιος να ερμηνεύσει με διάφορους τρόπους. Θα μπορούσε κάποιος να εννοήσει την χρήση firewalls, χρήση antivirus endpoint προστασία, την εφαρμογή ελέγχου ταυτότητας πολλαπλών παραγόντων, την κρυπτογράφηση και πολλές άλλες ερμηνείες.

Οι οργανισμοί σαν πρώτες ενέργειες για την κάλυψη του όρου "επαρκής προστασία" μπορούν:

- Να διασφαλίσουν ότι η διοίκηση του κάθε οργανισμού έχει επίγνωση της κρισιμότητας της κυβερνοασφάλειας και των σχετικών ευθυνών που απορρέουν από αυτή.
- Να ορίσουν τα περιουσιακά τους στοιχεία, σε ότι αφορά τις διαδικασίες που ακολουθούνται, των πληροφοριών που διατηρούνται στον οργανισμό καθώς και των πληροφοριακών συστημάτων που εμπλέκονται στις διαδικασίες που ακολουθούνται.
- Να οικοδομήσουν ένα σταθερό πλαίσιο ασφαλείας με συστήματα διαχείρισης ποιότητας ISO ή με ένα διαρκώς επικαιροποιημανο framework NIST. Παράλληλα θα πρέπει αν υπάρχει και να εφαρμόζεται ένα σύστημα διαχείρισης κινδύνων για την διασφάλιση και ορθή λειτουργία του οργανισμού.
- Να ενσωματώσουν στον οργανισμό τους λύσεις δια λειτουργικότητας και ασφάλειας.
- Να εδραιωθούν διαδικασίες αναφοράς που αφορούν την NIS2 και την συμμόρφωση με τις απαιτήσεις αυτής, ώστε να διασφαλίζουν ότι μπορούν να χρησιμοποιηθούν προληπτικά για τον μετριασμό κακόβουλων ενεργειών κατά του οργανισμού. [30]

Το νέο κανονιστικό πλαίσιο NIS2 από την Ευρωπαϊκή Ένωση και η εναρμόνιση με την κοινοτική νομοθεσία επιταχύνουν ακόμα περισσότερο τις διαδικασίες αποδοχής και υιοθέτησης κατάλληλων μέτρων ασφαλείας ώστε να μπορεί να διαχειριστεί τον καλύτερο δυνατό τρόπο τις συνέπειες ενός περιστατικού παραβίασης ασφάλειας

5.9.3 Πως μπορούν τα SIEM να συνδράμουν

Η Οδηγία NIS 2 στοχεύει επίσης στην ενίσχυση του συνολικού επιπέδου ασφάλειας στον κυβερνοχώρο στην ΕΕ. Έχει ως απαίτηση από τα κράτη μέλη να διαθέτουν εθνικά CSIRT, να εκτελούν «αμυντικές» ασκήσεις κατά κυβερνοεπιθέσεων ώστε να είναι έτοιμοι να διαχειριστούν πιο αποτελεσματικά τους κινδύνους από περιστατικά παραβίασης ασφάλειας.

Η διασυνοριακή συνεργασία μεταξύ των χωρών της ΕΕ καθώς και σε παγκόσμιο επίπεδο, μέσω του δικτύου CSIRT και άλλων αρμόδιων ομάδων εργασίας είναι επιτακτική ανάγκη όσο ποτέ άλλοτε. Τέλος, απαιτεί από τα κράτη μέλη να εποπτεύουν τους τομείς ζωτικής σημασίας υποδομής τους (ενέργεια, μεταφορές, νερό, υγεία, ψηφιακές υποδομές και χρηματοδότηση) και να τους προστατεύουν επαρκώς από απειλές στον κυβερνοχώρο, για παράδειγμα ιδρύοντας εθνικές αρμόδιες αρχές NIS για να συνεργάζονται για την αξιολόγηση κινδύνων.

Μια τέτοια εποπτεία είναι εφικτή με κατάλληλους μηχανισμούς κυβερνοασφάλειας (π.χ. SIEM) που θα εγκατασταθούν στα πληροφοριακά συστήματα των οργανισμών. Ως εκ τούτου, η παρακολούθηση τέτοιων υποδομών θα βοηθήσει στην ευαισθητοποίηση για την ασφάλεια στον κυβερνοχώρο, καθώς οι διαχειριστές συστημάτων θα ενημερώνονται για τις απειλές στον κυβερνοχώρο που έχουν εντοπιστεί και οι οποίες στο παρελθόν περνούσαν απαρατήρητες. Επιπλέον, οι πληροφορίες σχετικά με τέτοιες κυβερνοαπειλές θα μπορούσαν να αξιοποιηθούν περαιτέρω με τη διαβίβασή τους σε αρμόδιες CERT/CSIRT και ως εκ τούτου να προωθήσουν την κυβερνοασφάλεια στον κυβερνοχώρο σε εθνικό και ευρωπαϊκό επίπεδο. [31]

Μια πιο προσεκτική ματιά σε αυτούς τους μηχανισμούς κυβερνοασφάλειας SIEM και τις επιπτώσεις τους στην οργανωτική ασφάλεια στον κυβερνοχώρο και στη διαχείριση συμβάντων, θα δοθεί στο επόμενο κεφάλαιο.

6

Security Information and Event Management

Μια σημαντική παράμετρος εφαρμογής που μπορεί να συμβάλει στην επίτευξη συμμόρφωσης με όλες τις τεχνικές πτυχές την νέας οδηγίας NIS 2 είναι τα Συστήματα Πληροφοριών Ασφάλειας και Διαχείρισης Περιστατικών (Security Information and Event Management - SIEM). Οι λύσεις SIEM αφού συγκεντρώσουν και κάνουν συσχέτιση τις καταγραφές ασφαλείας (logfiles) από τα εποπτευόμενα συστήματα, αναλύουν τις καταγραφές αυτές με σκοπό να εντοπίσουν ύποπτες δραστηριότητες και να αποφασίσουν αν αυτές υποδηλώνουν κάποιες πιθανές προπαρασκευαστικές ενέργειες μίας επίθεσης.

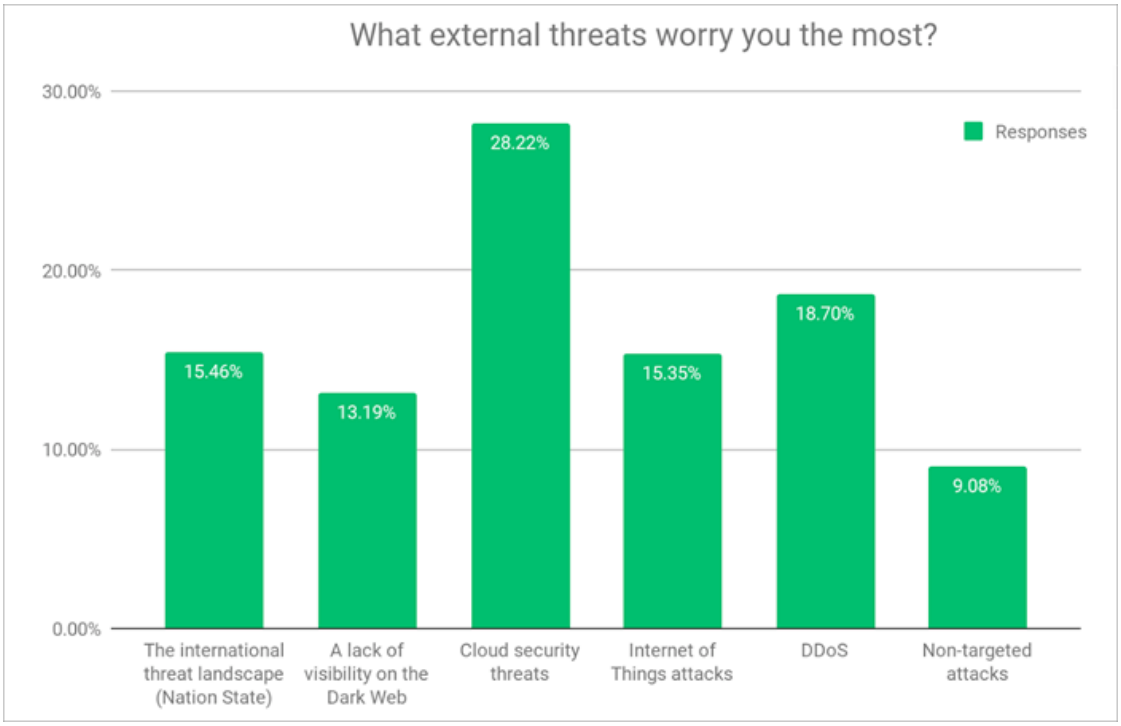
Επιπλέον, οι πληροφορίες που θα εξάγονται από τα συστήματα SIEM σχετικά με κυβερνοαπειλές θα μπορούσαν να αξιοποιηθούν περαιτέρω με τη διαβίβασή τους σε αρμόδιες CERT/CSIRT και ως εκ τούτου να προωθήσουν την κυβερνοασφάλεια στον κυβερνοχώρο σε εθνικό και ευρωπαϊκό επίπεδο. [31]

6.1 SIEM (Συστήματα Ανάλυσης Πληροφοριών Ασφάλειας & Διαχείρισης Περιστατικών)

Η τεχνολογία SIEM έχει ως πρωταρχικό στόχο να βοηθήσει τους υπευθύνους ασφαλείας να έχουν μια ολοκληρωμένη απεικόνιση και διαχείριση, του υπό επίβλεψης τους, πληροφοριακού σύστηματος. Η τεχνολογία SIEM παρέχει μια ενιαία εικόνα της κατάστασης ασφάλειας του πληροφοριακού συστήματος από ετερογενείς πόρους, συμβάλλοντας έτσι στη συνολική επίβλεψη της ασφάλειας ενός οργανισμού.

Οι κύρια λειτουργία ενός συστήματος SIEM είναι η συγκέντρωση όλων των καταγραφών λειτουργίας από όλα τα ανεξάρτητα συστήματα ασφαλείας του οργανισμού καθώς και έλεγχος των καταγραφών αυτών για πιθανές ευπάθειες σε κακόβουλες δραστηριότητες.

Μία έρευνα της εταιρίας AlienVault [32], ανέδειξε ότι υπάρχει μεγάλη ανησυχία στις επιχειρήσεις για απειλές ασφαλείας που αφορούν το cloud. Το 54% των επιχειρήσεων ανησυχεί για το ηλεκτρονικό ψάρεμα (phishing) και το 46% για απειλές τύπου ransomware. Εικόνα 6-1



Εικόνα 6-1 Αποτελέσματα έρευνας AlienVault [32]

Σήμερα, πολλές εταιρείες που χρησιμοποιούν τέτοιου είδους τεχνολογικές λύσεις θεωρούν τα σύστηματα SIEM σαν μια κάμερα παρακολούθησης για όλη την υποδομή IT στο σύνολό της καθώς αποτελούν τα αυτιά και τα μάτια του πληροφοριακού συστήματος, παρέχοντας υπηρεσίες εντοπισμού κακόβουλων ενεργειών σε σύντομο χρονικό διάστημα στο δίκτυο του οργανισμού. Με ένα τέτοιο σύστημα μπορούν να εντοπιστούν τα σημεία προσβολής, στην προκειμένη περίπτωση οι υποκλοπές δεδομένων, να αποκτηθεί μια εικόνα για όλες τις λειτουργίες του IT και να δει κανείς με μια ματιά, για το αν όλα λειτουργούν όπως έχει προβλεφθεί.

6.2 *Κίνητρα για την χρησιμοποίηση SIEM*

Τα εργαλεία SIEM έχουν πρωτεύοντα σκοπό την αποτελεσματικότητα, την αποδοτικότητα καθώς και η συμμόρφωση με την κοινοτική οδηγία NIS 2 και τα πρότυπα ασφάλειας που επιχειρούνται. Στις μέρες μας η πολυπλοκότητα των πληροφοριακών συστημάτων καθώς και η εμφάνιση νέον τεχνολογικών καινοτομιών όπως ψηφιοποίηση, υπολογιστικό νέφος, IoT, τεχνητή νοημοσύνη κ.λ.π, επιφέρει μία αβεβαιότητα στην ασφάλεια τους και η διασφάλιση τους αποτελεί επιτακτική ανάγκη. Απαιτείται η εγκατάσταση και λειτουργία εξειδικευμένου εξοπλισμού και προγραμμάτων παρακολούθησης του δικτύου γεγονός που οδηγεί στην

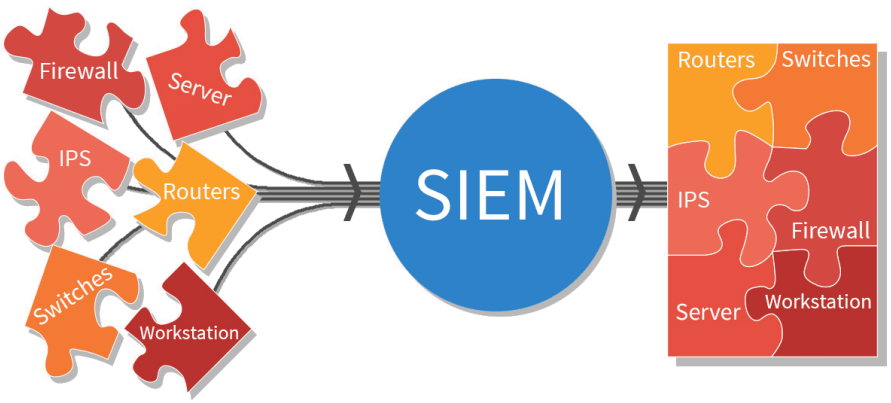
παραγωγή καθημερινά ένας τεράστιου αριθμού logfiles τα οποία πρέπει να παρακολουθούνται και να αναλύονται συνεχώς με σκοπό εξάγονται αναφορές για πιθανές απειλές στο δίκτυο και να μετριάζεται ή εκμηδενίζοντας τον αντίκτυπο των κακόβουλων επιθέσεων. Επίσης, ο υπεύθυνος του δικτύου, παρακολουθεί το δίκτυο του συστήματός που υποστηρίζει, καθώς έχει αποδειχθεί ότι κακόβουλοι χρήστες με προχωρημένο γνωσιολογικό επίπεδο μπορούν να παρακάμψουν ανά πάσα στιγμή την αδιάλειπτη λειτουργία των συστημάτων.

Συμπεραίνοντας λοιπόν, διαπιστώνουμε ότι όταν τα συστήματα ασφαλείας του πληροφοριακού συστήματος που λειτουργούν ανεξάρτητα και όταν ο έλεγχος του δικτύου γίνεται χειροκίνητα, ότι δεν είναι πάντα δυνατό να επιτευχθεί ένα υψηλό επίπεδο ασφάλειας Συνεπώς, είναι απαραίτητο να υπάρχει ένα συγκεντρωτικό σύστημα (Εικόνα 6-2) το οποίο:

Α. θα έχει την δυνατότητα να συλλέγει τα αρχεία καταγραφής ασφαλείας από όλα τα ανεξάρτητα συστήματα που βρίσκονται στο δίκτυό μας

Β. θα κάνει συσχέτιση των εξαγόμενων πληροφοριών και στην συνέχεια θα εξάγονται οι περιττές πληροφορίες

Γ. Μετά την συγκέντρωση των αποτελεσμάτων που αφορούν την κατάσταση του δικτύου θα προχωράει βάση ενός πλήθους προκαθορισμένων ενεργειών στον εντοπισμό των ύποπτων δραστηριοτήτων και στην ανάλογη αντίδραση.



Εικόνα 6-2 Αυτόνομο σύστημα SIEM [33]

6.3 Αρχιτεκτονική των SIEM

Οι λύσεις SIEM (Security Information and Event Management) αποτελούν την ναυαρχίδα υπέρ της ασφάλειας κάθε οργανισμού, καθώς παρέχουν υπηρεσίες συλλογής και ενοποίησης όλων των συστημάτων ασφαλείας, ενώ έχουν την δυνατότητα να ανιχνεύσουν μια στοχευμένη κυβερνοεπίθεση στην αρχική της φάση, μετριάζοντας τις ζημιές που μπορεί να προκληθούν

από αυτή. Τα SIEM προσφέρουν εκείνες τις λειτουργίες, οι οποίες χρειάζονται σε όλες τις περιπτώσεις διαχείριση περιστατικών ασφάλειας και για την τήρηση των κανόνων συμμόρφωσης όπως της κοινοτικής οδηγίας NIS.

Όλες οι λύσεις SIEM λειτουργούν διενεργώντας ένα σύνολο ενεργειών. Αυτές είναι η συγκέντρωση των αρχείων καταγραφής, η ενοποίηση αυτών των καταγραφών και η ταξινόμηση αυτών με στόχο των εντοπισμό κακόβουλων ενεργειών και την συμμόρφωσης με τις εκάστοτε απαιτήσεις ασφαλείας. Κάποιες λύσεις siem διαφέρουν ως προς τις δυνατότητες που προσφέρουν, αλλά οι περισσότερες προσφέρουν το βασικό σύνολο λειτουργιών όπως:

Διαχείριση καταγραφών - Τα siem καταγράφουν όλα τα συμβάντα ασφαλείας από ένα μεγάλο φάσμα πηγών που βρίσκονται στο υπό παρακολούθηση δίκτυο. Τα αρχεία καταγραφής και τα δεδομένα χρηστών και εφαρμογές, συλλέγονται, αποθηκεύονται και αναλύονται σε πραγματικό χρόνο, δίνοντας στους υπευθύνους ασφαλείας τη δυνατότητα να διαχειρίζονται αυτόματα τα αρχεία καταγραφής συμβάντων και τα δεδομένα δικτύου σε μια κεντρική πλατφόρμα. Κάποιες λύσεις siem ενσωματώνουν επίσης με πληροφορίες απειλών τρίτων, προκειμένου να συσχετιστούν οι εσωτερικές καταγραφές ασφαλείας με προηγουμένως αναγνωρισμένες καταγραφές απειλών. Η ενσωμάτωση αυτή των απειλών σε πραγματικό χρόνο επιτρέπει στους διαχειριστές ασφαλείας να αποκλείουν ή να εντοπίζουν νέους τύπους επίθεσης.

Συσχέτιση συμβάντων και Analytics - Η συσχέτιση των καταγραφών ασφαλείας είναι ουσιώδης λειτουργία οποιασδήποτε λύσης SIEM. Χρησιμοποιώντας προηγμένα αναλυτικά στοιχεία για τον εντοπισμό και την κατανόηση περίπλοκων καταγραφών ασφαλείας, η συσχέτιση συμβάντων παρέχει πληροφορίες για τον γρήγορο εντοπισμό και τον μετριασμό πιθανών απειλών για την ασφάλεια του υπό παρακολούθηση δικτύου .

Παρακολούθηση συμβάντων και ειδοποιήσεις ασφαλείας – οι λύσεις siem παρέχοντας την δυνατότητα της κεντρική διαχείριση μίας εσωτερικής υποδομής είναι σε θέση να εντοπίσουν όλες τις οντότητες που είναι συνδεδεμένες στο δίκτυο. Αυτό επιτρέπει στα εργαλεία siem να παρακολουθούν συμβάντα ασφαλείας όλων των συνδεδεμένων χρηστών, συσκευών και εφαρμογών, ενώ ταξινομεί όλες τις ύποπτες ενέργειες που εντοπίζει στο δίκτυο. Κάνοντας χρήση προσαρμοσμένων, προκαθορισμένων κανόνων συσχέτισης, οι διαχειριστές μπορούν να ειδοποιηθούν αμέσως και να λάβουν τις κατάλληλες οδηγίες για τον μετριασμό σημαντικών ζητημάτων ασφάλειας.

6.4 Χαρακτηριστικά ενός SIEM

Σήμερα στα πλαίσια θωράκισης των Πληροφοριακών Συστημάτων έναντι των ουκ ολίγων πολυσύνθετων απειλών, έχουν κάνει την εμφάνισή τους πολλά εμπορικά προϊόντα SIEM. Αυτά

επιδιώκουν να κερδίσουν την εμπιστοσύνη αγοραστικού κοινού. Οι λύσεις SIEM προσφέρουν μία γκάμα από λειτουργίες κρίσιμες για τη διαχείριση των απειλών ή για την τήρηση των κανόνων συμμόρφωσης. Μία λύση SIEM μπορούν να παρέχουν στους υπευθύνους ασφαλείας μια συνολική εικόνα της υποδομής, αλλά και των ροών εργασίας σε αυτήν, καθώς διαχείριση των αρχείων καταγραφής με τρόπο που επιβάλει η κανονιστική συμμόρφωση. Πριν την επιλογή και υλοποίηση μιας λύσης SIEM οι οργανισμοί πρέπει να εξετάσουν αν διαθέτει τα ακόλουθα χαρακτηριστικά, αλλά και με ποιο τρόπο τα υποστηρίζει:

- Επεκτάσιμη αρχιτεκτονική και ευελιξία ανάπτυξης

Στο στάδιο του σχεδιασμού, οι περισσότεροι οργανισμοί υποτιμούν τον όγκο των δεδομένων που θα συλλεχθούν κατά τη διάρκεια ενός περιστατικού και τον όγκο των αναφορών ανάλυσης που θα απαιτηθούν, καθώς μια αρχιτεκτονική που υποστηρίζει την επεκτασιμότητα και την ευελιξία στην ανάπτυξη λύσεων SIEM θα τους επιτρέψει να αντιμετωπίσουν τον απροσδόκητο όγκο δεδομένων που θα παραχθούν κατά τη διάρκεια ενός περιστατικού.

- Συλλογή και παρακολούθηση καταγραφών ασφαλείας σε πραγματικό χρόνο (Real-time monitoring)

Οι λύσεις SIEM συγκεντρώνουν τις καταγραφές που σχετίζονται με ένα περιστατικό σχεδόν σε πραγματικό χρόνο, επιτρέποντας την άμεση ανάλυσή τους. Η κύρια λειτουργία ενός SIEM εργαλείου είναι να συγκεντρώνει από ανεξάρτητα συστήματα ασφαλείας (firewalls, antivirus, κ.τ.λ) τα αρχεία καταγραφών τους και με κάποια κλειστά πρότυπα που διαθέτουν να τα επεξεργάζεται για να προσαρμοστούν σε μια συγκεκριμένη μορφή. Στο επόμενο στάδιο παρέχει πληροφορίες ανάλυσης των καταγραφών αυτών και σε περίπτωση ανίχνευσης μια ύποπτης δραστηριότητας παράγει ειδοποιήσεις και αναφορές στον διαχειριστή ασφαλείας του οργανισμού.

- Κανονικοποίηση περιστατικών και ταξινόμηση

Λειτουργία δύο σταδίων. Στο πρώτο στάδιο “μεταφράζονται” τα περιστατικά ασφαλείας σε κατανοητή μορφή δεδομένων. Στο δεύτερο στάδιο γίνεται η ταξινόμηση/κατηγοριοποίηση αυτών των δεδομένων συμβάλλοντας έτσι στην ευκολότερη επεξεργασία και αξιοποίηση των περιστατικών που ανακαλύφτηκαν.

- Ευφυής εντοπισμός

Η ευφυΐα έγκειται στο γεγονός ότι οι πληροφορίες δημιουργούνται με τη χρήση ποικίλων πηγών, συμπεριλαμβανομένων των καταλόγων ανοικτού κώδικα, της γνώσης των απειλών που αποκτούν οι ερευνητικές ομάδες των παρόχων λύσεων ασφαλείας και των δεδομένων που παράγονται από τους ελέγχους ασφαλείας. Τα δεδομένα που παράγονται από την ευφυή ανάλυση των κακόβουλων ενεργειών μπορούν να συγκεντρωθούν και ενσωματωθούν σε λίστες παρακολούθησης SIEM, ρολών συσχέτισης και σειρών, συμβάλλοντας στην αύξηση του

βαθμού επιτυχούς ανίχνευσης σε περίπτωση επίθεσης στο υπο παρακολούθηση πληροφοριακό σύστημα.

- Απλοποιημένες αναφορές κανονιστικής συμμόρφωσης

Η ανάπτυξη μιας λύσης SIEM γίνεται εστιάζοντας στη διαχείριση logs και στις ειδικές απαιτήσεις μιας αναφοράς συμμόρφωσης. Πολλοί οργανισμοί κάνουν χρήση τέτοιων τεχνολογιών για να μπορούν να έχουν μια εξορθολογισμένη και απλοποιημένη υποβολή εκθέσεων στα πλαίσια των κανονιστικών συμμορφώσεων. Ένα διακομιστής SIEM που είναι εγκαταστημένος στην υποδομή ενός οργανισμού μπορεί να λαμβάνει καταγραφές ασφαλείας από μία πληθώρα πηγών και να εκδίδει μια ενιαία έκθεση που να περιέχει όλα τα σχετικά καταγεγραμμένα συμβάντα ασφαλείας από όλες αυτές τις πηγές.

6.5 Συγκριτική αξιολόγηση των ανοιχτού κώδικα SIEM

Για να αξιολογήσουμε τα προϊόντα SIEM θα πρέπει πρωταρχικά να ορίσουμε τα χαρακτηριστικά των συστημάτων αυτών τα οποία θα αποτελέσουν το μέτρο σύγκρισης και αξιολόγησης των προϊόντων. Τα SIEM συστήματα μπορούν να είναι cloud-based λογισμικά, hardware συσκευές υλικού, virtual appliances και παραδοσιακά λογισμικά διακομιστή. Όλα τα open source προϊόντα που θα παρουσιαστούν σε αυτήν την ενότητα προσφέρουν σχεδόν παρόμοιες δυνατότητες, και διαφέρουν κυρίως ως προς τις επιδόσεις και το κόστος. Στην παρούσα εργασία λαμβάνουμε σαν άξονα σύγκρισης επτά βασικά χαρακτηριστικά για την βάση σύγκρισης.

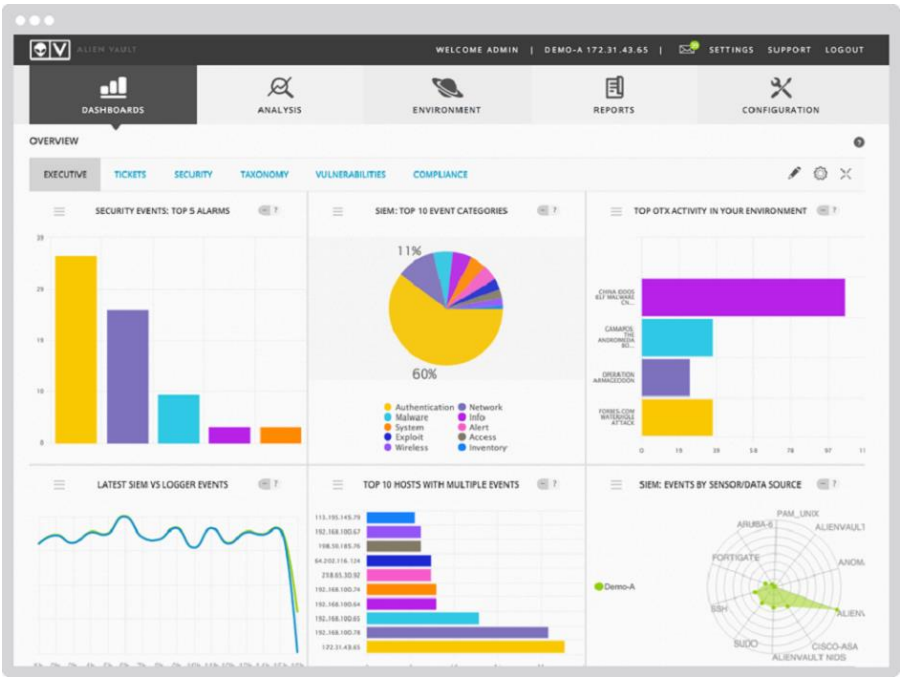
- Δυνατότητες νοημοσύνης απειλών (Threat intelligence capabilities)
- Σε ποιο βαθμό το SIEM παρέχει εγγενή υποστήριξη για τις σχετικές πηγές καταγραφής;
- Ποιες forensic δυνατότητες μπορούν να παρέχουν;
- Ποια χαρακτηριστικά προσφέρουν τα προϊόντα SIEM για ανάλυση δεδομένων
- Δυνατότητες αυτοματοποιημένης απόκρισης του SIEM Analytics
- Ενσωματωμένη υποστήριξη για την έκδοση αναφορών σύμφωνα συμμορφώσεις ασφαλείας

6.6 Δημοφιλή προϊόντα ανοιχτού κώδικα

ALIENVAULT OSSIM

Το OSSIM (Εικόνα 6-3) είναι η έκδοση ανοιχτού κώδικα του AlienVault, η οποία έχει λιγότερες δυνατότητες από την πλήρη εταιρική έκδοση USM, αλλά εξακολουθεί να είναι ένα χρήσιμο εργαλείο για οργανισμούς με περιορισμένους προϋπολογισμούς και ανάγκη για μια λύση SIEM. Για μικρές επιχειρήσεις, η έκδοση ανοιχτού κώδικα μπορεί να χρησιμοποιηθεί σε

έναν μόνο διακομιστή. Το OSSIM αξιοποιεί τη δύναμη του AT&T Open Threat Exchange (OTX)—το οποίο παρέχει ανοιχτή πρόσβαση σε μια παγκόσμια κοινότητα ερευνητών απειλών και επαγγελματιών ασφάλειας. Το OSSIM περιλαμβάνει βασικά στοιχεία SIEM, όπως συλλογή συμβάντων, κανονικοποίηση και συσχέτιση. Η δωρεάν έκδοση δεν διαθέτει επίσης δυνατότητες διαχείρισης αρχείων καταγραφής ή παρακολούθησης υποδομής cloud.



Εικόνα 6-3 OSSIM της AlienVault

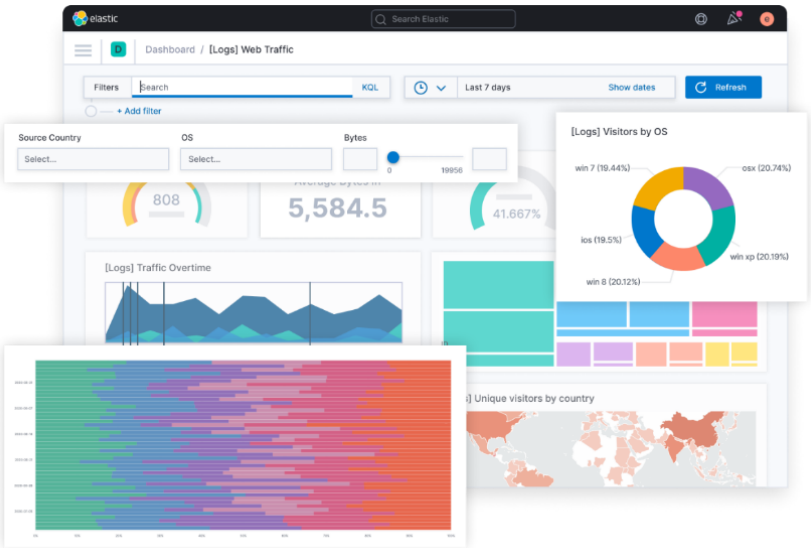
PRELUDE

Παρόμοια με το AlienVault, το Prelude OSS είναι η έκδοση ανοιχτού κώδικα του εταιρικού SIEM του προγραμματιστή. Είναι μια εξαιρετική επιλογή για μικρές επιχειρήσεις που χρειάζονται SIEM αλλά δοκιμάζουν διάφορες λύσεις ή χρειάζονται μια οικονομική εναλλακτική λύση. Το πλεονέκτημα του Prelude OSS είναι ότι υποστηρίζει πολλές μορφές αρχείων καταγραφής και ενσωματώνεται με άλλα εργαλεία όπως το OSSEC, το Snort και το Suricata. Το Prelude OSS χρησιμοποιεί τη μορφή IDMEF , επομένως τα δεδομένα του μπορούν να χρησιμοποιηθούν με συστήματα ανίχνευσης εισβολής. Επειδή το Prelude OSS προορίζεται για μικρές αναπτύξεις, έχει λιγότερες δυνατότητες από το εταιρικό SIEMS και η απόδοση είναι περιορισμένη. Για επιχειρήσεις που πρέπει να αξιολογήσουν τα SIEM πριν αγοράσουν μια εταιρική έκδοση, το Prelude OSS είναι μια καλή επιλογή. Εικόνα 6-4

Εικόνα 6-4 Prelude OSS

ELK STACK

Το Elastic Stack είναι το πιο δημοφιλές εργαλείο ανοιχτού κώδικα σήμερα. Είναι μέρος της αρχιτεκτονικής των OSSEC Apache Metron, SIEMonster και Wazuh. Είναι συνδιασμός του SIEM Elasticsearch, Logstash και Kibana and Beats. Το Elasticsearch είναι το δεύτερο λογισμικό ανοιχτού κώδικα με τις περισσότερες λήψεις μετά τον πυρήνα Linux. Βασικά κάνει τη δουλειά της ευρετηρίασης και αποθήκευσης δεδομένων και χρησιμοποιεί έναν μηχανισμό ουράς, έτσι ώστε οι συνδέσεις μεταξύ των δεδομένων να διατηρούνται. Το Logstash παρέχει log record, καθώς συλλέγει δεδομένα καταγραφής και στη συνέχεια φιλτράρει, επεξεργάζεται και βελτιώνει τα δεδομένα και ενεργοποιεί τα custom plug-ins. Το Kibana παρέχει οπτικοποίηση και εξαιρετικά ισχυρό σε αυτό και επιτρέπει στους χρήστες να αναλύουν τα δεδομένα με τρόπο που τους αρέσει. Εικόνα 6-5



Εικόνα 6-5 Elastic Stack

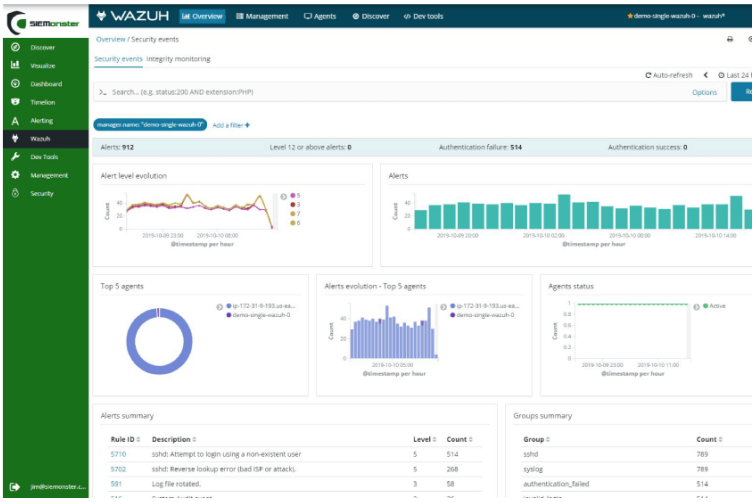
APACHE METRON

Το Apache Metron παρέχει ένα επεκτάσιμο προηγμένο πλαίσιο ανάλυσης ασφαλείας που έχει δημιουργηθεί σε συνεργασία με την κοινότητα Hadoop που εξελίσσεται από την Cisco OpenSOC Project. Ένα πλαίσιο εφαρμογών ασφάλειας στον κυβερνοχώρο παρέχει στους οργανισμούς τη δυνατότητα να ανιχνεύουν ανωμαλίες στον κυβερνοχώρο, να ανταποκρίνονται γρήγορα σε εντοπισμένες ανωμαλίες. Η Metron παρέχει δυνατότητες συγκέντρωση αρχείων καταγραφής, ευρετηρίασης, αποθήκευσης, ανάλυσης συμπεριφοράς και τον εμπλουτισμό δεδομένων, ενώ εφαρμόζει τις πιο πρόσφατες threat-intelligence πληροφορίες. Από αρχιτεκτονική άποψη, το ισχυρότερο χαρακτηριστικό της Metron είναι η επεκτασιμότητά του. Εικόνα 6-6

Εικόνα 6-6 Apache Metron

SIEMonster

Το SIEMonster είναι μια συλλογή των καλύτερων εργαλείων ασφαλείας ανοιχτού κώδικα. Σχεδιασμένο για μικρούς οργανισμούς, φιλανθρωπικά ιδρύματα, αίθουσες διδασκαλίας ή ακόμα και για όσους θέλουν απλώς να ελέγξουν ένα Fully Loaded SIEM. Αυτή η έκδοση είναι εντελώς δωρεάν, για την κοινότητα και για την υποστήριξη της κοινότητας. Η Community Edition παρέχει την υπηρεσία παρακολούθησης όλων των στοιχείων του δικτύου σε μια οικονομικά προσιτή επεκτάσιμη λύση. Αυτή η λύση ενός διακομιστή διευκολύνει τους οργανισμούς που έχουν λίγα end-points. Για να αποκτήσει κάποιος πρόσβαση στην Community Edition, θα πρέπει να εγγραφεί σε αυτή, και να ανταλλάξει πληροφορίες με άλλους χρήστες του Community Edition. Εικόνα 6-7



Εικόνα 6-7 SIEMonster

Πίνακας 6-1 Σύγκριση κορυφαίων λύσεων SIEM

Ανοιχτού Κώδικα SIEM	Επιλογές ανάπτυξης	Κύρια χαρακτηριστικά	Περιορισμοί
The ELK Stack Μια συλλογή από τρία προϊόντα ανοιχτού κώδικα: Elasticsearch, Logstash, and Kibana. Αυτά τα τρία εργαλεία παρέχουν την δυνατότητα οπτικοποίησης και ανάλυσης συμβάντων.	Ανάπτυξη σε εικονική μηχανή, φυσική μηχανή, ιδιωτικό η δημόσιο cloud (π.χ. Google, Azure, AWS).	Καταγραφή και ανάλυση αρχείων καταγραφής Επεξεργάζεται, φιλτράρει, συσχετίζει και βελτιώνει τα δεδομένα καταγραφής που συλλέγει Δημιουργία ευρετηρίου και αποθήκευση δεδομένων	Φτωχή ανάλυση αρχείων καταγραφής Δεν έχει σχεδιαστεί ως σύστημα SIEM Δεν υπάρχει ενσωματωμένη δυνατότητα αναφοράς ή ειδοποίησης Δεν υπάρχουν ενσωματωμένοι κανόνες ασφαλείας
Apache Metron Ένας σχετικά νέο εργαλείο στον κλάδο. Συνδυάζει πολλά εργαλεία ανοιχτού κώδικα σε μια ενιαία πλατφόρμα.	Λειτουργεί με τρεις αποθήκες δεδομένων: HBase, HDFS, και Elastic Search	Αποθηκεύει εμπλουτισμένα δεδομένα τηλεμετρίας Αλγόριθμοι ανίχνευσης ανωμαλιών και μηχανικής μάθησης που μπορούν να εφαρμοστούν σε πραγματικό χρόνο	Μπορεί να εγκατασταθεί σε περιορισμένο αριθμό περιβάλλοντων και λειτουργικών συστημάτων Το UI βρίσκεται στο στάδιο αρχικής ανάπτυξη και δεν υποστηρίζει έλεγχο ταυτότητας
SIEMonster Βασίζεται σε τεχνολογία	Ανάπτυξη σε cloud με χρήση Docker containers, εικονική μηχανή, φυσική μηχανή,	Πλαίσιο επεξεργασίας Threat intelligence Το Elk Stack	Η δωρεάν έκδοση δεν προσφέρει user behavioral analytics, μηχανική μάθηση,

Ανοιχτού Κώδικα SIEM	Επιλογές ανάπτυξης	Κύρια χαρακτηριστικά	Περιορισμοί
ανοιχτού κώδικα. Διατίθεται δωρεάν και επί πληρωμή.	(Mac, Ubuntu, CentOS, and Debian).	χρησιμοποιείται για αποθήκευση, συλλογή, επεξεργασία και οπτικοποίηση	HoneyNet και Threat Kill δυνατότητες Έλλειψη ηλεκτρονικού εγχειριδίου
Prelude Συνδιάζει άλλα siem εργαλεία ανοιχτού κώδικα. Είναι η έκδοση ανοιχτού κώδικα του εμπορικού εργαλείου με το ίδιο όνομα.	Ανάπτυξη σε Linux, OpenBSD, FreeBSD, NetBSD, Sun/Solaris, MacOSX, Tru64, και άλλα παρεμφερές UNIX συστήματα.	Συσχέτιση, φιλτράρισμα και ειδοποίηση Δυνατότητες ανάλυσης και οπτικοποίησης	Δεν έχει σχεδιαστεί για χρήση σε μικρής κλιμακας συστήματα Η απόδοση ανοιχτού κώδικα κατώτερη του εμπορικού προϊόντος
OSSIM Πλατφόρμα SIEM που περιλαμβάνει συλλογή συμβάντων, κανονικοποίηση και συσχέτιση.	Ανάπτυξη σε φυσικά και εικονικά περιβάλλοντα.	Συσχέτιση Περιστατικών Ανακάλυψη Asset Αξιολόγηση τρωτότητας Συσχέτιση συμβάντων SIEM Ανίχνευση εισβολής Παρακολούθηση συμπεριφοράς	Ζητήματα απόδοσης Περιορισμένη διαχείριση αρχείων καταγραφής Ανάπτυξη σε έναν μόνο διακομιστή Καμία ενσωμάτωση με τις λύσεις της UEBA Περιορισμένη παρακολούθηση εφαρμογών/βάσεων δεδομένων

7

Εισαγωγή στο AlienVault OSSIM

7.1 Εισαγωγή

Το ακρωνύμιο OSSIM προέρχεται από το Open Source Security Information Management. Ταξινομείται ως ένα εργαλείο διαχείρισης πληροφοριών ασφαλείας, το οποίο μπορεί να παρέχει αξιόλογες υπηρεσίες για την αντιμετώπιση περιστατικών ασφαλείας, τη συμμόρφωση με τα κανονιστικά πλαίσια και την ανίχνευση απειλών.

Το OSSIM της AlienVault βρίσκεται στην αγορά SIEM από το 2003. Σύμφωνα με την AlienVault, οι εγκατεστημένες πλατφόρμες OSSIM σε όλο τον κόσμο ξεπερνούν τις 18.000, ένας καθόλου ευκαταφρόνητος αριθμός στον χώρο των SIEM λύσεων. Η AlienVault εκτός από την open source λύση OSSIM έχει κυκλοφορήσει στην αγορά και την επαγγελματική έκδοση που ονομάζεται Unified Security Management Platform (USM) η οποία βασίζεται στην πλατφόρμα OSSIM.

Το AlienVault OSSIM αξιοποιεί τη δύναμη του AlienVault Open Threat Exchange (OTX) επιτρέποντας στους χρήστες να συνεισφέρουν και να λαμβάνουν πληροφορίες σε πραγματικό χρόνο σχετικά με κακόβουλους κεντρικούς υπολογιστές. Επιπλέον, παρέχει συνεχή ανάπτυξη για το AlienVault OSSIM παρέχοντας πρόσβαση σε εξελιγμένες τεχνολογίες ασφαλείας. Το AlienVault OSSIM προσφέρει την ευκαιρία στους ειδικούς ασφαλείας να αυξήσουν την ορατότητα και τον έλεγχο της ασφάλειας στο δίκτυό τους. [34]

Το AlienVault OSSIM παρέχει μια ενοποιημένη πλατφόρμα με πολλές δυνατότητες ασφαλείας όπως:

1. Διαχείριση πληροφοριών ασφαλείας
2. Διαχείριση συμβάντων ασφαλείας
3. Διαχείριση και ανακάλυψη περιουσιακών στοιχείων
4. Διαχείριση αρχείων καταγραφής

5. Διαχείριση δικτύου

6. IDS (ανίχνευση εισβολής)

7. HID (ανίχνευση εισβολής κεντρικού υπολογιστή)

8. Αξιολόγηση της ευπάθειας

9. Ανίχνευση απειλών

10. Παρακολούθηση συμπεριφοράς

11. Υποστήριξη Netflow

12. Απόκριση περιστατικού

13. Αναφορά

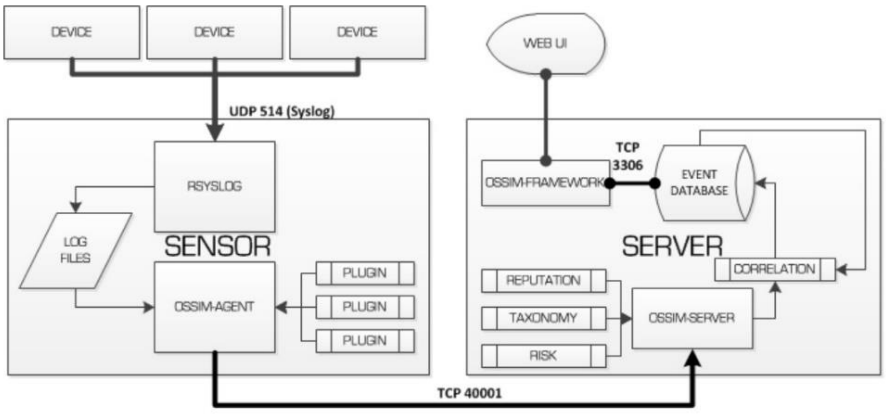
14. Ισχυρό και φιλικό προς το χρήστη

7.1.1 Αρχιτεκτονική του OSSIM

Το OSSIM της AlienVault αποτελείται από πέντε κύρια μέρη: (α) αισθητήρας (Sensor), (β) εξυπηρετητής (server), (γ) πλαίσιο εργασίας (Framework), (δ) βάση δεδομένων (Database) και (ε) επιπρόσθετα στοιχεία (DS Plug-ins).

Μπορεί να γίνει εγκατάσταση των τεσσάρων αυτών στοιχείων σε ένα μόνο φυσικό μηχάνημα (physical machine), σε μία εικονική μηχανή (virtual machine), σε διαφορετικές εικονικές μηχανές ή/και φυσικές μηχανές, ανάλογα με το μέγεθος και τη διαμόρφωση του δικτύου πρός παρακολούθηση.

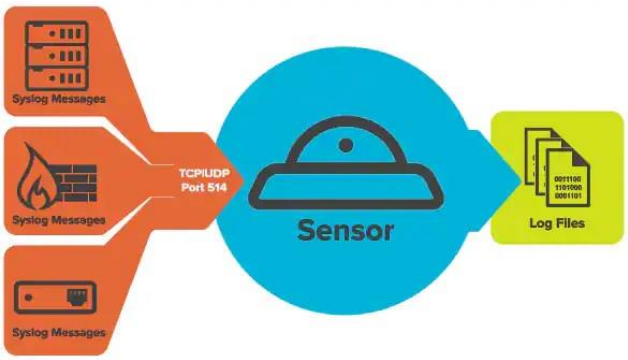
Για ένα σχετικά μικρό δίκτυο, η εγκατάσταση σε ένα μόνο μηχάνημα, μπορεί να είναι η σωστή λύση. Για μεγαλύτερα δίκτυα, συνιστάται εγκατάσταση αισθητήρων και της βάσης δεδομένων ξεχωριστά. Εικόνα 7-1 δείχνει την αρχιτεκτονική του OSSIM.



Εικόνα 7-1 Αρχιτεκτονική OSSIM

(α) αισθητήρας (Sensor)

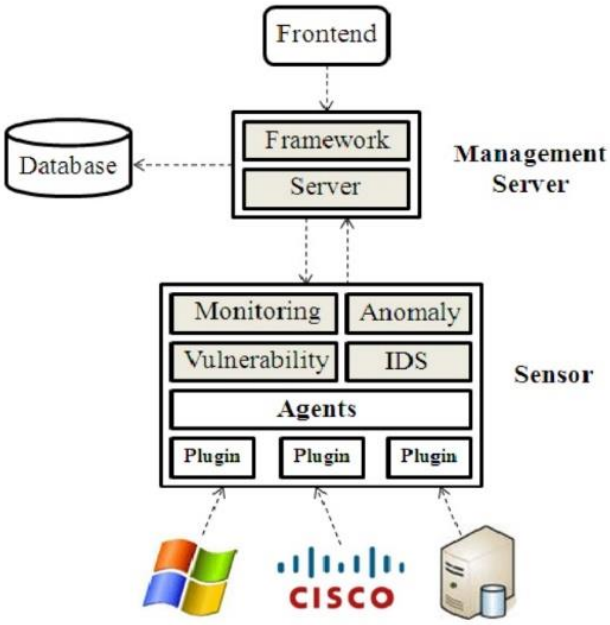
Ο αισθητήρας μπορεί να είναι υπηρεσία rsyslog, η οποία ακούει στη θύρα TCP/UDP 514 από όπου λαμβάνει τα αρχεία καταγραφής από συσκευές δικτύου και τα αποθηκεύει τοπικά, είτε πράκτορες που εκτελούν ανάλυση και κανονικοποίηση αρχείων καταγραφής και τα στέλνει στον server για τις επιπλέον επεξεργασίες. Εικόνα 7-2



Εικόνα 7-2 OSSIM Sensor

(β) εξυπηρετητής (server)

Ο διακομιστής εκτελεί τις βασικές λειτουργίες SIEM: συγκέντρωση, εκτίμηση κινδύνου και συσχέτιση συμβάντων που λαμβάνονται από τον αισθητήρα μέσω της θύρας TCP 40001. Ο διακομιστής στέλνει επίσης τις πληροφορίες σχετικά με τα συμβάντα στη βάση δεδομένων για αποθήκευση.



Εικόνα 7-3 Διαφορετικά στοιχεία του OSSIM [35]

(γ) πλαίσιο εργασίας (Framework)

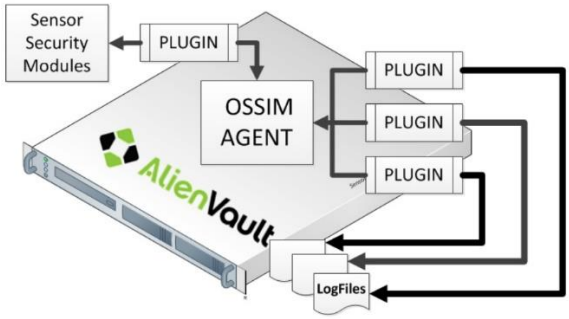
Το Πλαίσιο συνδέει και διαχειρίζεται τα στοιχεία OSSIM και τα εργαλεία ασφαλείας που περιλαμβάνονται και παρέχει το γραφικό περιβάλλον διαχείρισης του συστήματος.

(δ) βάση δεδομένων (Database)

Η βάση δεδομένων χρησιμοποιείται για την αποθήκευση όλων των ρυθμίσεων, των αγαθών, και των αρχείων καταγραφών ασφαλείας. Εικόνα 7-4

(ε) επιπρόσθετα στοιχεία (DS Plug-ins)

Τα DS Plug-ins είναι configuration files τα οποία περιέχουν όλες τις απαραίτητες οδηγίες που για τον αισθητήρα που επιβάλλονται για να κανονικοποιήσει τις εγγραφές ασφαλείας που λαμβάνει.



Εικόνα 7-4 OSSIM Plugin [36]

7.2 Εγκατάσταση OSSIM

Σε αυτό το σημείο θα παρουσιάσουμε τις οδηγίες για την εγκατάσταση του OSSIM σε μια εικονική μηχανή. Το OSSIM βασίζεται στη διανομή του λειτουργικού συστήματος Debianlinux. Πρόκειται για ένα σύστημα ανοικτού κώδικα.

Στο πρώτο βήμα είναι να κατεβάσουμε ένα ασφαλές αντίγραφο του OSSIM από το επίσημο website της εταιρίας AlienVault. (http://www.alienvault.com/free-downloads-services)

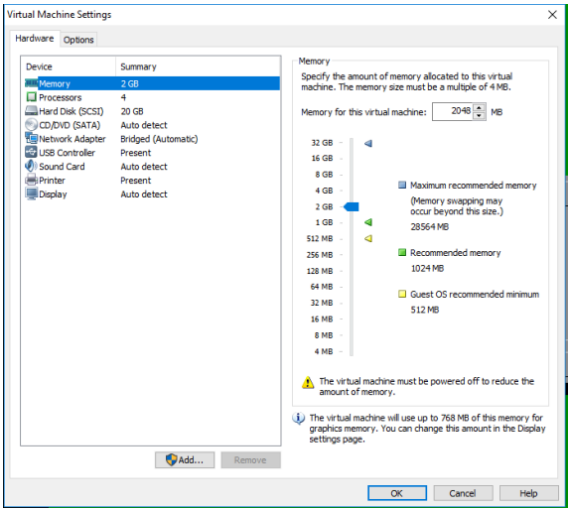
Πριν από την εγκατάσταση, θα πρέπει να προχωρήσουμε στην δημιουργία του Virtual Machine που θα φιλοξενήσει τον OSSIM server πληρώντας τις ελάχιστες απαιτήσεις συστήματος που αναφέρονται παρακάτω. Εικόνα 7-5

(α) 2 CPU cores

(β) 4-8 GB RAM

(γ) 50 GB HDD

(δ) E1000 compatible network cards



Εικόνα 7-5 Απαιτήσεις συστήματος

Αφού έχουμε δημιουργήσει το Virtual Machine που θα φιλοξενήσει τον OSSIM server προχωράμε στην εγκατάσταση όπως αυτή παρουσιάζεται στα επόμενα βήματα:

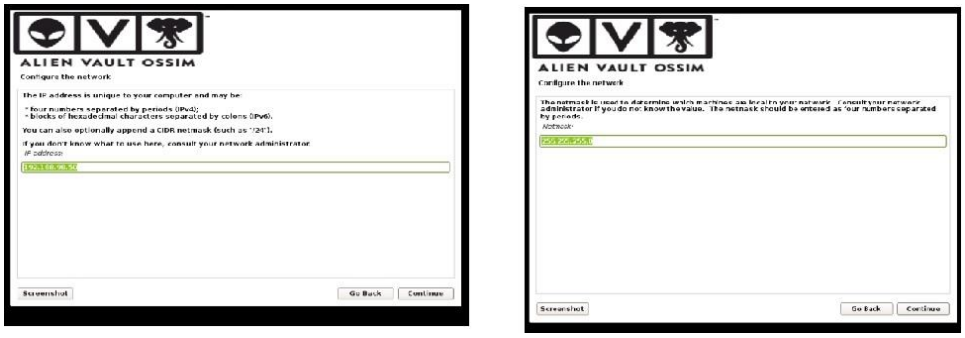
1. Κατά την εκκίνηση του OSSIM iso, ένας οδηγός εγκατάστασης όπως φαίνεται στην Εικόνα 7-6 μας καλωσορίζει.

Εικόνα 7-6 Οδηγός εγκατάστασης

2. Επιλέγουμε γλώσσα, την ζώνη ώρας, τοποθεσία κ.λ.π που επιθυμούμε Εικόνα 7-7

Εικόνα 7-7 Επιλογή γλώσσα, ζώνη ώρας, τοποθεσία

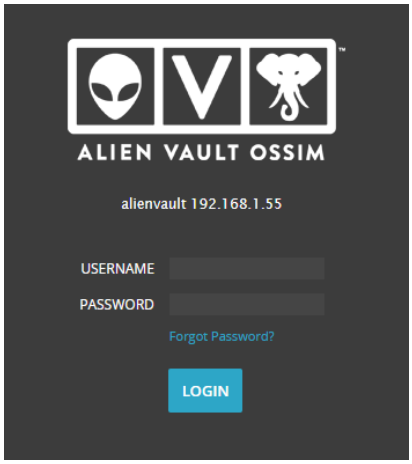
3. Ορίζουμε την IP διεύθυνση του OSSIM, το netmask, το gateway και το DNS (Εικόνα 7-8)



Εικόνα 7-8 IP διεύθυνση του OSSIM

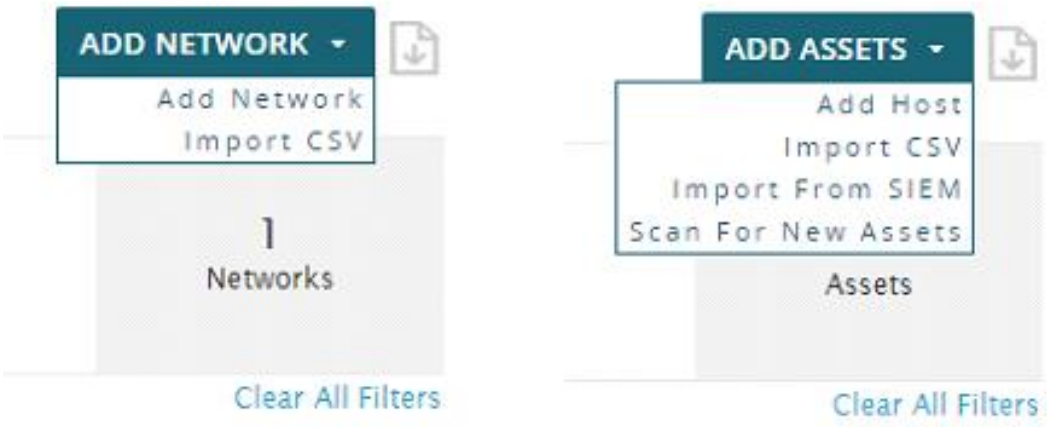
4. Στο επόμενο βήμα εισάγουμε τον κωδικό root (administrator password) του συστήματος.

5. Μετά την ολοκλήρωση των άνω βημάτων μας δίνεται η δυνατότητα για είσοδο στο διαχειριστικό περιβάλλον του OSSIM. (Εικόνα 7-9)



Εικόνα 7-9 είσοδο στο διαχειριστικό του OSSIM

6. Στην συνέχεια θα πρέπει καθοριστούν τα δικτυακά στοιχεία που θα παρακολουθούνται από το OSSIM καθώς και τα αγαθά (assets). Τα assets είναι δικτυακές συσκευές, οι οποίες είναι στην πραγματικότητα όλα τα στοιχεία εκείνα για τα οποία το OSSIM συλλέγει και επεξεργάζεται αρχεία καταγραφής και δεδομένα ασφαλείας. Εικόνα 7-10

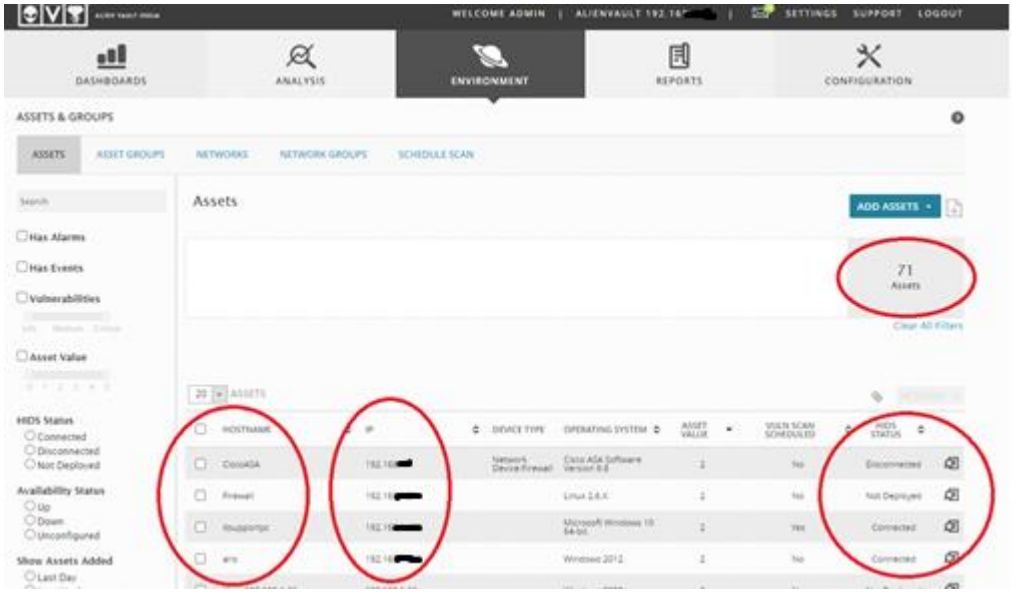


Εικόνα 7-10 Καθορισμός δικτύων

7.3 Προσθήκη πρακτόρων OSSEC στο OSSIM

Το OSSIM της AlienVault χρησιμοποιεί το λογισμικό ανοικτού κώδικα OSSEC για την παρακολούθηση των διακομιστών δικτύου, και μάλιστα, παράλληλα με τον διακομιστή OSSIM, εκτελείται ένας άλλος διακομιστής αυτός του OSSEC που είναι υπεύθυνος για τη συλλογή αρχείων καταγραφής ασφαλείας από τους πράκτορα OSSEC που εκτελούνται στους διακομιστές που θέλουμε εποπτεύσουμε στο δίκτυο μας.

Για την εποπτεία των πρακτόρων OSSEC από το OSSIM θα ακολουθήσουμε την διαδρομή “Environment” → “Detection” όπου εκεί απεικονίζονται όλοι οι πράκτορες OSSEC που είναι εγκατεστημένοι στο σύστημα μας καθώς και πληροφορίες σχετικές με το αν είναι ενεργοί καθώς και την διεύθυνση IP τους. Εικόνα 7-11



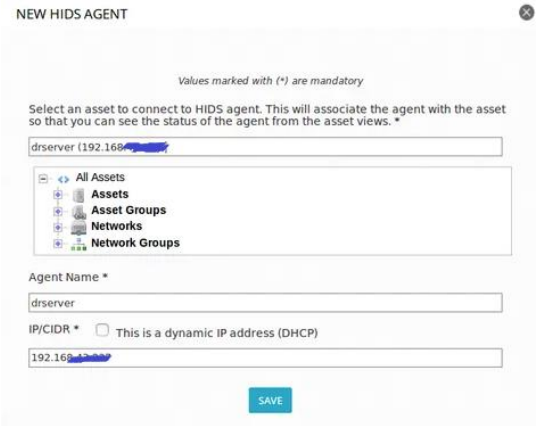
Εικόνα 7-11 Πράκτορες OSSEC

7.3.1 Εγκατάσταση του OSSEC HIDS agent σε περιβάλλον Linux

Για να μπορέσουμε να παρακολουθήσουμε οποιοδήποτε κεντρικό υπολογιστή, πρέπει να τον δηλώσουμε στον OSSIM AlienVault διακομιστή. Μόλις εισαχθεί ο κεντρικός υπολογιστής, προσθέτουμε τα HIDS για κάθε κεντρικό υπολογιστή στον διακομιστή OSSIM όπως περιγράφεται παρακάτω.

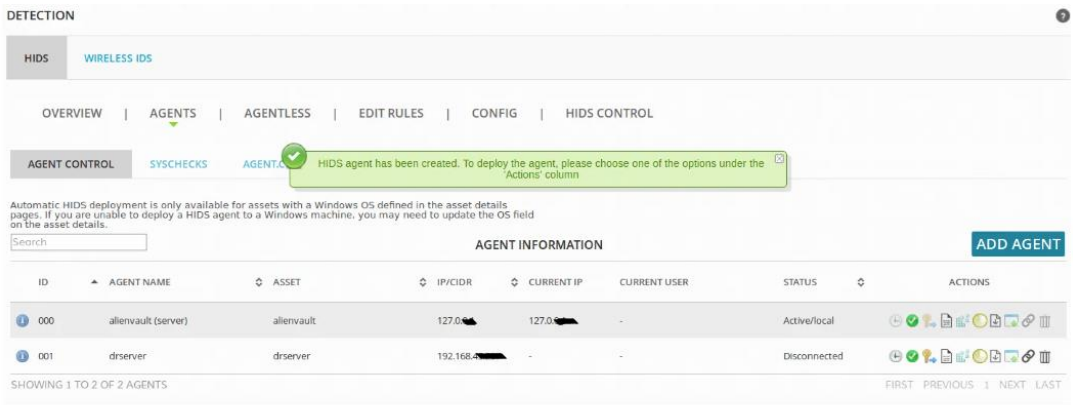
Προσθήκη των πρακτόρων HIDS στον διακομιστή OSSIM

1. Στον web διακομιστή του OSSIM μεταβαίνουμε στο
   Περιβάλλον > Ανίχνευση
2. Στην ενότητα Ανίχνευση, επιλέγουμε
   HIDS > Agents > Agent Control > Add Agent
3. Επιλέγοντας ADD Agents, ανοίγει ένα παράθυρο NEW HIDS AGENT
4. Στο NEW HIDS AGENT , εισάγουμε το όνομα κεντρικού υπολογιστή/διεύθυνση IP Εικόνα 7-12



Εικόνα 7-12 Προσθήκη πρακτόρων HIDS

5. Επιλέγουμε Save (Αποθήκευση) για να αποθηκεύσουμε τις πληροφορίες του πράκτορα. Μόλις προστεθεί ο πράκτορας, μπορούμε να δούμε τις Πληροφορίες του Πράκτορα. Για παράδειγμα, ο πράκτορας που μόλις προστέθηκε είναι ο πρώτος και έχει αναγνωριστικό 001. Εικόνα 7-13



Εικόνα 7-13 Προσθήκη 001 agent

Αφού κάνουμε login στο Linux host και κατεβάσουμε τον OSSEC HIDS agent installer, κάνουμε extract με τις ακόλουθες εντολές και στην συνέχεια εγκαθιστούμε τον ossec agent.

```
# wget https://github.com/ossec/ossec-hids/archive/3.0.0.tar.gz - P /tmp/
# cd /tmp/
# tar xzf 3.0.0.tar.gz
# cd ossec-hids-3.0.0/
# ./install.sh
```

Αφού έχουμε ξεκινήσει την εγκατάσταση του ossec-hids agent στα επόμενα βήματα αποδεχόμαστε τις προεπιλογές που αφορούν την γλώσσα, το είδος εγκατάστασης (διακομιστής, πράκτορας, τοπική, τη διεύθυνση IP του διακομιστή κ.τ.λ).
Όταν η εγκατάσταση ολοκληρωθεί με επιτυχία λαμβάνουμε τη ακόλουθη έξοδο. (Εικόνα 7-14)

```
- System is Redhat Linux.

- Init script modified to start OSSEC HIDS during boot.

- Configuration finished properly.

- To start OSSEC HIDS:

/var/ossec/bin/ossec-control start

- To stop OSSEC HIDS:

/var/ossec/bin/ossec-control stop

- The configuration can be viewed or modified at /var/ossec/etc/ossec.conf

                ...

--- Press ENTER to finish (maybe more information below). ---
```

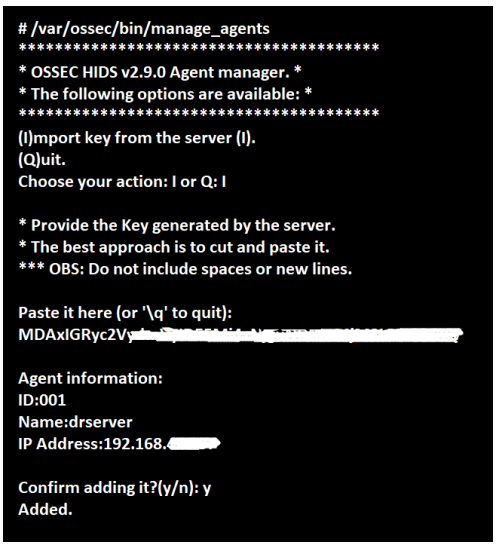
Εικόνα 7-14 Ολοκλήρωση εγκατάστασης ossec-hids agent

Μόλις τελειώσει η εγκατάσταση του agent πρέπει να εισάγουμε το κλειδί για τον agent από τον διακομιστή.

Θα συνδεθούμε στον πίνακα ελέγχου του διακομιστή και θα μεταβούμε στο Environment > Detection > HIDS > Agent και θα εξαγάγουμε το κλειδί του συγκεκριμένου agent.

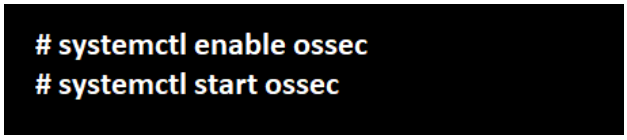
Στον server, εκτελούμε την ακόλουθη εντολή για να εισάγουμε το κλειδί,
/var/ossec/bin/manage_agents

Επιλέγουμε «*(I)mport key from the server (I)*», και επικολλούμε το κλειδί (Εικόνα 7-15).



Εικόνα 7-15 Εισαγωγή κλειδιού agent

Ολοκληρώσουμε την εγκατάσταση κάνοντας ενεργοποίηση του agent στην επανεκκίνηση. Εικόνα 7-16



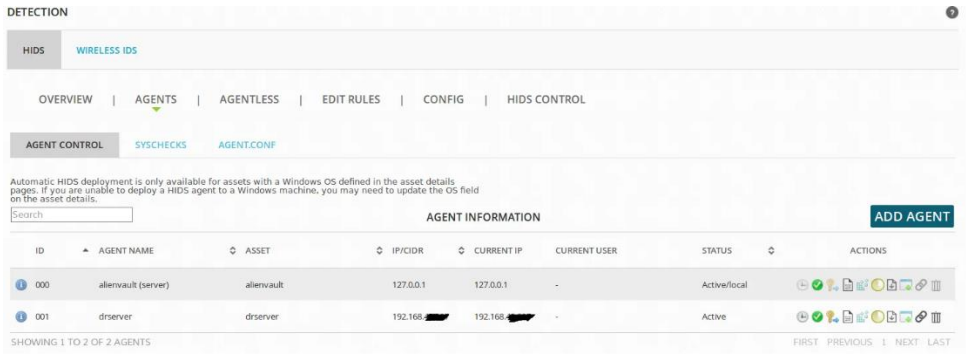
Εικόνα 7-16 Ενεργοποίηση OSSEC agent

Στο web διακομιστή του OSSIM μεταβαίνουμε στο

Environment > Detection > HIDS > HIDS Control > HIDS service is UP > RESTART

Εάν ελέγξουμε τώρα στην κατάσταση του πράκτορα θα είναι ενεργή και θα πρέπει να στέλνει logs στον OSSIM server. Εικόνα 7-17

Environment > Detection > HIDS > Agent

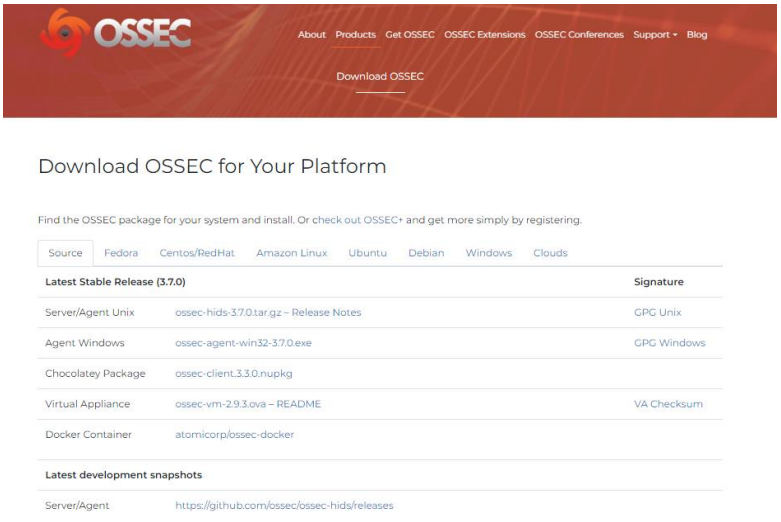


Εικόνα 7-17 Κατάσταση πράκτορα

7.3.2 Εγκατάσταση του OSSEC HIDS agent σε περιβάλλον Windows

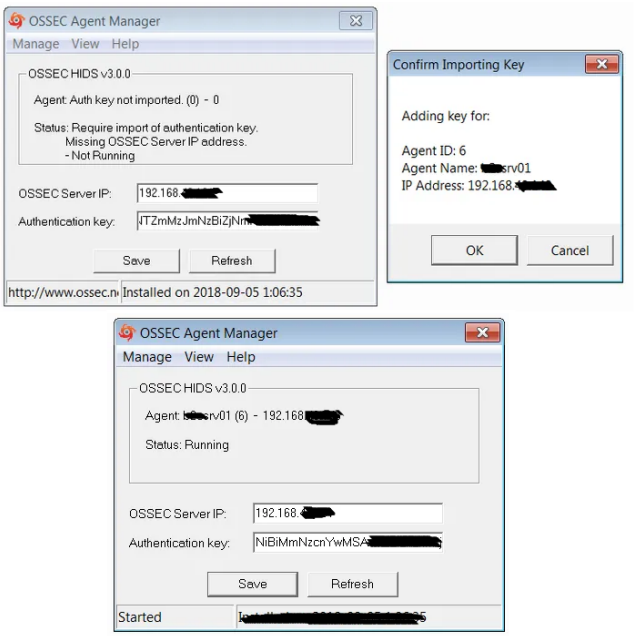
Η διαδικασία εγκατάστασης του OSSEC HIDS agent σε περιβάλλον Microsoft Windows είναι πιο σύννομη και πιο απλοποιημένη.

Αφού κάνουμε λήψη του προγράμματος εγκατάστασης από την επίσημη σελίδα της OSSEC [37] (Εικόνα 7-18), αντιγράφουμε το αρχείο εγκατάστασης στον υπολογιστή που θέλουμε να παρακολουθήσουμε τα logs.



Εικόνα 7-18 Λήψη OSSEC

Μετά την ολοκλήρωση εγκατάστασης θα μεταβούμε στον OSSEC Agent Manager, και θα εισάγουμε τη διεύθυνση IP του διακομιστή για να εξάγουμε το authentication key του agent από το διακομιστή και το επικολλούμε στον agent manager. Όταν αποθηκεύσουμε τις παραμετροποιήσεις μας εμφανίζεται το αναγνωριστικό του agent καθώς και η IP διεύθυνση η οποία θα πρέπει να συμφωνεί με αυτή του agent στον server (Εικόνα 7-19).



Εικόνα 7-19 OSSEC Agent Manager

7.4 Ενεργοποίηση Plug-ins

Αφού εκτελέσουμε την σάρωση δικτύου για να ανακαλύψουμε Assets στοιχεία, τα Assets που εντοπίστηκαν αποθηκεύονται στη βάση δεδομένων του OSSIM. Στη συνέχεια, μπορούμε να επιλέξουμε να ενεργοποιήσουμε τα plugins που εντοπίστηκαν (Εικόνα 7-20). Μπορούμε να ενεργοποιήσουμε έως και 10 plugins ανά asset. Υπάρχουν δύο τρόποι να ενεργοποιήσουμε ένα plugin:

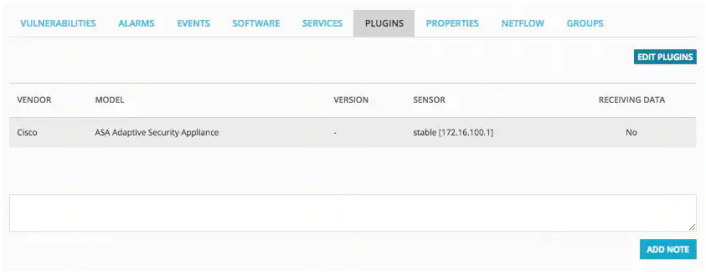
Ενεργοποίηση plugin στον αισθητήρα μέσω web ui

Για την ενεργοποίηση ενός plugin ακολουθούμε τα εξής βήματα:

1. Θα μεταβούμε στο Environment > Assets & Groups > Assets

2. Επιλέγουμε το Asset για το οποίο θέλουμε να ενεργοποιήσουμε το plugin

3. Κάνουμε edit το Plugin ( )

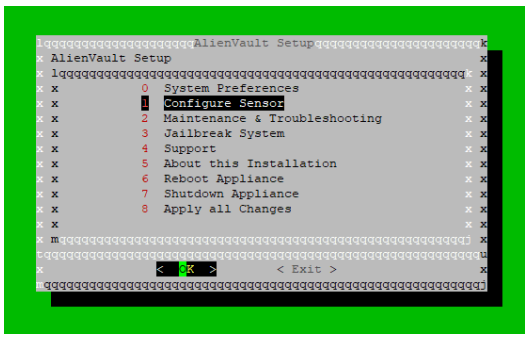


Εικόνα 7-20 Ενεργοποιήση plugin

Ενεργοποίηση plugin από την κονσόλα του **AlienVault**

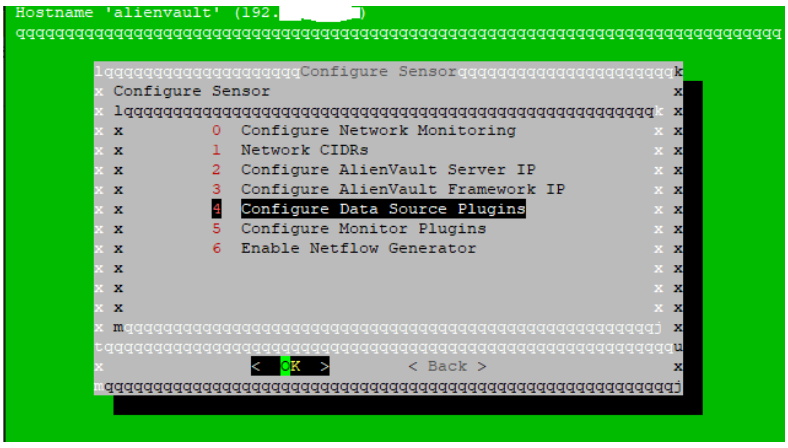
1. Συνδεόμαστε στο AlienVault Console με χρήση SSH και δίνουμε τα διαπιστευτήριά μας.

2. Επιλέγουμε «Configure Sensor» (Εικόνα 7-21)



Εικόνα 7-21 Ενεργοποίηση plugin με χρήση AlienVault Console

2. Επιλέγουμε «Configure Data Source Plugins» (Εικόνα 7-22)



Εικόνα 7-22 AlienVault Console

3. Επιλέγουμε το plugin που θέλουμε να ενεργοποιήσουμε και στην συνέχεια με την επιλογή back και Apply all Changes ολοκληρώνουμε την διαδικασία

7.5 Διαχείριση Πολιτικών & Alerting

Οι λύσεις SIEM συσσωρεύουν πολλές πληροφορίες από τις συσκευές οι οποίες είναι υπό παρακολούθηση, με αποτέλεσμα να έχουμε υπερπλήρωση αυτών και τελικά η παρακολούθηση του συστήματος να είναι μη διαχειρίσιμη. Με την χρήση των Πολιτικών μπορούμε να διαμορφώσουμε τον τρόπο επεξεργασίας των συμβάντων (Εικόνα 7-23). Οι πολιτικές ορίζουν μία ή περισσότερες συνθήκες που αξιολογούνται για κάθε εισερχόμενο συμβάν, προκειμένου να καθοριστεί εάν ενεργοποιείται η σχετική ενέργεια. Οι πολιτικές διαδραματίζουν κρίσιμο ρόλο στη διαχείριση της αποτελεσματικής απόκρισης συμβάντων καθώς χρησιμοποιούν συνθήκες για να καθορίσουν ποια συμβάντα επεξεργάζεται η πολιτική και συνέπειες για να καθορίσουν τι θα συμβεί όταν τα συμβάντα ταιριάζουν με τις καθορισμένες συνθήκες. [38]

Οι πολιτικές (policies) στο OSSIM φιλτράρουν τις καταγραφές ασφαλείας και στοχεύουν στην ελαχιστοποίηση των άχρηστων πληροφοριών που οδηγούν σε κορεσμό πληροφορίας. Με αυτόν τον τρόπο δημιουργούν απόθεμα πόρων του συστήματος μιας και μειώνεται ο όγκος των δεδομένων προς επεξεργασία. Κάποια παραδείγματα πολιτικών παρουσιάζονται παρακάτω:

- Αποστολή ειδοποίησης μέσω email. Μπορούμε να δημιουργήσουμε μια πολιτική για την αυτόματη ενεργοποίηση ενός μηνύματος ηλεκτρονικού ταχυδρομείου σε διαχειριστές ή άλλους, όποτε εμφανίζεται ένα υψηλού κινδύνου συμβάν.

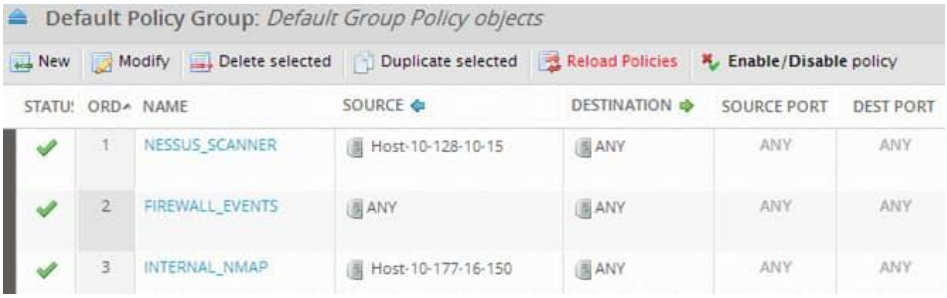
- Να ορίσουμε πόσο επικίνδυνο είναι ένα συμβάν. Για μια συγκεκριμένη διεύθυνση IP ή μια συγκεκριμένη θύρα, μπορούμε να χρησιμοποιήσουμε πολιτικές για τη δημιουργία allerting κάθε φορά που εμφανίζονται συμβάντα που περιλαμβάνουν τη συγκεκριμένη διεύθυνση IP, χωρίς να γράψουμε κάποιον κανόνα συσχέτισης.

- Δημιουργία πολιτικής για την απόρριψη συμβάντων .. Μπορούμε να αποφύγουμε την αποθήκευση ορισμένων συμβάντων π.χ. συμβάντα τείχους προστασίας, για εξοικονόμηση χώρου.

- Αποθήκευση συμβάντων χωρίς συσχέτιση, Γενικά, θα πρέπει πάντα να επιτρέπετε η συσχέτιση συμβάντων, αλλά μπορούμε έχουμε αυτήν την δυνατότητα σε περίπτωση π.χ. που έχουμε ένα honeypot στο δίκτυό μας, δεν χρειάζεστε το OSSIM Appliance να δημιουργήσει alert για αυτό.

- Συσχέτηση συμβάντων και προώθηση σε άλλο OSSIM διακομιστή χωρίς να τα αποθήκευση. Για παράδειγμα, μπορούμε να συσχετίσουμε συμβάντα σε έναν θυγατρικό διακομιστή και να τα προωθήσετε σε έναν υψηλότερου επιπέδου διακομιστή, για πρόσθετη συσχέτιση ή αποθήκευση.

- Μείωση ψευδών συναγερμών. Καθώς συλλέγουμε περισσότερα συμβάντα από διαφορετικά εξωτερικά συστήματα, ενδέχεται να αντιμετωπίσουμε ένα σενάριο που παράγει περισσότερους συναγερμούς από αυτούς που θα θέλαμε. Μπορούμε να χρησιμοποιήσετε τέτοιου είδους πολιτικές για να φιλτράρουμε τα συμβάντα και να μειώσουμε τον αριθμό των συναγερμών που δημιουργούνται. [38]



Εικόνα 7-23 Πολιτικές & Alerting [39]

7.5.1 Κατασκευή πολιτικών

Η AlienVault δίνει την δυνατότητα στον διαχειριστή να δημιουργήσει προσαρμοσμένες πολιτικές, επιτρέποντάς του έτσι να ενεργοποιήσει μία ή περισσότερες από τις ακόλουθες ενέργειες έναντι αυτών των πολιτικών.

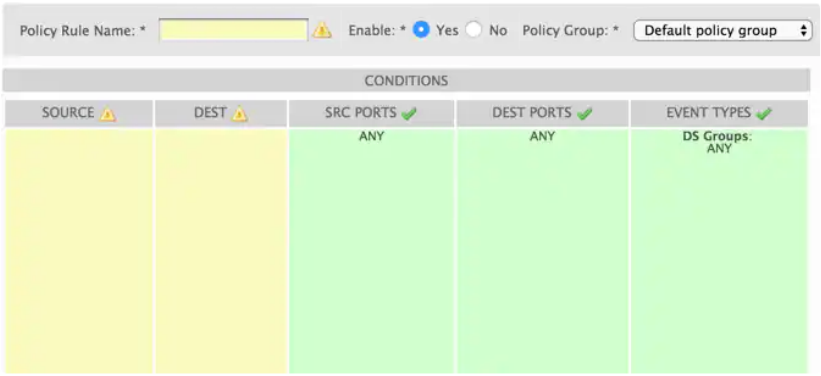
1. Ανοίξτε ένα εισιτήριο (Open a ticket)
2. Ηλεκτρονική διεύθυνση (Email)
3. Εκτέλεση σεναρίων (Run scripts)

Για να δημιουργήσουμε μια πολιτική θα μεταβούμε στο Configuration > Threat Intelligence > Policy .

Εάν θέλουμε να δημιουργήσετε μια πολιτική για ένα εξωτερικό συμβάν, κάνουμε κλικ στην επιλογή *New* στην *Default Policy Group*.

Εάν θέλουμε να δημιουργήσουμε μια πολιτική για ένα συμβάν συστήματος, κάνουμε κλικ στο *New* στις *Policies for Events Generated in Server*.

Εισάγουμε ένα όνομα στη Πολιτική (*Policy Configuration page*) (Εικόνα 7-24).



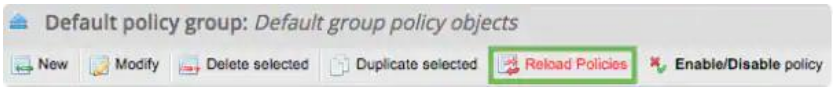
Εικόνα 7-24 Δημιουργία πολιτικής

Ορίζουμε τις συνθήκες που θέλουμε για τα συμβάντα.

Διαμορφώνουμε τις παραμέτρους όταν τα συμβάντα ταιριάζουν με τις συνθήκες.

Κάνουμε κλικ στην Ενημέρωση πολιτικής. (*Update Policy*)

Κάνουμε κλικ στην επιλογή Επανάληψη φόρτωσης πολιτικών (*Reload Policies*). (Εικόνα 7-25).



Εικόνα 7-25 Πολιτικές & Alerting

7.5.2 Κατασκευή αντιδράσεων

Μπορούμε να δημιουργήσουμε ενέργειες σε περίπτωση ενός συμβάντος ασφαλείας. Τέτοιες ενέργειες είναι η αποστολή email, η εκτέλεση ενός σεναρίου ή το άνοιγμα ενός ticket. Ένα τέτοιο παράδειγμα θα μπορούσε να είναι "Όταν συμβεί μια επίθεση κατά της IP 192.168.1.1, να σταλεί ένα email στον διαχειριστή. [40]

Για να διαμορφώσουμε μια ενέργεια

Κάνουμε κλικ στο *Configure* > *Threat Intelligence* > *Actions* , και επιλέγουμε *New* .

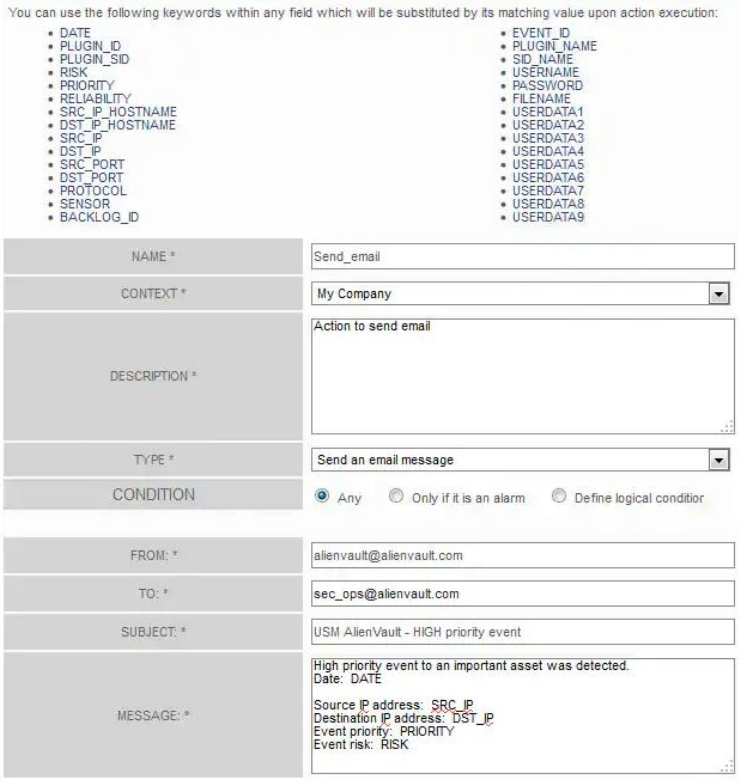
Πληκτρολογούμε το όνομα της ενέργειας (*Action).*

Από τη λίστα πλαισίου, επιλέγουμε το πλαίσιο κάτω από το οποίο θα πρέπει να εκτελεστεί η ενέργεια.

Στο πεδίο Περιγραφή , κάνουμε κλικ σε οποιεσδήποτε ισχύουσες λέξεις-κλειδιά στο επάνω μέρος της σελίδας για να τις προσθέσουμε αυτόματα στο πεδίο.

Για παράδειγμα, εάν θέλουμε να δημιουργήσουμε μια ενέργεια για να στέλνει ένα μήνυμα ηλεκτρονικού ταχυδρομείου στον διαχειριστή, θα μπορούσαμε να συμπεριλάβουμε

πληροφορίες από το κανονικοποιημένο συμβάν στο μήνυμα ηλεκτρονικού ταχυδρομείου, όπως SRC_IP, DST_IP, PRIORITY και RISK. (Εικόνα 7-26)



Εικόνα 7-26 Δημιουργία Ενέργειας (create action) [40]

Από τη λίστα Τύπος, επιλέγουμε την επιθυμητή ενέργεια.

Οι επιλογές περιλαμβάνουν:

- Στείλτε ένα μήνυμα ηλεκτρονικού ταχυδρομείου
- Εκτελέστε ένα εξωτερικό πρόγραμμα μέσω ενός σεναρίου.
- Ανοίξτε ένα εισιτήριο

Στο πεδίο *Conditions* , επιλέγουμε κάτω υπό ποια συνθήκη θα πρέπει να ενεργοποιηθεί η ενέργεια:

Οι επιλογές περιλαμβάνουν:

- Οποιοδήποτε (*Any*)
- Μόνο εάν υπάρχει συναγερμός (*Only if it is an alarm*)
- Ορισμός λογικής συνθήκης (*Only if it is an alarm*)

Για να στείλει το OSSIM ένα μήνυμα ηλεκτρονικού ταχυδρομείου:

- Στο πεδίο FROM , πληκτρολογούμε τη διεύθυνση email από την οποία αποστέλλεται το μήνυμα

- Στο πεδίο ΠΡΟΣ , πληκτρολογούμε τη διεύθυνση email στην οποία θα στείλει το μήνυμα

- Στο πεδίο Θέμα , πληκτρολογούμε ένα θέμα για το email

- Στο πεδίο Μήνυμα , πληκτρολογούμε το περιεχόμενο του email.

7.6 Παρουσίαση OSSIM

Σκοπός της ενότητας αυτής είναι να παρουσιάσει μια ολοκληρωμένη εικόνα του εργαλείου AlienVault OSSIM, εμπεριέχοντας τα μέρη που την αποτελούν, τη μεθοδολογία εγκατάστασης, καθώς επίσης και τις επιλογές παραμετροποίησης. Στόχος του κεφαλαίου αυτού είναι πως το AlienVault OSSIM προσφέρει στον διαχειριστή την ικανότητα να αντιλαμβάνεται έγκαιρα τις δικτυακές επιθέσεις που μπορεί να λάβουν χώρα στα υπό την εποπτεία του δίκτυα.[41]

7.6.1 Εργαλεία του OSSIM

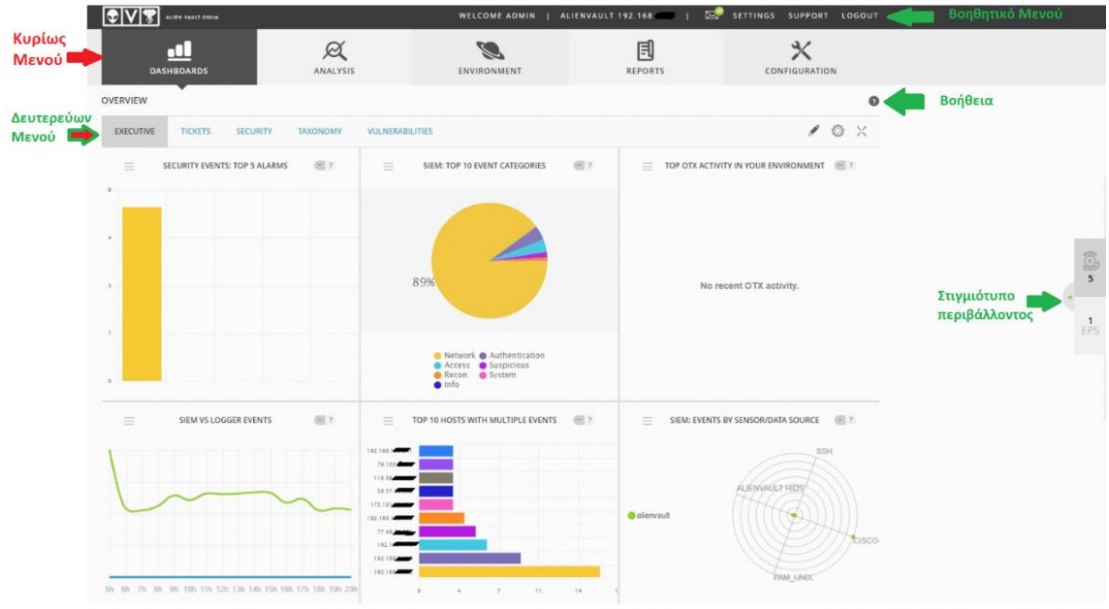
Το AlienVault OSSIM παρέχει πρόσβαση σε όλα τα εργαλεία και τις δυνατότητες που διαθέτει το OSSIM για τη διαχείριση της ασφάλειας του δικτύου, των υπολογιστών και άλλων συσκευών του οργανισμού. Με το OSSIM, μπορούμε να δούμε όλες τις βασικές πληροφορίες σχετικά με τις συσκευές δικτύου, τις εφαρμογές, τη δραστηριότητα των χρηστών και την κίνηση δικτύου στο περιβάλλον μας. Καθώς παρακολουθούμε πληροφορίες που έρχονται από συσκευές, μπορούμε να ορίσουμε και να βελτιώσουμε τις πολιτικές και τις οδηγίες συσχέτισης για να ρυθμίσουμε με ακρίβεια τη συμπεριφορά του συστήματος OSSIM ώστε να μας ειδοποιεί για πιθανά ζητήματα ασφάλειας και ευπάθειες.

Το OSSIM εκτελείται σε ένα τυπικό πρόγραμμα περιήγησης ιστού. Ο διαχειριστής του συστήματός αφού πληκτρολογήσει τη διεύθυνση URL του ιστού και υποβάλει τα διαπιστευτήριά του μπορεί να συνδεθεί και να συγκεντρώσει καταγραφές ασφαλείας από πολλές γνωστές δικτυακές συσκευές, να επεξεργαστεί τις καταγραφές αυτές που στη συνεχεία μπορεί να τα χρησιμοποιήσει για την εξαγωγή συμπερασμάτων στη λειτουργία ασφαλείας του οργανισμού του.

Όταν συνδεθούμε στο OSSIM εμφανίζεται η σελίδα του Πίνακα Εργαλείων (Executive Dashboard) > Επισκόπηση (OVERVIEW).

Η προεπιλεγμένη Επισκόπηση του OSSIM εμφανίζει διάφορα "γραφικά στοιχεία" (γραφήματα, πίνακες) που συνοψίζουν διάφορες πτυχές της ασφάλειας του δικτύου και άλλες δραστηριότητες και συμβάντα που συμβαίνουν στο δίκτυό μας.

Τα επεξηγηματικά βέλη στην (Εικόνα 7-27) που ακολουθεί προσδιορίζουν τα κύρια στοιχεία πλοήγησης και τις επιλογές που παρέχονται στον χρήστη.



Εικόνα 7-27 OSSIM Dashboard

- **Κύριο μενού** — Παρέχει πρόσβαση στις κύριες λειτουργίες του OSSIM όπως:

Πίνακες εργαλείων (Dashboards) — Εμφάνιση όλων των διαγραμμάτων, πινάκων και γραφημάτων ασφαλείας δικτύου. Κατάσταση δικτύου και συσκευών που είναι συνδεδεμένες. Οπτικοποιήσεις απειλών και παλμών OTX .

Ανάλυση (Analysis) — Παρέχει αναζήτηση, ταξινόμηση, επιλογή φιλτραρίσματος και εμφάνιση συναγερμών, συμβάντων ασφαλείας (SIEM).

Περιβάλλον (Environment) — Παρέχει εμφάνιση και διαχείριση Assets&Groups ευπάθειας, δεδομένων, NetFlow, Traffic Capture, διαθεσιμότητας και ανίχνευσης.

Αναφορές (Reports) — Παρέχει εμφάνιση και διαχείριση διαφόρων ενσωματωμένων και προσαρμοσμένων αναφορών με δυνατότητα επιλογής ανά κατηγορίες όπως συναγερμοί, στοιχεία, συμμόρφωση, πρωτογενή αρχεία καταγραφής και λειτουργίες ασφαλείας.

Παραμετροποίηση (Configuration) — Παρέχει επιλογές για την προβολή και τη διαχείριση των αναπτυγμένων στοιχείων ossim. Οι επιλογές διαχείρισης μάς επιτρέπουν να διαχειριζόμαστε τους χρήστες, τη διαμόρφωση του συστήματος και τη δημιουργία αντιγράφων ασφαλείας και επαναφορά ρυθμίσεων.

- **Δευτερεύων μενού** —Για κάθε επιλογή του πρωτεύοντος μενού, υπάρχουν συνήθως πρόσθετες επιλογές για το συγκεκριμένο θέμα, που εμφανίζονται όταν κάνουμε κλικ στην κύρια επιλογή, για παράδειγμα, Analysis > Alarms.

- **Βοήθεια** — σύνδεσμοι προς ηλεκτρονική τεκμηρίωση και θέματα που σχετίζονται με την τρέχουσα προβολή και το περιεχόμενο.

- **Στιγμιότυπο περιβάλλοντος** — Η οθόνη πλευρικής γραμμής εμφανίζεται στη δεξιά πλευρά του OSSIM. Χωρίς επέκταση, η οθόνη εμφανίζει τους τρέχοντες συναγερμούς και τον τρέχοντα ρυθμό συμβάντων ανά δευτερόλεπτο (EPS). Μπορούμε να κάνουμε κλικ στην καρτέλα Στιγμιότυπο περιβάλλοντος για να επεκτείνουμε την οθόνη και να εμφανιστούν περισσότερες πληροφορίες σχετικά ενεπίλυτους συναγερμούς, την υγεία του συστήματος, τη τελευταία δραστηριότητα σε συμβάντα και τον αριθμό των συσκευών που παρακολουθούνται.

8

Μελέτη περίπτωσης σε έναν εικονικό δημόσιο οργανισμό

Στο προηγούμενο κεφάλαιο αναπτύξαμε το AlienVault OSSIM στους διακομιστές ενός εικονικού δημόσιου φορέα. Στην ενότητα που ακολουθεί θα γίνει η παρουσίαση του εργαλείου AlienVault OSSIM στην μελέτη εφαρμογής που πραγματοποιήθηκε σε έναν δημόσιο φορέα.

Θα γίνει παρουσίαση του κεντρικού πίνακα ελέγχου (Dashboard) του συστήματος και θα περιηγηθούμε σε μερικές ενδιαφέρουσες λειτουργίες που μας προσφέρει.

8.1 Πίνακας εργαλείων του OSSIM (Dashboard)

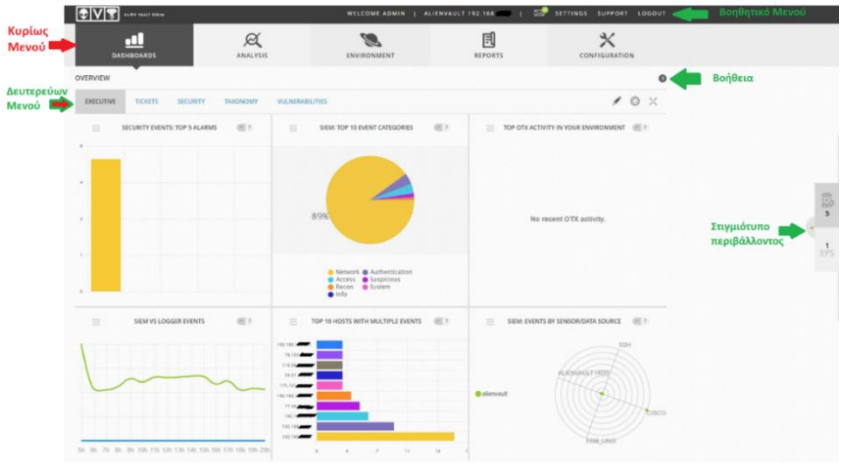
Το AlienVault OSSIM παρέχει όλα εκείνα τα εργαλεία και τις δυνατότητες για τη διαχείριση της ασφάλειας του δικτύου, των υπολογιστών και άλλων συσκευών του οργανισμού. Με το OSSIM, μπορούμε να δούμε όλες τις βασικές πληροφορίες σχετικά με τις συσκευές δικτύου, τις εφαρμογές, τη δραστηριότητα των χρηστών και την κίνηση δικτύου στο περιβάλλον μας. Καθώς παρακολουθούμε πληροφορίες που έρχονται από συσκευές, μπορούμε να ορίσουμε και να βελτιώσουμε τις πολιτικές και τις οδηγίες συσχέτισης για να ρυθμίσουμε με ακρίβεια τη συμπεριφορά του συστήματος OSSIM ώστε να μας ειδοποιεί για πιθανά ζητήματα ασφάλειας και ευπάθειες.

Το OSSIM εκτελείται σε ένα τυπικό πρόγραμμα περιήγησης ιστού. Ο διαχειριστής του συστήματός αφού πληκτρολογήσει τη διεύθυνση URL του ιστού και υποβάλει τα διαπιστευτήριά του μπορεί να συνδεθεί και να συγκεντρώσει καταγραφές ασφαλείας από πολλές γνωστές δικτυακές συσκευές, να επεξεργαστεί τις καταγραφές αυτές που στη συνεχεία μπορεί να τα χρησιμοποιήσει για την εξαγωγή συμπερασμάτων στη λειτουργία ασφαλείας του οργανισμού του.

Όταν συνδεθούμε στο OSSIM εμφανίζεται η σελίδα του Πίνακα Εργαλείων (Executive Dashboard) > Επισκόπηση (OVERVIEW).

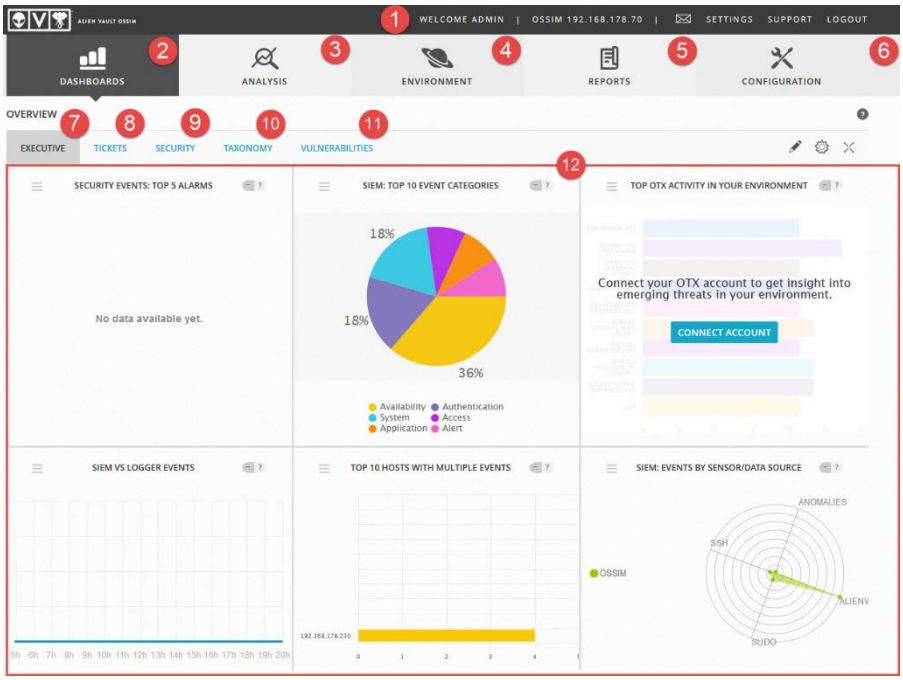
Η προεπιλεγμένη Επισκόπηση του OSSIM εμφανίζει διάφορα "γραφικά στοιχεία" (γραφήματα, πίνακες) που συνοψίζουν διάφορες πτυχές της ασφάλειας του δικτύου και άλλες δραστηριότητες και συμβάντα που συμβαίνουν στο δίκτυό μας.

Τα επεξηγηματικά βέλη στην (Εικόνα 8-1) που ακολουθεί προσδιορίζουν τα κύρια στοιχεία πλοήγησης και τις επιλογές που παρέχονται στον χρήστη.



Εικόνα 8-1 Πίνακας ελέγχου OSSIM

Ας ρίξουμε μια πιο προσεκτική ματιά στα συγκεκριμένα μέρη του OSSIM: (Εικόνα 8-2)



Εικόνα 8-2 OSSIM Dashboard

1. Βοηθητικό μενού

Στο βοηθητικό μενού βρίσκουμε μια σειρά από επιλογές, όπως τις βασικές ρυθμίσεις του συστήματός μας, το κουμπί αποσύνδεσης, τη διεύθυνση IP του διακομιστή OSSIM και όλα τα μηνύματα. Μέσω των ρυθμίσεων μπορούμε κυρίως να διαμορφώσουμε τις ρυθμίσεις χρήστη και να προβάλουμε τις τρέχουσες περιόδους σύνδεσης.

2. Dashboard

Κάτω από τους πίνακες εργαλείων μπορείτε να βρείτε διάφορους χρήσιμους πίνακες εργαλείων που παρέχουν περισσότερες πληροφορίες σχετικά με την τρέχουσα κατάσταση ανάπτυξης, τους κινδύνους, τα περιστατικά και οπτικοποιήσεις απειλών και παλμών OTX. Οι πίνακες εργαλείων μπορούν να ρυθμιστούν πλήρως σύμφωνα με τις δικές απαιτήσεις.

3. Analysis

Αυτή η καρτέλα "Analytics" παρέχει περισσότερες πληροφορίες σχετικά με τις ειδοποιήσεις που δημιουργούνται (συναγερμοί), τα τρέχοντα tickets και τα συμβάντα ασφαλείας. Όλα αυτά τα δεδομένα φιλτράρονται εύκολα, έτσι ώστε να μπορούν να βρεθούν εύκολα συγκεκριμένα συμβάντα.

4. Environment

Παρέχει εμφάνιση και διαχείριση Assets&Groups ευπάθειας, δεδομένων, NetFlow, Traffic Capture, διαθεσιμότητας και ανίχνευσης.

5. Reports

Παρέχει εμφάνιση και διαχείριση διαφόρων ενσωματωμένων και προσαρμοσμένων αναφορών με δυνατότητα επιλογής ανά κατηγορίες όπως συναγερμοί, στοιχεία, συμμόρφωση, πρωτογενή αρχεία καταγραφής και λειτουργίες ασφαλείας.

6. Configuration

Παρέχει επιλογές για την προβολή και τη διαχείριση των αναπτυγμένων στοιχείων ossim. Οι επιλογές διαχείρισης μάς επιτρέπουν να διαχειριζόμαστε τους χρήστες, τη διαμόρφωση του συστήματος και τη δημιουργία αντιγράφων ασφαλείας και επαναφορά ρυθμίσεων.

7, 8, 9, 10 & 11. Πίνακες εργαλείων

Παρέχει γρήγορη πρόσβαση σε διάφορα στοιχεία, όπως στατιστικά σχετικά με τα τρέχοντα tickets, taxonomy και ευπάθειες.

12. Πίνακας οργάνων.

Παρέχει επιλογές για την προβολή διαγραμμάτων, πινάκων και γραφημάτων ασφαλείας δικτύου. Κατάσταση δικτύου και συσκευών που είναι συνδεδεμένες. Οπτικοποιήσεις απειλών και παλμών OTX .

8.1.1 Ανάλυση συναγερμών, συμβάντων και αρχείων καταγραφής

Το OSSIM μας δίνει την δυνατότητα να εξετάζουμε και να αναλύουμε την ασφάλεια δικτύου χρησιμοποιώντας διάφορες επιλογές που παρέχονται στο μενού Ανάλυση (Analysis) στο κυρίως μενού.

Το μενού Ανάλυση (Analysis) παρέχει τις ακόλουθες επιλογές:

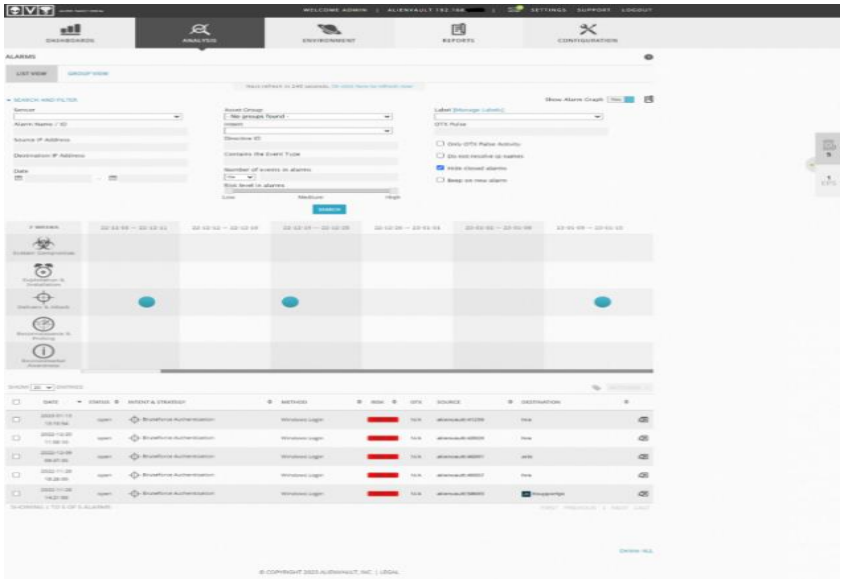
Alarms — Εμφανίζει όλους τους συναγερμούς που δημιουργούνται στο OSSIM. (Οποιοδήποτε συμβάν με υπολογισμένη τιμή κινδύνου 1 ή μεγαλύτερη παράγει έναν συναγερμό.) Μπορούμε επίσης να αναζητήσουμε συναγερμούς χρησιμοποιώντας φίλτρα.

Συμβάντα ασφαλείας (SIEM) — Εμφανίζει όλα τα συμβάντα που υποβλήθηκαν σε επεξεργασία ή δημιουργήθηκαν από τον διακομιστή συσκευών USM. Μας δίνει επίσης την δυνατότητα να αναζητήσουμε και να φιλτράρουμε συμβάντα που εμφανίζονται στην οθόνη, καθώς και να προβάλουμε λεπτομέρειες συγκεκριμένων συμβάντων.

Raw Logs — Παρέχει πρόσβαση και εμφανίζει όλα τα συμβάντα που αποθήκευσε το OSSIM Logger σε log αρχεία καταγραφής, για μακροπρόθεσμη αποθήκευση και περαιτέρω διερεύνηση. Το OSSIM Logger υπογράφει και σφραγίζει ψηφιακά τα αρχειοθετημένα αρχεία καταγραφής, για να διασφαλίσει την ακεραιότητά τους και να εγγυηθεί, για την αναφορά συμμόρφωσης, ότι τα δεδομένα στα αρχεία καταγραφής δεν έχουν παραβιαστεί.

Tickets —Τα Ticket παρέχουν παρακολούθηση της ροής εργασιών της δραστηριότητας που σχετίζεται με εντοπισμένους συναγερμούς ή άλλα ζητήματα που θέλουμε να παρακολουθήσουμε.

Όταν επιλέγουμε από το μενού ANALYSIS>ALARMS, εμφανίζεται η ακόλουθη σελίδα. (Εικόνα 8-3)



Εικόνα 8-3 Πίνακας ελέγχου ANALYSIS

Στην σελίδα αυτή μπορούμε να δούμε τους συναγερμούς με αντίστροφη χρονολογική σειρά (πρώτος εμφανίζεται ο πιο πρόσφατος συναγερμός).

Το μεσαίο τμήμα της οθόνης περιλαμβάνει έναν πίνακα που παρέχει μια γραφική συγκεντρωτική αναπαράσταση των συναγερμών που εμφανίστηκαν τις τελευταίες 31 ημέρες. Οι μπλε κύκλοι υποδεικνύουν το πλήθος εμφάνισης ενός συναγερμού ανά κατηγορία συναγερμών. Ένας μεγαλύτερος κύκλος υποδηλώνει ότι εμφανίστηκε μεγαλύτερος αριθμός συναγερμών. Μπορούμε να τοποθετήσουμε το ποντίκι πάνω από κάθε έναν από τους κύκλους για να λάβουμε τον πραγματικό αριθμό διαφορετικών τύπων συμβάντων, καθώς και μια λίστα των κορυφαίων 5 συμβάντων με πιθανές λύσεις για κάθε τύπο συναγερμού.

Οι συναγερμοί ταξινομούνται σε πέντε διαφορετικές κατηγορίες, οι οποίες αντιπροσωπεύονται από τα γραφικά εικονίδια στην (Εικόνα 8-4)

Εικόνα 8-4 Τύποι συναγερμών

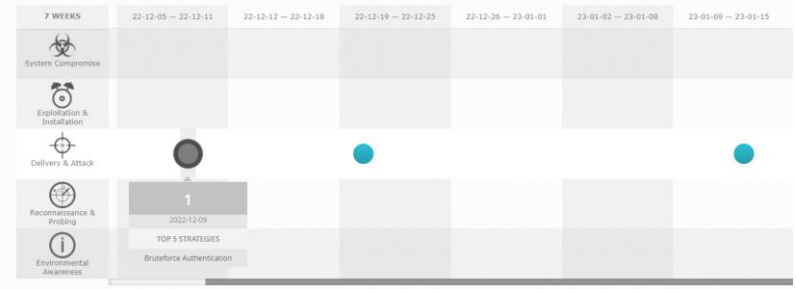
Οι τύποι των συναγερμών είναι κατηγοριοποιημένοι βάση της τακτικής που μπορεί να ακολουθήσει ένας εισβολέας για να διεισδύσει επιτυχώς σε ένα δίκτυο, να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε δεδομένα ή να εκτελέσει κάποια κακόβουλη ενέργεια. Οι τύποι συναγερμών είναι ακολουθούν ένα μοντέλο επίθεσης που περιγράφεται από τη Lockheed Martin που ονομάζεται Cyber Kill Chain.

Επιπλέον, εάν κάνουμε κλικ σε οποιονδήποτε από τους μπλε κύκλους, το OSSIM θα εμφανίσει μόνο τους συναγερμούς που αντιστοιχούν στον επιλεγμένο κύκλο. Από τη λίστα των συναγερμών, μπορούμε να κάνουμε κλικ σε οποιαδήποτε μεμονωμένη σειρά συναγερμών για να αναπτύξουμε την εμφάνιση πληροφοριών σχετικά με τον συναγερμό. Στη συνέχεια, μπορούμε να κάνουμε κλικ στο κουμπί Προβολή λεπτομερειών ( ) για να εμφανίσουμε περισσότερες πληροφορίες σχετικά με τον επιλεγμένο συναγερμό.

Το επάνω τμήμα της εμφάνισης της σελίδας Συναγερμών μάς επιτρέπει να αναζητήσουμε και να φιλτράρουμε τους συναγερμούς που επιθυμούμε. Μπορούμε να χαρακτηρίσουμε συναγερμούς με χαρακτηριστικά συμβάντων, όπως τοποθεσία αισθητήρα, ομάδα στοιχείων, επίπεδο κινδύνου ή παλμό OTX.

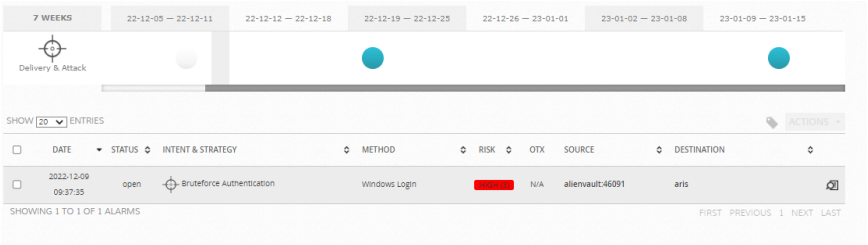
Στη μελέτη περίπτωσης που εξετάζουμε μπορούμε να δούμε ότι στη γραφική συγκεντρωτική αναπαράσταση των συναγερμών υπάρχουν 3 μπλε κύκλοι στην κατηγορία συναγερμού «Delivery & Attack» 

(Εικόνα 8-5)



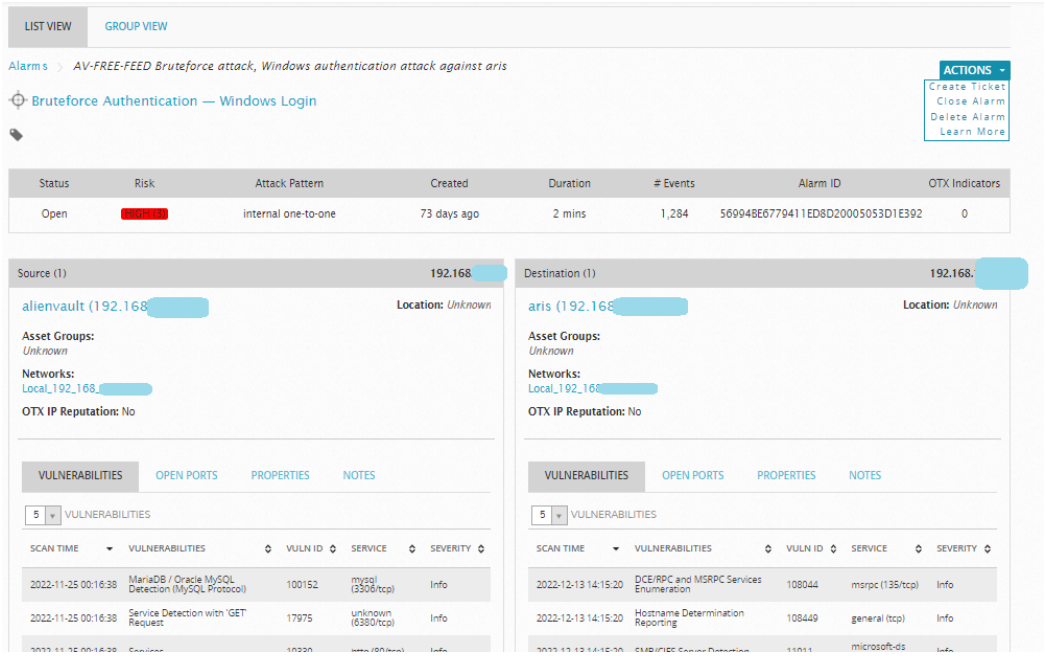
Εικόνα 8-5 Γραφική συγκεντρωτική συναγερμών

Κάνοντας κλικ επάνω σε ένα από του 3 μπλε κύκλους μας εμφανίζει την κατηγορία του συναγερμού την συγκεκριμένη χρονική περίοδο. Στο στιγμιότυπο οθόνης που ακολουθεί (Εικόνα 8-6) βλέπουμε ότι ο τύπος συναγερμού είναι «Bruteforce Authentication» και αφορά τον διακομιστή του συστήματος μας με το όνομα «ARIS»



Εικόνα 8-6 Συναγερμός Bruteforce Authentication

Κάνοντας κλικ στο κουμπί Προβολή λεπτομερειών ( ) θα να εμφανίσουμε περισσότερες πληροφορίες σχετικά με τον «Bruteforce Authentication» συναγερμό στον διακομιστή «ARIS» (Εικόνα 8-7)

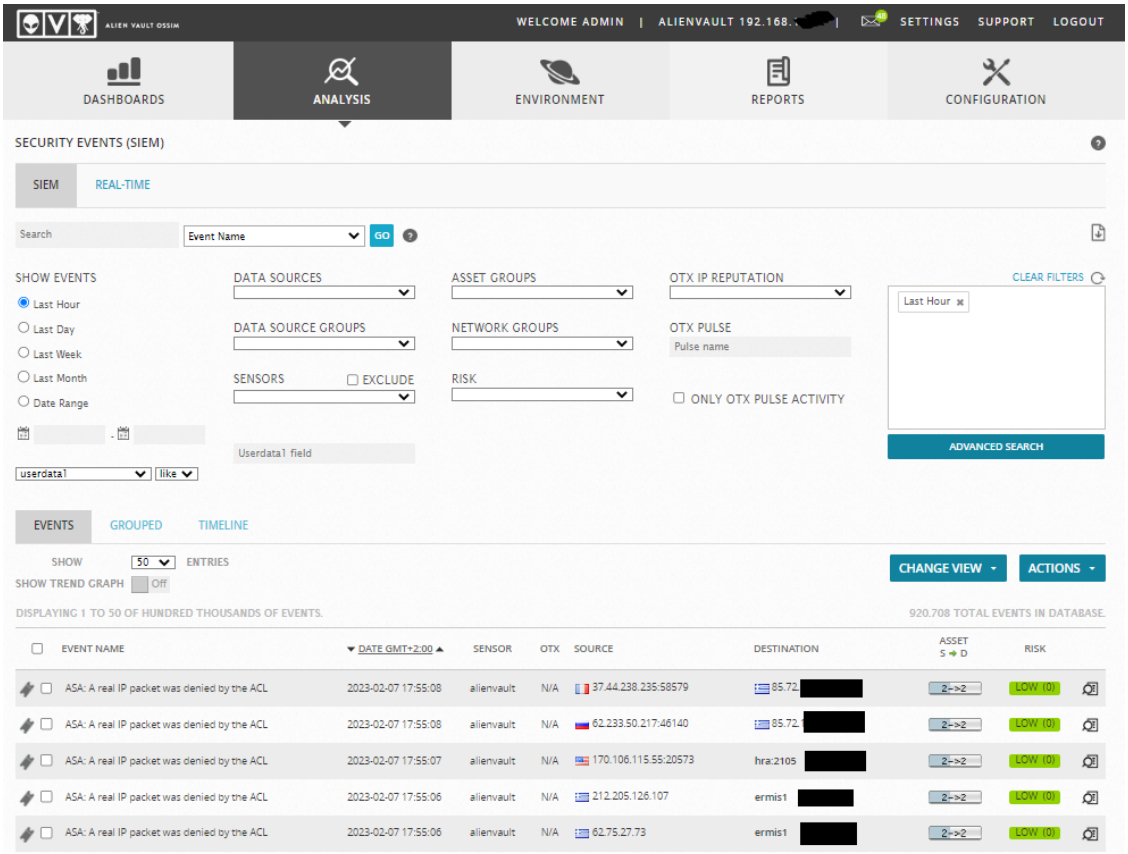


Εικόνα 8-7 Προβολή λεπτομερειών συναγερμού

Στο δεξί μέρος της οθόνης μας δίνεται η επιλογή ACTIONS με την οποία μπορούμε να δημιουργήσουμε ένα Ticket για τον συγκεκριμένο συναγερμό είτε να τον αγνοήσουμε να τον διαγράψουμε η να μάθουμε περισσότερες λεπτομέρειες για τον συγκεκριμένο συναγερμό.

8.1.2 Σελίδα συμβάντων ασφαλείας (SIEM)

Όταν επιλέγουμε από το μενού Analysis > Security Events (SIEM), εμφανίζεται η ακόλουθη σελίδα. (Εικόνα 8-8)



Εικόνα 8-8 Συμβάντα ασφαλείας (SIEM)

Από προεπιλογή, η σελίδα Συμβάντα ασφαλείας (SIEM) εμφανίζει την προβολή των συμβάντων SIEM. Το OSSIM παρέχει επίσης δύο άλλες επιλογές για την εμφάνιση συμβάντων ασφαλείας:

Σε πραγματικό χρόνο — προβολή που δείχνει τρέχον συμβάντα στο δίκτυό μας.

Εξωτερικές βάσεις δεδομένων — εμφάνιση συμβάντων ασφαλείας από μια εξωτερική βάση δεδομένων της AlienVault.

Από την SIEM προβολή, μπορούμε να αναζητήσουμε και να φιλτράρουμε συμβάντα χρησιμοποιώντας χρονικά εύρη και άλλα χαρακτηριστικά συμβάντων.

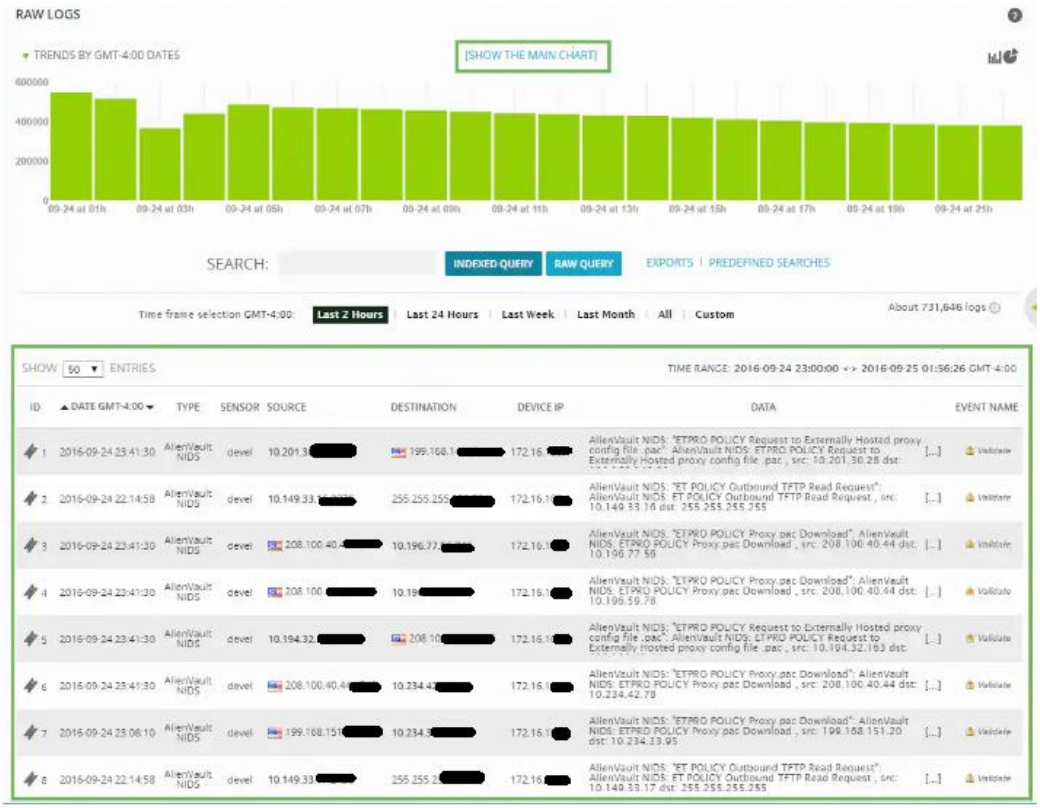
Κάτω από την ενότητα Φίλτρο αναζήτησης της σελίδας, το OSSIM παρέχει μια την δυνατότητα εμφάνισης όλων των συμβάντων. Οποιοδήποτε κανονικοποιημένο συμβάν ή οποιοδήποτε άλλο συμβάν που λαμβάνεται ή δημιουργείται από οποιονδήποτε αισθητήρα θα εμφανιστεί στην οθόνη, εκτός εάν έχουμε ενεργοποιημένη κάποια πολιτική που το φιλτράρει ή έχουμε ορίσει κριτήρια αναζήτησης.

Από τον πίνακα σύνοψης λίστα συμβάντων, μπορούμε να κάνετε κλικ σε ένα συγκεκριμένο συμβάν για να δούμε περισσότερες λεπτομέρειες σχετικά με αυτό το συμβάν σε ένα αναδυόμενο παράθυρο. Μπορούμε επίσης να κάνουμε κλικ στο εικονίδιο Περισσότερες λεπτομέρειες (🔍) για να εμφανίσουμε τις λεπτομέρειες του συμβάντος σε μια νέα σελίδα, η οποία μας επιτρέπει επίσης να επιλέξουμε περαιτέρω ενέργειες για το τρέχον συμβάν.

8.1.3 Εμφάνιση σελίδας καταγραφής ακατέργαστων αρχείων (Raw Logs)

Όταν επιλέγουμε από το μενού Analysis > Raw Logs, εμφανίζεται η ακόλουθη σελίδα.

(Εικόνα 8-9)



Εικόνα 8-9 Καταγραφή ακατέργαστων αρχείων

Σε αυτή την σελίδα μπορούμε να δούμε τα κανονικοποιημένα συμβάντα που αποθήκευσε το OSSIM Logger, Το OSSIM Logger υπογράφει και σφραγίζει ψηφιακά τα αρχειοθετημένα αρχεία καταγραφής, για να διασφαλίσει την ακεραιότητά τους και να εγγυηθεί, για την

αναφορά συμμόρφωσης, ότι τα δεδομένα στα αρχεία καταγραφής δεν έχουν παραβιαστεί. Από τη σελίδα Raw Logs, μπορούμε να κάνουμε κλικ στο εικονίδιο Validate για να επιβεβαιώσουμε ότι κάποιο συγκεκριμένο συμβάν δεν έχει τροποποιηθεί.

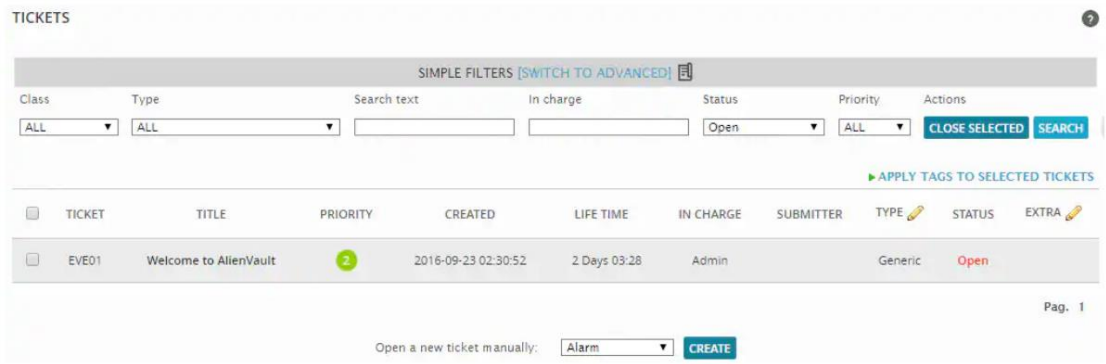
Από προεπιλογή, η σελίδα "Ακατέργαστα αρχεία καταγραφής" εμφανίζει ένα γράφημα τάσεων για συμβάντα μη επεξεργασμένων αρχείων καταγραφής, το οποίο δείχνει τον αριθμό των συμβάντων που συμβαίνουν μέσα σε ένα καθορισμένο χρονικό διάστημα. Μπορούμε να κάνουμε κλικ σε οποιαδήποτε γραμμή για να εμφανίσουμε μόνο τα συμβάντα που συνέβησαν εντός αυτού του χρονικού πλαισίου.

Το OSSIM παρέχει επίσης την επιλογή εμφάνισης του κύριου γραφήματος, η οποία παρέχει μια άλλη προβολή συμβάντων μη επεξεργασμένων αρχείων καταγραφής. Μπορούμε επίσης να κάνουμε κλικ στο εικονίδιο Προβολή γραφημάτων πίτας ( ) για να αλλάξουμε την εμφάνιση σε μια συλλογή γραφημάτων πίτας που εμφανίζουν την κατανομή των συμβάντων ανά αισθητήρα, τύπους συμβάντων, πηγές και προορισμούς.Κάτω από το γράφημα των τάσεων, μπορούμε να καθορίσουμε τη διάρκεια του χρονικού πλαισίου, όπως τις τελευταίες 2 ώρες, τις τελευταίες 24 ώρες ή την προηγούμενη εβδομάδα.

8.1.4 Εμφάνιση σελίδας Tickets

Όταν επιλέγουμε από το μενού Analysis > Tickets, εμφανίζεται η ακόλουθη σελίδα.

(Εικόνα 8-10)



Εικόνα 8-10 Σελίδα Tickets

Τα Tickets παρέχουν παρακολούθηση της ροής εργασιών της δραστηριότητας που σχετίζεται με εντοπισμένους συναγερμούς ή άλλα ζητήματα που θέλουμε να παρακολουθούμε. Από προεπιλογή, το OSSIM εμφανίζει μια λίστα με όλα τα Tickets. Επιπλέον, μπορούμε να κάνετε κλικ στο κουμπί Δημιουργία για να δημιουργήσουμε ένα νέο Ticket συγκεκριμένου τύπου ή κατηγορίας.

Από τη λίστα σύνοψης Tickets, μπορούμε να κάνουμε κλικ σε ένα συγκεκριμένο Ticket για να το ανοίξουμε και να εμφανίσουμε όλες τις λεπτομέρειές του σε μια νέα σελίδα. Από αυτήν την

οθόνη λεπτομερειών, μπορούμε να εκτελέσουμε διάφορες ενέργειες, όπως επεξεργασία πεδίων στο Ticket, εκχώρηση, προσθήκη σημειώσεων και συνημμένων και αλλαγή της κατάστασης και της προτεραιότητας, ανάλογα με τη μέθοδο ή τη διαδικασία που θέλουμε να χρησιμοποιήσουμε για την διαλεύκανση ενός θέματος ασφάλειας.

8.1.5 Διαχείριση του Περιβάλλοντος OSSIM

Εκτός από την παρακολούθηση και την ανάλυση συμβάντων και συναγερμών, υπάρχουν και άλλες πτυχές ασφάλειας που θα πρέπει να παρακολουθούμε στο δίκτυο μας. Η επιλογή στο μενού Environment παρέχει πρόσβαση σε αυτές τις περιοχές ασφάλειας δικτύου μέσω των ακόλουθων επιλογών:

Assets & Groups — Αυτή η επιλογή σάς επιτρέπει να προβάλλετε και να διαχειρίζεστε στοιχεία, δίκτυα, ομάδες στοιχείων και ομάδες δικτύων.

Vulnerabilities — Αυτή η επιλογή μάς επιτρέπει να παρακολουθούμε και να σαρώνουμε για ευπάθειες. Η σάρωση ευπάθειας μπορεί να εκτελεστεί σε έναν ή και περισσότερους αισθητήρες AlienVault .

NetFlow — Αυτή η επιλογή μας παρέχει τη δυνατότητα παρακολούθησης του NetFlow.

Traffic Capture — Αυτή η επιλογή μας επιτρέπει να διαχειριζόμαστε την απομακρυσμένη καταγραφή κίνησης μέσω του AlienVault Sensor. Υπάρχουν πολλές επιλογές παρακολούθησης, όπως το χρονικό όριο, το μέγεθος του πακέτου, το όνομα του αισθητήρα και η πηγή και ο προορισμός του πακέτου.

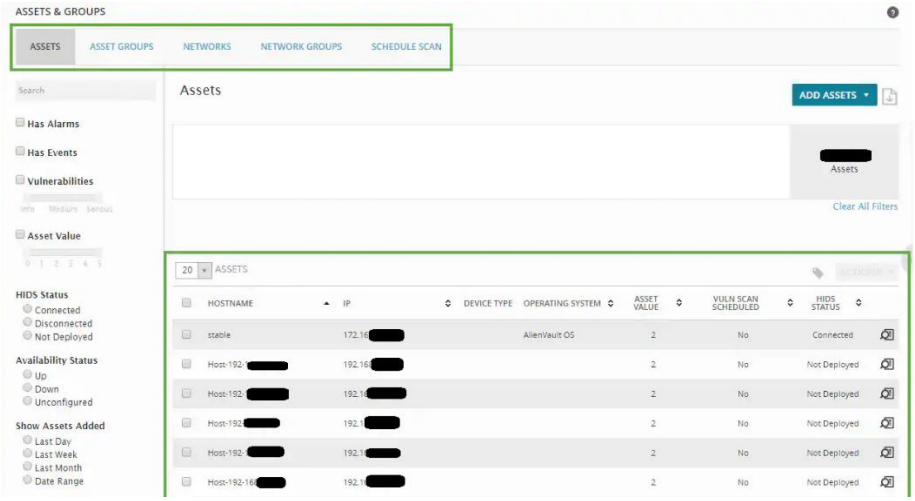
Availability — Μπορούμε να χρησιμοποιούμε αυτήν την επιλογή για να παραμετροποιήσουμε την διαθεσιμότητα παρακολούθησης.

Detection — Αυτή η επιλογή χρησιμοποιείται για τη διαχείριση της ανιχνεύσιμης εισβολής. Εμφανίζει επίσης ανάλυση αρχείων καταγραφής, έλεγχο ακεραιότητας, παρακολούθηση μητρώου των Windows, ανίχνευση rootkit, ειδοποίηση βάσει χρόνου και ενεργή απόκριση.

Reports — Εμφανίζει όλες τις διαθέσιμες αναφορές του AlienVault OSSIM και μας επιτρέπει να εκτελούμε λειτουργίες όπως Διαγραφή, Εξαγωγή, Αντιγραφή, Επεξεργασία, Προσαρμοσμένη εκτέλεση και Αναφορά Εκτέλεσης.

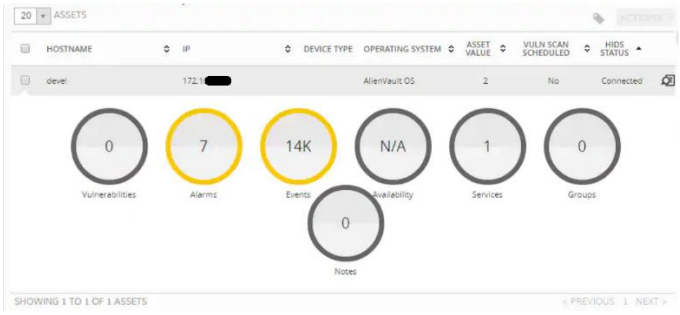
8.1.6 Εμφάνιση σελίδας Assets & Groups

Όταν επιλέγουμε μενού Environment>Assets&Groups, εμφανίζεται η ακόλουθη σελίδα. (Εικόνα 8-11)



Εικόνα 8-11 Assets & Groups

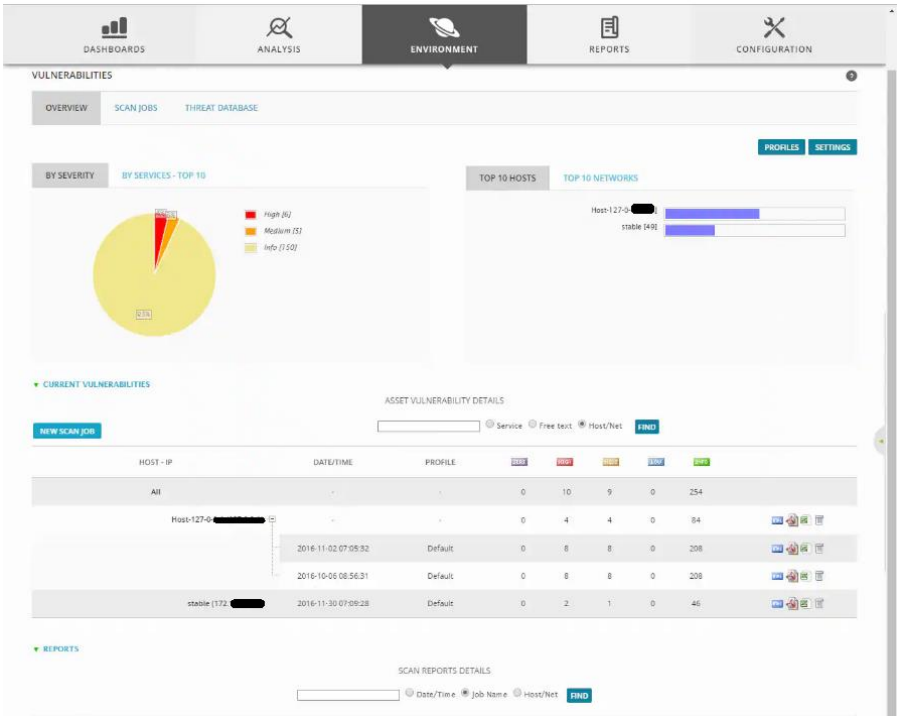
Η αρχική οθόνη Environment > Assets & Groups εμφανίζει όλα τα στοιχεία (Assets) στο δίκτυό μας, είτε αυτά προστέθηκαν με μη αυτόματο τρόπο ή δημιουργήθηκαν με χρήση της ανακάλυψης στοιχείων (Assets). Μπορούμε να κάνουμε κλικ στο κουμπί Προσθήκη στοιχείων (Assets) για να προσθέσουμε στοιχεία, όπως προσθήκη κεντρικού υπολογιστή, Εισαγωγή από CSV, Εισαγωγή από SIEM και Σάρωση για νέα στοιχεία. Μπορούμε να επιλέξουμε ένα συγκεκριμένο στοιχείο εκτελέσουμε σάρωση στοιχείων, σάρωση για ευπάθειες και ενεργοποίηση της παρακολούθησης διαθεσιμότητας (availability monitoring). Κάνοντας κλικ σε ένα συγκεκριμένο στοιχείο (Asset) στη λίστα με τα στοιχεία (Assets), επεκτείνονται οι πληροφορίες που εμφανίζονται για το επιλεγμένο στοιχείο. Αυτές περιλαμβάνουν σχετικές πληροφορίες, όπως ο αριθμός των τρωτών σημείων, οι συναγερμοί και τα συμβάντα που σχετίζονται με το στοιχείο (Asset). (Εικόνα 8-12)



Εικόνα 8-12 Πληροφορίες για ένα στοιχείο (Assets)

8.1.7 Εμφάνιση σελίδας ευπαθειών

Όταν επιλέγουμε από το μενού Environment>Vulnerabilities εμφανίζεται η ακόλουθη σελίδα. (Εικόνα 8-13)



Εικόνα 8-13 Πληροφορίες για Ευπάθειες

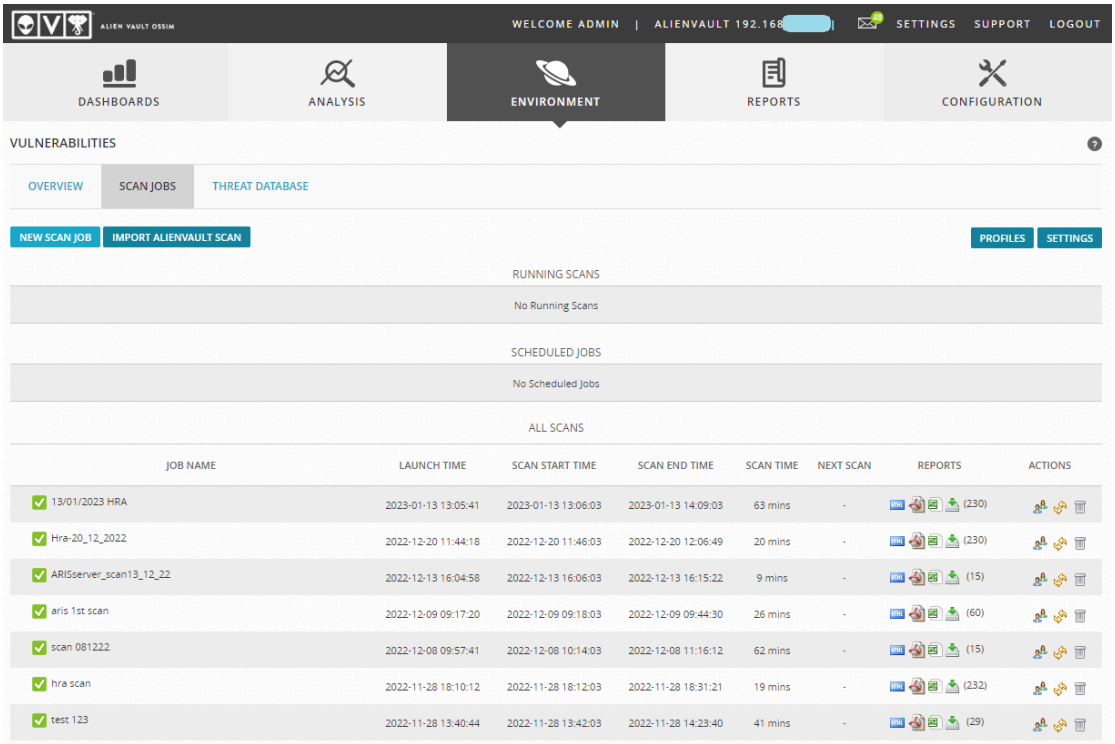
Η προεπιλεγμένη οθόνη Environment > Vulnerabilities απεικονίζει τα πιο σημαντικά τρωτά σημεία στο περιβάλλον μας. Από αυτήν την οθόνη, μπορούμε επίσης να προβάλουμε αποτελέσματα από προηγούμενες σαρώσεις ευπάθειας στοιχείων (σε HTML ή PDF) μορφή ή να προγραμματίσουμε μια νέα εργασία σάρωσης.

Εκτός από την οθόνη Επισκόπησης ευπαθειών (**Overview**), OSSIM παρέχει επίσης τις ακόλουθες επιλογές:

Εργασίες σάρωσης (**Scan Jobs**) — Παρέχει τη δυνατότητα προβολής σαρώσεων σε εξέλιξη, εισαγωγής αναφορών σάρωσης αξιολόγησης ευπάθειας και δημιουργία ή προγραμματισμό νέων εργασιών σάρωσης.

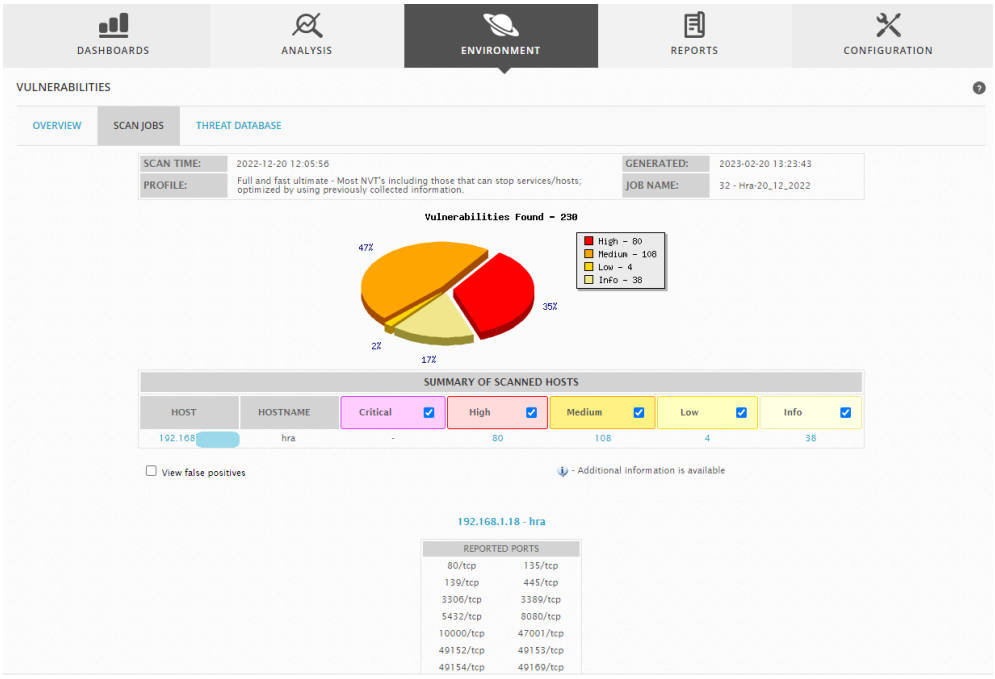
Βάση δεδομένων απειλών (**Threat Database**) — Παρέχει τη δυνατότητα αναζήτησης και εμφάνισης τρεχουσών απειλών.

Στη μελέτη περίπτωσης που εξετάζουμε μπορούμε να δούμε στην Εικόνα 8-14 τις εργασίες σάρωσης (scan jobs) που εκτελέσαμε.



Εικόνα 8-14 Εργασίες σάρωσης (scan jobs)

Κάνοντας κλικ πάνω σε μία εργασία σάρωσης (scan jobs) π.χ. «Hra-20_12_2022» που αφορά την σάρωση που πραγματοποιήθηκε στις 20-12-2022 στον διακομιστή «HRA» θα να εμφανίσουμε περισσότερες πληροφορίες σχετικά με την συγκεκριμένη σάρωση.(Εικόνα 8-15) Καθώς και αναλυτικές πληροφορίες και προτεινόμενες λύσεις για την κάθε ευπάθεια που συγκέντρωσε κατά την σάρωση. (Εικόνα 8-16)



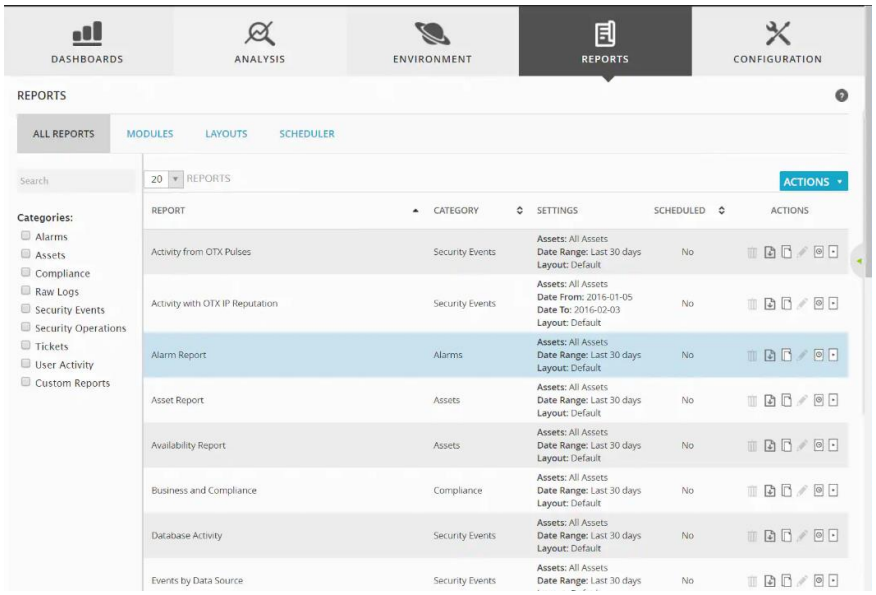
Εικόνα 8-15 Πληροφορίες σάρωσης

Εικόνα 8-16 Λεπτομέρειες μίας ευπάθειας

8.1.8 Δημιουργία Αναφορών

Αν και το μενού του Dashboard μας παρέχει την δυνατότητα εμφάνιση διαφόρων μετρήσεων ασφάλειας δικτύου για το περιβάλλον του δικτύου μας, το OSSIM μας παρέχει επιπλέον με περισσότερες από 200 διαφορετικές αναφορές που μπορούμε να δημιουργήσουμε, οι οποίες παρέχουν λεπτομέρειες σχετικά με διάφορες πτυχές της ασφάλειας του δικτύου.

Όταν επιλέγουμε από το μενού Reports > All Reports, εμφανίζεται η ακόλουθη σελίδα. (Εικόνα 8-17)



Εικόνα 8-17 Δημιουργία Αναφορών

Αυτή η σελίδα εμφανίζει ολόκληρη τη συλλογή αναφορών που είναι διαθέσιμες στο OSSIM, εμφανίζοντας το όνομα κάθε αναφοράς, τις κατηγορίες της, τις ρυθμίσεις αναφοράς και εάν η αναφορά έχει προγραμματιστεί να δημιουργηθεί. Μπορούμε επίσης από τον αριστερό πίνακα επιλέγοντας τις επιθυμητές κατηγορίες να περιορίσουμε την εμφάνιση τους, ώστε να εμφανίζονται μόνο εκείνες οι αναφορές που ανήκουν στις επιλεγμένες κατηγορίες.

Η τελευταία στήλη στη λίστα των αναφορών περιγράφει τις διαθέσιμες ενέργειες για μια επιλεγμένη αναφορά. Αυτές περιλαμβάνουν Διαγραφή, Εξαγωγή, Αντιγραφή, Επεξεργασία, Προσαρμοσμένη εκτέλεση και Αναφορά Εκτέλεσης. Μπορούμε να δημιουργήσουμε ή να εκτελέσουμε μια αναφορά, κατ' απαίτηση ή να προγραμματίσουμε μια εργασία για την περιοδική εκτέλεση μιας αναφοράς. Αφού εκτελέσουμε μια αναφορά, έχουμε την δυνατότητα να την αποθηκεύουμε ως PDF για εκτύπωση ή να την αποστείλουμε μέσω email.

Εκτός από τις προεπιλεγμένες σελίδες εμφάνισης οπου μπορούμε να αποκτήσουμε πρόσβαση και να εκτελέσουμε αναφορές, το OSSIM μπορεί να μας δώσει εναλλακτικές προβολές για τα ακόλουθα:

Modules — Παρέχει επιλογή από περισσότερα από 2600 στοιχεία αναφορών που θα μπορούσαν να συμπεριληφθούν στις αναφορές μας. Μπορούμε να ορίσετε queries για την ανάκτηση δεδομένων που χρησιμοποιούνται για τη δημιουργία γραφημάτων και πινάκων που περιλαμβάνονται στις αναφορές.

Layouts — Παρέχει επιλογές για τον καθορισμό των γραφικών πτυχών των αναφορών ορίζοντας την κεφαλίδα και το υποσέλιδο, το συνδυασμό χρωμάτων και τα εικονίδια που θα χρησιμοποιηθούν στις αναφορές μας.

Scheduler — Παρέχει επιλογές για τον καθορισμό της περιοδικής δημιουργίας αναφορών, προσδιορίζοντας επίσης ποιος μπορεί να δει μια αναφορά και σε ποιον αποστέλλονται οι αναφορές.

8.1.9 Διαχείριση και διαμόρφωση

Κατά τη διάρκεια της χρήσης του OSSIM για τη διαχείριση και τη διατήρηση της ασφάλειας του δικτύου μας, θα χρειαστεί να κάνουμε πολλές παραμετροποιήσεις και ενημερώσεις. Τα δίκτυα μπορεί να αλλάξουν, νέα στοιχεία (assets) θα προστεθούν, ή θα αφαιρεθούν. Το Configuration παρέχει την δυνατότητα εκτέλεσης πολλών από αυτών των εργασιών μέσω διαφόρων επιλογών όπως:

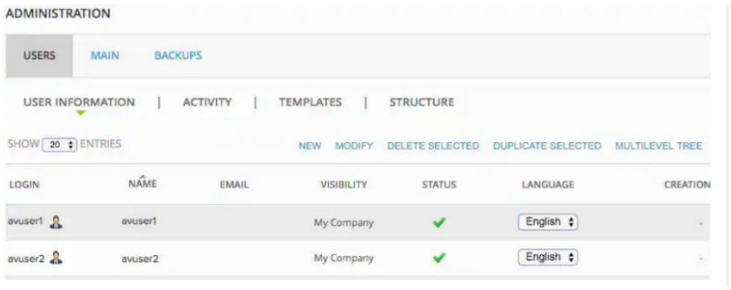
Διαχείριση — Παρέχει επιλογές διαχείρισης χρηστών, διαμόρφωσης συστήματος και δημιουργίας αντιγράφων ασφαλείας και επαναφοράς ρυθμίσεων.

Deployment — Παρέχει επιλογές για τη διαμόρφωση και τη διαχείριση των στοιχείων του OSSIM.

Threat Intelligence — Παρέχει επιλογές για τη διαμόρφωση των πολιτικών, των ενεργειών, των θυρών, των οδηγιών, της συμμόρφωσης, των κανόνων συσχέτισης και των πηγών δεδομένων. Μπορούμε επίσης να ελέγξουμε και να επεξεργαστούμε τη βάση γνώσεων, η οποία περιέχει πληροφορίες και προτεινόμενες ενέργειες για διαφορετικούς τύπους συμβάντων ασφαλείας.

Open Threat Exchange (OTX) — Παρέχει επιλογές για τη διαμόρφωση των OTX ρυθμίσεων και την προβολή μεμονωμένων παλμών OTX και ενδείξεων συμβιβασμού (IoC).

Όταν επιλέγουμε από το μενού Configuration > Administration, εμφανίζεται η ακόλουθη σελίδα. (Εικόνα 8-18)



Εικόνα 8-18 Διαχείριση

Η σελίδα αυτή εμφανίζει πληροφορίες σύνδεσης και πληροφορίες σχετικές με τους χρήστες του συστήματος. Οι χρήστες που έχουν πρόσβαση σε αυτήν τη σελίδα μπορούν να κάνουν διπλό κλικ στη σειρά του πίνακα που περιέχει το όνομα σύνδεσής τους για να προβάλουν και να ενημερώσουν τις πληροφορίες του δικού τους προφίλ, συμπεριλαμβανομένης της δυνατότητας αλλαγής του ονόματος χρήστη σύνδεσής, της διεύθυνσης ηλεκτρονικού ταχυδρομείου και του κωδικού πρόσβασης.

Από τη σελίδα Users, οι χρήστες μπορούν επίσης να επιλέξουν τις ακόλουθες επιλογές εμφάνισης:

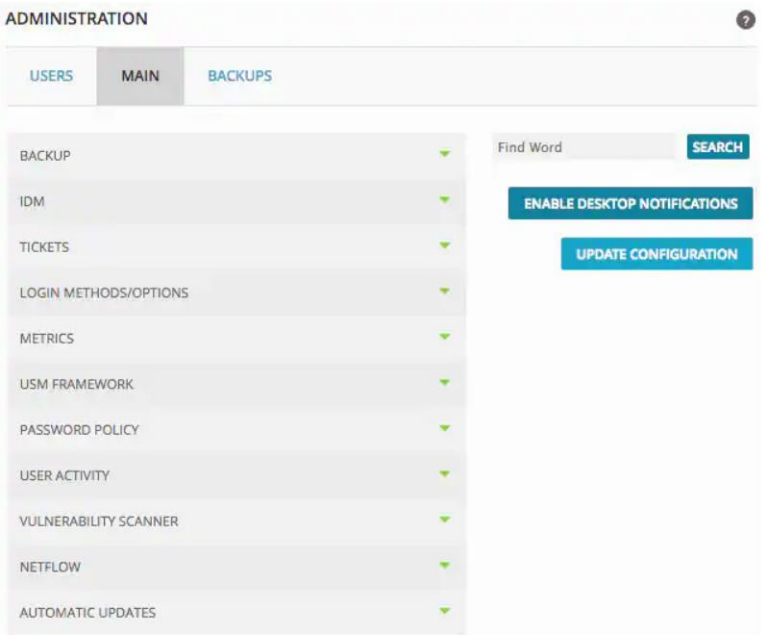
Activity — Προβάλλονται δραστηριότητες ή ενέργειες που έχουν καταγραφεί.

Templates —Προβολή και ενημέρωση της πρόσβασης χρήστη σε διαφορετικές ενότητες του OSSIM.

Structure — Προβάλλονται και πραγματοποιήστε ενημερώσεις στα Asset και στα Inventory που διατηρούνται από το OSSIM.

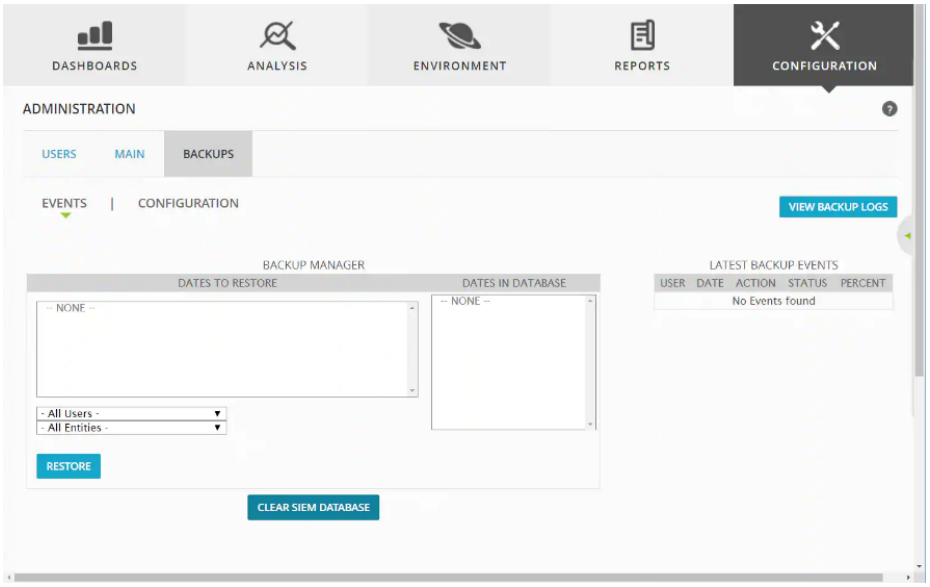
Εκτός από την κύρια προβολή σελίδας χρηστών , υπάρχουν και δύο άλλες επιλογές εμφάνισης:

Main — Παρέχει επιλογές προβολής και ενημέρωσης ρυθμίσεων για μια σειρά από λειτουργίες που περιλαμβάνουν Backup, IDM (διαχείριση ταυτότητας), Tickets, Μέθοδοι σύνδεσης, Μετρήσεις, Πολιτική κωδικού πρόσβασης, Δραστηριότητα χρήστη και σαρωτής ευπάθειας. (Εικόνα 8-19)



Εικόνα 8-19 Προβολή και ενημέρωση ρυθμίσεων

Δημιουργία αντιγράφων ασφαλείας — Παρέχει επιλογές για την προβολή αρχείων καταγραφής αντιγράφων ασφαλείας και επίσης την προβολή και ενημέρωση των ρυθμίσεων του Backup Manager. Τα καθημερινά αντίγραφα ασφαλείας περιλαμβάνουν όλες τις πληροφορίες διαμόρφωσης συστήματος, συμπεριλαμβανομένων του προφίλ συστήματος, της διαμόρφωσης δικτύου, των κανόνων πολιτικής, των plugins και των οδηγιών συσχέτισης. (Εικόνα 8-20)



Εικόνα 8-20 Δημιουργία αντιγράφων ασφαλείας

9

Επίλογος

9.1 Σύνοψη και συμπεράσματα

Τα τελευταία χρόνια οι επιθέσεις στον κυβερνοχώρο έχουν αναμφίβολα γίνει πιο συχνές και εξιδεικευμένες. Η τεχνολογία των επικοινωνιών και των πληροφοριών πλέον αποτελεί ένα από τα σπουδαιότερα στοιχεία της κοινωνικής αλλά και οικονομικής ανάπτυξης ενός έθνους, και βασικό εργαλείο για την κοινωνική ευημερία μιας χώρας. Οι τελευταίες τεχνολογικές εξελίξεις, σε συνδυασμό με την ενεστώσα γεωπολιτική κατάσταση καθιστούν αναγκαία την αναπροσαρμογή των μέτρων κυβερνοασφάλειας. Οι επιθέσεις στο κυβερνοχώρο κατά των υφιστάμενων υποδομών, παρουσίασαν αυξητική τάση. Κατά την περίοδο την πανδημία του κορονοϊού στη χώρα μας, παρατηρήθηκε μία έξαρση των κυβερνοεπιθέσεων, στοχοποιώντας την τηλεργασίας που αναγκαστικά χρησιμοποιούσαν οι εργαζόμενοι κατά την περίοδο αυτή. Ο ENISA, σε έρευνα που διενέργησε το 2021, διαπίστωσε ότι η δημόσια διοίκηση καθώς και η ηλεκτρονική διακυβέρνηση είχαν πληγεί από πληθώρα κυβερνοεπιθέσεων καθώς συγκαταλέγονταν στους πέντε πρώτους τομείς που αντιμετώπισαν τις περισσότερες απειλές στον κυβερνοχώρο. Το 2022 αναφέρθηκε ότι μεγάλοι φορείς του Ελληνικού Δημοσίου δέχτηκαν επίθεση από κυβερνοεγκληματίες. Πρόκειται, μεταξύ άλλων, για το Taxisnet, τον ΔΕΣΦΑ, τη ΔΕΗ και τα Ελληνικά Ταχυδρομεία. Οι τελευταίες κυβερνοεπιθέσεις, σε συνδυασμό με την ενεστώσα γεωπολιτική κατάσταση καθιστούν αναγκαία την διασφάλιση και τον συνεχής έλεγχος της ασφάλειας των κρίσιμων υποδομών των συστημάτων της ΓΓΠΣΔΔ, ο έγκαιρος εντοπισμός τρωτών σημείων και τα περιστατικών καθώς και η λήψη των κατάλληλων ενεργειών πρόληψης και αντιμετώπισης των εν λόγω περιστατικών σε 24ωρη βάση. Πρόσφατη έκθεση της EUROPOL αποκάλυψε ότι καταγράφηκε αύξηση της κακόβουλης διαδικτυακής δραστηριότητας σε δημόσιους φορείς των πολλών κρατών μελών της ΕΕ, καθιστώντας τα θέματα κυβερνοασφάλειας καθημερινό αγώνα για την ΕΕ και τα κράτη μέλη της [27].

Η ΕΕ πολύ σύντομα αντιλήφθηκε ότι τα ζητήματα κυβερνοασφάλειας θα πρέπει να τύχουν σοβαρής και οργανωμένης ανταπόκρισης. Η διαμορφωθείσα νέα πραγματικότητα καθιστά επιτακτική την ανάγκη τα κράτη μέλη να μιλούν την ίδια «γλώσσα» και ν` αναπτύξουν τα ίδια καλά αντανακλαστικά, καθώς ο διασυνοριακός χαρακτήρας και οι αλληλεξαρτήσεις που υπάρχουν δεν αφήνουν περιθώρια για οποιαδήποτε παρέκκλιση.

Η οδηγία NIS άνοιξε τον δρόμο και έθεσε τις βάσεις της ορθής και συντονισμένης λειτουργίας. Η ΕΕ έπρεπε με κάθε κόστος να αναπτύξει διαδικασίες και πολιτικές ασφάλειας για την διασφάλιση των τριών βασικών αρχών: της ασφάλειας, της ακεραιότητα, της εμπιστευτικότητας και της διαθεσιμότητας των πληροφοριών. Η επερχόμενη αναθεώρησή της, η οδηγία NIS2, κινούμενη στις ίδιες καλές πρακτικές και με εμπλουτισμένη στόχευση φιλοδοξεί να βελτιώσει κάθε δυσλειτουργία της αρχικής της μορφής, να συμπληρώσει με επάρκεια τα τρωτά σημεία του αρχικού σχήματος και να συμπεριλάβει τις όποιες τεχνολογικές εξελίξεις. Παράλληλα, φιλοδοξεί να δημιουργήσει προοπτική συμπερίληψης των επερχόμενων τεχνολογικών αλμάτων, θεσπίζοντας εκτός των άλλων και ένα πλαίσιο διαρκούς επικαιροποίησης. Και στην περίπτωση της οδηγίας NIS2 θα δοθεί διετής προθεσμία στα κράτη μέλη να εντάξουν τις προβλέψεις στην εθνική τους νομοθεσία.

Οι υποχρεώσεις που γεννώνται από τη συμμόρφωση με την οδηγία, όπως μπορούμε να αναλογιστούμε είναι δαπανηρές. Τα κόστη από την προκαλούμενη ζημία όμως είναι πολλαπλάσια. Το ζητούμενο είναι να δημιουργηθεί κουλτούρα κυβερνοσεβασμού από το σύνολο των υπόχρεων μερών, η οποία θα οδηγεί σε συμμόρφωση με τις απαιτήσεις της οδηγίας όχι λόγω της υποχρεωτικότητας, αλλά συνεπεία της αντίληψης της σπουδαιότητας των αγαθών που προασπίζει.

Μια σημαντική παράμετρος εφαρμογής που μπορεί να συμβάλει στην επίτευξη συμμόρφωσης με όλες τις τεχνικές πτυχές την νέας οδηγίας NIS 2 είναι τα Συστήματα Πληροφοριών Ασφάλειας και Διαχείρισης Περιστατικών (Security Information and Event Management - SIEM). Όλες οι λύσεις SIEM λειτουργούν διενεργώντας ένα σύνολο ενεργειών. Αυτές είναι η συγκέντρωση των αρχείων καταγραφής, η ενοποίηση αυτών των καταγραφών και η ταξινόμηση αυτών με στόχο των εντοπισμό κακόβουλων ενεργειών σε πραγματικό χρόνο και την συμμόρφωσης με τις εκάστοτε απαιτήσεις ασφαλείας. Ενσωματώνουν επίσης την έρευνα των περιστατικών και την παρακολούθηση της τήρησης των κανονιστικών πλαισίων χρησιμοποιώντας ιστορικά δεδομένα από αξιόπιστες πηγές. Είναι σημαντικό να διαχωρίσουμε τα SIEM εργαλεία από τα υπάρχοντα συστήματα ασφαλείας όπως τοίχοι προστασίας, συστήματα ανίχνευσης επιθέσεων κ.τ.λ. Τα υπάρχοντα αυτά συστήματα ασφαλείας παρέχουν μία βασική ασφάλεια στο δίκτυο και αποτελούν μία πρώτη γραμμή άμυνας, αλλά δεν μπορούν να εγγυηθούν μια πλήρως ολοκληρωμένη προστασία κατά των απειλών. Αυτός είναι ο λόγος για τον οποίο χρειάζεστε μια ολοκληρωμένη λύση ανίχνευσης απειλών όπως το SIEM, η οποία

ειδοποιεί κάθε φορά που εμφανίζεται ύποπτη δραστηριότητα δικτύου. Οι λύσεις SIEM έχουν σχεδιαστεί για να συλλέγουν και να αναλύουν τα δεδομένα καταγραφής από όλα τα υπάρχοντα συστήματα ασφαλείας. Δεν μπορούν αυτόνομα να αποτρέψουν μια επίθεση αλλά με την συνεργασία με όλα τα συστήματα ελέγχου ασφάλειας μπορεί να προτρέψει μια κακόβουλη ενέργεια που ελλοχεύει στο υπό παρακολούθηση πληροφοριακό μας σύστημα. Αυτό δίνει την δυνατότητα στους υπευθύνους ασφαλείας να αναγνωρίζουν σε σύντομο χρονικά διάστημα την εκδήλωση μίας επίθεσης και να περιορίσει τις πηγές της επίθεσης.

Σήμερα υπάρχουν πολλά διαθέσιμα συστήματα SIEM ανοιχτού κώδικα, σχεδιασμένα για μικρούς και για μεγάλους οργανισμούς που μπορούν συμβάλουν στην επίτευξη συμμόρφωσης με όλες τις τεχνικές πτυχές την νέας οδηγίας NIS 2. Η πρόκληση της επιλογής της κατάλληλης λύσης SIEM αποτελεί μείζονος σημασία για την έυρυθμη λειτουργεία ενός πληροφοριακού συστήματος. Στα πλαίσια αξιολόγηση των συστημάτων αυτών θα πρέπει οι υπεύθυνοι ασφαλείας να τηρήσουν μια αυστηρή λίστα κριτηρίων τα οποία θα θωρακίζουν τα πληροφοριακά συστήματα με την ανίχνευση και διαχείριση συμβάντων που είναι δύσκολο να εντοπιστούν και θα προσφέρουν απλοποιημένες αναφορές κανονιστικής συμμόρφωσης.

Έχοντας ως γνώμονα τα ανωτέρω και αναλύοντας τα βασικά μέρη από τα οποία αποτελείται μία ανοιχτού κώδικα λύση SIEM, έγινε παρουσίαση των πέντε δημοφιλέστερων εργαλείων στην εργασία αυτή και αναπτύχθηκε μια διερευνητική μελέτη εφαρμογής σε έναν δημόσιο φορέα κάνοντας εγκατάσταση στους διακομιστές του φορέα ένα από τα πιο δημοφιλής εργαλεία SIEM ανοιχτού κώδικα, το OSSIM της AlienVault. Έγινε περιγραφή των βημάτων που ακολουθήθηκαν για την ανάπτυξη του εργαλείου στο δίκτυο του Φορέα και αναλύθηκε ο τρόπος με τον οποίο το OSSIM διαχειρίζεται τις απειλές και τα περιστατικά ασφάλειας μέσω της συλλογής και την ανάλυση των συμβάντων από μια ευρύτερη ποικιλία περιστατικών και δεδομένων σε πραγματικό χρόνο. Στο πλαίσιο αυτό αναδείχθηκε και ένα από τα μεγάλα πλεονεκτήματα του εργαλείου αυτού που είναι η εύκολη δημιουργία πολιτικών ασφαλείας που μπορεί να συμβάλει στην άμεση τήρηση των κανονιστικών πλαισίων της κοινοτικής οδηγίας NIS2.

Το γενικό συμπέρασμα αυτής της εργασίας ήταν να κατανοήσουμε τις δυσκολίες που έχουν να αντιμετωπίσουν οι δημόσιοι φορείς στο νέο ψηφιακό περιβάλλον που διαμορφώνεται, και η επιτακτική ανάγκη ανάπτυξης διαδικασιών και πολιτικών ασφάλειας για την ψηφιακή θωράκιση του Δημοσίου και την διασφάλιση των τριών βασικών αρχών της ασφάλειας: της ακεραιότητα, της εμπιστευτικότητας και της διαθεσιμότητας των πληροφοριών. Σε εθνικό επίπεδο, ιδιαίτερα οι φορείς Δημόσιας Διοίκησης θα πρέπει να «οχυρώσουν» την δικτυακή υποδομή των πληροφοριακών τους συστημάτων, με την χρήση SIEM εργαλείων, για εδραίωση ενός ασφαλούς ηλεκτρονικού περιβάλλοντος και την λήψη μέτρων «επιθετικής» άμυνας για την πρόληψη και την αντιμετώπιση μελλοντικών κινδύνων, λειτουργώντας πάντα βάσει των

κεντρικών οδηγιών του Υπουργείου Ψηφιακής Διακυβέρνησης και των θεσμοθετημένων κανόνων της κοινοτικής οδηγίας NIS2 για την κυβερνοασφάλεια.

9.2 Μελλοντική Επέκταση

Σε αυτήν την εργασία, στα πλαίσια της επίτευξη συμμόρφωσης με όλες τις τεχνικές πτυχές την νέας οδηγίας NIS 2, αποτυπώθηκε η εμπειρία που αποκτήθηκε κάνοντας χρήση ένα από τα δημοφιλέστερα εργαλεία SIEM ανοιχτού κώδικα που υπάρχουν, αυτό του OSSIM της AlienVault. Το OSSIM ανταπεξήλθε ικανοποιητικά στη θωράκιση και στην ενίσχυση της ασφάλειας του φορέα σε μεγάλο βαθμό. Υπήρχαν κάποια πρακτικά προβλήματα κατά την παραμετροποίησή του, αλλά συγχρόνως άνοιξε το δρόμο για νέες προσεγγίσεις που μπορούν να συμπληρώσουν την τρέχουσα πρακτική SIEM. Στο μέλλον, θα γίνει διερεύνηση για την δυνατότητα χρήσης περισσότερων plugin με σκοπό την επέκταση των παραδοσιακών δυνατοτήτων του OSSIM. Η AlienVault παρέχει μεγάλο αριθμό plugin και υποστηρίζει τη δημιουργία νέων plugin από την αρχή. Θα συνεχιστούν τα πειράματα για να γίνει επικύρωση των ευρημάτων και να αντιμετωπιστούν τεχνικές συσχέτισης για την ανίχνευση κρυφών και πολλαπλών βημάτων επιθέσεις στα αρχεία καταγραφής.

Μια άλλη μελλοντική επέκταση θα μπορούσε να είναι η ανάπτυξη ενός άλλου ολοκληρωμένου SIEM μοντέλου που θα συνδυάζει πρότυπα και μεθόδους Μηχανικής Μάθησης και AI. Στις μέρες μας πάνω από τις μισές παραβιάσεις ασφαλείας προκαλούνται από αξιόπιστους υπαλλήλους που είτε ακούσια είτε κακόβουλα συμμετείχαν σε μια επίθεση, προκαλώντας απώλεια δεδομένων, παραβιάσεις συμμόρφωσης, καταστροφή συστημάτων και άλλες σοβαρές και δαπανηρές συνέπειες. Οι απειλές εσωτερικών χρηστών είναι εμφανώς πιο δύσκολο να εντοπιστούν επειδή απαιτούν μια βαθύτερη ανάλυση της συμπεριφοράς των χρηστών για να αποκαλυφθούν, που δεν μπορούν να επιτύχουν τα απλά SIEM εργαλεία που χρησιμοποιούν απλούς αλγόριθμους. Το User Behavior Analytics είναι μία από τις πολλές λειτουργίες που περιλαμβάνονται στις «Ευφυής» SIEM λύσεις, τις οποίες άλλα εργαλεία διαχείρισης συμβάντων πληροφοριών ασφαλείας είτε χρεώνουν επιπλέον είτε απαιτούν έναν τρίτο πάροχο λύσεων. Ένα τέτοιο SIEM εργαλείο είναι το QRadar το οποίο χρησιμοποιεί τεχνολογία ασφάλειας τεχνητής νοημοσύνης και μηχανικής μάθησης για να αναλύσει τα αρχεία καταγραφής ροών δικτύου και συμβάντων χρήστη για τη διάκριση μεταξύ της κανονικής και μη φυσιολογικής συμπεριφοράς χρήστη, τον εντοπισμό πρώιμων προειδοποιητικών ενδείξεων για παράτυπες ενέργειες χρήστη, την κατηγοριοποίηση της επικίνδυνης συμπεριφοράς των χρηστών, παρέχοντας στους Αναλυτές Ασφαλείας τα εργαλεία για την αποτροπή τέτοιου είδους περιστατικών ασφαλείας.

Η κυβερνοασφάλεια αποτελεί μείζονα πρόκληση για τις δημόσιες αρχές μετά τις τελευταίες τεχνολογικές εξελίξεις, σε συνδυασμό με την ενεστώσα γεωπολιτική κατάσταση. Το κράτος έχει επωμιστεί την ευθύνη της ασφάλειας των πληροφοριών και για το λόγο αυτό το Υπουργείο Ψηφιακής Διακυβέρνησης θα πρέπει να συμμετέχει ενεργά στην θέσπιση πολιτικών ασφαλείας σε όλους του δημόσιους φορείς αναλμβάνωντας συγκεκριμένες θεσμικές πρωτοβουλίες για την διασφάλισης της κυβερνοασφάλειας. Γνώμονας του Υπουργείου Ψηφιακής Διακυβέρνησης θα πρέπει να είναι η συνεισφορά του στην οικονομική και κοινωνική σταθερότητα και ανάπτυξη της χώρας.

Σε ένα περιβάλλον απειλών που αλλάζει δυναμικά και επηρεάζεται από το ευρύτερο πλαίσιο των απειλών στον κυβερνοχώρο, πρέπει να εδραιωθεί σε όλους μας η αντίληψη ότι η ασφάλεια των πληροφοριών δεν αποτελεί τεχνολογικό θέμα αλλά, αλλά μία σημαντική λειτουργία που θα πρέπει να ενταχθεί μέσα στον στρατηγικό σχεδιασμό και στο επιχειρησιακό πλάνο των δημόσιων φορέων.

10

Βιβλιογραφία

[1] D. Schatz, R. Bashroush, and J. Wall, "Towards a More Representative Definition of Cyber Security," *J. Digit. Forensics, Secur. Law*, vol. 12, no. 2, 2017, doi: 10.15394/jdfsl.2017.1476.

[2] Europol, "INTERNET ORGANISED CRIME," 2017. doi: 10.2813/55735.

[3] Z. Bederna, Z. Rajnai, and T. Szadeczky, "Attacks against energy, water and other critical infrastructure in the EU," *CANDO-EPE 2020 - Proceedings, IEEE 3rd Int. Conf. Work. Obuda Electr. Power Eng.*, pp. 125–130, 2020, doi: 10.1109/CANDO-EPE51100.2020.9337751.

[4] ΕΥΡΩΠΑΪΚΟ ΕΛΕΓΚΤΙΚΟ ΣΥΝΕΔΡΙΟ, "Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνοασφάλεια," *Ενημερωτικό έγγραφο*, 2019.

[5] Ε. Ε.-Δ. Τύπου, "Κατάσταση της Ένωσης 2017 – Κυβερνοασφάλεια : Η Επιτροπή αναβαθμίζει την απόκριση της ΕΕ στις κυβερνοεπιθέσεις," 2017.

[6] ENISA, "Hackers-for-Hire drive the Evolution of the New ENISA Threat Landscape." [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/hackers-for-hire-drive-the-evolution-of-the-new-enisa-threat-landscape.

[7] ENISA, *ENISA Threat Landscape 2021*, no. October. 2021.

[8] ENISA, "ENISA Threat Landscape 2021 April 2020 to mid-July 2021," 2021. doi: 10.2824/324797.

[9] Pierluigi Paganini, "Port of San Diego hit by a cyber attack a few days after the attack on the Port of Barcelona," 2018. https://securityaffairs.co/76623/hacking/port-of-san-diego-attack.html.

[10] Kaspersky Lab, "Attackers Created Unique, Highly-Flexible Malware to Steal Data and Geopolitical Intelligence from Target Victims' Computer Systems, Mobile Phones and Enterprise Network Equipment." https://www.kaspersky.com/about/press-releases/2013_kaspersky-lab-identifies-operation--red-october--an-advanced-cyber-espionage-campaign-targeting-diplomatic-and-government-institutions-worldwide.

[11] securelist, "The 'Red October' Campaign – An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies," *securelist*. https://securelist.com/the-red-october-campaign/57647/.

[12] computerweekly, "Exxon, Shell, BP hacked in Night Dragon attacks," *computerweekly.com*. https://www.computerweekly.com/news/1280095257/Exxon-Shell-BP-hacked-in-Night-Dragon-attacks.

[13] wired.com, "Now Cryptojacking Threatens Critical Infrastructure, Too." https://www.wired.com/story/cryptojacking-critical-infrastructure/.

[14] N. Tripathi and B. Mehtre, "DoS and DDos Attacks: Impact, Analysis and Countermeasures," *Proc. Natl. Conf. Adv. Comput. Netw. Secur.*, no. July, pp. 1–6, 2013.

[15] ΕΥΡΩΠΑΪΚΟ ΕΛΕΓΚΤΙΚΟ ΣΥΝΕΔΡΙΟ, "Επισκόπηση αριθ. 02/2019: Προκλήσεις για μια αποτελεσματική ενωσιακή πολιτική για την κυβερνοασφάλεια." [Online]. Available: https://www.eca.europa.eu/el/Pages/DocItem.aspx?did=49416.
[16] S. Vosoughi, R. Deb, and S. Aral, "False news is big news," *MIT Initiat. Digit. Econ. Res. Br.*, vol. 359, no. 6380, pp. 1146–1151, 2018, [Online]. Available: http://ide.mit.edu/sites/default/files/publications/2017 IDE Research Brief False News.pdf.
[17] A. Morse, "Investigation: WannaCry cyber attack on the NHS," *UK Natl. Audit Off.*, no. April 2018, pp. 1–35, 2017, [Online]. Available: https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/.
[18] EY Global Information Security Survey 2021, "The EY Global Information Security Survey 2021 finds CISOs and security leaders battling against a new wave of threats unleashed by COVID-19." https://www.ey.com/en_gr/cybersecurity/cybersecurity-how-do-you-rise-above-the-waves-of-a-perfect-storm.
[19] EY, "Το αύριο είναι εδώ. Η ηγεσία του μέλλοντος, είναι; | EY Greece," *EY*. https://www.ey.com/el_gr/workforce-resources/greek--leadership-survey-.
[20] C. Nabe, "Impact-Covid-Cybersecurity," 2020. https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html.
[21] ΔΙΕΥΘΥΝΣΗ ΣΤΡΑΤΗΓΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ, "ΕΘΝΙΚΗ ΣΤΡΑΤΗΓΙΚΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ 2020 - 2025," 2020. [Online]. Available: https://primeminister.kz/kz/gosprogrammy/kr-bilim-berudi-zhane-gylymdy-damytudyn-2020-2025-zhyldarga-arnalgan-memlekettik-bagdarlamasy--9115948.
[22] N. C. Authority, "Εθνικη στρατηγικη κυβερνοασφαλειασ 2020 -2025," 2020, [Online]. Available: https://mindigital.gr/εθνικη-στρατηγικη-κυβερνοασφαλει.
[23] Εθνική Στρατηγική Κυβερνοασφάλειας 2020-2025, "5 Στρατηγικοί Στόχοι." .
[24] spearit.net, "EU NIS Directive Receives Update Proposal." https://www.spearit.net/blog/eu-nis-directive-receives-update-proposal.
[25] ENISA News, "What is a CSIRT and how can it help me?" https://www.enisa.europa.eu/news/enisa-news/what-is-a-csirt.
[26] Ε. Υ. Πληροφοριών, "Εθνικό CERT." https://www.nis.gr/el/national-cert/useful-info.
[27] Lawspot.gr, "Νέοι ισχυρότεροι κανόνες στην ΕΕ για την κυβερνοανθεκτικότητα και τη φυσική ανθεκτικότητα κρίσιμων οντοτήτων και δικτύων," *Lawspot*, 2023. https://www.lawspot.gr/nomika-nea/neoi-ishyroteroi-kanones-stin-ee-gia-tin-kyvernoanthektikotita-kai-ti-fysiki.
[28] Ε. Ε. της Ε. Ένωσης, "ΟΔΗΓΙΑ (ΕΕ) 2022/2555 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ," vol. 2022, no. 3, 2022.
[29] splunk.com, "NIS2 is coming.What does it mean?," *www.splunk.com*, 2022. https://www.splunk.com/en_us/blog/security/nis2-is-coming-what-does-it-mean.html.
[30] Itsecuritypro, "Η οδηγία NIS2 είναι ήδη εδώ. Τι σημαίνει όμως αυτό για τις επιχειρήσεις;," *itsecuritypro*, 2023. https://www.itsecuritypro.gr/i-odigia-nis2-einai-idi-edo-ti-simainei-omos-ayto-gia-tis-epicheiriseis/.
[31] L. Kim, *Cybersecurity awareness*, vol. 47, no. 6. 2017.
[32] AlienVault, "Threats, Politics, and Cryptocurrency-Mining - Infosecurity Europe 2018 Survey Results," 2018. https://cybersecurity.att.com/blogs/security-essentials/threats-politics-and-cryptocurrency-mining-infosecurity-europe-2018-survey-results.
[33] LTS Secure, "LTS Secure SIEM Tools." https://ltssecure.com/security-information-and-event-management/.
[34] AlienVault, "AlienVault OSSIM." https://cybersecurity.att.com/products/ossim.
[35] S. D. Sajjadi Torshizi, S. Rostampour, and M. Tanha, "New secure and low-cost design for defense in depth implementation using open source software," *Proc. - 2011 IEEE Student Conf. Res. Dev. SCOReD 2011*, no. March 2018, pp. 448–453, 2011, doi: 10.1109/SCOReD.2011.6148781.
[36] M. Alamanni, "OSSIM: a careful, free and always available guardian for your network," *Linux J.*, vol. 2014, no. 242, p. 2, 2014, [Online]. Available: http://dl.acm.org/ft_gateway.cfm?id=2642924&type=html.

[37] OSSEC, “Download OSSEC for Your Platform.” https://www.ossec.net/download-ossec/.
[38] A. Cybersecurity, “Policy Management.” https://cybersecurity.att.com/documentation/usm-appliance/policy-management/about-policies-usm.htm.
[39] A. Cybersecurity, “Policy Order and Grouping.” https://cybersecurity.att.com/documentation/usm-appliance/policy-management/managing-policies.htm.
[40] A. Cybersecurity, “Policy Management›Create an Action.” [Online]. Available: https://cybersecurity.att.com/documentation/usm-appliance/policy-management/action-exec-ext.htm?tocpath=Documentation%7CUSM Appliance™%7CUser Guide%7CPolicy Management%7CCreate a New Policy%7C_____1.
[41] AlienVault, “OSSIM Appliance Documentation.” [Online]. Available: https://cybersecurity.att.com/documentation/usm-appliance.htm?Highlight=ossim Documentation.