Τίτλος Έργου	Προηγμένη ανίχνευση εισβολών και παράνομου ηλεκτρονικού περιεχομένου για τη διασφάλιση επιχειρησιακής και λειτουργικής ασφάλειας σε κατανεμημένα συστήματα συστημάτων		
Ακρωνύμιο Έργου	ΜΥΡΙΩΠΟΣ		
Κωδικός Έργου	Τ2ΕΔΚ-04665		
Πρόσκληση / Θέμα	ΕΡΕΥΝΩ – ΔΗΜΙΟΥΡΓΩ - ΚΑΙΝΟΤΟΜΩ Β' ΚΥΚΛΟΣ / ΑΝΤΑΓΩΝΙΣΤΙΚΟΤΗΤΑ, ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΤΗΤΑ & ΚΑΙΝΟΤΟΜΙΑ		
Ημερομηνία Εκκίνησης	16/06/2020	Διάρκεια	30 Μήνες

Π3.1 Προηγμένοι αλγόριθμοι και μηχανισμοί μοντελοποίησης απειλών, αξιολόγησης κινδύνων και εφαρμογής πολιτικών ανάκαμψης

Ενότητα Εργασίας	**ΕΕ3 Κατανεμημένη Βαθιά Ανάλυση και Νοημοσύνη Κυβερνοαπειλών**
Επικεφαλής	**UBITECH**
Συνεισφορές	**MAGGIOLI**

Περιεχόμενα

Συντομογραφίες

API	Application Programming Interface
APL	Attack Pattern Likelihood
CPE	Common Platform Enumeration
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
NIST	National Institute of Standards and Technology
VSL	Vulnerability Severity Level

Λίστα Εικόνων

Λίστα Πινάκων

Περίληψη

Το παραδοτέο Π3.1, περιγράφει τους αλγορίθμους και τις υπηρεσίες λογισμικού που αναπτύχθηκαν για την αξιολόγηση του κυβερνο-κινδύνου ενός οργανισμού, λαμβάνοντας υπόψη τους ψηφιακούς του πόρους. Στο παραδοτέο Π3.1 παρουσιάζεται και αναλύεται όλη η διαδικασία υπολογισμού και εξαγωγής ποσοτικών μετρικών που εκφράζουν την κρισιμότητα του κάθε πόρου ξεχωριστά, αλλά και την κρισιμότητα των ψηφιακών πόρων συνολικά εντός του οργανισμού. Το επίπεδο αξιολόγησης κινδύνου του συστήματος του ΜΥΡΙΩΠΟΥ, αξιοποιεί υπάρχοντα ανοικτά δεδομένα για ευπάθειες, αδυναμίες λογισμικού και υλικού από διεθνείς έγκριτες συλλογές, καθώς και πιθανών επιθέσεων, τα οποία συνδυάζονται με τους ψηφιακούς πόρους του οργανισμού ώστε να υπολογιστούν πιθανά μονοπάτια επιθέσεων και να παραχθούν σχετικές αναφορές που αποτυπώνουν τόσο ποσοτικά όσο και ποιοτικά την αξιολόγηση του κυβερνο-κινδύνου ανά ψηφιακό πόρο και συνολικά εντός του οργανισμού.

1. Εισαγωγικά Στοιχεία

1.1 Πεδίο Εφαρμογής και Στόχοι Παραδοτέου

Σε ένα κόσμο ολοένα και πιο ψηφιακό, οι οργανισμοί προσαρμόζονται ψηφιοποιώντας όσο είναι δυνατόν τις διεργασίες τους, εμπλουτίζοντας τις υπηρεσίες του με ψηφιακούς πόρους τόσο σε επίπεδο υλικού όσο και λογισμικού. Εκτός από την πληθώρα των πλεονεκτημάτων που επιφέρει ένας τέτοιος ψηφιακός μετασχηματισμός, ένα σύνολο απειλών έρχεται να προστεθεί στους κινδύνους που μπορεί να επηρεάσουν την εύρυθμη λειτουργία των ψηφιακών συστημάτων/πόρων και των εφαρμογών που υποστηρίζουν σε πελάτες και στην αγορά. Αδυναμίες υλικού ή λογισμικού, μπορεί να χρησιμοποιηθούν από κακόβουλους χρήστες, ώστε να προσβάλουν τη λειτουργία του οργανισμού ή να αποσπάσουν κρίσιμες πληροφορίες. Η καταγραφή/μοντελοποίηση των ψηφιακών πόρων καθώς και των αδυναμιών τους, που δύναται να χρησιμοποιηθούν από κακόβουλους χρήστες, είναι μια δύσκολη διαδικασία που απαιτεί την εναρμόνιση και το συνεχή συγχρονισμό με εξωτερικές και έγκριτες πήγες ανοικτών δεδομένων.

Το παραδοτέο Π3.1 παρουσιάζει και περιγράψει λεπτομερώς τον τρόπο με τον οποίο το σύστημα ΜΥΡΙΩΠΟΣ, υλοποιεί την καταγραφή/μοντελοποίηση των ψηφιακών πόρων ενός οργανισμού, πως τους συνδέει με πιθανές απειλές, αξιοποιώντας τις επίσημες εξωτερικές πηγές (NIST, MITRE). Επίσης, εκτός από τη συσχέτιση ενός ψηφιακού πόρου με απειλές, το σύστημα ΜΥΡΙΩΠΟΣ παράγει μετρικές που αντανακλούν την κρισιμότητα κάθε ψηφιακού πόρου ξεχωριστά αλλά και συνολικά του οργανισμού, ως το άθροισμα των ψηφιακών πόρων που διαθέτει. Το εύρος της τεχνικής αρχιτεκτονικής του ΜΥΡΙΩΠΟΥ, αφορά τόσο στην περιμετρική θωράκιση ενός οργανισμού μέσω Συστημάτων Ανίχνευσης και Αποτροπής Εισβολής, όσο και στην συνεχή αξιολόγηση των ευπαθειών των ψηφιακών πόρων. Το παραδοτέο Π3.1 παρουσιάζει και περιγράφει σε τεχνικό βάθος το τμήμα της αρχιτεκτονικής λύσης και των υπηρεσιών λογισμικού που αναπτύχθηκαν που αφορούν στην αξιολόγηση του κυβερνο-κινδύνου μέσω των ευπαθειών των ψηφιακών πόρων.

1.2 Συσχέτιση με Δράσεις και Ενότητες Εργασίας του ΜΥΡΙΩΠΟΥ

Το παραδοτέο Π3.1 παρουσιάζει τα αποτελέσματα σε επίπεδο σχεδιασμού της αρχιτεκτονικής λύσης και των υπηρεσιών λογισμικού που αναπτύχθηκαν στα πλαίσια της Δράσης 3.1 Μοντελοποίηση απειλών, πλαίσιο αξιολόγησης κινδύνων και εφαρμογής πολιτικών ανάκαμψης. Επίσης, είναι το πρώτο (1ο) παραδοτέο της ενότητας εργασίας αναφορικά με την ΕΕ3 Κατανεμημένη Βαθιά Ανάλυση και Νοημοσύνη Κυβερνοαπειλών. Ως τμήμα του ενοποιημένου Πλαισίου ΜΥΡΙΩΠΟΣ τόσο η Δράση 3.1 όσο και το παραδοτέο Π3.1 είναι υπεύθυνα και υποστηρίζουν το σύνολο των υφιστάμενων συστημάτων διαχείρισης δεδομένων, των προγραμματιστικών διεπαφών (APIs – Application Programming Interfaces) και των υπολογισμών που είναι απαραίτητα για τη ποιοτική και ποσοτική αξιολόγηση των κυβερνο-κινδύνων.

1.3 Δομή Παραδοτέου

Το παραδοτέο Π3.1 περιγράφει στο **Κεφάλαιο 1 – Εισαγωγή**, τον γενικό σκοπό του παραδοτέου. Τεκμηριώνει επίσης τη θέση του παραδοτέου στο έργο, δηλαδή τη σχέση του συγκεκριμένου παραδοτέου με τα υπόλοιπα

παραδοτέα, δράσεις και ενότητες εργασίας του έργου ΜΥΡΙΩΠΟΣ, καθώς και πώς η γνώση που παράγεται στα άλλα παραδοτέα και ενότητες εργασίας χρησιμεύουν ως είσοδο στο εν λόγω παραδοτέο.

Στη συνέχεια στο **Κεφάλαιο 2 – Μοντελοποίηση Απειλών και Ανάλυση Ευπάθειας**, επικεντρωνόμαστε στην ανάλυση των απειλών και στις μετρικές που βασιζόμαστε για τον υπολογισμό και την αποτύπωση του επιπέδου επικινδυνότητας, συνεπώς και ρίσκου-κινδύνου.

Στη συνέχεια στο **Κεφάλαιο 3 – Γράφοι Αλληλεξάρτησης Ψηφιακών Πόρων**, περιγράφουμε πώς μοντελοποιούνται και αναπαρίστανται οι ψηφιακοί πόροι (π.χ. σε επίπεδο λογισμικό και υλικό) ενός οργανισμού, καθώς και τη διαδικασία καταχώρησής τους στο σύστημα ΜΥΡΙΩΠΟΣ.

Στη συνέχεια στο **Κεφάλαιο 4 – Αξιολόγηση και Ποσοτικοποίηση του Κινδύνου**, αναλύουμε τον τρόπο με τον οποίο οδηγούμαστε στην εξαγωγή των μετρικών του κινδύνου. Συγκεκριμένα, αναφέρουμε τον τρόπο με τον οποίο συσχετίζουμε τους ψηφιακούς πόρους του οργανισμού με επιθέσεις, καθώς και τη διαδικασία δημιουργίας του υπολογισμού της εκτίμησης κινδύνου στην πλατφόρμα ΜΥΡΙΩΠΟΣ.

Στη συνέχεια στο **Κεφάλαιο 5 – Υπολογισμός Κρισιμότητας Ψηφιακών Πόρων**, περιγράφουμε πως η αξία ενός ψηφιακού πόρου συμβάλει στον υπολογισμό της κρισιμότητας του.

Στη συνέχεια στο **Κεφάλαιο 6 – Ροή Διεργασιών Αξιολόγησης Κινδύνου**, αποτυπώνουμε την αρχιτεκτονική του συστήματος ΜΥΡΙΩΠΟΣ, που σχετίζεται με την αξιολόγηση του κινδύνου.

Στη συνέχεια στο **Κεφάλαιο 7 – Αξιολόγηση Κινδύνου στο Σύστημα ΜΥΡΙΩΠΟΣ**, περιγράφουμε την εμπειρία του χρήστη στο ενοποιημένο σύστημα ΜΥΡΙΩΠΟΣ καθώς και τη ροή εργασιών που χρειάζεται να ακολουθήσει για να πάρει ως αποτέλεσμα την εκτίμηση του κυβερνο-κινδύνου .

Στη συνέχεια στο **Κεφάλαιο 8 – Εφαρμογή Πολιτικών Ανάκαμψης**, παρουσιάζουμε την εφαρμογή διαφορετικών πολιτικών ανάκαμψης σε επίπεδο δικτύου, IP διευθύνσεων, θυρών (π.χ. ports) εφαρμογής, οι οποίες έχουν ως αποτέλεσμα το μετριασμό και τη μείωση του συνολικού ρίσκου/κινδύνου ενός οργανισμού.

Τέλος, το παραδοτέο ολοκληρώνεται με το **Κεφάλαιο 9 – Επίλογος**, το οποίο αναφέρει τα κύρια αποτελέσματα και ευρήματα του παραδοτέου και παρέχει ένα πλάνο που θα καθοδηγήσει τις μελλοντικές ερευνητικές και τεχνολογικές προσπάθειες της σύμπραξης.

2. Μοντελοποίηση Απειλών και Ανάλυση Ευπάθειας

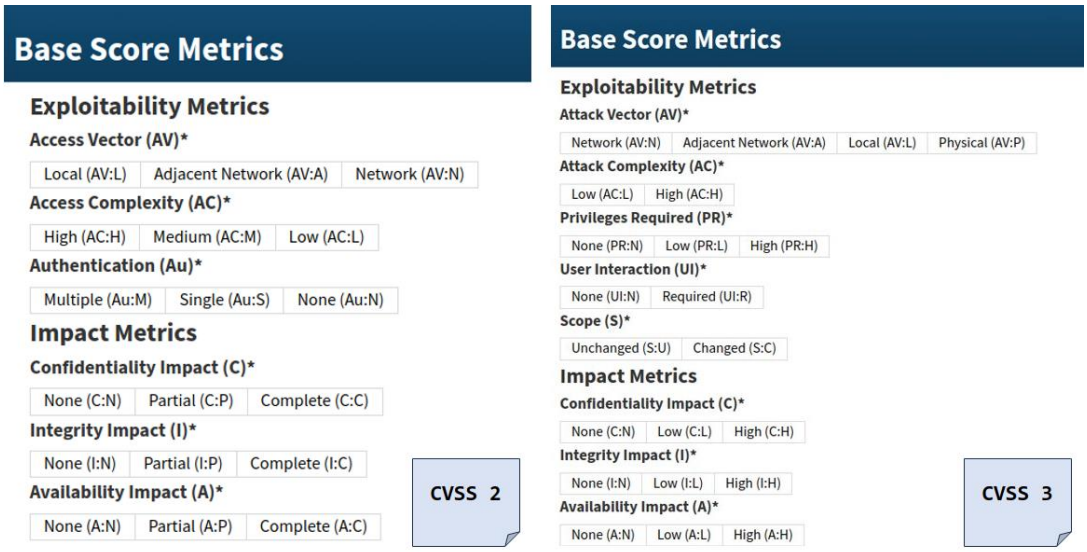
Σε αυτήν την ενότητα παρουσιάζουμε το σύνολο των απειλών στα πλαίσια ενός οργανισμού και το αντιστοιχίζουμε στην ανοικτή βάση δεδομένων κοινών ευπαθειών (CVE[1]). Ως εσωτερική διαδικασία (background process) έχουμε αυτοματοποιήσει και υλοποιήσει την αντιστοίχιση των ψηφιακών πόρων-απειλών και ευπαθειών που αξιοποιείται και παρουσιάζεται ενδελεχώς στην ενότητα αξιολόγησης και ποσοτικοποίησης του κινδύνου (βλ. Κεφάλαιο 4).

Η ανάλυση ευπάθειας του ΜΥΡΙΩΠΟΥ παράγει μια μετρική (δλδ. την VSL = Vulnerability Severity Level), διακριτού μεγέθους, που αντικατοπτρίζει το επίπεδο επικινδυνότητας της ευπάθειας. Η μετρική αυτή, λαμβάνει υπόψη το συνολικό σκορ (εκμεταλλευσιμότητα πόρου και επιπτώσεις) επικινδυνότητας της ευπάθειας κληρονομώντας τους υπολογισμούς και τους κανόνες από τις μεθόδους CVSS 2 και CVSS 3. Προς διευκόλυνση του αναγνώστη, υπενθυμίζουμε ότι το CVSS 2 υποστηρίζεται για την αποτίμηση παλιών ευπαθειών και το CVSS 3 υποστηρίζεται για την αποτίμηση νέων ευπαθειών. Ως εκ τούτου, η μοντελοποίηση απειλών υποστηρίζει συμβατότητα με το παρελθόν και συγχρονικότητα με τις νέες μεθόδους. Οι παλαιότερες ευπάθειες υποστηρίζουν μόνο τη παλιά μέθοδο CVSS 2, ενώ πιο νέες υποστηρίζουν είτε μόνο τη μέθοδο 3 ή και τις δυο.

Η μετρική CVSS αποτελείται από 3 επιμέρους μετρικές, το Base Score, το Temporal Score και το Environmental Score. Το Base Score του CVSS υπολογίζεται θεωρώντας σταθερά τα χαρακτηριστικά της ευπάθειας στο χρόνο καθώς στα διαφορετικά περιβάλλοντα εκτέλεσης, σύμφωνα με το MITRE CVE. Όσον αφορά στο Temporal Score του CVSS, αυτό συμπληρώνεται από τον οργανισμό, λαμβάνοντας υπόψη τα εφαρμοσμένα στοιχεία ελέγχου από αυτόν και αναφέρεται σε χαρακτηριστικά ευπάθειας που μπορεί να αλλάξουν με τη πάροδο του χρόνου. Ενδεικτικά, αυτά μπορεί να είναι η αναβάθμιση έκδοσης λογισμικού, η επιδιόρθωση λογισμικού μέσω patch, κτλ. Τέλος, στο Environmental Score λαμβάνουμε υπόψη τα χαρακτηριστικά ευπάθειας που επηρεάζονται από το περιβάλλον εκτέλεσης που διαθέτει ο οργανισμός. Στο σύστημα ΜΥΡΙΩΠΟΣ υποστηρίζουμε μόνο τη μετρική Base από τις μεθόδους CVSS 2 [1] και του CVSS 3 [2], καθώς οι υπόλοιπες (Temporal και Environmental) έχουν υποκειμενικό χαρακτήρα και ορίζονται από το χρήστη. Επίσης να τονίσουμε, ότι η συμπλήρωση των παραμέτρων της μετρικής Base γίνεται από την NIST και είναι σταθερή για κάθε διαφορετική ευπάθεια.

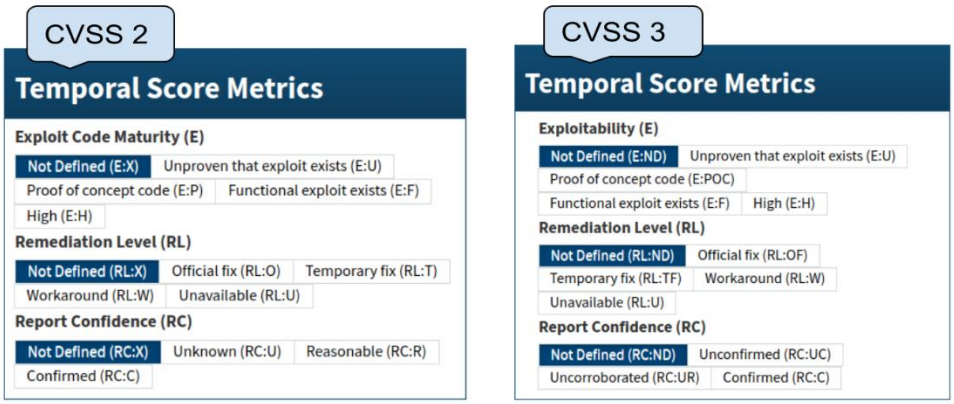
Στη παρακάτω εικόνα βλέπουμε πως διαμορφώνεται η Base μετρική για το CVSS 2 και το CVSS 3.

[1] σαν πηγή των CVE χρησιμοποιούμε τη NIST: https://nvd.nist.gov/vuln

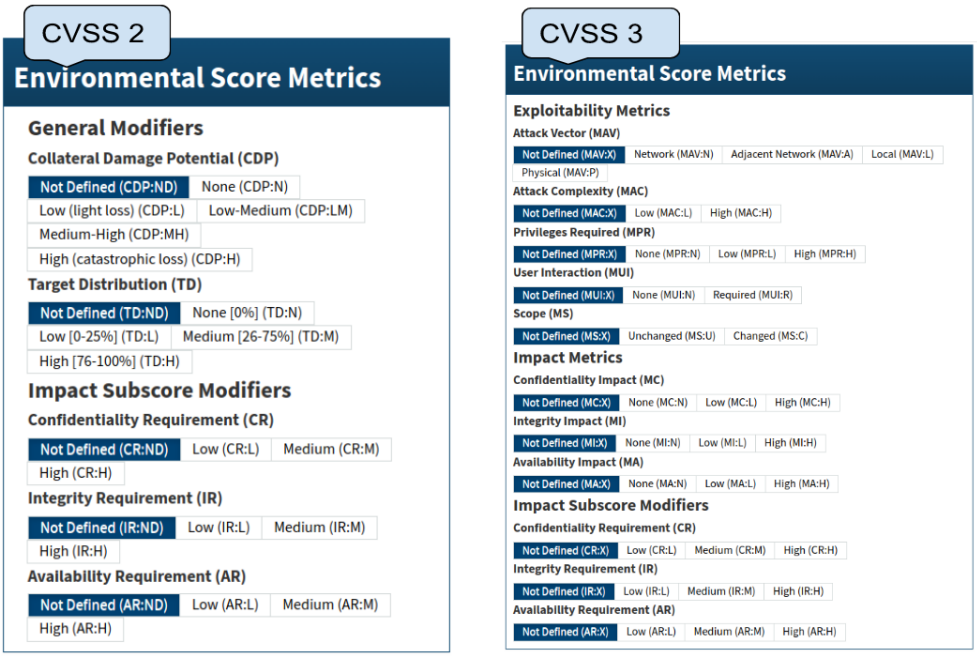


Εικόνα 1. Το Base Score στο CVSS 2 και στο CVSS 3.

Ενδεικτικά, παραθέτουμε στις εικόνες που ακολουθούν πως διαμορφώνονται και οι άλλες δυο μετρικές του CVSS 2 και 3, το Temporal και Environmental Score. Ποιοτικά, αυτό σημαίνει ότι στην αξιολόγηση κινδύνου σημαντικό παράγοντα παίζει ο χρόνος και οι ενέργειες που έχουν μεσολαβήσει (π.χ. αναβάθμιση λογισμικού, εφαρμογή patch, κτλ.) μεταξύ 2 αξιολογήσεων. Επίσης, σημαντικό ρόλο παίζει και η διαμόρφωση του υπολογιστικού περιβάλλοντος που φιλοξενεί μια εφαρμογή (π.χ. αν λαμβάνονται τακτικά backups, αν εφαρμόζονται ισχυροί κανόνες για credentials, κτλ.).



Εικόνα 2. Το Temporal Score στο CVSS 2 και στο CVSS 3.

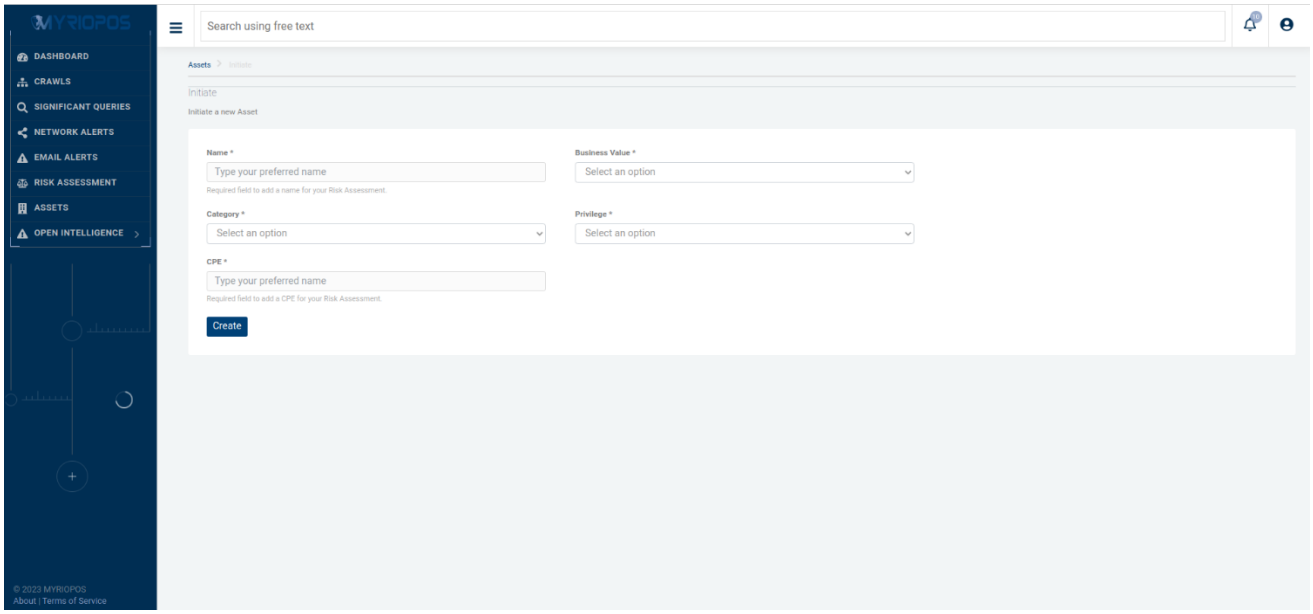


Εικόνα 3. Το Environmental Score στο CVSS 2 και στο CVSS 3.

3. Αναπαράσταση Ψηφιακών Πόρων

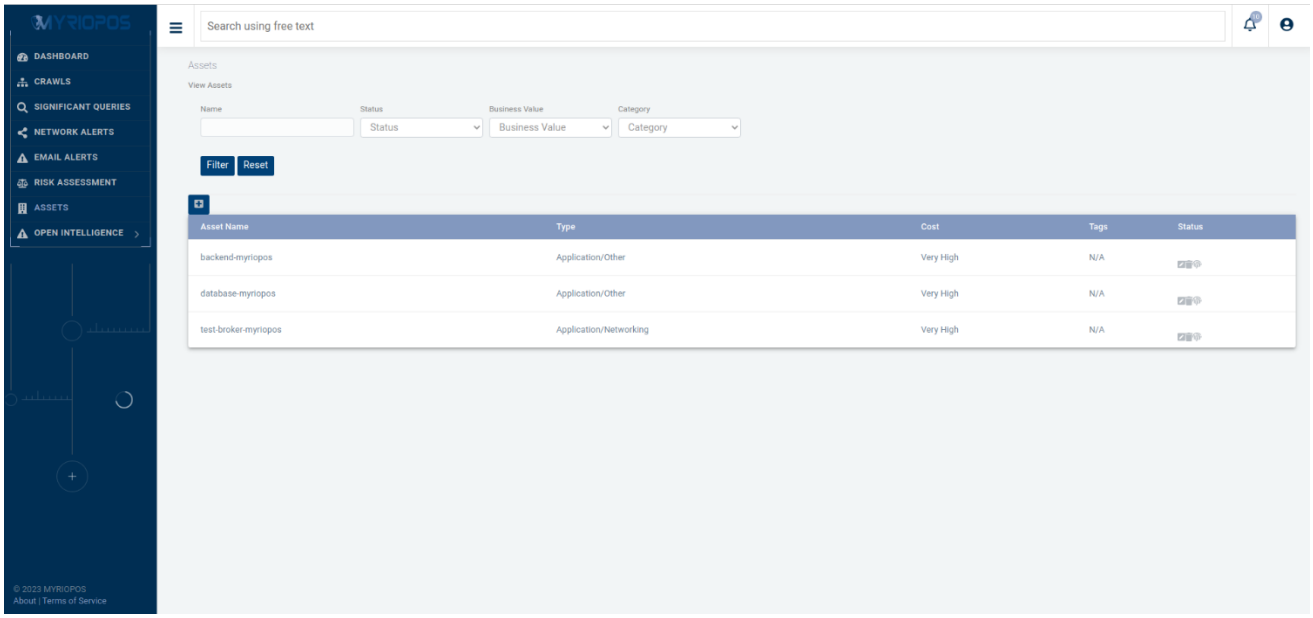
Στο έργο ΜΥΡΙΩΠΟΣ, ένας ψηφιακός πόρος διαθέτει ένα σύνολο από χαρακτηριστικά, όπως ο τύπος του, το CPE (Common Platform Enumeration – ταυτίζεται με το υλικό και λογισμικό που υποστηρίζει), η κρισιμότητα, τα οποία είναι απαραίτητα προκειμένου να γίνει η αξιολόγηση του κινδύνου.

Σχετικά με το CPE, το μοντέλο της MITRE CPE (MITRE Common Platform Enumeration) αναφέρεται σε κάθε υπολογιστική (σταθερός/φορητός υπολογιστής, εξυπηρετητής κλπ.) και διαδικτυακή μονάδα (δρομολογητής κλπ.), σε εκτυπωτή, σε ηλεκτρονικές συσκευές (κάμερες που συνδέονται στο διαδίκτυο), σε εφαρμογές, σε λογισμικά και υπολογιστικά συστήματα. Η αναπαράσταση αυτών και των χαρακτηριστικών τους γίνεται σε μορφή συμβολοσειράς, όπου θα δούμε στη συνέχεια (εκδόσεις κλπ.). Μέσω της πλατφόρμας του ΜΥΡΙΩΠΟΣ, δίνεται η δυνατότητα στον οργανισμό να εισάγει τους ψηφιακούς πόρους που διαθέτει. Στην Εικόνα 4 βλέπουμε τη διεπαφή χρήστη του ΜΥΡΙΩΠΟΣ στην οποία γίνεται εισαγωγή ενός πόρου.



Εικόνα 4. Δημιουργία Νέου Ψηφιακού Πόρου του Συστήματος ΜΥΡΙΩΠΟΣ.

Εκτός από την ονομασία του πόρου, συμπληρώνονται και η αξία του πόρου στα πλαίσια του οργανισμού, η κατηγορία που ανήκει, με τι δικαιώματα έχουν πρόσβαση σε αυτό τον πόρο (privilege), καθώς και το CPE, όπως αναφέραμε πιο πάνω. Έχοντας εισάγει τους ψηφιακούς πόρους ο χρήστης του οργανισμού στο σύστημα ΜΥΡΙΩΠΟΣ, αυτοί στη συνέχεια φαίνονται συγκεντρωτικά με τη χρήση πίνακα, όπως απεικονίζεται στην Εικόνα 5.



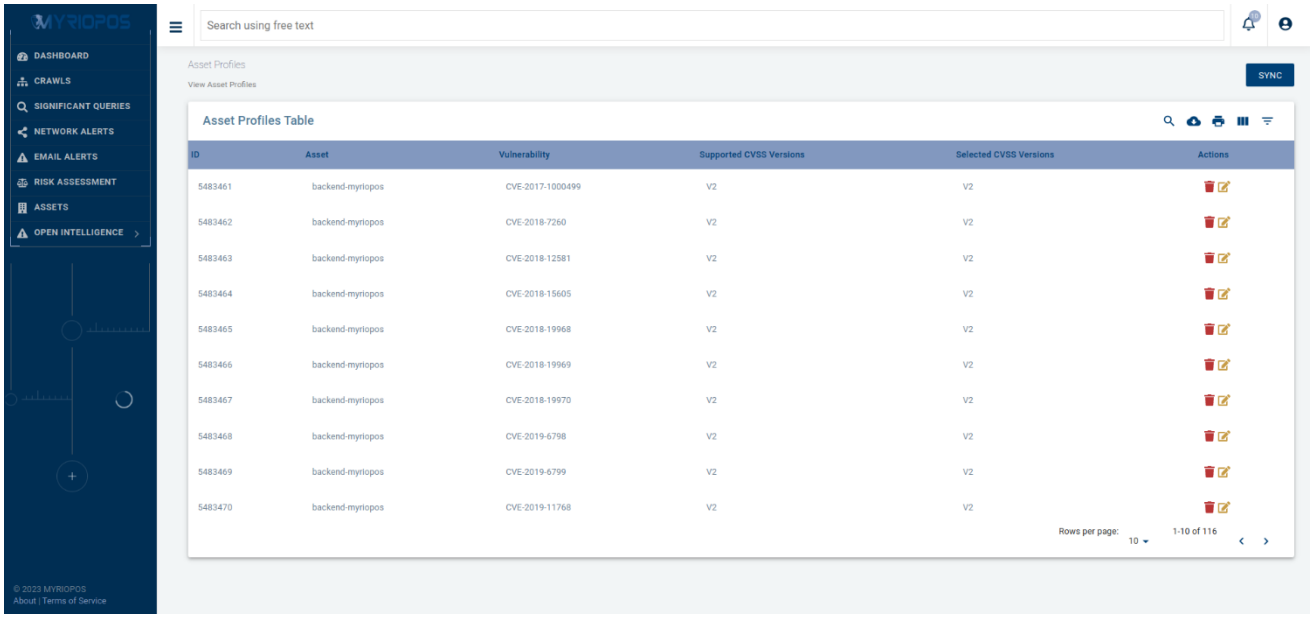
Εικόνα 5. Ψηφιακοί Πόροι του Συστήματος ΜΥΡΙΩΠΟΣ.

4. Αξιολόγηση και Ποσοτικοποίηση Κινδύνου

Σε αυτή την ενότητα, περιγράφουμε πως τελικά από μια λίστα ψηφιακών πόρων, εξάγουμε μετρικές κινδύνου, εκτός από τις μεθόδους CVSS. Στην προηγούμενη ενότητα παρουσιάσαμε τη δημιουργία των ψηφιακών πόρων, κατά την οποία σχετίζουμε έναν πόρο με ένα CPE. Το CPE είναι μια συμβολοσειρά που έχει την εξής μορφή:

```
cpe:/ <part>:<vendor>:<product>:<version>:<update>:<edition>:<language>
```

Βλέπουμε ότι με μεγάλη ακρίβεια μπορούμε να περιγράψουμε κάθε είδους ψηφιακού πόρου, εισάγοντας συγκεκριμένες εκδόσεις, αναβαθμίσεις, κλπ. Έχοντας ενώσει ψηφιακούς πόρους με CPEs, το σύστημα ΜΥΡΙΩΠΟΣ, αξιοποιεί τις ανοικτές βάσεις δεδομένων της NIST vulnerabilities και products, προκειμένου να λάβει τις ευπάθειες (CVEs) που αντιστοιχούν στα συγκεκριμένα CPEs και κατά επέκταση στους ψηφιακούς πόρους του οργανισμού. Αυτό δημιουργεί για κάθε ψηφιακό πόρο, ένα προφίλ που περιλαμβάνει τις ευπάθειες που αντιστοιχούν σε αυτόν. Το προφίλ των πόρων του οργανισμού είναι διαθέσιμο μέσω της πλατφόρμας ΜΥΡΙΩΠΟΣ και φαίνεται στην Εικόνα 6.

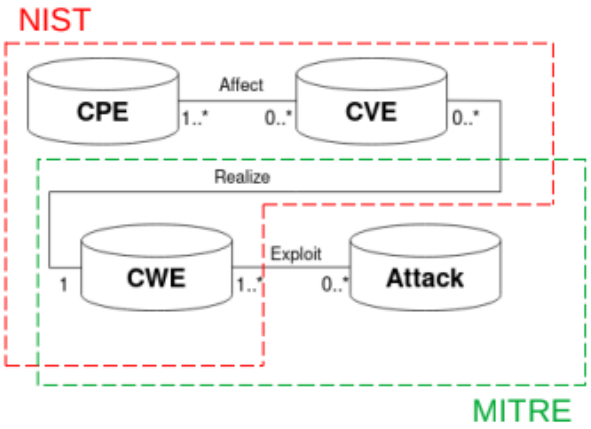


Εικόνα 6. Προφίλ Ψηφιακών Πόρων του Συστήματος ΜΥΡΙΩΠΟΣ.

Επιπλέον, δίνεται η δυνατότητα να γίνει συγχρονισμός με την εξωτερική ανοικτή βάση δεδομένων της NIST, ανά πασά στιγμή, προκειμένου να συμπεριληφθούν στο προφίλ των ψηφιακών πόρων ακόμη και οι πιο πρόσφατες ευπάθειες. Αυτό επιτυγχάνεται μέσω του κουμπιού “SYNC”.

Σύμφωνα με τις ευπάθειες της MITRE, κάθε ευπάθεια συσχετίζεται με ορισμένες αδυναμίες λογισμικού (software) ή υλικού (hardware) (CWE – Common Weakness Enumeration), οι οποίες περιγράφουν μια κατάσταση όπου υπό ορισμένες συνθήκες, θα μπορούσε να συμβάλει στην εισαγωγή ευπαθειών στο σύστημα ενός οργανισμού.

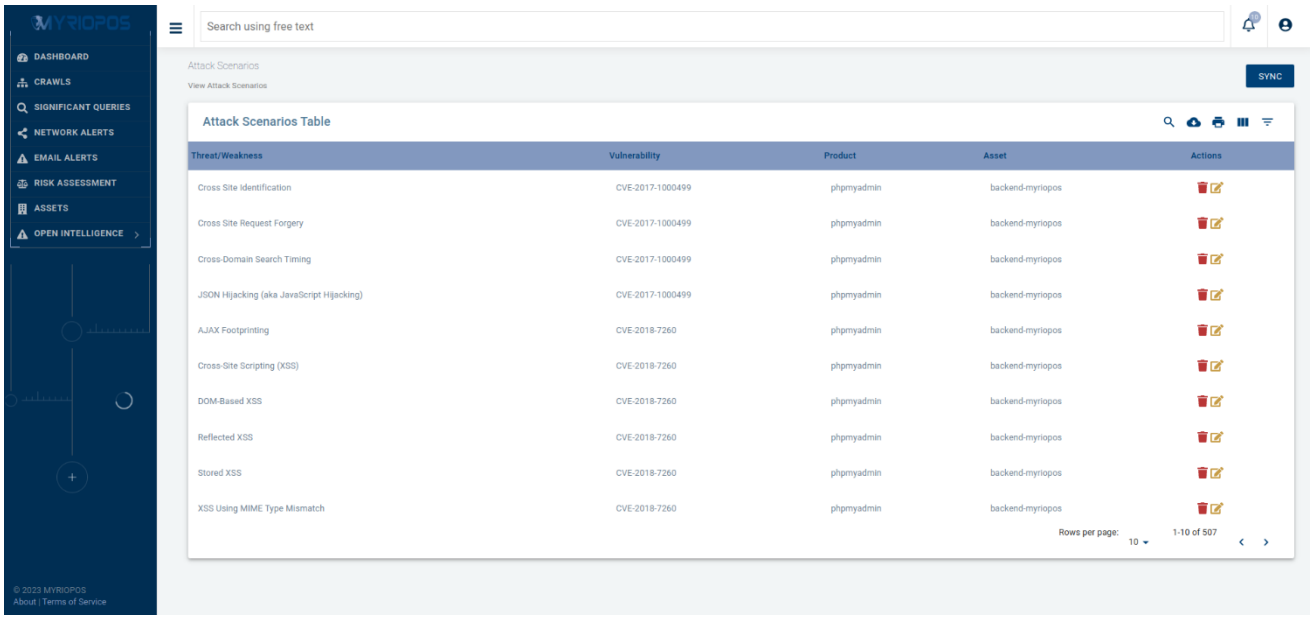
Επιπροσθέτως, κάθε CWE, σχετίζεται με ορισμένα **μοτίβα επιθέσεων** (**Attack Patterns**), τα οποία, πρακτικά είναι η επίθεση που μπορεί να κάνει ο επιτιθέμενος (πχ SQL Injection). Συνεπώς έχουμε μια αντιστοίχιση μεταξύ CVE σε CWE και σε Attack Pattern (ή αλλιώς Threat). Η παρακάτω εικόνα περιγράφει τις σχέσεις μεταξύ των διαφορετικών απαριθμήσεων και την ένωση που κάναμε στα πλαίσια του ΜΥΡΩΠΟΣ (CPE, CVE, CWE, Attack/Threat).



Εικόνα 7. Σχέσεις μεταξύ διαφορετικών απαριθμήσεων (CPE, CVE, CWE) και επιθέσεων (Attacks).

Συνολικά, μέσω της πλατφόρμας του ΜΥΡΙΩΠΟΣ υπάρχει μια πλήρης εικόνα, για τις διαφορετικές επιθέσεις ("Attack Patterns") που μπορεί να κάνει ο επιτιθέμενος σε έναν οργανισμό καθώς και τους ψηφιακούς πόρους που έχουν τις ευπάθειες που αντιστοιχούν στις διαφορετικές επιθέσεις. Μια τριπλέτα που αποτελείται από ένα ψηφιακό πόρο, μια ευπάθεια και μια επίθεση, αποτελεί ένα **σενάριο επίθεσης** (**Attack Scenario**).

Για παράδειγμα, η παρακάτω εικόνα δείχνει τις διαφορετικές **απειλές** (**Threats**), που μπορεί να πραγματοποιηθούν, σε ποιες ευπάθειες αντιστοιχούν, καθώς και ποιος ψηφιακός πόρος έχει αυτή την ευπάθεια. Οπότε κατά επέκταση, ο πίνακας παρουσιάζει τους ψηφιακούς πόρους ενός οργανισμού και τις πιθανές απειλές προς αυτόν, πάντα σύμφωνα με τα τελευταία δεδομένα από τη NIST.



Εικόνα 8. Σενάρια επιθέσεων του Συστήματος ΜΥΡΙΩΠΟΣ.

Τα Asset Profiles και τα Attack Scenarios που ορίσαμε παραπάνω, είναι τα θεμέλια για την εξαγωγή των μετρικών του κινδύνου, καθώς με βάση αυτά συνδέουμε τους ψηφιακούς πόρους με τις ευπάθειες και κατά επέκταση με τις απειλές. Η δυνατότητα ποσοτικοποίησης του κινδύνου μας δίνεται μέσω ορισμένων εξισώσεων που βασίζονται στις παραμέτρους της μετρικής Base Score του CVSS 2 ή 3. Συγκεκριμένα, για κάθε ευπάθεια (CVE) υπολογίζουμε δυο επιπλέον μετρικές, την εκμεταλλευσιμότητα (exploitability) και τις επιπτώσεις (impact), όπου κάθε μια βασίζεται σε διαφορετικές παραμέτρους του Base Score.

Το Exploitability (Exp) εκφράζει πόσο πιθανό είναι μια ευπάθεια να χρησιμοποιηθεί από έναν επιτιθέμενο και υπολογίζεται με βάση την παρακάτω εξίσωση:

- $Exp = 8.22 \times AV \times AC \times PR \times UI\ (CVSS\ 3)$
  - AV είναι το Attack Vector
  - AC είναι το Attack Complexity
  - PR είναι το Privileges Required
  - UI είναι το User Interaction
- $Exp = 8.22 \times AV \times AC \times AU\ (CVSS\ 2)$
  - AV είναι το Attack Vector
  - AC είναι το Attack Complexity
  - AU είναι το Authenticaiton

Το αποτέλεσμα της εξίσωσης είναι μια τιμή από το 0 ως το 10, και προκειμένου το αποτέλεσμα να είναι πιο φιλικό προς το χρήστη το αντιστοιχούμε σε ονομαστικές τιμές σύμφωνα με το παρακάτω πίνακα:

Αριθμητική τιμή	Ονομαστική τιμή
$0 \leq Exp < 2$	Very Low
$2 \leq Exp < 4$	Low
$4 \leq Exp < 6$	Medium
$6 \leq Exp < 8$	High
$8 \leq Exp \leq 10$	Very High

Πίνακας 1. Αντιστοίχιση Αριθμητικής Τιμής σε Ονομαστική της μεταβλητής Exp.

Αντίστοιχα, το Impact Level (IL), εκφράζει τις επιπτώσεις μια ευπάθειας σε έναν οργανισμό, με βάση την παρακάτω εξίσωση η οποία ισχύει και για το CVSS 2 και 3:

$$IL = 1 - [(1 - C) \times (1 - I) \times (1 - A)]$$

Όπου "C" αντιστοιχεί στο Confidentiality, "I" στο Integrity και "A" στο Availability.

Στη περίπτωση του CVSS 3, υπάρχει ένας επιπλέον υπολογισμός που βασίζεται στη τιμή της παραμέτρου Scope:

$$IL = \begin{cases} 6.42 * IL, & \text{if } Scope = Unchanged \\ 7.52 * [IL - 0.029] & \\ -3.25 * [IL - 0.02]^{15}, & \text{otherwise} \end{cases}$$

Το αποτέλεσμα των παραπάνω εξισώσεων παίρνει αριθμητικές τιμές από 0 έως 10 και με βάση τον Πίνακας 1, αντιστοιχίζουμε ονομαστικές τιμές για να είναι πιο φιλικές προς τον τελικό χρήστη.

Στο σύστημα του ΜΥΡΙΩΠΟΣ έχουμε δημιουργήσει τα σενάρια επίθεσης (attack scenarios), που αποτελούνται από ένα ψηφιακό πόρο, μια ευπάθεια και μια επίθεση. Η βιβλιοθήκη της MITRE μας παρέχει μια πολύ σημαντική πληροφορία για κάθε επίθεση, την οποία εκμεταλλευόμαστε για να παράξουμε την πιθανότητα να συμβεί ένα σενάριο επίθεσης. Συγκεκριμένα, η MITRE μας δίνει την πιθανότητα να πραγματοποιηθεί μια επίθεση (APL = Attack Pattern Likelihood), την οποία συνδυάζουμε με την πιθανότητα μια ευπάθεια να χρησιμοποιηθεί, βρίσκοντας έτσι την πιθανότητα ενός σεναρίου επίθεσης. Ο συνδυασμός των δυο πιθανοτήτων γίνεται με την παρακάτω εξίσωση:

$$P_{\Sigma ΕΝΑΡΙΟΥ} = \frac{Exp + APL}{2}$$

Για καλύτερη εμπειρία χρήστη, τοποθετούμε στον άξονα Χ τις τιμές της μεταβλητής $P_{\Sigma ΕΝΑΡΙΟΥ}$ και στον αξονα Υ τις τιμές της μεταβλητής IL και δημιουργούμε ένα χάρτη θερμότητας (heatmap) όπως παρουσιάζεται στον Πίνακας 2.

ΚΙΝΔΥΝΟΣ						
	Very High	*Very High*	*Very High*	*Very High*	*Very High*	*Very High*

IL	High	*High*	*High*	*High*	*Very High*	*Very High*
	Medium	*Medium*	*Medium*	*Medium*	*High*	*High*
	Low	*Low*	*Low*	*Low*	*Medium*	*Medium*
	Very Low	*Very Low*	*Very Low*	*Low*	*Low*	*Low*
		Very Low	Low	Medium	High	Very High
		Πιθανότητα σεναρίου επίθεσης [Υπολογισμός - Εξίσωση]				

Πίνακας 2. Υπολογισμός ρίσκου για σενάρια επίθεσης.

Ένα σενάριο επίθεσης έχει IL (Impact Level) και μια πιθανότητα πραγματοποίησης, το κελί από τον παραπάνω πίνακα που αντιστοιχεί στις προηγούμενες τιμές, αντιπροσωπεύει τον κίνδυνο για το σενάριο επίθεσης και κατά επέκταση για τον ψηφιακό πόρο του σεναρίου. Το χρώμα κάθε κελιού δηλώνει την κρισιμότητα του κίνδυνου. Για παράδειγμα το χρώμα μωβ, δηλώνει Μεσαίο - Medium κίνδυνο. Οπότε, πλέον κάθε σενάριο επίθεσης αντιστοιχεί σε ένα συγκεκριμένο κελί $(\boldsymbol{P_{\Sigma\text{ΕΝΑΡΙΟΥ}}}, \boldsymbol{IL})$, το οποίο έχει μια συγκριμένη τιμή κινδύνου. Για παράδειγμα, έστω ότι ένα σενάριο αποτελείται από τα εξής:

- Ψηφιακός πόρος είναι η “PHP”
- Η ευπάθεια είναι η CVE-2006-5525 με $Exp = 4.9$ και $IL = 6.4$ (CVSS 2)
- Η επίθεση είναι “SQL Injection” με $APL = 7$

Με βάση τον Πίνακας 2, το Impact Level είναι High και η πιθανότητα σεναρίου επίθεσης είναι:

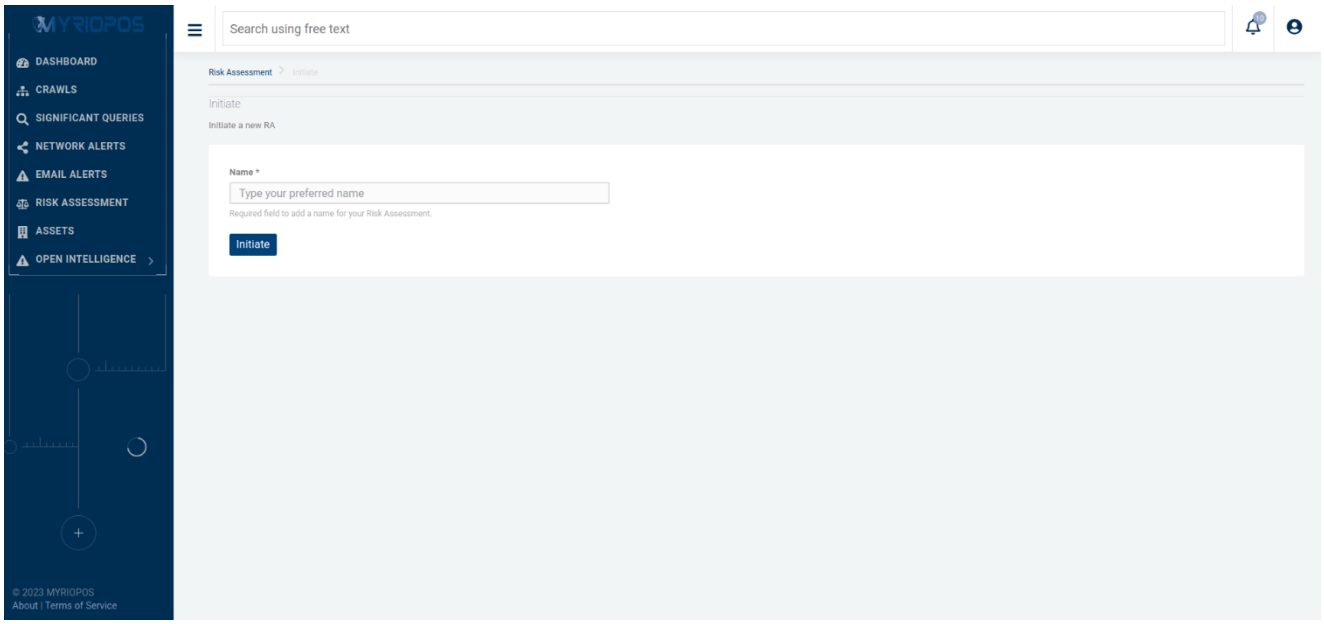
$$P_{\Sigma\text{ΕΝΑΡΙΟΥ}} = \frac{4.9 + 7}{2} = 5.95 \rightarrow Medium$$

Από το χάρτη θερμότητας (Πίνακας 2 και Πίνακας 3) βλέπουμε ότι ο κίνδυνος για αυτό το σενάριο επίθεσης είναι “High”, όπως βλέπουμε και στον ακόλουθο πίνακα.

ΚΙΝΔΥΝΟΣ						
IL	Very High					
	High			***High***		
	Medium					
	Low					
	Very Low					
		Very Low	Low	Medium	High	Very High
		Πιθανότητα σεναρίου επίθεσης				

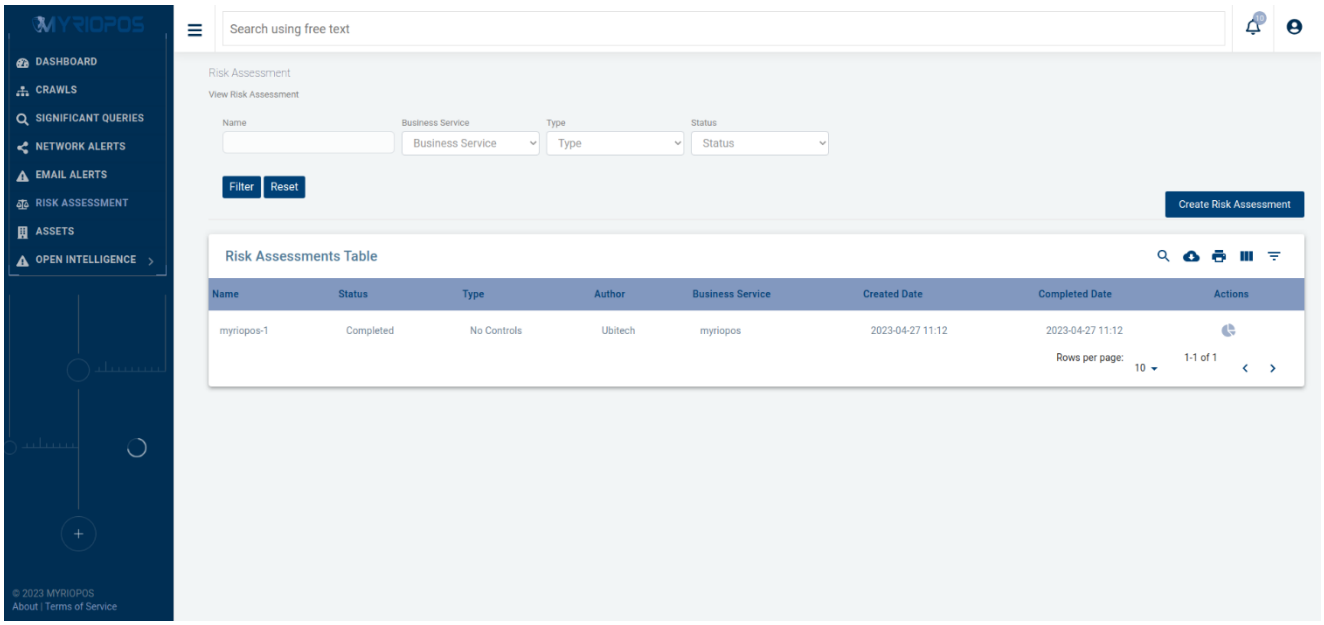
Πίνακας 3. Υπολογισμός κινδύνου για σενάριο με IL High και πιθανότητα Medium.

Στο σύστημα ΜΥΡΙΩΠΟΣ, η αξιολόγηση κινδύνου μπορεί δημιουργηθεί δηλώνοντας μόνο το επιθυμητό όνομα εκτέλεσης και αξιόλογης του κινδύνου, όπως φαίνεται στη παρακάτω εικόνα.



Εικόνα 9. Υπολογισμός Αξιολόγησης Κινδύνου του Συστήματος ΜΥΡΙΩΠΟΣ.

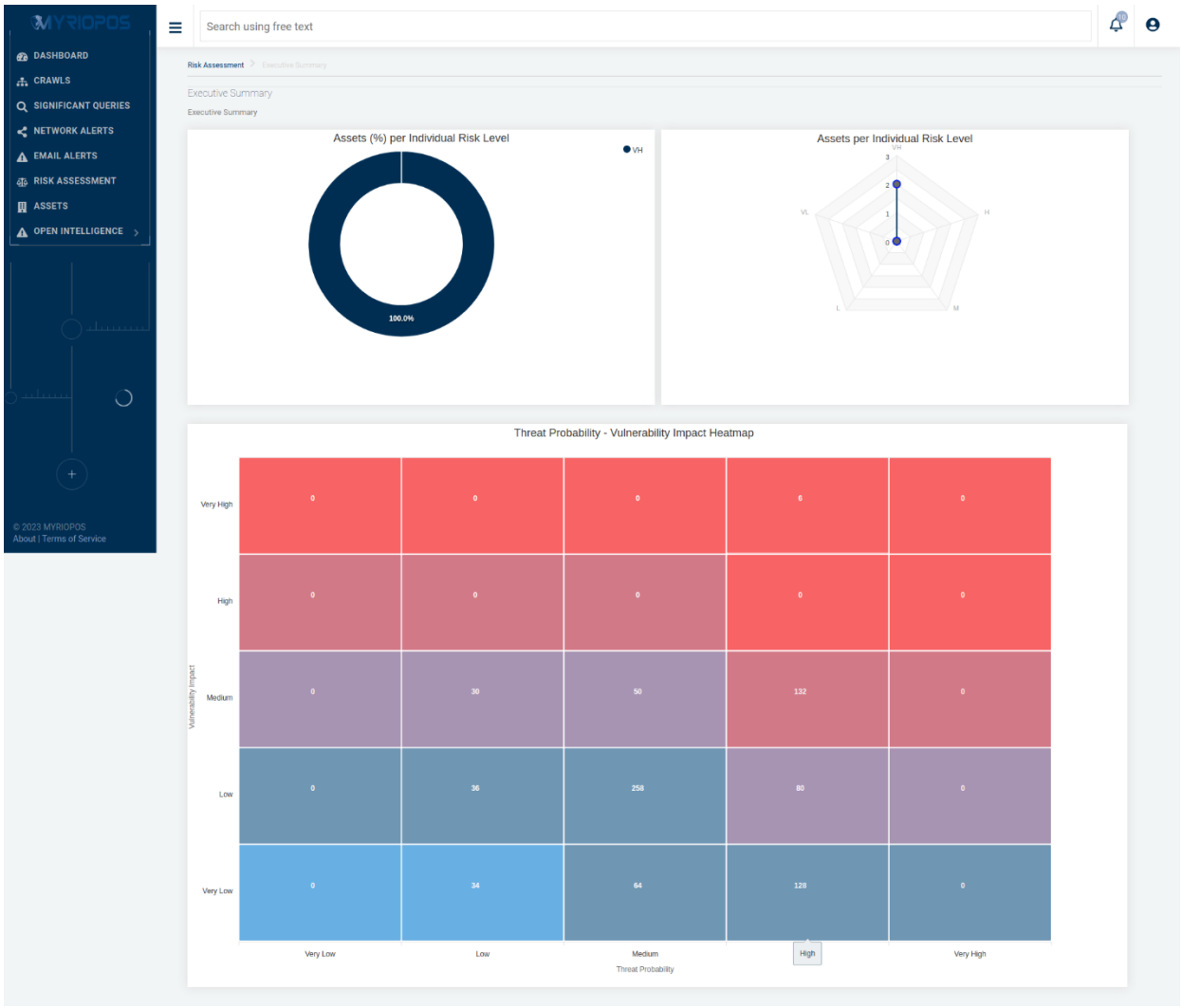
Οι διαφορετικές αξιολογήσεις κινδύνου που υπολογίζονται πίσω από τις υπηρεσίες του ΜΥΡΙΩΠΟΣ απεικονίζονται συγκεντρωτικά με τη μορφή πίνακα, όπως φαίνεται παρακάτω:



Εικόνα 10. Συγκεντρωτικά αξιολογήσεις κινδύνου του Συστήματος ΜΥΡΙΩΠΟΣ.

Επιπλέον, για κάθε ολοκληρωμένη αξιολόγηση κινδύνου υποστηρίζουμε 3 διαγράμματα από τα οποία προκύπτει ο συνολικός κίνδυνος για τον οργανισμό, με τη διαδικασία που περιγράψαμε παραπάνω. Συγκεκριμένα μια ολοκληρωμένη αξιολόγηση κινδύνου περιλαμβάνει ένα σύνολο από **σενάρια επίθεσης**

(**ψηφιακός πόρος-ευπάθεια-επίθεση**), όπου για καθένα έχουμε υπολογίσει τον κίνδυνο. Το αποτέλεσμα της αξιολόγησης φαίνεται στην Εικόνα 11.



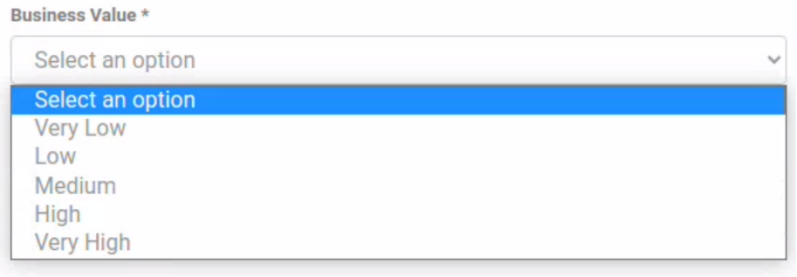
Εικόνα 11. Α**ποτέλεσμα αξιολόγησης κινδύνου του Συστήματος ΜΥΡΙΩΠΟΣ.**

Η πίτα (π.χ. Assets (%) per Individual Risk Level) απεικονίζει το ποσοστό των ψηφιακών πόρων ανά επίπεδο κρισιμότητας. Το διάγραμμα αράχνης (π.χ. πλήθος Assets per Individual Risk Level) απεικονίζει των αριθμό των ψηφιακών πόρων ανά επίπεδο κρισιμότητας.

Ο χάρτης θερμότητας ερμηνεύεται όμοια με τον Πίνακας 3 και απεικονίζει τον αριθμό των σεναρίων σε κάθε κελί που εντοπίστηκαν σε threat probability και vulnerability impact ως “Very Low” ως “Very High”. Ο χάρτης θερμότητας που παρουσιάζεται στην Εικόνα 11 περιγράφει το συνολικό κίνδυνο για όλα τα σενάρια επίθεσης, που βρέθηκαν για τον οργανισμό. Για παράδειγμα, το κελί με τη τιμή 258 δηλώνει ότι 258 σενάρια επίθεσης έχουν κίνδυνο “Low”, ή έχουν “Medium” πιθανότητα να συμβούν (Exp) και ταυτόχρονα η ευπάθεια έχει “Low” ως πιθανή επίπτωση (IL). Ένα αποτέλεσμα αξιολόγησης κίνδυνου, είναι λιγότερο ανησυχητικό και δεν επιβάλει πολίτικες άμυνας, όσο το μεγαλύτερο μέρος των σεναρίων επίθεσης δεν βρίσκονται στα κελιά με χρώμα κόκκινο που υποδηλώνουν το “Very High”.

5. Υπολογισμός Κρισιμότητας Ψηφιακών Πόρων

Στην προηγούμενη ενότητα παρουσιάσαμε την ποσοτικοποίηση του κινδύνου, αλλά δεν περιγράψαμε όλα τα διαγράμματα του αποτελέσματος της αξιολόγησης κινδύνου. Πριν προχωρήσουμε στην επεξήγηση των υπόλοιπων διαγραμμάτων, χρειάζεται να αναφέρουμε ότι στον υπολογισμό της αξιολόγησης κινδύνου, λαμβάνουμε υπόψη μας και την αξία στον οργανισμό ή την επιχείρηση (π.χ. business value) των ψηφιακών πόρων η οποία ορίζεται κατά την αρχικοποίηση του ψηφιακού πόρου και παίρνει τιμές που φαίνονται στη παρακάτω εικόνα:



Εικόνα 12. Διαφορετικές τιμές για την αξία ενός ψηφιακού πόρου στον οργανισμό.

Η αλλαγή που κάνουμε στον κίνδυνο, για να λάβουμε υπόψη την αξία του ψηφιακού πόρου είναι η ακόλουθη. Για σενάρια επίθεσης με κίνδυνο μεγαλύτερο ή ίσο του “Medium”, εάν η αξία του ψηφιακού πόρου (του σεναρίου) είναι μεγαλύτερη από αυτό, τότε αυξάνουμε κατά μια κλίμακα τον κίνδυνο. Αυτό πρακτικά σημαίνει ότι ο ψηφιακός πόρος εξυπηρετεί μια κρίσιμη εφαρμογή για τον οργανισμό και η αξία του μπορεί να οριστεί από τον τελικό χρήστη, όπως π.χ. εφαρμογή μισθολογίου εταιρίας, χώρος αποθήκευσης προσωπικών δεδομένων υπαλλήλων, κτλ. Στο παράδειγμα της προηγούμενης ενότητας, το αποτέλεσμα του κινδύνου ήταν “High”, οπότε εάν η αξία του ψηφιακού πόρου “PHP” ήταν “Very High”, τότε ο κίνδυνος θα έπαιρνε νέα τιμή, μια κλίμακα παραπάνω από το “High”, δηλαδή “Very High”. Επισημαίνουμε ότι, στη περίπτωση που ο κίνδυνος είναι “Very High”, δεν λαμβάνουμε υπόψη την αξία του ψηφιακού πόρου, διότι ακόμη και στη περίπτωση που η αξία είναι μεγαλύτερη, το σκορ δεν μπορεί να πάρει υψηλότερη τιμή.

Πλέον, για κάθε σενάριο επίθεσης έχουμε μια νέα τιμή κινδύνου. Για κάθε ψηφιακό πόρο επιλέγουμε από τα σενάρια επίθεσης που τον περιέχουν, εκείνο με το μεγαλύτερο κίνδυνο. Η τιμή του κινδύνου αυτού είναι και η κρισιμότητα του ψηφιακού πόρου.

Συνεπώς, τα δυο πρώτα διαγράμματα του αποτελέσματος της αξιολόγησης του κινδύνου (διάγραμμα πίτας και αράχνης), παρουσιάζουν τον αριθμό των ψηφιακών πόρων στο κάθε επίπεδο κρισιμότητας (από “Very Low” έως “Very High”).

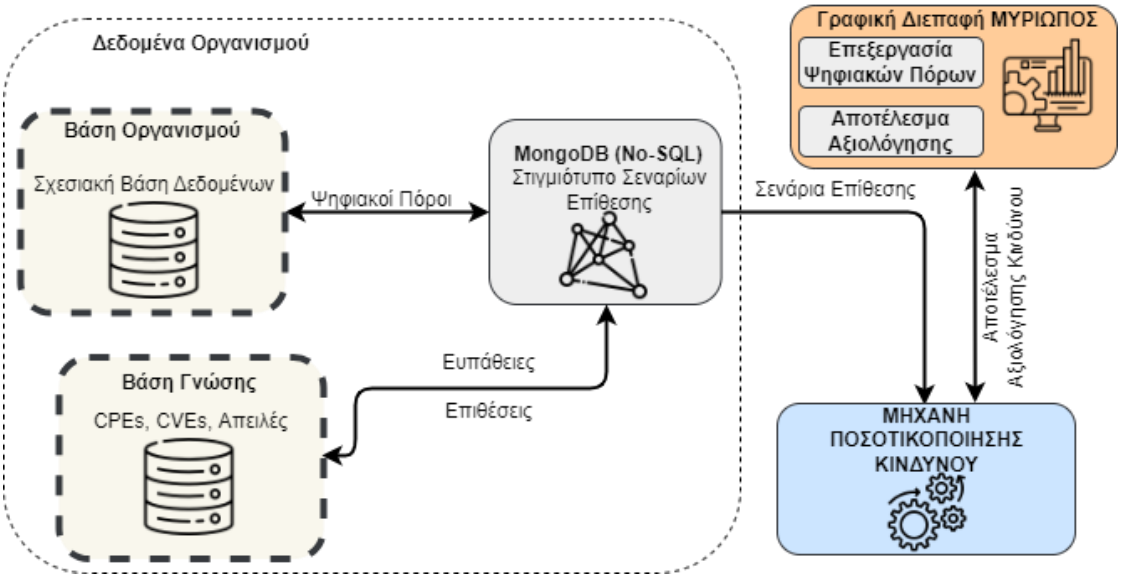
Ένα ακόμη διάγραμμα που είναι διαθέσιμο μέσω της πλατφόρμας ΜΥΡΙΩΠΟΣ, είναι επίσης ένας χάρτης θερμότητας, αλλά αυτή τη φορά τα σενάρια επίθεσης που σχετίζονται αφορούν μόνο ένα συγκεκριμένο ψηφιακό πόρο. Στα πλαίσια της αξιολόγησης του κινδύνου ο χάρτης θερμότητας, παρουσιάζεται ως το “αποτύπωμα” του ψηφιακού πόρου, όπως παρουσιάζεται στην Εικόνα 13.

Εικόνα 13. Αποτύπωμα ενός ψηφιακού πόρου.

Η Εικόνα 13 απεικονίζει για τον συγκεκριμένο ψηφιακό πόρο, πώς κατανέμονται τα σενάρια επίθεσης του σε κάθε επίπεδο κινδύνου του χάρτη θερμότητας.

6. Ροή Διεργασιών Αξιολόγησης Κινδύνου

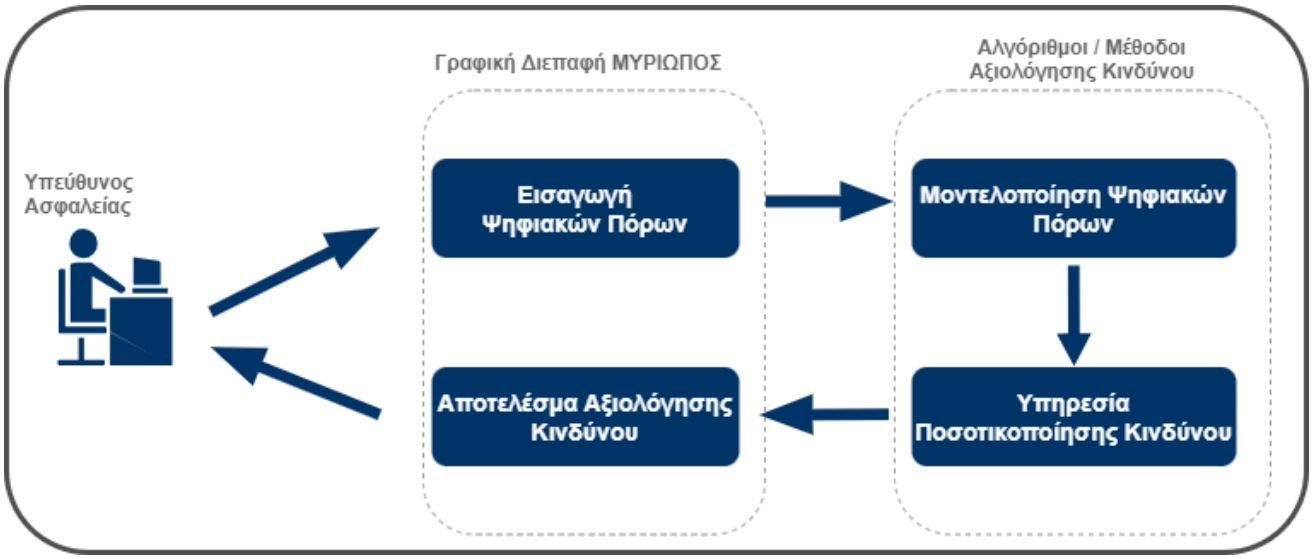
Το σημείο εκκίνησης για να εκτελεστεί μια αξιολόγηση κινδύνου, όπως έχουμε δείξει και στις προηγούμενες ενότητες είναι η γραφική διεπαφή του συστήματος ΜΥΡΙΩΠΟΣ, στο οποίο έχουμε συνδέσει όλες τις απαραίτητες υπηρεσίες λογισμικού για την υλοποίηση της αξιολόγησης. Η γραφική διεπαφή διευκολύνει το χρήστη να δημιουργήσει τους ψηφιακούς πόρους που περιγράφουν τον οργανισμό του. Οι υπηρεσίες αυτές, υλοποιημένες σε Quarkus επικοινωνούν με τη βάση γνώσης του οργανισμού (υποστηρίζεται σε MySQL) και δημιουργούν τις συνδέσεις μεταξύ ψηφιακού πόρου και CPE. Στη συνέχεια, με επερωτήσεις συνδέουμε τους ψηφιακούς πόρους με τις ευπάθειες που τους αντιστοιχούν και μέσω των CWE που έχουμε περιγράψει γίνεται η σύνδεση με τις πιθανές επιθέσεις. Έτσι μια αξιολόγηση κινδύνου μπορεί να δημιουργηθεί και να εκτελεστεί από τον τελικό χρήστη πατώντας το κουμπί “Execute”. Τη στιγμή της δημιουργίας της αξιολόγησης, ένα στιγμιότυπο της βάσης του οργανισμού (ψηφιακοί πόροι) και των αντίστοιχων ευπαθειών και επιθέσεων (σενάρια επίθεσης) δημιουργείται και αποθηκεύεται σε μια MongoDB. Στη συνέχεια το στιγμιότυπο αυτό είναι διαθέσιμο στη μηχανή ποσοτικοποίησης του κινδύνου προκειμένου να πραγματοποιήσει όλους του απαραίτητους υπολογισμούς που περιγράψαμε στις παραπάνω ενότητες και να παράξει την αναφορά αξιολόγησης του κινδύνου. Η σχετική αρχιτεκτονική και η ροή διεργασιών παρουσιάζεται στην Εικόνα 14.



Εικόνα 14. Αρχιτεκτονική Αξιολόγησης Κινδύνου του Συστήματος ΜΥΡΙΩΠΟΣ.

7. Αξιολόγηση Κινδύνου στο Σύστημα ΜΥΡΙΩΠΟΣ

Σε αυτή την ενότητα, παρουσιάζουμε τη ροή διαδικασίας στην εμπειρία του χρήση κατά τη χρήση του εργαλείου της αξιολόγησης του κινδύνου στο σύστημα ΜΥΡΙΩΠΟΣ. Ο τελικός χρήστης (πιθανόν, ο υπεύθυνος ασφαλείας του οργανισμού) μπορεί να αρχικοποιήσει και να εκτελέσει όλους τους υπολογισμούς και να συγκεντρώσει όλες τις αναφορές και τα αποτελέσματα που παρουσιάστηκαν στις προηγούμενες ενότητες. Αρχικά, οι ψηφιακοί πόροι εισάγονται στο σύστημα του ΜΥΡΙΩΠΟΣ μέσω της γραφικής διεπαφής. Στη συνέχεια, εκτελείται η μοντελοποίηση των απειλών των ψηφιακών πόρων και η ποσοτικοποίηση του κινδύνου. Τέλος, τα αποτελέσματα, μέσω γραφημάτων καταλήγουν στον τελικό χρήστη μέσω της γραφικής διεπαφής.



Εικόνα 15. Ενοποιημένο Σύστημα ΜΥΡΙΩΠΟΣ - Ροή διαδικασίας αξιολόγησης και ποσοτικοποίησης κινδύνου.

8. Εφαρμογή Πολιτικών Ανάκαμψης

Πλέον, εκτελώντας τις μεθόδους αξιολόγησης και ποσοτικοποίησης κινδύνων με το σύστημα ΜΥΡΙΩΠΟΣ έχουμε μια ολοκληρωμένη εικόνα για τους πιθανούς κινδύνους ενός οργανισμού. Γνωρίζουμε ποιοι ψηφιακοί πόροι είναι πιο ευάλωτοι και με ποιους τρόπους μπορεί ένας κακόβουλος χρήστης να επιτεθεί. Επομένως, μέσω του συστήματος ΜΥΡΙΩΠΟΣ, ο υπεύθυνος ασφαλείας ενός οργανισμού μπορεί να προβεί σε πολιτικές και αλλαγές που θα μειώσουν τον κίνδυνο ενός ψηφιακού πόρου και κατά επέκταση ενός οργανισμού στο σύνολό του. Η βασικότερη πολιτική ανάκαμψης που μπορεί να ακολουθηθεί για την αντιμετώπιση ευπαθειών ενός λογισμικού, είναι η ενημέρωση αυτού, σε τελευταίες εκδόσεις που έχουν επιδιορθωθεί τα σφάλματα / αστοχίες, που επέτρεπαν ορισμένες ευπάθειες. Άλλες πολιτικές που μπορεί να εφαρμόσει είναι ο τερματισμός μιας υπηρεσίας, η δρομολόγηση της κίνησης που δέχεται μια διεύθυνση και πόρτα η οποία λαμβάνει μηνύματα / κίνηση σε κάποια άλλη διεύθυνση και πόρτα, κτλ.

Όπως αναφέραμε νωρίτερα, το αποτύπωμα ενός ψηφιακού πόρου δείχνει τον αριθμό των πιθανών σεναρίων επίθεσης που μπορεί να γίνουν σε αυτόν. Τα σενάρια επίθεσης είναι μια τριπλέτα ψηφιακού πόρου, ευπάθειας και επίθεσης. Επομένως, για παράδειγμα η ενημέρωση ενός ψηφιακού πόρου μπορεί να οδηγήσει στη μείωση των γνωστών ευπαθειών και κατά επέκταση στον περιορισμό των διαφορετικών επιθέσεων.

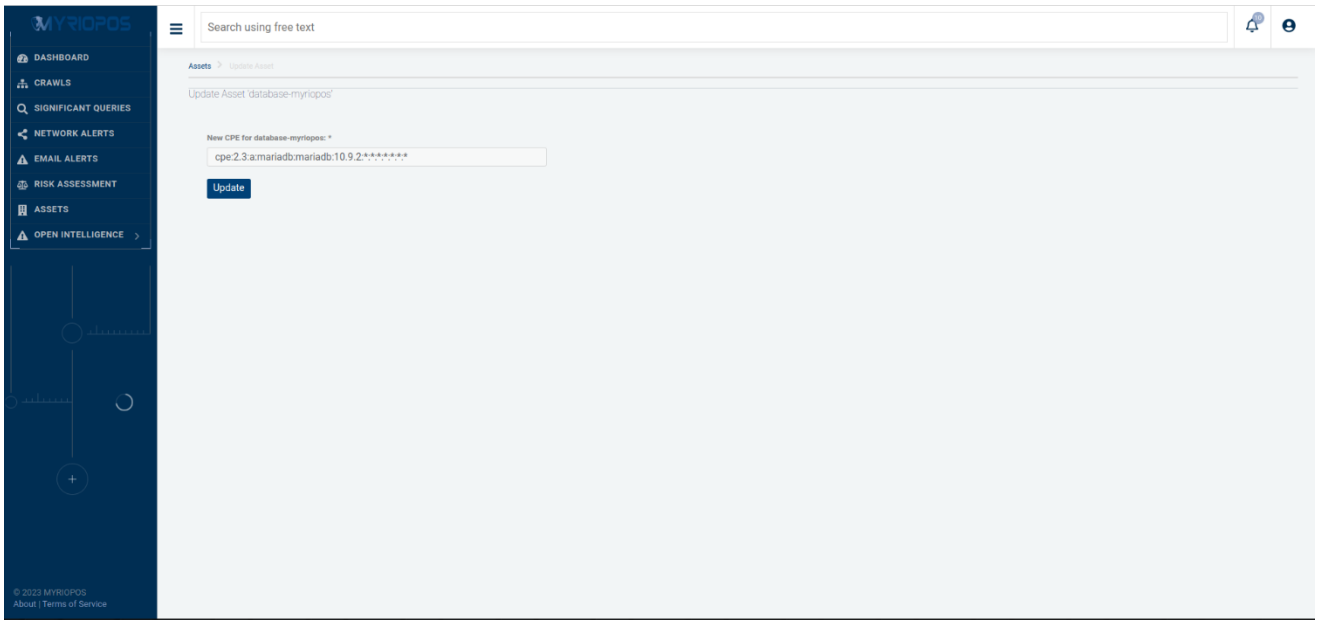
Στη παρακάτω εικόνα βλέπουμε το αποτύπωμα για τη βάση δεδομένων “mariaDB” με την έκδοση 10.2.17:

Εικόνα 16. Αποτύπωμα για τον ψηφιακό πόρο mariaDB έκδοσης 10.2.17.

Παρατηρούμε ότι έχει αρκετά σενάρια επίθεσης, άλλα με αυξημένη πιθανότητα και υψηλό επηρεασμό (44 σενάρια) και άλλα που έχουν μικρότερο αντίκτυπο στον οργανισμό.

Μια πολιτική ανάκαμψης, θα ήταν η ενημέρωση σε πιο πρόσφατη έκδοσης της “mariaDB”, ώστε να έχουν διορθωθεί οι αδυναμίες που επέτρεπαν τις ευπάθειες. Μέσω του συστήματος ΜΥΡΙΩΠΟΣ, όπως φαίνεται στη

παρακάτω εικόνα, αλλάζουμε το CPE ώστε να αντιστοιχεί στην ενημερωμένη έκδοση (έστω ότι επιλέγουμε την έκδοση 10.9.2).



Εικόνα 17. Αλλαγή CPE για έναν ψηφιακό πόρο.

Επόμενο βήμα είναι να συγχρονίσουμε τα προφίλ των ψηφιακών πόρων και τα σενάρια επίθεσης, ώστε να ληφθεί υπόψη η νέα έκδοση της βάση δεδομένων και να γίνουν οι υπολογισμοί με τις ευπάθειες που αντιστοιχούν (αν υπάρχουν) σε αυτή τη νέα. Μόλις πραγματοποιηθούν τα παραπάνω βήματα και ολοκληρωθεί ο υπολογισμός, το νέο αποτύπωμα της “mariaDB” είναι το εξής:

Εικόνα 18. Αποτύπωμα ψηφιακού πόρου mariaDB έκδοσης 10.9.2.

Παρατηρούμε μεγάλη μείωση στα πιθανά σενάρια, και πλέον δεν υπάρχουν σενάρια με υψηλό αντίκτυπο.

9. Επίλογος

Ένα από τα βασικά χαρακτηριστικά του συστήματος ΜΥΡΙΩΠΟΣ είναι η αξιολόγηση του κινδύνου ενός οργανισμού μέσω της μοντελοποίησης των απειλών. Το παραδοτέο Π3.1 περιγράφει τις διαδικασίες και τους μηχανισμούς που συμβάλλουν στην ανάπτυξη μετρικών κινδύνου για τον οργανισμό, καθώς και τις πολιτικές ανάκαμψης που μπορούν να υιοθετηθούν. Οι πολιτικές ανάκαμψης μπορεί να είναι ήπιες, π.χ. η αναβάθμιση του λογισμικού ή υλικού σε νεότερη έκδοση, ή πιο ντετερμινιστικές π.χ. ο τερματισμός μιας υπηρεσίας.

Αρχικά, γίνεται ανάλυση της μοντελοποίησης απειλών και ψηφιακών πόρων του οργανισμού μέσω του συστήματος ΜΥΡΙΩΠΟΣ. Χρησιμοποιώντας εξωτερικές πηγές δεδομένων για ευπάθειες και πλατφόρμες / συστήματα δημιουργούνται διαφορετικά σενάρια επίθεσης.

Το κάθε σενάριο συσχετίζεται με ένα επίπεδο κινδύνου μέσω υπολογισμών και αναφέρεται σε έναν ψηφιακό πόρο, ο οποίος κληρονομεί το επίπεδο κινδύνου. Με βάση επίσης την αξία που έχει ο εκάστοτε ψηφιακός πόρος για τον οργανισμό, παράγεται η κρισιμότητά του. Στη συνέχεια, το παραδοτέο παρουσίασε την τεχνική αρχιτεκτονική του υποσυστήματος μοντελοποίησης απειλών και αξιολόγησης κινδύνων καθώς και τη ροή διαδικασιών που ακολουθεί ο τελικός χρήστης αλληλοεπιδρώντας με αυτό.

Τέλος παρουσιάζεται ένα παράδειγμα εφαρμογής πολιτικής ανάκαμψης μέσω αναβάθμισης της έκδοσης υφιστάμενου λογισμικού. Παρουσιάστηκε το αποτέλεσμα που υπολογίστηκε εκ νέου, αναδεικνύοντας ότι η σωστή καταγραφή και διασύνδεση των ψηφιακών πόρων και οι προσεκτικές ενέργειες και αποφάσεις από έναν υπεύθυνο ασφαλείας επικουρικά με εκτενείς αναφορές και αύξηση της γνώσης σχετικά με τις υφιστάμενες υποδομές και υπηρεσίες μπορούν να οδηγήσουν αισθητά στη μείωση του κυβερνο-κινδύνου.

10. Αναφορές

[1] A Complete Guide to the Common Vulnerability Scoring System Version 2.0. Διαθέσιμο: https://www.first.org/cvss/v2/cvss-v2-guide.pdf

[2] Common Vulnerability Scoring System version 3.1 Specification Document, Revision 1. Διαθέσιμο: https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf