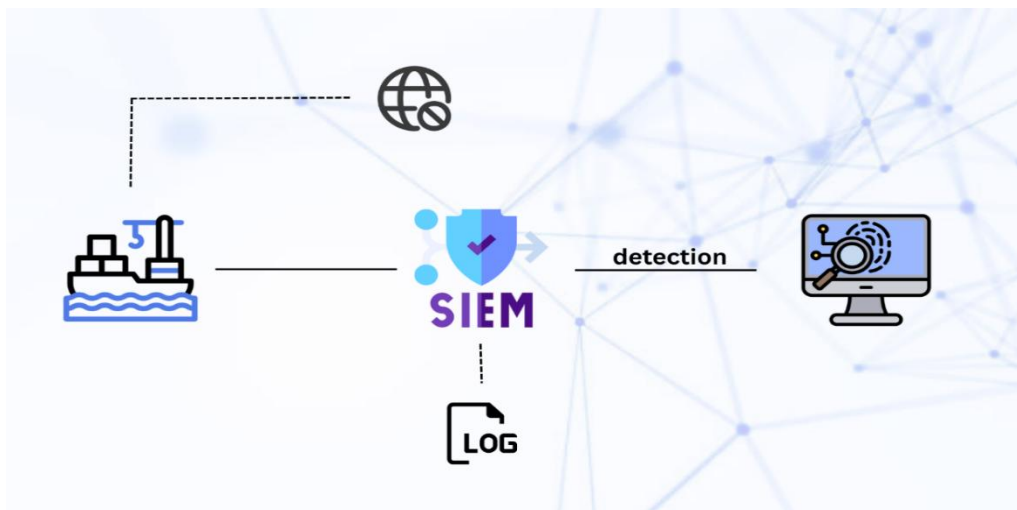


ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

« Κυβερνοασφάλεια Πλοίων μέσω Αυτόνομου
Συστήματος Διαχείρισης Πληροφοριών και Συμβάντων
Ασφάλειας»



Της φοιτήτριας
Πηνελόπης Τσακιτζίδου
Αρ. Μητρώου: 2020174

Επιβλέπων
Δρ. Περικλής Χατζημίσσιος
Καθηγητής

Ημερομηνία 29/05/2026

Κυβερνοασφάλεια Πλοίων μέσω Αυτόνομου Συστήματος Διαχείρισης Πληροφοριών και Συμβάντων
Ασφάλειας
Κωδικός Δ.Ε. 25307
Πηνελόπη Τσακιτζίδου
Περικλής Χατζημίσσιος
Ημερομηνία ανάληψης Δ.Ε. 30/08/2025
Ημερομηνία περάτωσης Δ.Ε. 29/05/2026

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως διπλωματική εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

Η παρούσα εργασία αποτελεί πνευματική ιδιοκτησία της φοιτήτριας Πηνελόπης Τσακιτζίδου που την εκπόνησε. Στο πλαίσιο της πολιτικής ανοικτής πρόσβασης, ο συγγραφέας/δημιουργός εκχωρεί στο Διεθνές Πανεπιστήμιο της Ελλάδος άδεια χρήσης του δικαιώματος αναπαραγωγής, δανεισμού, παρουσίασης στο κοινό και ψηφιακής διάχυσης της εργασίας διεθνώς, σε ηλεκτρονική μορφή και σε οποιοδήποτε μέσο, για διδακτικούς και ερευνητικούς σκοπούς, άνευ ανταλλάγματος. Η ανοικτή πρόσβαση στο πλήρες κείμενο της εργασίας, δεν σημαίνει καθ' οιονδήποτε τρόπο παραχώρηση δικαιωμάτων διανοητικής ιδιοκτησίας του συγγραφέα/δημιουργού, ούτε επιτρέπει την αναπαραγωγή, αναδημοσίευση, αντιγραφή, πώληση, εμπορική χρήση, διανομή, έκδοση, μεταφόρτωση (downloading), ανάρτηση (uploading), μετάφραση, τροποποίηση με οποιονδήποτε τρόπο, τμηματικά ή περιληπτικά της εργασίας, χωρίς τη ρητή προηγούμενη έγγραφη συναίνεση του συγγραφέα/δημιουργού.

Η έγκριση της διπλωματικής εργασίας από το Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του Διεθνούς Πανεπιστημίου της Ελλάδος, δεν υποδηλώνει απαραίτητα και αποδοχή των απόψεων του συγγραφέα, εκ μέρους του Τμήματος.

«Σε όλους όσους με στηρίζουν»

Πρόλογος

Εισαγωγικά, η υιοθέτηση του θέματος της παρούσας διπλωματικής εργασίας στηρίχθηκε σε προσωπικό μου βίωμα, μέσω εργασιακής μου ενασχόλησης με τα πλοία. Αποτέλεσε μία εργασιακή εμπειρία που συνέβαλε στη διαπίστωσή μου ότι η κεντρική εποπτεία και η λειτουργική διερεύνηση συμβάντων ασφαλείας στο χώρο της ναυτιλίας, δύναται να αποβεί απαιτητική και κρίσιμη. Το πλοίο εν γένει αποτελεί από μόνο του μία πρόκληση, μία περίπλοκη και δυσχερή επιχειρησιακή δραστηριότητα, στο οποίο ενυπάρχουν ανομοιογενή πληροφοριακά συστήματα, οριοθετημένη συνδεσιμότητα, εκτεταμένες απαιτήσεις διαθεσιμότητας, γεωγραφικές δυσκολίες καθώς και αέναη λειτουργία. Υπό αυτές τις συνθήκες, ένα περιστατικό που φαντάζει απλό και σύνηθες δύναται να αποβεί μοιραίο στον εντοπισμό του και στην έγκαιρη αξιολόγηση του. Εν συνεχεία, η ενασχόληση μου με διαδικασίες παρακολούθησης και διαχείρισης τέτοιων γεγονότων στο πλαίσιο της ασφάλειας, επιβεβαίωσε τη δυσκολία που ακολουθεί την εποπτεία καταγραφών και ειδοποιήσεων και ότι δεν πρόκειται για μία απλή, συνήθης διαδικασία. Αδιαμφισβήτητα επιβεβαίωσε και την αναγκαιότητα για την έγκαιρη ανίχνευση ύποπτων ενεργειών, την κατανόηση της αλληλουχίας ενός περιστατικού και τη διατήρηση της επιχειρησιακής συνέχειας. Αξίζει να σημειωθεί η στροφή της προσοχής μου στις διαθέσιμες λύσεις και ιδίως στην αδυναμία τους να κοστολογούνται χαμηλά και προσιτά ή και στη δύσκολη προσαρμογή τους σε ιδιαίτερες συνθήκες που περικλείουν την ναυτιλία. Βάσει των ανωτέρω, η παρούσα διπλωματική εργασία εστιάζει στην υλοποίηση και πραγμάτωση ενός λειτουργικού υποδείγματος μίας πλατφόρμας ικανής να διαχειριστεί συμβάντα ασφαλείας ανοιχτού κώδικα, με τη δυνατότητα να συλλέγει και να οργανώνει δεδομένα από ετερογενείς πηγές. Συνοψίζοντας, θα αξιολογηθεί η καταλληλότητα για βάση σε κεντρική εποπτεία και διερεύνηση γεγονότων και συμβάντων στον ναυτιλιακό επιχειρείν, λαμβάνοντας υπόψη όλες τις παραμέτρους οι οποίες παρεμποδίζουν την ομαλή λειτουργία, όπως λόγου χάριν προαναφέρθηκε το υψηλό κόστος, η συνδεσιμότητα και η περιπλοκότητα εν τω συνόλω.

Περίληψη

Στον χώρο της ναυτιλίας η κυβερνοασφάλεια καταλαμβάνει υψηλή θέση, καθώς αποτελεί ζήτημα μείζονος σημασίας. Η σημαντικότητα της θέσης της αιτιολογείται καθώς τα περισσότερα πλοία στηρίζονται σε δικτυωμένα πληροφοριακά συστήματα και αυτοματισμούς. Αναμφίβολα, στην καθημερινή και τακτική λειτουργία τους παράγουν μεγάλο όγκο καταγραφών και συμβάντων. Για αυτούς τους λόγους η διακεκομμένη παρακολούθηση των προαναφερθέντων δεδομένων δυσχεραίνει την αξιόπιστη ανίχνευση ύποπτων και ανησυχητικών ενεργειών, καθώς και την αποτελεσματική μελέτη των περιστατικών. Με την παρούσα διπλωματική εργασία, πρόκειται να παρουσιαστεί ο σχεδιασμός και η υλοποίηση ενός πλήρους συστήματος ικανού για συλλογή και ανάλυση συμβάντων ασφάλειας ανοιχτού κώδικα, με γνώμονα τη ναυτιλία και απώτερο σκοπό την εποπτεία και την αρωγή σε ανιχνεύσεις απειλών, βάσει οργάνωσης δεδομένων.

Κατόπιν έρευνας, η πλατφόρμα ασφαλείας ανοιχτού κώδικα Wazuh κρίθηκε η καταλληλότερη, διότι με τη συνεισφορά της αξιοποιούνται πολλαπλές πηγές δεδομένων από τερματικά συστήματα και αρχεία καταγραφής δικτυακού χαρακτήρα, μέχρι μηχανισμούς αποκωδικοποίησης και κανόνων συσχέτισης. Στην παρούσα εκπόνηση διπλωματικής εργασίας, πραγματώνεται ο τρόπος εγκατάστασης και παραμετροποίησης της πλατφόρμας καθώς και η μεθοδολογία επεξεργασίας δεδομένων. Επιπρόσθετα, αναλύεται ο τρόπος με τον οποίο τα συμβάντα μετατρέπονται σε ωφέλιμη πληροφορία και ειδοποίηση. Τέλος, θα απαριθμηθούν τα αποτελέσματα που επιφέρει η αποδοτική επαλήθευση και αξιολόγηση, όπως για παράδειγμα η ορατότητα συμβάντων, η δημιουργία ειδοποιήσεων και η χρήση πόρων, επιβεβαιώνοντας ότι το λογισμικό ανοιχτού κώδικα κρίνεται ικανό να απαρτίσει ουσιώδη βάση για κεντρική παρακολούθηση και διερεύνηση γεγονότων ασφαλείας, σε περιβάλλοντα με ανομοιογενή δεδομένα.

«Cybersecurity of Ships through an Autonomous Security Information and Event Management System»

«Pinelopi Tsakiltzidou»

Abstract

The maritime industry has become increasingly dependent on networked information systems and automated infrastructure to support daily vessel operations. This growing digital footprint exposes ships and shipping companies to a wide range of cyber threats, while at the same time generating vast volumes of logs and events that are often monitored in a fragmented manner. Without centralized oversight, suspicious activity can easily go undetected, and incident investigation becomes slow and unreliable. These conditions make continuous and structured security monitoring a critical necessity for the sector.

The present thesis addresses this need through the design and implementation of an open source system for the collection and analysis of security events, tailored to maritime environments. After evaluating available solutions, the Wazuh platform was selected for its ability to integrate diverse data sources and to transform raw events into actionable alerts through decoders and rule sets. The thesis describes the installation, configuration, and data processing methodology, and concludes with an evaluation of event visibility, alert generation, and resource utilization. The results confirm that open source software can serve as a solid foundation for large scale security monitoring in the heterogeneous environments characteristic of the maritime sector.

Ευχαριστίες

Έχοντας ολοκληρώσει την παρουσίαση της διπλωματικής μου εργασίας, θα ήθελα να δώσω τις θερμές μου ευχαριστίες πρώτα από όλα στον επιβλέποντα καθηγητή μου, τον κύριο Περικλή Χατζημίσιο, για την αρωγή του και ιδίως για τον ορθό προσανατολισμό στην εκπόνηση της παρούσας εργασίας. Οι εύστοχες παρατηρήσεις του σε συνδυασμό με τη συνεχή υποστήριξη που έλαβα σε όλη τη διάρκεια της διεργασίας, διαδραμάτισαν καθοριστικό ρόλο στην ομαλή συγγραφή της εργασίας. Ταυτόχρονα, θα ήθελα να εκφράσω τις ευχαριστίες μου στο επαγγελματικό περιβάλλον στο οποίο εργάζομαι και έχει άμεση σύνδεση με την κυβερνοασφάλεια, καθώς τα εμπειρικά βιώματα και η επαφή με ρεαλιστικές διαδικασίες παρακολούθησης και διαχείρισης συμβάντων συνέβαλαν καθοριστικά στην εμβάθυνση του νοήματος και της κατανόησης των διαδικασιών. Ιδιαίτερως, ένα μεγάλο ευχαριστώ αποδίδω στους φίλους μου Χαράλαμπο και Κατερίνα, τόσο για τη στήριξη τους, όσο και για τις ουσιαστικές παρεμβάσεις τους κατά τη διαδικασία της μελέτης και συγγραφής της εργασίας, καθώς με τις εύστοχες παρατηρήσεις τους και την ενθάρρυνσή τους, κατάφερα να παραμείνω συγκεντρωμένη στον στόχο μου και να διεξάγω ομαλά την έρευνα μου. Οδεύοντας στο τέλος, θα ήθελα να ευχαριστήσω την οικογένειά μου, για την υπομονή και την κατανόηση που μου παρείχαν από την αρχή της ακαδημαϊκής μου πορείας, στηρίζοντας τις αποφάσεις και τα όνειρά μου.

Περιεχόμενα

Πρόλογος.....	iv
Περίληψη.....	v
Abstract	vi
Ευχαριστίες	vii
Περιεχόμενα	viii
Κατάλογος Σχημάτων	xi
Κατάλογος Πινάκων.....	xiii
Συντομογραφίες.....	xiv
Κεφάλαιο 1ο: Εισαγωγή	1
1.1 Πλαίσιο της εργασίας	1
1.2 Στόχοι και σκοπός της εργασίας.....	2
1.3 Παρουσίαση κεφαλαίων.....	2
Κεφάλαιο 2ο: Θεωρητικό υπόβαθρο	4
2.1 Βασικές αρχές ασφάλειας πληροφοριών.....	4
2.1.1 Ορισμοί βασικών εννοιών	4
2.1.2 Πλαίσιο MITRE ATT&CK	6
2.1.3 Πρότυπα και πλαίσια ασφάλειας πληροφοριών	7
2.2 Τεχνολογικό και επιχειρησιακό περιβάλλον πλοίου	8
2.2.1 Πληροφοριακά συστήματα πλοίου.....	9
2.2.2 Συστήματα επιχειρησιακής τεχνολογίας πλοίου.....	10
2.2.3 Δίκτυα και συνδεσιμότητα	11
2.2.4 Κανονιστικό πλαίσιο ασφάλειας στη ναυτιλία.....	12
2.3 Βιβλιογραφική επισκόπηση και συναφείς προσεγγίσεις.....	14
2.3.1 Ερευνητικές προσεγγίσεις	14
2.3.2 Συγκριτική επισκόπηση λύσεων SIEM	15
2.3.3 Τοποθέτηση της παρούσας εργασίας.....	22
Κεφάλαιο 3ο: Σχεδιασμός και Υλοποίηση	24
3.1 Σκοπός και απαιτήσεις της υλοποίησης	24
3.1.1 Στόχος της υλοποίησης.....	24
3.1.2 Λειτουργικές απαιτήσεις	25
3.1.3 Μη λειτουργικές απαιτήσεις.....	27
3.2 Επιλογή τεχνολογιών και εργαλείων.....	28

3.2.1	Επιλογή SIEM ανοιχτού κώδικα	29
3.2.2	Επιλογή της πλατφόρμας Wazuh.....	30
3.2.3	Βασικά υποσυστήματα του Wazuh και ροή δεδομένων.....	31
3.3	Ανάλυση περιβάλλοντος υλικού και λογισμικού	33
3.3.1	Φυσικό σύστημα υποδοχής και τερματικό παρακολούθησης	33
3.3.2	Πλατφόρμα εικονικοποίησης	34
3.3.3	Λειτουργικό σύστημα εικονικής μηχανής	34
3.3.4	Δικτυακή διασύνδεση φυσικού συστήματος με εικονική μηχανή.....	35
3.4	Εγκατάσταση και βασική παραμετροποίηση εξυπηρετητή Wazuh	36
3.4.1	Διαδικασία εγκατάστασης	36
3.4.2	Έλεγχος ορθής λειτουργίας	40
3.4.3	Έλεγχος πρόσβασης και ασφαλούς επικοινωνίας υπηρεσιών	43
3.5	Εγκατάσταση και παραμετροποίηση του πράκτορα Wazuh	45
3.5.1	Διαδικασία εγκατάστασης	46
3.5.2	Επικοινωνία πράκτορα με κεντρικό εξυπηρετητή.....	47
3.5.3	Εμπλουτισμός τηλεμετρίας με χρήση Sysmon	48
3.6	Πηγές δεδομένων και πεδίο εφαρμογής	50
3.6.1	Η έννοια της πηγής δεδομένων σε ένα SIEM.....	50
3.6.2	Πηγές δεδομένων της παρούσας υλοποίησης.....	51
3.6.3	Εισαγωγή του συνόλου δεδομένων syslog	52
3.6.4	Πεδίο εφαρμογής του συστήματος	53
3.7	Μηχανισμός ανίχνευσης.....	54
3.7.1	Ρόλος και λειτουργία των αποκωδικοποιητών	54
3.7.2	Κανόνες ανίχνευσης και παραγωγή ειδοποιήσεων.....	55
3.7.3	Συσχέτιση αποκωδικοποιητών και κανόνων	57
3.7.4	Μεθοδολογία ανάπτυξης και επαλήθευσης.....	58
Κεφάλαιο 4ο:	Αποτελέσματα και πειραματική αξιολόγηση.....	59
4.1	Στόχος αξιολόγησης	59
4.1.1	Αντικείμενο αξιολόγησης.....	59
4.1.2	Κριτήρια και τεκμήρια επαλήθευσης	60
4.1.3	Μεθοδολογία και σενάρια δοκιμών.....	60
4.2	Αποτελέσματα λειτουργικότητας της υποδομής.....	61
4.2.1	Έλεγχος δικτυακής συνδεσιμότητας.....	61
4.2.2	Εμφάνιση συμβάντων στον πίνακα ελέγχου	63
4.2.3	Επαλήθευση αποκωδικοποίησης	64

4.2.4	Επαλήθευση ανίχνευσης.....	65
4.3	Παραγωγή και ανάλυση ειδοποιήσεων	66
4.3.1	Ενδεικτικές ειδοποιήσεις από τερματικό και σύνολο δεδομένων	66
4.3.2	Ανάλυση περιεχομένου ειδοποίησης.....	67
4.3.3	Αξιολόγηση επιπέδων σοβαρότητας	68
4.4	Απόδοση και λειτουργία σε περιορισμένο περιβάλλον.....	69
4.4.1	Κατανάλωση πόρων σε τυπική λειτουργία.....	69
4.4.2	Κατανάλωση πόρων υπό αυξημένο φορτίο	71
4.4.3	Συμπεριφορά σε απώλεια και επαναφορά σύνδεσης στο διαδίκτυο	72
4.4.4	Επιχειρησιακή αξία στο ναυτιλιακό περιβάλλον.....	73
4.5	Συγκριτική αξιολόγηση με άλλες πλατφόρμες.....	74
4.5.1	Κριτήρια σύγκρισης και απαιτήσεις ναυτιλιακής χρήσης	74
4.5.2	Αποτίμηση εναλλακτικών λύσεων βάσει κριτηρίων	75
4.5.3	Συνολική αποτίμηση της πλατφόρμας βάσει των ναυτιλιακών απαιτήσεων	77
Κεφάλαιο 5ο:	Συμπεράσματα	79
5.1	Συμπεράσματα.....	79
5.2	Περιορισμοί της μελέτης.....	80
5.3	Βελτιώσεις και μελλοντικές επεκτάσεις.....	81
ΒΙΒΛΙΟΓΡΑΦΙΑ.....		82

Κατάλογος Σχημάτων

Σχήμα 2.1: Ιεραρχία TTPs στο MITRE ATT&CK	6
Σχήμα 2.2: Τακτικές MITRE ATT&CK Enterprise	7
Σχήμα 2.3: Ενδεικτική σύνδεση IT και OT συστημάτων με την ξηρά	9
Σχήμα 2.4: Βασικές κατηγορίες OT συστημάτων σε πλοίο	10
Σχήμα 2.5: Ενδεικτική αρχιτεκτονική επικοινωνίας πλοίου με ξηρά	12
Σχήμα 2.6: Πρακτική αξία MSC.428 (98) σε πλοίο	13
Σχήμα 2.7: Ενδεικτική διεπαφή IBM QRadar Log Activity	16
Σχήμα 2.8: Αρχιτεκτονική συλλογής και ανάλυσης στο Splunk SIEM	17
Σχήμα 2.9: Αρχιτεκτονική συλλογής και επεξεργασίας δεδομένων στο Microsoft Sentinel	18
Σχήμα 2.10: Επίπεδα και βασικά εργαλεία του Security Onion	19
Σχήμα 2.11: Σύγκριση βασικών και εμπορικών λειτουργιών του Elastic Security.....	21
Σχήμα 2.12: Διεπαφή του Graylog	22
Σχήμα 3.1: Αρχιτεκτονική και ροή δεδομένων του συστήματος Wazuh.....	25
Σχήμα 3.2: Διεπαφή διαχείρισης τερματικών στο Wazuh	26
Σχήμα 3.3: Κεντρικός πίνακας ελέγχου Wazuh	27
Σχήμα 3.4: Αρχιτεκτονική του συστήματος Wazuh.....	31
Σχήμα 3.5: Υποστηριζόμενα λειτουργικά συστήματα από τους Wazuh Agents	32
Σχήμα 3.6: Ροή συλλογής, αποκωδικοποίησης και παραγωγής ειδοποιήσεων στο Wazuh.....	33
Σχήμα 3.7: Εργαστηριακή υποδομή και αρχιτεκτονική υλοποίησης	35
Σχήμα 3.8: Επιβεβαίωση δικτυακών ρυθμίσεων στην εικονική μηχανή	36
Σχήμα 3.9: Εικονική μηχανή Ubuntu που φιλοξενεί τον εξυπηρετητή Wazuh	37
Σχήμα 3.10: Εντολές επαλήθευσης της εγκατάστασης του Wazuh	38
Σχήμα 3.11: Απεικόνιση του καταλόγου ρυθμίσεων του Wazuh dashboard	39
Σχήμα 3.12: Έλεγχος δομής καταλόγων του Wazuh Indexer	40
Σχήμα 3.13: Έλεγχος κατάστασης υπηρεσίας Wazuh Indexer	41
Σχήμα 3.14: Έλεγχος κατάστασης υπηρεσίας Wazuh Dashboard	41
Σχήμα 3.15: Έλεγχος κατάστασης υπηρεσίας Wazuh Manager	42
Σχήμα 3.16: Έλεγχος διαθέσιμων θυρών των βασικών υπηρεσιών του Wazuh	42
Σχήμα 3.17: Έλεγχος κατάστασης της υπηρεσίας Wazuh Agent στα Windows	47
Σχήμα 3.18: Ροή δεδομένων από πηγές καταγραφής προς το Wazuh	51
Σχήμα 3.19: Προβολή Sysmon events	52
Σχήμα 3.20: Απόσπασμα του αρχείου 0490-junos_decoders.xml	55
Σχήμα 3.21: Απόσπασμα του αρχείου 0640-junos_rules.xml.....	56
Σχήμα 4.1: Επιβεβαίωση δικτυακής συνδεσιμότητας με χρήση της εντολής ping	62
Σχήμα 4.2: Έλεγχος διαθεσιμότητας των κρίσιμων θυρών στον εξυπηρετητή.....	62
Σχήμα 4.3: Εμφάνιση και ταξινόμηση συμβάντων από το τερματικό Windows	63
Σχήμα 4.4: Εμφάνιση συμβάντων από αρχείο καταγραφής Syslog	64
Σχήμα 4.5: Επιτυχής αποκωδικοποίηση συμβάντος vSRX σε δομημένα πεδία	64
Σχήμα 4.6: Καταγραφή ειδοποίησης στο αρχείο alerts.json του Wazuh	65
Σχήμα 4.7: Εμφάνιση ειδοποίησης και πεδίων Sysmon στον πίνακα ελέγχου Wazuh.....	66
Σχήμα 4.8: Κατανομή ειδοποιήσεων ανά επίπεδο σοβαρότητας στο Wazuh Dashboard.....	69
Σχήμα 4.9: Χρήση πόρων της εικονικής μηχανής σε τυπική λειτουργία	70
Σχήμα 4.10: Έλεγχος μνήμης και αποθηκευτικού χώρου μέσω τερματικού	71
Σχήμα 4.11: Χρήση πόρων της εικονικής μηχανής υπό αυξημένο φορτίο	72

Σχήμα 4.12: Συνέχιση εμφάνισης συμβάντων κατά την απώλεια σύνδεσης στο διαδίκτυο	73
Σχήμα 4.13: Κάλυψη ναυτιλιακών απαιτήσεων από την υλοποίηση.....	77

Κατάλογος Πινάκων

Πίνακας 2.1: Συνοπτική τοποθέτηση της εργασίας σε σχέση με τις ανάγκες.....	23
Πίνακας 3.1: Προδιαγραφές και λειτουργίες της λύσης SIEM.....	30
Πίνακας 3.2: Επίπεδα πρόσβασης στην πλατφόρμα Wazuh.....	44
Πίνακας 3.3: Ενδεικτική συσχέτιση συμβάντων Sysmon με το MITRE ATT&CK.....	49
Πίνακας 3.4: Ροή λειτουργίας αποκωδικοποιητών και κανόνων της υλοποίησης.....	58
Πίνακας 4.1: Κριτήρια αξιολόγησης του συστήματος.....	60
Πίνακας 4.2: Ενδεικτικά πεδία ειδοποίησης και ρόλος τους στη διερεύνηση	68
Πίνακας 4.3: Συγκριτική αποτίμηση κατηγοριών SIEM για ναυτιλιακή χρήση.....	76

Συντομογραφίες

API	Application Programming Interface
AIS	Automatic Identification System
ATT&CK	Adversarial Tactics, Techniques and Common Knowledge
BIMCO	Baltic and International Maritime Council
CAN-BUS	Controller Area Network Bus
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoC	Document of Compliance
ECDIS	Electronic Chart Display and Information System
ERP	Enterprise Resource Planning
ELK	Elasticsearch, Logstash, Kibana
GB	Gigabyte
GiB	Gibibyte
GMDSS	Global Maritime Distress and Safety System
GPS	Global Positioning System
HTTPS	Hypertext Transfer Protocol Secure
IBM	International Business Machines
ICMP	Internet Control Message Protocol
ICS	Industrial Control Systems
ID	Identifier
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IMO	International Maritime Organization
IoT	Internet of Things
IP	Internet Protocol
ISA	International Society of Automation
ISM	International Safety Management Code
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISPS	International Ship and Port Facility Security Code

IT	Information Technology
KQL	Kusto Query Language
MB	Megabyte
MSC	Maritime Safety Committee
NAT	Network Address Translation
NOC	Network Operations Center
OT	Operational Technology
PLC	Programmable Logic Controller
RADAR	Radio Detection and Ranging
RAM	Random Access Memory
RT_FLOW	Real-Time Flow
SATCOM	Satellite Communications
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Center
SMS	Safety Management System
SOLAS	Safety of Life at Sea
SPL	Search Processing Language
TCP	Transmission Control Protocol
TTPs	Tactics, Techniques, and Procedures
UHF	Ultra High Frequency
VHF	Very High Frequency
VM	Virtual Machine
vSRX	Virtual SRX
Wi-Fi	Wireless Fidelity
XDR	Extended Detection and Response
XML	Extensible Markup Language

Κεφάλαιο 1ο: Εισαγωγή

1.1 Πλαίσιο της εργασίας

Στις μέρες μας, η ναυτιλία αποτελεί έναν από τους πιο σημαντικούς τομείς της παγκόσμιας οικονομίας. Πάνω της στηρίζεται το μεγαλύτερο μέρος της παγκόσμιας εφοδιαστικής αλυσίδας και του διεθνούς εμπορίου. Ωστόσο, ο τρόπος λειτουργίας των σύγχρονων πλοίων έχει αλλάξει ριζικά. Ένα πλοίο δεν βασίζεται πλέον μόνο σε μηχανικά ή αυτόνομα συστήματα, αλλά αποτελεί στην ουσία έναν πλωτό τεχνολογικό κόμβο με πολύπλοκα δίκτυα. Μέσα στο ίδιο περιβάλλον λειτουργούν ταυτόχρονα ο εξοπλισμός πλοήγησης, οι δορυφορικές επικοινωνίες, οι υπολογιστές του καραβιού και τα συστήματα ελέγχου και αυτοματισμού του μηχανοστασίου. Ο εξοπλισμός αυτός λειτουργεί αδιάκοπα και παράγει μεγάλο όγκο δεδομένων, που σχετίζεται με την επιχειρησιακή ικανότητα και την ασφάλεια κάθε ταξιδιού.

Η ναυτιλία τα τελευταία χρόνια έχει αρχίσει να υιοθετεί ολοένα και περισσότερο την έννοια του ψηφιακού μετασχηματισμού με σκοπό τη βελτιστοποίηση των λειτουργιών, τη μείωση του κόστους, τη βελτίωση των ταχυτήτων επεξεργασίας δεδομένων, την προώθηση της βιωσιμότητας και την ενίσχυση της ασφάλειας. Οι τεχνολογικές εξελίξεις στον τομέα των πληροφοριών και των επικοινωνιών, ιδίως μέσω των δορυφορικών συνδέσεων στο Διαδίκτυο, έχουν επιτρέψει την απρόσκοπτη επικοινωνία μεταξύ των πληροφοριακών συστημάτων και των λειτουργικών συστημάτων των πλοίων με αντίστοιχα συστήματα που βρίσκονται στην ξηρά. Ωστόσο, αυτή η σύνδεση των συγκεκριμένων συστημάτων με το Διαδίκτυο, εισήγαγε μια σειρά από σημαντικούς κινδύνους ως προς την ασφάλειά τους. Αυτό το είδος ασφάλειας, γνωστό ως κυβερνοασφάλεια, ήταν μια άγνωστη έννοια για τον τομέα της ναυτιλίας, ο οποίος μέχρι τώρα θεωρούνταν ασφαλής λόγω της έλλειψης σύνδεσης στο Διαδίκτυο και της απομονωμένης φύσης των πλοίων στη θάλασσα.

Η ψηφιακή ασφάλεια στη ναυτιλία έχει ιδιαίτερα χαρακτηριστικά, καθώς το πλοίο αποτελεί ουσιαστικά μία απομονωμένη εγκατάσταση. Η λειτουργία των συστημάτων του διαφέρει σημαντικά σε σχέση με σταθερά δίκτυα που συναντάμε σε μία εταιρία στη στεριά. Η σύνδεση στο διαδίκτυο μπορεί να είναι περιορισμένη, ασταθής ή πολύ ακριβή. Για αυτό τον λόγο, η απομακρυσμένη υποστήριξη από τους τεχνικούς δεν είναι πάντα δεδομένη τη στιγμή που απαιτείται. Ταυτόχρονα, στο ίδιο περιβάλλον λειτουργούν δύο διαφορετικές κατηγορίες συστημάτων. Τα πληροφοριακά συστήματα, που χειρίζονται δεδομένα και επικοινωνία και τα επιχειρησιακά συστήματα, που ελέγχουν τις βασικές λειτουργίες του πλοίου. Κάθε ένα από αυτά έχει διαφορετικές ανάγκες και προτεραιότητες, κάτι που κάνει τη διαχείρισή τους αρκετά δύσκολη. Σε αυτές τις συνθήκες, η μεμονωμένη προστασία των συστημάτων δεν επαρκεί και κρίνεται απαραίτητη η ύπαρξη ενός κεντρικού σημείου συλλογής, ελέγχου και αξιολόγησης συμβάντων ασφαλείας.

Καθώς η τεχνολογία συνεχίζει να εξελίσσεται και να ενσωματώνεται σε κάθε πτυχή των ναυτιλιακών δραστηριοτήτων, ο τομέας αρχίζει να παρουσιάζει πολλές ευπάθειες σε πολλαπλά μέτωπα. Το βασικό πρόβλημα που αναδεικνύεται είναι η έλλειψη κεντρικού ελέγχου. Κάθε σύστημα παράγει τα δικά του δεδομένα και ειδοποιήσεις, με αποτέλεσμα οι πληροφορίες αυτές να μένουν διάσπαρτες σε διαφορετικές συσκευές. Η έλλειψη αυτή, καθιστά δύσκολη την έγκαιρη ανίχνευση των ύποπτων ενεργειών και καθιστά πιο αργή τη διερεύνηση ενός περιστατικού. Ένα μεμονωμένο συμβάν μπορεί να φαίνεται αρχικά ασήμαντο μόνο του, αλλά να αποτελεί ένδειξη μίας στοχευμένης επίθεσης όταν συσχετίζεται με άλλα γεγονότα από διαφορετικά συστήματα. Για τον λόγο αυτό, η συγκέντρωση και η

συνδυαστική ανάλυση συμβάντων αποτελεί απαραίτητη προϋπόθεση για τον πλήρη έλεγχο της ασφάλειας.

Τη λύση σε αυτές τις προκλήσεις προσφέρουν τα Συστήματα Διαχείρισης Πληροφοριών και Συμβάντων Ασφάλειας (Security Information and Event Management-SIEM). Χρησιμοποιούνται για τη συλλογή, την αποθήκευση και την ανάλυση δεδομένων ασφαλείας από διάφορες πηγές. Ουσιαστικά, μετατρέπουν τις ακατέργαστες καταγραφές σε αξιοποιήσιμη πληροφορία, αξιοποιώντας ειδικούς κανόνες, αποκωδικοποιητές και μηχανισμούς ειδοποίησης. Ωστόσο, η εφαρμογή ενός SIEM σε ναυτιλιακό περιβάλλον δεν μπορεί στην πράξη να αντιμετωπιστεί με τον ίδιο τρόπο όπως σε ένα εταιρικό δίκτυο. Υπάρχουν αρκετοί περιορισμοί όπως η ασταθής συνδεσιμότητα, το κόστος μεταφοράς των δεδομένων και η μεγάλη ποικιλία σε διαφορετικά συστήματα. Επομένως, ο σχεδιασμός μίας τέτοιου είδους λύσης πρέπει να προσαρμοστεί με στόχο να λειτουργεί εξ ολοκλήρου αυτόνομα μέσα στο πλοίο, χωρίς να εξαρτάται συνεχώς από εξωτερικές υπηρεσίες.

Αντικείμενο της παρούσας διπλωματικής εργασίας είναι η μελέτη, υλοποίηση και αξιολόγηση ενός αυτόνομου συστήματος SIEM ειδικά προσαρμοσμένου για πλοία. Η υλοποίηση γίνεται με χρήση λογισμικού ανοιχτού κώδικα. Η έρευνα επικεντρώνεται στην πρακτική εφαρμογή της συλλογής δεδομένων από τερματικά και συστήματα. Επίσης, εξετάζεται και η επεξεργασία αυτών των δεδομένων μέσω κανόνων και αποκωδικοποιητών, με στόχο την τελική παραγωγή ειδοποιήσεων που διευκολύνουν τον άμεσο εντοπισμό απειλών. Η παρούσα προσέγγιση δεν έχει στόχο να αντικαταστήσει πλήρως τα συστήματα ασφαλείας των οργανισμών. Αντίθετα, εξετάζει εάν μία αυτόνομη λύση σαν και αυτή μπορεί να λειτουργήσει ως αξιόπιστη βάση για την ενίσχυση της κυβερνοασφάλειας στο απαιτητικό αυτό περιβάλλον.

1.2 Στόχοι και σκοπός της εργασίας

Η εργασία επικεντρώνεται στον τομέα της ψηφιακής ασφάλειας στη ναυτιλία και πιο συγκεκριμένα στην ανάγκη για κεντρική συλλογή και ανάλυση συμβάντων ασφαλείας μέσα σε ένα πλοίο. Για τον λόγο αυτό, η παρούσα εξετάζει μια μέθοδο για τοπική και αυτόνομη επίβλεψη των απειλών. Κύριος στόχος είναι η ανάπτυξη και η αξιολόγηση ενός συστήματος SIEM, το οποίο αποτελεί την πρακτική βάση για την ενίσχυση της ασφάλειας πληροφοριών στο πλοίο. Η προσέγγιση διαμορφώθηκε εξ αρχής βάσει των πραγματικών αναγκών και των προκλήσεων που υπάρχουν. Συγκεκριμένα, επιδιώκεται η κεντρική συλλογή και οργάνωση των δεδομένων ασφαλείας από ετερογενή συστήματα του δικτύου. Σκοπός είναι η δυνατότητα για τοπική και αυτόνομη λειτουργία της υλοποίησης, χωρίς σταθερή και μόνιμη σύνδεση με εξωτερικές υπηρεσίες. Επίσης, επιδιώκεται η διερεύνηση περιστατικών μέσα από ένα ενιαίο περιβάλλον ελέγχου. Παράλληλα, επιδιώκεται η μείωση του κόστους εγκατάστασης και λειτουργίας, μέσω της χρήσης λογισμικού ανοιχτού κώδικα. Τελικός στόχος είναι να αποδειχθεί στην πράξη ότι μία λύση όπως αυτή παραμένει αποδοτική, ακόμη και κάτω από τους καθημερινούς περιορισμούς που υπάρχουν πραγματικά σε ένα πλοίο.

1.3 Παρουσίαση κεφαλαίων

Η εργασία οργανώνεται σε πέντε κεφάλαια. Ακολουθεί μία δομή η οποία ξεκινάει με το θεωρητικό υπόβαθρο, συνεχίζει με τον σχεδιασμό της υλοποίησης και την πειραματική αξιολόγηση, ενώ στο τέλος υπάρχουν τα συμπεράσματα.

Το κεφάλαιο δύο αφορά το θεωρητικό μέρος της εργασίας. Πιο συγκεκριμένα γίνεται μία αναφορά σε βασικές έννοιες κυβερνοασφάλειας που θα χρησιμοποιηθούν στην εργασία, για να γίνει ξεκάθαρη η ορολογία στη συνέχεια. Γίνεται επίσης αναφορά στο πλαίσιο MITRE ATT&CK και στα κυριότερα

πρότυπα ασφαλείας, που δείχνουν τον λόγο που χρειάζεται η καταγραφή και η αξιολόγηση των συμβάντων. Το επόμενο κομμάτι αφιερώνεται στο περιβάλλον του πλοίου. Εξετάζονται τα πληροφοριακά και επιχειρησιακά συστήματα, το δίκτυο, η συνδεσιμότητα και αναφέρεται επιγραμματικά το κανονιστικό πλαίσιο στη ναυτιλία. Το κεφάλαιο τελειώνει με τη σύγκριση ανάμεσα σε διαφορετικά συστήματα SIEM, με σκοπό να φανεί το κενό που επιχειρεί να καλύψει η υλοποίηση.

Στο κεφάλαιο τρίτο, παρουσιάζεται μια ανάλυση με στόχο να εξηγήσει τον σχεδιασμό του πειραματικού σκέλους, αναφέροντας όλα τα στάδια από τα οποία πέρασε η τελική μορφή του έργου. Στην αρχή καθορίζεται ο σκοπός της ανάπτυξης, βάσει των λειτουργικών απαιτήσεων που υποχρεούνται να καλύπτει η λύση, καθώς και των μη λειτουργικών απαιτήσεων που είναι εξίσου χρήσιμες. Για αυτούς τους λόγους λοιπόν, μετά από έρευνα και μελέτη πιθανών επιλογών, η ανοιχτού κώδικα πλατφόρμα ασφαλείας Wazuh κρίθηκε η πιο κατάλληλη. Γίνεται αναφορά στα επιμέρους υποσυστήματα της πλατφόρμας και στον τρόπο ροής των δεδομένων της. Ακολουθεί η περιγραφή του περιβάλλοντος υλικού και λογισμικού, όπως και ο τρόπος δικτυακής επικοινωνίας μεταξύ τους. Πάνω σε αυτή την υποδομή, παρουσιάζεται η εγκατάσταση του εξυπηρετητή και οι απαραίτητοι έλεγχοι του, ώστε να επιτυγχάνεται η ορθή επικοινωνία των υπηρεσιών του. Στο επόμενο στάδιο ρυθμίζεται ο πράκτορας στο τερματικό, περιγράφεται η σύνδεση του με τον κεντρικό εξυπηρετητή και αναφέρεται η χρήση του εργαλείου παρακολούθησης Sysmon. Έπειτα παρουσιάζεται η διαδικασία εισαγωγής των δεδομένων τύπου Syslog και το πεδίο εφαρμογής του συστήματος. Το κεφάλαιο κλείνει με την παρουσίαση του μηχανισμού ανίχνευσης και συγκεκριμένα την περιγραφή του ρόλου των αποκωδικοποιητών και τη χρήση των κανόνων, με στόχο την παραγωγή ειδοποιήσεων.

Το τέταρτο κεφάλαιο, επικεντρώνεται στην πειραματική αξιολόγηση της προτεινόμενης υλοποίησης, με αντικειμενικό σκοπό την επαλήθευση της επιχειρησιακής της ικανότητας ως πλατφόρμα κεντρικής συλλογής και ανάλυσης συμβάντων ασφαλείας. Η αξιολόγηση υπερβαίνει τη θεωρητική παράθεση χαρακτηριστικών. Εστιάζει στην απόκριση του συστήματος σε ελεγχόμενες εργαστηριακές συνθήκες, εξετάζοντας την πλήρη αλυσίδα λειτουργίας από τη συλλογή των δεδομένων έως την τελική παραγωγή των ειδοποιήσεων. Η ροή του κεφαλαίου ξεκινάει με τον προσδιορισμό των στόχων, των κριτηρίων και της μεθοδολογίας των δοκιμών. Παράλληλα θέτει το πλαίσιο για την ανάλυση που ακολουθεί. Στη συνέχεια, παρουσιάζονται αναλυτικά τα αποτελέσματα λειτουργικότητας της υποδομής και η επεξεργασία των ειδοποιήσεων. Ιδιαίτερη έμφαση δίνεται και στην αξιολόγηση της απόδοσης, καθώς και στη συμπεριφορά της υποδομής σε συνθήκες περιορισμένης συνδεσιμότητας, οι οποίες υπάρχουν στο ναυτιλιακό περιβάλλον. Το κεφάλαιο ολοκληρώνεται με μια συγκριτική αξιολόγηση της λύσης έναντι εναλλακτικών πλατφορμών, αναδεικνύοντας τα πλεονεκτήματα της παρούσας υλοποίησης.

Το πέμπτο κεφάλαιο, αποτελεί τον επίλογο της εργασίας και παρουσιάζει τα συμπεράσματα που προέκυψαν από τη σχεδίαση και τις δοκιμές του συστήματος. Γίνεται η αποτίμηση των αποτελεσμάτων, βάσει των απαιτήσεων που τέθηκαν και αναλύεται η χρησιμότητα της εργασίας για τον τομέα της ναυτιλίας. Στο ίδιο κεφάλαιο εντοπίζονται και οι βασικοί περιορισμοί της μελέτης, καθώς οι δοκιμές περιορίστηκαν σε εργαστηριακό κομμάτι. Η εργασία ολοκληρώνεται με τις προτάσεις για μελλοντικές επεκτάσεις της εργασίας και την εφαρμογή της σε πραγματικά σενάρια πλοίων.

Κεφάλαιο 2ο: Θεωρητικό υπόβαθρο

Προκειμένου να αξιολογηθεί σωστά ένα σύστημα SIEM σε ναυτιλιακό περιβάλλον, είναι απαραίτητο να κατανοηθούν πρώτα οι βασικές αρχές της κυβερνοασφάλειας, σε συνδυασμό με τις ιδιαιτερότητες που παρουσιάζει η λειτουργία ενός πλοίου.

Το δίκτυο σε ένα καράβι διαφέρει αρκετά σε σχέση με αυτό ενός τυπικού οργανισμού στην ξηρά. Πρόκειται για ένα σύνθετο περιβάλλον, στο οποίο τα συστήματα πληροφορικής διασυνδέονται με τα συστήματα επιχειρησιακής λειτουργίας. Επιπλέον, η σύνδεση στο διαδίκτυο είναι συχνά περιορισμένη ή ασταθής, ενώ την ίδια στιγμή είναι απαραίτητο να λειτουργούν όλα τα συστήματα συνεχώς και χωρίς διακοπές.

Μέσα από το θεωρητικό υπόβαθρο, γίνεται κατανοητό το γιατί η συγκέντρωση, η ανάλυση και ο έλεγχος των περιστατικών ασφαλείας από ένα κεντρικό σημείο αποτελούν βασική ανάγκη για τη σύγχρονη ναυτιλία.

2.1 Βασικές αρχές ασφάλειας πληροφοριών

Η κατανόηση της βασικής ορολογίας των συστημάτων SIEM, είναι απαραίτητη για οποιαδήποτε μελέτη πάνω στον τομέα της ασφάλειας των πληροφοριακών συστημάτων. Οι όροι που αναλύονται στην παρούσα υποενότητα συχνά συγχέονται, προκαλώντας λάθος ερμηνείες τόσο στην τεχνική ανάλυση όσο και στη διαχείριση απειλών. Παρακάτω ξεκαθαρίζεται η ερμηνεία κάθε λέξης.

2.1.1 Ορισμοί βασικών εννοιών

2.1.1.1 Συμβάν

Με τον όρο συμβάν (event), αναφερόμαστε σε οτιδήποτε συμβαίνει σε ένα σύστημα ή δίκτυο υπολογιστών. Στην πράξη, εννοούμε κάθε ενέργεια η οποία καταγράφεται από το σύστημα. Παραδείγματα συμβάντων αποτελούν η σύνδεση ενός χρήστη, η αποτυχημένη προσπάθεια εισόδου σε ένα λογαριασμό, η φόρτωση μίας ιστοσελίδας ή και η επανεκκίνηση μίας υπηρεσίας. Τα γεγονότα αυτά έχουν τη δυνατότητα να προέρχονται από διαφορετικές πηγές ταυτόχρονα. Οι πιο συνηθισμένες είναι τα τείχη προστασίας, τα λειτουργικά συστήματα των διακομιστών και οι εφαρμογές που τρέχουν στο δίκτυο [1].

Ένα συμβάν δεν θεωρείται από μόνο αν είναι επικίνδυνο ή αθώο, αποτελεί μία απλή πληροφορία. Ένα περιστατικό, όπως έξι αποτυχημένες προσπάθειες σύνδεσης, χαρακτηρίζεται από πολλαπλές σημασίες. Για παράδειγμα ένας χρήστης που ενδεχομένως έχει ξεχάσει τον κωδικό του αλλά μπορεί να δηλώνει και μία προσπάθεια τρίτου να αποκτήσει πρόσβαση χωρίς άδεια. Σε μεγάλους οργανισμούς, ο αριθμός παραγωγής συμβάντων καθημερινά είναι τεράστιος, με αποτέλεσμα να μην αρκεί η ανθρώπινη ανάλυση για την επεξήγηση της σημασίας τους [2].

2.1.1.2 Καταγραφή

Μία καταγραφή (log) είναι η καταγεγραμμένη αναπαράσταση ενός ή περισσότερων συμβάντων. Με άλλα λόγια, είναι το γραπτό αρχείο που κρατάει το σύστημα. Κάθε αρχείο καταγραφής αποτελείται από ξεχωριστές εγγραφές, όπου η κάθε μία αναφέρεται σε ένα συγκεκριμένο συμβάν. Περιέχει πληροφορίες όπως η ώρα που συνέβη, η πηγή που προέρχεται και μια σύντομη περιγραφή. Αρχικά τα αρχεία καταγραφής χρησιμοποιήθηκαν κυρίως στον εντοπισμό τεχνικών σφαλμάτων. Πλέον εξυπηρετούν

σκοπούς όπως η ανίχνευση επιθέσεων, η έρευνα τυχόν παραβιάσεων και η τήρηση νομικών απαιτήσεων [1].

Σε ένα SIEM, ο ρόλος της καταγραφής είναι κεντρικός. Τα συστήματα έχουν τη δυνατότητα συλλογής εγγραφών από πολλαπλές και διαφορετικές πηγές. Στη συνέχεια, τις μετατρέπουν σε όμοια μορφή ώστε να μπορούν να συγκριθούν μεταξύ τους και έπειτα να αποθηκευτούν για μελλοντική χρήση. Η σημασία της αποθήκευσης έχει ιδιαίτερη σημασία, κυρίως σε αργές ή συγκαλυμμένες επιθέσεις, όπου εξελίσσονται σε βάθος χρόνου και δεν γίνονται αντιληπτές κατευθείαν. Ωστόσο, η ποιότητα μίας καταγραφής δεν είναι πάντα εγγυημένη. Η πηγή μπορεί να είναι εκτός λειτουργίας, να μην συμπληρώνει όλα τα απαραίτητα πεδία και στη χειρότερη περίπτωση, να έχει παραβιαστεί από κακόβουλο χρήστη ο οποίος εισάγει ψεύτικες εγγραφές [2].

2.1.1.3 Ειδοποίηση

Η ειδοποίηση (alert) είναι ένα αυτόματο μήνυμα που παράγει ένα σύστημα SIEM. Στις περιπτώσεις όπου ένα ή περισσότερα συμβάντα πληρούν συγκεκριμένα κριτήρια, εμφανίζονται ειδοποιήσεις οι οποίες ενδέχεται να αφορούν κακόβουλη δραστηριότητα. Τα κριτήρια αυτά καθορίζονται από κανόνες που είτε έχει δημιουργήσει ο αναλυτής είτε παράγει αυτόματα το σύστημα, μέσω αναγνώρισης μοτίβων. Για παράδειγμα, ένας κανόνας μπορεί να δημιουργήσει μία ειδοποίηση στην περίπτωση όπου έχουν καταγραφεί πέντε συνεχόμενες αποτυχημένες προσπάθειες σύνδεσης μέσα σε μόνο ένα λεπτό ή όταν ένα από τα συστήματα προσπαθεί να επικοινωνήσει με μία γνωστή κακόβουλη διεύθυνση στο διαδίκτυο. Στις περιπτώσεις ενεργοποίησης μίας ειδοποίησης, εμφανίζεται στην οθόνη του αναλυτή για την περαιτέρω αξιολόγηση της [2].

Μία ειδοποίηση δεν αφορά απαραίτητα κάποιο σημαντικό πρόβλημα. Συνήθως χρειάζεται και η ανθρώπινη επαλήθευση. Ο αναλυτής είναι αυτός που καλείται να κρίνει εάν πρόκειται για αληθινή απειλή ή αν πρόκειται για ψευδές αποτέλεσμα που ταξινομήθηκε ως ύποπτο. Το κυριότερο πρόβλημα που υπάρχει είναι ο γρήγορος πολλαπλασιασμός των ειδοποιήσεων. Τα αθώα συμβάντα είναι κατά κύριο λόγο πολύ περισσότερα από τα κακόβουλα. Ακόμα και ένας κανόνας με χαμηλό ποσοστό σφάλματος είναι ικανός να παράγει εκατοντάδες ψευδείς ειδοποιήσεις ημερησίως. Ως αποτέλεσμα, ο αναλυτής έρχεται αντιμέτωπος με μεγάλο όγκο δουλειάς και αναγκάζεται να κάνει δειγματοληπτικό έλεγχο αντί για πλήρη αξιολόγηση του συνόλου [2].

2.1.1.4 Περιστατικό

Ένα περιστατικό (Incident), αποτελεί το επιβεβαιωμένο περιστατικό που παραβιάζει την ασφάλεια ή τους κανόνες ενός οργανισμού [1]. Το περιστατικό δεν αντιμετωπίζεται αυτόματα παρά μόνο επιβεβαιώνεται από τον αναλυτή, σε συνέχεια σχετικής του έρευνας. Πιο συγκεκριμένα, εξετάζει τις ύποπτες ειδοποιήσεις, αναλύει τυχόν πρόσθετες πηγές πληροφοριών και στο τέλος αποφασίζει αν πρόκειται για πραγματική επίθεση ή παραβίαση. Στην περίπτωση επιβεβαίωσης, ανοίγει μία υπόθεση και η έρευνα αναθέτεται σε εξειδικευμένες ομάδες ανάλυσης με στόχο τον προσδιορισμό της έκτασης και του αντίκτυπου που έχει η επίθεση [2].

Η πιο απαιτητική φάση ολόκληρης της διαδικασίας είναι η διαχείριση του περιστατικού. Συχνά εμπλέκονται διαφορετικοί τομείς πέρα από την τεχνική ομάδα. Στις σοβαρές περιπτώσεις η ομάδα ασφαλείας έχει ως ρόλο τον συντονισμό με το νομικό τμήμα, τη διοίκηση και τις αρχές επιβολής του νόμου. Ταυτόχρονα, οι διαχειριστές ενδέχεται να χρειαστεί να αλλάξουν άμεσα τις ρυθμίσεις καταγραφής. Έτσι, υπάρχει η δυνατότητα συλλογής μεγαλύτερου όγκου πληροφοριών που αφορούν το συμβάν ή αντίθετα ο περιορισμός των καταγραφών που κατακλύζουν το σύστημα [1].

2.1.2 Πλαίσιο MITRE ATT&CK

Το πλαίσιο MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge), είναι μία ελεύθερη βάση δεδομένων. Αναφέρει τον τρόπο με τον οποίο κακόβουλοι δράστες δρουν σε συστήματα και στο δίκτυο [3]. Σε αντίθεση με άλλα θεωρητικά μοντέλα, αποτελεί συλλογή παρατηρήσεων η οποία βασίζεται σε πραγματικές επιθέσεις που έχουν πραγματοποιηθεί. Σημαντικό είναι το γεγονός ότι ανανεώνεται συνεχώς από την ευρύτερη κοινότητα της ψηφιακής ασφάλειας. Κύριο χαρακτηριστικό του αποτελεί ότι εστιάζει στη συμπεριφορά ενός επιτιθέμενου, αφότου παραβιαστεί το σύστημα. Αναλύει το πως κινείται στο δίκτυο, πως κρύβει τα ίχνη του και πως φτάνει στον τελικό στόχο. Στην ουσία προσφέρει ένα κοινό σημείο αναφοράς, επιτρέποντας τη χρήση κοινής ορολογίας για την ανάλυση τεχνικών επιθέσεων [4].

Το πλαίσιο έχει υιοθετηθεί ευρέως, λόγω της μεγάλης πρακτικής του αξίας. Μεγάλοι οργανισμοί το αξιοποιούν για ανάλυση πληροφοριών και τη δημιουργία ρεαλιστικών σεναρίων επιθέσεων. Ταυτόχρονα, εταιρίες και συστήματα SIEM, το ενσωματώνουν στα προϊόντα τους με στόχο τη γρήγορη ανίχνευση και τη διαχείριση ειδοποιήσεων [4].

Το ATT&CK χωρίζεται σε τρεις βασικούς τομείς εφαρμογής [4]:

- Εταιρικά δίκτυα (Enterprise),
- Βιομηχανικά συστήματα ελέγχου (ICS),
- Κινητές συσκευές (Mobile).



Σχήμα 2.1: Ιεραρχία TTPs στο MITRE ATT&CK [4]

Όπως φαίνεται στο Σχήμα 2.1, η γνώση στο πλαίσιο MITRE ATT&CK οργανώνεται σε τρία βασικά επίπεδα. Το επίπεδο της τακτικής, της τεχνικής και οι διαδικασίες αποτελούν τα λεγόμενα TTPs [3]. Για λόγους καλύτερης οργάνωσης, οι τεχνικές χωρίστηκαν αργότερα σε υποτεχνικές, προσφέροντας μεγαλύτερη λεπτομέρεια.

Κεφάλαιο 2

Οι τακτικές προσδιορίζουν τον σκοπό που έχει ένας κακόβουλος χρήστης σε κάθε φάση της επίθεσης. Παράδειγμα τακτικών αποτελεί η απόκτηση της αρχικής πρόσβασης σε ένα σύστημα, η εκτέλεση κώδικα, η διατήρηση της παρουσίας του και η υποκλοπή δεδομένων [3]. Στο εταιρικό δίκτυο, το πλαίσιο εμφανίζει 15 τακτικές, που καλύπτουν ένα ολόκληρο κύκλο ζωής μίας επίθεσης, από τα πρώτα βήματα αναγνώρισης έως τον στόχο [4]. Από την άλλη, οι τεχνικές περιγράφουν τις μεθόδους που χρησιμοποιήθηκαν για την υλοποίηση της επίθεσης του εκάστοτε στόχου. Για ακόμα μεγαλύτερη λεπτομέρεια, οι τεχνικές μπορούν να αναλυθούν σε επιμέρους υποτεχνικές. Τέλος, οι διαδικασίες αποτελούν παραδείγματα από πραγματικές επιθέσεις. Καταγράφουν τον τρόπο με τον οποίο ένας χρήστης, μία ομάδα ή ένα κακόβουλο λογισμικό εφάρμοσε τις τεχνικές στην πράξη [3].

ID	Name	Description
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Stealth	The adversary is trying to hide and conceal their actions, appearing as normal behavior.
TA0112	Defense Impairment	The adversary is trying to break security mechanisms, pipelines, and tooling so defenders can't see or trust what's happening.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Σχήμα 2.2: Τακτικές MITRE ATT&CK Enterprise [3]

Η πρακτική χρησιμότητα της δομής είναι ότι επιτρέπει τη σύνδεση απλών καταγραφών του συστήματος με πραγματικές απειλές. Κάθε συμβάν δεν θεωρείται απαραίτητα ένδειξη επίθεσης. Με τη χρήση του πλαισίου αυτού, οποιαδήποτε ενέργεια μπορεί να αξιολογηθεί ως μια πιθανή τεχνική που ανήκει σε κάποια τακτική. Το MITRE ATT&CK προτείνει συγκεκριμένους τρόπους ανίχνευσης για κάθε τεχνική. Παράλληλα, υποδεικνύει τα απαραίτητα δεδομένα που πρέπει να συλλέγονται και διάφορα μέτρα για τον περιορισμό του κινδύνου. Οι πληροφορίες αυτές είναι ιδιαίτερα σημαντικές για την ανάπτυξη κανόνων σε ένα σύστημα SIEM [3] [4].

2.1.3 Πρότυπα και πλαίσια ασφάλειας πληροφοριών

2.1.3.1 ISO/IEC 27001

Το ISO/IEC 27001 αποτελεί κορυφαίο παγκόσμιο πρότυπο πιστοποίησης για τη διαχείριση της ασφάλειας πληροφοριών. Παράλληλα είναι βασικό σημείο αναφοράς των οργανισμών που επιδιώκουν συστηματική προστασία των δεδομένων τους. Το πρότυπο αυτό δεν έχει στόχο την εφαρμογή συγκεκριμένων τεχνολογικών λύσεων. Επιδιώκει, τον καθορισμό ενός ολοκληρωμένου πλαισίου διαδικασιών, το λεγόμενο Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (Information Security

Management System - ISMS). Έτσι, ένας οργανισμός έχει τη δυνατότητα να εντοπίζει κινδύνους που αντιμετωπίζει, να επιλέγει τα κατάλληλα μέτρα προστασίας και να τα τεκμηριώνει επίσημα [5]. Ως φιλοσοφία είναι βασισμένο σε έναν κύκλο συνεχούς βελτίωσης το οποίο σχεδιάζει πολιτικές, τις εφαρμόζει, παρακολουθεί την αποτελεσματικότητά τους και τέλος τις αναθεωρεί [6].

Στην παρούσα εργασία, το πρότυπο ISO/IEC 27001 είναι άμεσα συνδεδεμένο με το αντικείμενο της μελέτης. Συγκεκριμένα ορίζει ρητά την παρακολούθηση και την καταγραφή των συμβάντων ενός συστήματος, ως απαραίτητους ελέγχους ασφαλείας [6]. Άρα, κάθε οργανισμός που επιθυμεί να συμμορφωθεί με τις απαιτήσεις που έχει το πρότυπο, οφείλει να διατηρεί τα αρχεία καταγραφής και να τα αναλύει συστηματικά. Αυτή η ανάγκη καλύπτεται πλήρως στην πράξη από ένα σύστημα SIEM [5]. Το πλαίσιο αυτό, αποτελεί το γενικό κανονιστικό και θεωρητικό υπόβαθρο που τεκμηριώνει την αναγκαιότητα που υπάρχει στην υλοποίηση του εργαλείου που αναπτύσσεται στα επόμενα κεφάλαια.

2.1.3.2 IEC 62443

Το πρότυπο IEC 62443 είναι ένα διεθνές πρότυπο ασφαλείας, το οποίο αναπτύχθηκε από τον Διεθνή Οργανισμό Αυτοματισμού (International Society of Automation - ISA). Ως στόχο έχει τη θωράκιση των βιομηχανικών συστημάτων αυτοματισμού και ελέγχου. Οργανώνεται σε τέσσερις κατηγορίες [7]:

- Τις γενικές αρχές,
- Τις πολιτικές και διαδικασίες,
- Την ασφάλεια των κεντρικών συστημάτων και
- Την ασφάλεια των επιμέρους εξαρτημάτων.

Μία σημαντική έννοια που εισάγει, είναι ο διαχωρισμός του δικτύου στις λεγόμενες ζώνες ασφαλείας (zones). Συγκεκριμένα ομαδοποιεί τα στοιχεία που έχουν παρόμοιες ανάγκες προστασίας. Η επικοινωνία και η ανταλλαγή δεδομένων ανάμεσα στις ζώνες ελέγχεται μέσα από συγκεκριμένα κανάλια επικοινωνίας, τους αγωγούς (conduits). Η αρχιτεκτονική αυτή, βασίζεται στη φιλοσοφία της άμυνας σε βάθος. Το σύστημα προστατεύεται από πολλαπλά και διαδοχικά επίπεδα ασφαλείας. Έτσι, εάν ο κακόβουλος χρήστης καταφέρει να σπάσει την άμυνα που υπάρχει σε μία ζώνη, να μην αποκτήσει πρόσβαση σε ολόκληρη την υποδομή [7].

Είναι σημαντικό στην παρούσα υλοποίηση να αναφερθεί το IEC 62443, καθώς τα σύγχρονα πλοία διαθέτουν βιομηχανικά συστήματα ελέγχου, τα οποία λειτουργούν παράλληλα με τα τυπικά δίκτυα πληροφορικής [8]. Παράλληλα, το πρότυπο τονίζει ότι η συνεχής παρακολούθηση του συστήματος αποτελεί απαραίτητο μηχανισμό προστασίας. Σε αυτό συμπεριλαμβάνεται η υλοποίηση SIEM για τη συγκέντρωση και την αυτόματη ανάλυση των δεδομένων ασφαλείας από όλες τις συσκευές ελέγχου [7]. Αν και η συγκεκριμένη εργασία εστιάζει κυρίως στο περιβάλλον πληροφορικής του πλοίου, η αρχιτεκτονική που προτείνεται μπορεί να επεκταθεί και σε βιομηχανικά συστήματα που χρησιμοποιούν λειτουργικά συστήματα γενικής χρήσης. Παράδειγμα αποτελεί το σύστημα ηλεκτρονικής ναυτιλιακής πλοήγησης, το οποίο κρατάει συνεχώς δεδομένα μέσω του καταγραφέα συμβάντων.

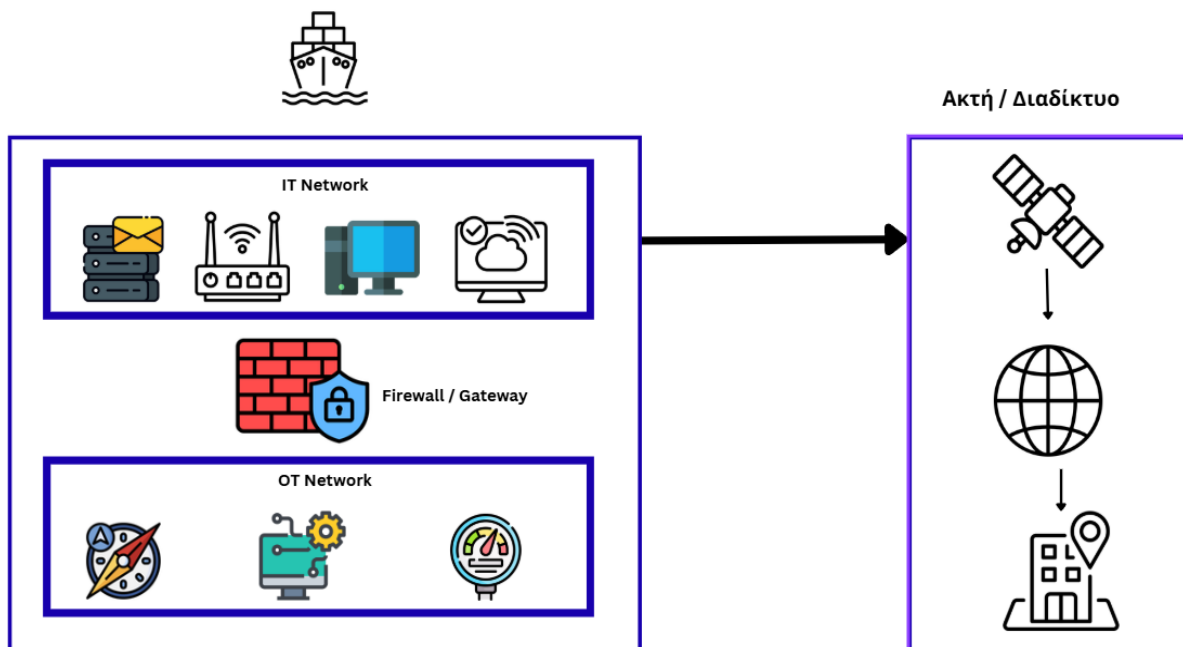
2.2 Τεχνολογικό και επιχειρησιακό περιβάλλον πλοίου

Στην ενότητα αυτή παρουσιάζονται τα βασικά τεχνολογικά και κανονιστικά χαρακτηριστικά του περιβάλλοντος της ναυτιλίας. Αναλύονται τα πληροφοριακά συστήματα (Information Technology - IT) καθώς και τα συστήματα επιχειρησιακής τεχνολογίας (Operational Technology - OT), που υπάρχουν σε ένα πλοίο και οι ιδιαιτερότητες της δικτυακής υποδομής. Τέλος, παρουσιάζεται το κανονιστικό πλαίσιο της κυβερνοασφάλειας στη ναυτιλία.

2.2.1 Πληροφοριακά συστήματα πλοίου

Ένα σύγχρονο πλοίο στηρίζεται σε μία πλήρη υποδομή πληροφορικής. Η ποικιλόμορφη μορφή και η έκταση αυτής της υποδομής καθορίζεται κυρίως από το μέγεθος, τον τύπο και τις επιχειρησιακές ανάγκες του κάθε καραβιού. Στις περισσότερες περιπτώσεις, το δίκτυο χωρίζεται σε δύο κύριες κατηγορίες, το επιχειρηματικό (business network) και του πληρώματος (crew network). Το επιχειρηματικό δίκτυο αποτελείται από υπολογιστές και διακομιστές που υποστηρίζουν κρίσιμες λειτουργίες όπως το ηλεκτρονικό ταχυδρομείο, το σύστημα διαχείρισης των πόρων (ERP) και τον αυτόματο συγχρονισμό αρχείων. Σε αυτό η πρόσβαση είναι εφικτή μόνο από εξουσιοδοτημένο προσωπικό του πληρώματος. Ταυτόχρονα η προσθήκη μίας νέας συσκευής επιτρέπεται αποκλειστικά και μόνο από τον διαχειριστή του συστήματος. Από την άλλη πλευρά, το δίκτυο του πληρώματος προσφέρει ασύρματη σύνδεση δικτύου για την επικοινωνία και την ψυχαγωγία των μελών του καραβιού. Η αρχιτεκτονική του, παρέχει ασύρματη πρόσβαση στο διαδίκτυο για την ψυχαγωγία και την επικοινωνία του προσωπικού μέσω σημείων πρόσβασης σε κάθε κατάσταση. Επίσης υπάρχουν και ενσύρματες συνδέσεις στις καμπίνες, χωρίς περιορισμό στο εύρος των συνδεδεμένων συσκευών [9].

Η δικτυακή υποδομή του πλοίου παρουσιάζει σημαντική εξέλιξη τα τελευταία χρόνια, ενώ έχει ενσωματώσει και εργαλεία παρακολούθησης που διασφαλίζουν την ασφάλεια της. Ο διαχωρισμός αυτός εξυπηρετεί διπλό σκοπό. Από τη μία παρέχει εύκολη διαχείριση και αφετέρου περιορίζει τις επιπτώσεις μίας πιθανής επίθεσης. Πιο συγκεκριμένα αν παραβιαστεί ένα τμήμα, τα υπόλοιπα συνεχίζουν τη λειτουργία τους κανονικά και μπορούν να χρησιμοποιηθούν για την αποκατάσταση [9]. Ωστόσο η σύνδεση συστημάτων IT και OT που έχουν στόχο την ασφαλή πλεύση, αυξάνει τυχόν ψηφιακούς κινδύνους. Πλέον παραδοσιακά συστήματα που σχεδιάστηκαν χωρίς προδιαγραφές ασφαλείας, βρίσκονται εκτεθειμένα σε δίκτυα με πρόσβαση στο διαδίκτυο [10]. Όπως φαίνεται και στο Σχήμα 2.3, αυτά τα δύο δίκτυα απομονώνονται μέσω του τείχους προστασίας και η επικοινωνία τους με τη στεριά πραγματοποιείται κυρίως μέσω δορυφορικών συστημάτων.

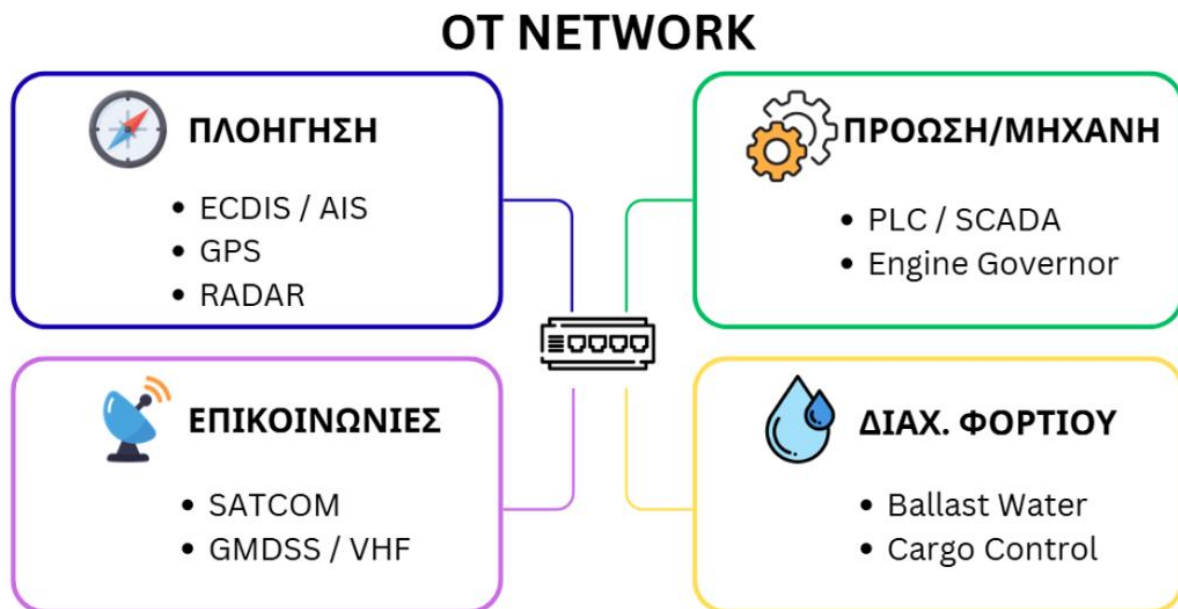


Σχήμα 2.3: Ενδεικτική σύνδεση IT και OT συστημάτων με την ξηρά

Παρά την εξέλιξη αυτή, η ψηφιακή ετοιμότητα στα πλοία παρουσιάζει ακόμη ένα αδύναμο σημείο. Σε έρευνα με δείγμα 133 έμπειρων ναυτικών και στελεχών από το χερσαίο προσωπικό, τα αποτελέσματα έδειξαν ότι το 79% από τους ερωτηθέντες θεωρεί τους υπολογιστές του πλοίου και τη χρήση του διαδικτύου το πιο ευάλωτο σημείο. Παράλληλα, οι τιμές έδειξαν ότι η πλειοψηφία θεωρεί πως τα συστήματα πληροφορικής επί του πλοίου δεν είναι πλήρως προστατευμένα για τυχόν απειλές ασφαλείας και απαιτούν επενδύσεις για την αναβάθμισή τους. Επιπρόσθετα, η χρήση ξεπερασμένων λογισμικών αποτελούν πρόβλημα με μόνιμο κίνδυνο, καθώς η καθυστέρηση στην εγκατάσταση ενημερώσεων ασφαλείας αφήνει τα συστήματα εκτεθειμένα [11]. Συμπερασματικά από τα δεδομένα που αναφέρθηκαν, επιβεβαιώνεται η ανάγκη για συνεχή έλεγχο στο περιβάλλον της ναυτιλίας και κρίνεται αναγκαίος ο ρόλος που καλείται να επιλύσει ένα σύστημα SIEM.

2.2.2 Συστήματα επιχειρησιακής τεχνολογίας πλοίου

Τα συστήματα επιχειρησιακής τεχνολογίας είναι το σύνολο του υλικού και του λογισμικού, που ελέγχει, παρακολουθεί και αυτοματοποιεί τις φυσικές λειτουργίες του πλοίου. Σε αντίθεση με τα συστήματα πληροφορικής, τα συγκεκριμένα αλληλοεπιδρούν άμεσα με τον φυσικό κόσμο. Τα δεδομένα και οι αποφάσεις που λαμβάνονται από αυτά έχουν άμεσο αντίκτυπο στη λειτουργία και στην ασφάλεια του σκάφους. Όπως φαίνεται και στο Σχήμα 2.4, μπορούν να χωριστούν σε τέσσερις κατηγορίες. Τα συστήματα επικοινωνίας, τα συστήματα πρόωσης και μηχανής, τα συστήματα πλοήγησης και τα συστήματα διαχείρισης φορτίου. Ο διεθνής ναυτιλιακός οργανισμός, έχει επισημάνει και τα τέσσερα αυτά υποσυστήματα ως τα πιο ευάλωτα σε ένα πλοίο [12]. Στην πράξη ορισμένα υποσυστήματα επικοινωνιών βρίσκονται στο όριο IT με OT τεχνολογιών. Στην παρούσα εργασία ταξινομούνται ως επιχειρησιακά όταν υποστηρίζουν λειτουργίες που αφορούν την ασφάλεια της ναυσιπλοΐας και ως πληροφοριακά όταν αναφέρονται στην επικοινωνία του πληρώματος.



Σχήμα 2.4: Βασικές κατηγορίες OT συστημάτων σε πλοίο [12]

Η διαφορά μεταξύ των δύο κατηγοριών συστημάτων δεν είναι μόνο τεχνική, αλλά και φιλοσοφική. Τα πληροφοριακά δίκτυα εστιάζουν στην εμπιστευτικότητα των δεδομένων, ενώ τα επιχειρησιακά δίκτυα στη διαθεσιμότητα. Μια διακοπή στα μηχανήματα, μπορεί να επιφέρει σημαντικές βλάβες οι οποίες θέτουν σε κίνδυνο τη ζωή του πληρώματος. Ως αποτέλεσμα δεν μπορούν να σταματήσουν τη λειτουργία

τους εύκολα για τυχόν αναβαθμίσεις, ενώ σε περίπτωση ανάγκης ο χειριστής πρέπει να αντιδράσει σε δευτερόλεπτα [13]. Πολλά μέτρα ασφαλείας που εφαρμόζονται αυτονόητα στα συστήματα πληροφορικής, είναι δύσκολο ή ακόμα αδύνατο να εφαρμοστούν σε επιχειρησιακά μηχανήματα χωρίς να τεθεί σε κίνδυνο η λειτουργική τους συνέχεια.

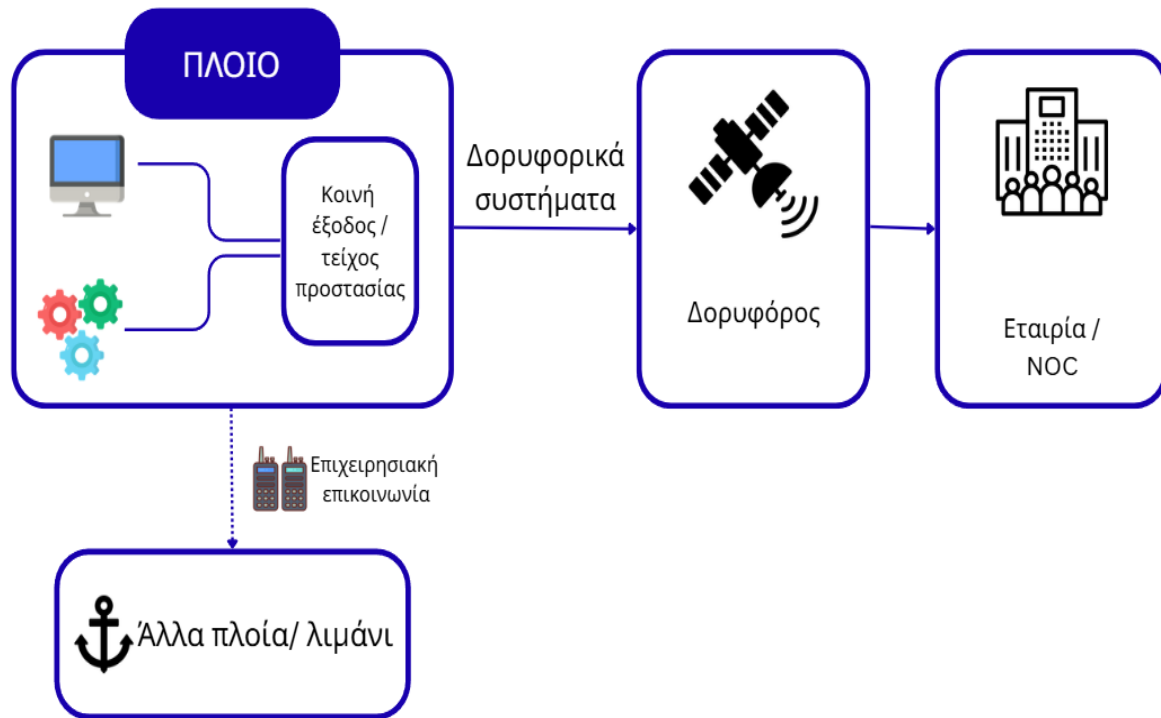
Η σύνδεση των υπολογιστών με τα μηχανικά συστήματα του πλοίου, εμφανίζει σοβαρά προβλήματα στην ασφάλεια. Βασική αιτία είναι η χρήση τεχνολογιών παλιάς γενιάς από αυτά τα συστήματα, που επιφέρει σημαντικές δυσκολίες στη θωράκιση τους [14]. Παράδειγμα αποτελεί η χρήση του πρωτοκόλλου CAN-BUS στα μηχανολογικά συστήματα του πλοίου. Το συγκεκριμένο σχεδιάστηκε χωρίς προδιαγραφές κρυπτογράφησης ή αυθεντικοποίησης. Έτσι, κάθε συσκευή που συνδέεται μαζί του, έχει τη δυνατότητα να διαβάσει τα μηνύματα του καθώς και να στείλει ψευδή δεδομένα [8]. Παράλληλα, το γεγονός ότι πλέον συνδέονται οι υπολογιστές με τις μηχανές φέρνει νέους κινδύνους. Τα συστήματα που είχαν σχεδιαστεί για να λειτουργούν απομονωμένα, πλέον συνδέονται στο διαδίκτυο για τυχόν ενημερώσεις και άλλες εργασίες. Η πρακτική αυτή φέρνει στο στόχαστρο τις συσκευές αυτές μετατρέποντας τις σε πιθανά σημείο εισόδου για κακόβουλες επιθέσεις [14].

2.2.3 Δίκτυα και συνδεσιμότητα

Για την κατανόηση των τεχνικών προκλήσεων, είναι απαραίτητο να εξεταστεί και το περιβάλλον επικοινωνίας των πλοίων. Σε αντίθεση με τις χερσαίες εγκαταστάσεις που η συνδεσιμότητα θεωρείται δεδομένη, ένα πλοίο αποτελεί μια απομονωμένη οντότητα που πρέπει να διατηρεί τη σύνδεση της κάτω από δύσκολες συνθήκες. Τα ναυτιλιακά δίκτυα απαιτούν ξεχωριστή μελέτη και αντιμετώπιση, διότι η διαθεσιμότητα δεν εξαρτάται μόνο από τις τεχνολογίες που χρησιμοποιούνται [15].

Στις περιπτώσεις που το πλοίο βρίσκεται εν πλω, η επικοινωνία του στηρίζεται κατά κύριο λόγο σε δύο τεχνολογίες. Η πρώτη αφορά τη δορυφορική επικοινωνία, η οποία αποτελεί τη βασική επιλογή για τη σύνδεση του πλοίου με τη στεριά. Επιτρέπεται η πρόσβαση στο διαδίκτυο σε σχεδόν οποιοδήποτε σημείο του κόσμου μέσω δορυφόρων γεωστατικής τροχιάς. Επίσης, οι ναυτιλιακές εταιρίες έχουν τη δυνατότητα να παρακολουθούν τον στόλο τους σε πραγματικό χρόνο παρέχοντας ταυτόχρονα απομακρυσμένη υποστήριξη για την ασφαλή πλοήγηση [16]. Η δεύτερη τεχνολογία είναι η ασύρματη επικοινωνία μέσω συχνοτήτων, όπως VHF για πολύ υψηλές συχφνότητες και UHF για υπέρ υψηλές συχνότητες. Χρησιμοποιείται για άμεση επαφή μεταξύ πλοίου με πλοίο ή και πλοίου με ξηρά. Λειτουργεί μόνο σε μικρές αποστάσεις και με χαμηλές ταχύτητες, οι οποίες δεν είναι αρκετές για να καλύψουν τις ανάγκες των σύγχρονων ψηφιακών εφαρμογών [15]. Η ενδεικτική αρχιτεκτονική επικοινωνίας πλοίου με την ξηρά αποτυπώνεται στο Σχήμα 2.5.

Η δικτυακή συνδεσιμότητα ενός πλοίου έχει δύο βασικές ιδιαιτερότητες σε σύγκριση με δίκτυα στη στεριά. Από τη μία πλευρά, παρατηρείται συχνή ασταθής σύνδεση, με χαμηλές ταχύτητες και περιορισμένο εύρος ζώνης. Από την άλλη, χαρακτηρίζονται από δυναμική τοπολογία η οποία εξαρτάται από τις συνθήκες του θαλάσσιου περιβάλλοντος. Αυτό σημαίνει ότι το δίκτυο δεν είναι σταθερό, καθώς το πλοίο αλλάζει θέση συνεχώς και η επικοινωνία από και προς αυτό εξαρτάται άμεσα από τον καιρό και την κίνηση της θάλασσας. Η δορυφορική σύνδεση παρουσιάζει μεγάλες καθυστερήσεις επειδή οι γεωστατικοί δορυφόροι βρίσκονται σε μακρινές αποστάσεις, ενώ το κόστος της παραμένει πολύ υψηλό. Επιπλέον, η σύνδεση δεν είναι πάντα σταθερή, καθώς τα έντονα κύματα κρύβουν την οπτική επαφή ανάμεσα στις κεραίες, προκαλώντας συχνές διακοπές. Σημαντικό είναι να αναφερθεί ότι υπάρχουν περιοχές χωρίς καθόλου κάλυψη όπως τα φιόρδ και πολικές περιοχές υψηλού γεωγραφικού πλάτους. Αυτοί οι περιορισμοί σημαίνει ότι η δορυφορική σύνδεση χρησιμοποιείται επιλεκτικά και συχνά μόνο για μεγάλα συμπιεσμένα αρχεία [15].



Σχήμα 2.5: Ενδεικτική αρχιτεκτονική επικοινωνίας πλοίου με ξηρά

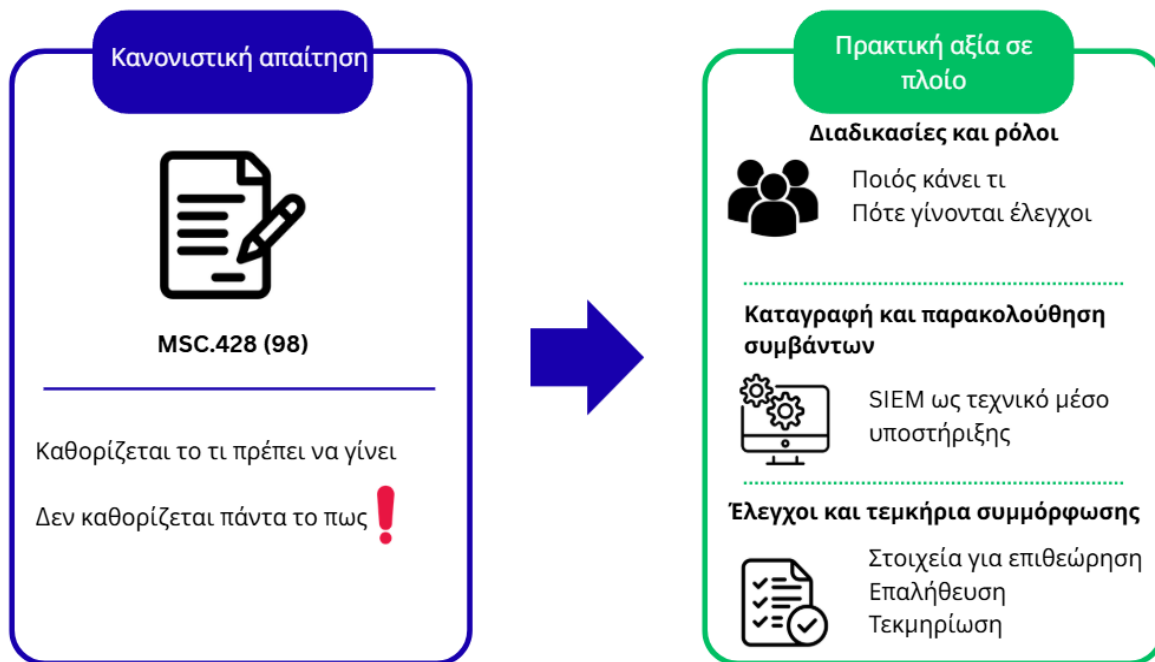
Ο μεγάλος αυτός όγκος δεδομένων που διακινούνται, καθιστά το θέμα της ασφάλειας πληροφοριών κρίσιμο ζήτημα. Η δορυφορική σύνδεση δεν χρησιμοποιείται μόνο για γενική χρήση, αλλά υποστηρίζει και επιχειρησιακές λειτουργίες. Η ύπαρξη διαφορετικών ειδών δεδομένων στο ίδιο δίκτυο, δυσκολεύει την εφαρμογή των κλασικών μεθόδων ασφαλείας. Ερευνητική ανάλυση που πραγματοποιήθηκε από δορυφορικές εκπομπές ναυτιλιακών δικτύων, έδειξε ότι ευαίσθητα δεδομένα μεταδίδονται χωρίς κρυπτογράφηση. Για παράδειγμα ενημερώσεις ναυτιλιακών χαρτών, εμπορικά δρομολόγια, ηλεκτρονικές συνομιλίες και πληροφορίες του πληρώματος βρίσκονται εκτεθειμένες σε κινδύνους υποκλοπής ή ακόμα και αλλοίωσης δεδομένων από κακόβουλους χρήστες [16]. Τα ζητήματα αυτά αναδεικνύουν τις ιδιαίτερες δυσκολίες που υπάρχουν κατά τον σχεδιασμό πιθανών λύσεων για την ψηφιακή ασφάλεια στο περιβάλλον της ναυτιλίας.

2.2.4 Κανονιστικό πλαίσιο ασφάλειας στη ναυτιλία

Η ναυτιλία ακολουθεί ένα διεθνές πλαίσιο για την ασφάλεια, το οποίο διαμορφώθηκε σταδιακά μέσα στα χρόνια. Η εμφάνιση νέων κινδύνων ανάγκασε τον κλάδο να εφαρμόσει υποχρεωτικούς κανόνες και απαιτήσεις. Πριν το έτος 1914, αναφέρεται ότι δεν υπήρχε κάποια παγκόσμια συνθήκη που να θεσπίζει κανόνες για την ασφάλεια στη θάλασσα. Η υιοθέτηση της διεθνούς σύμβασης για την ασφάλεια της ανθρώπινης ζωής στη θάλασσα (Safety Of Life At Sea - SOLAS), αποτέλεσε θεμέλιο της ενίσχυσης άμυνας των θαλάσσιων απειλών. Σε κοινή λογική εντάχθηκαν και μεταγενέστερες ρυθμίσεις για την προστασία από σκόπιμες απειλές, όπως ο διεθνής κώδικας για την ασφάλεια των πλοίων και των λιμενικών εγκαταστάσεων (ISPS), του Διεθνούς Ναυτιλιακού Οργανισμού IMO. Στην ουσία λειτουργεί ως μέτρο ενίσχυσης της θαλάσσιας ασφάλειας έναντι σημαντικών κινδύνων. Επίσης, επιβάλλει ένα αυστηρό πλαίσιο λειτουργίας, καθορίζοντας ξεκάθαρα τα καθήκοντα του προσωπικού και δηλώνοντας συγκεκριμένα βήματα που πρέπει να ακολουθούνται για την προστασία των υποδομών [17].

Όσον αφορά την καθημερινή λειτουργία, βασικός πυλώνας είναι ο διεθνής κώδικας ασφαλούς διαχείρισης (ISM), ο οποίος υποχρεώνει κάθε εταιρία να εφαρμόζει και να συμμορφώνεται με ένα συγκεκριμένο σύστημα ασφαλούς διαχείρισης (SMS). Στην πράξη, πρόκειται για ένα γραπτό πλαίσιο πολιτικών και διαδικασιών που δείχνει πως ένας οργανισμός εντοπίζει τους κινδύνους, τι μέτρα λαμβάνει και πως ελέγχει την αποτελεσματικότητά τους. Έτσι, η προστασία του πλοίου σταμάτησε να βασίζεται σε εμπειρικές και άτυπες πρακτικές, δημιουργώντας μία δομημένη διαδικασία με στόχο τον έλεγχο, την επιθεώρηση και τη συνεχόμενη αξιολόγηση [17].

Η ενσωμάτωση της κυβερνοασφάλειας στη ναυτιλία εντάχθηκε επίσημα σε αυτό το υποχρεωτικό πλαίσιο μέσω της απόφασης MSC.428 (98) του IMO. Εφαρμόστηκε την 1^η Ιανουαρίου το 2021. Η απόφαση αυτή ορίζει ότι η αντιμετώπιση των απειλών ασφάλειας πληροφοριών αποτελεί μέρος του συστήματος ασφαλούς διαχείρισης του πλοίου [17]. Πλέον η ψηφιακή ασφάλεια δεν θεωρείται ένα προαιρετικό τεχνικό ζήτημα, αλλά κύριο κομμάτι της καθημερινής λειτουργίας. Το συγκεκριμένο πλαίσιο δίνει τον στόχο και θέτει την υποχρέωση για την ενσωμάτωση τεχνικών ασφάλειας, αλλά δεν παρέχει κάποιο έτοιμο και αναλυτικό πρότυπο με τεχνικά μέτρα. Σημαντικό είναι να αναφερθεί ότι εάν μία εταιρία δεν διαχειρίζεται σωστά αυτούς τους κινδύνους, ρισκάρει να χάσει το πιστοποιητικό συμμόρφωσης της (Document of Compliance - DoC) [18].



Σχήμα 2.6: Πρακτική αξία MSC.428 (98) σε πλοίο [17]

Για την εφαρμογή αυτής της νομικής υποχρέωσης στην πράξη, μπορούν να χρησιμοποιηθούν διεθνή πρότυπα που προαναφέρθηκαν και καθορίζουν τα συγκεκριμένα τεχνικά και οργανωτικά μέτρα. Το ISO/IEC 27001 είναι πιο στοχευμένο στην ασφάλεια των συστημάτων πληροφορικής, ενώ το ISO/IEC 62443 εξειδικεύεται στα λειτουργικά και τα βιομηχανικά συστήματα του πλοίου. Παράλληλα, προτείνεται η χρήση του πλαισίου Nist, που αναπτύχθηκε από το εθνικό ινστιτούτο προτύπων και τεχνολογίας των ΗΠΑ. Το πλαίσιο αυτό οργανώνει τη διαχείριση του ψηφιακού κινδύνου σε πέντε διαδοχικά στάδια με τον εντοπισμό των απειλών, την προστασία των συστημάτων, την ανίχνευση τυχόν επιθέσεων, την άμεση απόκριση και τέλος την αποκατάσταση. Έτσι, προσφέρεται ένα ολοκληρωμένο μοντέλο θωράκισης που προσαρμόζεται εύκολα στις ανάγκες του ναυτιλιακού περιβάλλοντος [18].

2.3 Βιβλιογραφική επισκόπηση και συναφείς προσεγγίσεις

Η ενότητα αυτή παρουσιάζει συνοπτικά τη βιβλιογραφία και τις βασικές κατηγορίες λύσεων SIEM που σχετίζονται με το αντικείμενο της εργασίας. Αρχικά, αναφέρονται οι ερευνητικές προσεγγίσεις ως προς την παρακολούθηση και την ανίχνευση συμβάντων, με έμφαση στις ιδιαιτερότητες που παρουσιάζει η ναυτιλία. Στη συνέχεια, πραγματοποιείται συγκριτική ανάλυση των πλατφορμών διαχείρισης πληροφοριών και συμβάντων ασφαλείας, βάσει συνολικών χαρακτηριστικών. Τέλος, προσδιορίζεται το βασικό κενό το οποίο καλύπτει η παρούσα υλοποίηση και η τεκμηρίωση επιλογής της προσέγγισης που ακολουθεί.

2.3.1 Ερευνητικές προσεγγίσεις

Ο σύγχρονος ναυτιλιακός τομέας σε παγκόσμιο επίπεδο βασίζεται ολοένα και περισσότερο στον ψηφιακό μετασχηματισμό και τον αυτοματισμό μεγάλου μέρους των επιχειρησιακών διαδικασιών του. Στο πλαίσιο αυτό, το πεδίο της κυβερνοασφάλειας προσελκύει όλο και μεγαλύτερο ερευνητικό ενδιαφέρον [19]. Πιο συγκεκριμένα, αντλώντας στοιχεία από συγκεκριμένες και εξειδικευμένες βάσεις δεδομένων, παρατηρήθηκε ότι ο αριθμός των επίσημα καταγεγραμμένων περιστατικών αυξήθηκε από έξι επιθέσεις το έτος 2014 σε εκατό σαράντα πέντε το έτος 2023 [19]. Οι τιμές αυτές προέκυψαν από τη σύγκριση δύο πηγών, με την επιλογή της μέγιστης τιμής για κάθε έτος. Παρά την άνοδο αυτή, η συστηματική παρακολούθηση της ασφάλειας στον κυβερνοχώρο παραμένει σχετικά πρόσφατο αντικείμενο μελέτης, με ποσοστό 94% των ακαδημαϊκών εργασιών να έχει δημοσιευθεί μετά το έτος 2017 [20].

Σημαντικό ρόλο για τη διαμόρφωση του ερευνητικού τοπίου διαδραμάτισαν οι κατευθυντήριες γραμμές των διεθνών οργανισμών, οι οποίες όμως παρουσιάζουν σημαντικές ελλείψεις. Ο Διεθνής Ναυτιλιακός οργανισμός (International Maritime Organization - IMO), ενσωμάτωσε την ασφάλεια πληροφοριών στα συστήματα διαχείρισης ασφάλειας, ωστόσο οι οδηγίες του δεν καλύπτουν το ζήτημα παρακολούθησης των κυβερνοεπιθέσεων. Αντίστοιχα, το Βαλτικό και διεθνές ναυτιλιακό συμβούλιο (BIMCO) αναφέρεται μόνο επιφανειακά στη χρήση των συστημάτων ανίχνευσης εισβολών (Intrusion detection system - IDS), χωρίς να αναφέρονται πρακτικές οδηγίες για την υλοποίηση και την ανάπτυξη ολοκληρωμένων αρχιτεκτονικών παρακολούθησης [20].

Σύμφωνα με τη βιβλιογραφική επισκόπηση του Vaarandi [20], η έρευνα πάνω στον τομέα της παρακολούθησης περιστατικών ασφαλείας στη ναυτιλία έχει ακολουθήσει τέσσερις κύριες κατευθύνσεις:

- Την παρακολούθηση των συστημάτων πλοήγησης, με έμφαση στην ανίχνευση επιθέσεων απομίμησης του σήματος μέσω της ανάλυσης δεδομένων από εξειδικευμένα πρωτόκολλα επικοινωνίας πλοίων,
- Την παρακολούθηση των δικτύων και των πληροφοριακών συστημάτων, με έμφαση στις συσκευές του Διαδικτύου των Πραγμάτων (Internet Of Things - IoT) ενός πλοίου,
- Την εξέταση των αρχιτεκτονικών παρακολούθησης και του κέντρου επιχειρήσεων ασφαλείας (Security Operations Center - SOC), οι οποίες αντιμετωπίζουν τις ιδιαιτερότητες του τομέα της ναυτιλίας και
- Τη δημιουργία περιβαλλόντων δοκιμής της κυβερνοασφάλειας, σε συνθήκες που προσομοιώνουν πραγματικά πλοία.

Παρά τη σημαντική συμβολή των παραπάνω κατευθύνσεων οι οποίες έχουν αποφέρει σημαντικά αποτελέσματα, εμφανίζονται συγκεκριμένα ερευνητικά κενά που πρέπει να αναφερθούν. Αρχικά, η πλειονότητα των βιβλιογραφιών εστιάζει σε εξειδικευμένα δίκτυα, παραβλέποντας έτσι την ολοκληρωμένη εποπτεία των ευρύτερων ναυτιλιακών υποδομών και υποσυστημάτων [20]. Επιπλέον, αρκετές από τις λύσεις που παρουσιάζονται αντιμετωπίζουν το πλοίο ως ένα ενιαίο σύστημα, αντί να εστιάζουν σε μεμονωμένα εξαρτήματα [21]. Τέλος, η αξιοποίηση πραγματικών δεδομένων καταγραφής από επιχειρησιακά συστήματα πλοίων έχει λάβει ελάχιστη προσοχή, παρά το γεγονός ότι τα δεδομένα αυτά αποτελούν τη βασική πηγή πληροφοριών για τον εντοπισμό ανωμαλιών [20]. Συμπερασματικά, η υπάρχουσα έρευνα επιβεβαιώνει ότι ο σχεδιασμός λειτουργικών συστημάτων παρακολούθησης, τα οποία είναι ειδικά σχεδιασμένα και ικανά για επεξεργασία ετερογενή δεδομένων από αληθινά πλοία, αποτελεί ένα πεδίο που δεν έχει μελετηθεί επαρκώς [21].

2.3.2 Συγκριτική επισκόπηση λύσεων SIEM

2.3.2.1 IBM QRadar

Η πλατφόρμα IBM QRadar, αποτελεί μία εμπορική λύση η οποία χρησιμοποιείται για τη συλλογή, τη συσχέτιση και την ανάλυση συμβάντων ασφαλείας από διαφορετικές πηγές σε ένα πληροφοριακό περιβάλλον. Απαρτίζεται από αρχιτεκτονική βασισμένη σε αυτόνομα υποσυστήματα όπως [22]:

- Συλλέκτες και επεξεργαστές συμβάντων και ροών,
- Κόμβοι δεδομένων,
- Κεντρική διεπαφή,
- Εργαλεία αξιολόγησης κινδύνων και ευπαθειών και
- Πλαίσιο εφαρμογών για επέκταση.

Αποτελεί μια ισχυρή λύση για περιβάλλοντα στα οποία απαιτείται επεξεργασία μεγάλου όγκου δεδομένων, καθώς προσφέρει κεντρική διαχείριση, ορατότητα και ταχεία απόκριση σε απειλές. Σε πειραματικές αξιολογήσεις έναντι διαφορετικών ειδών επιθέσεων ασφαλείας, επέδειξε υψηλά επίπεδα αποτελεσματικότητας μέσω της παραγωγής αλυσιδωτών παραβιάσεων. Οι δυνατότητες αυτές, συσχετίζουν αυτόματα μεμονωμένα γεγονότα ως μία ενιαία επίθεση. Με τον τρόπο αυτό, ο αναλυτής δεν χρειάζεται να ψάχνει χειροκίνητα μεμονωμένα συμβάντα, γεγονός που του εξοικονομεί πολύτιμο χρόνο [22].

Παρά το γεγονός ότι συγκροτεί ισχυρή λύση, αποτελεί βασικό περιορισμό για εγκαταστάσεις με περιορισμένο οικονομικό προϋπολογισμό. Επίσης, ο πηγαίος κώδικας δεν είναι διαθέσιμος στους τελικούς χρήστες και η χρήση της πλατφόρμας προϋποθέτει την αγορά των κατάλληλων αδειών [22]. Το μοντέλο χρήσης βασίζεται σε συμβάντα ανά δευτερόλεπτο και ροές ανά λεπτό. Ως συμπέρασμα, ο σχεδιασμός της λύσης συνδέεται άμεσα με τον όγκο των αρχείων καταγραφής και των ροών του δικτύου που εισάγονται και οδηγεί σε μεγάλες απαιτήσεις αδειοδότησης και υποδομής [23]. Ένας βασικός περιορισμός αφορά τη μεγάλη πολυπλοκότητα της διεπαφής του, η οποία συνεπάγεται με απαίτηση εξειδικευμένου προσωπικού για την αποδοτική λειτουργία του [22]. Τέλος η ενσωμάτωση μη τυποποιημένων πηγών καταγραφών παρουσιάζει δυσκολίες. Η υποστήριξη τους δεν είναι αυτοματοποιημένη και απαιτείται προχωρημένη τεχνική γνώση για τη χειροκίνητη παραμετροποίηση και διόρθωση των δεδομένων μέσω ειδικών εργαλείων [23].

Dashboard Offenses Log Activity Network Activity Assets Reports						
Search... ▾ Quick Searches ▾ Add Filter Save Criteria Save Results Cancel False Positive Rules ▾ Actions ▾						
Update Details						
(Hide Charts)						
	Event Name	Log Source	Event Count	Time ▾	Low Level Category	Source IP
	Open_File	Spectrum_Demo	1	10 Jun 2019, 10:15:09	Successful File Mod...	172.16.1.3
	ChangeFile_Permis...	Spectrum_Demo	1	10 Jun 2019, 10:15:09	Failed File Modificat...	172.16.1.3
	Close_File	Spectrum_Demo	1	10 Jun 2019, 10:15:09	Successful File Mod...	172.16.1.3
	Modify_Attribute	Spectrum_Demo	1	10 Jun 2019, 10:15:09	Successful File Mod...	172.16.1.3
	Open_File	Spectrum_Demo	1	10 Jun 2019, 10:15:09	Successful File Mod...	172.16.1.3
	Modify_Attribute	Spectrum_Demo	1	10 Jun 2019, 10:15:08	Successful File Mod...	172.16.1.3
	Close_File	Spectrum_Demo	1	10 Jun 2019, 10:15:08	Successful File Mod...	172.16.1.3
	Move_File	Spectrum_Demo	1	10 Jun 2019, 10:15:08	Successful File Mod...	172.16.1.3
	Move_File	Spectrum_Demo	1	10 Jun 2019, 10:15:08	Successful File Mod...	172.16.1.3
	Rename_File	Spectrum_Demo	1	10 Jun 2019, 10:15:08	Successful File Mod...	172.16.1.3
	Modify_Attribute	Spectrum_Demo	1	10 Jun 2019, 10:15:08	Successful File Mod...	172.16.1.3
	Modify_Attribute	Spectrum_Demo	1	10 Jun 2019, 10:15:08	Successful File Mod...	172.16.1.3
	Close_File	Spectrum_Demo	1	10 Jun 2019, 10:15:08	Successful File Mod...	172.16.1.3
	Open_File	Spectrum_Demo	1	10 Jun 2019, 10:15:08	Successful File Mod...	172.16.1.3
	Open_File	Spectrum_Demo	1	10 Jun 2019, 10:15:08	Successful File Mod...	172.16.1.3
	Modify_Attribute	Spectrum_Demo	1	10 Jun 2019, 10:15:08	Successful File Mod...	172.16.1.3
	Close_File	Spectrum_Demo	1	10 Jun 2019, 10:15:08	Successful File Mod...	172.16.1.3
	Modify_Attribute	Spectrum_Demo	1	10 Jun 2019, 10:15:08	Successful File Mod...	172.16.1.3
	Create_File	Spectrum_Demo	1	10 Jun 2019, 10:15:08	File Created	172.16.1.3
	Remove_directory	Spectrum_Demo	1	10 Jun 2019, 10:15:08	Failed File Modificat...	172.16.1.3

Σχήμα 2.7: Ενδεικτική διεπαφή IBM QRadar Log Activity [22]

Για την παρούσα υλοποίηση, το QRadar κρίθηκε ακατάλληλο για την αυτόνομη εγκατάσταση επί του πλοίου, καθώς έχει σχεδιαστεί για μεγάλης κλίμακας υποδομές με υψηλούς προϋπολογισμούς. Τα πλοία έχουν αυστηρούς περιορισμούς σε εύρος ζώνης, υλικό και διαθέσιμο εξειδικευμένο προσωπικό. Έτσι, σε συνδυασμό με το μοντέλο αδειοδότησης, καθιστά την οικονομική και τεχνική πρόβλεψη δύσκολη λόγω του μεταβαλλόμενου όγκου δεδομένων καταγραφής. Συνεπώς, για τους σκοπούς της παρούσας εργασίας απαιτείται μια οικονομική, τοπική και ευέλικτη λύση, η οποία απορρίπτει το QRadar ως επιλογή με την αναφορά ότι είναι ένα απαιτητικό σύστημα αναφοράς [22] [23].

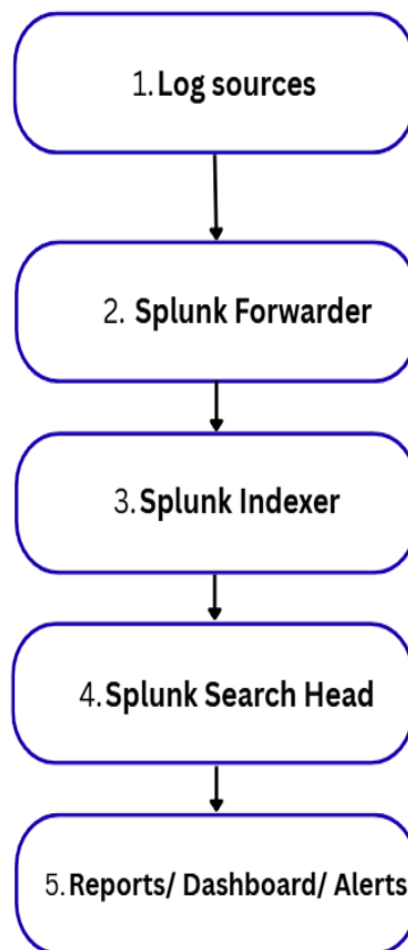
2.3.2.2 Splunk Enterprise Security

Το Splunk Enterprise Security αποτελεί μία επίσης εμπορική λύση Διαχείρισης πληροφοριών και συμβάντων ασφαλείας, η οποία προορίζεται για την ανίχνευση, τη διερεύνηση και την αντιμετώπιση απειλών ασφαλείας. Η λύση αυτή, ενσωματώνει διευρυμένες δυνατότητες για αυτοματοποίηση και ανάλυση συμπεριφοράς τοπικά, σε υπολογιστικό νέφος ή και σε υβριδικά περιβάλλοντα [24].

Η πλατφόρμα αυτή χρησιμοποιείται για την ενίσχυση της ορατότητας και την κεντρική διαχείριση των αρχείων καταγραφής, καθώς προσφέρει μια ενιαία κεντρική εικόνα εποπτείας στον αναλυτή. Η αρχιτεκτονική της λειτουργίας του συστήματος ακολουθεί ιεραρχική ροή επεξεργασίας. Οι προωθητές συλλέγουν δεδομένα από ετερογενείς πηγές, ο ευετηριαστής αναλαμβάνει την κατηγοριοποίηση και την αποθήκευση τους και η αναζήτηση εκτελεί την τελική ανάλυση. Η δομή αυτή επιτρέπει τη διαχείριση πληροφοριών από συστήματα και συσκευές δικτύου καταλήγοντας στην τελική παραγωγή των αναφορών ασφαλείας [25].

Η υιοθέτηση του Splunk Enterprise Security στο πλαίσιο της παρούσας εργασίας, παρά το τεχνικό βάθος του, προσκρούει σε σημαντικούς περιορισμούς όσο αφορά κυρίως το οικονομικό και το λειτουργικό σκέλος της υλοποίησης. Ως κλειστού κώδικα λογισμικό, η χρήση του προϋποθέτει την αγορά των κατάλληλων αδειών, με το κόστος να επηρεάζεται άμεσα και από τον όγκο δεδομένων ή τον φόρτο των αναζητήσεων. Η εμπορική του φύση δυσκολεύει αρκετά την προσαρμογή του σε ειδικές απαιτήσεις και το σύστημα κρίνεται ασύμβατο για μικρό οικονομικό πλαίσιο. Επίσης, εμφανίζει υψηλούς χρόνους εκτέλεσης, καθώς οι πολλές ενσωματωμένες λειτουργίες του το καθιστούν πιο βαρύ [26]. Τέλος, η χρήση του απαιτεί γνώσεις της αποκλειστικής γλώσσα SPL και σωστή οργάνωση όσον αφορά την αποθήκευση των δεδομένων [25].

Η χρήση του σε ένα περιβάλλον όπως αυτό της ναυτιλίας, προσφέρει σημαντική ορατότητα λόγω της συλλογής δεδομένων από διαφορετικές πηγές, όμως η εφαρμογή του περιορίζεται σε θέμα κόστους και λόγω της ανάγκης για εξειδικευμένη διαχείριση. Συμπληρωματικά η σύνθετη αρχιτεκτονική του απαιτεί μεγάλους υπολογιστικούς πόρους που συχνά σπανίζουν πάνω σε ένα πλοίο [25]. Αν και μπορεί να χρησιμοποιηθεί ως λύση σε υπολογιστικό νέφος ή υβριδικά, η δορυφορική σύνδεση που υπάρχει σε ένα πλοίο περιορίζεται λόγω των απαιτήσεων που ζητάει σε εύρος ζώνης και της πιθανής αστάθειας ή περιορισμένης σύνδεσης με το δίκτυο. Επομένως, το Splunk Enterprise Security δεν απορρίπτεται λόγω έλλειψης δυνατοτήτων, αλλά επειδή οι δυνατότητες του συνοδεύονται από αυξημένο κόστος, μεγάλη πολυπλοκότητα, αυξημένες ανάγκες για υποδομή και ανάγκες για εξειδικευμένη γνώση.

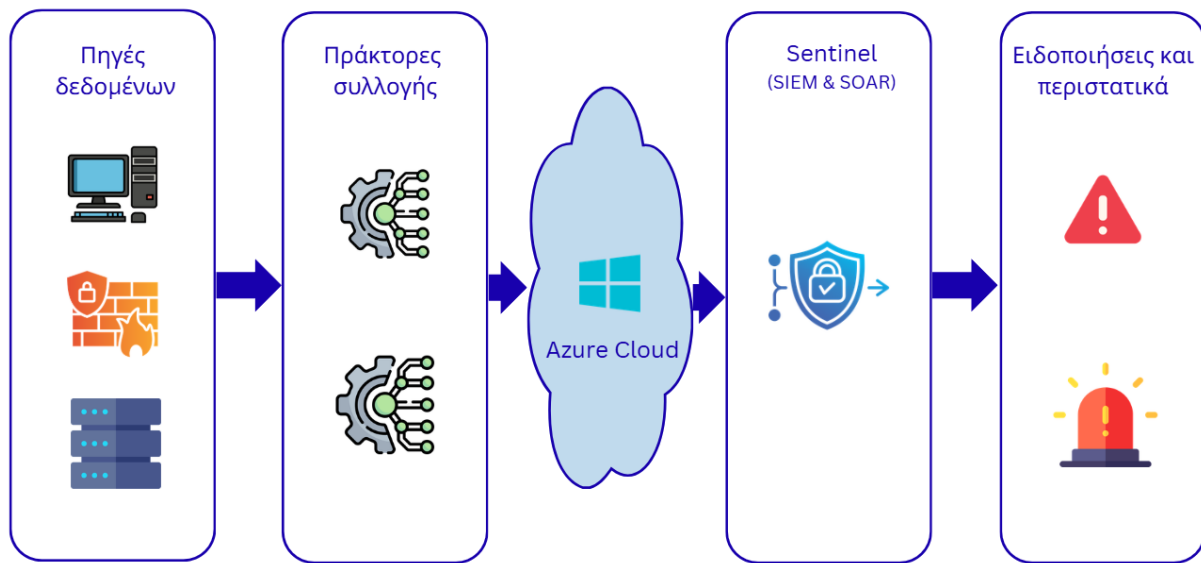


Σχήμα 2.8: Αρχιτεκτονική συλλογής και ανάλυσης στο Splunk SIEM [24]

2.3.2.3 Microsoft Sentinel

Το Microsoft Sentinel είναι μία εμπορική λύση SIEM, που ενσωματώνει ταυτόχρονα και δυνατότητες ορχήστρωσης, αυτοματοποίησης και απόκρισης ασφαλείας (Security Orchestration, Automation, and Response - SOAR). Αναπτύχθηκε από την εταιρία Microsoft και είναι σχεδιασμένη σαν υπηρεσία στο υπολογιστικό νέφος. Αξιοποιεί καινοτόμες τεχνολογίες όπως η τεχνητή νοημοσύνη και η μηχανική μάθηση με στόχο τον εντοπισμό, τη διερεύνηση και την αντιμετώπιση απειλών [27].

Η δομή του συστήματος στηρίζεται στο περιβάλλον της Microsoft Azure και χρησιμοποιεί έναν συγκεντρωτικό χώρο (Log Analytics Workspace), ως κεντρική βάση δεδομένων [27]. Για την αναζήτηση, την ανάλυση και τη διερεύνηση των δεδομένων χρησιμοποιείται η γλώσσα Kusto Query Language (KQL), προσφέροντας ισχυρές δυνατότητες στην ανίχνευση και τη διαχείριση μεγάλου όγκου δεδομένων [28].



Σχήμα 2.9: Αρχιτεκτονική συλλογής και επεξεργασίας δεδομένων στο Microsoft Sentinel [27]

Ένα αρκετά σημαντικό πλεονέκτημα της πλατφόρμας είναι η άμεση ενσωμάτωση της με άλλες υπηρεσίες της Microsoft, όπως για παράδειγμα το σύστημα ασφαλείας Microsoft Defender και η υπηρεσία νέφους Azure Active Directory. Επιπλέον, υπάρχει το μοντέλο χρέωσης βάσει του όγκου δεδομένων, το οποίο προσφέρει ευελιξία στη διαχείριση του κόστους [27].

Ωστόσο, η πλατφόρμα παρουσιάζει περιορισμούς σε περιβάλλοντα στα οποία απαιτείται τοπική αυτονομία και περιορισμένη εξάρτηση από τις εξωτερικές υποδομές. Παρά το γεγονός ότι το Microsoft Sentinel μπορεί να συνδεθεί με συστήματα άλλων εταιριών ή με διαφορετικές πλατφόρμες υπολογιστικού νέφους, η πλήρης λειτουργία του εξαρτάται από την πλατφόρμα του Azure και τη συνεχή αποστολή δεδομένων στον κεντρικό χώρο αποθήκευσης [27] [28]. Επίσης, η χρήση της γλώσσας KQL απαιτεί εξειδικευμένη εκπαίδευση και η δημιουργία προσαρμοσμένων κανόνων ανίχνευσης υψηλό επίπεδο σε τεχνικές γνώσεις [28].

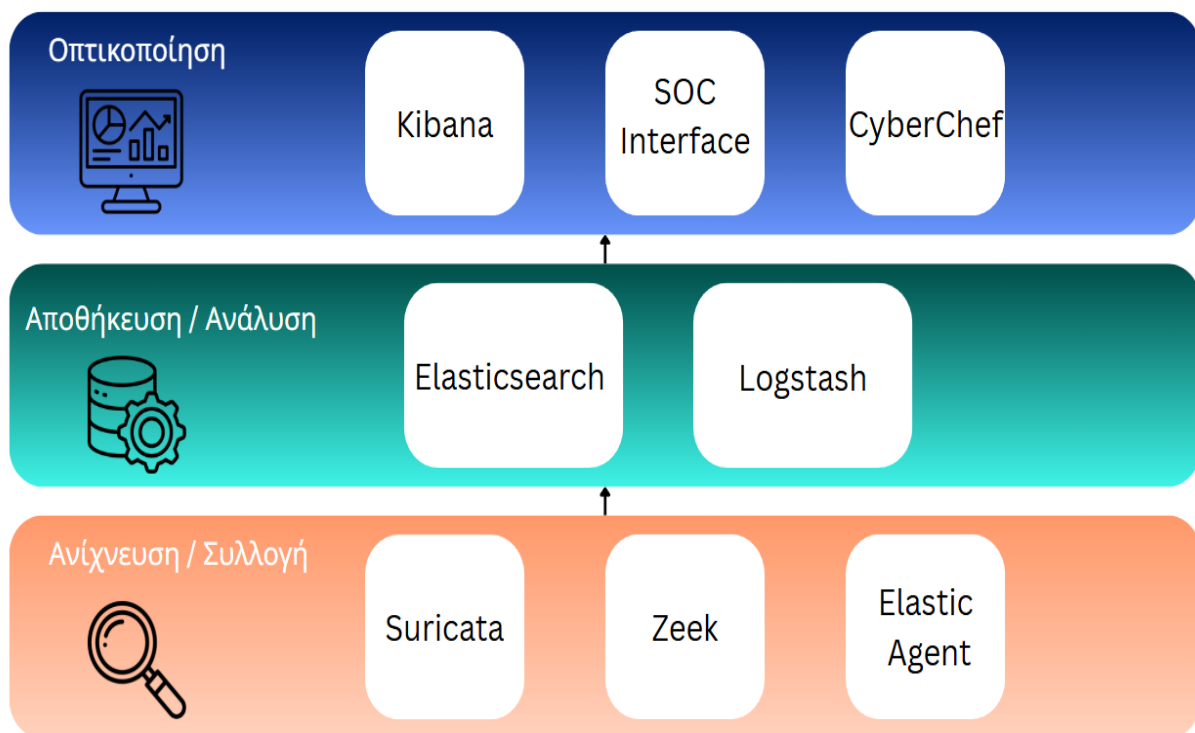
Στην παρούσα υλοποίηση το Microsoft Sentinel κρίθηκε λιγότερο κατάλληλο λόγω της αρχιτεκτονικής του, που στηρίζεται σε υπολογιστικό νέφος. Η συλλογή, η αποθήκευση και η ανάλυση των δεδομένων προϋποθέτει σταθερή και αξιόπιστη συνδεσιμότητα, καθώς αποστέλλονται στον κεντρικό συγκεντρωτικό χώρο του Azure [28]. Οι συνθήκες που υπάρχουν σε ένα πλοίο εν πλω μπορεί να επιφέρουν περιορισμένη, διακοπτόμενη αλλά και υψηλού κόστους σύνδεση, μέσω των δορυφορικών συστημάτων του. Συνοψίζοντας, η πλατφόρμα δεν απορρίπτεται λόγω περιορισμένων δυνατοτήτων. Η

αρχιτεκτονική της δεν εξυπηρετεί πλήρως στην ανάγκη που υπάρχει για τοπική και αυτόνομη λειτουργία, στο εξεταζόμενο περιβάλλον της ναυτιλίας.

2.3.2.4 Security Onion

Σε αντίθεση με τις εμπορικές λύσεις που αναφέρθηκαν προηγουμένως, το Security Onion αποτελεί πλατφόρμα ανοιχτού κώδικα, βασισμένη στο λειτουργικό σύστημα Linux. Έχει σχεδιαστεί με στόχο την παρακολούθηση ασφάλειας του δικτύου, τον εντοπισμό απειλών, την ανάλυση συμβάντων και τη διαχείριση των αρχείων καταγραφής. Παράλληλα, ενσωματώνει μία σειρά από εξειδικευμένα εργαλεία ασφαλείας, όπως τα Suricata, Zeek, Elasticsearch, Logstash, Kibana και Elastic Agent, παρέχοντας έτσι ένα ενιαίο περιβάλλον για την ανίχνευση εισβολών και την κεντρική εποπτεία της ασφάλειας [29]

Η αρχιτεκτονική της πλατφόρμας παρέχει τη δυνατότητα να διαφοροποιηθεί αναλόγως το μέγεθος και τις απαιτήσεις της εγκατάστασης. Συγκεκριμένα, σε μικρότερα περιβάλλοντα η υλοποίηση μπορεί να αναπτυχθεί σε ένα ενιαίο σύστημα, ενώ σε μεγαλύτερες εγκαταστάσεις μπορεί να αναπτυχθεί καταναμημένα με κόμβο διαχείρισης, κόμβους αισθητήρων και κόμβους αναζήτησης [29]. Η πλατφόρμα εστιάζει κυρίως στην ανάλυση της δικτυακής κίνησης με στόχο την ανίχνευση εισβολών και την παραγωγή μεταδεδομένων, με τη χρήση εργαλείων όπως το Suricata και το Zeek [30].



Σχήμα 2.10: Επίπεδα και βασικά εργαλεία του Security Onion [30]

Ένα από τα βασικά πλεονεκτήματα της πλατφόρμας είναι η δωρεάν διάθεσή της ως ανοιχτού κώδικα. Επιπλέον, σημαντική είναι και η ενσωμάτωση των εργαλείων ανίχνευσης και ανάλυσης σε μία ενιαία εγκατάσταση [29]. Η ανίχνευση ύποπτης δραστηριότητας σε πραγματικό χρόνο είναι πολύ χρήσιμη και το Security Onion το επιτυγχάνει με την εστίαση του στην παρακολούθηση κίνησης του δικτύου. Επιπλέον θετική είναι η ύπαρξη ενεργής κοινότητας και η συνεχής ενημέρωση της πλατφόρμας. Τέλος αξίζει να σημειωθεί, η δυνατότητα να αξιοποιεί εργαλεία ανίχνευσης όπως Suricata, Zeek και Elastic Agent ενισχύουν την πρακτική του αξία.

Ωστόσο, υπάρχουν σημαντικοί περιορισμοί που αξίζει να αναφερθούν. Αρχικά η πλήρης αξιοποίηση των δυνατοτήτων του μπορεί να δημιουργήσει αυξημένες απαιτήσεις υλικού σε ισχύ, μνήμη και αποθηκευτικό χώρο. Επιπλέον, ο κόμβος διαχείρισης έχει αυξημένους χρόνους εκκίνησης σε σχέση με τους κόμβους αναζήτησης. Έτσι, επηρεάζεται αρνητικά η ανάκαμψη του μετά από τυχόν βλάβες [29].

Για την παρούσα υλοποίηση το Security opinion κρίθηκε λιγότερο κατάλληλο. Παρά τις υψηλές του δυνατότητες, εστιάζει κυρίως στην ανάλυση δικτυακής κίνησης, ενώ η παρούσα υλοποίηση έχει ως στόχο την εισαγωγή καταγραφών από ετερογενείς πηγές. Επιπλέον, η κατανεμημένη ανάπτυξη, απαιτεί σημαντικές υποδομές υλικού οι οποίες δεν είναι εφικτές πάντα σε ένα περιβάλλον ενός πλοίου.

2.3.2.5 Elastic Security

Το Elastic Security είναι μία λύση SIEM ανοιχτού κώδικα. Συνδυάζει δυνατότητες για αναζήτηση, αποθήκευση και τελική οπτικοποίηση των δεδομένων που αφορούν την ψηφιακή ασφάλεια, σε ένα ενιαίο περιβάλλον παρακολούθησης. Ο σχεδιασμός του αποτελούσε εξ αρχής μία ολοκληρωμένη πλατφόρμα που καλύπτει ανίχνευση απειλών και ανάλυση συμπεριφοράς. Η βασική του έκδοση διατίθεται δωρεάν, ενώ κάποιες βασικές λειτουργίες απαιτούν εμπορική συνδρομή [31].

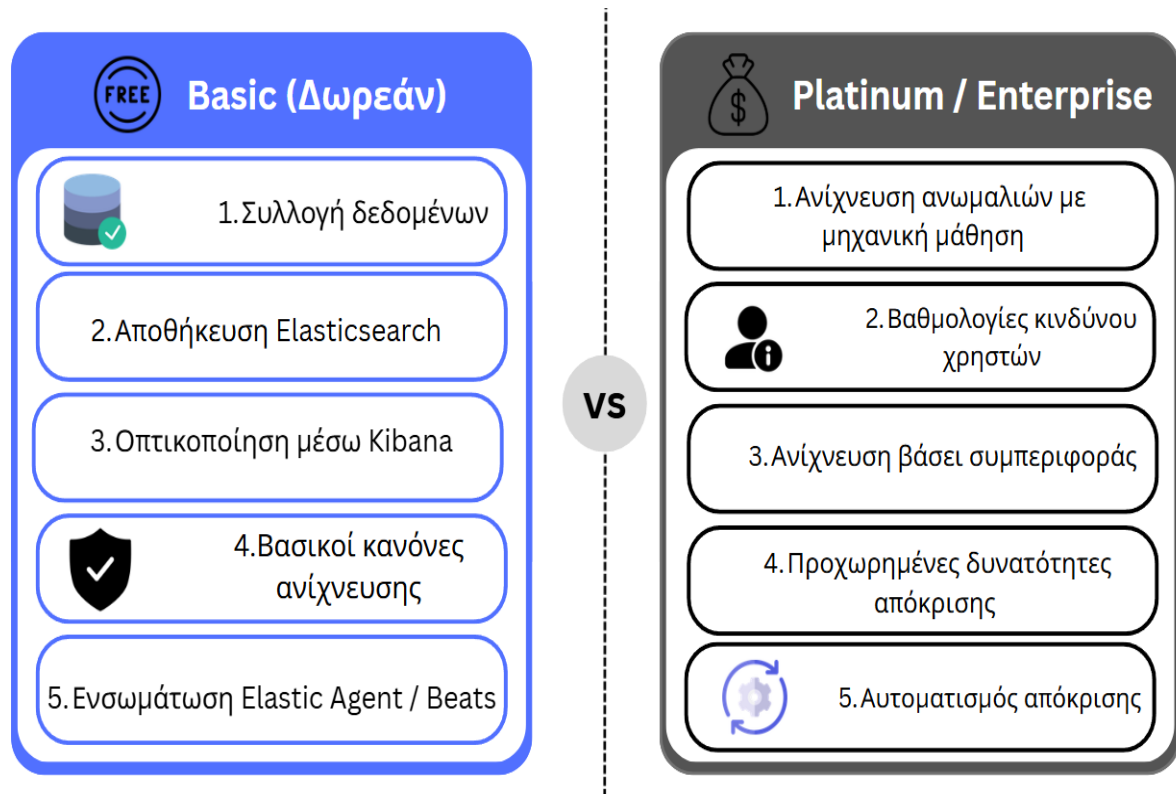
Με βάση την επίσημη ιστοσελίδα, η αρχιτεκτονική του συστήματος βασίζεται στη στοίβα ELK που οργανώνεται σε τρία επίπεδα [32]:

- Το επίπεδο αποθήκευσης και ανάλυσης. Χρησιμοποιείται το εργαλείο Elasticsearch που λειτουργεί ως βάση δεδομένων που αποθηκεύει μεγάλο όγκο πληροφοριών και επιτρέπει την αναζήτηση μέσα σε αυτό,
- Το επίπεδο συλλογής. Σε αυτό χρησιμοποιούνται ελαφριά προγράμματα σε συνδυασμό με το εργαλείο Logstash. Είναι το αρχικό στάδιο στο οποίο συλλέγονται δεδομένα από τις πηγές,
- Το επίπεδο οπτικοποίησης. Ο αναλυτής έχει πρόσβαση στο σύστημα μέσω του εργαλείου Kibana. Το περιβάλλον αυτό προσφέρει μία διεπαφή που μετατρέπει τα δεδομένα σε γραφήματα και πίνακες ελέγχου.

Ταυτόχρονα, ανάλογα με τις ανάγκες κάθε οργανισμού η συγκεκριμένη λύση παρέχει την ευελιξία εγκατάστασης είτε τοπικά ή σε περιβάλλον υπολογιστικού νέφους [32].

Στα πλεονεκτήματα του αναφέρονται η ισχυρή μηχανή αναζήτησης και ανάλυσης δεδομένων που έχει. Επίσης συγκαταλέγεται η ευελιξία στην παραμετροποίηση, που αφήνουν το χρήστη να διαμορφώσει το σύστημα στα μέτρα του και η ενσωμάτωση προκαθορισμένων κανόνων, που εντοπίζουν αυτόματα ένα μεγάλο εύρος γνωστών απειλών [31].

Παρά τα πλεονεκτήματα του, παρουσιάζει ορισμένους σημαντικούς περιορισμούς. Βασικό μειονέκτημα είναι το γεγονός ότι οι πιο προχωρημένες λειτουργίες του δεν διατίθενται δωρεάν. Συγκεκριμένες λειτουργίες όπως η ολοκληρωμένη διαχείριση περιστατικών ή η ανάλυση ύποπτων συμπεριφορών, απαιτούν την αγορά της εμπορικής συνδρομής. Αυτό το γεγονός αυξάνει αισθητά το συνολικό κόστος της υποδομής [31]. Επιπρόσθετα, για τη δημιουργία νέων κανόνων από τον αναλυτή, χρειάζονται εξειδικευμένες γνώσεις πάνω στη συγκεκριμένη γλώσσα ερωτημάτων που χρησιμοποιεί η πλατφόρμα [32].



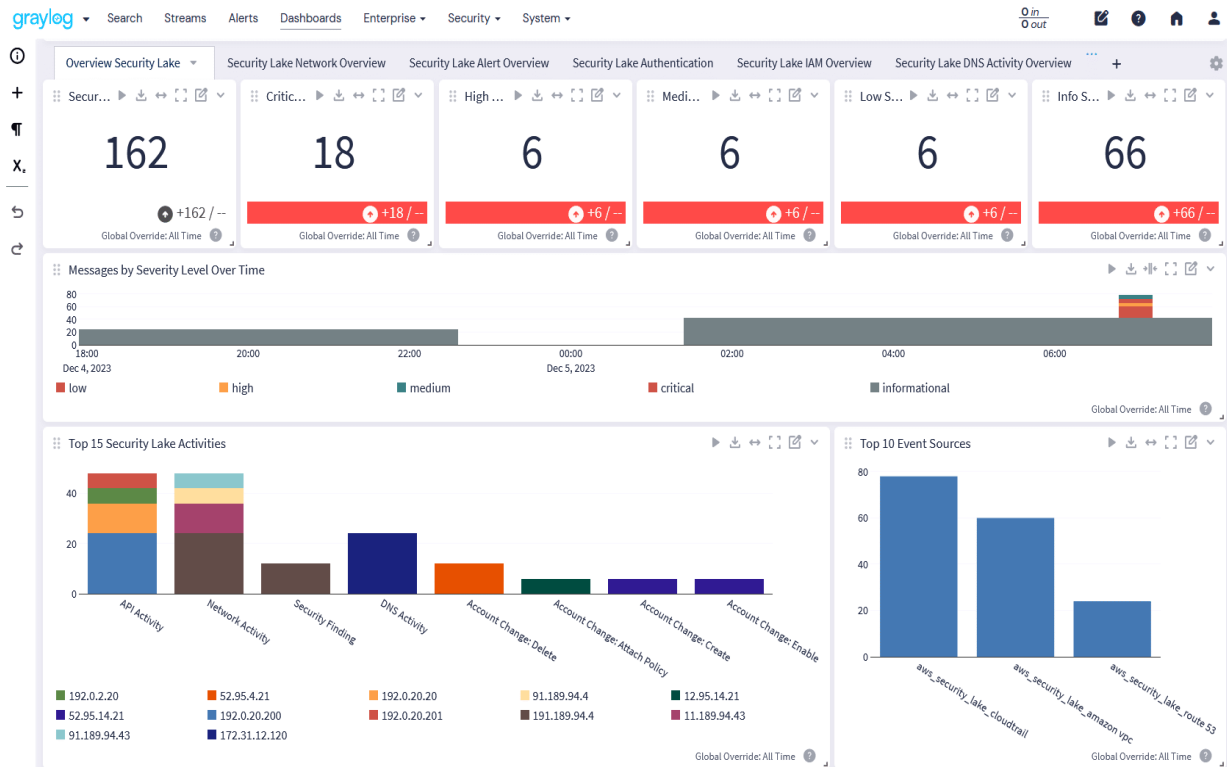
Σχήμα 2.11: Σύγκριση βασικών και εμπορικών λειτουργιών του Elastic Security

Λαμβάνοντας υπόψη τα παραπάνω και τις ανάγκες της παρούσας υλοποίησης στο προσαρμοσμένο περιβάλλον ναυτιλίας, το Elastic Security κρίθηκε λιγότερο κατάλληλη επιλογή. Αρχικά ο λόγος ήταν καθαρά πρακτικός, καθώς οι ειδικές λειτουργίες που απαιτούνται για μία ολοκληρωμένη προστασία σε ένα πλοίο απαιτούν συνδρομή. Επίσης, η ανάπτυξη εξειδικευμένων αποκωδικοποιητών αποδείχθηκε μια διαδικασία με μεγαλύτερη τεχνική πολυπλοκότητα σε σχέση με άλλες, πιο προσιτές λύσεις ανοιχτού κώδικα.

2.3.2.6 Graylog Security

Τελευταία λύση που εξετάστηκε, ήταν η πλατφόρμα Graylog. Αρχικά ξεκίνησε ως ένα καθαρό εργαλείο διαχείρισης για τα αρχεία καταγραφής και με την πάροδο του χρόνου εξελίχθηκε σε μία ολοκληρωμένη λύση SIEM. Πλέον είναι μια ολοκληρωμένη λύση, εξειδικευμένη στην ανίχνευση και παρακολούθηση κινδύνων ψηφιακής ασφάλειας. Διαθέτει δύο εκδόσεις, τη δωρεάν και την εμπορική που αφορά επιχειρήσεις [33].

Βασικό χαρακτηριστικό του Graylog είναι η ισχυρή διαχείριση που παρέχει στην διαχείριση των αρχείων καταγραφής. Αυτό επιτυγχάνεται μέσα από ένα σύστημα ροών και διοχετεύσεων. Πιο αναλυτικά ο όγκος δεδομένων των ακατέργαστων δεδομένων ομαδοποιείται σε συγκεκριμένες κατηγορίες και έπειτα περνάει μέσα από κανάλια επεξεργασίας όπου φιλτράρονται με βάση τους κανόνες που έχουν οριστεί από τον χρήστη. Για την αποθήκευση και την αναζήτηση αυτών των πληροφοριών, το σύστημα δεν διαθέτει ενσωματωμένη βάση δεδομένων. Χρησιμοποιεί εργαλεία όπως το OpenSearch και το Elasticsearch στο παρασκήνιο [33]. Η προσέγγιση αυτή σημαίνει ότι κατά την εγκατάσταση απαιτείται εγκατάσταση και συντήρηση ενός επιπλέον συστήματος υποδομής.



Σχήμα 2.12: Διεπαφή του Graylog [33]

Στα πλεονεκτήματα του διακρίνεται η ευέλικτη διαχείριση των αρχείων καταγραφής από ετερογενής πηγές. Επίσης, διαθέτει εύχρηστο περιβάλλον το οποίο είναι φιλικό ακόμα και για μη εξειδικευμένους χρήστες. Τέλος σε πειραματικές δοκιμές, έδειξε θετικά αποτελέσματα στην έγκαιρη ανίχνευση κακόβουλου λογισμικού από ύποπτες και συνεχόμενες συμπεριφορές μέσα στα δεδομένα [34].

Σε αξιολόγηση που ακολούθησε, τα αποτελέσματα έδειξαν πως η πλατφόρμα υστερεί σε σύγκριση με το Wazuh. Συγκεκριμένα, οι χρόνοι που αφορούν την άμεση παρακολούθηση και αντίδραση τη στιγμή που εκδηλώνεται ένα περιστατικό ήταν πιο αργοί. Κατά την επεξεργασία μεγάλου όγκου δεδομένων παρουσίασε αυξημένη κατανάλωση πόρων σε επεξεργαστή και μνήμη [34]. Οι λόγοι αυτοί, σε συνδυασμό με το γεγονός ότι οι προχωρημένες λειτουργίες ασφαλείας διατίθενται αποκλειστικά στην εμπορική έκδοση και η υποχρεωτική του ενσωμάτωση με το εργαλείο OpenSearch αυξάνει την πολυπλοκότητα της υποδομής, έκριναν την ανάγκη εύρεσης μίας πιο ικανοποιητικής λύσης.

2.3.3 Τοποθέτηση της παρούσας εργασίας

Στην ανάλυση που προηγήθηκε, αναδείχθηκε η σημασία χρήσης συστημάτων SIEM ως το βασικό εργαλείο συλλογής και αξιολόγησης συμβάντων ασφαλείας. Η πρακτική εφαρμογή τους σε πλοία δεν θεωρείται αυτονόητη, καθώς παρουσιάζει σημαντικές δυσκολίες σε σύγκριση με τη στεριά.

Πίνακας 2.1: Συνοπτική τοποθέτηση της εργασίας σε σχέση με τις ανάγκες

A/A	Κενό που αναδεικνύεται	Κατεύθυνση της εργασίας
1	Διάσπαρτες καταγραφές από διαφορετικά συστήματα	Κεντρική συλλογή και οργάνωση συμβάντων
2	Περιορισμένη ή ασταθής σύνδεση	Τοπική λειτουργία στο πλοίο
3	Υψηλό κόστος εμπορικών λύσεων	Αξιοποίηση λογισμικού ανοιχτού κώδικα
4	Ανάγκη αξιοποίησης ετερογενών δεδομένων	Χρήση μηχανισμών αποκωδικοποίησης και κανόνων

Με βάση τα παραπάνω, η παρούσα εργασία εστιάζει στην πρακτική διερεύνηση μίας αυτόνομης λύσης SIEM, προσαρμοσμένη στις ανάγκες του εξεταζόμενου περιβάλλοντος. Ο στόχος δεν είναι η δημιουργία μίας νέας πλατφόρμας, αλλά η υλοποίηση και η αξιολόγηση της λύσης που κρίθηκε κατάλληλη για την ενίσχυση της ασφάλειας. Το πειραματικό μέρος αυτής της προσέγγισης παρουσιάζεται αναλυτικά στα επόμενα κεφάλαια.

Κεφάλαιο 3ο: Σχεδιασμός και Υλοποίηση

Λαμβάνοντας υπόψη τη θεωρητική προσέγγιση του προηγούμενου κεφαλαίου, στο κεφάλαιο αυτό θα αναλυθεί η πρακτική υλοποίηση της προτεινόμενης λύσης. Η υλοποίηση που παρουσιάζεται δεν αποτελεί μια απλή εγκατάσταση λογισμικού, αλλά αποτελεί μία ολοκληρωμένη πρόταση. Η υποδομή αυτή αφορά την προσαρμογή ενός συστήματος SIEM, στις ιδιαίτερες ανάγκες και την ασφάλεια σε ένα ναυτιλιακό περιβάλλον. Στο πλαίσιο αυτό αναλύεται η πλατφόρμα και τα εργαλεία που επιλέχθηκαν, ο τρόπος που διαμορφώθηκε το εργαστηριακό περιβάλλον και το πως λειτουργεί ο μηχανισμός ανίχνευσης. Ουσιαστικά, η ανάλυση δείχνει πως η θεωρητική ανάγκη εφαρμόζεται στην πράξη.

3.1 Σκοπός και απαιτήσεις της υλοποίησης

Στην παρούσα ενότητα, παρουσιάζεται ο στόχος της υλοποίησης του συστήματος, καθώς αναλύονται οι βασικές απαιτήσεις που καθόρισαν την πορεία ανάπτυξής του. Με στόχο την αρτιότερη προσέγγιση του δεδομένου προβλήματος, πραγματοποιήθηκε διαχωρισμός των απαιτήσεων σε δύο βασικές κατηγορίες:

- Τις λειτουργικές, που αφορούν τις ικανότητες που πρέπει να υποστηρίζει το σύστημα.
- Τις μη λειτουργικές, που αφορούν παραμέτρους όπως η αξιοπιστία, η συνδεσιμότητα και η προστασία δεδομένων.

Και οι δύο κατηγορίες αναλύονται στις υποενότητες που ακολουθούν.

3.1.1 Στόχος της υλοποίησης

Βασικός στόχος της υλοποίησης του συστήματος μας, είναι η ανάπτυξη ενός λειτουργικού πρωτοτύπου SIEM, το οποίο θα μπορεί να συλλέγει, να επεξεργάζεται και να αναλύει δεδομένα ασφαλείας από διαφορετικές πηγές. Παράλληλα, το σύστημα παρέχει στον αναλυτή ένα εύχρηστο και ενιαίο περιβάλλον παρακολούθησης. Η υλοποίηση αυτή υπερβαίνει την απλή παραμετροποίηση ενός λογισμικού. Συγκεκριμένα, επιδιώκει να αποδείξει ότι μια υποδομή η οποία βασίζεται σε εργαλεία ανοιχτού κώδικα μπορεί να υποστηρίξει κρίσιμες λειτουργίες ανίχνευσης και επιτήρησης των απειλών κυβερνοασφάλειας.

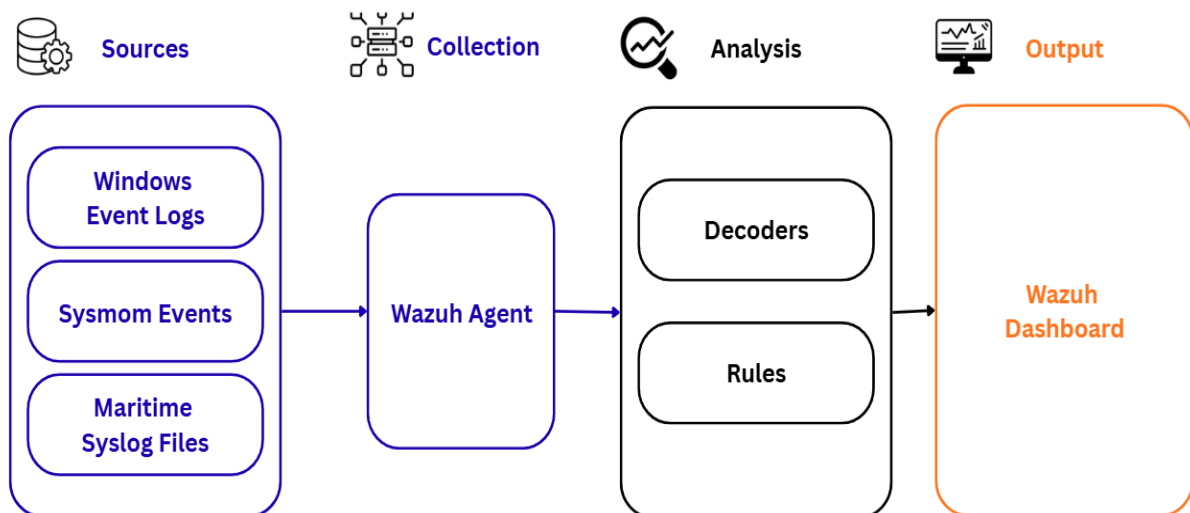
Πιο συγκεκριμένα, επιδιώχθηκε να αναπτυχθεί ένα περιβάλλον με χαμηλό κόστος και περιορισμένες απαιτήσεις πόρων, το οποίο να μπορεί να διατηρεί παράλληλα όλες τις βασικές παραμέτρους που απαιτούνται για την κεντρική διαχείριση συμβάντων. Για αυτόν τον λόγο, ο κεντρικός εξυπηρετητής εγκαταστάθηκε σε ένα λειτουργικό σύστημα ανοιχτού κώδικα, το Ubuntu, το οποίο εκτελείται σε ένα περιβάλλον εικονικής μηχανής μέσω του λογισμικού εικονικοποίησης VMware Workstation. Το τερματικό σημείο παρακολούθησης υλοποιήθηκε στο κεντρικό υπολογιστή (host) με τη χρήση του λειτουργικού συστήματος Windows στο οποίο έγινε εγκατάσταση του πράκτορα (agent) του Wazuh. Η διάταξη αυτή δημιουργήθηκε με στόχο να απλοποιήσει την εγκατάσταση και να διευκολύνει την επαναληψιμότητα, χωρίς την ανάγκη για πρόσθετο φυσικό εξοπλισμό.

Σε λειτουργικό επίπεδο, η υλοποίηση επιδιώκει τη συλλογή συμβάντων από ένα τερματικό σημείο (endpoint) μέσω του Wazuh Agent. Για τον εμπλουτισμό της τηλεμετρίας χρησιμοποιήθηκε το Sysmon (System Monitor), ένα δωρεάν εργαλείο παρακολούθησης συστήματος των Windows. Παράλληλα το σύστημα υποστηρίζει την εισαγωγή και την ανάλυση δεδομένων τύπου Syslog (System Logging Protocol) από πραγματικά ναυτιλιακά περιβάλλοντα. Αυτά τα δεδομένα εισάγονται, όπως αναλύεται σε

επόμενες ενότητες, σε ελεγχόμενο φάκελο. Έτσι ενισχύεται η ρεαλιστικότητα της υλοποίησης και αποδεικνύεται η ικανότητα του συστήματος να διαχειρίζεται διαφορετικές κατηγορίες καταγραφών.

Η υλοποίηση ολοκληρώνεται με την επεξεργασία των καταγραφών, μέσω χρήσης μηχανισμών αποκωδικοποίησης (Decoders) και τη χρήση κανόνων (Rules), οι οποίοι μπορούν να επεξεργάζονται τα ακατέργαστα δεδομένα. Στη συνέχεια παράγονται ειδοποιήσεις (Alerts) με την κατάλληλη διαβάθμιση σοβαρότητας από χαμηλή έως και υψηλή σοβαρότητα. Η τελική οπτικοποίηση προς τον χρήστη για την ανάλυση των περιστατικών, πραγματοποιείται μέσω του κεντρικού πίνακα ελέγχου (Dashboard) ο οποίος προσφέρει ένα ενιαίο και εύκολο περιβάλλον διαχείρισης για τη διερεύνηση των περιστατικών. Η υλοποίηση απεικονίζεται στο Σχήμα 3.1

Το κριτήριο της επιτυχίας της υλοποίησης τεκμηριώνεται όταν λειτουργεί ορθά σε όλα τα στάδια της ροής των δεδομένων. Με άλλα λόγια, όταν διασφαλίζεται ότι τα δεδομένα εισάγονται επιτυχώς, αποκωδικοποιούνται σωστά, αξιολογούνται από τους κανόνες και τέλος εμφανίζονται ως ειδοποιήσεις στον πίνακα ελέγχου. Ως εκ τούτου, δεν εξετάζεται απλώς το κάθε υποσύστημα. Η τελική αξιολόγηση εστιάζει στη συνεργασία των υποσυστημάτων ως μια ενιαία, αδιάσπαστη αλυσίδα που ξεκινά από τη συλλογή και καταλήγει στην ανίχνευση.

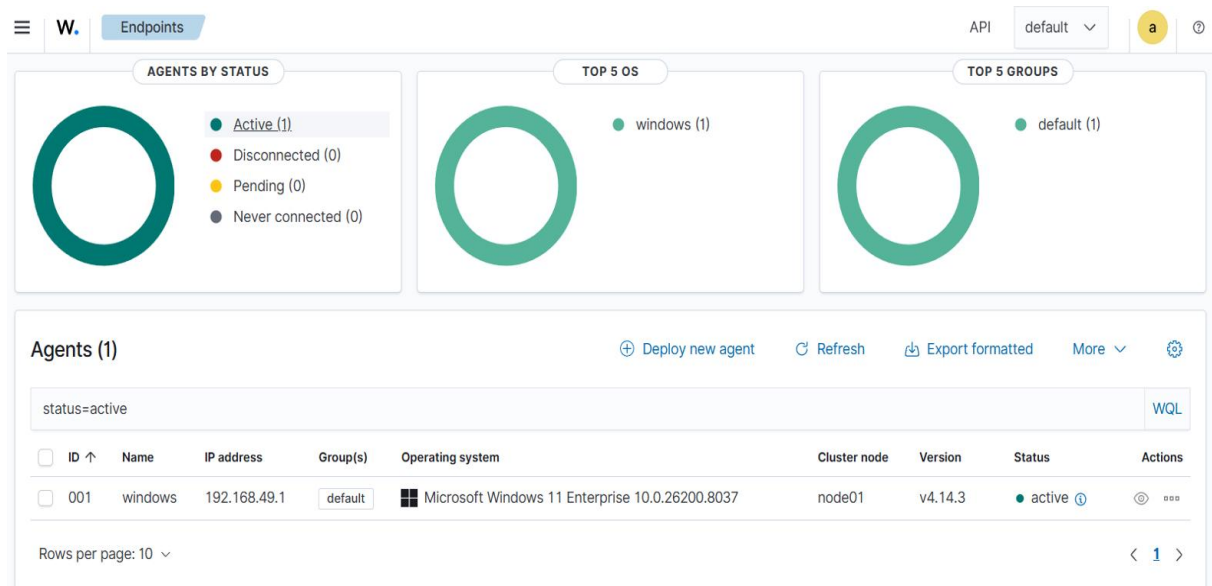


Σχήμα 3.1: Αρχιτεκτονική και ροή δεδομένων του συστήματος Wazuh

3.1.2 Λειτουργικές απαιτήσεις

Με βάση τον παραπάνω στόχο, προσδιορίστηκαν οι λειτουργικές απαιτήσεις που πρέπει να παρέχει το συγκεκριμένο σύστημα, ώστε να φέρει εις πέρας τον ρόλο του ως λειτουργικό πρωτότυπο SIEM. Ειδικότερα, επιλέχθηκαν επτά συγκεκριμένες λειτουργίες οι οποίες, στη συνέχεια υλοποιήθηκαν και επαληθεύθηκαν πειραματικά.

Συλλογή δεδομένων και διασύνδεση τερματικών σημείων: Η πρώτη λειτουργική απαίτηση αφορά την εγκατάσταση πράκτορα για τη συλλογή συμβάντων από ένα τερματικό σύστημα. Η απαίτηση αυτή αποτελεί θεμέλιο του συστήματος διότι η κεντρική συλλογή και η ανάλυση των δεδομένων ασφαλείας εξαρτάται άμεσα από τη σταθερή επικοινωνία του πράκτορα με τον εξυπηρετητή. Η επιτυχής υλοποίηση επιβεβαιώνεται από την ορατότητα του πράκτορα στον πίνακα ελέγχου, όπου η κατάσταση του πρέπει να εμφανίζεται ως ενεργή. Έτσι διασφαλίζεται η απαραίτητη ορατότητα για την εποπτεία του συστήματος.



Σχήμα 3.2: Διεπαφή διαχείρισης τερματικών στο Wazuh

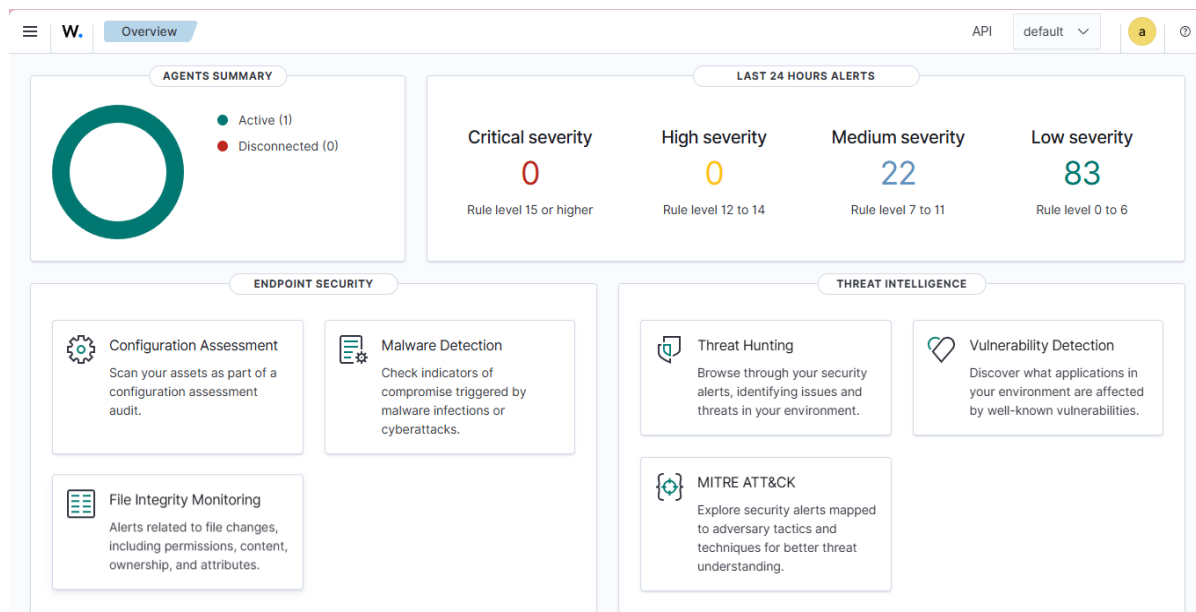
Εμπλουτισμός τηλεμετρίας μέσω Sysmon: Σημαντική απαίτηση για την υλοποίηση ήταν η ενίσχυση των πληροφοριών που συλλέγονται από τερματικά συστήματα. Οι βασικές καταγραφές του λειτουργικού συστήματος παρέχουν μια ορθή πρώτη εικόνα, αλλά για μια εις βάθος αξιολόγηση ενσωματώθηκε το εργαλείο παρακολούθησης συστήματος Sysmon. Με αυτόν τον τρόπο επιτρέπεται η συλλογή εξειδικευμένων συμβάντων από το αντίστοιχο κανάλι του συστήματος. Με αυτή την απαίτηση αυξάνεται η λεπτομέρεια των δεδομένων και βελτιώνεται σημαντικά η έγκαιρη ανίχνευση των σύνθετων απειλών και των ύποπτων ή κακόβουλων δραστηριοτήτων.

Εισαγωγή και διαχείριση εξωτερικών δεδομένων: Η τρίτη λειτουργική απαίτηση αναφέρεται στη δυνατότητα του συστήματος να διαχειρίζεται εξωτερικά δεδομένα της μορφής Syslog. Πρέπει να μπορεί να επεξεργάζεται και εξωτερικές καταγραφές από δικτυακές συσκευές, προσφέροντας έτσι μια γενική εικόνα της ασφάλειας του δικτύου. Στην παρούσα πειραματική υλοποίηση, η εισαγωγή αυτού του τύπου δεδομένων πραγματοποιήθηκε μέσω φακέλου παρακολούθησης και χρησιμοποιήθηκαν ανωνυμοποιημένα αρχεία καταγραφής από ναυτιλιακό περιβάλλον. Η προσέγγιση αυτή έγινε αποκλειστικά για σκοπούς πειραματικών ελέγχων και αξιολόγησης των αποτελεσμάτων.

Αποκωδικοποίηση και κανονικοποίηση δεδομένων: Σημαντικό παράγοντα αποτελεί η διαδικασία αποκωδικοποίησης των δεδομένων καταγραφής. Η απλή αποθήκευση ακατέργαστων δεδομένων δεν επαρκεί για ανάλυση. Για τον λόγο αυτό το σύστημα πρέπει να διαθέτει αποκωδικοποιητές οι οποίοι μετατρέπουν τις εγγραφές σε δομημένα πεδία όπως την πηγή, τον προορισμό, τον τύπο του συμβάντος, την υπηρεσία και άλλα στοιχεία τα οποία διευκολύνουν την ερμηνεία. Αποτελεί πολύ σημαντικό βήμα της υλοποίησης και χωρίς την ύπαρξη του δεν θα μπορούσαν να εφαρμοστούν κανόνες ασφαλείας αλλά ούτε και η ανίχνευση απειλών.

Ανίχνευση συμβάντων και παραγωγή ειδοποιήσεων: Αφού τα δεδομένα οργανωθούν, πρέπει να εφαρμοστεί μια έξυπνη παρακολούθηση η οποία θα ελέγχει αυτόματα τα δεδομένα χρησιμοποιώντας συγκεκριμένους κανόνες. Στην περίπτωση που υπάρχει ύποπτη κίνηση το σύστημα πρέπει να παράγει ειδοποίηση προς τον χρήστη. Οι ειδοποιήσεις αυτές συνοδεύονται από βασικά στοιχεία όπως το επίπεδο σοβαρότητας, την περιγραφή και την κατηγορία που ανήκει ώστε η πληροφορία να αξιολογηθεί με λεπτομέρειες από τον αναλυτή.

Προβολή δεδομένων και αναζήτηση συμβάντων: Η εύκολη πρόσβαση στην παρουσίαση των πληροφοριών όπως τα αρχικά δεδομένα και οι ειδοποιήσεις ασφαλείας αποτέλεσε σημαντική λειτουργία. Ο χρήστης πρέπει να έχει τη δυνατότητα άμεσης αναζήτησης και εφαρμογής φίλτρων για την απομόνωση των σημαντικών γεγονότων. Η απαίτηση θεωρείται καθοριστική, διότι το σύστημα έχει αξία μόνο όταν ο χειριστής μπορεί να καταλάβει και να ερευνήσει γρήγορα ένα πρόβλημα.



Σχήμα 3.3: Κεντρικός πίνακας ελέγχου Wazuh

Είσοδος στο σύστημα και πρόσβαση στις υπηρεσίες: Τελευταία λειτουργική απαίτηση ήταν η διαχείριση της πρόσβασης των χρηστών και η ορθή διασύνδεση των υπηρεσιών. Συγκεκριμένα το σύστημα πρέπει να διασφαλίζει την ασφαλή είσοδο στον πίνακα ελέγχου και την ορθή επικοινωνία των επιμέρους εργαλείων. Η παρούσα υλοποίηση επικεντρώνεται στη βασική λειτουργικότητα πιστοποίησης και πρόσβασης, η οποία αποτελεί αναγκαία προϋπόθεση και δεν στοχεύει σε πλήρη επιχειρησιακή ανάπτυξη. Χωρίς αυτή την απαίτηση ο αναλυτής δεν θα μπορούσε να χρησιμοποιήσει το σύστημα με ασφάλεια και ούτε θα υπήρχε εγγύηση ότι τα δεδομένα μεταφέρονται ορθά.

3.1.3 Μη λειτουργικές απαιτήσεις

Το εξεταζόμενο περιβάλλον, λόγω της πολυπλοκότητάς του, απαιτεί δυνατότητες οι οποίες αφορούν σημαντικά χαρακτηριστικά και περιορισμούς του συστήματος. Για τον λόγο αυτό, εξετάζονται και έξι μη λειτουργικές, αλλά εξίσου σημαντικές απαιτήσεις που ως στόχο έχουν να αναδείξουν εάν η προτεινόμενη λύση είναι πρακτικά εφαρμόσιμη. Ακόμη και αν ένα σύστημα καλύπτει τις βασικές λειτουργίες συλλογής και ανίχνευσης, δεν θεωρείται ολοκληρωμένο εάν είναι υπερβολικά δαπανηρό, δύσχρηστο, μη επεκτάσιμο ή αδύνατο να αναπαραχθεί. Ως εκ τούτου, οι απαιτήσεις αυτές αποτελούν ουσιώδες μέρος του συνολικού σχεδιασμού της υλοποίησης.

Χαμηλό κόστος: Στο σύγχρονο επιχειρηματικό περιβάλλον, ο προϋπολογισμός μιας υλοποίησης αποτελεί καθοριστική παράμετρο. Για αυτό τον λόγο, σημαντική απαίτηση αποτελεί το χαμηλό κόστος κτήσης. Στην παρούσα εργασία επιλέχθηκε τεχνολογία ανοιχτού κώδικα, η οποία δεν απαιτεί εμπορικές άδειες χρήσης. Αποδεικνύεται αναλυτικά ότι είναι εφικτή η ανάπτυξη ενός πλήρως λειτουργικού και αξιόπιστου πρωτοτύπου ασφαλείας ακόμα και με περιορισμένους πόρους. Παράλληλα αποτρέπεται η εξάρτηση από συγκεκριμένους προμηθευτές και προσφέρεται μια λύση η οποία επιτρέπει την πλήρη

παραμετροποίηση και προσαρμογή του συστήματος στις ιδιαίτερες ανάγκες που υπάρχουν στο ναυτιλιακό τομέα.

Τοπική εγκατάσταση και αυτονομία: Δεύτερη απαίτηση της συγκεκριμένης υλοποίησης αποτελεί η ικανότητα του συστήματος να είναι πλήρως λειτουργικό τοπικά. Στον τομέα της ναυτιλίας, δεν διασφαλίζεται πάντα η συνεχόμενη και ασφαλής επικοινωνία, συνεπώς έπρεπε να βρεθεί μια λύση που δεν απαιτεί υποχρεωτική εξάρτηση από εξωτερικές υπηρεσίες. Στη συγκεκριμένη εργασία, η επικοινωνία του εξυπηρετητή με τα τερματικά σημεία αναπτύσσεται εξ ολοκλήρου σε τοπικό περιβάλλον. Με την προσέγγιση αυτή, διασφαλίζεται ο πλήρης έλεγχος μεταφοράς δεδομένων ακόμα και σε περιπτώσεις που αυτό δεν είναι εφικτό ή επιθυμητό.

Λειτουργία χωρίς σύνδεση: Ένα ακόμα συχνό πρόβλημα σε ναυτιλιακές υποδομές είναι η ολική ή και διαλείπουσα απώλεια συνδεσιμότητας. Είναι πολύ σημαντικό το σύστημα να διαχειρίζεται τη συλλογή και αποθήκευση των διαθέσιμων δεδομένων συνεχώς, ώστε να υπάρχει ο τρόπος να εξεταστούν ακόμα και μεταγενέστερα. Η απαίτηση έχει ιδιαίτερη σημασία στη λειτουργία της υλοποίησης, καθώς συνδέεται άμεσα με τα συγκεκριμένα επιχειρησιακά περιβάλλοντα, συμβάλλοντας στην αποφυγή απώλειας κρίσιμων πληροφοριών σε περιπτώσεις δικτυακών προβλημάτων.

Επεκτασιμότητα: Η αρχιτεκτονική της λύσης θα πρέπει να είναι σε θέση να επιτρέπει μια μελλοντική επέκταση και ανάπτυξη. Η αρχιτεκτονική σχεδιάστηκε με στόχο να μπορούν να προστεθούν εύκολα νέες συσκευές και χρήστες. Επιπλέον θα πρέπει να επιτρέπει τη μελλοντική προσθήκη νέων πηγών δεδομένων, νέων αποκωδικοποιητών και νέων κανόνων σε ένα τέτοιο περιβάλλον που συνεχώς αναπτύσσεται. Με αυτόν το τρόπο, η υλοποίηση δεν αποτελεί ένα απλό τεχνικό πείραμα αλλά μια βάση για περαιτέρω ανάπτυξη.

Ασφάλεια και εμπιστευτικότητα: Σε ένα πλοίο, τα δεδομένα που συλλέγονται καθημερινά περιέχουν ευαίσθητες πληροφορίες με μεγάλη επιχειρησιακή αξία, που συχνά γίνονται στόχος από τρίτους. Επομένως η πρόσβαση σε αυτά είναι σημαντικό να παραμένει υπό τον έλεγχο του διαχειριστή και να προστατεύονται με κατάλληλους μηχανισμούς ασφαλείας και ελέγχου πρόσβασης. Η τοπική εγκατάσταση της πλατφόρμας περιορίζει την πρόσβαση μόνο σε εξουσιοδοτημένους χρήστες, οι οποίοι διαθέτουν δικαίωμα πρόσβασης στο περιβάλλον διαχείρισης και στις υπηρεσίες με τη χρήση κωδικών πρόσβασης, ενώ η πρόσβαση είναι διαβαθμισμένη σε επίπεδα ανάλογα με τον ρόλο και τα δικαιώματα κάθε χρήστη.

Επαναληψιμότητα: Κάθε επιστημονική δοκιμή οφείλει να χαρακτηρίζεται από αναπαραγωγιμότητα, ώστε τα αποτελέσματα να ελέγχονται και να επαληθεύονται. Η χρήση εικονικής μηχανής και η σαφής καταγραφή των ρυθμίσεων διευκολύνουν την επανάληψη της διαδικασίας. Η επαναληψιμότητα αποτελεί κρίσιμο στοιχείο όχι μόνο για επιστημονικούς λόγους εγκυρότητας αλλά και για λόγους πρακτικής συντήρησης με στόχο την πραγματοποίηση μελλοντικών δοκιμών.

3.2 Επιλογή τεχνολογιών και εργαλείων

Στην ενότητα αυτή αναλύονται οι θεμελιώδεις τεχνολογικές επιλογές που υιοθετήθηκαν για την ανάπτυξη του προτεινόμενου συστήματος, καθώς και τα κριτήρια με βάση τα οποία διαμορφώθηκαν. Στόχος δεν είναι η παρουσίαση των τελικών αποτελεσμάτων της υλοποίησης, αλλά η τεκμηρίωση του σχεδιασμού της. Πιο συγκεκριμένα αιτιολογείται η χρήση της πλατφόρμας Wazuh ως η πιο κατάλληλη λύση για τη συγκεκριμένη υποδομή. Η ανάλυση που ακολουθεί, αποσκοπεί στη συσχέτιση των αποφάσεων σχεδιασμού που πάρθηκαν με στόχο να αποτελέσει γέφυρα με τη θεματολογία των επόμενων ενοτήτων, οι οποίες αφορούν την εγκατάσταση, την παραμετροποίηση και την πειραματική αξιολόγηση.

Το Wazuh αποτελεί μια ολοκληρωμένη λύση ασφάλειας, η οποία συνδυάζει τις δυνατότητες διαχείρισης των πληροφοριών και των συμβάντων ασφαλείας (SIEM) με τις τεχνολογίες διευρυμένης ανίχνευσης και απόκρισης (XDR). Στο πλαίσιο αυτό, αναλύεται η αρχιτεκτονική του, η οποία χωρίζεται σε τέσσερα κύρια δομικά στοιχεία, καθώς και η ροή των δεδομένων από το στάδιο της συλλογής έως την τελική οπτικοποίηση.

3.2.1 Επιλογή SIEM ανοιχτού κώδικα

Η αρχική σχεδιαστική απόφαση της υλοποίησης, αφορούσε την επιλογή της κατηγορίας της λύσης που θα χρησιμοποιούνταν, δηλαδή αν το πειραματικό περιβάλλον θα στηριζόταν σε εμπορική πλατφόρμα ή σε ανοιχτού κώδικα πλατφόρμα SIEM. Για τις ανάγκες της μελέτης υιοθετήθηκε η δεύτερη κατηγορία, καθώς ζητούμενο ήταν η ανάπτυξη ενός περιβάλλοντος που να επιτρέπει την εγκατάσταση, την παραμετροποίηση και τον τεχνικό έλεγχο των επιμέρους μηχανισμών του. Μια λύση ανοιχτού κώδικα εξυπηρετεί καλύτερα αυτή τη λογική διότι προσφέρει άμεση πρόσβαση στη δομή του συστήματος, τη δυνατότητα προσαρμογής των ρυθμίσεων και την αναπαραγωγιμότητα της εγκατάστασης σε ελεγχόμενο εργαστηριακό περιβάλλον. Στο πλαίσιο της παρούσας ενότητας η απόφαση αυτή αντιμετωπίζεται ως τεχνική απόφαση σχεδιασμού και όχι ως συγκριτική αξιολόγηση εμπορικών και μη εμπορικών λύσεων.

Η επιλογή μιας πλατφόρμας SIEM ανεξάρτητα από το επιχειρησιακό περιβάλλον στο οποίο πρόκειται να εγκατασταθεί, απαιτεί ένα σαφές σύνολο τεχνικών κριτηρίων. Πρώτη απαίτηση είναι η συλλογή δεδομένων από διαφορετικές πηγές. Στην παρούσα υλοποίηση έπρεπε να εξεταστούν εξωτερικά δεδομένα καταγραφής τα οποία θα ελεγχθούν μέσω πειραμάτων. Επίσης σημαντική ήταν και η δυνατότητα επεξεργασίας δεδομένων που προέρχονται από λειτουργικά συστήματα προσομοιώνοντας ένα πραγματικό ναυτιλιακό σενάριο. Έτσι θα μπορεί το σύστημα να αποδώσει ως ολοκληρωμένο σενάριο SIEM. Κρίθηκε απαραίτητη και η δυνατότητα αποκωδικοποίησης και εξαγωγής πεδίων ώστε να είναι κατάλληλα για περαιτέρω επεξεργασία. Βάσει αυτού, το σύστημα έπρεπε να εφαρμόζει τεχνικές ανίχνευσης ώστε τα δεδομένα να υποστηρίζουν λειτουργίες ανάλυσης των συμβάντων ασφαλείας. Τέλος σημαντική ήταν η εύρεση μιας λύσης που προσφέρει κεντρική αποθήκευση, αναζήτηση και οπτικοποίηση. Ο αναλυτής πρέπει να είναι σε θέση να αναζητεί και να φιλτράρει δεδομένα από ένα ενιαίο περιβάλλον.

Τα κριτήρια αυτά δεν διαμορφώθηκαν με στόχο μια γενική θεωρητική κατάταξη των λύσεων αλλά ως πρακτικό πλαίσιο λήψης απόφασης για τη συγκεκριμένη υλοποίηση. Με άλλα λόγια, το ζητούμενο δεν ήταν να απαντηθεί ποια πλατφόρμα είναι συνολικά καλύτερη αλλά ποια μπορεί να καλύψει τις απαιτήσεις της παρούσας εργασίας. Έτσι η επιλογή της κατηγορίας ανοιχτού κώδικα SIEM λειτούργησε ως ενδιάμεσο στάδιο ανάμεσα στον προσδιορισμό των τεχνικών αναγκών και στην τελική επιλογή του Wazuh ως εργαλείου υλοποίησης.

Πίνακας 3.1: Προδιαγραφές και λειτουργίες της λύσης SIEM

A/A	Απαίτηση	Περιγραφή
1	Συλλογή δεδομένων	Υποστήριξη πολλαπλών πηγών
2	Παρακολούθηση τερματικών	Δυνατότητα συλλογής δεδομένων από τερματικά
3	Κανονικοποίηση	Μετατροπή αρχείων σε δομημένα πεδία
4	Ανίχνευση	Υποστήριξη κανόνων και παραγωγή ειδοποιήσεων
5	Αποθήκευση	Κεντρική αποθήκευση και δυνατότητα αναζήτησης
6	Οπτικοποίηση	Προβολή και άμεση διερεύνηση
7	Παραμετροποίηση	Προσαρμογή ρυθμίσεων και κανόνων

Η επιλογή μιας πλατφόρμας SIEM ανεξάρτητα από το επιχειρησιακό περιβάλλον στο οποίο πρόκειται να εγκατασταθεί, απαιτεί ένα σαφές σύνολο τεχνικών κριτηρίων. Πρώτη απαίτηση είναι η συλλογή δεδομένων από διαφορετικές πηγές. Στην παρούσα υλοποίηση έπρεπε να εξεταστούν εξωτερικά δεδομένα καταγραφής τα οποία θα ελεγχθούν μέσω πειραμάτων. Επίσης σημαντική ήταν και η δυνατότητα επεξεργασίας δεδομένων που προέρχονται από λειτουργικά συστήματα προσομοιώνοντας ένα πραγματικό ναυτιλιακό σενάριο. Έτσι θα μπορεί το σύστημα να αποδώσει ως ολοκληρωμένο σενάριο SIEM. Κρίθηκε απαραίτητη και η δυνατότητα αποκωδικοποίησης και εξαγωγής πεδίων ώστε να είναι κατάλληλα για περαιτέρω επεξεργασία. Βάσει αυτού, το σύστημα έπρεπε να εφαρμόζει τεχνικές ανίχνευσης ώστε τα δεδομένα να υποστηρίζουν λειτουργίες ανάλυσης των συμβάντων ασφαλείας. Τέλος σημαντική ήταν η εύρεση μιας λύσης που προσφέρει κεντρική αποθήκευση, αναζήτηση και οπτικοποίηση. Ο αναλυτής πρέπει να είναι σε θέση να αναζητεί και να φιλτράρει δεδομένα από ένα ενιαίο περιβάλλον.

Τα κριτήρια αυτά δεν διαμορφώθηκαν με στόχο μια γενική θεωρητική κατάταξη των λύσεων αλλά ως πρακτικό πλαίσιο λήψης απόφασης για τη συγκεκριμένη υλοποίηση. Με άλλα λόγια, το ζητούμενο δεν ήταν να απαντηθεί ποια πλατφόρμα είναι συνολικά καλύτερη αλλά ποια μπορεί να καλύψει τις απαιτήσεις της παρούσας εργασίας. Έτσι η επιλογή της κατηγορίας ανοιχτού κώδικα SIEM λειτούργησε ως ενδιάμεσο στάδιο ανάμεσα στον προσδιορισμό των τεχνικών αναγκών και στην τελική επιλογή του Wazuh ως εργαλείου υλοποίησης.

3.2.2 Επιλογή της πλατφόρμας Wazuh

Με βάση τις παραπάνω ανάγκες, έπρεπε να επιλεγθεί μία πλατφόρμα η οποία παρέχει όλες τις βασικές δυνατότητες που απαιτήθηκαν. Το Wazuh, παρέχει σε μια ενιαία αρχιτεκτονική σημαντικό μέρος του φάσματος της ανάλυσης δεδομένων ασφαλείας που ζητείται, γι' αυτό επιλέχθηκε ως κεντρική πλατφόρμα.

Το πρώτο και βασικότερο κριτήριο ήταν η ευελιξία που προσφέρει στη συλλογή πληροφοριών από ετερογενείς πηγές, καθώς ένα περιβάλλον όπως αυτό της ναυτιλίας απαιτεί συνδυασμό τηλεμετρίας από διάφορα τερματικά. Με αυτό τον τρόπο διαφορετικές μορφές καταγραφής αρχείων, μπορούν να λειτουργούν σε ένα κοινό περιβάλλον συγκέντρωσης, χωρίς να χρειάζεται η χρήση πολλών ξεχωριστών εργαλείων. Παράλληλα, η πλατφόρμα διαθέτει μια πολύ ξεκάθαρη δομή αποτελούμενη από υποσυστήματα με διακριτούς ρόλους. Η διάκριση ρόλων σε συλλογή των στοιχείων, η κεντρική ανάλυση τους και η αποθήκευση για οπτικοποίηση βοήθησε τόσο στη δημιουργία του συστήματος όσο και στην κατανοητή παρουσίαση της υποδομής. Ιδιαίτερη σημασία δόθηκε και στο γεγονός ότι το Wazuh δεν περιορίζεται σε απλή αποθήκευση πληροφοριών. Οι έξυπνοι μηχανισμοί που παρέχει για την ανάλυση δίνουν τη δυνατότητα να αναγνωρίζονται ύποπτες δραστηριότητες και να παράγονται ειδοποιήσεις σε σχεδόν πραγματικό χρόνο. Αυτό επιτυγχάνεται με χρήση αποκωδικοποιητών και κανόνων οι οποίοι μετατρέπουν τα συχνά δυσνόητα δεδομένα σε δομημένη πληροφορία.

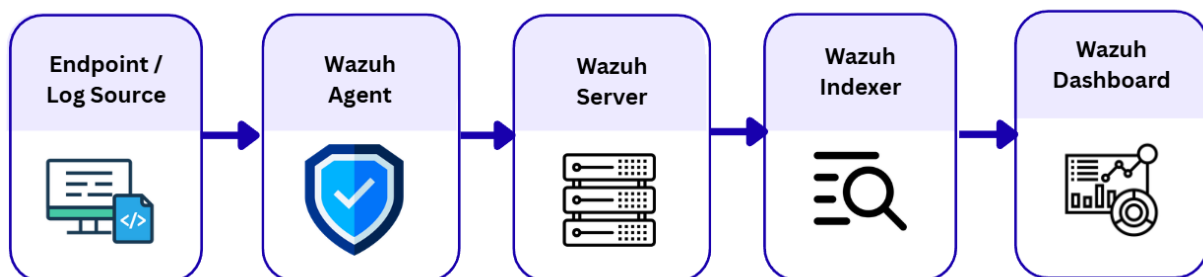
Τέλος, η καταλληλότητα της υποδομής κρίθηκε και από τη δυνατότητα που παρέχει στον χειριστή για παραμετροποίηση και της εκτενούς τεκμηρίωσης της. Είναι πολύ απαραίτητο το λογισμικό να προσαρμόζεται σε ειδικές απαιτήσεις. Για παράδειγμα, το περιβάλλον της ναυτιλίας απαιτεί δημιουργία προσωποποιημένων και ειδικά προσαρμοσμένων κανόνων ασφαλείας. Η ευκολία στην παραμετροποίηση σε συνδυασμό με την ύπαρξη αναλυτικών οδηγιών για κάθε λειτουργία, επέτρεψε όχι μόνο την επιτυχή υλοποίηση του συστήματος αλλά και τη συστηματική επαλήθευση κάθε βήματος της διαδικασίας. Αυτό προσδίδει στο σύστημα μεγαλύτερη αξιοπιστία στο τελικό αποτέλεσμα.

3.2.3 Βασικά υποσυστήματα του Wazuh και ροή δεδομένων

Σε συνέχεια της τεκμηρίωσης επιλογής της πλατφόρμας, θα παρουσιαστούν τα βασικά υποσυστήματα που τη συνθέτουν. Η αρχιτεκτονική του συστήματος Wazuh, όπως φαίνεται στο Σχήμα 3.4, ορίζεται από τέσσερα κύρια στοιχεία:

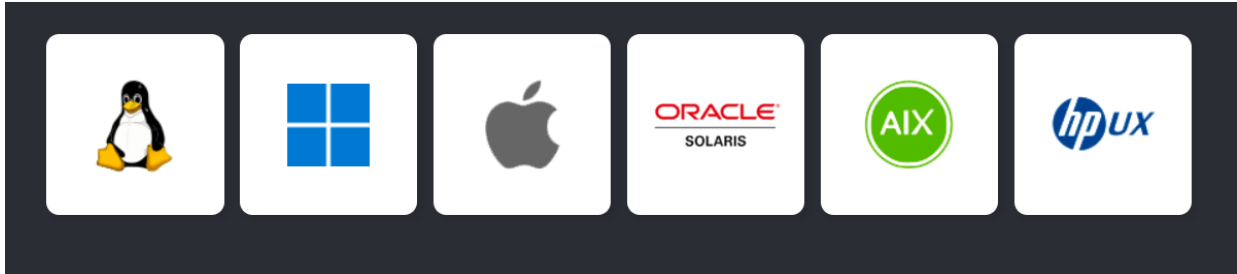
- Τον πράκτορα (Agent),
- Τον εξυπηρετητή (Server),
- Τον ευρετηριαστή (Indexer) και
- Τον πίνακα ελέγχου (Dashboard)

Είναι πολύ σημαντικό να αναφερθεί η χρήση τους για την κατανόηση της γενικής λογικής λειτουργίας της πλατφόρμας.



Σχήμα 3.4: Αρχιτεκτονική του συστήματος Wazuh

Wazuh Agent: Ο πράκτορας είναι το λογισμικό που εγκαθίσταται στα τερματικά σημεία και ως ρόλο έχει την παρακολούθηση και τη συλλογή των δεδομένων ασφαλείας. Επικοινωνεί σε πραγματικό χρόνο με τον εξυπηρετητή προωθώντας τα δεδομένα. Η χρήση του είναι μείζονος σημασίας, καθώς εξασφαλίζει την άμεση πρόσβαση στις πληροφορίες του συστήματος που επιτηρείται.



Σχήμα 3.5: Υποστηριζόμενα λειτουργικά συστήματα από τους Wazuh Agents [35]

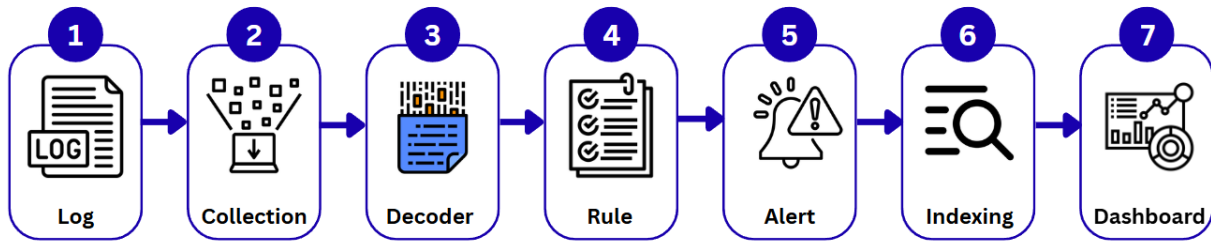
Wazuh Server: Ο εξυπηρετητής αποτελεί το κεντρικό στοιχείο της ανάλυσης. Είναι υπεύθυνος για τη συλλογή των αρχείων καταγραφής, την ανάλυση τους και τη συνολική διαχείριση της πληροφορίας. Για να επιτευχθεί αυτό χρησιμοποιεί τρεις σημαντικές υπηρεσίες. Η υπηρεσία Logcollector είναι υπεύθυνη για τη συλλογή, οι αποκωδικοποιητές για την περαιτέρω ανάλυση και η υπηρεσία Analysisd για την αξιολόγηση των συμβάντων σύμφωνα με τους κανόνες που έχουν οριστεί. Συνολικά συμπεραίνουμε ότι λειτουργεί ως ο πυρήνας του μηχανισμού ανίχνευσης.

Wazuh Indexer: Ο ευρετηριαστής λειτουργεί ως μηχανή αναζήτησης αλλά και ανάλυσης του κειμένου. Σκοπός του είναι η αρχειοθέτηση των ειδοποιήσεων που εμφανίζονται και επιτρέπει την ανάλυση τους σε σχεδόν πραγματικό χρόνο. Αναλαμβάνει την οργάνωση, την αναζήτηση και την αποθήκευση των δεδομένων επιτρέποντας στον αναλυτή την πρόσβαση του σε αυτά οποιαδήποτε στιγμή.

Wazuh Dashboard: Η διεπαφή χρήστη, που αποτελεί το γραφικό περιβάλλον της πλατφόρμας, παρέχει αναλυτικά την παρακολούθηση των καταγραφών και των στατιστικών καθώς και τη διαμόρφωση του server και τη δημιουργία προσαρμοσμένων κανόνων. Με άλλα λόγια δεν αποτελεί ένα απλό εργαλείο προβολής αλλά είναι το κεντρικό σημείο της διαχείρισης και της παραμετροποίησης ολόκληρης της πλατφόρμας.

Η ροή που προαναφέρθηκε αποκτά νόημα όταν εξεταστεί και ως ροή δεδομένων (Σχήμα 3.6). Αρχικά η διαδικασία περιλαμβάνει τη συλλογή των αρχείων καταγραφής από τα τερματικά. Στην συνέχεια, τα δεδομένα αυτά προωθούνται στο κύριο εξυπηρετητή. Εκεί εφαρμόζονται οι αποκωδικοποιητές για την εξαγωγή των δομημένων πεδίων και εφαρμόζονται οι κανόνες ώστε να γίνει η αξιολόγηση των γεγονότων. Οι παραγόμενες ειδοποιήσεις προωθούνται στον ευρετηριαστή όπου γίνεται η μόνιμη αποθήκευση και οργάνωση τους. Τέλος τα δεδομένα γίνονται ορατά στον κεντρικό πίνακα ελέγχου. Έτσι ολοκληρώνεται ο κύκλος της επεξεργασίας που αφορά τη μετατροπή ακατέργαστων δεδομένων σε σημαντική πληροφορία.

Η ακολουθία αυτή της επεξεργασίας είναι κρίσιμη για τη λογική της παρούσας εργασίας. Εξηγείται πως ένα ακατέργαστο αρχείο μιας απλής καταγραφής μετατρέπεται σε σημαντική πληροφορία για τον αναλυτή. Η επιλογή της ανοιχτού κώδικα πλατφόρμας Wazuh βασίστηκε στην ικανότητα να υποστηρίζει ολόκληρη αυτή τη διαδρομή σε ένα ενοποιημένο και κατανοητό περιβάλλον.



Σχήμα 3.6: Ροή συλλογής, αποκωδικοποίησης και παραγωγής ειδοποιήσεων στο Wazuh

3.3 Ανάλυση περιβάλλοντος υλικού και λογισμικού

Στην παρούσα ενότητα παρουσιάζεται το περιβάλλον υλικού αλλά και λογισμικού στο οποίο βασίστηκε η συγκεκριμένη υλοποίηση του προτεινόμενου συστήματος. Σκοπός είναι να αποτυπωθεί η εργαστηριακή υποδομή και να εξηγηθεί ο τρόπος με τον οποίο έγινε η οργάνωση του περιβάλλοντος των δοκιμών. Η ανάλυση που ακολουθεί αποτελεί τεχνικό υπόβαθρο πάνω στο οποίο στηρίχθηκε η ανάπτυξη.

Η υλοποίηση πραγματοποιήθηκε σε μικρό εργαστηριακό περιβάλλον το οποίο βασίστηκε σε έναν υπολογιστή. Η χρήση του λειτουργικού συστήματος Windows βοήθησε στην εύκολη εγκατάσταση του λογισμικού εικονικοποίησης VMware Workstation, μέσα στο οποίο δημιουργήθηκε μια εικονική μηχανή με το λειτουργικό σύστημα Ubuntu. Η εικονική μηχανή χρησιμοποιήθηκε ως κύριος κόμβος στον οποίο έγινε η εγκατάσταση των βασικών υποσυστημάτων του Wazuh. Παράλληλα το φυσικό περιβάλλον του συστήματος Windows αξιοποιήθηκε και ως τερματικό παρακολούθησης με την εγκατάσταση του πράκτορα Wazuh.

Η συγκεκριμένη διάταξη επιλέχθηκε καθώς επιτρέπει την ανάπτυξη ολόκληρης της υποδομής αλλά και την εφαρμογή του πειραματικού μέρους από ένα μόνο φυσικό υπολογιστή.

Η συνολική αρχιτεκτονική οργανώθηκε σε τέσσερα βασικά στοιχεία. Το φυσικό σύστημα υποδοχής, την πλατφόρμα εικονικοποίησης, την εικονική μηχανή εξυπηρέτησης και το τερματικό σύστημα παρακολούθησης τα οποία θα παρουσιαστούν στις επόμενες υποενότητες.

3.3.1 Φυσικό σύστημα υποδοχής και τερματικό παρακολούθησης

Για την παρούσα υποδομή χρησιμοποιήθηκε προσωπικός υπολογιστής με το λειτουργικό σύστημα Windows ως βασική φυσική πλατφόρμα πάνω στην οποία αναπτύχθηκε ολόκληρη η υπόλοιπη εργαστηριακή υποδομή. Το συγκεκριμένο λειτουργικό σύστημα γενικής χρήσης παρέχει γραφικό περιβάλλον, υποστήριξη εφαρμογών καθώς και τη δυνατότητα εκτέλεσης του λογισμικού εικονικοποίησης που θα χρειαστούμε παρακάτω.

Ο ρόλος του κρίθηκε διπλής σημασίας. Αρχικά χρησιμοποιήθηκε ως φυσικό σύστημα το οποίο παρέχει τους απαραίτητους υπολογιστικούς πόρους που χρειαζόταν για την εκτέλεση της εικονικής μηχανής. Στην παρούσα υλοποίηση φιλοξενεί τη μηχανή Ubuntu VM, η οποία χρησιμοποιήθηκε ως το κεντρικό σύστημα εξυπηρέτησης της πλατφόρμας Wazuh. Ο δεύτερος ρόλος του ήταν επιτηρούμενο τερματικό σημείο. Ο πράκτορας του Wazuh εγκαταστάθηκε εκεί ώστε να είναι δυνατή η συλλογή συμβάντων και η αποστολή του προς το κεντρικό κόμβο. Με αυτόν τον τρόπο το σύστημα Windows δεν λειτούργησε ως βάση της υποδομής αλλά και ως πηγή τερματικής τηλεμετρίας.

Οι δύο αυτοί ρόλοι παρόλο που αντιστοιχούν στην ίδια φυσική συσκευή διαχωρίζονται σε ρόλο λειτουργίας. Η επιλογή αυτή έγινε για πειραματικούς λόγους και επέτρεψε την ανάπτυξη ενός πλήρους εργαστηριακού σεναρίου χωρίς την ανάγκη επιπλέον εξοπλισμού. Η διάκριση των δύο αυτών ρόλων είναι σημαντική για την κατανόηση της αρχιτεκτονικής της υλοποίησης.

3.3.2 Πλατφόρμα εικονικοποίησης

Για τη δημιουργία του εργαστηριακού περιβάλλοντος χρησιμοποιήθηκε το VMware Workstation. Το συγκεκριμένο αποτελεί λογισμικό εικονικοποίησης το οποίο επιτρέπει την εκτέλεση εικονικών υπολογιστών πάνω στο φυσικό σύστημα υποδοχής. Οι εικονικοί υπολογιστές έχουν τη δυνατότητα να διαθέτουν το δικό τους λειτουργικό σύστημα με εικονικό δίσκο, μνήμη, επεξεργαστικούς πόρους και δικτυακές διεπαφές.

Στο πλαίσιο της παρούσας η πλατφόρμα αυτή αποτέλεσε τη βάση για την ανάπτυξη μια υποδομής τύπου server με endpoint. Το VMware ρυθμίστηκε έτσι ώστε να δεσμεύει τους απαραίτητους πόρους από το σύστημα υποδοχής, ώστε να μπορεί να εκτελέσει τον ρόλο του κεντρικού κόμβου. Έτσι κατέστη δυνατή η υλοποίηση με πλήρη λογικό διαχωρισμό των ρόλων της αρχιτεκτονικής επιτρέποντας τον φυσικό υπολογιστή να εκτελεί άλλες λειτουργίες.

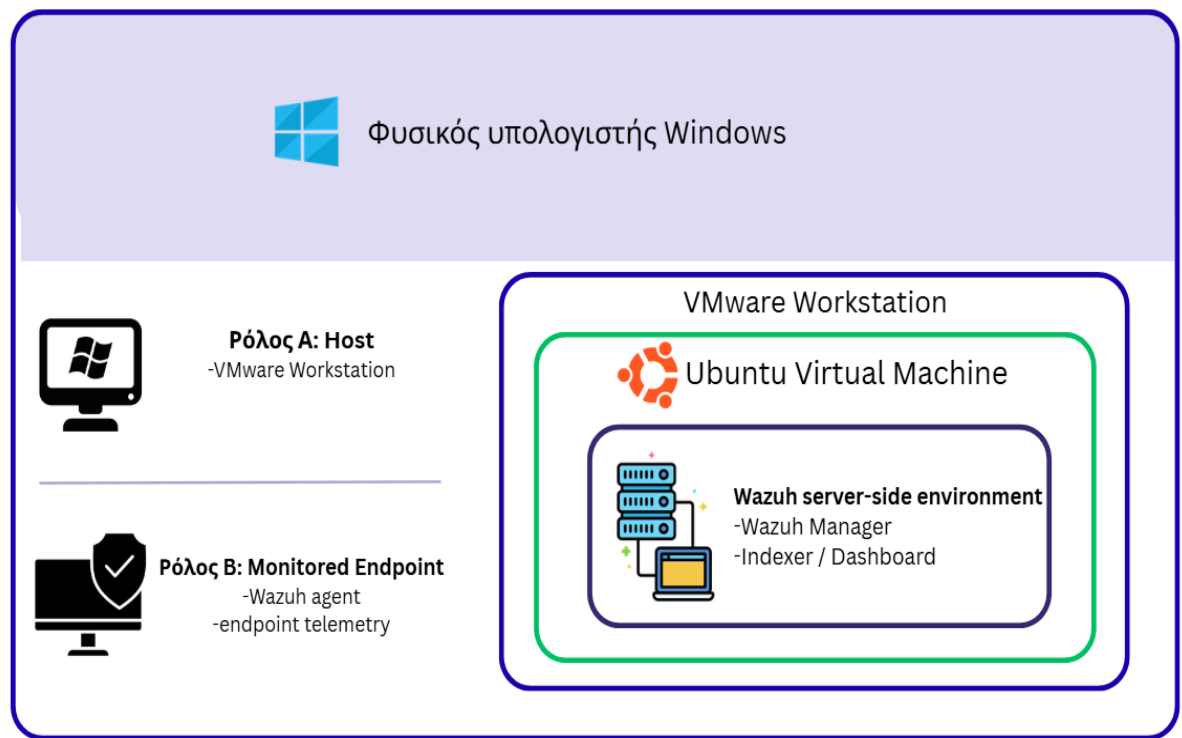
Εκτός της εξοικονόμησης υλικού η χρήση του VMware Workstation πρόσφερε σημαντικά τεχνικά πλεονεκτήματα. Αρχικά έγινε δυνατή η ανεξάρτητη διαχείριση και παραμετροποίηση του κεντρικού κόμβου χωρίς να επηρεάζεται το βασικό λειτουργικό σύστημα. Παράλληλα μέσω εικονικής δικτύωσης δημιουργήθηκαν εικονικοί προσαρμογείς για να επιτρέψουν τη σταθερή επικοινωνία των συστημάτων. Η δυνατότητα αυτή υπήρξε καθοριστική στη διαδικασία των δοκιμών καθώς προσομοιώνει με ακρίβεια συνθήκες επικοινωνίας μιας πραγματικής εγκατάστασης.

3.3.3 Λειτουργικό σύστημα εικονικής μηχανής

Σε συνέχεια της εγκατάστασης του λογισμικού της πλατφόρμας εικονικοποίησης αναπτύχθηκε σε αυτή το λειτουργικό σύστημα. Συγκεκριμένα επιλέχθηκε το Ubuntu που αποτελεί μια διανομή Linux. Η επιλογή αυτή έγινε λόγω της σταθερότητας, της ευελιξίας και της εξαιρετικής συμβατότητας της με εργαλεία ανοιχτού κώδικα. Τα Ubuntu αποτελούν μια σημαντική λύση για τεχνικά περιβάλλοντα καθώς επιτρέπουν την πλήρη παραμετροποίηση των υπηρεσιών που έχει το σύστημα και τη διαχείριση τους μέσω τερματικού. Η επιλογή αυτή προσφέρει ασφάλεια και υπόβαθρο για την υποστήριξη πιο σύνθετων εργαστηριακών υποδομών.

Στην παρούσα υλοποίηση η εικονική μηχανή λειτουργεί ως κεντρικός κόμβος, καθώς αναλαμβάνει να φιλοξενήσει τον ρόλο του διακομιστή της πλατφόρμας Wazuh. Το σύστημα αυτό λειτουργεί ως πυλώνας της αρχιτεκτονικής αναλαμβάνοντας τον ρόλο της λήψης, επεξεργασίας και ανάλυσης των δεδομένων ασφαλείας. Με τον τρόπο αυτό η εικονική μηχανή γίνεται αυτόνομος server που επιπλέον παρέχει τα απαραίτητα εργαλεία αποθήκευσης και οπτικοποίησης των αποτελεσμάτων.

Η χρήση της εικονικής μηχανής προσφέρει σαφήνεια στην αρχιτεκτονική επιτρέποντας τον λογικό διαχωρισμό μεταξύ των ρόλων κεντρικού κόμβου και τερματικού. Επίσης διευκολύνει τον έλεγχο των υπηρεσιών σε ένα ελεγχόμενο και απομονωμένο περιβάλλον. Η επιλογή αυτή προσεγγίζει με ακρίβεια τις συνθήκες λειτουργίας μιας επαγγελματικής πλατφόρμας ανοιχτού κώδικα SIEM χωρίς επιπλέον φυσικό εξοπλισμό. Η συνολική εργαστηριακή διάταξη της υλοποίησης παρουσιάζεται στο Σχήμα 3.7.



Σχήμα 3.7: Εργαστηριακή υποδομή και αρχιτεκτονική υλοποίησης

3.3.4 Δικτυακή διασύνδεση φυσικού συστήματος με εικονική μηχανή

Κατά την διάρκεια δοκιμών η δικτυακή διασύνδεση αποτέλεσε κρίσιμο παράγοντα στην επιτυχία της διασύνδεσης. Έπρεπε να βρεθεί τρόπος μιας αδιάλειπτης επικοινωνίας μεταξύ του φυσικού συστήματος και της εικονικής μηχανής. Η χρήση του πρωτοκόλλου δυναμικής διαμόρφωσης κεντρικού υπολογιστή (DHCP) καθιστούσε την υποδομή ασταθή. Οι μεταβαλλόμενες διευθύνσεις IP επέβαλαν συνεχείς χειροκίνητες αναπροσαρμογές στις ρυθμίσεις της πλατφόρμας. Για την επίλυση του προβλήματος δημιουργήθηκε ένα σταθερό υποδίκτυο το οποίο επέτρεψε στα δύο συστήματα την απευθείας επικοινωνία ανεξάρτητα από το δίκτυο στο οποίο ήταν συνδεδεμένος ο φυσικός υπολογιστής.

Αρχικά δημιουργήθηκε ο Host-Only Adapter, ένας τύπος δικτύωσης που βρίσκουμε σε εικονικές μηχανές και δημιουργεί ένα απομονωμένο και ιδιωτικό δίκτυο. Οργανώθηκε ένα υποδίκτυο 192.168.49.X και δόθηκε από μία διεύθυνση στον φυσικό υπολογιστή και μία στην εικονική μηχανή. Η σταθερότητα μεταξύ των δύο αυτών διευθύνσεων επέτρεψε τη συνεχόμενη αποστολή δεδομένων προς τον κεντρικό. Έτσι διασφαλίστηκε η σταθερή ροή δεδομένων ακόμα και αν άλλαζαν οι δικτυακές παράμετροι του φυσικού περιβάλλοντος.

Παράλληλα για την εικονική μηχανή Ubuntu δημιουργήθηκε μια δεύτερη δικτυακή διεπαφή μετάφρασης διευθύνσεων δικτύου (NAT). Αυτή λειτούργησε ως πύλη προς τη σύνδεση με το διαδίκτυο για τη λήψη ενημερώσεων και απαραίτητων πακέτων λογισμικού. Με αυτήν την υβριδική λύση το πειραματικό περιβάλλον παρέμεινε απόλυτα σταθερό, διατηρώντας παράλληλα τη συνοχή του κάτω από οποιοδήποτε συνθήκες εξωτερικής δικτύωσης. Οι τελικές δικτυακές ρυθμίσεις της εικονικής μηχανής, επιβεβαιώνονται στο Σχήμα 3.8 όπως φαίνεται παρακάτω.

```

pinelopi@pinelopi-VMware-Virtual-Platform:/var/log$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:24:6a:dc brd ff:ff:ff:ff:ff:ff
    inet 192.168.49.128/24 brd 192.168.49.255 scope global noprefixroute ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe24:6adc/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:24:6a:e6 brd ff:ff:ff:ff:ff:ff
    altname enp2s5
    altname enx000c29246ae6
    inet 192.168.32.130/24 brd 192.168.32.255 scope global dynamic noprefixroute ens37
        valid_lft 1693sec preferred_lft 1693sec
    inet6 fe80::a551:f7d7:1e57:8724/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

```

Σχήμα 3.8: Επιβεβαίωση δικτυακών ρυθμίσεων στην εικονική μηχανή

3.4 Εγκατάσταση και βασική παραμετροποίηση εξυπηρετητή Wazuh

Στην ενότητα αυτή περιγράφεται η υλοποίηση της πλατφόρμας Wazuh ως κεντρικό σύστημα διαχείρισης της ασφάλειας στην εικονική μηχανή Ubuntu. Όπως ήδη αναφέρθηκε, έχει επιλεγεί μια ενιαία δομή στην οποία ο διακομιστής, ο ευρετηριαστής και ο πίνακας ελέγχου έχουν εγκατασταθεί στον ίδιο κόμβο. Αυτή η επιλογή κάνει πιο εύκολη τη διαχείριση της συλλογής και της ανάλυσης των δεδομένων.

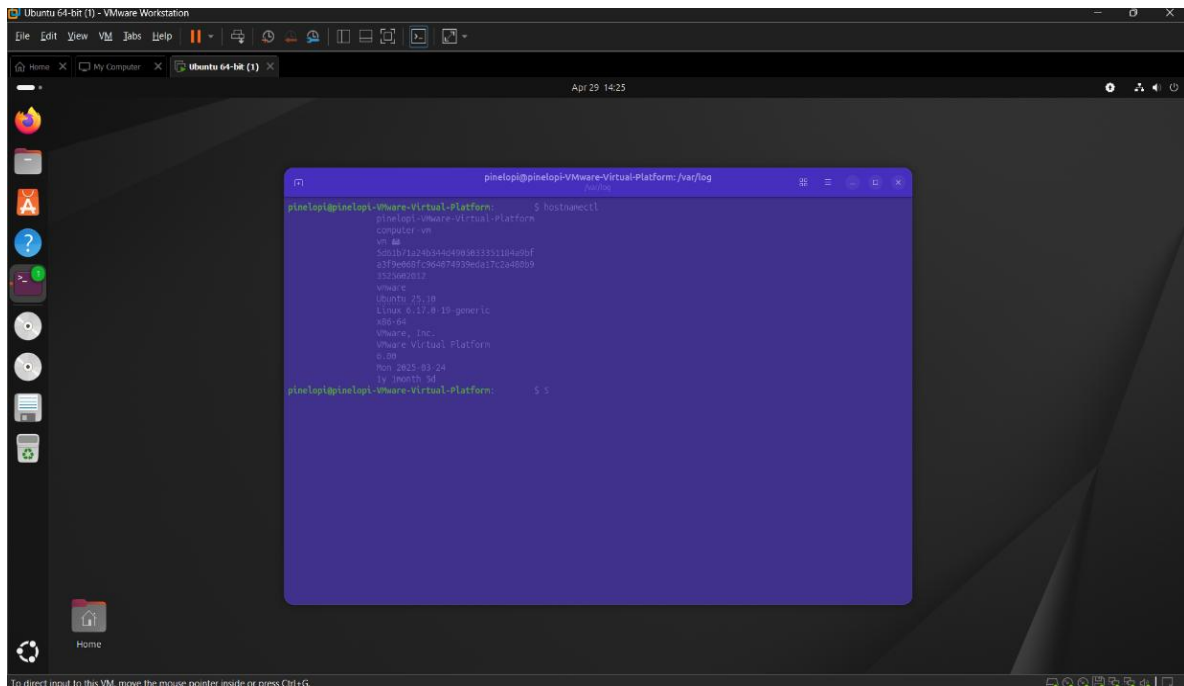
Αρχικά παρουσιάζεται αναλυτικά η διαδικασία της εγκατάστασης των βασικών μερών η οποία ρυθμίζει όλες τις απαραίτητες παραμέτρους. Έπειτα ακολουθεί ο έλεγχος ότι οι υπηρεσίες λειτουργούν σωστά ορθά και επιβεβαιώνεται η ανταπόκριση τους. Τέλος θα δοθεί έμφαση στην ασφάλεια του συστήματος, με την οποία στοχεύεται η προστασία των δεδομένων.

3.4.1 Διαδικασία εγκατάστασης

Η παρούσα υποενότητα έχει δημιουργηθεί με στόχο την περιγραφή της διαδικασίας εγκατάστασης της πλατφόρμας Wazuh στον κεντρικό εξυπηρετητή της υποδομής. Η εγκατάσταση δεν αναφέρεται μόνο σε απλές εκτελέσεις εντολών αλλά ως διαμόρφωση πλήρους συστήματος στο οποίο μπορούν να λειτουργούν συντονισμένα τα υποσυστήματα της πλατφόρμας. Για τον λόγο αυτό θα αναφερθεί τόσο η λογική της εγκατάστασης όσο και το είδος των στοιχείων που προέκυψαν από αυτή.

3.4.1.1 Σκοπός της εγκατάστασης

Η εγκατάσταση της πλατφόρμας πραγματοποιήθηκε στην εικονική μηχανή Ubuntu η οποία λειτούργησε ως κεντρικός εξυπηρετητής. Επιλέχθηκε η μορφή αυτή καθώς η λογική της πλατφόρμας είναι τα κύρια στοιχεία να λειτουργούν ενιαία και η διαχείριση τους να γίνεται μέσα από έναν κόμβο. Τα υποσυστήματα του Wazuh εγκαθίστανται στο ίδιο λειτουργικό περιβάλλον. Στην παρούσα υλοποίηση αυτή η μορφή επιτρέπει μια πλήρη αλλά και απλοποιημένη μορφή κατάλληλη για πειραματική χρήση ακολουθώντας πάντα τα πραγματικά πρότυπα.



Σχήμα 3.9: Εικονική μηχανή Ubuntu που φιλοξενεί τον εξυπηρετητή Wazuh

3.4.1.2 Προετοιμασία του περιβάλλοντος εγκατάστασης

Πριν την εγκατάσταση της πλατφόρμας έπρεπε να προετοιμαστεί κατάλληλα το λειτουργικό περιβάλλον της εικονικής μηχανής Ubuntu VM, ώστε να διασφαλιστεί η σταθερή και πλήρως ενημερωμένη βάση. Είναι ένα πολύ σημαντικό στάδιο για την εξασφάλιση της σταθερότητας. Αρχικά όλες οι εργασίες έγιναν με δικαίωμα διαχειριστή μέσω της εντολής `sudo` καθώς το Wazuh απαιτεί παρεμβάσεις στο σύστημα. Η ενημέρωση της λίστας του συστήματος με τις τελευταίες εκδόσεις των προγραμμάτων έγινε με την εντολή:

```
Sudo apt update
```

Στη συνέχεια έγινε η εγκατάσταση εργαλείων για την ασφαλή λήψη αρχείων και την επαλήθευση της ταυτότητας του λογισμικού:

```
sudo apt -y install curl ca-certificates gnupg
```

Τέλος πραγματοποιήθηκε έλεγχος των πόρων της μηχανής.

Ο ελεύθερος χώρος του σκληρού δίσκου με την εντολή:

```
df -h
```

και η διαθέσιμη μνήμη RAM τη δεδομένη στιγμή με την εντολή:

```
free -h
```

3.4.1.3 Εκτέλεση της εγκατάστασης

Η εγκατάσταση της πλατφόρμας πραγματοποιήθηκε από το επίσημο installer script του Wazuh. Για την έναρξη της εγκατάστασης χρησιμοποιήθηκε η εντολή:

```
curl -sO https://packages.wazuh.com/4.14/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

Η εντολή αυτή επιτρέπει αυτόματα την εγκατάσταση των κεντρικών υποσυστημάτων του Wazuh σε μια μηχανή. Μετά την ολοκλήρωση της εγκατάστασης ο έλεγχος για την επιβεβαίωση της ορθής

εγκατάστασης του λογισμικού αλλά και των υπηρεσιών του έγιναν με εντολές όπως φαίνεται στο παρακάτω σχήμα.

```

pinelopi@pinelopi-VMware-Virtual-Platform: /var/log
pinelopi@pinelopi-VMware-Virtual-Platform: /var/log$ dpkg -l | egrep -i 'wazuh|filebeat' | head -n 50
ii filebeat                                7.10.2-2                                amd64                                Filebeat sends log file
s to Logstash or directly to Elasticsearch.
ii wazuh-dashboard                        4.14.3-1                                amd64                                Wazuh dashboard is a us
er interface and visualization tool for security-related data. This Wazuh central component enables exploring, visualizing, and a
nalyzing the stored security alerts generated by the Wazuh server. Wazuh dashboard enables inspecting the status and managing the
configurations of the Wazuh cluster and agents as well as creating and managing users and roles. In addition, it allows testing
the ruleset and making calls to the Wazuh API. Documentation can be found at https://documentation.wazuh.com/current/getting-star
ted/components/wazuh-dashboard.html
ii wazuh-indexer                          4.14.3-1                                amd64                                Wazuh indexer is a near
real-time full-text search and analytics engine that gathers security-related data into one platform.
ii wazuh-manager                          4.14.3-1                                amd64                                Wazuh manager
pinelopi@pinelopi-VMware-Virtual-Platform: /var/log$ sudo systemctl list-unit-files | egrep 'wazuh|filebeat' | head -n 50
[sudo: authenticate] Password:
filebeat.service                          enabled      enabled
wazuh-dashboard.service                  enabled      enabled
wazuh-indexer-performance-analyzer.service disabled     enabled
wazuh-indexer.service                   enabled      enabled
wazuh-manager.service                   enabled      enabled
pinelopi@pinelopi-VMware-Virtual-Platform: /var/log$ s

```

Σχήμα 3.10: Εντολές επαλήθευσης της εγκατάστασης του Wazuh

Η πρώτη εντολή επιβεβαιώνει ότι τα πακέτα του Wazuh υπάρχουν στη λίστα των προγραμμάτων που είναι εγκατεστημένα στη μηχανή Ubuntu. Η δεύτερη έχει ως στόχο την επιβεβαίωση ότι οι υπηρεσίες έχουν δημιουργηθεί και η ρύθμιση τους για εκκίνηση γίνεται αυτόματα.

3.4.1.4 Υπηρεσίες και βασικά αρχεία εγκατάστασης

Μετά την ολοκλήρωση της διαδικασίας εγκατάστασης, η πλατφόρμα Wazuh λειτουργεί ως το σύνολο των διαφορετικών υπηρεσιών και των αρχείων ρυθμίσεων που συνεργάζονται μεταξύ τους. Στο περιβάλλον του Ubuntu είναι σημαντικό να κατανοηθεί ότι οι λειτουργίες αυτές εκτελούνται στο παρασκήνιο. Με άλλα λόγια ο server τρέχει μόνιμα τις υπηρεσίες αυτές, χωρίς να χρειάζεται η παρέμβαση του χρήστη.

Σημαντική είναι η αναφορά στο κατάλογο `/var/ossec/` ο οποίος αποτελεί πολύ σημαντικό στοιχείο. Η ύπαρξη του επιβεβαιώνει ότι κατά την εγκατάσταση έχουν δημιουργηθεί όλοι οι απαραίτητοι υποκατάλογοι που χρειάζεται ο Wazuh Manager για να λειτουργήσει. Η εντολή ελέγχου του είναι:

```
ls -la /var/ossec/
```

Το αρχείο `wazuh.yml` ανήκει στο κατάλογο ρυθμίσεων του Dashboard. Το αρχείο θεωρείται απαραίτητο καθώς περιέχει τις ρυθμίσεις για την επικοινωνία του πίνακα ελέγχου με τη διεπαφή προγραμματισμού εφαρμογών (Application Programming Interface-API), ένα μέρος του manager δηλαδή που επιτρέπει στα διάφορα κομμάτια της πλατφόρμας να επικοινωνούν μεταξύ τους.

```

pinelopi@pinelopi-VMware-Virtual-Platform: /var/log
/var/log
pinelopi@pinelopi-VMware-Virtual-Platform:/var/log$ sudo ls -la /usr/share/wazuh-dashboard/data/wazuh/config/ 2>/dev/null
[sudo: authenticate] Password:
total 16
drwxr-xr-x 2 wazuh-dashboard wazuh-dashboard 4096 Mar 30 00:54 .
drwxr-xr-x 4 wazuh-dashboard wazuh-dashboard 4096 Feb 27 00:36 ..
-rw-r--r-- 1 wazuh-dashboard wazuh-dashboard 8153 Mar 30 00:54 wazuh.yml
pinelopi@pinelopi-VMware-Virtual-Platform:/var/log$ s

```

Σχήμα 3.11: Απεικόνιση του καταλόγου ρυθμίσεων του Wazuh dashboard

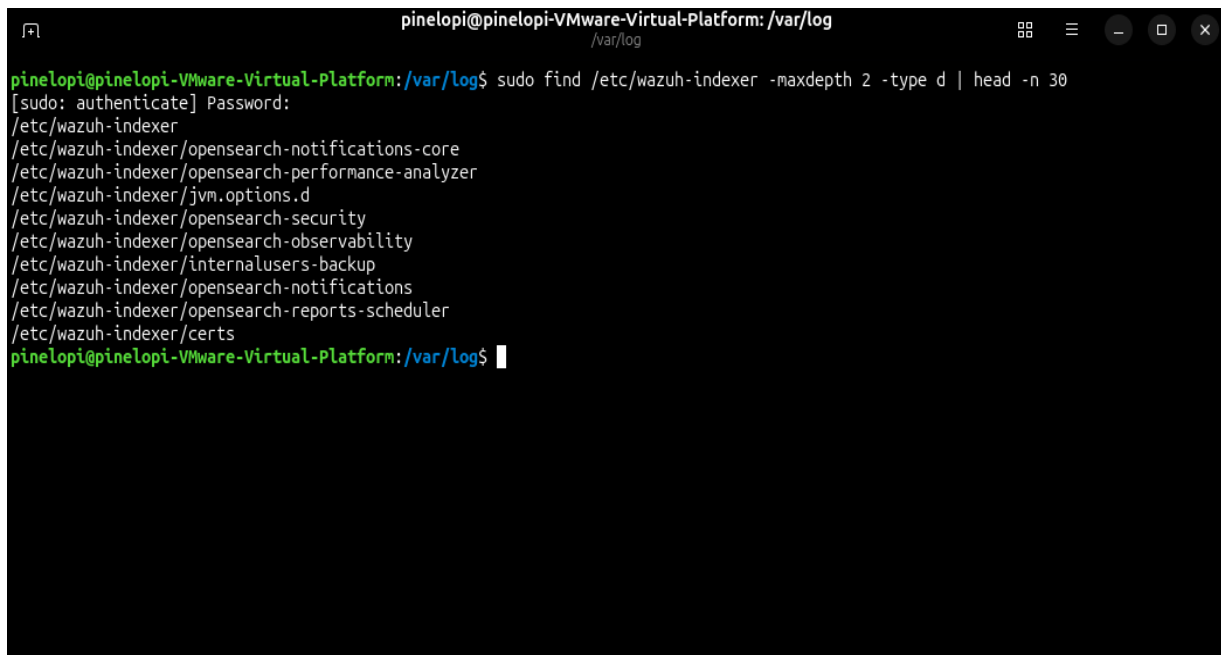
3.4.1.5 Αρχικοποίηση της πρόσβασης και διαπιστευτήρια

Το επόμενο κρίσιμο βήμα μετά το πέρας της εγκατάστασης είναι η διαχείριση της πρόσβασης στην πλατφόρμα. Είναι προφανές ότι σε ένα τέτοιο σύνθετο περιβάλλον δεν αρκεί μόνο ένας κωδικός πρόσβασης για όλες τις λειτουργίες. Για τον λόγο αυτό υπάρχουν διαφορετικά επίπεδα διαπιστευτηρίων από τα οποία καθένα εξυπηρετεί συγκεκριμένο σκοπό.

Συγκεκριμένα το διαπιστευτήριο εισόδου στον πίνακα ελέγχου αναφέρεται στους κωδικούς που θα χρησιμοποιήσει ο χρήστης για να συνδεθεί στο γραφικό περιβάλλον της πλατφόρμας. Επίσης υπάρχουν οι εσωτερικοί χρήστες `indexer`, όπου οι κωδικοί τους αφορούν την εσωτερική επικοινωνία του συστήματος με τον μηχανισμό αποθήκευσης και αναζήτησης. Τέλος τα διαπιστευτήρια API χρησιμοποιούνται για την επικοινωνία του πίνακα ελέγχου με τη διεπαφή του Wazuh manager για την ανταλλαγή δεδομένων και τις λειτουργίες διαχείρισης.

Σε τυπικές εγκαταστάσεις, οι αρχικοί κωδικοί περιέχονται σε ένα αρχείο που δημιουργείται κατά την εγκατάσταση. Όπως θα αναφερθούμε σε επόμενη υποενότητα, στην συγκεκριμένη εργασία, χρησιμοποιήθηκαν είτε επίσημα εργαλεία της πλατφόρμας για επανακαθορισμό κωδικών όπου ήταν εφικτό είτε χειροκίνητη ενημέρωση των σχετικών αρχείων ρυθμίσεων. Είναι μια πολύ σημαντική παράμετρος καθώς η εγκατάσταση δεν θεωρείται ολοκληρωμένη χωρίς τη διασφάλιση της σωστής επικοινωνίας μέσω των κατάλληλων διαπιστευτηρίων.

Τέλος πραγματοποιήθηκε επιβεβαιωτικός έλεγχος των δομών ασφάλειας του Wazuh Indexer. Ο έλεγχος των βασικών καταλόγων ρυθμίσεων που σχετίζονται με την ασφάλεια έγινε με την επιβεβαίωση της ύπαρξης του καταλόγου `/etc/wazuh-indexer/opensearch-security` ο οποίος σχετίζεται με τα βασικά στοιχεία ελέγχου πρόσβασης και τον κατάλογο `/etc/wazuh-indexer/certs` που αφορά τα πιστοποιητικά για την κρυπτογραφημένη επικοινωνία.



```

pinelopi@pinelopi-VMware-Virtual-Platform: /var/log
[sudo: authenticate] Password:
pinelopi@pinelopi-VMware-Virtual-Platform:/var/log$ sudo find /etc/wazuh-indexer -maxdepth 2 -type d | head -n 30
/etc/wazuh-indexer
/etc/wazuh-indexer/opensearch-notifications-core
/etc/wazuh-indexer/opensearch-performance-analyzer
/etc/wazuh-indexer/jvm.options.d
/etc/wazuh-indexer/opensearch-security
/etc/wazuh-indexer/opensearch-observability
/etc/wazuh-indexer/internalusers-backup
/etc/wazuh-indexer/opensearch-notifications
/etc/wazuh-indexer/opensearch-reports-scheduler
/etc/wazuh-indexer/certs
pinelopi@pinelopi-VMware-Virtual-Platform:/var/log$

```

Σχήμα 3.12: Έλεγχος δομής καταλόγων του Wazuh Indexer

3.4.2 Έλεγχος ορθής λειτουργίας

Μετά την ολοκλήρωση της εγκατάστασης, έπρεπε να εκτελεστούν έλεγχοι για την επιβεβαίωση της πλήρους λειτουργικότητας. Η διαδικασία θεωρείται απαραίτητη. Δίχως αυτή η απλή εκτέλεση της εγκατάστασης δεν μας εγγυάται ότι όλα τα υποσυστήματα επικοινωνούν με ορθό τρόπο μεταξύ τους. Οι έλεγχοι επικεντρώθηκαν στην κατάσταση των υπηρεσιών, στη διαθεσιμότητα των θυρών του δικτύου και την πρόσβαση στο γραφικό περιβάλλον.

3.4.2.1 Έλεγχος εκκίνησης υπηρεσιών

Σε πρώτο στάδιο ελέγχου έπρεπε να επιβεβαιωθεί ότι οι βασικές υπηρεσίες που χρησιμοποιεί η πλατφόρμα έχουν εκκινηθεί σωστά. Σε περιβάλλον Linux ο έλεγχος αυτός πραγματοποιείται μέσω του system, συγκεκριμένα με τη χρήση της εντολής systemctl, η οποία ελέγχει αν η σύνδεση είναι ενεργή ή αν παρουσιάζει σφάλμα καθώς και βασικές πληροφορίες για τυχόν σφάλματα.

Σκοπός ήταν οι υπηρεσίες που βασίζονται στα βασικά υποσυστήματα να ελεγχθούν. Η ορθή λειτουργία του indexer, του manager και του dashboard είναι απαραίτητη για την συνολική λειτουργία της πλατφόρμας. Οι εντολές και ο έλεγχος που πραγματοποιήθηκε φαίνονται στις τρεις παρακάτω εικόνες. Η ένδειξη Active: active (running) μας επιβεβαιώνει ότι έχει γίνει εκκίνηση και εκτελείται στο σύστημα.

```

pinelopi@pinelopi-VMware-Virtual-Platform: /var/log
/var/log

pinelopi@pinelopi-VMware-Virtual-Platform: /var/log$ sudo systemctl status wazuh-indexer --no-pager -l
[sudo: authenticate] Password:
● wazuh-indexer.service - wazuh-indexer
   Loaded: loaded (/usr/lib/systemd/system/wazuh-indexer.service; enabled; preset: enabled)
   Active: active (running) since Tue 2026-05-26 12:20:00 EEST; 24min ago
   Invocation: 13af1c58724d4947bcff915c99748d5e
   Docs: https://documentation.wazuh.com
   Main PID: 1795 (java)
     Tasks: 83 (limit: 7548)
    Memory: 1.5G (peak: 1.6G)
       CPU: 3min 24.085s
    CGroup: /system.slice/wazuh-indexer.service
            └─1795 /usr/share/wazuh-indexer/jdk/bin/java -Xshare:auto -Dopensearch.networkaddress.cache.ttl=60 -Dopensearch.networkaddress.cache.negative.ttl=10 -XX:+AlwaysPreTouch -Xss1m -Djava.awt.headless=true -Dfile.encoding=UTF-8 -Djna.nosys=true -XX:-OmitStackTraceInFastThrow -XX:+ShowCodeDetailsInExceptionMessages -Dio.netty.noUnsafe=true -Dio.netty.noKeySetOptimization=true -Dio.netty.recycler.maxCapacityPerThread=0 -Dio.netty allocator.numDirectArenas=0 -Dlog4j.shutdownHookEnabled=false -Dlog4j2.disable.jmx=true -Djava.security.manager=allow -Djava.locale.providers=SPI,COMPAT -Xms1024m -Xmx1024m -XX:+UseG1GC -XX:G1ReservePercent=25 -XX:InitiatingHeapOccupancyPercent=30 -Djava.io.tmpdir=/tmp/opensearch-2871680108152493110 -XX:+HeapDumpOnOutOfMemoryError -XX:HeapDumpPath=/var/lib/wazuh-indexer -XX:ErrorFile=/var/log/wazuh-indexer/hs_err_pid%p.log "-Xlog:gc*,gc+age=trace,safepoint:file=/var/log/wazuh-indexer/gc.log:utctime,pid,tags:filecount=32,filesize=64m" -Djava.security.manager=allow --add-modules=jdk.incubator.vector -Djava.util.concurrent.ForkJoinPool.common.threadFactory=org.opensearch.secure_sm.SecuredForkJoinWorkerThreadFactory -Dclk.tck=100 -Djdk.attach.allowAttachSelf=true -Djava.security.policy=file:///etc/wazuh-indexer/opensearch-performance-analyzer/opensearch_security.policy --add-opens=jdk.attach/sun.tools.attach=ALL-UNNAMED -XX:MaxDirectMemorySize=536870912 -Dopensearch.path.home=/usr/share/wazuh-indexer -Dopensearch.path.conf=/etc/wazuh-indexer -Dopensearch.distribution.type=deb -Dopensearch.bundled_jdk=true -cp /usr/share/wazuh-indexer/lib/* org.opensearch.bootstrap.OpenSearch -p /run/wazuh-indexer/wazuh-indexer.pid --quiet

May 26 12:18:58 pinelopi-VMware-Virtual-Platform systemd-entrypoint[1795]: WARNING: System::setSecurityManager has been called by org.opensearch.bootstrap.OpenSearch (file:/usr/share/wazuh-indexer/lib/opensearch-2.19.4.jar)
May 26 12:18:58 pinelopi-VMware-Virtual-Platform systemd-entrypoint[1795]: WARNING: Please consider reporting this to the maintainers of org.opensearch.bootstrap.OpenSearch
May 26 12:18:58 pinelopi-VMware-Virtual-Platform systemd-entrypoint[1795]: WARNING: System::setSecurityManager will be removed in a future release
May 26 12:19:07 pinelopi-VMware-Virtual-Platform systemd-entrypoint[1795]: May 26, 2026 12:19:06 PM sun.util.locale.provider.LocaleProviderAdapter <clinit>
May 26 12:19:07 pinelopi-VMware-Virtual-Platform systemd-entrypoint[1795]: WARNING: COMPAT locale provider will be removed in a future release
May 26 12:19:13 pinelopi-VMware-Virtual-Platform systemd-entrypoint[1795]: WARNING: A terminally deprecated method in java.lang.System has been called
May 26 12:19:13 pinelopi-VMware-Virtual-Platform systemd-entrypoint[1795]: WARNING: System::setSecurityManager has been called by org.opensearch.bootstrap.Security (file:/usr/share/wazuh-indexer/lib/opensearch-2.19.4.jar)
May 26 12:19:13 pinelopi-VMware-Virtual-Platform systemd-entrypoint[1795]: WARNING: Please consider reporting this to the maintainers of org.opensearch.bootstrap.Security
May 26 12:19:13 pinelopi-VMware-Virtual-Platform systemd-entrypoint[1795]: WARNING: System::setSecurityManager will be removed in a future release
May 26 12:20:00 pinelopi-VMware-Virtual-Platform systemd[1]: Started wazuh-indexer.service - wazuh-indexer.
pinelopi@pinelopi-VMware-Virtual-Platform: /var/log$

```

Σχήμα 3.13: Έλεγχος κατάστασης υπηρεσίας Wazuh Indexer

```

pinelopi@pinelopi-VMware-Virtual-Platform: /var/log
/var/log

pinelopi@pinelopi-VMware-Virtual-Platform: /var/log$ sudo systemctl status wazuh-dashboard --no-pager -l
[sudo: authenticate] Password:
● wazuh-dashboard.service - wazuh-dashboard
   Loaded: loaded (/etc/systemd/system/wazuh-dashboard.service; enabled; preset: enabled)
   Active: active (running) since Tue 2026-05-26 12:18:18 EEST; 31min ago
   Invocation: e859084b89de47a6aa4db31f51c95f75
   Main PID: 1430 (node)
     Tasks: 11 (limit: 7548)
    Memory: 277.1M (peak: 449.8M)
       CPU: 32.063s
    CGroup: /system.slice/wazuh-dashboard.service
            └─1430 /usr/share/wazuh-dashboard/node/bin/node --no-warnings --max-http-header-size=65536 --unhandled-rejections=warn /usr/share/wazuh-dashboard/src/cli/dist

May 26 12:20:39 pinelopi-VMware-Virtual-Platform opensearch-dashboards[1430]: {"type":"log","@timestamp":"2026-05-26T09:20:39Z","tags":["info","plugins","wazuh","cron-scheduler"],"pid":1430,"message":"Updated the wazuh-statistics template"}
May 26 12:20:39 pinelopi-VMware-Virtual-Platform opensearch-dashboards[1430]: {"type":"log","@timestamp":"2026-05-26T09:20:39Z","tags":["info","plugins","wazuh","monitoring"],"pid":1430,"message":"Updated the wazuh-agent template"}
May 26 12:20:40 pinelopi-VMware-Virtual-Platform opensearch-dashboards[1430]: {"type":"log","@timestamp":"2026-05-26T09:20:40Z","tags":["listening","info"],"pid":1430,"message":"Server running at https://0.0.0.0:443"}
May 26 12:20:41 pinelopi-VMware-Virtual-Platform opensearch-dashboards[1430]: {"type":"log","@timestamp":"2026-05-26T09:20:41Z","tags":["info","http","server","OpenSearchDashboards"],"pid":1430,"message":"http server running at https://0.0.0.0:443"}
May 26 12:20:41 pinelopi-VMware-Virtual-Platform opensearch-dashboards[1430]: {"type":"log","@timestamp":"2026-05-26T09:20:41Z","tags":["info","plugins","wazuh","monitoring"],"pid":1430,"message":"Settings added to wazuh-monitoring-2026.22w index"}
May 26 12:20:41 pinelopi-VMware-Virtual-Platform opensearch-dashboards[1430]: {"type":"log","@timestamp":"2026-05-26T09:20:41Z","tags":["info","plugins","wazuh","monitoring"],"pid":1430,"message":"Bulk data to index wazuh-monitoring-2026.22w for 1 agents completed"}
May 26 12:30:00 pinelopi-VMware-Virtual-Platform opensearch-dashboards[1430]: {"type":"log","@timestamp":"2026-05-26T09:30:00Z","tags":["info","plugins","wazuh","monitoring"],"pid":1430,"message":"Settings added to wazuh-monitoring-2026.22w index"}
May 26 12:30:00 pinelopi-VMware-Virtual-Platform opensearch-dashboards[1430]: {"type":"log","@timestamp":"2026-05-26T09:30:00Z","tags":["info","plugins","wazuh","monitoring"],"pid":1430,"message":"Bulk data to index wazuh-monitoring-2026.22w for 1 agents completed"}
May 26 12:45:00 pinelopi-VMware-Virtual-Platform opensearch-dashboards[1430]: {"type":"log","@timestamp":"2026-05-26T09:45:00Z","tags":["info","plugins","wazuh","monitoring"],"pid":1430,"message":"Settings added to wazuh-monitoring-2026.22w index"}
May 26 12:45:00 pinelopi-VMware-Virtual-Platform opensearch-dashboards[1430]: {"type":"log","@timestamp":"2026-05-26T09:45:00Z","tags":["info","plugins","wazuh","monitoring"],"pid":1430,"message":"Bulk data to index wazuh-monitoring-2026.22w for 1 agents completed"}
pinelopi@pinelopi-VMware-Virtual-Platform: /var/log$

```

Σχήμα 3.14: Έλεγχος κατάστασης υπηρεσίας Wazuh Dashboard

```

pinelopi@pinelopi-VMware-Virtual-Platform: /var/log
[sudo: authenticate] Password:
● wazuh-manager.service - Wazuh manager
   Loaded: loaded (/usr/lib/systemd/system/wazuh-manager.service; enabled; preset: enabled)
   Active: active (running) since Tue 2026-05-26 12:20:09 EEST; 31min ago
   Invocation: efc42ddcd8341749dcbce944655db64
     Tasks: 211 (limit: 7540)
    Memory: 1.7G (peak: 1.9G)
       CPU: 18min 35.112s
   CGroup: /system.slice/wazuh-manager.service
           └─3226 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
             └─3241 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
               └─3243 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
                 └─3253 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
                   └─3256 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh_apid.py
                     └─3730 /var/ossec/bin/wazuh-authd
                       └─4261 /var/ossec/bin/wazuh-db
                         └─4296 /var/ossec/bin/wazuh-execd
                           └─4314 /var/ossec/bin/wazuh-analysisd
                             └─4357 /var/ossec/bin/wazuh-syscheckd
                               └─4376 /var/ossec/bin/wazuh-remoted
                                 └─4444 /var/ossec/bin/wazuh-logcollector
                                   └─4465 /var/ossec/bin/wazuh-monitord
                                     └─4487 /var/ossec/bin/wazuh-modulesd

May 26 12:20:01 pinelopi-VMware-Virtual-Platform env[4165]: Started wazuh-syscheckd...
May 26 12:20:03 pinelopi-VMware-Virtual-Platform env[4165]: Started wazuh-remoted...
May 26 12:20:04 pinelopi-VMware-Virtual-Platform env[4165]: Started wazuh-logcollector...
May 26 12:20:05 pinelopi-VMware-Virtual-Platform env[4165]: Started wazuh-monitord...
May 26 12:20:05 pinelopi-VMware-Virtual-Platform env[4484]: 2026/05/26 12:20:05 wazuh-modulesd:router: INFO: Loaded router module.
May 26 12:20:05 pinelopi-VMware-Virtual-Platform env[4484]: 2026/05/26 12:20:05 wazuh-modulesd:content_manager: INFO: Loaded content_manager module.
May 26 12:20:05 pinelopi-VMware-Virtual-Platform env[4484]: 2026/05/26 12:20:05 wazuh-modulesd:inventory-harvester: INFO: Loaded Inventory harvester module.
May 26 12:20:07 pinelopi-VMware-Virtual-Platform env[4165]: Started wazuh-modulesd...
May 26 12:20:09 pinelopi-VMware-Virtual-Platform env[4165]: Completed.
May 26 12:20:09 pinelopi-VMware-Virtual-Platform systemd[1]: Started wazuh-manager.service - Wazuh manager.
pinelopi@pinelopi-VMware-Virtual-Platform: /var/log$

```

Σχήμα 3.15: Έλεγχος κατάστασης υπηρεσίας Wazuh Manager

3.4.2.2 Έλεγχος διαθεσιμότητας θυρών

Στη συνέχεια έπρεπε να εκτελεστεί και ο έλεγχος των θυρών στις οποίες οι αντίστοιχες διεργασίες ήταν διαθέσιμες. Μια υπηρεσία μπορεί να εμφανίζεται ενεργή αλλά να μην είναι διαθέσιμη δικτυακά ή και να μην ακούει στην αναμενόμενη θύρα.

Η εντολή ss εμφανίζει όπως φαίνεται και στο Σχήμα 3.16, τις ενεργές δικτυακές συνδέσεις και τις θύρες που ακούν οι υπηρεσίες. Ο έλεγχος πραγματοποιήθηκε στις βασικές θύρες που σχετίζονται με τη λειτουργία του Wazuh όπως η θύρα του API, η θύρα πρόσβασης στο dashboard και οι θύρες επικοινωνίας με τον agent.

```

pinelopi@pinelopi-VMware-Virtual-Platform: /var/log
[sudo: authenticate] Password:
pinelopi@pinelopi-VMware-Virtual-Platform: /var/log$ sudo ss -tulnp | egrep '55000|443|1514|1515'
[::]:55000 [::]:* users:(("python3",pid=3226,fd=46))
tcp LISTEN 0 2048 0.0.0.0:55000 0.0.0.0:* users:(("python3",pid=3226,fd=44))
tcp LISTEN 0 128 0.0.0.0:1515 0.0.0.0:* users:(("wazuh-authd",pid=3730,fd=6))
tcp LISTEN 0 128 0.0.0.0:1514 0.0.0.0:* users:(("wazuh-remoted",pid=4376,fd=4))
tcp LISTEN 0 511 0.0.0.0:443 0.0.0.0:* users:(("node",pid=1430,fd=19))
tcp LISTEN 0 2048 [::]:55000 [::]:* users:(("python3",pid=3226,fd=46))
pinelopi@pinelopi-VMware-Virtual-Platform: /var/log$

```

Σχήμα 3.16: Έλεγχος διαθέσιμων θυρών των βασικών υπηρεσιών του Wazuh

3.4.2.3 Έλεγχος απόκρισης του Wazuh API

Στη συνέχεια έγινε ένας πρώτος έλεγχος αν το API του Wazuh λειτουργεί ορθά. Αποτελεί ένα από τα σημαντικότερα σημεία καθώς η λειτουργία του επιτρέπει στα διάφορα μέρη του συστήματος να ανταλλάσσουν πληροφορίες και να εκτελούν εργασίες στον κεντρικό εξυπηρετητή. Για τον αρχικό έλεγχο χρησιμοποιήθηκε η εντολή:

```
curl -k https://127.0.0.1:55000/ ; echo
```

Σε αυτό το στάδιο θέλαμε να επιβεβαιώσουμε ότι υπάρχει η υπηρεσία και όχι η πλήρης σύνδεση. Ακόμα και η εμφάνιση απάντησης μη εξουσιοδοτημένης πρόσβασης θεωρείται επιτυχία καθώς το API είναι ενεργό και ανταποκρίνεται στα αιτήματα. Η παράμετρος -k στην εντολή χρησιμοποιήθηκε ώστε η εντολή να προχωρήσει ακόμα και αν το πιστοποιητικό ασφαλείας είναι αυτό υπογεγραμμένο, κάτι που είναι αναμενόμενο σε δοκιμαστικά περιβάλλοντα.

3.4.2.4 Πρόσβαση στο Wazuh Dashboard

Τελευταίο στάδιο των αρχικών ελέγχων αποτέλεσε η πρόσβαση στον πίνακα ελέγχου. Στην ουσία αναφερόμαστε στο γραφικό περιβάλλον που φιλοξενεί την πλατφόρμα. Σε αυτό ο αναλυτής έχει τη δυνατότητα να παρακολουθεί τις ειδοποιήσεις ασφαλείας, να αναζητά τα δεδομένα και να διαχειρίζεται όλα τα στοιχεία που αφορούν την εγκατάσταση σε ένα κεντρικό σημείο.

Η σύνδεση πραγματοποιήθηκε μέσω προγράμματος περιήγησης. Η επιτυχής φόρτωση της σελίδας εισόδου επιβεβαιώνει ότι το περιβάλλον είναι λειτουργικό. Η είσοδος στο σύστημα ήταν το πρώτο βήμα που απέδειξε ότι ο εξυπηρετητής είναι έτοιμος να δεχτεί παραμετροποίηση σύμφωνα με τις ανάγκες της υλοποίησης και έχει τη δυνατότητα να προβάλλει πληροφορίες για την κατάσταση της ασφάλειας της υποδομής.

Για την πρόσβαση μέσω προγράμματος περιήγησης χρησιμοποιήθηκε το ασφαλές πρωτόκολλο μεταφοράς υπερκειμένου (HTTPS). Το συγκεκριμένο μας εξασφαλίζει την κρυπτογραφημένη επικοινωνία και προστατεύει τα διαπιστευτήρια από υποκλοπές. Παρόλο που το πρόγραμμα περιήγησης εμφάνισε προειδοποίηση η οποία αφορά χρήση αυτό-υπογεγραμμένων πιστοποιητικών (self-signed certificates), η λειτουργία δεν επηρεάζεται και είναι αναμενόμενο σε ένα εργαστηριακό περιβάλλον.

3.4.3 Έλεγχος πρόσβασης και ασφαλούς επικοινωνίας υπηρεσιών

Αφού επιβεβαιώθηκε η βασική λειτουργία της πλατφόρμας, έπρεπε να εξεταστεί η διαχείριση της πρόσβασης και των διαπιστευτηρίων. Παρόλο που δεν θεωρείται διαδικασία εγκατάστασης, είναι πολύ σημαντικό να παρουσιαστεί, καθώς η ασφάλεια πρόσβασης στα επιμέρους στοιχεία της πλατφόρμας αποτελεί ένα από τα πιο σημαντικά βήματα.

Σε ένα σύστημα ανοιχτού κώδικα SIEM, η διαχείριση των διαπιστευτηρίων χρήζει μεγάλης σημασίας, ιδιαίτερα στην περίπτωση μας, όπου όλη η σημαντική πληροφορία των δεδομένων συγκεντρώνεται και επεξεργάζεται σε ένα σημείο. Για αυτό τον λόγο, θα εξεταστεί ο διαχωρισμός των επιπέδων πρόσβασης, η διαχείριση κωδικών, η ρύθμιση της επικοινωνίας του πίνακα ελέγχου με τη διεπαφή και ο μηχανισμός αυθεντικοποίησης μέσω διακριτικών πρόσβασης (token).

3.4.3.1 Διαχωρισμός επιπέδων πρόσβασης

Η πλατφόρμα του Wazuh βασίζει την ασφάλεια της στον διαχωρισμό των λογαριασμών πρόσβασης ανάλογα με τη λειτουργία που εκτελούν. Για να μην υπάρχει ένας ενιαίος λογαριασμός σε όλα τα υποσυστήματα, χρησιμοποιούνται διαφορετικά επίπεδα πρόσβασης ώστε το κάθε μέρος του

συστήματος να έχει μόνο τα δικαιώματα που χρειάζεται. Η παρούσα διαμόρφωση είναι πολύ σημαντική στην ανταλλαγή δεδομένων του συγκεκριμένου συστήματος καθώς κάποιοι λογαριασμοί προορίζονται για πρόσβαση από τον χειριστή ενώ άλλοι λειτουργούν στο παρασκήνιο για εσωτερική επικοινωνία των υπηρεσιών.

Πίνακας 3.2: Επίπεδα πρόσβασης στην πλατφόρμα Wazuh

A/A	Επίπεδο Πρόσβασης	Ενδεικτικός Χρήστης	Ρόλος
1	Είσοδος στο dashboard	Admin	Πρόσβαση στο γραφικό περιβάλλον
2	Εσωτερικός χρήστης indexer	kibanaserver	Σύνδεση dashboard με indexer
3	Χρήστης wazuh API	Wazuh-wui	Επικοινωνία dashboard με API

Αυτός ο διαχωρισμός έχει ως στόχο την ανάδειξη του πίνακα ελέγχου ως ενδιάμεσου κόμβου επικοινωνίας και όχι ως μια σελίδα εισόδου. Για την ορθή λειτουργία της πλατφόρμας πρέπει όλοι οι λογαριασμοί να είναι ορθά ρυθμισμένοι. Αν έστω και ένας κωδικός είναι λάθος, η επικοινωνία που υπάρχει μεταξύ των υποσυστημάτων διακόπτεται και το περιβάλλον παύει να εμφανίζει τις απαραίτητες πληροφορίες ασφαλείας.

3.4.3.2 Διαχείριση κωδικών και πολιτική ισχυρών διαπιστευτηρίων

Κρίσιμο παράγοντα της λειτουργίας της πλατφόρμας Wazuh αποτελεί η ορθή διαχείριση των κωδικών πρόσβασης. Η διαδικασία αυτή είναι απαραίτητη τόσο κατά την αρχική εγκατάσταση όσο και σε περιπτώσεις ανανέωσης των στοιχείων μετέπειτα. Η παρούσα υλοποίηση, δεν βασίστηκε μόνο στο αρχείο διαπιστευτηρίων του installer. Αντίθετα χρησιμοποιήθηκαν τα επίσημα αρχεία για επανακαθορισμό κωδικών και ενημερώθηκαν χειροκίνητα οι ρυθμίσεις για να διασφαλιστεί η συμβατότητα μεταξύ των υποσυστημάτων.

Μετά από οποιαδήποτε αλλαγή κωδικού θεωρείται απαραίτητο ότι πρέπει να ενημερώνονται οι υπηρεσίες που χρησιμοποιούν τα συγκεκριμένα διαπιστευτήρια. Πιο συγκεκριμένα σε περίπτωση αλλαγής, για παράδειγμα του κωδικού πρόσβασης του API, η νέα τιμή πρέπει να μεταφέρεται και στο αρχείο ρυθμίσεων του πίνακα ελέγχου ώστε να μην διακοπεί η ροή των δεδομένων στο γραφικό περιβάλλον. Σε κάποιες περιπτώσεις ενδέχεται να χρειαστεί επανεκκίνηση των σχετικών υπηρεσιών για να αναγνωριστούν από το σύστημα οι νέες ρυθμίσεις και να επανέλθει η ορθή λειτουργία.

Παράλληλα η πλατφόρμα παρέχει αυστηρούς κανόνες στη χρήση κωδικών. Αδύναμοι κωδικοί που μπορούν να παραβιαστούν εύκολα δεν γίνονται αποδεκτοί. Η συνολική θωράκιση της εγκατάστασης ενισχύεται και με αυτό τον τρόπο διασφαλίζεται η προστατευμένη πρόσβαση. Τέλος για την τεκμηρίωση αυτών των ενεργειών θα παρουσιαστούν αποσπάσματα από τις ρυθμίσεις του συστήματος. Οι πραγματικοί κωδικοί έχουν αποκρυφθεί για την προστασία ευαίσθητων πληροφοριών.

3.4.3.3 Ρύθμιση επικοινωνίας πίνακα ελέγχου με API

Για την επικοινωνία του πίνακα ελέγχου Wazuh με το Wazuh API, χρησιμοποιούνται κάποιοι παράμετροι οι οποίοι ορίζονται στο αρχείο ρυθμίσεων wazuh.yml. Αυτό το αρχείο περιλαμβάνει στοιχεία που είναι απαραίτητα για την συγκεκριμένη σύνδεση όπως η διεύθυνση του API, η θύρα της

επικοινωνίας, το όνομα χρήστη και ο αντίστοιχος κωδικός πρόσβασης. Η διαδρομή του αρχείου στην παρούσα υλοποίηση ήταν η εξής:

```
/usr/share/wazuh-dashboard/data/wazuh/config/wazuh.yml
```

Η ορθότητα που περιέχουν οι τιμές στο συγκεκριμένο αρχείο είναι απαραίτητη για την ομαλή λειτουργία του συστήματος. Ο πίνακας ελέγχου πρέπει να περιέχει ορθά και τα τέσσερα σημεία που προαναφέρθηκαν. Αν οι τιμές που δηλώνονται στο wazuh.yml δεν αντιστοιχούν σε πραγματικά στοιχεία πρόσβασης του API, τότε δεν θα είναι εφικτή η σωστή επικοινωνία.

Η προβολή του αρχείου μπορεί να γίνει χωρίς αποκάλυψη ευαίσθητων πληροφοριών. Συγκεκριμένα με την παρακάτω εντολή η πραγματική τιμή του κωδικού πρόσβασης αντικαθίσταται από τη λέξη KODIKOS:

```
sudo sed -n '1,120p' /usr/share/wazuh-dashboard/data/wazuh/config/wazuh.yml | sed -E 's/(password:).*\1 "<KODIKOS>"/'
```

Στο ίδιο αρχείο μπορούν να βρεθούν πρόσθετες παράμετροι λειτουργίας. Η run_as σχετίζεται με έλεγχο δικαιωμάτων μέσω API. Άρα το wazuh.yml δεν είναι ένα απλό αρχείο αποθήκευσης διαπιστευτηρίων αλλά ένα βασικό σημείο παραμετροποίησης επικοινωνίας του πίνακα ελέγχου με το API. Σε περίπτωση αδυναμίας ολοκλήρωσης των ελέγχων μέσω API ή ασυμφωνίας των παραμέτρων της σύνδεσης ο πίνακας ελέγχου θα εμφανίσει μήνυμα αποτυχίας λήψης authorization token.

3.4.3.4 Έλεγχος αυθεντικοποίησης μέσω token

Η πρόσβαση στο API δεν είναι ελεύθερη και απαιτεί ταυτοποίηση. Για να επικοινωνήσει μια εφαρμογή μαζί του πρέπει πρώτα να λάβει ένα ψηφιακό διακριτικό (authorization token). Το token λειτουργεί σαν προσωρινό πάσο της σύνδεσης. Ο χρήστης δίνει τα διαπιστευτήρια του και το σύστημα επιστρέφει το κλειδί. Έτσι για τις υπόλοιπες κινήσεις επιδεικνύεται το token αντί για τον κωδικό, κάνοντας τη διαδικασία γρήγορη και πιο ασφαλή. Για την επιβεβαίωση της λειτουργίας αυτού του μηχανισμού μπορεί να εκτελεστεί δοκιμαστικός έλεγχος με την εντολή:

```
curl -k -u 'wazuh-wui:<KODIKOS>' \
'https://127.0.0.1:55000/security/user/authenticate?raw=true'
```

Το όρισμα -u στέλνει τα στοιχεία του χρήστη. Η επιλογή raw = true ζητάει από το API να μας επιστρέψει το token σε μορφή κειμένου. Αν η διαδικασία γίνει επιτυχής, στέλνεται μια σειρά από χαρακτήρες και επιβεβαιώνει την ορθότητα των διαπιστευτηρίων και ετοιμάζεται η έκδοση του πάσο πρόσβασης.

Το token αποτελεί ευαίσθητο δεδομένο καθώς η κατοχή του δίνει πρόσβαση στο σύστημα όσο αυτό είναι ενεργό. Για λόγους ασφαλείας αναλύεται στην παρούσα μόνο η διαδικασία και δεν εμφανίζεται η πραγματική τιμή του.

3.5 Εγκατάσταση και παραμετροποίηση του πράκτορα Wazuh

Ακολουθεί η εγκατάσταση και η παραμετροποίηση του πράκτορα του Wazuh. Για τη συγκεκριμένη υλοποίηση επιλέχθηκε ο πράκτορας να εγκατασταθεί σε τερματικό σύστημα παρακολούθησης που χρησιμοποιεί Windows.

Ο Wazuh agent, όπως έχει αναφερθεί αποτελεί λογισμικό το οποίο εγκαθίσταται σε ένα τερματικό και είναι υπεύθυνο για τη συλλογή συμβάντων από το τοπικό σύστημα και την αποστολή τους στον εξυπηρετητή Wazuh. Μέσω του πράκτορα το τερματικό σύστημα εντάσσεται στην κεντρική μας

υποδομή. Έτσι γίνεται δυνατή η συλλογή των δεδομένων που αφορούν τη λειτουργία του συστήματος, τις υπηρεσίες και τα αρχεία καταγραφής.

Η ενότητα θα οργανωθεί σε τρία βασικά μέρη. Αρχικά θα παρουσιαστεί η διαδικασία εγκατάστασης του πράκτορα στο τερματικό σύστημα. Στη συνέχεια περιγράφεται η ρύθμιση και η επιβεβαίωση της επικοινωνίας με τον κεντρικό κόμβο ο οποίος λειτουργεί με την εικονική μηχανή Ubuntu. Τέλος θα αναλυθεί η χρήση του μηχανισμού συλλογής τηλεμετρίας Sysmon με στόχο την ενίσχυση ορατότητας σε επίπεδο τερματικού.

3.5.1 Διαδικασία εγκατάστασης

Ο ρόλος του πράκτορα είναι να λειτουργεί ως ενδιάμεσος μηχανισμός ανάμεσα από το τοπικό σύστημα και τον κεντρικό εξυπηρετητή. Συγκεκριμένα, συλλέγει τα δεδομένα ασφαλείας από το λειτουργικό σύστημα και να τα μεταφέρει στο κεντρικό εξυπηρετητή, ο οποίος θα τα επεξεργαστεί, θα τα συσχετίσει μεταξύ τους και στη συνέχεια θα τα αναλύσει για τυχόν απειλές.

Η διαδικασία της εγκατάστασης ακολούθησε τη λογική μια τυπικής εφαρμογής. Αρχικά έγινε λήψη του αρχείου εγκατάστασης από την επίσημη ιστοσελίδα του Wazuh και στη συνέχεια η εγκατάσταση του στο σύστημα. Η λήψη και η παραμετροποίηση συνδυάστηκαν με την εντολή:

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.14.3-1.msi -  
OutFile $env:tmp\wazuh-agent; msixec.exe /i $env:tmp\wazuh-agent /q  
WAZUH_MANAGER='192.168.49.128'
```

Εάν το αρχείο έχει ήδη ληφθεί τοπικά εκτελείται η παρακάτω εντολή:

```
.\wazuh-agent-4.14.3-1.msi /q WAZUH_MANAGER="192.168.49.128"
```

Αφού ολοκληρωθεί η διαδικασία ο πράκτορας ενσωματώνεται στο λειτουργικό σύστημα ως υπηρεσία των Windows. Αυτό είναι πολύ σημαντικό καθώς ο πράκτορας εκκινείται αυτόματα μόλις ανοίξει ο υπολογιστής και λειτουργεί συνεχόμενα στο παρασκήνιο. Η συλλογή δεδομένων δεν εξαρτάται από το εάν ο χρήστης θα ανοίξει κάποιο πρόγραμμα αλλά γίνεται μέρος της βασικής λειτουργίας του υπολογιστή. Μετά την εγκατάσταση είναι βασικό να ελέγξουμε αν η υπηρεσία είναι ενεργή όπως φαίνεται στο Σχήμα 3.17.

Σε περίπτωση που η υπηρεσία τρέχει για πρώτη φορά η χρειαστεί να γίνει επανεκκίνηση για τυχόν νέες ρυθμίσεις θα πρέπει να γίνει χρήση των εντολών:

```
Start-Service -Name "WazuhSvc"
```

```
Restart-Service -Name "WazuhSvc"
```

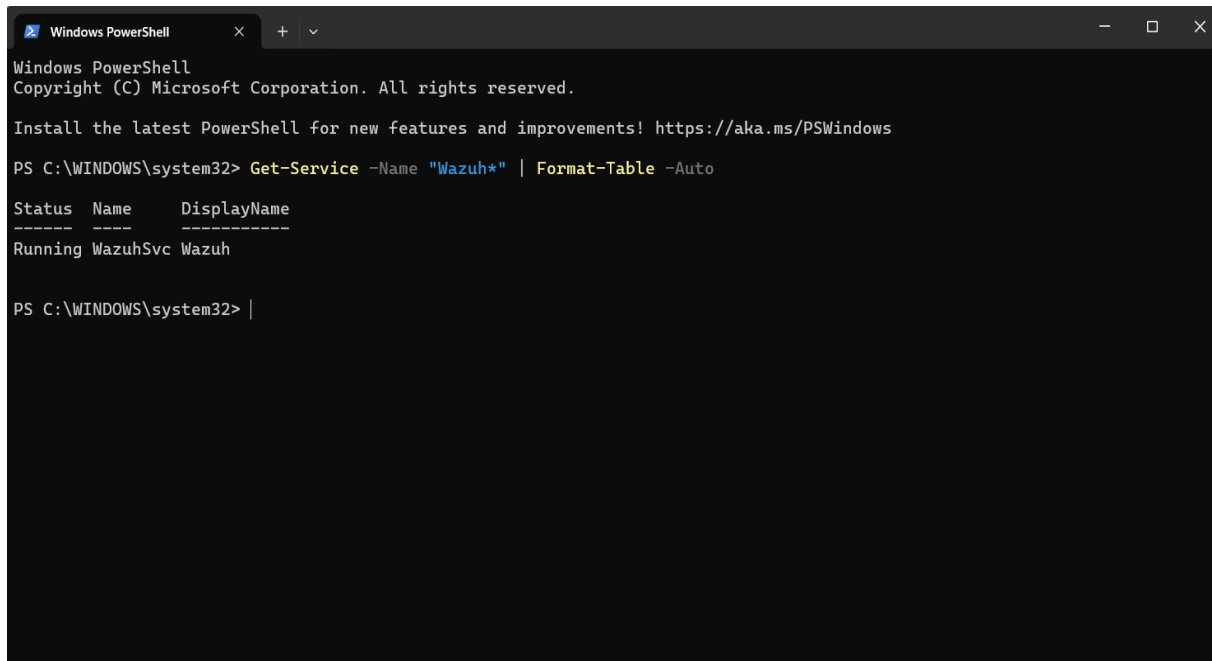
Οι βασικές ρυθμίσεις και παραμετροποιήσεις του πράκτορα γίνονται από ένα κεντρικό αρχείο με την ονομασία ossec.conf. Στη συγκεκριμένη υλοποίηση βρίσκεται στη διαδρομή:

```
C:\Program Files (x86)\ossec-agent\ossec.conf
```

Σε αυτό το αρχείο βρίσκονται όλες οι κρίσιμες παράμετροι με τη σημαντικότερη να αποτελεί η διεύθυνση IP του κεντρικού εξυπηρετητή. Ο πράκτορας πρέπει να γνωρίζει τη συγκεκριμένη διεύθυνση της εικονικής μηχανής ώστε να μπορεί να στείλει ορθά τα δεδομένα του. Για να γίνει επιβεβαίωση ότι η IP έχει γραφεί σωστά χωρίς να ανοίξουμε όλο το αρχείο μπορεί να χρησιμοποιηθεί η εξής εντολή με δικαιώματα διαχειριστή:

```
Get-Content "C:\Program Files (x86)\ossec-agent\ossec.conf" | Select-String -Pattern "<server>",
"<address>", "</server>" -Context 0,2
```

Συμπερασματικά, η επιτυχής εγκατάσταση επιβεβαιώνεται από τρία βασικά στοιχεία. Πρώτον ότι το λογισμικό υπάρχει στο σύστημα, δεύτερον ότι η υπηρεσία είναι σε κατάσταση λειτουργίας και τέλος ότι στο αρχείο έχει ρυθμιστεί η σωστή διεύθυνση IP του κεντρικού εξυπηρετητή.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> Get-Service -Name "Wazuh*" | Format-Table -Auto

Status  Name      DisplayName
-----
Running WazuhSvc Wazuh

PS C:\WINDOWS\system32> |
```

Σχήμα 3.17: Έλεγχος κατάστασης της υπηρεσίας Wazuh Agent στα Windows

3.5.2 Επικοινωνία πράκτορα με κεντρικό εξυπηρετητή

Η επαλήθευση της επικοινωνίας όπως προαναφέρθηκε χωρίστηκε σε τρία στάδια. Ο έλεγχος της παραμετροποίησης, ο έλεγχος της δικτυακής προσβασιμότητας και η επιβεβαίωση από τον πίνακα ελέγχου του Wazuh αποτελούν απαραίτητη διαδικασία για την επιβεβαίωση ότι ο πράκτορας έχει ενταχθεί λειτουργικά.

Στη συγκεκριμένη υλοποίηση η ρύθμιση της διεύθυνσης IP έγινε μέσω του αρχείου ρυθμίσεων ossec.conf. Αφού εντοπίστηκε το αρχείο και ανοίχτηκε με δικαιώματα διαχειριστή έγινε η παραμετροποίηση της διεύθυνσης IP του διακομιστή στο αντίστοιχο τμήμα κώδικα, όπως φαίνεται παρακάτω:

```
<client>

  <server>

    <address>192.168.49.128</address>

    <port>1514</port>

    <protocol>tcp</protocol>

  </server>

</client>
```

Μετά την ολοκλήρωση αλλαγής της διεύθυνσης πραγματοποιήθηκε επανεκκίνηση της υπηρεσίας ώστε να εφαρμοστούν οι νέες ρυθμίσεις. Η διαδικτυακή προσβασιμότητα ελέγχθηκε από τις εντολές:

```
Test-NetConnection 192.168.49.128 -Port 1514
```

```
Test-NetConnection 192.168.49.128 -Port 1515
```

Η χρήση της πόρτας 1514/TCP είναι η προεπιλεγμένη θύρα της σύνδεσης του πράκτορα για την αποστολή μηνυμάτων προς τον server. Η χρήση της πόρτας 1515 χρησιμοποιείται για τις διαδικασίες εγγραφής όπου απαιτείται.

Τα αρχεία καταγραφής του πράκτορα βοηθάνε στην επιβεβαίωση ότι η υπηρεσία έχει εκκινηθεί σωστά, διαβάσει την παραμετροποίηση και προσπαθεί να επικοινωνήσει με τον manager. Η τελική επιβεβαίωση έγινε από τον πίνακα ελέγχου όπου η κατάσταση του πράκτορα πρέπει να εμφανίζεται ως ενεργή. Η χρήση της διεύθυνσης 192.168.49.128 στο δίκτυο τύπου Host Only εξασφάλισε την σταθερότητα στο σημείο επικοινωνίας. Με αυτό τον τρόπο η σύνδεση τερματικού με τον κεντρικό κόμβο δεν εξαρτιέται από μεταβαλλόμενες διευθύνσεις IP που μπορεί να αποδίδονται από τα διαφορετικά εξωτερικά δίκτυα κάθε φορά.

3.5.3 Εμπλουτισμός τηλεμετρίας με χρήση Sysmon

Η χρήση του πράκτορα προσφέρει μια πρώτη και πολύ σημαντική εικόνα για την κατάσταση του συστήματος. Ωστόσο όταν ο στόχος είναι η σε βάθος ανάλυση της ασφάλειας μια απλή καταγραφή δεν αρκεί. Πρέπει να πραγματοποιηθεί μια πιο λεπτομερής ροή δεδομένων, την οποία ονομάζουμε τηλεμετρία, με στόχο την παρακολούθηση με ακρίβεια των κρίσιμων ενεργειών. Η δημιουργία νέων διεργασιών οι δικτυακές συνδέσεις που πραγματοποιούνται και οποιαδήποτε αλλαγή στα αρχεία του υπολογιστή είναι παραδείγματα τέτοιων ενεργειών. Για την υλοποίηση αυτού του επιπέδου ασφάλειας στην παρούσα εργασία χρησιμοποιήθηκε το εργαλείο Sysmon ως πρόσθετος μηχανισμός καταγραφής συμβάντων ασφαλείας.

Το Sysmon (System Monitor), είναι ένα εργαλείο της συλλογής Microsoft Sysinternals. Λειτουργεί στο παρασκήνιο του λειτουργικού συστήματος και έχει ως σκοπό την παραγωγή λεπτομερών συμβάντων που αποθηκεύονται στην υπηρεσία καταγραφής συμβάντων των Windows (Windows Event Log). Στην παρούσα εργασία το συγκεκριμένο εργαλείο αξιοποιείται για τον εμπλουτισμό της τηλεμετρίας με τη βασική του λειτουργία, χωρίς την εφαρμογή εξειδικευμένου αρχείου παραμετροποίησης με χρήση XML. Έτσι εμπλουτίστηκε η βασική τηλεμετρία του τερματικού και ενισχύθηκε η ορατότητα του συστήματος με στόχο την καλύτερη ορατότητα και διερεύνηση.

3.5.3.1 Συσχέτιση με το πλαίσιο MITRE ATT&CK

Η παρούσα υποενότητα εστιάζει στην πρακτική εφαρμογή του πλαισίου MITRE ATT&CK μέσω των δεδομένων που λαμβάνουμε από το Sysmon. Η αναφορά αυτή είναι απαραίτητη καθώς μια απλή καταγραφή ενός συμβάντος θα πρέπει να ερμηνευτεί. Ένα συμβάν δεν αποτελεί από μόνο του ένδειξη επίθεσης. Πολλές καταγραφές αφορούν τη νόμιμη λειτουργία του συστήματος. Έτσι αντί για μεμονωμένα και ασύνδετα αρχεία καταγραφής, ο αναλυτής μπορεί να κατανοήσει το σκοπό πίσω από κάθε ενέργεια καθώς το σύστημα παρέχει πλέον τεχνικό πλαίσιο. Στον πίνακα που ακολουθεί παρουσιάζονται κάποιες ενδεικτικές καταγραφές ως παραδείγματα με στόχο να φανεί πως οι διαφορετικοί τύποι συμβάντων Sysmon, μπορούν να συσχετιστούν με τεχνικές και κατηγορίες του συγκεκριμένου πλαισίου.

Πίνακας 3.3: Ενδεικτική συσχέτιση συμβάντων Sysmon με το MITRE ATT&CK

A/A	Sysmon event ID	Καταγραφή	Συσχέτιση MITRE ATT&CK
1	1	Δημιουργία διεργασίας	Execution
2	3	Δικτυακή Σύνδεση	Command and Control
3	7	Φόρτωση βιβλιοθήκης	Defense evasion
4	11	Δημιουργία αρχείου	Persistence
5	13	Μεταβολή μητρώου	Privilege Escalation
6	22	Ερώτημα DNS	Discovery

Συμπερασματικά η αξία χρήσης του Sysmon δεν έχει να κάνει με την αύξηση του όγκου δεδομένων. Μπορεί να παρέχει το απαραίτητο τεχνικό πλαίσιο για την κατανόηση των γεγονότων που παράγονται. Για την αποτελεσματική ανίχνευση της απειλής τα δεδομένα δεν εξετάζονται μεμονωμένα. Όπως δείξαμε αξιολογούνται συνδυαστικά με κρίσιμες παραμέτρους όπως ο χρήστης, η χρονική στιγμή και η δικτυακή συμπεριφορά και σύμφωνα με το πλαίσιο των κανόνων ανάλυσης στο κεντρικό σύστημα SIEM.

3.5.3.2 Υλοποίηση και ενσωμάτωση

Η εγκατάσταση υλοποιήθηκε με τη χρήση της έκδοσης Sysmon64 v15.15. Συγκεκριμένα η σωστή εγκατάσταση του εργαλείου έγινε μέσω της διεπαφής της γραμμής εντολών με δικαιώματα διαχειριστή και τη χρήση της ακόλουθης εντολής:

```
Sysmon64.exe -accepteula -i
```

Η παράμετρος -accepteula χρησιμοποιήθηκε για την αυτόματη αποδοχή των όρων χρήσης και η παράμετρος -i ορίζει την εγκατάσταση ως μόνιμη υπηρεσία των Windows. Αφού ολοκληρωθεί, το εργαλείο συλλογής Sysmon ξεκινάει την καταγραφή δεδομένων σε αποκλειστικό κανάλι μέσα στο Windows Event Log. Η επιβεβαίωση της παραγωγής συμβάντων έγινε με τη χρήση της εντολής:

```
wevtutil qe Microsoft-Windows-Sysmon/Operational /c:5 /f:text
```

Με τη συγκεκριμένη εντολή εμφανίζονται οι πέντε πιο πρόσφατες εγγραφές και επιβεβαιώνεται η ενεργή λειτουργία του εργαλείου. Η επιχειρησιακή αξιοποίηση των δεδομένων προϋποθέτει την ενσωμάτωσή τους στο SIEM. Για να είναι δυνατή η προώθηση των συμβάντων Sysmon προς τον Wazuh Server, ο πράκτορας Wazuh μπορεί να ρυθμιστεί ώστε να παρακολουθεί το αντίστοιχο κανάλι συμβάντων των Windows. Η ρύθμιση αυτή δηλώνεται στο αρχείο ossec.conf του πράκτορα, για παράδειγμα ως εξής:

<localfile>

<location>Microsoft-Windows-Sysmon/Operational</location>

<log_format>eventchannel</log_format>

</localfile>

Αφού εμφανιστούν στο περιβάλλον διαχείρισης αξιοποιούνται από τους μηχανισμούς ανάλυσης και τους κανόνες με στόχο την τελική τους οπτικοποίηση και την παραγωγή των σχετικών ειδοποιήσεων. Η συγκεκριμένη προσέγγιση ενισχύει σημαντικά την ορατότητα στο επίπεδο του τερματικού χωρίς όμως να παρουσιάζεται ως πλήρως εξειδικευμένη παραμετροποίηση.

3.6 Πηγές δεδομένων και πεδίο εφαρμογής

Στην ενότητα αυτή θα παρουσιαστούν οι πηγές δεδομένων από τις οποίες το σύστημα μπορεί να αντλεί πληροφορίες καθώς θα αναφερθεί και ο ρόλος τους στην υλοποίηση. Σε ένα σύστημα διαχείρισης πληροφοριών και συμβάντων ασφαλείας, οι πηγές δεδομένων αποτελούν βασικό σημείο της ανάλυσης. Με άλλα λόγια είναι καταγραφές που δείχνουν τι συμβαίνει κάθε στιγμή. Το σύστημα συλλέγει αυτές τις πληροφορίες και τις αξιοποιεί για την εύρεση τυχόν ύποπτων δραστηριοτήτων.

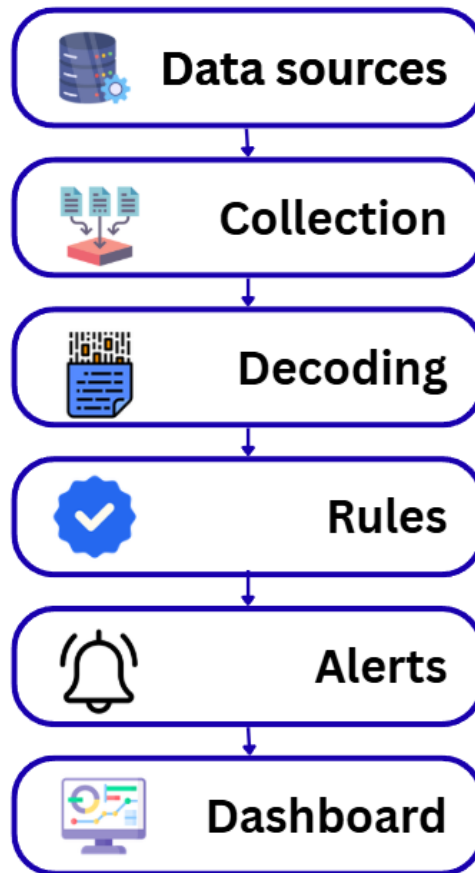
Για την υλοποίηση αυτή επιλέχθηκαν δύο βασικές κατηγορίες δεδομένων. Όπως έχει ήδη αναφερθεί η πρώτη κατηγορία αφορά την άμεση παρακολούθηση από το τερματικό σύστημα των Windows, η οποία υλοποιείται μέσω του πράκτορα. Η δεύτερη κατηγορία αφορά την επεξεργασία των πληροφοριών από το δίκτυο. Στη συγκεκριμένη εργασία για την πραγματοποίηση των δοκιμών έγινε εισαγωγή δεδομένων εξωτερικών αρχείων καταγραφής, τα οποία προσομοιώνουν τη ροή δεδομένων σε ένα ψηφιακό περιβάλλον και βασίζονται σε δεδομένα τύπου Syslog από περιβάλλον Juniper vSRX. Έτσι ο συνδυασμός αυτός δεν περιορίζει τις δοκιμές μόνο σε έλεγχο μεμονωμένων συσκευών, αλλά επεκτείνεται στην υλοποίηση και επεξεργασία των δικτυακών δεδομένων σε επίπεδο εργαστηρίου.

3.6.1 Η έννοια της πηγής δεδομένων σε ένα SIEM

Σε ένα σύστημα ανοιχτού κώδικα SIEM, ως πηγή δεδομένων ορίζεται κάθε οντότητα, υπηρεσία ή εφαρμογή η οποία παράγει καταγραφές δραστηριότητας. Οι πηγές αυτές αποτελούν την κύρια βάση για την συλλογή και την μετέπειτα ανάλυση της πληροφορίας από τις τερματικές συσκευές έως και δικτυακό εξοπλισμό και εφαρμογές ασφαλείας.

Ο ρόλος ενός SIEM επεκτείνεται σημαντικά και δεν στέκεται μόνο στην αρχειοθέτηση των δεδομένων. Κύριο ρόλο του αποτελεί και η συγκέντρωση των πληροφοριών από πολλαπλά και συχνά ανομοιογενή συστήματα, η μετατροπή τους σε μια αξιοποιήσιμη μορφή καθώς και η αξιολόγηση τους μέσω συγκεκριμένων κανόνων. Με τον τρόπο αυτό διευκολύνεται η άμεση ανίχνευση των απειλών και υποστηρίζεται η περαιτέρω διερεύνηση των πιθανών περιστατικών ασφαλείας.

Οι πηγές δεδομένων διαφέρουν ως προς τη μορφή και το περιεχόμενό τους. Παρότι αυτές οι μορφές παρουσιάζουν διαφορετικά χαρακτηριστικά, το σύστημα πρέπει να μπορεί να τις συλλέγει όλες και να τις μετατρέπει σε χρήσιμη πληροφορία για τον αναλυτή. Με αυτό τον τρόπο ενισχύεται η επίγνωση της κατάστασης ασφαλείας ολόκληρης της υποδομής.



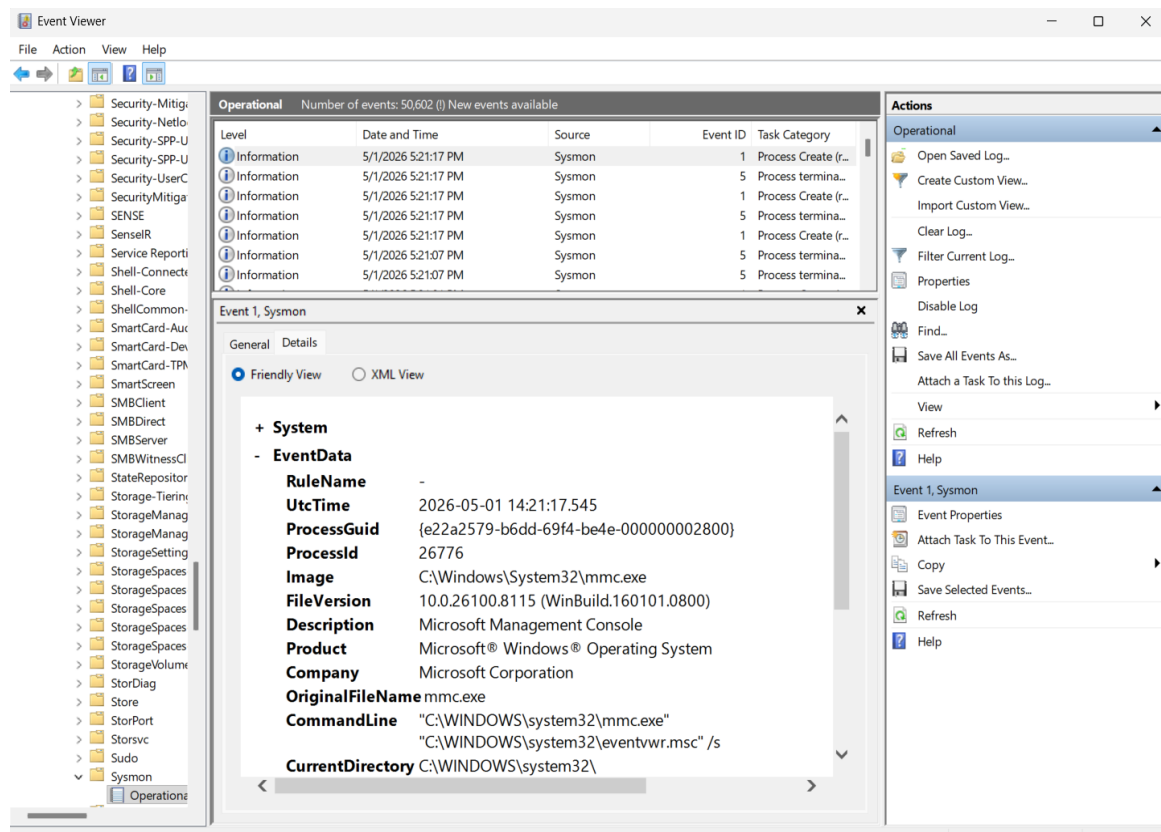
Σχήμα 3.18: Ροή δεδομένων από πηγές καταγραφής προς το Wazuh

3.6.2 Πηγές δεδομένων της παρούσας υλοποίησης

Στην παρούσα υλοποίηση έγινε αξιοποίηση δύο κεντρικών πηγών δεδομένων. Η επιλογή τους επέτρεψε την αξιολόγηση δύο διαφορετικών μεθόδων συλλογής και επεξεργασίας πληροφοριών ασφαλείας.

Η πρώτη πηγή αφορά το τερματικό σύστημα των Windows, στο οποίο έγινε η εγκατάσταση του πράκτορα για τη διασύνδεση με το κεντρικό διακομιστή του Wazuh. Η επιλογή αυτή μας παρείχε τα τυπικά αρχεία καταγραφής του τερματικού ενώ παράλληλα η χρήση του εργαλείου Sysmon επέτρεψε την συλλογή ακόμη πιο λεπτομερούς τηλεμετρίας. Έτσι έγινε εστίαση σε κρίσιμα συμβάντα που αφορούν τη δημιουργία διεργασιών και τις συνδέσεις δικτύου του συστήματος. Η δεύτερη πηγή δεδομένων προέρχεται από ένα σύνολο δεδομένων τύπου syslog βασισμένο σε μορφή δεδομένων Juniper vSRX. Η συγκεκριμένη πηγή χρησιμοποιήθηκε για την αποτελεσματική προσομοίωση δικτυακών συμβάντων εντός του δοκιμαστικού περιβάλλοντος που υλοποιήθηκε. Η εισαγωγή του πραγματοποιήθηκε μέσω μηχανισμού σε αρχείο ρυθμίσεων όπου τα δεδομένα αντλούνται από τοπικό αρχείο.

Η συνδυαστική χρήση αυτών των δύο πηγών πρόσφερε δυνατότητα μελέτης δύο σεναρίων. Την αρχική παρακολούθηση και λήψη της τηλεμετρίας σε πραγματικό χρόνο και την επεξεργασία δικτυακών δεδομένων από την πλατφόρμα του Wazuh. Με τον τρόπο αυτό, τεκμηριώνεται η ικανότητα του συστήματος να διαχειρίζεται ετερογενή δεδομένα κάτι το οποίο είναι πολύ σημαντικό στο περιβάλλον ανάπτυξης της ναυτιλίας.



Σχήμα 3.19: Προβολή Sysmon events

3.6.3 Εισαγωγή του συνόλου δεδομένων syslog

Προκειμένου να αναπαραστήσουμε την κίνηση ενός δικτύου σε ένα πλοίο, χρησιμοποιήθηκαν ανωνυμοποιημένα πραγματικά δεδομένα πλοίων από το εικονικό τείχος προστασίας Juniper vSRX. Στόχος ήταν να αξιολογηθεί η δυνατότητα λειτουργίας της πλατφόρμας του Wazuh ως κεντρικό σύστημα καταγραφής, το οποίο επεξεργάζεται και εξωτερικές πηγές δεδομένων σε πραγματικές συνθήκες δικτύου.

Οι εγγραφές από τη βάση δεδομένων που χρησιμοποιήθηκαν περιλαμβάνουν τύπους συμβάντος οι οποίοι αντιστοιχούν σε διαφορετικές μορφές δραστηριότητες του δικτύου. Οι τύποι αυτοί ήταν η δημιουργία σύνδεσης, η απόρριψη σύνδεσης, ο τερματισμός μιας συνεδρίας και συμβάντα ανίχνευσης.

Η εισαγωγή των καταγραφών πραγματοποιήθηκε μέσω ενός τοπικού αρχείου στο εικονικό περιβάλλον Ubuntu. Αρχικά δημιουργήθηκε ο ειδικός κατάλογος και το αρχείο καταγραφής στη διαδρομή `/var/log/vessel/vsrx.log`. Η δημιουργία και η ρύθμιση έγινε από τέσσερις εντολές.

- **sudo mkdir -p /var/log/vessel:** Δημιουργία φακέλου με όνομα vessel στον κατάλογο των αρχείων καταγραφής (/var/log)
- **sudo touch /var/log/vessel/vsrx.log:** Δημιουργία κενού αρχείου με το όνομα vsrx.log

- **sudo chown root:wazuh /var/log/vessel/vsrx.log:** Αλλαγή του ιδιοκτήτη (owner) και της ομάδας (group) του αρχείου
- **sudo chmod 640 /var/log/vessel/vsrx.log:** Ορίζει τα δικαιώματα πρόσβασης (permissions) στο αρχείο

Στη συνέχεια έπρεπε να πραγματοποιηθεί παραμετροποίηση στο αρχείο ρυθμίσεων του Wazuh manager /var/ossec/etc/ossec.conf. Η ρύθμιση αυτή θα επέτρεπε στο Wazuh να παρακολουθεί το συγκεκριμένο αρχείο ως πηγή δεδομένων καταγραφών τύπου Syslog. Συγκεκριμένα έγινε η προσθήκη της ενότητας:

```
<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/vessel/vsrx.log</location>
</localfile>
```

Η παράμετρος log_format ορίζει ότι οι εγγραφές που περιέχει το αρχείο θα αναλύονται ως μηνύματα τύπου syslog. Η παράμετρος location καθορίζει τη διαδρομή του αρχείου. Στην συνέχεια πραγματοποιήθηκε επανεκκίνηση της υπηρεσίας του Manager ώστε να εφαρμοστούν οι νέες ρυθμίσεις:

```
sudo systemctl restart wazuh-manager
```

Για το πειραματικό σκέλος αναπτύχθηκε ένα εξατομικευμένο σενάριο κελύφους (bash script) με την ονομασία generate_logs.sh. Σκοπός ήταν το συγκεκριμένο script να παράγει δυναμικές εγγραφές τύπου vSRX προσομοιώνοντας μια συνεχή ροή δικτυακών δεδομένων. Η διαδικασία περιλάμβανε την απόδοση δικαιωμάτων εκτέλεσης και την έναρξη παραγωγής νέων εγγραφών.

```
chmod +x generate_logs.sh
```

```
./generate_logs.sh
```

Η παρακολούθηση των δεδομένων σε πραγματικό χρόνο πραγματοποιείται από:

```
sudo tail -f /var/log/vessel/vsrx.log
```

Μετά την επιβεβαίωση της τοπικής εγγραφής των αρχείων καταγραφής, επαληθεύτηκε η συλλογή τους μέσα από την πλατφόρμα του Wazuh. Χρησιμοποιώντας το φίλτρο location: /var/log/vessel/vsrx.log διαπιστώθηκε η επιτυχής εισαγωγή των δεδομένων στην ροή της επεξεργασίας. Η απλή εμφάνιση των γεγονότων δεν συνεπάγεται την αυτόματη παραγωγή ειδοποιήσεων. Σε επόμενη ενότητα θα αναλυθεί πως έγινε η παραγωγή καθώς αυτό απαιτούσε τη χρήση κατάλληλων κανόνων και αποκωδικοποίησης.

3.6.4 Πεδίο εφαρμογής του συστήματος

Στο περιβάλλον ενός πλοίου απαιτείται η ανίχνευση απειλών από πολλαπλές πηγές με διαφορετικά λειτουργικά συστήματα και ρόλους, όπως συστήματα επιχειρησιακής τεχνολογίας, συστήματα πληροφορικής και δίκτυα. Για τον λόγο αυτό, η παρούσα εφαρμογή αξιολογεί το προτεινόμενο πρωτότυπο SIEM, ως προς την ικανότητα του στην επεξεργασία δεδομένων από ανόμοιες πηγές. Η υποενότητα αυτή λειτουργεί ως συνέχεια της ανάλυσης των πηγών δεδομένων καθώς προσδιορίζει το τι καλύπτει στην πράξη το σύστημα που αναπτύχθηκε.

Στο πεδίο εφαρμογής περιλαμβάνεται τόσο η συλλογή τηλεμετρίας από τερματικό σύστημα των Windows μέσω του πράκτορα όσο και η εισαγωγή εξωτερικών δεδομένων τύπου Syslog. Επιπλέον στη συνέχεια θα αξιολογηθούν και τα αποτελέσματα των αρχείων καταγραφής στον κεντρικό πίνακα ελέγχου, μέσω χρήσης αποκωδικοποιητών και κανόνων στην επόμενη ενότητα. Η λύση μπορεί να αποτελέσει βάση για εφαρμογή σε περιβάλλοντα όπου απαιτείται κεντρική συλλογή και ανάλυση συμβάντων. Ωστόσο στην παρούσα εργασία δεν θα αναπτυχθεί ολοκληρωμένο επιχειρησιακό κέντρο ασφάλειας το οποίο είναι εκτός του παρόντος πεδίου εφαρμογής.

Συνεπώς το πεδίο εφαρμογής οριοθετεί με σαφήνεια τον ρόλο που έχει η παρούσα υλοποίηση. Το σύστημα παρουσιάζεται ως λειτουργική αλλά και επεκτάσιμη βάση πάνω στην οποία μπορούν να αναπτυχθούν ακόμα πιο σύνθετες δυνατότητες παρακολούθησης και ανίχνευσης.

3.7 Μηχανισμός ανίχνευσης

Η συγκεκριμένη ενότητα αναλύει την αρχιτεκτονική ανίχνευσης που εφαρμόστηκε για την επεξεργασία των καταγραφών του τύπου vSRX μέσω της πλατφόρμας Wazuh. Η παρούσα διαδικασία δεν αποτελεί απλή συλλογή δεδομένων αλλά βασίζεται σε έναν κύκλο επεξεργασίας στον οποίο οι ακατέργαστες εγγραφές κειμένου μετατρέπονται σε δεδομένη πληροφορία. Κεντρικό ρόλο έχουν οι αποκωδικοποιητές, όπου αναλαμβάνουν την εξαγωγή των κρίσιμων πεδίων από το περιεχόμενο των καταγραφών και οι κανόνες, οι οποίοι αξιολογούν τα δεδομένα και αποδίδουν το επίπεδο σοβαρότητας. Μέσω αυτής της διαδικασίας παράγονται οι σχετικές ειδοποιήσεις στο κεντρικό περιβάλλον του Wazuh.

Στο πλαίσιο της μελέτης, αξιοποιήθηκαν τόσο οι ενσωματωμένοι μηχανισμοί της πλατφόρμας για περιβάλλοντα Junos όσο παράλληλα αναπτύχθηκαν εξατομικευμένοι αποκωδικοποιητές και κανόνες για την κάλυψη των απαιτήσεων. Στόχος ήταν τόσο η αξιολόγηση της λειτουργικότητας όσο και η μελλοντική επεκτασιμότητα σε μη τυποποιημένες μορφές. Έτσι ενισχύεται η πλήρης ορατότητα συμβάντων και η προσαρμογή του συστήματος στις ιδιαίτερες ανάγκες που χρειάζεται η υποδομή.

3.7.1 Ρόλος και λειτουργία των αποκωδικοποιητών

Οι αποκωδικοποιητές είναι η πρώτη γραμμή επεξεργασίας του μηχανισμού ανίχνευσης. Ο ρόλος τους είναι να μετατρέπουν μια ακατέργαστη γραμμή κειμένου σε δομημένη πληροφορία. Ως παράδειγμα χωρίζεται σε συγκεκριμένα πεδία όπως η διεύθυνση IP προέλευσης, η διεύθυνση IP προορισμού, η θύρα που χρησιμοποιεί και η ενέργεια που εκτελέστηκε. Με αυτό τον τρόπο ένα αρχείο αποκτά νόημα και δεν παραμένει απλό κείμενο που δεν μπορεί να αναλυθεί ή να συσχετιστεί με κανόνες.

Στην πλατφόρμα Wazuh οι αποκωδικοποιητές ορίζονται σε αρχεία τα οποία είναι της μορφής XML. Για την αποκωδικοποίηση των συμβάντων Junos/vSRX τύπου syslog χρησιμοποιούνται οι προεγκατεστημένοι αποκωδικοποιητές οι οποίοι βρίσκονται στη διαδρομή /var/ossec/ruleset/decoders/0490-junos_decoders.xml. Για διαφοροποιημένα ή μη τυποποιημένα μορφότυπα απαιτείται έλεγχος και πιθανώς προσαρμοσμένος αποκωδικοποιητής. Κάποιοι από τους αποκωδικοποιητές του αρχείου που αναφέρθηκε είναι:

- **junos-ids:** Για συμβάντα που αφορούν το σύστημα ανίχνευσης εισβολών
- **junos-ids-ip-spoofing:** Για την αναγνώριση πλαστογράφησης διευθύνσεων IP
- **junos-ids-no-tcp-flags:** Για τον εντοπισμό ανώμαλης κυκλοφορίας δικτύου

Επιπλέον οι αποκωδικοποιητές χρησιμοποιούν μηχανισμούς όπως είναι το προφιλτράρισμα (Prematch). Ο συγκεκριμένος μηχανισμός λειτουργεί ως αρχικό φίλτρο για τον εντοπισμό των σχετικών μηνυμάτων. Στη συνέχεια χρησιμοποιούνται κανονικές εκφράσεις (Regular Expressions – Regex) για την εξαγωγή συγκεκριμένων τιμών από το log. Τέλος η ταξινόμηση (order) καθορίζει την αντιστοίχιση αυτών των τιμών σε ονόματα πεδίων.

< 0490-junos_decoders.xml

```

1 <!--
2   - Junos decoders
3   - Created by Wazuh, Inc.
4   - Copyright (C) 2015, Wazuh Inc.
5   - This program is a free software; you can redistribute it and/or modify it under the terms of GPLv2.
6 -->
7
8
9 <decoder name="junos-ids">
10   <program_name>junos-ids</program_name>
11 </decoder>
12
13
14
15
16 <decoder name="junos-ids-ip-spoofing">
17   <parent>junos-ids</parent>
18   <prematch>IP spoofing</prematch>
19   <regex offset="after_parent"> (\.) (\S+) - (\S+) [\S+ attack-name="(\S+)" source-address="(\S+)" destination-address="(\S+)" protocol-id="(\S+)" source
20     -zone-name="(\S+)" interface-name="(\S+)" action="(\S+)"]</regex>
21   <order>firewall_name, cat, sub_cat, attack.name, srcip, dstip, protocol_id, source_zone, interface, action</order>
22 </decoder>
23
24
25
26 <decoder name="junos-ids-no-tcp-flags">
27   <parent>junos-ids</parent>
28   <prematch>No TCP flag</prematch>
29   <regex offset="after_parent"> (\.) (\S+) - (\S+) [\S+ attack-name="(\S+)" source-address="(\S+)" source-port="(\S+)" destination-address="(\S+)"
30     destination-port="(\S+)" source-zone-name="(\S+)" interface-name="(\S+)" action="(\S+)"]</regex>
31   <order>firewall_name, cat, sub_cat, attack.name, srcip, srcport, dstip, dstport, source_zone, interface, action</order>
32 </decoder>
33 <!--
34 Generic

```

Σχήμα 3.20: Απόσπασμα του αρχείου 0490-junos_decoders.xml

Κατά τη διάρκεια της υλοποίησης, οι καταγραφές των πλοίων (vSRX) υποβλήθηκαν σε ένα αρχικό στάδιο προ-αποκωδικοποίησης. Σε αυτή τη φάση το σύστημα μπορεί να αναγνωρίζει τα βασικά στοιχεία της εγγραφής. Σαν παράδειγμα θα αναφερθεί το πεδίο program_name το οποίο προσδιορίζει το υποσύστημα προέλευσης. Αν το αρχείο καταγραφής δει την τιμή junos-flow ξέρει ότι αφορά κίνηση δικτύου και το στέλνει σε αποκωδικοποιητή που γνωρίζει να διαβάσει διευθύνσεις IP και θύρες. Η πληροφορία αυτή λειτουργεί ως κύριο κριτήριο στην αντιστοίχιση της εγγραφής με τη κατάλληλη οικογένεια αποκωδικοποιητών. Έτσι διευκολύνεται η επεξεργασία με βάση το σωστό πρότυπο δεδομένων.

Μια απλή εισαγωγή αρχείου δεν σημαίνει απαραίτητα πως θα υλοποιηθεί και πλήρης αξιοποίηση του από τον μηχανισμό της ανίχνευσης. Η επιτυχία αποκωδικοποίησης εξαρτάται από τη συμβατότητα της εγγραφής με τα κριτήρια που αναμένει ο αποκωδικοποιητής. Έτσι, αν η μορφή της καταγραφής διαφέρει από αυτή που έχει προβλεφθεί στο σύνολο των κανόνων ενδέχεται να μην αποκωδικοποιηθεί ή να απαιτείται τοπικά προσαρμογή.

3.7.2 Κανόνες ανίχνευσης και παραγωγή ειδοποιήσεων

Σε συνέχεια της αποκωδικοποίησης, οι κανόνες ανίχνευσης αποτελούν το επόμενο στάδιο της ανάλυσης. Χρησιμοποιούνται από το σύστημα για την αξιολόγηση των δομημένων πεδίων που προκύπτουν από την αποκωδικοποίηση ή και ακατέργαστων εγγραφών (full log). Ωστόσο, όπως ειπώθηκε η ύπαρξη δομημένων πεδίων αυξάνει την ακρίβεια της ανίχνευσης.

Όταν ικανοποιούνται οι συνθήκες ενός κανόνα, το σύστημα καταφέρνει να παράγει ειδοποιήσεις με συγκεκριμένο επίπεδο σοβαρότητας. Τα δεδομένα που προκύπτουν κατά την ενεργοποίηση του κανόνα είναι πεδία όπως το αναγνωριστικό κανόνα (rule.id), το επίπεδο κανόνα (rule.level) και η περιγραφή κανόνα (rule.description). Αυτά τα μεταδεδομένα επιτρέπουν την ταξινόμηση και το φιλτράρισμα των αποτελεσμάτων. Στην πλατφόρμα Wazuh οι κανόνες ορίζονται σε αρχεία με χρήση XML. Οι ενσωματωμένοι κανόνες βρίσκονται στο αρχείο /var/ossec/ruleset/rules/0640-junos_rules.xml.

Οι κανόνες του Wazuh λειτουργούν ιεραρχικά. Ως βάση υπάρχει ένας γενικός κανόνας ενώ η ενεργοποίηση πιο εξειδικευμένου κανόνα ενεργοποιείται εφόσον έχει προηγηθεί αντιστοίχιση του γενικού. Αυτό υλοποιείται με μηχανισμούς όπως το if_Sid, έναν μηχανισμό ο οποίος δηλώνει ότι ένας κανόνας εξαρτάται από προηγούμενο rule.id.

Όπως φαίνεται στο Σχήμα 3.21, ο κανόνας 67102 λειτουργεί ως κανόνας επιπέδου 0 για καταγραφές που έχουν αποκωδικοποιηθεί ως ροή επεξεργασίας σε πραγματικό χρόνο (junos-rt-flow). Έπειτα, ο κανόνας 67103 βασίζεται στον προηγούμενο μέσω του if_sid 67102 και αποδίδει επίπεδο σοβαρότητας 5, με περιγραφή υποκατηγορίας ροής πραγματικού χρόνου (Junos RT flow: \$(subcat)). Έτσι εξηγείται η λογική της ιεράρχησης των κανόνων στην οποία ο αρχικός κανόνας ταξινομεί ένα συμβάν και ο επόμενος που εξαρτάται από τον αρχικό αποδίδει επίπεδο σοβαρότητας και πιο κατανοητή περιγραφή.



Σχήμα 3.21: Απόσπασμα του αρχείου 0640-junos_rules.xml

Η πλατφόρμα wazuh, πέρα από τους ενσωματωμένους κανόνες επιτρέπει την τοπική προσαρμογή των κανόνων του μηχανισμού ανίχνευσης. Η δυνατότητα αυτή είναι πολύ σημαντική, καθώς τα αρχεία καταγραφής που εισάγονται στο σύστημα δεν καλύπτονται πλήρως από τα προ εγκατεστημένα αρχεία ή ακόμα απαιτείται ειδική λογική ανίχνευσης. Οι τοπικοί κανόνες ορίζονται στο αρχείο /var/ossec/etc/rules/local_rules.xml.

Αντίστοιχα, μπορούν να οριστούν και προσαρμοσμένοι τοπικοί αποκωδικοποιητές. Σαν συμπέρασμα, το σύστημα μπορεί να αναγνωρίζει συγκεκριμένες εγγραφές και να παράγει ειδοποιήσεις όταν ικανοποιούνται τα αντίστοιχα κριτήρια. Το συγκεκριμένο είναι πολύ σημαντικό για ένα περιβάλλον όπως της ναυτιλίας, στο οποίο συναντάμε διαφορετικούς τύπους συστημάτων, συσκευών και μορφών καταγραφής. Επιπλέον το πλοίο λειτουργεί σε μεταβαλλόμενες συνθήκες στις οποίες η τοποθεσία και ο τρόπος σύνδεσης με το δίκτυο μπορούν να επηρεάσουν την ερμηνεία ενός συμβάντος. Έτσι η πλατφόρμα επεκτείνεται πέρα από τις προεγκατεστημένες δυνατότητες και προσαρμόζεται στις ανάγκες της εκάστοτε υποδομής.

3.7.3 Συσχέτιση αποκωδικοποιητών και κανόνων

Πυρήνα της διαδικασίας ανίχνευσης αποτελεί η σχέση μεταξύ των αποκωδικοποιητών και των κανόνων. Σε αυτή τη σύνδεση, ο αποκωδικοποιητής κατέχει τον ρόλο που μεταφράζει την ακατέργαστη πληροφορία και την αναλύει σε μικρότερα, επιμέρους και αναγνωρίσιμα πεδία. Αφού ολοκληρωθεί αυτός ο μετασχηματισμός σε δομημένα πεδία την ανάλυση αναλαμβάνουν οι κανόνες. Ειδικότερα, οι κανόνες λειτουργούν ως μηχανισμός αξιολόγησης της διαδικασίας, αξιολογώντας τα δεδομένα που εξήγαγε ο αποκωδικοποιητής. Στόχος είναι ο προσδιορισμός του εάν η δραστηριότητα που έχει καταγραφεί συνιστά τυχόν πιθανή απειλή ή κάποιο σημαντικό συμβάν που απαιτεί την έκδοση ειδοποίησης.

Η συνεργασία αυτή τονίζει τη σημασία της στο γεγονός ότι αποτελεί τη βάση για την εισαγωγή σύνθετων κριτηρίων ανίχνευσης. Εάν η πληροφορία δεν χωριστεί σε συγκεκριμένα πεδία το σύστημα αδυνατεί να εκτελέσει πιο στοχευμένους ελέγχους. Σε μια τέτοια περίπτωση, η ανίχνευση θα περιοριζόταν σε πολύ γενικά κριτήρια και ως αποτέλεσμα ένα συμβάν θα εμφανιζόταν στο περιβάλλον διερεύνησης ως μια απλή καταγραφή. Ουσιαστικά η συσχέτιση αυτών των δύο μηχανισμών προετοιμάζει το έδαφος και λαμβάνει μια τεκμηριωμένη απόφαση για τη σοβαρότητα του συμβάντος.

Στην περίπτωση της παρούσας υλοποίησης, οι καταγραφές που υπήρχαν από τα πλοία αναδεικνύουν τη σημασία από το κομμάτι της αποκωδικοποίησης, κρίσιμης σημασίας. Οι καταγραφές περιέχουν ένα πλούσιο πληροφοριακό περιεχόμενο όπως υποκατηγορίες συμβάντων, διευθύνσεις δικτύου IP, θύρες, πολιτικές ασφαλείας και αιτιολογίες για τη δημιουργία ή την απόρριψη των συνδέσεων. Παρόλα αυτά η πληροφορία αυτή αρχικά παραμένει ως απλή μορφή κειμένου. Για να καταστεί δυνατή η αυτοματοποιημένη ανάλυση και η λήψη αποφάσεων από το σύστημα, πρέπει η πληροφορία να εξαχθεί και να μετατραπεί σε δομημένα πεδία.

Η ροή αυτή όπως φαίνεται στον Πίνακα 3.4, δείχνει τον λόγο για τον οποίο η ανάπτυξη ενός μηχανισμού ανίχνευσης πρέπει να αντιμετωπίζεται συνολικά. Δεν αρκεί η ύπαρξη ενός κανόνα αν δεν υπάρχει αποκωδικοποιητής, ο οποίος παρέχει τα απαραίτητα πεδία. Αντίστοιχα, δεν μπορεί να παραχθεί μια στοχευμένη ειδοποίηση χωρίς τον σχετικό κανόνα. Συνεπώς, η παραμετροποίηση των αρχείων καταγραφής στην πλατφόρμα Wazuh αποτελεί συνεργασία δύο συστημάτων. Η διαδικασία αυτή αποτέλεσε βασικό σημείο της υλοποίησης και αποδείχθηκε πρακτικά πως η μορφή του αρχείου καταγραφής επηρεάζει την επιτυχία της ανίχνευσης.

Πίνακας 3.4: Ροή λειτουργίας αποκωδικοποιητών και κανόνων της υλοποίησης

A/A	Βήμα	Είσοδος	Έξοδος	Ρόλος
1	Προ-αποκωδικοποίηση	Ακατέργαστη syslog εγγραφή	Hostname, program_name, timestamp	Βασική ταξινόμηση εγγραφής
2	Αποκωδικοποίηση	Σώμα εγγραφής	Δομημένα πεδία	Προετοιμασία για εφαρμογή κανόνων
3	Αξιολόγηση κανόνων	Πεδία αποκωδικοποίησης	Rule.id, rule.level, Rule description	Ανίχνευση και κατηγοροποίηση
4	Οπτικοποίηση	Ειδοποιήσεις	Discover/ Threat Hunting	Διερεύνηση από τον αναλυτή

3.7.4 Μεθοδολογία ανάπτυξης και επαλήθευσης

Για την επιβεβαίωση της ορθής λειτουργίας του μηχανισμού, πραγματοποιήθηκε έλεγχος με επαναληπτική διαδικασία. Στόχος ήταν να ελεγχθεί ότι τα αρχεία καταγραφής των πλοίων, μπορούν να αποκωδικοποιηθούν και να αξιοποιηθούν από τους κανόνες ανίχνευσης.

Ως κεντρική πηγή του συνόλου δεδομένων χρησιμοποιήθηκε το αρχείο που είχε δημιουργηθεί /var/log/vessel/vsrx.log. Η διασύνδεση του αρχείου με την πλατφόρμα wazuh έγινε μέσω του αρχείου ossec.conf και με τη χρήση του μηχανισμού localfile, έναν μηχανισμό ο οποίος παρακολουθεί και μεταφέρει δεδομένα σε πραγματικό χρόνο. Η ρύθμιση αυτή επέτρεψε και διασφάλισε την άμεση διοχέτευση των δεδομένων στον μηχανισμό ανάλυσης με στόχο την επεξεργασία των εγγραφών ως εισερχόμενη ροή τύπου Syslog. Για το πειραματικό στάδιο χρησιμοποιήθηκε το σενάριο κειμένου (script), το οποίο ονομάστηκε generate_logs.sh. Σκοπός ήταν η παραγωγή δοκιμαστικών εγγραφών προσομοιώνοντας τη δομή των πραγματικών αρχείων καταγραφής. Η σωστή καταγραφή τους στο αρχείο εισόδου επιβεβαιώθηκαν από την εντολή:

```
Sudo tail -f /var/log/vessel/vsrx.log
```

Αυτό ήταν απαραίτητο βήμα για τη διασφάλιση ελέγχου στο περιβάλλον προσομοίωσης, καθώς επιτρέπει τον αξιόπιστο έλεγχο των επόμενων σταδίων της αποκωδικοποίησης. Στη συνέχεια του ελέγχου, χρησιμοποιήθηκε το εργαλείο wazuh-logtest. Είναι ένα εργαλείο το οποίο εξετάζει αν μια ενδεικτική γραμμή καταγραφής ταιριάζει με κάποιον από τους διαθέσιμους αποκωδικοποιητές, ποια πεδία εξάγονται και εάν ενεργοποιείται κάποιος κανόνας.

Η μεθοδολογία αυτή υπήρξε μέγιστης σημασίας στην παρούσα υλοποίηση. Ο διαχωρισμός των σταδίων της διαδικασίας επέτρεψε την άμεση εύρεση οποιουδήποτε προβλήματος. Έτσι, ήταν γνωστό αν για παράδειγμα, μια εγγραφή εμφανίζεται στο αρχείο αλλά όχι στην πλατφόρμα, ότι το πρόβλημα αφορά τη συλλογή. Αντίστοιχα αν εμφανίζεται στην πλατφόρμα αλλά δεν αποκωδικοποιείται, ότι αφορά τον αποκωδικοποιητή. Ενώ τέλος, αν δεν παράγεται η σχετική ειδοποίηση τότε το πρόβλημα αφορά τον συγκεκριμένο κανόνα.

Κεφάλαιο 4ο: Αποτελέσματα και πειραματική αξιολόγηση

4.1 Στόχος αξιολόγησης

Η παρούσα ενότητα έχει ως στόχο να παρουσιάσει τον τρόπο με τον οποίο έγινε η αξιολόγηση του προτεινόμενου συστήματος. Αρχικά, θα οριστεί το αντικείμενο της αξιολόγησης και ο τρόπος ανάλυσης της. Στη συνέχεια, θα παρουσιαστούν τα κριτήρια, τα τεκμήρια αλλά και τα σενάρια δοκιμών που εφαρμόστηκαν για την επιβεβαίωση των αποτελεσμάτων λειτουργίας του συστήματος.

4.1.1 Αντικείμενο αξιολόγησης

Αρχικά, καθορίζεται το αντικείμενο της πειραματικής αξιολόγησης. Η αξιολόγηση δεν αποσκοπεί να εξετάσει γενικά την πλατφόρμα Wazuh, αλλά τη συγκεκριμένη προτεινόμενη υλοποίηση διαχείρισης πληροφοριών και συμβάντων ασφάλειας στη ναυτιλία, η οποία αποτελεί το πρακτικό αντικείμενο της παρούσας εργασίας. Εξετάζει αν η αναπτυγμένη υποδομή μπορεί να συλλέξει, να επεξεργαστεί, να αναλύσει και να παρουσιάσει δεδομένα ασφαλείας από διάφορες πηγές, μέσα από ομοιογενείς και επαναλαμβανόμενες ροές λειτουργίας.

Η αξιολόγηση αναλύεται σε τέσσερις βασικούς άξονες. Ο πρώτος άξονας μελετά τη συλλογή δεδομένων από το τερματικό σύστημα Windows μέσω του πράκτορα Wazuh και των συμπληρωματικών καταγραφών τερματικού. Ο δεύτερος άξονας εστιάζει στην εισαγωγή εξωτερικών αρχείων καταγραφής τύπου Syslog, τα οποία ακολουθούν τη μορφή καταγραφής vSRX. Ο τρίτος άξονας ελέγχει την αποκωδικοποίηση των εγγραφών και την εξαγωγή των δομημένων πεδίων, προκειμένου τα δεδομένα να καθίστανται αναζητήσιμα, να επιδέχονται φιλτράρισμα και να αξιοποιούνται αποτελεσματικά από τους μηχανισμούς κανόνων. Ο τέταρτος άξονας επικεντρώνεται στην ενεργοποίηση κανόνων ανίχνευσης, οι οποίοι οδηγούν στην παραγωγή ειδοποιήσεων και συνοδεύονται από επίπεδο σοβαρότητας και περιγραφικά στοιχεία.

Αξίζει να επισημανθεί η διάκριση μεταξύ της απλής εμφάνισης ενός συμβάντος από την παραγωγή μιας πλήρους ειδοποίησης ασφαλείας. Ένα συμβάν, ενδεχομένως να εμφανίζεται στο διερευνητικό περιβάλλον ως καταγεγραμμένη δραστηριότητα, χωρίς να έγκειται απαραίτητα ως απειλή. Αντιθέτως, η ειδοποίηση παράγεται μόνο όταν το συμβάν πληροί ορισμένες συνθήκες και εμπλουτίζεται από μεταδεδομένα, όπως το αναγνωριστικό του κανόνα που ενεργοποιήθηκε, το επίπεδο σοβαρότητας του και η σχετική περιγραφή του. Η διάκριση αυτή κρίνεται κρίσιμη, καθώς ένα σύστημα το οποίο παράγει πολλά συμβάντα αλλά λίγες ουσιαστικές ειδοποιήσεις είναι πιο χρήσιμο από ένα που πλημμυρίζει τον αναλυτή με ειδοποιήσεις χαμηλής σημασίας, καθιστώντας δύσκολο τον πραγματικό εντοπισμό των απειλών.

Τέλος, λόγω του ναυτιλιακού προσανατολισμού της εργασίας, αξιολογούνται και οι πρακτικές παράμετροι λειτουργίας. Για παράδειγμα, η κατανάλωση των υπολογιστικών πόρων και η δυνατότητα τοπικής λειτουργίας χωρίς συνεχή εξάρτηση από το διαδίκτυο για τη συλλογή καταγραφών. Το ζητούμενο στο παρόν στάδιο, δεν είναι να αποδειχθεί ότι το σύστημα αποτελεί πλήρες επιχειρησιακό κέντρο ασφαλείας. Η αρχιτεκτονική που επιλέχθηκε το καθιστά ικανό να εξελιχθεί προς αυτή την κατεύθυνση, καθώς μπορεί να λειτουργήσει ως κέντρο συλλογής, αποθήκευσης και διερεύνησης συμβάντων, προσαρμοσμένο στις πραγματικές ανάγκες και τους περιορισμούς της ναυτιλίας.

4.1.2 Κριτήρια και τεκμήρια επαλήθευσης

Η επιλογή των κριτηρίων αξιολόγησης δεν υπήρξε τυχαία. Καλείται να αντικατοπτρίσει τις πραγματικές απαιτήσεις ενός συστήματος, προοριζόμενο για χρήση στη ναυτιλιακή βιομηχανία. Τα πρώτα τέσσερα κριτήρια, εστιάζουν στην ορθή λειτουργία της βασικής ροής των δεδομένων. Δίχως αυτά οποιαδήποτε άλλη αξιολόγηση δεν έχει νόημα. Τα επόμενα δύο, σχετίζονται με αξιολόγηση του συστήματος στην παραγωγή χρήσιμης πληροφορίας και την τελική αξιοποίηση από τον χρήστη. Στο τέλος, η αξιολόγηση εμπίπτει στο πεδίο της ναυτιλίας. Τα κριτήρια της κατανάλωσης πόρων και της λειτουργίας περιορισμένης συνδεσιμότητας αποκτούν ιδιαίτερη βαρύτητα, καθώς η συνδεσιμότητα δεν είναι δεδομένη και το υλικό συχνά είναι περιορισμένο.

Πίνακας 4.1: Κριτήρια αξιολόγησης του συστήματος

A/A	Κριτήριο	Έλεγχος
1	Σύνδεση τερματικού	Ενεργοποίηση πράκτορα και επικοινωνία με εξυπηρετητή
2	Εμφάνιση συμβάντων	Εμφάνιση των συμβάντων στον πίνακα διερεύνησης
3	Επιτυχής αποκωδικοποίηση	Έλεγχος μετατροπής ακατέργαστου κειμένου σε δομημένα πεδία
4	Ενεργοποίηση κανόνων	Επαλήθευση αναγνώρισης συγκεκριμένων μοτίβων
5	Παραγωγή ειδοποιήσεων	Έλεγχος παραγωγής ειδοποιήσεων
6	Κατανάλωση πόρων	Μετρήσεις επίδρασης του συστήματος στο τερματικό υπό φορτίο
7	Λειτουργία περιορισμένης συνδεσιμότητας	Έλεγχος τοπικής αποθήκευσης δεδομένων εκτός σύνδεσης
8	Δυνατότητα διερεύνησης	Δυνατότητα του χρήστη να εκτελεί αναζητήσεις

Για κάθε έλεγχο που αναφέρεται στον Πίνακα 4.1, παρουσιάζονται στις επόμενες ενότητες τα αντίστοιχα τεκμήρια, όπως στιγμιότυπα από το περιβάλλον διαχείρισης, πεδία συμβάντων, ειδοποιήσεις και μετρήσεις. Στα σημεία που εντοπίζονται ευαίσθητες πληροφορίες, όπως διαπιστευτήρια ή εσωτερικές διευθύνσεις οι οποίες δεν είναι απαραίτητες για την τεκμηρίωση, αυτές αποκρύπτονται. Με αυτόν τον τρόπο, η αξιολόγηση παραμένει επαληθεύσιμη χωρίς την έκθεση των ευαίσθητων στοιχείων της υποδομής.

4.1.3 Μεθοδολογία και σενάρια δοκιμών

Η μεθοδολογία αξιολόγησης οργανώθηκε από συγκεκριμένα σενάρια δοκιμών. Εξετάζεται η σταδιακή λειτουργία του συστήματος, από το βασικό επίπεδο σύνδεσης και συλλογής δεδομένων, έως το τελικό επίπεδο παραγωγής ειδοποιήσεων. Κάθε σενάριο περιλαμβάνει συγκεκριμένη είσοδο, συγκεκριμένη διαδικασία ελέγχου και αναμενόμενο αποτέλεσμα, με στόχο την καθαρή αποτύπωση της λειτουργίας της υλοποίησης.

Στο πρώτο σενάριο εξετάστηκε η σύνδεση του τερματικού συστήματος των Windows. Στόχος ήταν ο πράκτορας να λειτουργεί, επικοινωνεί με τον κεντρικό εξυπηρετητή και εμφανίζεται ως ενεργός στο περιβάλλον διαχείρισης της πλατφόρμας. Αναμενόμενο αποτέλεσμα είναι η αναγνώριση του τερματικού και η εμφάνιση πρόσφατων συμβάντων.

Στη συνέχεια, εξετάστηκε η εισαγωγή εξωτερικών καταγραφών δικτυακής κίνησης. Η διαδικασία αυτή περιλαμβάνει την τροφοδότηση του αρχείου `/var/log/vessel/vsrx.log`, με νέες εγγραφές και την επιβεβαίωση της εμφάνισής τους στον περιβάλλον της διερεύνησης. Αναμενόμενο αποτέλεσμα ήταν η εμφάνιση των εγγραφών ως συμβάντα και η δημιουργία δομημένων πεδίων, μέσω της χρήσης αποκωδικοποιητών.

Έπειτα, ελέγχθηκε η αποκωδικοποίηση και η ενεργοποίηση των κανόνων. Πρέπει να επιβεβαιώνεται ότι οι νέες εγγραφές μπορούν να μετατρέπονται σε δομημένη πληροφορία και να ενεργοποιούν τους αντίστοιχους κανόνες ανίχνευσης. Ως αποτέλεσμα, αναμένεται η εμφάνιση πεδίων όπως το αναγνωριστικό, το επίπεδο σοβαρότητας και η περιγραφή, καθώς και η παραγωγή ειδοποίησης όπου υπάρχει κατάλληλη αντιστοίχιση.

Κρίσιμο σενάριο αποτέλεσε η αξιολόγηση της κατανάλωσης των πόρων, τόσο στην τυπική λειτουργία του συστήματος όσο και στη λειτουργία υπό αυξημένο φορτίο. Οι μετρήσεις πραγματοποιήθηκαν σε κατάσταση κανονικής λειτουργίας και επαναλαμβανόταν σε περιπτώσεις που το σύστημα δεχόταν αυξημένο ρυθμό εισαγωγής δεδομένων. Στόχος ήταν η αποτύπωση συγκριτικών τιμών χρήσης επεξεργαστή, μνήμης και δίσκου για την αξιολόγηση της πρακτικής επιβάρυνσης της υποδομής.

Τέλος, εξετάστηκε η λειτουργία σε συνθήκες περιορισμένης συνδεσιμότητας. Το βασικό σημείο της αξιολόγησης είναι ότι η συλλογή και η αποθήκευση συμβάντων μπορούν να συνεχιστούν τοπικά, χωρίς την εξάρτηση από εξωτερικές υπηρεσίες. Σε περιπτώσεις απουσίας σύνδεσης, η διερεύνηση μπορεί να πραγματοποιηθεί τοπικά στο περιβάλλον του πλοίου, από τον χειριστή. Όταν η σύνδεση αποκατασταθεί, μπορεί να καταστεί δυνατή η απομακρυσμένη πρόσβαση από τον αναλυτή ή και ο συγχρονισμός των διαθέσιμων δεδομένων, ανάλογα με την τελική επιχειρησιακή διαμόρφωση.

4.2 Αποτελέσματα λειτουργικότητας της υποδομής

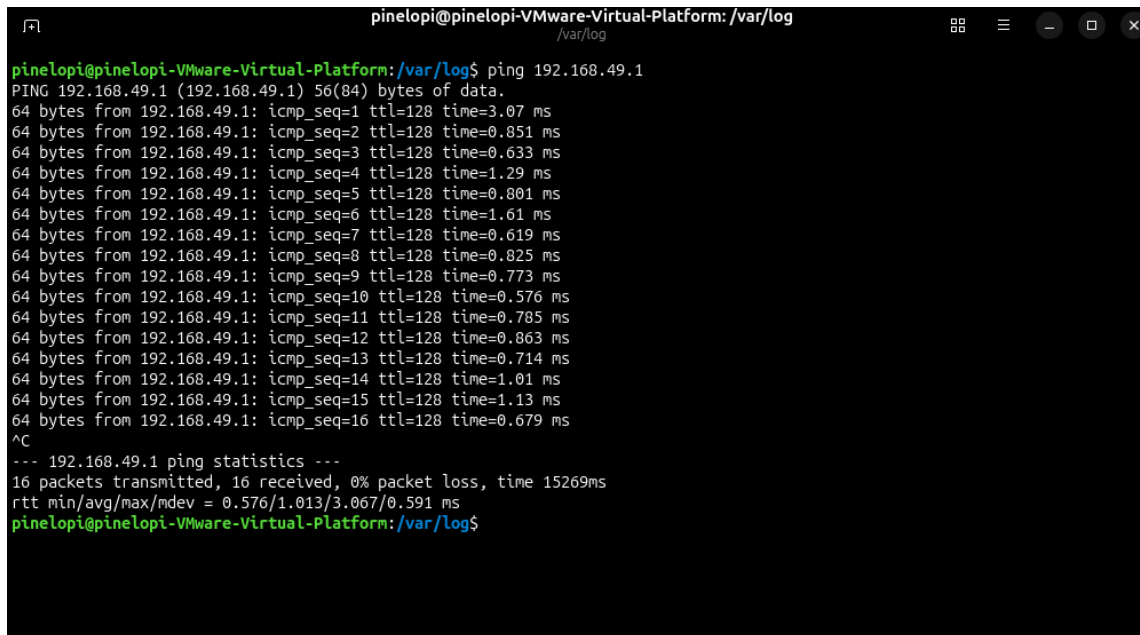
Στην παρούσα ενότητα παρουσιάζονται και τεκμηριώνονται τα βασικά αποτελέσματα λειτουργικότητας της υλοποίησης. Συγκεκριμένα, επιβεβαιώνεται η επιτυχής σύνδεση του τερματικού συστήματος, καθώς και η συλλογή δεδομένων, η αποκωδικοποίηση εγγράφων και η εμφάνιση των πληροφοριών σε δομημένα πεδία μέσα από το περιβάλλον διαχείρισης. Με τον τρόπο αυτό, τεκμηριώνεται η ορθή λειτουργία της βασικής ροής του συστήματος, πριν από την αναλυτικότερη διερεύνηση των παραγόμενων ειδοποιήσεων.

4.2.1 Έλεγχος δικτυακής συνδεσιμότητας

Σε αρχικό στάδιο, πραγματοποιήθηκε ο έλεγχος της επικοινωνίας μεταξύ του τερματικού συστήματος και του εξυπηρετητή του Wazuh. Η επιβεβαίωση αυτή είναι θεμελιώδης, καθώς η υποδομή πρέπει να είναι σε θέση να υποστηρίξει την αποστολή των συμβάντων από τον πράκτορα, προς τον κεντρικό κόμβο του συστήματος. Η αποτελεσματική παρακολούθηση των τερματικών προϋποθέτει μια σταθερή σύνδεση με τον διακομιστή, μέσω των κατάλληλων θυρών του δικτύου.

Ο πρώτος έλεγχος διεξήχθη από την πλευρά του εξυπηρετητή. Πραγματοποιήθηκε από την εικονική μηχανή Ubuntu, μέσω του πρωτοκόλλου μηνυμάτων ελέγχου διαδικτύου (Internet Control Message Protocol - ICMP), προς το κεντρικό σύστημα Windows με εσωτερική διεύθυνση IP 192.168.49.1. Ο

έλεγχος υλοποιήθηκε με τη χρήση της εντολής ping. Η επιτυχία της διαδικασίας, επιβεβαιώνεται από τη λήψη των απαντήσεων, με μηδενική απώλεια πακέτων (0% packet loss). Αυτό το γεγονός τεκμηριώνει τη λειτουργικότητα της διαδρομής IP μεταξύ των δύο κόμβων στο υποδίκτυο και τη ενεργή κατάσταση του εσωτερικού καναλιού της επικοινωνίας.



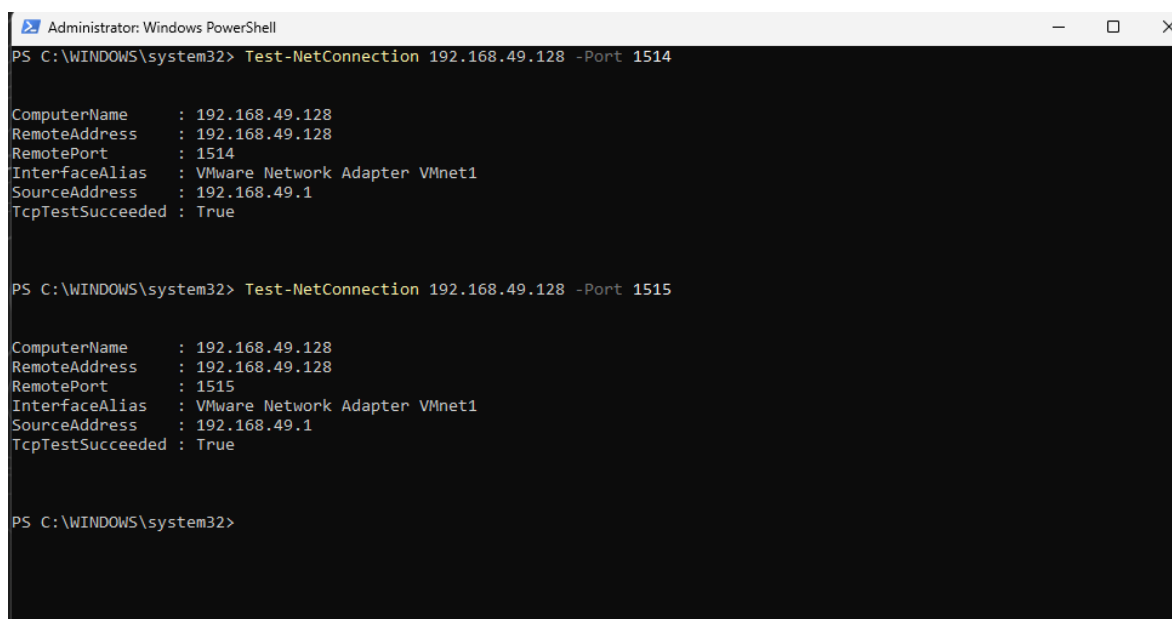
```

pinelopi@pinelopi-VMware-Virtual-Platform: /var/log
pinelopi@pinelopi-VMware-Virtual-Platform: /var/log$ ping 192.168.49.1
PING 192.168.49.1 (192.168.49.1) 56(84) bytes of data.
64 bytes from 192.168.49.1: icmp_seq=1 ttl=128 time=3.07 ms
64 bytes from 192.168.49.1: icmp_seq=2 ttl=128 time=0.851 ms
64 bytes from 192.168.49.1: icmp_seq=3 ttl=128 time=0.633 ms
64 bytes from 192.168.49.1: icmp_seq=4 ttl=128 time=1.29 ms
64 bytes from 192.168.49.1: icmp_seq=5 ttl=128 time=0.801 ms
64 bytes from 192.168.49.1: icmp_seq=6 ttl=128 time=1.61 ms
64 bytes from 192.168.49.1: icmp_seq=7 ttl=128 time=0.619 ms
64 bytes from 192.168.49.1: icmp_seq=8 ttl=128 time=0.825 ms
64 bytes from 192.168.49.1: icmp_seq=9 ttl=128 time=0.773 ms
64 bytes from 192.168.49.1: icmp_seq=10 ttl=128 time=0.576 ms
64 bytes from 192.168.49.1: icmp_seq=11 ttl=128 time=0.785 ms
64 bytes from 192.168.49.1: icmp_seq=12 ttl=128 time=0.863 ms
64 bytes from 192.168.49.1: icmp_seq=13 ttl=128 time=0.714 ms
64 bytes from 192.168.49.1: icmp_seq=14 ttl=128 time=1.01 ms
64 bytes from 192.168.49.1: icmp_seq=15 ttl=128 time=1.13 ms
64 bytes from 192.168.49.1: icmp_seq=16 ttl=128 time=0.679 ms
^C
--- 192.168.49.1 ping statistics ---
16 packets transmitted, 16 received, 0% packet loss, time 15269ms
rtt min/avg/max/mdev = 0.576/1.013/3.067/0.591 ms
pinelopi@pinelopi-VMware-Virtual-Platform: /var/log$

```

Σχήμα 4.1: Επιβεβαίωση δικτυακής συνδεσιμότητας με χρήση της εντολής ping

Έπειτα, πραγματοποιήθηκε έλεγχος της προσβασιμότητας των κρίσιμων θυρών από την πλευρά του τερματικού. Μέσω του περιβάλλοντος γραμμής εντολών PowerShell και με δικαιώματα διαχειριστή, εκτελέστηκε η εντολή Test-NetConnection προς την εσωτερική διεύθυνση IP 192.168.49.128 στις θύρες 1514 και 1515. Το αποτέλεσμα True και στις δύο περιπτώσεις, τεκμηριώνει ότι οι υπηρεσίες οι οποίες σχετίζονται με την επικοινωνία του πράκτορα είναι διαθέσιμες σε επίπεδο δικτύου και ο διακομιστής προσβάσιμος μέσω του πρωτοκόλλου ελέγχου μεταφοράς (Transmission Control Protocol- TCP) στο υποδίκτυο.



```

Administrator: Windows PowerShell
PS C:\WINDOWS\system32> Test-NetConnection 192.168.49.128 -Port 1514

ComputerName      : 192.168.49.128
RemoteAddress     : 192.168.49.128
RemotePort        : 1514
InterfaceAlias    : VMware Network Adapter VMnet1
SourceAddress     : 192.168.49.1
TcpTestSucceeded  : True

PS C:\WINDOWS\system32> Test-NetConnection 192.168.49.128 -Port 1515

ComputerName      : 192.168.49.128
RemoteAddress     : 192.168.49.128
RemotePort        : 1515
InterfaceAlias    : VMware Network Adapter VMnet1
SourceAddress     : 192.168.49.1
TcpTestSucceeded  : True

PS C:\WINDOWS\system32>

```

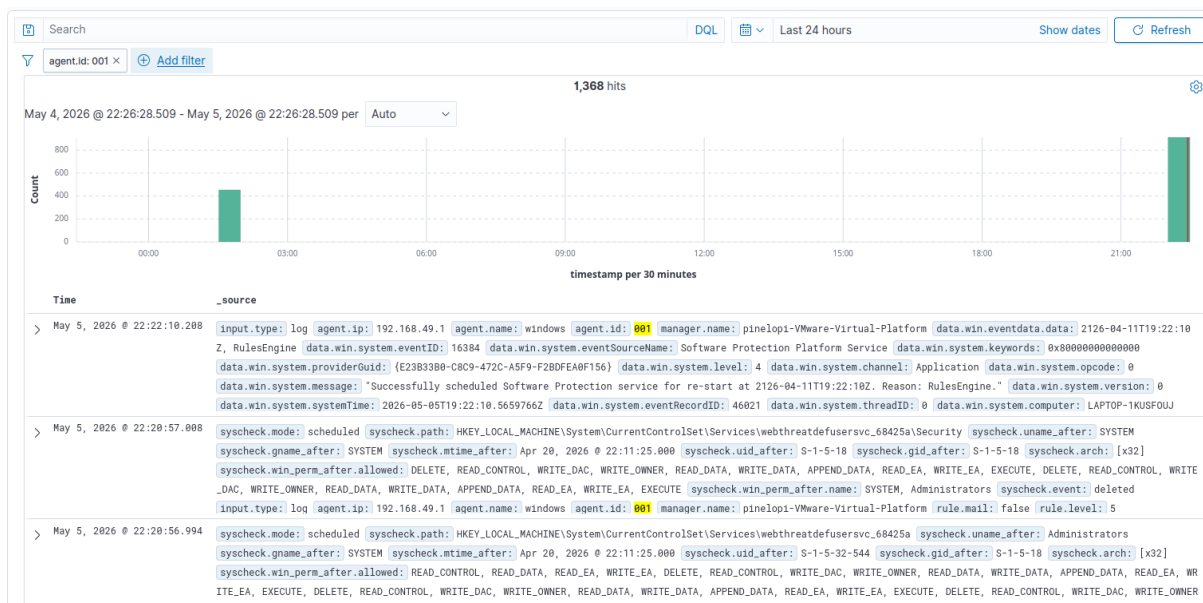
Σχήμα 4.2: Έλεγχος διαθεσιμότητας των κρίσιμων θυρών στον εξυπηρετητή

4.2.2 Εμφάνιση συμβάντων στον πίνακα ελέγχου

Σε συνέχεια της επιτυχημένης σύνδεσης του τερματικού, τεκμηριώνεται ότι τα δεδομένα που συλλέγονται μεταφέρονται και εμφανίζονται σωστά στον κεντρικό εξυπηρετητή. Επισημαίνεται ότι η απλή εμφάνιση των συμβάντων στον πίνακα ελέγχου δεν συνεπάγεται απαραίτητα με την ανίχνευση απειλής. Παρόλα αυτά, αποτελεί απαραίτητη προϋπόθεση για τα επόμενα στάδια της υλοποίησης και της τελικής ανάλυσης.

Ο έλεγχος πραγματοποιήθηκε από τον πίνακα ελέγχου του Wazuh και συγκεκριμένα από το περιβάλλον της διερεύνησης συμβάντων (Discover). Εκεί επιβεβαιώθηκε η εμφάνιση των πρόσφατων εγγραφών, οι οποίες αντιστοιχούν χρονικά στις δοκιμές που πραγματοποιήθηκαν. Παράλληλα, σε κάθε συμβάν εμφανίζονται μεταδεδομένα που βοηθάνε στην αναγνώριση της πηγής προέλευσης. Με τον τρόπο αυτό, ο αναλυτής έχει τη δυνατότητα να εφαρμόσει φίλτρα ταξινόμησης αλλά και να απομονώσει τα συμβάντα που προέρχονται από μία συγκεκριμένη πηγή.

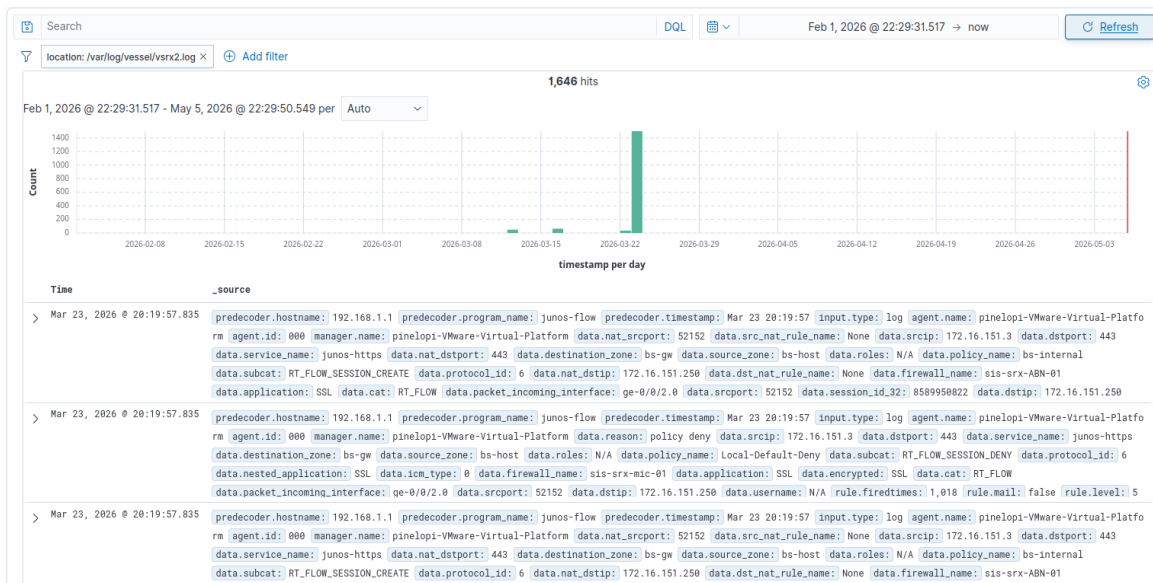
Στο Σχήμα 4.3 παρουσιάζεται παράδειγμα εμφάνισης της ροής συμβάντων, που προέρχονται από τον πράκτορα του τερματικού συστήματος Windows. Η διάκριση των εγγραφών, επιτεύχθηκε μέσω της παραμέτρου ταυτοποίησης agent.id: 001, η οποία αναφέρεται στον συγκεκριμένο πράκτορα. Τα πεδία agent.name, agent.ip και manager.name επιβεβαιώνουν ότι το τερματικό έχει ενταχθεί και λειτουργικά στην υποδομή παρακολούθησης.



Σχήμα 4.3: Εμφάνιση και ταξινόμηση συμβάντων από το τερματικό Windows

Αντίστοιχα, στο Σχήμα 4.4 επιβεβαιώνεται η εμφάνιση συμβάντων που προέρχονται από το αρχείο καταγραφής δεδομένων του τύπου Syslog. Η διάκριση των εγγραφών έγινε μέσω της παραμέτρου ταυτοποίησης location: /var/log/vessel/vsrx.log, η οποία επιβεβαιώνει ότι οι γραμμές που εισάγονται στο αρχείο αναγνωρίζονται ως συμβάντα. Η δυνατότητα αυτή είναι πολύ σημαντική, καθώς δείχνει ότι το σύστημα μπορεί να δεχθεί και εξωτερικές καταγραφές, πέρα από τη συλλογή δεδομένων μέσω πρακτόρων.

Στο στάδιο αυτό, στόχος είναι να επιβεβαιωθεί ότι τα δεδομένα φτάνουν στο σημείο όπου μπορούν να αναζητηθούν, να φιλτραριστούν και να αξιοποιηθούν από τους μηχανισμούς ανάλυσης. Η επιτυχής εμφάνιση των συμβάντων και από τις δύο πηγές, τεκμηριώνει την ικανότητα της υλοποίησης να παρέχει κεντρική ορατότητα στα δεδομένα που συλλέγει.



Σχήμα 4.4: Εμφάνιση συμβάντων από αρχείο καταγραφής Syslog

4.2.3 Επαλήθευση αποκωδικοποίησης

Μετά την εμφάνιση των δεδομένων, τεκμηριώθηκε ότι οι εγγραφές δεν εμφανίζονται μόνο ως απλά ακατέργαστο κείμενο. Συγκεκριμένα, πρέπει να μπορούν να αναλυθούν από την πλατφόρμα και να μετατραπούν σε δομημένη πληροφορία. Η αποκωδικοποίηση αποτελεί ιδιαίτερα σημαντικό στάδιο για έναν αναλυτή, καθώς του επιτρέπει να φιλτράρει και να συσχετίζει συμβάντα χωρίς να ξεετάζει χειροκίνητα κάθε γραμμή της καταγραφής. Όπως έχει ήδη αναφερθεί, η διαδικασία αποκωδικοποίησης αναγνωρίζει συγκεκριμένες μορφές καταγραφών και εξαγεί σε δομημένα πεδία. Αυτά τα πεδία, χρησιμοποιήθηκαν ως τεκμήριο ότι οι εγγραφές μετατρέπονται σε αξιοποιήσιμη για τον χρήστη πληροφορία.

† data.roles	N/A
† data.service_name	junos-https
† data.session_id_32	8589950822
† data.source_zone	bs-host
† data.src_nat_rule_name	None
† data.srcip	172.16.151.3
† data.srcport	52152
† data.subcat	RT_FLOW_SESSION_CREATE
† data.username	unauthenticated-user
† decoder.name	junos-rt-flow
† decoder.parent	junos-rt-flow
† full_log	>

Σχήμα 4.5: Επιτυχής αποκωδικοποίηση συμβάντος vSRX σε δομημένα πεδία

Όπως φαίνεται στο Σχήμα 4.5, μια εγγραφή από το σύνολο δεδομένων τύπου Vsrx, εμφανίζεται σε δομημένα πεδία. Ιδιαίτερα σημαντικό είναι το πεδίο `decoder.name` με τιμή `junos-rt-flow`, το οποίο μας δείχνει ότι η εγγραφή αντιστοιχίστηκε στον κατάλληλο αποκωδικοποιητή και αναγνωρίστηκε από την πλατφόρμα Wazuh ως συμβάν ροής δικτύου Junos.

Το ζητούμενο σε αυτό το στάδιο είναι να επιβεβαιωθεί ότι η πλατφόρμα μπορεί να μετατρέψει τις βασικές καταγραφές σε δομημένα πεδία, ώστε να εφαρμοστούν οι μηχανισμοί ανίχνευσης. Αυτό θεωρείται επιτυχής αποκωδικοποίηση. Δεν είναι απαραίτητο, στην παρούσα φάση υλοποίησης, ότι κάθε καταγραφή αποκωδικοποιείται πλήρως, καθώς αυτό εξαρτάται από τη μορφή της εγγραφής και τα κριτήρια που αναμένει ο αντίστοιχος αποκωδικοποιητής.

4.2.4 Επαλήθευση ανίχνευσης

Μετά την επιβεβαίωση της συλλογής και αποκωδικοποίησης, το επόμενο στάδιο αφορούσε την επιβεβαίωση της ανίχνευσης. Η πλατφόρμα δεν πρέπει να περιορίζεται μόνο στην καταγραφή των συμβάντων, αλλά να αξιολογεί μέσω των κανόνων ανίχνευσης του Wazuh. Η επιτυχία τεκμηριώνεται όταν ένα συμβάν αντιστοιχίζεται σε συγκεκριμένο κανόνα. Επίσης, συνοδεύεται από πληροφορίες όπως το αναγνωριστικό του κανόνα, η περιγραφή του και το επίπεδο της σοβαρότητας.

Για την επιβεβαίωση της διαδικασίας, αρχικά πραγματοποιήθηκε έλεγχος στο επίπεδο του εξυπηρετητή μέσω του αρχείου `/var/ossec/logs/alerts/alerts.json`. Ως παράδειγμα, όπως φαίνεται στο Σχήμα 4.6, παρουσιάζεται ένα συμβάν που προέρχεται από το τερματικό σύστημα των Windows. Η εγγραφή περιλαμβάνει στοιχεία όπως το επίπεδο σοβαρότητας σε βαθμό 12, η περιγραφή του κανόνα που ενεργοποιήθηκε, η συσχέτιση του με το πλαίσιο MITRE ATT&CK και πληροφορίες σχετικά με τον πράκτορα που παρήγαγε το συγκεκριμένο συμβάν. Τα πεδία αυτά, επιβεβαιώνουν ότι το συμβάν πέρασε από τον μηχανισμό ανάλυσης και αξιολογήθηκε από τους κανόνες ανίχνευσης.

```

{"timestamp": "2026-05-06T17:24:40.047+0300", "rule": {"level": 12, "description": "Application Compatibility Database launched", "id": "92058", "mitre": {"id": "T1546.011", "tactic": ["Privilege Escalation", "Persistence"], "technique": ["Application Shimming"]}, "firedtimes": 1, "mail": true, "groups": ["sysmon", "sysmon_eid1_detections", "windows"]}, "agent": {"id": "001", "name": "windows", "ip": "192.168.49.1"}, "manager": {"name": "pinelopi-VMware-Virtual-Platform"}, "id": "1778077480.577955", "decoder": {"name": "windows_eventchannel"}, "data": {"win": {"system": {"providerName": "Microsoft-Windows-Sysmon", "providerGuid": "{5770385f-c22a-43e0-bf4c-06f5698ffbd9}", "eventId": "1", "version": "5", "level": "4", "task": "1", "opcode": "0", "keywords": "0x8000000000000000", "systemTime": "2026-05-06T13:10:03.3654038Z", "eventRecordID": "157868", "processID": "5760", "threadID": "7420", "channel": "Microsoft-Windows-Sysmon/Operational", "computer": "LAPTOP-1KUSFOUJ", "severityValue": "INFORMATION", "message": "\Process Create:\r\nRuleName: -\r\nUtcTime: 2026-05-06 13:10:03.356\r\nProcessGuid: {e22a2579-3dab-69fb-25a4-000000002800}\r\nProcessId: 23016\r\nImage: C:\\Windows\\System32\\sdbinst.exe\r\nFileVersion: 10.0.26100.8115 (WinBuild.160101.0800)\r\nDescription: Application Compatibility Database Installer\r\nProduct: Microsoft® Windows® Operating System\r\nCompany: Microsoft Corporation\r\nOriginalFileName: sdbinst.exe\r\nCommandLine: C:\\WINDOWS\\System32\\sdbinst.exe -m -bg\r\nCurrentDirectory: C:\\WINDOWS\\system32\\r\nUser: NT AUTHORITY\\SYSTEM\r\nLogonGuid: {e22a2579-a614-69e5-e703-000000000000}\r\nLogonId: 0x3E7\r\nTerminalSessionId: 0\r\nIntegrityLevel: System\r\nHashes: SHA256=96102A4A9BED71B42AF5D910942306DAFA296621D2954AFEF3A994563F14420E\r\nParentProcessGuid: {e22a2579-a690-69e5-bf01-000000002800}\r\nParentProcessId: 7868\r\nParentImage: C:\\Windows\\System32\\svchost.exe\r\nParentCommandLine: C:\\WINDOWS\\system32\\svchost.exe -k LocalSystemNetworkRestricted -p -s PcaSvc\r\nParentUser: NT AUTHORITY\\SYSTEM"}, "eventdata": {"utcTime": "2026-05-06 13:10:03.356", "processGuid": "{e22a2579-3dab-69fb-25a4-000000002800}", "processId": "23016", "image": "C:\\\\Windows\\\\\\System32\\\\\\sdbinst.exe", "fileVersion": "10.0.26100.8115 (WinBuild.160101.0800)", "description": "Application Compatibility Database Installer", "product": "Microsoft® Windows® Operating System", "company": "Microsoft Corporation", "originalFileName": "sdbinst.exe", "commandLine": "C:\\\\WINDOWS\\\\\\System32\\\\\\sdbinst.exe -m -bg", "currentDirectory": "C:\\\\WINDOWS\\\\\\System32\\\\\\", "user": "NT AUTHORITY\\\\\\SYSTEM", "logonGuid": "{e22a2579-a614-69e5-e703-000000000000}", "logonId": "0x3e7", "terminalSessionId": "0", "integrityLevel": "System", "hashes": "SHA256=96102A4A9BED71B42AF5D910942306DAFA296621D2954AFEF3A994563F14420E", "parentProcessGuid": "{e22a2579-a690-69e5-bf01-000000002800}", "parentProcessId": "7868", "parentImage": "C:\\\\Windows\\\\\\System32\\\\\\svchost.exe", "parentCommandLine": "C:\\\\WINDOWS\\\\\\System32\\\\\\svchost.exe -k LocalSystemNetworkRestricted -p -s PcaSvc", "parentUser": "NT AUTHORITY\\\\\\SYSTEM"}}, "location": "EventChannel"}

```

Σχήμα 4.6: Καταγραφή ειδοποίησης στο αρχείο `alerts.json` του Wazuh

Επιβεβαίωση πραγματοποιήθηκε και μέσα από το γραφικό περιβάλλον της πλατφόρμας, με πιο κατανοητό τρόπο για τον αναλυτή. Το ίδιο συμβάν εμφανίζεται και στον πίνακα ελέγχου με αναλυτικά πεδία που αφορούν τη διεργασία και το τερματικό σύστημα. Παράλληλα, εμφανίζονται και πεδία τύπου Sysmon, όπως εκείνα που ξεκινούν με data.win.eventdata. Τα στοιχεία αυτά επιτρέπουν στον αναλυτή όχι μόνο να επιβεβαιώσει την ορθή λειτουργία των κανόνων, αλλά και να αναγνωρίσει τη διεργασία που σχετίζεται με το συμβάν.

May 6, 2026 @ 17:24:40.847

input.type: log agent.ip: 192.168.49.1 agent.name: windows agent.id: 001 manager.name: pinelopi-Vmware-Virtual-Platform data.win.eventdata.originalFileName: sdbinst.exe data.win.eventdata.image: C:\\Windows\\System32\\sdbinst.exe data.win.eventdata.product: Microsoft Windows Operating System data.win.eventdata.parentProcessId: {e22a2579-a69b-69e5-bf01-000000002800} data.win.eventdata.description: Application Compatibility Database Installer data.win.eventdata.logonId: {e22a2579-a614-69e5-e703-000000000000} data.win.eventdata.parentCommandLine: C:\\WINDOWS\\system32\\svchost.exe -k LocalSystemNetworkRestricted -p -s PcsSvc data.win.eventdata.processId: {e22a2579-3dab-69fb-2544-000000002800} data.win.eventdata.logonId: b3e7 data.win.eventdata.parentProcessId: 7868 data.win.eventdata.processId: 23016 data.win.eventdata.currentDirectory: C:\\WINDOWS\\system32\\ data.win.eventdata.utcTime: 2026-05-06 13:10:03.356 data.win.eventdata.hashes: SHA256=96182AA498ED71842AF5D9109423860FA296621D2954AFE3A994563F14428E data.win.eventdata.parentImage: C:\\Windows\\System32\\svchost.exe data.win.eventdata.company: Microsoft Corporation

Expanded document

Table JSON

#_index	wazuh-alerts-4.x-2026.05.06
#agent.id	001
#agent.ip	192.168.49.1
#agent.name	windows
#data.win.eventdata.commandLine	C:\\WINDOWS\\System32\\sdbinst.exe -n -bg
#data.win.eventdata.company	Microsoft Corporation
#data.win.eventdata.currentDirectory	C:\\WINDOWS\\system32\\
#data.win.eventdata.description	Application Compatibility Database Installer
#data.win.eventdata.fileVersion	10.0.26100.8115 (WinBuild.160101.0800)
#data.win.eventdata.hashes	SHA256=96182AA498ED71842AF5D9109423860FA296621D2954AFE3A994563F14428E
#data.win.eventdata.image	C:\\Windows\\System32\\sdbinst.exe
#data.win.eventdata.integrityLevel	System

Σχήμα 4.7: Εμφάνιση ειδοποίησης και πεδίων Sysmon στον πίνακα ελέγχου Wazuh

Η επιτυχία της ανίχνευσης, να εντοπίζει και να μετασχηματίζει συμβάντα του τερματικού σε δομημένη πληροφορία, αναδεικνύεται έμπρακτα. Οι ειδοποιήσεις δεν αποτελούν απλές γραμμές καταγραφής, ενώ πλέον εμπλουτίζονται με τεχνικά δεδομένα, διαβαθμίσεις σοβαρότητας και παραμέτρους των κανόνων. Η προσέγγιση αυτή βοηθάει τον αναλυτή να αντιληφθεί άμεσα το πλαίσιο και την κρισιμότητα ενός περιστατικού. Η επιτυχία επιβεβαιώνεται σε διπλό επίπεδο, τόσο μέσω της αρχικής καταγραφής στο αρχείο alerts.json όσο και της οργανωμένης τελικής παρουσίας στον πίνακα ελέγχου του Wazuh.

4.3 Παραγωγή και ανάλυση ειδοποιήσεων

Η ενότητα που ακολουθεί, παρουσιάζει το περιεχόμενο των ειδοποιήσεων που παράγονται από το σύστημα, καθώς και τον τρόπο που αυτές αξιοποιούνται στη διερεύνηση, από τον αναλυτή. Έμφαση δεν δίνεται μόνο στην ύπαρξη των ειδοποιήσεων, αλλά και στα πεδία που τις συνοδεύουν, στα δεδομένα που αποδίδονται από τους κανόνες και στην τελική πληροφορία που εμφανίζεται.

4.3.1 Ενδεικτικές ειδοποιήσεις από τερματικό και σύνολο δεδομένων

Αρχικά, παρουσιάζεται το είδος των ειδοποιήσεων που παρήχθησαν από τις βασικές πηγές δεδομένων της συγκεκριμένης υλοποίησης. Εφόσον τεκμηριώθηκε η ενεργοποίηση των μηχανισμών και των κανόνων, πρέπει να δοθεί έμφαση και στο είδος της πληροφορίας που λαμβάνει ο αναλυτής, καθώς και στο πως αυτή διαφοροποιείται ανάλογα με την προέλευση που έχει το συμβάν. Μόνο με αυτόν τον τρόπο διαχωρίζεται η τεχνική επιβεβαίωση της λειτουργίας από την πρακτική αξία των αποτελεσμάτων.

Οι ειδοποιήσεις που αφορούν τη δραστηριότητα του λειτουργικού συστήματος προέρχονται από το τερματικό σύστημα των Windows. Ο πράκτορας συλλέγει συμβάντα και καταγραφές, οι οποίες εμπλουτίζονται από λεπτομερέστερες καταγραφές τερματικού, όπου αυτές είναι διαθέσιμες. Αυτού του τύπου οι ειδοποιήσεις είναι πολύ χρήσιμες, καθώς αναφέρονται σε ενέργειες εντός του ίδιου

συστήματος. Υποστηρίζουν παράλληλα τη διερεύνηση αλλαγών σε ρυθμίσεις, τυχόν μεταβολές σε αρχεία ή οποιοδήποτε άλλο γεγονός σχετίζεται με την ασφάλεια του τερματικού.

Οι ειδοποιήσεις οι οποίες αφορούν δικτυακή δραστηριότητα προέρχονται από το σύνολο δεδομένων VsrX. Συγκεκριμένα, περιγράφουν λειτουργίες όπως η δημιουργία μίας σύνδεσης, η απόρριψη της ή ο τερματισμός συνεδριών. Παρέχουν επίσης πληροφορίες για πηγές, προορισμούς, θύρες, υπηρεσίες και ζώνες δικτύου. Αποτελεί πολύ σημαντική κατηγορία, καθώς συμπληρώνει την εικόνα που προέρχεται από το τερματικό και προσφέρει ορατότητα στο επίπεδο της δικτυακής ροής.

Η συνδυαστική αξιοποίηση των δύο πηγών δείχνει ότι η πλατφόρμα μπορεί να παρέχει μια πιο ολοκληρωμένη εικόνα στον χειριστή. Οι ειδοποιήσεις από τα τερματικά βοηθάνε στην κατανόηση της δραστηριότητας μέσα στο σύστημα, ενώ οι ειδοποιήσεις δικτύου αποτυπώνουν τη συμπεριφορά δικτυακής επικοινωνίας. Η διαφοροποίηση αυτή είναι ιδιαίτερα σημαντική, καθώς στο περιβάλλον της ναυτιλίας συνυπάρχουν συστήματα διαφορετικής φύσης και απαιτείται μια κεντρική εικόνα των συμβάντων.

4.3.2 Ανάλυση περιεχομένου ειδοποίησης

Η ανάλυση των ειδοποιήσεων που παράγονται από την πλατφόρμα, αποτελεί κομβικό σημείο στη διαδικασία της απόκρισης σε περιστατικά ασφαλείας. Μια ειδοποίηση δεν αποτελεί μόνο ένδειξη κινδύνου. Είναι ένα σύνολο μεταδεδομένων, το οποίο επιτρέπει στον αναλυτή να απαντήσει πρακτικά ερωτήματα, όπως τι συνέβη, πού συνέβη, πότε συνέβη και ποιο σύστημα εμπλέκεται. Η προστιθέμενη αξία του συστήματος, έγκειται ακριβώς στη δυνατότητα του μετασχηματισμού των ακατέργαστων καταγραφών σε δομημένη πληροφορία διερεύνησης.

Για τη διευκόλυνση της συστηματικής εξέτασης των δεδομένων, στο περιβάλλον διερεύνησης του Wazuh, η πληροφορία που συνοδεύει κάθε ειδοποίηση μπορεί να ταξινομηθεί σε τρεις διακριτές κατηγορίες.

Η πρώτη κατηγορία αφορά το γενικό πλαίσιο της καταγραφής και παρέχει την αρχική εικόνα της εγγραφής. Σε αυτή περιλαμβάνονται στοιχεία όπως το χρονικό σημείο της καταγραφής, η μέθοδος με την οποία το συμβάν εισήχθη στο σύστημα και το αρχικό κείμενο της καταγραφής μέσω του πεδίου `full_log`. Τα στοιχεία αυτά δίνουν την πρώτη εικόνα της εγγραφής πριν από την επιμέρους ανάλυσή της.

Η δεύτερη κατηγορία αφορά τα μεταδεδομένα πηγής, τα οποία συσχετίζουν την ειδοποίηση με το σύστημα από το οποίο προήλθε. Τα βασικά πεδία περιλαμβάνουν στοιχεία όπως το αναγνωριστικό αριθμό του τερματικού (`agent.id`), το όνομα του τερματικού (`agent.name`) και τη διεύθυνση IP (`agent.ip`). Η πληροφορία αυτή θεωρείται κρίσιμη, καθώς επιτρέπει την ομαδοποίηση των δεδομένων ανά τερματικό, πράκτορα ή πηγής δεδομένων.

Η τρίτη κατηγορία αφορά τα μεταδεδομένα ανίχνευσης, δηλαδή τα στοιχεία που δείχνουν τον τρόπο με τον οποίο η πλατφόρμα ερμήνευσε και ταξινόμησε το συμβάν. Περιλαμβάνει πεδία όπως το είδος της καταγραφής που αναγνωρίστηκε (`decoder.name`), τον κανόνα που ενεργοποιήθηκε (`rule.id`), το επίπεδο σοβαρότητας (`rule.level`) και ποια περιγραφή δόθηκε στο συμβάν (`rule.description`). Πρακτικά, τα πεδία αυτά παρέχουν ταξινόμηση και εκτίμηση για το εάν και κατά πόσο μια δραστηριότητα μπορεί να σχετίζεται με απειλή.

Στο πλαίσιο αυτό, τα πεδία μίας ειδοποίησης εξετάζονται ως σύνολο. Η χρησιμότητά τους προκύπτει από το συνδυασμό της πηγής, του περιεχόμενου και του κανόνα. Ανάλογα με την προέλευση των δεδομένων, ορισμένα πεδία είναι πιο σημαντικά για ειδοποιήσεις από το τερματικό σύστημα, ενώ άλλα είναι πιο χρήσιμα στις καταγραφές τύπου vSRX.

Πίνακας 4.2: Ενδεικτικά πεδία ειδοποίησης και ρόλος τους στη διερεύνηση

A/A	Κατηγορία	Ενδεικτικά πεδία	Ρόλος στη διερεύνηση
1	Πλαίσιο συμβάντος	timestamp location full_log	Χρονική στιγμή, Προέλευση, Αρχικό μήνυμα
2	Πηγή	agent.id agent.name agent.ip	Συσχέτιση με τερματικό
3	Αποκωδικοποίηση	decoder.name	Αποκωδικοποιητής
4	Κανόνας	rule.id rule.level rule.description	Αποτελέσματα κανόνων
5	Πεδία τερματικού συστήματος	data.win.eventdata.image data.win.eventdata.commandLine data.win.eventdata.hashes	Στοιχεία Windows συμβάντος
6	Πεδία δικτυακής ροής	data.subcat, data.srcip, data.dstip, data.srcport, data.dstport	Τύπος ροής και τερματικής επικοινωνίας
7	Πλαίσιο πολιτικής και ζωνών	data.policy_name data.source_zone data.destination_zone	Πολιτική και κατεύθυνση επικοινωνίας

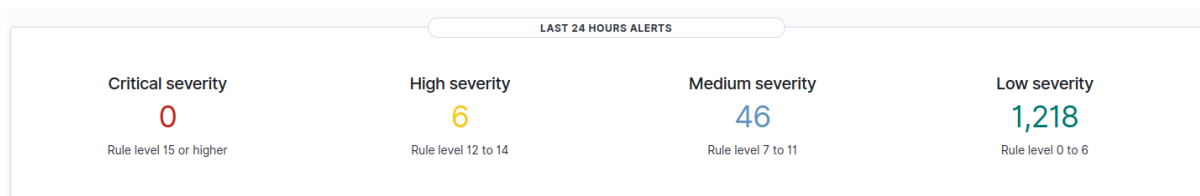
Ο πίνακας 4.2, δείχνει ότι μια ειδοποίηση δεν περιορίζεται μόνο στο επίπεδο σοβαρότητας. Η αξία της προκύπτει από τον συνδυασμό των πεδίων, όπως η περιγραφή της πηγής, το περιεχόμενο, ο κανόνας και το τεχνικό πλαίσιο. Από την ανάλυση φαίνεται ότι η πλατφόρμα Wazuh παρέχει ένα κοινό περιβάλλον διερεύνησης για διαφορετικές κατηγορίες δεδομένων. Επίσης, οι ειδοποιήσεις που προέρχονται από τερματικά απαντούν κυρίως στο τι συνέβη μέσα στο σύστημα, ενώ οι δικτυακές ειδοποιήσεις απαντούν στο ποια επικοινωνία πραγματοποιήθηκε και υπό ποιες συνθήκες. Από την ανάλυση περιεχομένου των ειδοποιήσεων, προκύπτει το συμπέρασμα ότι η συμπληρωματικότητα αυτή είναι ιδιαίτερα χρήσιμη σε περιβάλλον με ετερογενείς πηγές.

4.3.3 Αξιολόγηση επιπέδων σοβαρότητας

Η αξιολόγηση των επιπέδων σοβαρότητας χρησιμοποιείται για την εισαγωγή προτεραιότητας στις ειδοποιήσεις και την καλύτερη οργάνωση της διερεύνησης. Σε αυτή την πλατφόρμα, η σοβαρότητα αποτυπώνεται στο πεδίο rule.level, το οποίο αποδίδεται κατά την ενεργοποίηση του κανόνα. Έτσι, παρέχεται στον αναλυτή η δυνατότητα να διαχωρίζει τα συμβάντα που χρήζουν άμεσης προσοχής από εκείνα που έχουν περισσότερο πληροφοριακό χαρακτήρα.

Στον πίνακα ελέγχου του Wazuh, οι ειδοποιήσεις ταξινομούνται σε χαμηλής, μεσαίας, υψηλής και κρίσιμης σοβαρότητας. Στο Σχήμα 4.8, φαίνεται το χρονικό παράθυρο των τελευταίων είκοσι τεσσάρων ωρών. Στο συγκεκριμένο παράδειγμα καταγράφηκαν 0 κρίσιμες, 6 υψηλές, 46 μεσαίες και 1.218

χαμηλής σοβαρότητας ειδοποιήσεις. Η ύπαρξη μεγάλου αριθμού ειδοποιήσεων με χαμηλό επίπεδο σοβαρότητας είναι αναμενόμενη για περιβάλλον δοκιμών. Αρκετές από αυτές προέρχονται από φυσιολογικές λειτουργίες του συστήματος, όπως για παράδειγμα περιοδικοί έλεγχοι. Παράλληλα, η ύπαρξη ειδοποιήσεων υψηλότερης σοβαρότητας, επιβεβαιώνει ότι το σύστημα μπορεί να διαχωρίζει συμβάντα που απαιτούν μεγαλύτερη προσοχή, σύμφωνα με τους κανόνες που έχουν ενεργοποιηθεί.



Σχήμα 4.8: Κατανομή ειδοποιήσεων ανά επίπεδο σοβαρότητας στο Wazuh Dashboard

Συνολικά, η κατανομή αυτή δείχνει ότι το σύστημα δεν παρουσιάζει τις ειδοποιήσεις ως ενιαίο όγκο δεδομένων. Η αρχική αξιολόγηση οργανώνεται, με τρόπο που διευκολύνει τον αναλυτή στην αρχική αξιολόγηση. Οι υψηλότερες κατηγορίες, μπορούν να εξεταστούν αρχικά ενώ οι χαμηλότερες να χρησιμοποιηθούν υποστηρικτικά για την κατανόηση του πλαισίου ενός περιστατικού. Συνεπώς, η σοβαρότητα δεν αντιμετωπίζεται ως τελικό συμπέρασμα, αλλά ως πρακτικό εργαλείο της προτεραιότητας της διερεύνησης.

4.4 Απόδοση και λειτουργία σε περιορισμένο περιβάλλον

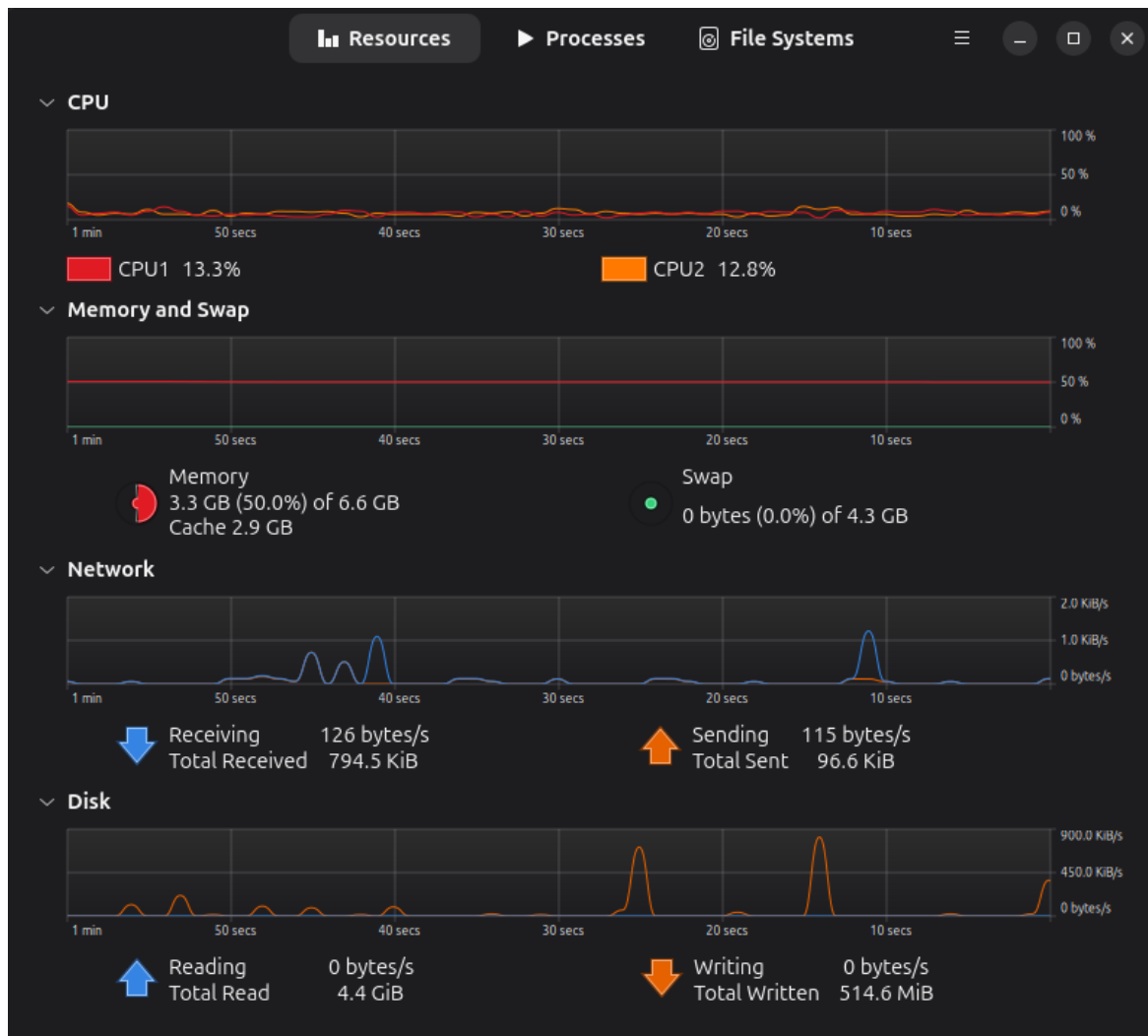
Ακολουθεί, η αξιολόγηση της συμπεριφοράς του συστήματος ως προς την κατανάλωση πόρων και τη λειτουργία της σε συνθήκες περιορισμένου περιβάλλοντος. Η αξιολόγηση εστιάζει τόσο σε τυπική λειτουργία όσο και σε συνθήκες αυξημένου φόρτου. Παράλληλα, εξετάζεται η συμπεριφορά της υποδομής σε απώλεια σύνδεσης στο διαδίκτυο.

4.4.1 Κατανάλωση πόρων σε τυπική λειτουργία

Σε πρώτη φάση, κρίθηκε σκόπιμο να καταγραφεί η κατανάλωση πόρων της εικονικής μηχανής σε συνθήκες τυπικής λειτουργίας της πλατφόρμας Wazuh. Ως τυπική λειτουργία, θεωρείται η κατάσταση κατά την οποία οι βασικές υπηρεσίες της πλατφόρμας είναι ενεργές και το περιβάλλον χρησιμοποιείται κανονικά, χωρίς εσκεμμένη αύξηση φόρτου. Σκοπός της μέτρησης, ήταν η αποτύπωση μιας βασικής εικόνας αναφοράς σχετικά με τις απαιτήσεις που χρειάζεται το σύστημα σε επεξεργαστή, μνήμη και αποθηκευτικό χώρο.

Η εικονική μηχανή δομείται από δύο εικονικούς επεξεργαστές, μνήμη RAM περίπου στα 7GB και αποθηκευτικό χώρο στα 60GB. Στην παρούσα εγκατάσταση ο εξυπηρετητής, ο ευρετηριαστής και ο πίνακας ελέγχου λειτουργούν ως ενιαίος κόμβος, γεγονός που επηρεάζει άμεσα τη συνολική απόκριση του συστήματος και τη κατανάλωση πόρων.

Κατά τη χρονική στιγμή των μετρήσεων, η χρήση του επεξεργαστή παρέμεινε σε χαμηλά επίπεδα, περίπου στο ποσοστό 13% για κάθε πυρήνα. Συνεπώς, σε τυπική λειτουργία, οι υπηρεσίες δεν ανεβάζουν τις τιμές στο φορτίο του επεξεργαστή. Παράλληλα, η χρήση μνήμης εμφανίζεται στο 50%. Συγκεκριμένα, χρησιμοποιούνται τα 3,3 GB από τα 6,6 GB που αναγνωρίζει το σύστημα. Τη συγκεκριμένη χρονική στιγμή παρατηρείται επίσης, περιορισμένη δραστηριότητα στις λειτουργίες δικτύου και δίσκου. Αυτό ήταν αναμενόμενο για συνθήκες τυπικής λειτουργίας και χωρίς αυξημένο ρυθμό εισαγωγής δεδομένων.



Σχήμα 4.9: Χρήση πόρων της εικονικής μηχανής σε τυπική λειτουργία

Συμπληρωματικά, χρησιμοποιήθηκαν και εντολές τερματικού για μία πιο λεπτομερή αποτύπωση της μνήμης και του αποθηκευτικού χώρου. Η χρήση της εντολής `free -h` επιβεβαιώνει ότι η συνολική μνήμη του συστήματος ήταν περίπου 6,2GiB, με περίπου τα 3,3GiB να βρίσκονται σε χρήση και τα 2,8GiB να είναι διαθέσιμα. Στο Linux, ένα μέρος της μνήμης χρησιμοποιείται ως προσωρινή μνήμη (cache), ώστε το σύστημα να λειτουργεί πιο γρήγορα. Η μνήμη αυτή δεν είναι πραγματικά δεσμευμένη, καθώς μπορεί να ελευθερωθεί αυτόματα και να χρησιμοποιηθεί πρακτικά, όταν κάποια υπηρεσία τη χρειαστεί. Για αυτόν τον λόγο, η ένδειξη της διαθέσιμης μνήμης (available), είναι περισσότερο αντιπροσωπευτική από την απλή τιμή της ελεύθερης μνήμης.

Όσον αφορά τον αποθηκευτικό χώρο, χρησιμοποιήθηκε η εντολή `df -h`. Το αποτέλεσμα εμφάνισε ότι το κύριο σύστημα αρχείων είχε μέγεθος περίπου στα 59GB, με χρήση των 29GB ή αλλιώς σε ποσοστό 52%. Η χρήση της εντολής `du -sh` έδειξε ότι ο κατάλογος `/var/ossec` καταλαμβάνει περίπου τα 14GB, ενώ ο κατάλογος `/var/lib/wazuh-indexer` περίπου τα 70MB.

Σαν συμπέρασμα, σε τυπική λειτουργία η πλατφόρμα δεν εμφανίζει υψηλή επιβάρυνση στον επεξεργαστή και τη μνήμη. Ωστόσο, σημαντική προσοχή πρέπει να δοθεί στον αποθηκευτικό χώρο. Συγκεκριμένα, φαίνεται να επηρεάζεται από τις καταγραφές, οι οποίες μπορούν να αυξηθούν με την πάροδο του χρόνου. Για τον λόγο αυτό, σε μελλοντικές εγκαταστάσεις είναι απαραίτητη η παρακολούθηση του διαθέσιμου χώρου και η πρόβλεψη πολιτικής διατήρησης δεδομένων.

```

pinelopi@pinelopi-VMware-Virtual-Platform: $ df -h
Filesystem      Size  Used Avail Use% Mounted on
tmpfs            1.3G  2.6M  1.3G   1% /run
/dev/sda2        59G   29G   28G  52% /
tmpfs            3.1G   80K  3.1G   1% /dev/shm
tmpfs            1.0M    0  1.0M   0% /run/credentials/systemd-journald.service
tmpfs            5.0M   8.0K  5.0M   1% /run/lock
tmpfs            1.0M    0  1.0M   0% /run/credentials/systemd-resolved.service
tmpfs            3.1G   1.2M  3.1G   1% /tmp
tmpfs            634M   84K  634M   1% /run/user/1000
/dev/sr0         102M  102M    0 100% /media/pinelopi/CDROM
/dev/sr1         5.4G   5.4G    0 100% /media/pinelopi/Ubuntu 25.10 amd64
pinelopi@pinelopi-VMware-Virtual-Platform: $ free -h
total        used        free      shared  buff/cache   available
Mem:         6.2Gi       3.3Gi       144Mi       22Mi       3.0Gi       2.8Gi
Swap:        4.0Gi         4.0Ki       4.0Gi
pinelopi@pinelopi-VMware-Virtual-Platform: $ sudo du -sh /var/ossec 2>/dev/null
14G    /var/ossec
pinelopi@pinelopi-VMware-Virtual-Platform: $ sudo du -sh /var/lib/wazuh-indexer 2>/dev/null || true
70M    /var/lib/wazuh-indexer
pinelopi@pinelopi-VMware-Virtual-Platform: $ █

```

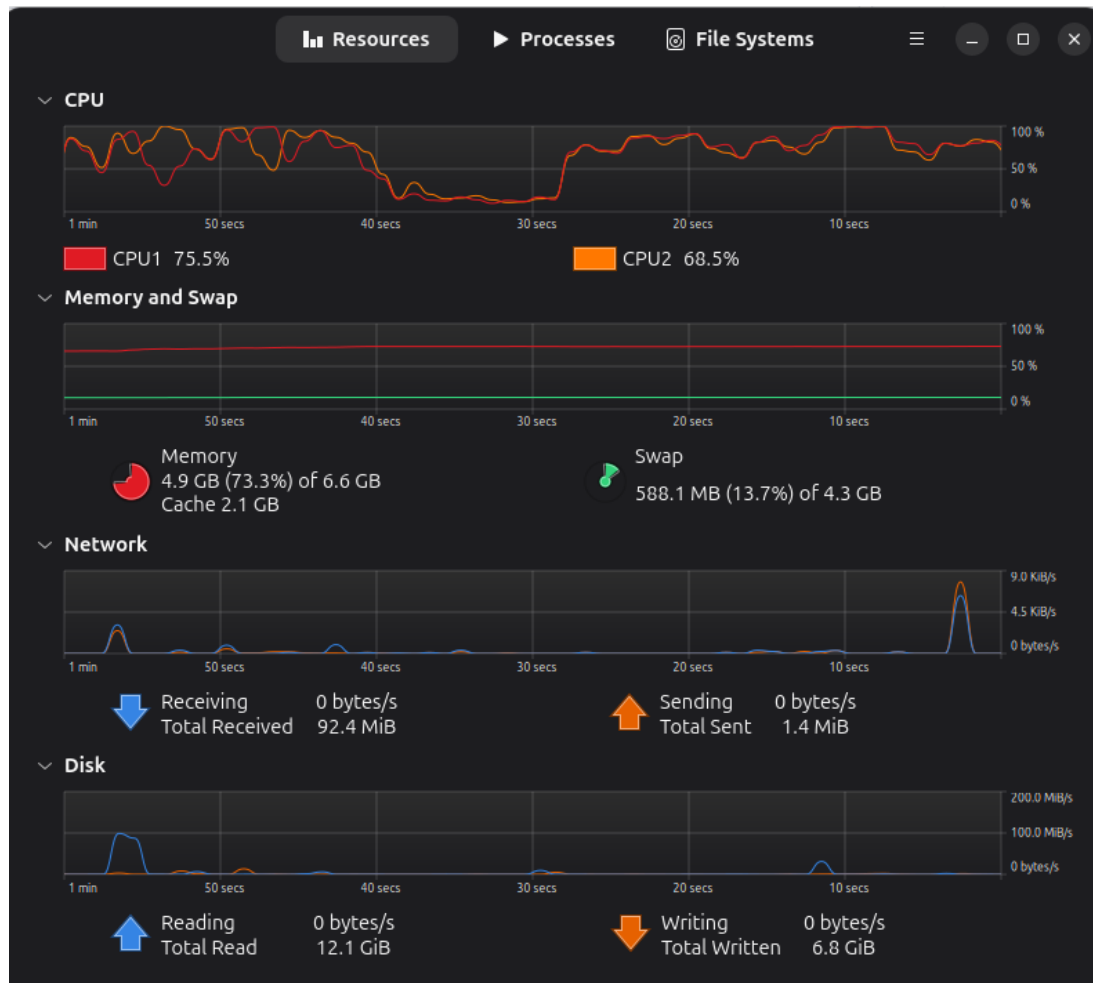
Σχήμα 4.10: Έλεγχος μνήμης και αποθηκευτικού χώρου μέσω τερματικού

4.4.2 Κατανάλωση πόρων υπό αυξημένο φορτίο

Στη συνέχεια, εξετάστηκε η κατανάλωση πόρων σε συνθήκες που το σύστημα βρίσκεται υπό αυξημένο φόρτο. Ως αυξημένος φόρτος θεωρείται η κατάσταση στην οποία γίνεται εισαγωγή μεγάλου όγκου δεδομένων σε μικρό χρονικό διάστημα. Αυτό το γεγονός ενεργοποιεί πιο έντονα τις λειτουργίες συλλογής, επεξεργασίας, εφαρμογής κανόνων και αποθήκευσης. Ο φόρτος δημιουργήθηκε με ελεγχόμενη τροφοδότηση εγγραφών καταγραφής μέσω δέσμης εντολών (script), με στόχο την προσομοίωση αυξημένου ρυθμού εισαγωγής συμβάντων στο εργαστηριακό περιβάλλον. Το script τροφοδότησε το αρχείο εισόδου με ρυθμό 50 εγγραφών ανά δευτερόλεπτο. Στόχος της συγκεκριμένης μέτρησης είναι η αποτύπωση της συμπεριφοράς της πλατφόρμας, σε πιο απαιτητικές συνθήκες σε σχέση με την τυπική λειτουργία η οποία παρουσιάστηκε προηγουμένως.

Όπως παρατηρήθηκε, η χρήση του επεξεργαστή αυξήθηκε σημαντικά κατά τη διάρκεια της μέτρησης. Πιο συγκεκριμένα, έφτασε περίπου το ποσοστό 75,5% για τον πρώτο πυρήνα και το ποσοστό 68,5% για τον δεύτερο. Παράλληλα, η χρήση της μνήμης αυξήθηκε περίπου στα 4,9GB, δηλαδή ποσοστό 73,3% της διαθέσιμης μνήμης. Ιδιαίτερη σημασία παρουσιάζει η εμφάνιση χρήσης του χώρου swap. Με περίπου 588MB από τα 4,3GB, αποτελεί χώρο του δίσκου που χρησιμοποιείται προσωρινά ως επέκταση της μνήμης RAM. Η ένδειξη αυτή δείχνει ότι, η μνήμη αποτελεί έναν από τους πιο βασικούς παράγοντες που επηρεάζουν την απόδοση του συστήματος σε απαιτητικά σενάρια.

Σε σύγκριση με την τυπική λειτουργία, παρατηρήθηκε αισθητά μεγαλύτερη κατανάλωση σε επεξεργαστή και μνήμη, χωρίς όμως να διακοπεί η λειτουργία των βασικών υποσυστημάτων της πλατφόρμας. Το αποτέλεσμα είναι ιδιαίτερα σημαντικό, καθώς η υλοποίηση πραγματοποιήθηκε αξιοποιώντας πόρους ενός τυπικού φορητού υπολογιστή και όχι με χρήση εξειδικευμένου εξοπλισμού. Συνεπώς, το λογισμικό ανοικτού κώδικα μπορεί να λειτουργήσει σε περιορισμένη υποδομή και χωρίς απαιτήσεις για υλικό υψηλών προδιαγραφών. Για περιβάλλοντα με υψηλότερους ρυθμούς, είναι αναγκαία η πρόβλεψη επιπλέον πόρων για τη διασφάλιση της ομαλής και αδιάλειπτης λειτουργίας του συστήματος.



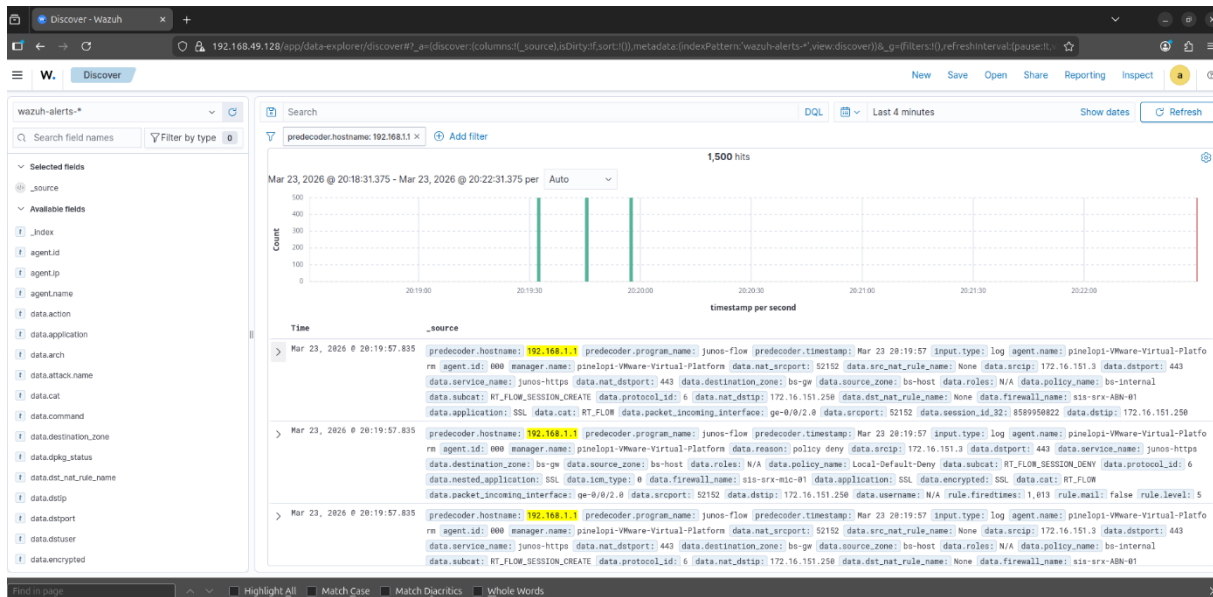
Σχήμα 4.11: Χρήση πόρων της εικονικής μηχανής υπό αυξημένο φορτίο

4.4.3 Συμπεριφορά σε απώλεια και επαναφορά σύνδεσης στο διαδίκτυο

Στη συνέχεια, εξετάστηκε η λειτουργία της πλατφόρμας σε συνθήκες απώλειας σύνδεσης στο διαδίκτυο. Ως στόχος της δοκιμής, έπρεπε οι βασικές λειτουργίες ενός τοπικά εγκατεστημένου SIEM να παραμένουν διαθέσιμες, χωρίς εξάρτηση από εξωτερικές υπηρεσίες. Η δοκιμή επικεντρώθηκε στη συνέχιση της συλλογής, επεξεργασίας και προβολής συμβάντων τοπικά και χωρίς να υπάρχει πρόσβαση στο διαδίκτυο.

Κατά την διάρκεια της δοκιμής έγινε χρήση της δέσμης εντολών `generate_logs.sh`. Όπως και στα προηγούμενα σενάρια, άρχισε η τροφοδότηση του αρχείου με νέες εγγραφές. Στη συνέχεια, απενεργοποιήθηκε η ασύρματη διεπαφή (Wi-Fi) στο σύστημα υποδοχής άλλα η επικοινωνία με την εικονική μηχανή παρέμεινε ενεργή μέσω του τοπικού δικτύου. Με αυτόν τον τρόπο ελέγχθηκε αν η απουσία διαδικτυακής σύνδεσης επηρεάζει τη λειτουργία της πλατφόρμας.

Όπως φαίνεται στο Σχήμα 4.12, με την απενεργοποίηση της εξωτερικής σύνδεσης τα νέα συμβάντα συνέχισαν να εμφανίζονται στο περιβάλλον διερεύνησης και να είναι διαθέσιμα προς αναζήτηση και φιλτράρισμα. Η ροή των δεδομένων τεκμηριώθηκε από την εμφάνιση νέων χρονικών στιγμιότυπων. Επίσης, διατηρήθηκαν τα μεταδεδομένα που συνδέουν κάθε συμβάν με την πηγή του. Επιπλέον ο πράκτορας του τερματικού συστήματος παρέμεινε σε ενεργή κατάσταση, γεγονός που επιβεβαιώνει ότι η εσωτερική επικοινωνία της υποδομής συνέχισε να λειτουργεί κανονικά.



Σχήμα 4.12: Συνέχιση εμφάνισης συμβάντων κατά την απώλεια σύνδεσης στο διαδίκτυο

Ως αποτέλεσμα επιβεβαιώνεται ότι η βασική λειτουργία της πλατφόρμας γίνεται τοπικά και μέσα στην ίδια υποδομή. Επίσης δείχνει ότι δεν εξαρτάται άμεσα από τη σύνδεση στο διαδίκτυο. Η απώλεια της ασύρματης διεπαφής δεν επηρέασε τη συλλογή, την αποθήκευση και την προβολή των δεδομένων ασφαλείας. Οι πηγές δεδομένων και ο τοπικός εξυπηρετητής παρέμεναν διαθέσιμα στο εσωτερικό δίκτυο. Μετά την επαναφορά της σύνδεσης, η πλατφόρμα συνέχισε να λειτουργεί χωρίς να απαιτηθούν αλλαγές στις ρυθμίσεις ή επανεκκίνηση υπηρεσιών. Η δοκιμή έδειξε ότι οι βασικές λειτουργίες συνεχίζονται ακόμη και σε περιβάλλοντα με διακοπτόμενη συνδεσιμότητα, χαρακτηριστικό ιδιαίτερα σημαντικό για απομακρυσμένες υποδομές.

4.4.4 Επιχειρησιακή αξία στο ναυτιλιακό περιβάλλον

Η παρούσα αξιολόγηση δείχνει ότι η προτεινόμενη υλοποίηση συγκεντρώνει και ενοποιεί καταγραφές από ετερογενείς πηγές σε ένα ενιαίο περιβάλλον, χωρίς να απαιτεί εξειδικευμένο εξοπλισμό. Σε ένα πλοίο συνυπάρχουν συστήματα διαφορετικών τεχνολογιών. Η ανάγκη της ύπαρξης κεντρικού ελέγχου είναι κρίσιμη, ειδικά όταν οι πόροι είναι περιορισμένοι και η τεχνική υποστήριξη δεν είναι πάντα άμεσα διαθέσιμη. Στο πλαίσιο αυτό, η προστιθέμενη αξία μίας τέτοιας λύσης σχετίζεται με τη δυνατότητα ανάλυσης και διερεύνησης υπό ρεαλιστικές συνθήκες λειτουργίας.

Ένα από τα κύρια χαρακτηριστικά που αναδείχθηκαν, είναι η ικανότητα του συστήματος να διατηρεί την επιχειρησιακή του συνέχεια ακόμα και σε συνθήκες έλλειψης εξωτερικής συνδεσιμότητας. Η αρχιτεκτονική που επιλέχθηκε διασφαλίζει την πλήρη λειτουργία της πλατφόρμας, εφόσον διατηρείται η επικοινωνία μεταξύ των υποσυστημάτων. Το στοιχείο αυτό κρίνεται απαραίτητο για τη ναυτιλιακή βιομηχανία, καθώς η δορυφορική σύνδεση των πλοίων συχνά παρουσιάζει υψηλή καθυστέρηση (latency), διακοπτόμενη ροή και να χρησιμοποιείται προτεραιότητα συνδεσιμότητας για άλλες λειτουργίες.

Παράλληλα, οι μετρήσεις κατανάλωσης των πόρων ανέδειξαν πως η εγκατάσταση της πλατφόρμας μπορεί να ανταπεξέλθει πλήρως βασιζόμενη σε συμβατικό υλικό και χωρίς την ανάγκη εξειδικευμένου με υψηλού κόστους υλικό. Κατά την αύξηση του ρυθμού των εγγραφών, παρατηρήθηκε η δυναμική απόκριση του συστήματος και η ικανότητά του να αξιοποιεί πλήρως τους διαθέσιμους πόρους. Η συγκεκριμένη συμπεριφορά τονίζει την ευελιξία της υλοποίησης. Επίσης, επιτρέπει την ακριβή

προσαρμογή της υποδομής σύμφωνα με τις ιδιαίτερες επιχειρησιακές ανάγκες κάθε πλοίου. Στο πλαίσιο αυτό, η βελτιστοποίηση της εγκατάστασης καθορίζεται από παραμέτρους όπως ο συνολικός αριθμός των τερματικών με πράκτορες, ο ρυθμός παραγωγής καταγραφών και η πολιτική διακράτησης των δεδομένων. Οι παράμετροι αυτοί απαιτούνται για τις ανάγκες διερεύνησης συμβάντων και διασφαλίζουν μια αποδοτική λύση παρακολούθησης.

Επομένως, η προτεινόμενη υλοποίηση διαμορφώνει μία στιβαρή βάση για την τοπική επιτήρηση συμβάντων ασφαλείας. Επίσης, επιβεβαιώνεται ότι οι τεχνικοί περιορισμοί που υπάρχουν σε ναυτιλιακά περιβάλλοντα μπορούν να αντιμετωπιστούν αποτελεσματικά μέσω τοπικών κόμβων. Απαραίτητη προϋπόθεση είναι η κατάλληλη επιλογή του υλικού (hardware), η σωστή παραμετροποίηση της πλατφόρμας και η πρόβλεψη των απαιτήσεων, οι οποίες προκύπτουν από τις ιδιαίτερες απαιτήσεις του εκάστοτε πλοίου.

4.5 Συγκριτική αξιολόγηση με άλλες πλατφόρμες

Η ενότητα αυτή, παραθέτει μια συγκριτική αξιολόγηση της λύσης έναντι κύριων κατηγοριών SIEM. Η ανάλυση πραγματοποιήθηκε εστιάζοντας στην ικανότητα των λύσεων να ικανοποιούν τις ειδικές απαιτήσεις του ναυτιλιακού τομέα όπως η λειτουργική αυτονομία και η διαχείριση ετερογενών πηγών δεδομένων. Η αξιολόγηση βασίζεται στα αποτελέσματα των δοκιμών που πραγματοποιήθηκαν, αναδεικνύοντας τον καλύτερο συνδυασμό ανάμεσα στους διαθέσιμους πόρους, τη σύνδεση στο διαδίκτυο και την αποτελεσματική λειτουργία στην πράξη.

4.5.1 Κριτήρια σύγκρισης και απαιτήσεις ναυτιλιακής χρήσης

Τα κριτήρια σύγκρισης επιλέχθηκαν βάσει των απαιτήσεων της παρούσας εργασίας και τους περιορισμούς που περιγράφουν ένα ναυτιλιακό περιβάλλον. Η σύγκριση αυτή δεν στοχεύει σε γενική κατάταξη των λύσεων, αλλά στην αξιολόγηση της καταλληλότητας τους σε συγκεκριμένες συνθήκες. Σε αυτές τις συνθήκες η συνδεσιμότητα, οι διαθέσιμοι πόροι, ο συνδυασμός διαφορετικών τεχνολογικών συστημάτων και η δυνατότητα τοπικής διαχείρισης επηρεάζουν άμεσα τη λειτουργία της υποδομής.

Αρχικά, εξετάστηκε το κριτήριο της απαίτησης συνδεσιμότητας. Στο περιβάλλον ενός πλοίου η πρόσβαση στο διαδίκτυο ενδέχεται να είναι περιορισμένη, ασταθής ή και να χρησιμοποιείται κατά προτεραιότητα για άλλες επιχειρησιακές λειτουργίες. Για τον λόγο αυτό, εξετάστηκε αν μια λύση λειτουργεί εξ ολοκλήρου τοπικά ή αν απαιτείτε αποστολή καταγραφών σε εξωτερική υποδομή.

Στη συνέχεια, σημαντική κρίθηκε η διατήρηση των δεδομένων ασφαλείας εντός της εγκατάστασης. Οι καταγραφές του πλοίου ενδέχεται να περιλαμβάνουν κρίσιμες εσωτερικές πληροφορίες όπως εσωτερικές διευθύνσεις, δικτυακή επικοινωνία και δραστηριότητες χρηστών. Επομένως, η τοπική αποθήκευση και ανάλυση μειώνει την συνεχή μεταφορά δεδομένων εκτός του ελεγχόμενου περιβάλλοντος.

Επιπλέον, αξιολογείται η υποστήριξη διαφορετικών τεχνολογικών συστημάτων. Μια υποδομή στη ναυτιλία περιλαμβάνει τερματικά συστήματα, δικτυακές συσκευές και εξοπλισμό από διαφορετικούς κατασκευαστές. Έτσι, είναι σημαντικό να εξασφαλίζεται ότι η πλατφόρμα μπορεί να δεχθεί και να επεξεργαστεί δεδομένα από ετερογενή περιβάλλοντα και κατασκευαστές.

Ένα πέμπτο ζήτημα αφορά τη δυνατότητα τοπικής προσαρμογής των κανόνων και των αποκωδικοποιητών. Σε ένα πλοίο συναντώνται συσκευές και συστήματα με ειδικές μορφές καταγραφών, οι οποίες δεν αναγνωρίζονται πάντα αυτόματα από τις προεπιλεγμένες ρυθμίσεις μιας πλατφόρμας. Έτσι σημαντική ήταν η λύση να επιτρέπει στον διαχειριστή να επεμβαίνει στη διαδικασία μετατροπής των δεδομένων σε αξιοποιήσιμη πληροφορία, χωρίς εξάρτηση από τον κατασκευαστή.

Οι διαθέσιμοι υπολογιστικοί πόροι είναι συχνά περιορισμένοι. Επομένως, οι απαιτήσεις σε υποδομή και πόρους αποτελούν κρίσιμο κριτήριο σύγκρισης. Η λύση πρέπει να αξιολογηθεί και ως προς την αποδοτική λειτουργία της σε υλικό μετριάσμενων δυνατοτήτων, χωρίς να επιβαρύνει την υπόλοιπη επιχειρησιακή υποδομή.

Τέλος, σε αυτό το περιβάλλον, το εξειδικευμένο τεχνικό προσωπικό δεν είναι πάντα διαθέσιμο επιτόπου. Συνεπώς, σημαντικό κριτήριο αποτελεί η διαχειρισιμότητα της λύσης. Είναι απαραίτητο να παρέχεται η δυνατότητα ενιαίας και άμεσης διαχείρισης των ρυθμίσεων. Επιπλέον, ουσιαστικό πλεονέκτημα αποτελεί και η δυνατότητα διερεύνησης. Η αναζήτηση, το φιλτράρισμα και η ανάλυση συμβάντων πρέπει να καθορίζουν την πρακτική χρησιμότητα για τον αναλυτή, ο οποίος καλείται να εντοπίσει απειλές μέσα σε μεγάλους όγκους δεδομένων.

4.5.2 Αποτίμηση εναλλακτικών λύσεων βάσει κριτηρίων

Σε αντίθεση με τη βιβλιογραφική επισκόπηση του Κεφαλαίου 2, η παρούσα ενότητα αξιολογεί τις εναλλακτικές πλατφόρμες με βάση τις πρακτικές απαιτήσεις που προέκυψαν από την υλοποίηση και την πειραματική αξιολόγηση της εργασίας. Η συγκριτική αποτίμηση που ακολουθεί, δεν αποσκοπεί σε πλήρη αξιολόγηση της αγοράς. Σκοπός είναι η ποιοτική σύγκριση των βασικών κατηγοριών λύσεων για τις ανάγκες της παρούσας εργασίας. Η προσέγγιση αυτή επιλέχθηκε ώστε η σύγκριση να παραμένει τεχνικά τεκμηριωμένη και να μην εξαρτάται από μεταβαλλόμενες εμπορικές παραμέτρους όπως η τιμολόγηση, τα πακέτα αδειοδότησης ή οι εμπορικές εκδόσεις των προϊόντων.

Ο Πίνακας 4.3, συνοψίζει ότι οι διαφορετικές κατηγορίες λύσεων εξυπηρετούν και διαφορετικές ανάγκες. Οι λύσεις που βασίζονται σε υποδομή υπολογιστικού νέφους (Cloud), προσφέρουν ισχυρές δυνατότητες κεντρικής ανάλυσης. Όμως εξαρτώνται καθοριστικά από σταθερή σύνδεση με απομακρυσμένη πλατφόρμα, προϋπόθεση που δεν μπορεί να εξασφαλιστεί σε ένα πλοίο εν πλω. Παράλληλα, η μεταφορά δεδομένων σε υποδομή τρίτου παρόχου θέτει ζητήματα ιδιοκτησίας της πληροφορίας.

Αντίστοιχα, οι εμπορικές λύσεις τοπικής εγκατάστασης, παρέχουν ισχυρές δυνατότητες ανάλυσης και διερεύνησης. Παρόλα αυτά, συνοδεύονται από υψηλό κόστος αδειοδότησης, σύνθετη αρχιτεκτονική και αυξημένες απαιτήσεις διαχείρισης. Επιπλέον, η εξάρτηση από τον κατασκευαστή περιορίζει την ευελιξία και δεσμεύει τον φορέα σε δαπάνες υποστήριξης.

Η υβριδική προσέγγιση, επιχειρεί τον συμβιβασμό μεταξύ δύο μοντέλων. Εισάγει όμως πρόσθετη πολυπλοκότητα στη διαχείριση και πιθανή διασπορά των δεδομένων μεταξύ των επιμέρους υποδομών. Στο πλαίσιο της ναυτιλίας, όπου η συνεχής συνδεσιμότητα είναι περιορισμένη, το λειτουργικό κόστος κρίσιμο και η αυτονομία της υποδομής επιβεβλημένη, η τοπική λύση με χρήση της πλατφόρμας Wazuh συγκεντρώνει τα χαρακτηριστικά που εξυπηρετούν τις ανάγκες λειτουργίας ενός πλοίου.

Πίνακας 4.3: Συγκριτική αποτίμηση κατηγοριών SIEM για ναυτιλιακή χρήση

A/A	Κριτήριο	Wazuh με τοπική εγκατάσταση	Cloud Native SIEM	Εμπορικό SIEM	Υβριδική λύση
1	Συνδεσιμότητα	Υψηλή τοπική αυτονομία	Αυξημένη εξάρτηση από εξωτερική σύνδεση	Τοπική λειτουργία με αυξημένες απαιτήσεις υποδομής	Μερική τοπική λειτουργία
2	Διατήρηση δεδομένων	Εντός πλοίου	Μεταφορά σε τρίτη υποδομή	Εντός πλοίου	Μικτό μοντέλο
3	Ετερογενείς πηγές	Υψηλή	Πολύ καλή	Εξαιρετική	Καλή
4	Μοντέλο κόστους	Ανοιχτού κώδικα, χωρίς κόστος αδειοδότησης	Συνδρομητικό	Άδειες χρήσης και υποστήριξη	Σύνθετο
5	Προσαρμογή	Πλήρης τοπικός έλεγχος κανόνων και αποκωδικοποιητών	Εξαρτάται από τις δυνατότητες της υπηρεσίας	Εξαρτάται από τον κατασκευαστή και το μοντέλο αδειοδότησης	Εξαρτάται από τον βαθμό τοπικής παραμετρο-ποίησης
6	Απαιτήσεις πόρων	Κλιμακούμενη	Μικρότερες τοπικές απαιτήσεις	Μεγαλύτερες απαιτήσεις	Μεσαίες απαιτήσεις
7	Διαχειρισιμότητα	Άμεση διαχείριση ρυθμίσεων	Κεντρική διαχείριση υπηρεσίας	Ισχυρή διαχείριση με αυξημένη πολυπλοκότητα	Μικτή διαχείριση
8	Διερεύνηση	Ενιαίο περιβάλλον με δομημένα πεδία	Ισχυρό περιβάλλον διερεύνησης	Ισχυρό περιβάλλον διερεύνησης	Ισχυρή λειτουργικότητα αλλά πιθανή διάσπαση περιβάλλοντος

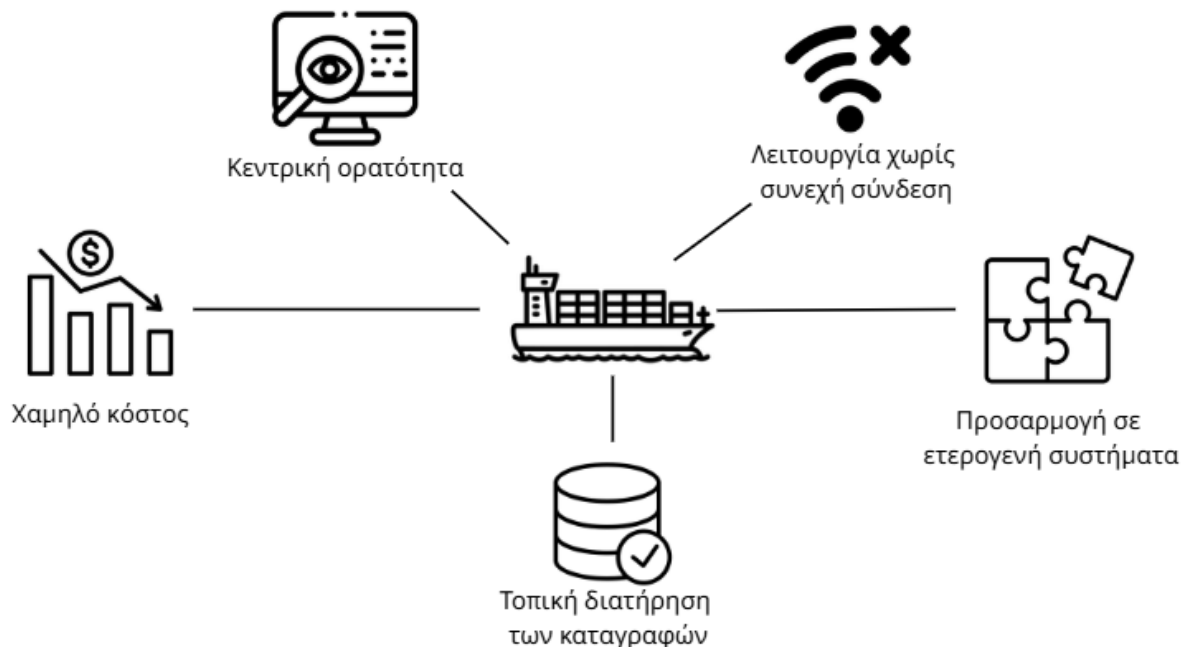
Ο πίνακας συνοψίζει ότι οι διαφορετικές κατηγορίες λύσεων εξυπηρετούν και διαφορετικές ανάγκες. Οι λύσεις που βασίζονται σε υποδομή υπολογιστικού νέφους (Cloud), προσφέρουν ισχυρές δυνατότητες κεντρικής ανάλυσης. Όμως εξαρτώνται καθοριστικά από σταθερή σύνδεση με απομακρυσμένη πλατφόρμα, προϋπόθεση που δεν μπορεί να εξασφαλιστεί σε ένα πλοίο εν πλω. Παράλληλα, η μεταφορά δεδομένων σε υποδομή τρίτου παρόχου θέτει ζητήματα ιδιοκτησίας της πληροφορίας.

Αντίστοιχα, οι εμπορικές λύσεις τοπικής εγκατάστασης, παρέχουν ισχυρές δυνατότητες ανάλυσης και διερεύνησης. Παρόλα αυτά, συνοδεύονται από υψηλό κόστος αδειοδότησης, σύνθετη αρχιτεκτονική και αυξημένες απαιτήσεις διαχείρισης. Επιπλέον, η εξάρτηση από τον κατασκευαστή περιορίζει την ευελιξία και δεσμεύει τον φορέα σε δαπάνες υποστήριξης.

Η υβριδική προσέγγιση, επιχειρεί τον συμβιβασμό μεταξύ δύο μοντέλων. Εισάγει όμως πρόσθετη πολυπλοκότητα στη διαχείριση και πιθανή διασπορά των δεδομένων μεταξύ των επιμέρους υποδομών. Στο πλαίσιο της ναυτιλίας, όπου η συνεχής συνδεσιμότητα είναι περιορισμένη, το λειτουργικό κόστος κρίσιμο και η αυτονομία της υποδομής επιβεβλημένη, η τοπική λύση με χρήση της πλατφόρμας Wazuh συγκεντρώνει τα χαρακτηριστικά που εξυπηρετούν τις ανάγκες λειτουργίας ενός πλοίου.

4.5.3 Συνολική αποτίμηση της πλατφόρμας βάσει των ναυτιλιακών απαιτήσεων

Από τη σύγκριση των λύσεων προκύπτει ότι η πλατφόρμα Wazuh ταιριάζει σε περιβάλλοντα που χρειάζονται τοπική εποπτεία των συμβάντων ασφαλείας, μειωμένη εξάρτηση από εξωτερικές υπηρεσίες και έλεγχο των δεδομένων. Στην πράξη, όταν αναφερόμαστε σε πλοία, η επιλογή ενός συστήματος ασφαλείας δεν αφορά μόνο την ικανότητα του στην ανίχνευση απειλών. Συγκεκριμένα, επηρεάζεται άμεσα από περιορισμούς όπως η διακοπτόμενη συνδεσιμότητα, το υψηλό κόστος δορυφορικής μεταφοράς δεδομένων και η ανάγκη διατήρησης των καταγραφών τοπικά σε ελεγχόμενο περιβάλλον.



Σχήμα 4.13: Κάλυψη ναυτιλιακών απαιτήσεων από την υλοποίηση

Η τοπική εγκατάσταση προσφέρει μια ουσιαστική σιγουριά, διότι το σύστημα συνεχίζει να λειτουργεί απρόσκοπτα ακόμα και σε περίπτωση διακοπής της σύνδεσης με το διαδίκτυο. Εφόσον υπάρχει εσωτερική επικοινωνία μεταξύ του κεντρικού κόμβου με τους πράκτορες και με τις πηγές, η συλλογή και η ανάλυση των δεδομένων συνεχίζεται κανονικά. Επιπλέον, το γεγονός ότι τα δεδομένα παραμένουν εντός της υποδομής επιτρέπει μεγαλύτερο έλεγχο από τον χειριστή. Έτσι, μειώνεται η ανάγκη για συνεχόμενη αποστολή σε εξωτερικές υποδομές, ιδιαίτερα σε περιπτώσεις που οι εγγραφές περιλαμβάνουν επιχειρησιακά και ευαίσθητα στοιχεία.

Σε θέμα κόστους, οι λύσεις που δεν απαιτούν άδειες δεν επιβαρύνουν τον χρήστη με συνδρομές. Το κόστος σε αυτές τις λύσεις, εστιάζει κυρίως στην υποδομή και τη διαχείριση της, όπως οι πόροι που χρησιμοποιούνται, η αποθήκευση και η συντήρηση. Η παρατήρηση αυτή είναι ιδιαίτερα κρίσιμη καθώς ο σχεδιασμός μπορεί να εξελίσσεται σταδιακά και ανάλογα με τον αριθμό των πηγών, τον ρυθμό των καταγραφών και την πολιτική διατήρησης.

Σημαντική είναι και η αναφορά της δυνατότητας προσαρμογής των αποκωδικοποιητών και των κανόνων. Στο περιβάλλον της ναυτιλίας συναντώνται διαφορετικοί κατασκευαστές και μορφές καταγραφών. Η παρούσα αξιολόγηση παρουσιάζει μεγάλη ευελιξία σε ετερογενή συστήματα η οποία τεκμηριώθηκε μέσω της εισαγωγής και επεξεργασίας εξωτερικών δικτυακών καταγραφών, οι οποίες μετατράπηκαν σε δομημένη πληροφορία με στόχο να αξιοποιηθούν στη διερεύνηση.

Κεφάλαιο 5ο: Συμπεράσματα

Σε συνέχεια της ανάλυσης του θεωρητικού υποβάθρου και της υλοποίησης του πρακτικού μέρους, παρακάτω συνοψίζονται τα βασικά συμπεράσματα που προέκυψαν. Μαζί με τα αποτελέσματα, εξετάζονται οι αδυναμίες της τρέχουσας υλοποίησης και καταγράφονται ιδέες και προτάσεις για μελλοντικές επεκτάσεις.

5.1 Συμπεράσματα

Με την ολοκλήρωση της υλοποίησης και των δοκιμών λειτουργίας, επιβεβαιώθηκε ότι η δημιουργία ενός εργαστηριακού συστήματος διαχείρισης πληροφοριών και συμβάντων ασφαλείας για πλοία είναι μία τεχνικά εφικτή λύση. Η μελέτη, λαμβάνοντας υπόψη τις ιδιαίτερες συνθήκες ενός περιβάλλοντος όπως αυτό της ναυτιλίας, εστίασε στην κεντρική συλλογή και ανάλυση των συμβάντων ασφαλείας. Η προσέγγιση βασίστηκε στην τοπική εγκατάσταση της πλατφόρμας ανοιχτού κώδικα Wazuh, σε εικονική μηχανή Ubuntu. Η κεντρική επιτήρηση αποδείχθηκε ότι μπορεί να λειτουργήσει στην πράξη, μέσα από τη συλλογή δεδομένων από ετερογενείς πηγές. Το σύστημα μπορεί να ανταποκριθεί ικανοποιητικά, ακόμα και σε ασταθή σύνδεση ή σε υποδομές με περιορισμένους διαθέσιμους υπολογιστικούς πόρους.

Στο επίπεδο της λειτουργικότητας, τεκμηριώθηκε ότι η πλατφόρμα υποστηρίζει τη βασική αλυσίδα λειτουργίας. Το σύστημα μπορεί επιτυχώς να συλλέγει καταγραφές, να εμφανίζει τα συμβάντα, να τα αποκωδικοποιεί, να τα αξιολογεί με τους κανόνες και τέλος να παράγει τις ειδοποιήσεις. Η συλλογή δεδομένων από το τερματικό σύστημα έγινε με τη χρήση του πράκτορα, ο οποίος με επιτυχία παρείχε τα γεγονότα από το λειτουργικό σύστημα. Χρησιμοποιήθηκε και η βασική λειτουργία του Sysmon ως πρόσθετη πηγή, για τη λεπτομερή τηλεμετρία. Η προσθήκη αυτή συνέβαλε στη συνολική αξιολόγηση του συστήματος, ως ένα χρήσιμο επιπλέον επίπεδο ορατότητας.

Μέρος της αξιολόγησης αποτέλεσε και η εισαγωγή του εξωτερικού συνόλου δεδομένων τύπου Syslog, το οποίο βασίστηκε σε καταγραφές από συσκευές vSRX στο περιβάλλον ενός πλοίου. Η εισαγωγή αυτή απέδειξε ότι η πλατφόρμα μπορεί να δεχθεί και να διαχειριστεί καταγραφές δικτύου με την ίδια ευκολία. Το σύνολο δεδομένων οργανώθηκε σε ένα τοπικό αρχείο όπου η πλατφόρμα το παρακολουθεί ενεργά. Η μέθοδος αυτή πετυχαίνει την πλήρως ελεγχόμενη αναπαραγωγή των συμβάντων ασφαλείας. Έτσι, τεκμηριώθηκε με ακρίβεια η συμπεριφορά του μηχανισμού ανίχνευσης στις περιπτώσεις που δέχεται πραγματικές μορφές καταγραφών.

Κρίσιμο τεχνικό συμπέρασμα προκύπτει από τον ρόλο χρήσης των αποκωδικοποιητών και των κανόνων. Αποδείχθηκε στην πράξη ότι η αξία μίας καταγραφής δεν βρίσκεται στην εμφάνιση της ως ένα ενιαίο κείμενο. Η ουσία βρίσκεται στη μετατροπή της σε δομημένα πεδία και τη σύνδεση κανόνων που αποδίδουν την κατηγορία και το επίπεδο σοβαρότητας. Στην παρούσα υλοποίηση χρησιμοποιήθηκαν σαν βάση τα έτοιμα σύνολα αποκωδικοποιητών και κανόνων για Junos. Πάνω σε αυτά εφαρμόστηκαν τοπικές προσαρμογές, με στόχο την κάλυψη σε ειδικούς τύπους μορφής καταγραφών που δεν καλύπτονταν από τα έτοιμα σύνολα. Ως αποτέλεσμα, τα συμβάντα εμφανίζονται στο περιβάλλον διερεύνησης με ουσιαστικά και χρήσιμα πεδία. Στις περιπτώσεις αντιστοίχισης με κάποιον από τους κανόνες, το συμβάν συνοδεύεται με απαραίτητα μεταδεδομένα για τον αναλυτή, όπως το επίπεδο σοβαρότητας και μία σύντομη περιγραφή.

Σε επίπεδο απόδοσης του συστήματος, πραγματοποιήθηκαν μετρήσεις σε συνθήκες τυπικής λειτουργίας καθώς και κάτω από αυξημένο ρυθμό εισαγωγής καταγραφών. Κατά τη μέτρηση σε τυπική λειτουργία, το σύστημα λειτουργούσε σταθερά και χωρίς κάποια έντονη επιβάρυνση στους πόρους. Όταν ο ρυθμός

εισαγωγής αυξήθηκε ελεγχόμενα, η κατανάλωση της μνήμης και του επεξεργαστή αυξήθηκε αισθητά. Παρά την πίεση, η λειτουργία της πλατφόρμας δεν διακόπηκε καθόλου και δεν παρατηρήθηκε κάποια αστοχία. Δεν αποτελεί κύριο συμπέρασμα ότι οποιοδήποτε τυχαίο σύστημα είναι αρκετό. Δείχνει όμως ότι μία ενιαία εγκατάσταση αποτελεί ρεαλιστική και πλήρως λειτουργική βάση, ως εργαστηριακή βάση και πιθανή πιλοτική εφαρμογή. Επίσης, η υποδομή παρουσιάζει ευελιξία ως προς την κλιμάκωση. Οι απαιτήσεις στους πόρους δεν είναι σταθερές αλλά δίνουν τη δυνατότητα διαμόρφωσης, ανάλογα με το μέγεθος του πλοίου, τον αριθμό των πηγών καταγραφών και τον οικονομικό προϋπολογισμό.

Τέλος, για την ανάδειξη της πρακτικής σημασίας στην τοπική αρχιτεκτονική, πραγματοποιήθηκε δοκιμή απώλειας της σύνδεσης με το διαδίκτυο. Χωρίς την εξωτερική σύνδεση, οι βασικές λειτουργίες συλλογής και διερεύνησης συμβάντων συνέχισαν να εκτελούνται κανονικά. Μοναδική προϋπόθεση παραμένει η ενεργή εσωτερική επικοινωνία μεταξύ των πηγών και του κεντρικού κόμβου. Το συγκεκριμένο αποτελεί ουσιαστικό πλεονέκτημα για ένα περιβάλλον πλοίου, στο οποίο η δορυφορική σύνδεση ενδέχεται να κριθεί ασταθής ή να δεσμευτεί κατά προτεραιότητα για επιχειρησιακούς σκοπούς. Το περιβάλλον της πλατφόρμας είναι αρκετά κατανοητό, ακόμα και για κάποιον χωρίς εξειδικευμένες γνώσεις ασφαλείας. Ως αποτέλεσμα, ακόμα και ένας χειριστής με βασική εκπαίδευση επί του πλοίου μπορεί να αναγνωρίσει ένα κρίσιμο συμβάν και να αναλάβει τις πρώτες ενέργειες, όπως η άμεση ειδοποίηση του αρμόδιου προσωπικού και η επικοινωνία με την ξηρά.

Τα αποτελέσματα της υλοποίησης δείχνουν ότι οι βασικοί στόχοι της εργασίας καλύφθηκαν σε εργαστηριακό επίπεδο. Η υλοποίηση πέτυχε την κεντρική συλλογή συμβάντων από ετερογενείς πηγές, την τοπική λειτουργία της πλατφόρμας χωρίς συνεχή εξάρτηση από σύνδεση στο διαδίκτυο, την αποκωδικοποίηση και την παραγωγή ειδοποιήσεων μέσω κανόνων. Τέλος η αξιολόγηση της χρήσης πόρων και της συμπεριφοράς κάτω από περιορισμένες συνθήκες, έδειξε ότι η υλοποίηση μπορεί να αποτελέσει βάση για περαιτέρω εφαρμογή σε ένα πλοίο.

5.2 Περιορισμοί της μελέτης

Η παρούσα εργασία αποτελεί εργαστηριακή υλοποίηση. Η εγκατάσταση της σε μία εικονική μηχανή, επέτρεψε την καθαρή αξιολόγηση της βασικής λειτουργίας του συστήματος. Παρόλα αυτά δεν αποτυπώνει με ακρίβεια όλες τις συνθήκες ενός πραγματικού πλοίου. Επιπλέον, η επεξεργασία των δικτυακών καταγραφών εξαρτάται άμεσα και από τη μορφή των δεδομένων. Για ειδικές περιπτώσεις, είναι απαραίτητη η δημιουργία κατάλληλα μορφοποιημένων αποκωδικοποιητών και κανόνων. Αυτό είναι απαραίτητο για κάθε παραλλαγή, ώστε να διασφαλιστεί η σωστή αξιοποίηση της πληροφορίας. Σε αυτό το πλαίσιο, η ενσωμάτωση της τηλεμετρίας τερματικού με τη χρήση Sysmon, αξιοποιήθηκε στη βασική της μορφή. Συγκεκριμένα έγινε χρήση με τις προεπιλεγμένες ρυθμίσεις, χωρίς τη χρήση κάποιου εξειδικευμένου αρχείου για παραμετροποίηση.

Η αξιολόγηση των πόρων που χρησιμοποιήθηκαν και του φόρτου πραγματοποιήθηκε σε ελεγμένες εργαστηριακές συνθήκες, με συγκεκριμένες πηγές και ρυθμό εισαγωγής. Επιβεβαιώνουν ότι το σύστημα λειτουργεί ικανοποιητικά σε εργαστηριακό περιβάλλον, χωρίς να αποτελούν πλήρη εκτίμηση των απαιτήσεων για μία πραγματική εγκατάσταση εντός πλοίου. Τέλος, η εργασία δεν έχει αντικειμενικό σκοπό την πλήρη ανάπτυξη ενός έτοιμου για χρήση, επιχειρησιακού κέντρου ασφαλείας. Για την εξέλιξη της παρούσας σε ένα πλήρως ολοκληρωμένο περιβάλλον, απαιτούνται επιπλέον στάδια με στόχο τη συνεχή στελέχωση, τη δημιουργία σχεδίων δράσης για περιστατικά ασφαλείας και την πλήρη θωράκιση όλων των συστημάτων.

5.3 Βελτιώσεις και μελλοντικές επεκτάσεις

Με βάση τα συμπεράσματα και τους περιορισμούς της παρούσας αξιολόγησης, οι μελλοντικές επεκτάσεις μπορούν να εστιάσουν στη βελτίωση του συστήματος. Αρχικά, μπορεί να γίνει μία αξιολόγηση των υπολογιστικών πόρων και του εξοπλισμού που χρειάζεται ένα πλοίο, ανάλογα με το μέγεθός του. Για τον σκοπό αυτό, χρειάζονται περισσότερες δοκιμές με διαφορετικές πηγές δεδομένων και διαφορετικούς ρυθμούς εισαγωγής. Επίσης, μπορεί να οριστεί και μια σαφής πολιτική, για το πόσο καιρό θα αποθηκεύονται τα αρχεία καταγραφής στο σύστημα. Για να μην επιβαρύνεται το δίκτυο του πλοίου, μπορεί να γίνει μελέτη μεταφοράς προς τη στεριά μόνο των απαραίτητων και κρίσιμων στοιχείων, όπως συγκεκριμένες ειδοποιήσεις ή σύντομες περιγραφές. Η δυνατότητα αυτή είναι ιδιαίτερα σημαντική στις περιπτώσεις που ένας αναλυτής δεν μπορεί να συνδεθεί απομακρυσμένα στον πίνακα ελέγχου.

Τέλος, μια μελλοντική έρευνα μπορεί να ενσωματώσει τεχνικές μηχανικής μάθησης. Η δημιουργία μοντέλων ανίχνευσης ανωμαλιών, θα μπορούσε να επιτρέψει στο σύστημα να μαθαίνει τη συνηθισμένη συμπεριφορά του δικτύου και να εντοπίζονται αποκλίσεις, μειώνοντας την απαίτηση δημιουργίας προσαρμοσμένων κανόνων για κάθε σενάριο. Επίσης τα γλωσσικά μοντέλα, θα μπορούσαν να βοηθούν οποιοδήποτε μέλος του πληρώματος χωρίς γνώσεις, να κατανοήσει ένα συμβάν και να το καθοδηγήσουν σε βασικές πρώτες ενέργειες.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- [1] K. Kent και M. Souppaya, «Guide to Computer Security Log Management,» National Institute of Standards and Technology, Gaithersburg, 2006.
- [2] S. Bhatt, P. K. Manadhata και L. Zomlot, «The Operational Role of Security Information and Event Management Systems,» *IEEE Security & Privacy*, τόμ. 12, αρ. 5, pp. 35-41, 2014.
- [3] «MITRE ATT&CK,» MITRE, [Ηλεκτρονικό]. Available: <https://attack.mitre.org/>. [Πρόσβαση 18 May 2026].
- [4] S. Roy, E. Panaousis, C. Noakes, A. Laszka, S. Panda και G. Loukas, «SoK: The MITRE ATT&CK Framework in Research and Practice,» arXiv, 2023.
- [5] G. Culot, G. Nassimbeni, M. Podrecca και M. Sartor, «The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda,» *The TQM Journal*, τόμ. 33, αρ. 7, pp. 76-105, 2021.
- [6] G. Disterer, «ISO/IEC 27000, 27001 and 27002 for Information Security Management,» *Journal of Information Security*, τόμ. 4, αρ. 2, pp. 92-100, 2013.
- [7] A. L. Franceschett, P. R. A. d. S. Junior, F. L. P. d. Barros και V. R. d. Carvalho, «A Holistic Approach - How to Achieve the State-of-art in Cybersecurity for a Secondary Distribution Automation Energy System Applying the IEC 62443 Standard,» σε *2019 IEEE PES Innovative Smart Grid Technologies Conference - Latin America (ISGT Latin America)*, Gramado, 2019.
- [8] M. Caprolu, R. D. Pietro, S. Raponi, S. Sciancalepore και P. Tedeschi, «Vessels Cybersecurity: Issues, Challenges, and the Road Ahead,» *IEEE Communications Magazine*, τόμ. 58, αρ. 6, pp. 90-96, 2020.
- [9] E. D. Charitos, N. A. Kounalakis και I. Kantzavelou, «Cybersecurity at Merchant Shipping,» σε *2022 IEEE International Conference on Cyber Security and Resilience (CSR)*, Rhodes, Greece, 2022.
- [10] G. Kavallieratos, V. Diamantopoulou και S. K. Katsikas, «Shipping 4.0: Security Requirements for the Cyber-Enabled Ship,» *IEEE Transactions on Industrial Informatics*, τόμ. 16, αρ. 10, pp. 6617-6625, 2020.
- [11] K. Kanwal, W. Shi, C. Kontovas, Z. Yang και C.-H. Chang, «Maritime cybersecurity: are onboard systems ready?,» *Maritime Policy & Management*, τόμ. 51, αρ. 3, pp. 484-502, 2024.
- [12] P. Rajaram, M. Goh και J. Zhou, «Guidelines for cyber risk management in shipboard operational technology systems,» *Journal of Physics: Conference Series*, τόμ. 2311, αρ. 1, p. 012002, 2022.
- [13] D. Dolezilek, D. Gammel και W. Fernandes, «Cybersecurity based on IEC 62351 and IEC 62443 for IEC 61850 systems,» σε *15th International Conference on Developments in Power System Protection (DPSP 2020)*, Liverpool, 2020.

- [14] M. Wiboonrat, «Cybersecurity in Industrial Control Systems: An integration of information technology and operational technology,» σε *IECON 2022 – 48th Annual Conference of the IEEE Industrial Electronics Society*, Brussels, 2022.
- [15] K.-L. A. Yau, A. R. Syed, W. Hashim, J. Qadir, C. Wu και N. Hassan, «Maritime Networking: Bringing Internet to the Sea,» *IEEE Access*, τόμ. 7, pp. 48236-48255, 2019.
- [16] J. Pavur, D. Moser, M. Strohmeier, V. Lenders και I. Martinovic, «A Tale of Sea and Sky: On the Security of Maritime VSAT Communications,» σε *2020 IEEE Symposium on Security and Privacy (SP)*, San Francisco, 2020.
- [17] T. Neumann, «Cybersecurity in Maritime Industry,» *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, τόμ. 18, αρ. 4, pp. 765-774, 2024.
- [18] N. Bharot, P. Verma, R. H. Jhaveri και J. G. Breslin, «Cybersecurity Recommendations for Planning and Securing Port 4.0 and Maritime Industry Against Cyberattacks,» σε *2025 IEEE 12th International Conference on Data Science and Advanced Analytics (DSAA)*, Birmingham, 2025.
- [19] M. Li, J. Zhou, S. Chattopadhyay και M. Goh, «Maritime Cybersecurity: A Comprehensive Review,» *IEEE Transactions on Intelligent Transportation Systems*, pp. 1-23, 2024.
- [20] R. Vaarandi, L. Tsipoulos, G. Visky, M. U. Rehman και H. Bahşi, «A Systematic Literature Review of Cyber Security Monitoring in Maritime,» *IEEE Access*, τόμ. 13, p. 85307–85329, 2025.
- [21] M. A. Ben Farah, E. Ukwandu, H. Hindy, D. Brosset, M. Bures, I. Andonovic και X. Bellekens, «Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends,» *Information*, τόμ. 13, αρ. 1, 2022.
- [22] D. Šuškaló, Z. Morić, J. Redžepagić και D. Regvart, «Comparative Analysis of IBM QRadar and Wazuh for Security Information and Event Management,» σε *34th DAAAM International Symposium on Intelligent Manufacturing and Automation*, Vienna, 2023.
- [23] «IBM QRadar,» IBM, [Ηλεκτρονικό]. Available: <https://www.ibm.com/products/qradar>. [Πρόσβαση 16 May 2026].
- [24] «Splunk Enterprise Security,» Splunk, [Ηλεκτρονικό]. Available: https://www.splunk.com/en_us/products/enterprise-security.html. [Πρόσβαση 16 May 2026].
- [25] M. Hristov, M. Nenova, G. Iliev και D. Avresky, «Integration of Splunk Enterprise SIEM for DDoS Attack Detection in IoT,» σε *2021 IEEE 20th International Symposium on Network Computing and Applications (NCA)*, Sofia, 2021.
- [26] K. Bezas και F. Filippidou, «Comparative Analysis of Open Source Security Information & Event Management Systems (SIEMs),» *Indonesian Journal of Computer Science*, τόμ. 12, αρ. 2, pp. 443-468, 2023.
- [27] «Microsoft Sentinel security information and event management,» Microsoft, 22 April 2026. [Ηλεκτρονικό]. Available: <https://learn.microsoft.com/en-us/azure/sentinel/overview?tabs=defender-portal>. [Πρόσβαση 16 May 2026].

- [28] V. Dakić, Z. Morić, A. Kapulica και D. Regvart, «Leveraging Microsoft Sentinel and Logic Apps for Automated Cyber Threat Response,» *Edelweiss Applied Science and Technology*, τόμ. 8, αρ. 6, p. 4319–4348, 2024.
- [29] W. Hongkamnerd, P. Watanapongse, W. Tangtrongpairoj και S. Sanguanpong, «Effects of SIEM Recovery Time: Case Study on Security Onion,» σε *2024 21st International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, Khon Kaen, 2024.
- [30] «Security Onion,» Security Onion Solutions, [Ηλεκτρονικό]. Available: <https://securityonionsolutions.com/software/>. [Πρόσβαση 17 May 2026].
- [31] J. Manzoor, A. Waleed, A. F. Jamali και A. Masood, «Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs,» *PLOS ONE*, τόμ. 19, αρ. 3, p. e0301183, 2024.
- [32] Elastic, «Elastic Security solution & project type overview,» Elastic, [Ηλεκτρονικό]. Available: <https://www.elastic.co/docs/solutions/security>. [Πρόσβαση May 2026].
- [33] Graylog, «Graylog Security,» Graylog, [Ηλεκτρονικό]. Available: <https://graylog.org/products/security/>. [Πρόσβαση May 2026].
- [34] O. Owolafe και A. Alabi, «Comparative Analysis of Wazuh, Graylog, and ELK Stack for Cyber Threat Detection and Response,» σε *19th International Conference for Internet Technology and Secured Transactions (ICITST-2024)*, Oxford, 2024.
- [35] Wazuh, «Wazuh - Open Source XDR. Open Source SIEM,» Wazuh, Inc, [Ηλεκτρονικό]. Available: <https://wazuh.com/>. [Πρόσβαση April 2026].