ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Εφαρμογή διαμοιρασμού δεδομένων κυβερνοασφάλειας σύμφωνα με πρότυπα σε ιδιωτικό blockchain

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Κίμων-Αντώνιος Προβατάς

Επιβλέπων : Βασίλειος Βεσκούκης
Καθηγητής Ε.Μ.Π.

Αθήνα, Φεβρουάριος 2023

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΤΕΧΝΟΛΟΓΙΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Εφαρμογή διαμοιρασμού δεδομένων κυβερνοασφάλειας σύμφωνα με πρότυπα σε ιδιωτικό blockchain

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Κίμων-Αντώνιος Προβατάς

Επιβλέπων : Βασίλειος Βεσκούκης
Αν. Καθηγητής Ε.Μ.Π

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 31η Οκτωβρίου

.....	.....	.....
Β.Βεσκούκης	Δ. Φωτάκης	Α.Παγουρτζής
Αν. Καθηγητής Ε.Μ.Π.	Καθηγητής Ε.Μ.Π.	Αν. Καθηγητής Ε.Μ.Π.

Αθήνα, Φεβρουάριος 2023

.....

Κίμων-Αντώνιος Προβατάς

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Περίληψη

Στο πεδίο της κυβερνοασφάλειας, οι επιτιθέμενοι και οι αμυνόμενοι προσπαθούν συνεχώς να υπερβούν ο ένας τον άλλον. Τα δεδομένα σχετικά με την επόμενη κίνηση ενός επιτιθέμενου είναι ζωτικής σημασίας για την προληπτική προσαρμογή των άμυνών και την πρόληψη μελλοντικών επιθέσεων. Η πληροφόρηση απειλών κυβερνοασφάλειας (Cybersecurity Threat Intelligence) αποτελεί το παράγωγο εφόσον τα κατάλληλα δεδομένα κυβερνοασφάλειας έχουν συλλεχθεί , αξιολογηθεί στο γενικό πλαίσιο της πηγής και της αξιοπιστίας τους και αναλυθεί με μεθοδικές και δομημένες τεχνικές από επαρκώς εξειδικευμένο προσωπικό. Η ανάπτυξη πληροφόρησης απειλών κυβερνοασφάλειας είναι μία κυκλική συνεχής διαδικασία που απαιτεί συνδυασμό αυτοματισμών για την εξαγωγή μόνο της σχετικής με τον οργανισμό πληροφόρησης από τις αντίστοιχες πηγές δεδομένων ενώ παράλληλα χρειάζεται την ανθρώπινη παρέμβαση ειδικών για τη βαθύτερη κατανόηση των συμπερασμάτων της πληροφόρησης και την ενσωμάτωση τους με τα υφιστάμενα συστήματα κυβερνοασφάλειας.

Η παρούσα διπλωματική εργασία στοχεύει στην ανάπτυξη μίας πλήρους εφαρμογής διαμοιρασμού Threat Intelligence μέσω του διεθνώς καθιερωμένου προτύπου STIX/TAXII στηριζόμενης στην τεχνολογία του ιδιωτικού δικτύου Blockchain Hyperledger Fabric ως υποδομή. Στόχος της παρούσας εργασίας επίσης είναι η ανάδειξη των πλεονεκτημάτων που παρουσιάζει ένα δίκτυο Blockchain στη βελτίωση της εμπιστευτικότητας (confidentiality) , της ακεραιότητας (integrity) , της διαθεσιμότητας (availability) , μη αποκήρυξης (non repudiation) και της ελεγξιμότητας (auditability) ιδιότητες σημαντικές στο πλαίσιο μίας εφαρμογής κυβερνοασφάλειας.

Λέξεις Κλειδιά

Πληροφόρηση απειλών κυβερνοασφάλειας, STIX, TAXII, Hyperledger Fabric, Blockchain, Έξυπνα Συμβόλαια, Ιδιωτικό Blockchain, Javascript, REST API

Abstract

In the field of cybersecurity, attackers and defenders are constantly trying to outdo each other. Data about an attacker's next move is critical to proactively adjusting defenses and preventing future attacks. Cybersecurity threat intelligence is the derivative since the appropriate cybersecurity data has been collected, evaluated in the general context of its source and reliability and analyzed with methodical and structured techniques by sufficiently specialized personnel. The development of cybersecurity threat intelligence is a cyclical continuous process that requires a combination of automation to extract only the information relevant to the organization from the respective data sources, while at the same time it needs the human intervention of experts to deeply understand the conclusions of the information and integrate them with the existing cyber security systems.

This thesis aims to develop a full stack Threat Intelligence sharing application through the internationally established STIX/TAXII standard based on the technology of the private Blockchain Hyperledger Fabric network as an infrastructure. The aim of this work is also to highlight the advantages presented by a Blockchain network in improving confidentiality, integrity, availability, non-repudiation and auditability, properties important in a cybersecurity application.

Λέξεις Κλειδιά

Cyber Threat Intelligence, STIX, TAXII, Hyperledger Fabric, Blockchain, Smart Contracts, Permissioned Blockchain, Javascript, REST API

Ευχαριστίες

Μετά την ολοκλήρωση της διπλωματικής μου εργασίας, ολοκληρώνεται το πενταετές ταξίδι μου στη Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Εθνικού Μετσόβιου Πολυτεχνείου (ΕΜΠ). Αυτό δε θα ήταν δυνατό χωρίς την οικογένεια και τους φίλους μου, που με στήριξαν καθ΄όλη τη διάρκεια των προπτυχιακών μου σπουδών. Θα ήθελα να εκφράσω τις ευχαριστίες μου στον καθηγητή και επιβλέποντα μου κ. Βασίλη Βεσκούκη, για την ευκαιρία που μου δόθηκε να εργαστώ και να αποκτήσω πρακτική εμπειρία πάνω σε αυτό το θέμα, αλλά και για την πολύτιμη καθοδήγηση, τα σχόλια και την άψογη συνεργασία του κατά τη διάρκεια της εκπόνησης της διπλωματικής μου. Επιπρόσθετα, θα ήθελα να ευχαριστήσω τη βοήθεια που παρείχε ο Υποψήφιος Διδάκτωρ και Ερευνητής Γιάννης Τζαννέτος, ο οποίος με βοήθησε καθ΄ όλη τη διάρκεια της εκπόνησης της διπλωματικής μου να κατανοήσω το θέμα σε βάθος. Τέλος, θα ήθελα να εκφράσω τις ιδιαίτερες ευχαριστίες μου σε όλους τους ανθρώπους που συμμετείχαν σε αυτό το ταξίδι στο Εθνικό Μετσόβιο Πολυτεχνείο

Αθήνα, Ιανουάριος 2023

Κίμων-Αντώνιος Προβατάς

Πίνακας Περιεχομένων

Κεφάλαιο 1 Εισαγωγή

1.1 Ο σκοπός της εργασίας

Την τελευταία δεκαετία παρατηρείται στην πληροφορική η τάση για την αποκέντρωση των εφαρμογών ενώ πολλοί ισχυρίζονται ότι οι αποκεντρωμένες εφαρμογές είναι το φυσικό επακόλουθο στην πορεία από τις στατικές , στις δυναμικές. Με αρχικό πεδίο εφαρμογής τα οικονομικά το blockchain έχει εξελιχθεί και έχει ξεφύγει πλέον από τον τον ορισμό του ως ένα ψηφιακό αποκεντρωμένο αρχείο καταγραφής οικονομικών συναλλαγών και έχει γίνει η κοινώς αποδεκτή δομή δεδομένων για το σχεδιασμό πολυμερών δικτύων, όπου η εμπίστοσύνη είναι κρίσιμης σημασίας και δε μπορεί να ανατεθεί σε έναν αποκλειστικά οργανισμό. Η κυβερνοασφάλεια στην πληροφορική, παραμένει ένα πεδίο όπου αν και έχει τεράστια περιθώρια για προγραμματισιμότητα και αυτοματισμούς προτιμάται η ανθρώπινη παρέμβαση στη διαδικασία του διαμοιρασμού των ευαίσθητων πληροφοριών στους εμπλεκόμενους και της διερεύνησης των περιστατικών ασφαλείας. Φυσική συνέπεια του παραπάνω γεγονότος είναι ο σκεπτικισμός από την πλευρά των ειδικών της κυβερνοασφάλειας απέναντι στον ενθουσιασμό που παρουσιάζει η παγκόσμια κοινότητα της πληροφορικής για το Blockchain και η βραδύτερη υιοθέτηση του στις υπάρχουσες υποδομές κυβερνοασφάλειας. Η παρούσα εργασία λοιπόν προσπαθεί να αναδείξει τα οφέλη που μπορεί να προσδώσει ένα σύστημα ανταλλαγής δεδομένων κυβερνοασφάλειας βασισμένο στην τεχνολογία του ιδιωτικού Blockchain, στους εμπλεκόμενους με το χώρο της κυβερνοασφάλειας. Το ιδιωτικό δίκτυο που χρησιμοποιήθηκε για την ανάπτυξη της εφαρμογής είναι το Hyperledger Fabric ενώ το πρότυπο πάνω στο οποίο στηρίζεται η κανονικοποίηση και ο διαμοιρασμός των πληροφοριών κυβερνοασφάλειας είναι το STIX/TAXII.

1.2 Η δομή της εργασίας

Στο κεφάλαιο 2 παρουσιάζεται ο ορισμός και οι βασικές έννοιες του Cyber Threat Intelligence το οποίο πιθανόν να είναι στους περισσότερους αναγνώστες άγνωστο, ως μία εξειδικευμένη υποκατηγορία της Κυβερνοσφάλειας μεγάλων οργανισμών. Στο κεφάλαιο επεξηγείται ο κύκλος του Cyber Threat Intelligence αλλά κυρίως, γίνονται οι απαιτούμενες αναφορές στο πρότυπο STIX / TAXII το οποίο θα αποτελέσει την βάση για να δομηθεί η εφαρμογή κυβερνοασφάλειας πάνω στο Blockchain.

Στο κεφάλαιο 3 θα γίνουν εκτεταμένες αναφορές στο ιδιωτικό δίκτυο Blockchain Hyperledger Fabric το οποίο θα αποτελέσει το επίπεδο διαχείρισης και πρόσβασης στα δεδομένα κυβερνοασφάλειας για την εφαρμογή. Θα εξεταστεί πρώτα από όλα η αρχιτεκτονική και οι δομικές μονάδες του Hyperledger. Στη συνέχεια θα γίνει αναφορά στις πτυχές του δικτύου που αφορούν τη συνεργασία και την εμπιστοσύνη σε πολυμερείς εφαρμογές (Multi Party Applications). Θα εξεταστεί το ζήτημα της αποδοχής και εγκατάστασης κοινού πηγαίου κώδικα σε ένα περιβάλλον αποτελούμενο από πολλαπλούς οργανισμούς και η έννοια του έξυπνου συμβολαίου (Chaincode and Smart Contracts). Τέλος θα γίνει αναφορά στο first network δίκτυο, τη βάση για την ανάπτυξη της εφαρμογής

Στο κεφάλαιο 4 θα παρουσιαστεί το προς επίλυση πρόβλημα και πως το Blockchain θα μπορούσε να διευκολύνει πτυχές του, που αφορούν κυρίως την ασφάλεια σε ένα πολυμερές περιβάλλον. Θα γίνει επίσης η παρουσίαση της αρχιτεκτονικής της εφαρμογής και θα οριστεί σαφώς η εμβέλεια της ώστε να υλοποιεί τη διεπαφή του προτύπου STIX/TAXII. Στη συνέχεια επανασχεδιάζεται ένας TAXII Server λαμβάνοντας υπόψιν ότι το επίπεδο διαχείρισης και πρόσβασης των δεδομένων γίνεται πλέον από ένα ιδιωτικό δίκτυο Blockchain και όχι από μία βάση δεδομένων.

Στο κεφάλαιο 5 γίνεται αναφορά στις τεχνολογίες που χρησιμοποιήθηκαν για την ανάπτυξη της εφαρμογής και επίδειξη των διεπαφών που την απαρτίζουν.

Στο κεφάλαιο 6 γίνονται αναφορές σε πιο θεωρητικά ζητήματα που αφορούν διάφορες δυσκολίες που παρουσιάστηκαν στο σχεδιασμό και την ανάπτυξη της

εφαρμογής. Δίνεται στη συνέχεια μία τεκμηριωμένη λίστα με τις αδυναμίες της εφαρμογής σε ζητήματα ασφαλείας και πιθανούς τρόπους με τους οποίους αυτά μπορούν να επιλυθούν. Τέλος γίνεται αναφορά σε ορισμένα χαρακτηριστικά που μπορούν να βελτιώσουν την εμπειρία και τις δυνατότητες της εφαρμογής από πλευράς χρήστη λαμβάνοντας υπόψιν ότι απευθύνεται σε ένα κοινό από αναλυτές και μηχανικούς ασφαλείας.

Κεφάλαιο 2 Εισαγωγή στις έννοιες του Cyber Threat Intelligence

Αυτό το κεφάλαιο επεξηγεί τον ορισμό του Cyber Threat intelligence και του προτύπου STIX/TAXII. Ο σκοπός αυτού του κεφαλαίου είναι η εξοικείωση του αναγνώστη με τις βασικές θεωρητικές έννοιες του CTI και πως το STIX / TAXII ήρθε να προτυποποιήσει και να εκσυγχρονίσει το παραπάνω πεδίο.

2.1 Τι είναι το Cyber Threat Intelligence

Το Threat Intelligence, γνωστό και ως Cyber Threat Intelligence (CTI), είναι πληροφορίες που συλλέγονται από μια σειρά πηγών σχετικά με τρέχουσες ή πιθανές επιθέσεις εναντίον ενός οργανισμού. Οι πληροφορίες αναλύονται, τελειοποιούνται ,οργανώνονται και στη συνέχεια χρησιμοποιούνται για την ελαχιστοποίηση και τον μετριασμό των κινδύνων για την ασφάλεια στον κυβερνοχώρο. Ο κύριος σκοπός του CTI είναι να δείξει στους οργανισμούς τους διάφορους κινδύνους που αντιμετωπίζουν από εξωτερικές απειλές, όπως οι απειλές μηδενικής ημέρας (Zero Day Threats) και οι προηγμένες επίμονες απειλές (Advanced Persistent Threats ή APT). Το CTI περιλαμβάνει εις βάθος πληροφορίες σχετικά με συγκεκριμένες απειλές, όπως ποιος επιτίθεται, τις ικανότητές και τα κίνητρά του και τους Indicators Of Compromise ή IOCs. [1]

2.2 Γιατί είναι χρήσιμο το Cyber Threat Intelligence

Σε ένα πλαίσιο στρατιωτικό ή εταιρικής κυβερνοασφάλειας, η πληροφόρηση, (Intelligence) είναι πληροφορίες που παρέχουν σε έναν οργανισμό υποστήριξη αποφάσεων και πιθανώς ένα στρατηγικό πλεονέκτημα. Οι πληροφορίες σχετικά με τις απειλές αποτελούν μέρος μιας μεγαλύτερης στρατηγικής πληροφοριών

ασφαλείας. Περιλαμβάνει πληροφορίες που σχετίζονται με την προστασία ενός οργανισμού από εξωτερικές και εσωτερικές απειλές, καθώς και τις διαδικασίες, τις πολιτικές και τα εργαλεία που χρησιμοποιούνται για τη συλλογή και ανάλυση αυτών των πληροφοριών. Το CTI παρέχει καλύτερη εικόνα για το τοπίο των γενικών και προηγμένων απειλών , μαζί με τις πιο πρόσφατες τακτικές, τεχνικές και διαδικασίες τους (Techniques, Tactics and Procedures). Το CTI επιτρέπει στους οργανισμούς να είναι προληπτικοί στη διαμόρφωση των προσαρμογών ασφαλείας τους για τον εντοπισμό και την πρόληψη προηγμένων επιθέσεων και απειλών μηδενικής ημέρας. Πολλές από αυτές τις προσαρμογές μπορούν να αυτοματοποιηθούν, ώστε η ασφάλεια να παραμένει ευθυγραμμισμένη με τις πιο πρόσφατες πληροφορίες σε πραγματικό χρόνο. [1]

2.3 Οι διαφορετικοί τύποι του Cyber Threat Intelligence

Υπάρχουν τέσσερις τύποι πληροφόρησης Cyber Threat : Στρατηγική , Τακτική , Τεχνική και Λειτουργική. Κάθε μία από τις τέσσερις είναι απαραίτητη για τη δημιουργία μίας ολοκληρωμένης αξιολόγησης των απειλών. [1]

1. **Στρατηγική Πληροφόρηση:** Αυτή η ανάλυση συνοψίζει πιθανές επιθέσεις στον κυβερνοχώρο και τις πιθανές συνέπειες για το μη τεχνικό κοινό και τα ενδιαφερόμενα μέρη, καθώς και τους υπεύθυνους λήψης αποφάσεων. Παρουσιάζεται σε μορφή εγγράφων και αναφορών ενώ συνοψίζει την υψηλού επιπέδου εικόνα
2. **Τακτική Πληροφόρηση:** Η θεώρηση αυτή παρέχει πληροφορίες σχετικά με τις τακτικές, τις τεχνικές και τις διαδικασίες (TTP) που χρησιμοποιούν οι φορείς απειλών. Προορίζεται για όσους ασχολούνται άμεσα με την προστασία των πόρων πληροφορικής και δεδομένων. Παρέχει λεπτομέρειες σχετικά με τον τρόπο με τον οποίο ένας οργανισμός μπορεί να δεχθεί επίθεση με βάση τις πιο πρόσφατες μεθόδους που χρησιμοποιούνται και τους καλύτερους τρόπους άμυνας έναντι ή μετριασμού των επιθέσεων.

3. **Τεχνική Πληροφόρηση:** Αυτές οι πληροφορίες επικεντρώνονται σε σημάδια που υποδεικνύουν ότι μια επίθεση ξεκινά. Αυτά τα σημάδια περιλαμβάνουν αναγνώριση (reconnaissance), οπλισμό (weaponization) και παράδοση (delivery), όπως spear phishing, baits και κοινωνική μηχανική. Η τεχνική πληροφόρηση παίζει σημαντικό ρόλο στην παρεμπόδιση των επιθέσεων κοινωνικής μηχανικής. Αυτός ο τύπος πληροφοριών συχνά ομαδοποιείται με το λειτουργικό Threat Intelligence. Ωστόσο, προσαρμόζεται γρήγορα καθώς οι επιτιθέμενοι ενημερώνουν τις τακτικές τους για να επωφεληθούν από νέα γεγονότα και τεχνάσματα.

4. **Λειτουργική Πληροφόρηση:** Με αυτήν την προσέγγιση, οι πληροφορίες συλλέγονται από διάφορες πηγές, συμπεριλαμβανομένων των chat rooms των μέσων κοινωνικής δικτύωσης, των αρχείων καταγραφής antivirus και των προηγούμενων περιστατικών που έχουν συμβεί. Το λειτουργικό CTI χρησιμοποιείται για την πρόβλεψη της φύσης και του χρόνου μελλοντικών επιθέσεων. Η εξόρυξη δεδομένων και η μηχανική εκμάθηση χρησιμοποιούνται συχνά για την αυτοματοποίηση της επεξεργασίας εκατοντάδων χιλιάδων data points. Οι ομάδες απόκρισης περιστατικών ασφάλειας χρησιμοποιούν το operational threat intelligence για να αλλάξουν τη διαμόρφωση των security controls, όπως κανόνες τείχους προστασίας (firewall), κανόνες ανίχνευσης συμβάντων (event detection rules) και στοιχεία ελέγχου πρόσβασης (access controls).

2.4 Ο κύκλος ζωής του Cyber Threat Intelligence

Υπάρχουν διάφορα βήματα που εμπλέκονται στη διαδικασία συλλογής πληροφοριών απειλών και αυτά είναι με τη σειρά . [1]

Καθορισμός Στόχων: Για να επιλέξει τις σωστές πηγές και εργαλεία CTI, ένας οργανισμός πρέπει να αποφασίσει τι ελπίζει να επιτύχει προσθέτοντας threat intelligence στις λύσεις και τη στρατηγική ασφαλείας του. Ο στόχος πιθανότατα είναι

να βοηθηθούν οι ομάδες ασφάλειας πληροφοριών να σταματήσουν πιθανές απειλές που εντοπίζονται κατά τη διάρκεια μιας άσκησης μοντελοποίησης απειλών (Threat Modeling). Αυτό απαιτεί την απόκτηση δεδομένων, πληροφοριών και εργαλείων που μπορούν να παρέχουν ενημερωμένες συμβουλές και ειδοποιήσεις σχετικά με τις απειλές που θεωρούνται υψηλού κινδύνου και υψηλού αντικτύπου.

1. **Συλλογή Δεδομένων:** Τα αρχεία καταγραφής από εσωτερικά συστήματα, ελέγχους ασφαλείας και υπηρεσίες cloud αποτελούν τη βάση του προγράμματος CTI ενός οργανισμού. Ωστόσο η απόκτηση πληροφοριών σχετικά με τις τελευταίες TTPs και την πληροφόρηση περί συγκεκριμένης βιομηχανίας (industry-specific intelligence) , καθιστά απαραίτητη τη συλλογή δεδομένων από εξωτερικές ροές απειλών τρίτων. Αυτές οι πηγές περιλαμβάνουν πληροφορίες που συλλέγονται από ιστότοπους κοινωνικής δικτύωσης, φόρουμ χάκερ, κακόβουλες διευθύνσεις IP και αναφορές ερευνών.

2. **Επεξεργασία Δεδομένων :** Η συλλογή και η οργάνωση των αδόμητων δεδομένων που απαιτούνται για τη δημιουργία αξιόπιστων πληροφοριών απειλών απαιτεί αυτοματοποιημένη επεξεργασία. Δεν είναι βιώσιμο να φιλτράρονται, να προστίθενται μεταδεδομένα και να συσχετίζονται με μη αυτόματο τρόπο. Οι πλατφόρμες ή οι εφαρμογές Threat Intel χρησιμοποιούν μηχανική μάθηση για την αυτοματοποίηση της συλλογής και επεξεργασίας δεδομένων, ώστε να μπορεί να παρέχει συνεχώς πληροφορίες σχετικά με τις δραστηριότητες των Threat Actors.

3. **Ανάλυση Δεδομένων:** Αυτό το βήμα περιλαμβάνει την εύρεση απαντήσεων από τα επεξεργασμένα δεδομένα σε ερωτήσεις όπως πότε, γιατί και πώς συνέβη ένα ύποπτο συμβάν. Αυτό το βήμα θα απαντούσε σε ερωτήσεις σχετικά με το πότε συνέβη ένα περιστατικό email phishing, τι επιζητά ο επιτιθέμενος και πώς συνδέονται τα phishing μηνύματα με ένα κακόβουλο domain.

4. **Αναφορά Ευρημάτων:** Οι αναφορές πρέπει να είναι προσαρμοσμένες σε ένα συγκεκριμένο κοινό, ώστε να είναι σαφές πώς οι απειλές που καλύπτονται επηρεάζουν τους τομείς ευθύνης τους. Οι αναφορές θα πρέπει να κοινοποιούνται στην ευρύτερη κοινότητα όταν είναι δυνατόν για τη βελτίωση των συνολικών λειτουργιών ασφάλειας.

Σχήμα 2.4.1

Συνοψίζοντας αυτό που προκύπτει από το συγκεκριμένο κεφάλαιο είναι ότι οι μεγάλοι οργανισμοί που λαμβάνουν σοβαρά υπόψιν τους την κυβερνοασφάλεια, έχουν ανάγκη από μία στρατηγική Cyber Threat Intelligence για την αποτροπή των επερχόμενων απειλών. Επιπλέον, στο τεχνικό κομμάτι είναι σαφές ότι η παραγωγή CTI είναι μία συνεχής διαδικασία και μοιάζει αρκετά με την κλασσική ανάλυση δεδομένων (Data Analysis) εφαρμοσμένη πάνω σε δεδομένα ασφάλειας και βοηθάει να ληφθούν αποφάσεις από τις πιό υψηλού επιπέδου, στρατηγικές μέχρι τις πιό χαμηλού επιπέδου, λειτουργικές.

2.5 Το πρότυπο STIX

2.5.1 Εισαγωγή στο Πρότυπο STIX και τα Αντικείμενα

Structured Threat information Expression η STIX είναι η γλώσσα και το πρότυπο σειριοποίησης για την ανταλλαγή δεδομένων Cyber Threat Intelligence. Το πρότυπο

STIX είναι ανοιχτού κώδικα και δωρεάν επιτρέποντας στους ενδιαφερόμενους με την κυβερνοασφάλεια να ρωτούν ερωτήσεις και να συνεισφέρουν ελεύθερα. [2]

Η συμβολή και η κατανάλωση δεδομένων CTI διευκολύνεται σημαντικά με την ακολούθηση του προτύπου STIX. Με το STIX, όλες οι πτυχές υποψίας (suspicion), της προσβολής (compromise) και της απόδοσης ευθυνών (attribution) μπορούν να αναπαρασταθούν καθαρά με αντικείμενα και περιγραφικές σχέσεις. Οι πληροφορίες STIX μπορούν να αναπαρασταθούν οπτικά για έναν αναλυτή κυβερνοασφάλειας ή να αποθηκευτούν ως JSON για να είναι γρήγορα αναγνώσιμες από μηχανή. Η επεκτασιμότητα και η διττή φύση του STIX επιτρέπει την ενσωμάτωση σε υπάρχοντα εργαλεία και προϊόντα που χρησιμοποιούνται για τις συγκεκριμένες ανάγκες του αναλυτή ή του δικτύου σας. Τα διαφορετικά αντικείμενα τύπου STIX για το νεότερο πρότυπο 2.1 είναι τα εξής και μοντελοποιούνται με JSON format [2] :

Αντικείμενο	**Όνομα**	**Περιγραφή**
	Μοτίβο Επίθεσης (Attack Pattern)	Είδος Τεχνική , Τακτικής ή Διαδικασίας (TTP) που περιγράφει τους τρόπους που οι επιτιθέμενοι προσπαθούν να προσβάλλουν τους στόχους τους
	Καμπάνια (Campaign)	Ομαδοποίηση εχθρικών συμπεριφορών που περιγράφει ένα σύνολο κακόβουλων δραστηριοτήτων ή επιθέσεων (μερικές φορές ονομάζονται κύματα) που συμβαίνουν σε μια χρονική περίοδο εναντίον συγκεκριμένου συνόλου στόχων.
	Σειρά αμυντικών δράσεων (Course of Action)	Σύσταση από έναν παραγωγό CTI σε έναν καταναλωτή σχετικά με τις ενέργειες που θα μπορούσαν να κάνουν ως απάντηση σε κάποια πληροφόρηση
	Ομαδοποίηση (Grouping)	Ισχυρίζεται ρητά ότι τα αναφερόμενα αντικείμενα STIX έχουν κοινό πλαίσιο, σε αντίθεση με ένα πακέτο STIX (bundle) (το οποίο ρητά δεν μεταφέρει κανένα πλαίσιο).
	Ταυτότητα (Identity)	Πραγματικά άτομα, οργανισμοί ή ομάδες καθώς και κατηγορίες ατόμων, οργανισμών, συστημάτων ή ομάδων (π.χ. ο χρηματοοικονομικός τομέας).
	Ένδειξη (Indicator)	Περιέχει ένα μοτίβο που μπορεί να χρησιμοποιηθεί για τον εντοπισμό ύποπτης ή κακόβουλης δραστηριότητας στον κυβερνοχώρο.
	Υποδομή (Infrastructure)	Αντιπροσωπεύει έναν τύπο TTP και περιγράφει οποιαδήποτε συστήματα, υπηρεσίες λογισμικού και οποιουσδήποτε σχετικούς φυσικούς ή εικονικούς πόρους που προορίζονται να υποστηρίξουν κάποιο σκοπό

	Σετ Εισβολής (Intrusion Set)	Ένα ομαδοποιημένο σύνολο κακόβουλων συμπεριφορών και πόρων με κοινές ιδιότητες που πιστεύεται ότι ενορχηστρώνονται από έναν μόνο οργανισμό.
	Τοποθεσία (Location)	Αναπαριστά μία γεωγραφική τοποθεσία
	Κακόβουλο Λογισμικό (Malware)	Ένας τύπος TTP ο οποίος αναπαριστά κακόβουλο κώδικα
	Ανάλυση Κακόβουλου Λογισμικού (Malware Analysis)	Τα μεταδεδομένα και τα αποτελέσματα μιας συγκεκριμένης στατικής ή δυναμικής ανάλυσης που εκτελούνται σε μια μονάδα ή οικογένεια κακόβουλου λογισμικού.
	Σημείωση (Note)	Μεταφέρει ενημερωτικό κείμενο για την παροχή περαιτέρω πλαισίου ή/και για την παροχή πρόσθετης ανάλυσης που δεν περιέχεται στα αντικείμενα STIX, τα αντικείμενα ορισμού σήμανσης ή τα αντικείμενα Περιεχομένου γλώσσας
	Παρατηρούμενα Δεδομένα (Observed Data)	Μεταφέρει πληροφορίες σχετικά με οντότητες που σχετίζονται με την ασφάλεια στον κυβερνοχώρο, όπως αρχεία, συστήματα και δίκτυα χρησιμοποιώντας τα STIX Cyber-Observable Objects (SCOs).
	Γνώμη (Opinion)	Αξιολόγηση της ορθότητας των πληροφοριών σε ένα αντικείμενο STIX που παράγεται από διαφορετική οντότητα.
	Αναφορά (Report)	Συλλογές CTI που επικεντρώθηκαν σε ένα ή περισσότερα θέματα, όπως μια περιγραφή ενός παράγοντα απειλής, κακόβουλου λογισμικού ή τεχνικής επίθεσης, συμπεριλαμβανομένου του πλαισίου και των σχετικών λεπτομερειών.
	Κακόβουλος Παράγων (Threat Actor)	Πραγματικά άτομα, ομάδες ή οργανισμοί που πιστεύεται ότι λειτουργούν με κακόβουλη πρόθεση.
	Εργαλείο (Tool)	Νόμιμο λογισμικό που μπορεί να χρησιμοποιηθεί από παράγοντες απειλών για την εκτέλεση επιθέσεων.
	Ευπάθεια (Vulnerability)	Ένα λάθος σε λογισμικό που μπορεί να χρησιμοποιηθεί απευθείας από έναν κακόβουλο παράγοντα για να αποκτήσει πρόσβαση σε ένα σύστημα ή ένα δίκτυο.

	Γενικού τύπου σχέση (Relationship)	Χρησιμοποιείται για τη σύνδεση δύο SDO ή SCO για να περιγράψει πώς σχετίζονται μεταξύ τους.
	Σχέση παρατήρησης (Sighting)	Υποδηλώνει την πεποίθηση ότι εμφανίστηκε κάτι, στο CTI (π.χ. δείκτης, κακόβουλο λογισμικό, εργαλείο, παράγοντας απειλής κ.λπ.).

Τα αντικείμενα STIX κατηγοριοποιούν κάθε πληροφορία με συγκεκριμένα χαρακτηριστικά που πρέπει να συμπληρωθούν. Η σύνδεση πολλαπλών αντικειμένων μεταξύ τους μέσω σχέσεων επιτρέπει εύκολες ή πολύπλοκες αναπαραστάσεις του CTI. [2]

2.5.2 Κατηγοριοποίηση και σημαντικές Ιδιότητες της Γλώσσας STIX

Το STIX είναι ένα σχήμα το οποίο ορίζει μία ταξινομία από CTI η οποία αναπαρίσταται από τα παρακάτω αντικείμενα:

STIX Core Objects

1. STIX Domain Objects (SDO) Αντικείμενα CTI υψηλότερου επιπέδου που αντιπροσωπεύουν συμπεριφορές και κατασκευές που οι αναλυτές intelligence συνήθως θα δημιουργούσαν για να κατανοήσουντο threat landscape.

2. STIX Cyber Observable Objects (SCO) Αντικείμενα που αντιπροσωπεύουν παρατηρούμενα γεγονότα σχετικά με ένα δίκτυο ή έναν κεντρικό υπολογιστή που μπορούν να χρησιμοποιηθούν και σχετίζονται με intelligence υψηλότερου επιπέδου για να σχηματίσουν μια πληρέστερη κατανόηση του τοπίου της απειλής

3. STIX Relationship Objects (SRO) Αντικείμενα που συνδέουν STIX SDO και STIX SCO μαζί για να σχηματίσουν μια πληρέστερη κατανόηση του τοπίου της απειλής.

STIX Meta Objects

Ένα αντικείμενο STIX που παρέχει την απαραίτητη επέκταση και τα σχετικά μεταδεδομένα για τον εμπλουτισμό των βασικών αντικειμένων STIX για την υποστήριξη ροών εργασίας χρήστη και συστήματος. Τα 3 Meta Objects είναι τα Extension Definition Objects , Language Content Objects και Marking Definition Objects

Τέλος υπάρχουν και τα **STIX Bundle Objects** τα οποία είναι ένας wrapper μηχανισμός για την αυθαίρετη ομαδοποίηση οποιουδήποτε συνδυασμού των προαναφερθέντων αντκειμένων. [3]

Το STIX είναι ένα πρότυπο το οποίο μοντελοποιεί τα δεδομένα της κυβερνοασφάλειας με τέτοιο τρόπο ώστε στο μέλλον να υπάρχει μία κοινή γλώσσα αναφοράς. Η τεκμηρίωση του οργανισμού OASIS είναι εκτενής για κάθε γλωσσικό χαρακτηριστικό του STIX οπότε έχει νόημα να γίνει αναφορά μόνο στα κομμάτια που αφορούν τη συγκεκριμένη εργασία. Πολύ σημαντικό κομμάτι στο πλαίσιο αυτής της εργασίας είναι τα **STIX Common Properties,** τα οποία έχουν τη μεγαλύερη πιθανότητα να εμφανίζονται σε κάποια υλοποίηση της γλώσσας. Αυτά είναι τα:

STIX Core Objects			STIX Meta Objects				
Property Name	**SDOs**	**SROs**	**SCOs**	**Extension**	**Language**	**Markings**	**Bundle**
`type`	Required	Required	Required	Required	Required	Required	Required
`spec_version`	Required	Required	Optional	Required	Required	Required	N/A
`id`	Required	Required	Required	Required	Required	Required	Required
`created_by_ref`	Optional	Optional	N/A	Required	Optional	Optional	N/A
`created`	Required	Required	N/A	Required	Required	Required	N/A
`modified`	Required	Required	N/A	Required	Required	N/A	N/A
`revoked`	Optional	Optional	N/A	Optional	Optional	N/A	N/A
`labels`	Optional	Optional	N/A	Optional	Optional	N/A	N/A
`confidence`	Optional	Optional	N/A	N/A	Optional	N/A	N/A
`lang`	Optional	Optional	N/A	N/A	N/A	N/A	N/A
`external_references`	Optional	Optional	N/A	Optional	Optional	Optional	N/A
`object_marking_refs`	Optional	Optional	Optional	Optional	Optional	Optional	N/A
`granular_markings`	Optional	Optional	Optional	Optional	Optional	Optional	N/A
`defanged`	N/A	N/A	Optional	N/A	N/A	N/A	N/A
`extensions`	Optional	Optional	Optional	N/A	Optional	Optional	N/A

2.6 Το πρότυπο TAXII

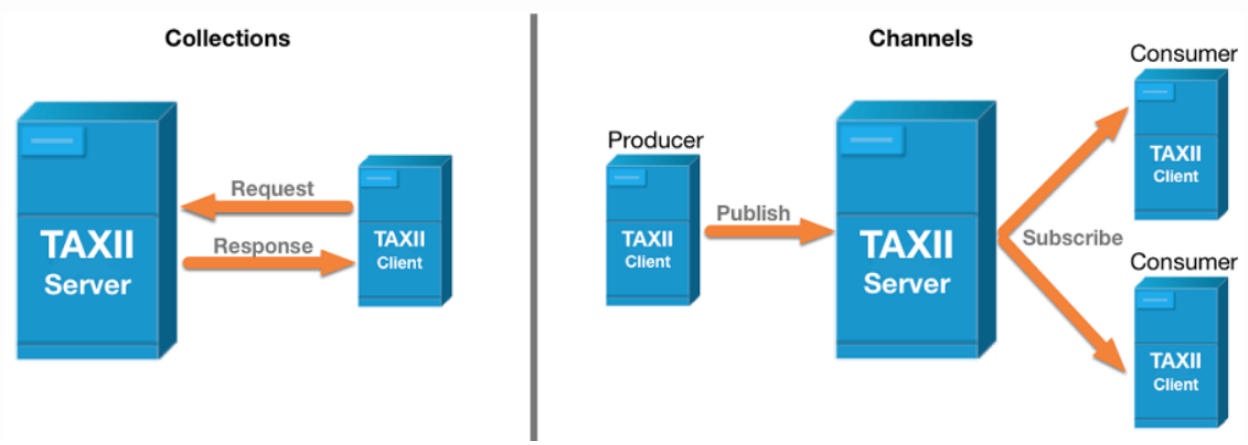
Το Trusted Automated Exchange of Intelligence Information (TAXII™) είναι ένα πρωτόκολλο εφαρμογής για την ανταλλαγή CTI μέσω HTTPS. Το TAXII ορίζει ένα RESTful API (ένα σύνολο υπηρεσιών και ανταλλαγών μηνυμάτων) και ένα σύνολο απαιτήσεων για Πελάτες και Διακομιστές TAXII.

Όπως απεικονίζεται παρακάτω, το TAXII ορίζει δύο κύριες υπηρεσίες για την υποστήριξη μιας ποικιλίας κοινών μοντέλων:

Collection (Συλλογή) Μια συλλογή είναι μια διεπαφή σε μια λογική αποθήκη αντικειμένων CTI που παρέχεται από έναν Server TAXII που επιτρέπει σε έναν producer CTI να φιλοξενεί ένα σύνολο δεδομένων που μπορούν να ζητηθούν από τους consumers CTI: Clients TAXII και Server ανταλλάσσουν πληροφορίες σε ένα μοντέλο request response.

Channel (Κανάλι) Διατηρούμενο από έναν Server TAXII, ένα κανάλι επιτρέπει στους producers να προωθήσουν δεδομένα σε πολλούς consumers και στους consumers να λαμβάνουν δεδομένα από πολλαπλούς producers αντίστιχα: Οι clients TAXII ανταλλάσσουν πληροφορίες με άλλους TAXII clients σε ένα μοντέλο publish subscribe. [4]

Σημείωση: Η προδιαγραφή TAXII 2.1 διατηρεί τις λέξεις-κλειδιά που απαιτούνται για τα κανάλια, αλλά δεν καθορίζει τις υπηρεσίες καναλιού. Τα κανάλια και οι υπηρεσίες τους θα καθοριστούν σε νεότερη έκδοση του TAXII.



Σχήμα 2.6.1

Οι συλλογές και τα κανάλια μπορούν να οργανωθούν με διαφορετικούς τρόπους. Για παράδειγμα, μπορούν να ομαδοποιηθούν για να υποστηρίξουν τις ανάγκες ενός συγκεκριμένου trust group. Οι βασικοί κανόνες που θεμελιώνουν έναν TAXII Server είναι οι εξής [4]

- Ένα instance ενός TAXII Server μπορεί να υποστηρίξει μία ή πολλές API Roots. Οι API roots είναι λογικές ομαδοποιήσεις καναλιών και συλλογών TAXII και μπορούν να θεωρηθούν instances του API TAXII που διατίθενται σε διαφορετικές διευθύνσεις URL, όπου κάθε API Root είναι η "ριζική" διεύθυνση URL του συγκεκριμένου TAXII API.
- Το TAXII βασίζεται σε υπάρχοντα πρωτόκολλα όταν είναι δυνατόν. Ειδικότερα, οι διακομιστές TAXII ανακαλύπτονται μέσα σε ένα δίκτυο μέσω DNS Service Records (ή/και από ένα Discovery Endpoint που περιγράφεται στην επόμενη ενότητα). Επιπλέον, το TAXII χρησιμοποιεί το HTTPS ως μέσο μεταφοράς για όλες τις επικοινωνίες και χρησιμοποιεί το HTTP για Content Negotiation και Authentication.
- Το TAXII σχεδιάστηκε ειδικά για να υποστηρίζει την ανταλλαγή CTI που εκπροσωπείται στο STIX και η υποστήριξη για την ανταλλαγή περιεχομένου STIX 2.1 είναι υποχρεωτική για εφαρμογή. Ωστόσο, το TAXII μπορεί επίσης να χρησιμοποιηθεί για την κοινή χρήση δεδομένων σε άλλες μορφές. Είναι σημαντικό να σημειωθεί ότι το STIX και το TAXII είναι ανεξάρτητα πρότυπα:

οι δομές και οι σειριοποιήσεις του STIX δεν βασίζονται σε κανένα συγκεκριμένο μηχανισμό μεταφοράς και το TAXII μπορεί να χρησιμοποιηθεί για τη μεταφορά δεδομένων εκτός STIX.

Συνοψίζοντας τα κεφάλαια 2.5 και 2.6 για το πρότυπο STIX / TAXII τα σημαντικότερα σημεία είναι ότι το STIX αποτελεί τη μοντελοποίηση του Threat Intelligence σε επίπεδο δεδομένων και το TAXII, τη μοντελοποίηση του Threat Intelligence sharing σε επίπεδο εφαρμογής. Αν κα τα δύο πρότυπα είναι θεωρητικά ανεξάρτητα, η σχέση μεταξύ τους είναι αρκετά στενή καθώς στην πράξη οι TAXII servers που υπάρχουν αυτή τη στιγμή υλοποιούν ένα υποσύνολο των δυνατοτήτων του προτύπου STIX v2.1. Περισσότερες λεπτομέρειες για τα δύο πρότυπα θα αναδειχθούν στο σχεδιασμό και την υλοποίηση της εφαρμογής.

Κεφάλαιο 3 Εισαγωγή στις έννοιες του Ιδιωτικού Blockchain και του Hyperledger Fabric

3.1 Τι είναι το Blockchain

Το Blockchain είναι ένα κοινόχρηστο, αμετάβλητο αρχείο καταγραφής που διευκολύνει τη διαδικασία ελέγχου συναλλαγών και παρακολούθησης περιουσιακών στοιχείων (asset) σε ένα επιχειρηματικό δίκτυο. Ένα περιουσιακό στοιχείο (asset) μπορεί να είναι υλικό ή άυλο. Ουσιαστικά οτιδήποτε έχει αξία μπορεί να παρακολουθηθεί και να διαπραγματευτεί σε ένα δίκτυο blockchain, μειώνοντας τον κίνδυνο και μειώνοντας το κόστος για όλους τους εμπλεκόμενους. [5]

3.2 Πως λειτουργεί το Blockchain

Καθώς πραγματοποιείται κάθε συναλλαγή, καταγράφεται σε ένα «μπλοκ» δεδομένων Αυτές οι συναλλαγές δείχνουν την κίνηση ενός περιουσιακού στοιχείου που μπορεί να είναι υλικό (product) ή άυλο (intellectual).

Κάθε μπλοκ συνδέεται με αυτά πριν και μετά Αυτά τα μπλοκ σχηματίζουν μια αλυσίδα δεδομένων καθώς ένα περιουσιακό στοιχείο μετακινείται από μέρος σε μέρος ή η ιδιοκτησία αλλάζει χέρια. Τα μπλοκ επιβεβαιώνουν τον ακριβή χρόνο και τη σειρά των συναλλαγών ενώ συνδέονται με ασφάλεια μεταξύ τους για να αποτρέψουν την αλλαγή οποιουδήποτε μπλοκ ή την εισαγωγή μπλοκ μεταξύ δύο υπαρχόντων.

Οι συναλλαγές συναθροίζονται μαζί σε μια μη αναστρέψιμη αλυσίδα: μια αλυσίδα μπλοκ (Blockchain). Κάθε πρόσθετο μπλοκ ενισχύει την επαλήθευση του προηγούμενου μπλοκ και ως εκ τούτου ολόκληρου του blockchain. Αυτό καθιστά προφανή την παραβίαση του blockchain, παρέχοντας τη βασική δύναμη της μη μεταβλητότητας (immutability). Αυτό αφαιρεί την πιθανότητα παραβίασης από

κακόβουλο παράγοντα — και δημιουργεί ένα μαθηματικά ασφαλές αρχείο συναλλαγών για όλα τα εμπλεκόμενα μέλη. [5]

3.3 Τύποι δικτύων Blockchain

Υπάρχουν διάφοροι τρόποι για τη δημιουργία ενός δικτύου blockchain. Μπορούν να είναι δημόσια, ιδιωτικά, αδειοδοτημένα ή κατασκευασμένα από κοινοπραξία.

Δημόσια δίκτυα blockchain (Public) Ένα δημόσιο blockchain είναι αυτό στο οποίο ο καθένας μπορεί να εγγραφεί και να συμμετάσχει, όπως το Bitcoin. Τα μειονεκτήματα περιλαμβάνουν: σημαντική υπολογιστική ισχύ για την εξασφάλιση των ιδιοτήτων του δικτύου, ελάχιστο ή καθόλου απόρρητο για συναλλαγές και αδύναμη ασφάλεια. Αυτά είναι σημαντικά ζητήματα για περιπτώσεις επιχειρηματικής χρήσης blockchain.

Ιδιωτικά δίκτυα blockchain (Private) Ένα ιδιωτικό δίκτυο blockchain, παρόμοιο με ένα δημόσιο δίκτυο blockchain, είναι ένα αποκεντρωμένο δίκτυο peer-to-peer. Ωστόσο, ένας οργανισμός κυβερνά το δίκτυο, ελέγχοντας ποιος επιτρέπεται να συμμετέχει, να εκτελεί ένα πρωτόκολλο συναίνεσης και να διατηρεί το κοινό ledger. Ανάλογα με την περίπτωση χρήσης, αυτό μπορεί να ενισχύσει σημαντικά την εμπιστοσύνη μεταξύ των συμμετεχόντων. Ένα ιδιωτικό blockchain μπορεί να λειτουργήσει πίσω από ένα εταιρικό firewall η ακόμη και να φιλοξενηθεί εσωτερικά, on premises.

Αδειοδοτημένα δίκτυα blockchain (Permissioned) Οι επιχειρήσεις που δημιουργούν ένα ιδιωτικό blockchain θα δημιουργήσουν γενικά ένα αδειοδοτημένο δίκτυο blockchain. Είναι σημαντικό να σημειωθεί ότι τα δημόσια δίκτυα blockchain μπορούν επίσης να λάβουν άδεια. Αυτό θέτει περιορισμούς στο ποιος επιτρέπεται να συμμετέχει στο δίκτυο και σε ποιες συναλλαγές. Οι συμμετέχοντες πρέπει να λάβουν πρόσκληση ή άδεια συμμετοχής.

Δίκτυα κοινοπραξίας blockchain (Consortium) Πολλοί οργανισμοί μπορούν να μοιραστούν τις ευθύνες της διατήρησης ενός blockchain. Αυτοί οι προεπιλεγμένοι οργανισμοί καθορίζουν ποιος μπορεί να υποβάλλει συναλλαγές ή να έχει πρόσβαση στα δεδομένα. Μια κοινοπραξία blockchain είναι ιδανική για επιχειρήσεις όταν όλοι οι συμμετέχοντες πρέπει να έχουν άδεια και να έχουν κοινή ευθύνη για το blockchain. [5]

3.4 Τι είναι το Hyperledger Fabric

Το Hyperledger Fabric, ένα έργο ανοιχτού κώδικα από το Linux Foundation είναι το αρθρωτό σύστημα (modular framework) blockchain και de facto πρότυπο για εταιρικές πλατφόρμες blockchain. Προορισμένη ως βάση για την ανάπτυξη εταιρικών εφαρμογών και βιομηχανικών λύσεων, η ανοιχτή, αρθρωτή αρχιτεκτονική χρησιμοποιεί δομικά μέρη που έχουν ελεγχθεί επαρκώς και λειτουργούν άμεσα, για να φιλοξενήσει ένα ευρύ φάσμα περιπτώσεων χρήσης. [6]

3.5 Πως δουλεύει σε υψηλό επίπεδο το Hyperledger Fabric

ο Hyperledger Fabric διαθέτει προηγμένα στοιχεία ελέγχου απορρήτου, έτσι ώστε μόνο τα δεδομένα που είναι θεμιτό να κοινοποιηθούν κοινοποιούνται μεταξύ των «εξουσιοδοτημένων» (γνωστών) συμμετεχόντων στο δίκτυο. Τα έξυπνα συμβόλαια τεκμηριώνουν τις επιχειρηματικές διαδικασίες που είναι επιθυμτό να αυτοματοποιηθούν με όρους αυτόματης εκτέλεσης μεταξύ των εμπλεκόμενων σε κώδικα γραμμένο σε γενικού σκοπού γλώσσα προγραμματισμού. Ο κώδικας και οι συμφωνίες που περιέχονται σε αυτόν υπάρχουν σε όλο το κατανεμημένο, αποκεντρωμένο δίκτυο blockchain. Οι συναλλαγές είναι ανιχνεύσιμες και μη αναστρέψιμες, δημιουργώντας εμπιστοσύνη μεταξύ των οργανισμών. [6]

3.6 Το μοντέλο του Hyperledger Fabric

Αυτή η ενότητα περιγράφει τα βασικά χαρακτηριστικά σχεδιασμού του Hyperledger Fabric που εκπληρώνουν την υπόσχεσή του για μια ολοκληρωμένη, αλλά προσαρμόσιμη, επιχειρηματική λύση blockchain: [7]

Περιουσιακά στοιχεία (Assets) Οι ορισμοί περιουσιακών στοιχείων επιτρέπουν την ανταλλαγή σχεδόν οτιδήποτε έχει χρηματική αξία. Τα assets αντιπροσωπεύονται στο Hyperledger Fabric ως μια συλλογή ζευγών κλειδιών-τιμών, με τις αλλαγές κατάστασης να καταγράφονται ως συναλλαγές σε ένα Channel Ledger

Κώδικας αλυσίδας (Chaincode) Η εκτέλεση κώδικα χωρίζεται από την διάταξη συναλλαγών (ordering), περιορίζοντας τα απαιτούμενα επίπεδα εμπιστοσύνης και επαλήθευσης μεταξύ των τύπων κόμβων και βελτιστοποιώντας την επεκτασιμότητα και την απόδοση του δικτύου. Το Chaincode είναι κατά βάση ο κώδικας που υλοποιεί το business logic. Το Chaincode επιβάλλει τους κανόνες για την ανάγνωση ή την τροποποίηση ζευγών κλειδιών-τιμών ή άλλων πληροφοριών της State Database. Οι συναρτήσεις Chaincode εκτελούνται σε σχέση με την τρέχουσα State Database του ledger και ξεκινούν μέσω μιας πρότασης συναλλαγής (transaction proposal). Η εκτέλεση Chaincode έχει ως αποτέλεσμα ένα σύνολο εγγραφών από Key Values το οποίο ονομάζεται Write Set και εφαρμόζεται τελικά στα Ledgers όλων των peers.

Δυνατότητες Ledger (Ledger Features) Το Ledger κωδικοποιεί ολόκληρο το ιστορικό συναλλαγών για κάθε κανάλι και περιλαμβάνει δυνατότητα ερωτημάτων τύπου SQL για αποτελεσματικό έλεγχο και επίλυση διαφορών.

Απόρρητο (Privacy) Τα κανάλια και οι private data collections [10] επιτρέπουν ιδιωτικές και εμπιστευτικές πολυμερείς συναλλαγές που συνήθως απαιτούνται από ανταγωνιστικές επιχειρήσεις και ρυθμιζόμενες βιομηχανίες που ανταλλάσσουν περιουσιακά στοιχεία σε ένα κοινό δίκτυο.

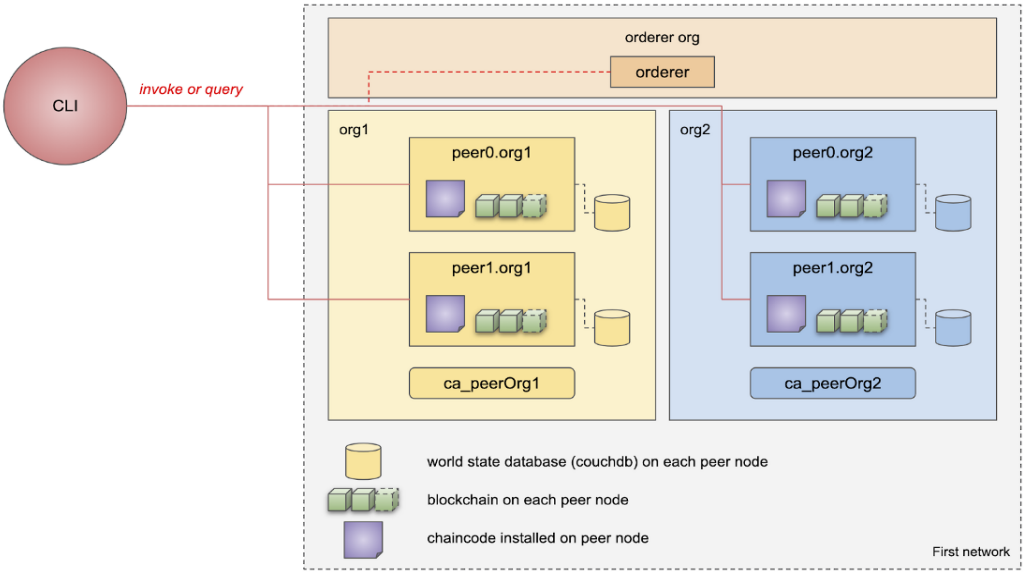
Υπηρεσίες Ασφάλειας και Συνδρομής (Security & Membership Services) Η δυνατότητα για αδειοδοτούμενο membership παρέχει ένα αξιόπιστο δίκτυο blockchain, όπου οι συμμετέχοντες γνωρίζουν ότι όλες οι συναλλαγές μπορούν να εντοπιστούν από εξουσιοδοτημένους ρυθμιστές και ελεγκτές. Το Hyperledger Fabric

υποστηρίζει ένα δίκτυο συναλλαγών όπου όλοι οι συμμετέχοντες έχουν γνωστές ταυτότητες. Η υποδομή δημόσιου κλειδιού (PKI) χρησιμοποιείται για τη δημιουργία κρυπτογραφικών πιστοποιητικών που συνδέονται με οργανισμούς, network components και τελικούς χρήστες ή client applications

Συναίνεση (Consensus) Μια μοναδική προσέγγιση συναίνεσης επιτρέπει την ευελιξία και την επεκτασιμότητα που απαιτούνται για την επιχείρηση. Ο αλγόριθμος συναίνεσης είναι plugable και μπορεί να υλοποιηθεί με πολλούς τρόπους.

3.7 Το First Network του Hyperledger Fabric

Η εφαρμογή έχει βασιστεί σε μία custom εκδοχή του First Network (Fabcar) [8] του Hyperledger Fabric η οποία αποτελείται από 3 κόμβους. Σε αυτό το κεφάλαιο περιγράφεται το First Network σε μεγαλύτερο βάθος για να αναδειχθεί καλύτερα η αρχιτεκτονική του Fabric , να είναι ξεκάθαρο το δίκτυο που χρησιμοποιήθηκε για την ανάπτυξη της εφαρμογής και τέλος να μπορέσουν να υποστηριχθούν στο τέλος θεωρητικά επιχειρήματα για την ενίσχυση της ασφάλειας του δικτύου βασισμένη στην επεξεργασία συγκεκριμένων δομικών μονάδων στην τελευταία ενότητα. Το First Network είναι το εξής:



Σχήμα 3.7.1

Το δίκτυο απαρτίζεται από τρεις οργανισμούς: org1, org2 και orderer org. Όπως δηλώνουν τα ονόματα αλλά και το διάγραμμα οι οργανισμοί 1 και 2 είναι μέλη του δικτύου που αλληλεπιδρούν με το business logic του δικτύου ενώ ο orderer org είναι ένας ανεξάρτητος οργανισμός ο οποίος έχει ως ευθύνη τη διάταξη τον συναλλαγών που που προέρχονται από τους peers των άλλων δύο οργανισμών. Οι οργανισμοί 1 και 2 είναι ισότιμοι από αρχιτεκτονικής πλευράς και απαρτίζονται απο δύο πανομοιότυπους Peer nodes και μία Certificate Authority Node η οποία εκδίδει πιστοποιητικά για τις οντότητες που απαιτείται πιστοποίηση για την ταυτότητα τους ενώ ταυτόχρονα διασφαλίζεται η κρυπτογραφημένη επικοινωνία στα ενδιάμεσα κανάλια και η ακεραιότητα των μεταφερόμενων δεδομένων. Οι Peers είναι πανομοιότυποι εντός του ίδιου οργανισμού και χειρίζονται ένα αντίγραφο της World State Database , του Blockchain και του Chaincode. Ο κώδικας που είναι εγκατεστημένος στους peer nodes είναι ένα απλό παράδειγμα όπου τα assets είναι αυτοκίνητα σε μία εταιρεία και οι οργανισμοί ενδιαφερόμενοι για τον εκάστοτε κάτοχο των αυτοκινήτων. Ο κώδικας αναδεικνύει τόσο τις πτυχές του Ledger Querying που αφορούν ζεύγη κλειδιών-τιμών όσο και πτυχές που αφορούν την ιστορική πορεία των assets, δηλαδή την οπτική Blockchain. Όλοι οι hosts που αναφέρθηκαν είναι μέρος ενός Docker Network στο ίδιο φυσικό μηχάνημα παρόλα αυτά οι επικοινωνίες γίνονται όλες δικτυακά μέσω gRPC calls σε διευθύνσεις οι οποίες ανακαλύπτονται από channel configuration αρχεία ώστε να προσομοιώνεται όσο το δυνατόν καλύτερα το πραγματικό σενάριο. Επιπλέον δε γίνονται υποθέσεις ασφάλειας και οι ενδιάμεσες επικοινωνίες κρυπτογραφούνται και επαληθεύονται ως προς την ακεραιότητα σύμφωνα με το TLS πρωτόκολλο μεταξύ των containers [9].

Κεφάλαιο 4 Μελέτη περίπτωσης χρήσης

4.1 Η επεξήγηση του προβλήματος

Μέχρι αυτό το σημείο έχει γίνει φανερό πρώτον ότι ο διαμοιρασμός CTI μέσω TAXII Servers είναι κατα βάση μία πολυμερής εφαρμογή και δεύτερον ότι είναι κρίσιμη διαδικασία με αυξημένες απαιτήσεις σε ιδιότητες που αφορούν την ασφάλεια. Οι δύο παραπάνω λόγοι καθιστούν μία πλατφόρμα ιδιωτικού blockchain ιδανική επιλογή για την ανάπτυξη μία εφαρμογής CTI. Παρακάτω θα αναφερθούν οι ιδιότητες ασφαλείας που έδρασαν ως κριτήρια επιλογής μίας πλατφόρμας blockchain και το πως εκείνες υλοποιούνται με τον αντίστοιχο μηχανισμό του Hyperledger Fabric.

Εμπιστευτικότητα μεταξύ οργανισμών (Organization Level Privacy)

Το πρότυπο TAXII επιβάλλει εμπιστευτικότητα στις συλλογές αντικειμένων STIX μεταξύ των οργανισμών και μόνο που έχουν δικαίωμα να τα αναγνώσουν. Το Hyperledger Fabric προσφέρει το μηχανισμό των Private Data Collections για αυτό το σκοπό, όπου τα πραγματικά δεδομένα μίας συναλλαγής αποθηκεύονται μόνο στους κόμβους των οργανισμών που έχουν την απαιτούμενη πρόσβαση ενώ οι υπόλοιποι λαμβάνουν μεταδεδομένα και hashes για τη συναλλαγή. Στην περίπτωση του κλασσικού client server μοντέλου του TAXII Server, ο οργανισμός που έχει αναλάβει τη φιλοξενία έχει πλήρη δικαιώματα ανάγνωσης σε κάθε δεδομένο που αποθηκεύεται στη βάση.

Έλεγχος πρόσβασης μεταξύ οργανισμών (Organization Level Access Control)

Το πρότυπο TAXII επιβάλλει τη δυνατότητα εγγραφής στα δεδομένα μόνο στους οργανισμούς που έχουν δικαίωμα για εγγραφή. Το Hyperledger Fabric προσφέρει και για αύτη την περίπτωση τα Private Data Collections. Στην περίπτωση του κλασσικού client server μοντέλου του TAXII Server, ο οργανισμός που έχει αναλάβει τη φιλοξενία έχει πλήρη δικαιώματα εγγραφής σε κάθε δεδομένο που αποθηκεύεται στη βάση.

Ακεραιότητα των δεδομένων (Data Integrity)

Το πρότυπο TAXII δεν επιβάλλει ισχυρή απαίτηση για την επαλήθευση της ακεραιότητας των δεδομένων παρόλα αυτά κρίνεται ότι μία εφαρμογή στο πεδίο της κυβερνοασφάλειας θα έπρεπε σε κάθε περίπτωση να διαθέτει μηχανισμό επαλήθευσης της ακεραιότητας των δεδομένων. Εάν και οι οργανισμοί που συμμετέχουν σε ένα δίκτυο διαμοιρασμού CTI εμπιστεύονται κατα βάση την πληροφόρηση των μερών ο έλεγχος της ακεραιότητας πρέπει να υπάρχει καθώς η παραποίηση των δεδομένων επί του TAXII Server από κακόβουλους παράγοντες οδηγεί σε λανθασμένη πληροφόρηση για όλους τους καταναλωτές CTI και αποτελεί συνεπώς κεντρικό σημείο αποτυχίας. Η ιδιότητα αυτή επιτυγχάνεται από τη φύση των δικτύων blockchain και συνεπώς και από το Hyperledger Fabric καθώς ελέγχεται η ακεραιότητα των δεδομένων από όλους τους peers που κατέχουν την πληροφορία.

Υψηλή διαθεσιμότητα (High Availability)

Μία εφαρμογή πληροφόρησης πρέπει να έχει υψηλή διαθεσιμότητα. Η διαχείριση του TAXII Server ακόμα και εντός του εταιρικού δικτύου και προστατευόμενο απο τείχος προστασίας (firewall) από έναν οργανισμό αποτελεί μοναδικό σημείο αποτυχίας καθώς κακόβουλοι παράγοντες μπορούν με διαφορετικούς τρόπους να καταστήσουν την εφαρμογή μη λειτουργική για τα υπόλοιπα μέρη αποκόβοντας την πληροφόρηση. Το Hyperledger Fabric προσφέρει τη δυνατότητα για έναν οργανισμό να διαχειρίζεται πολλαπλούς peers οι οποίοι δίνουν πλεονασμό (redundancy) δεδομένων και υπηρεσίας σε επίπεδο οργανισμού. Επίσης το γεγονός ότι και οι κόμβοι των υπόλοιπων οργανισμών διαθέτουν κάθε στιγμή το distributed ledger σημαίνει ότι έχουμε πλεονασμό ακόμα και εάν αποσυνδεθούν απ το δίκτυο όλοι οι κόμβοι ενός οργανισμού.

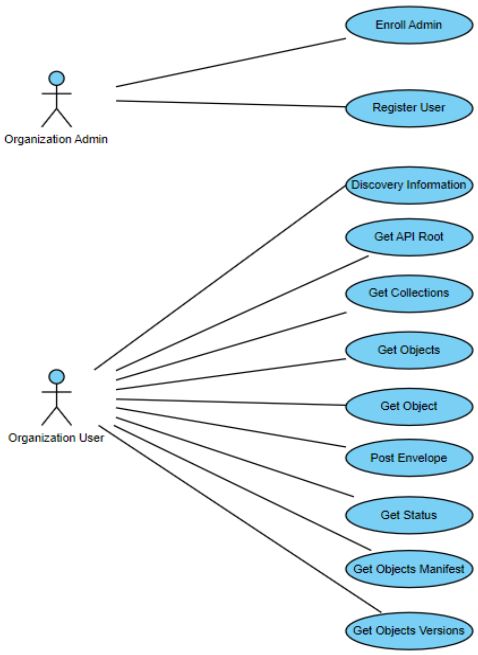
Μη Αποκήρυξης και Ελεγξιμότητας (Non Repudiation and Auditability)

Μία λανθασμένη πληροφόρηση κυβερνοασφάλειας ενός μέρους του CTI δικτύου μπορεί να έχει καταστροφικές συνέπειες. Στην περίπτωση αυτή θα πρέπει να μην μπορεί να ισχυριστεί ο παραγωγός της πληροφορίας ότι δεν ευθύνεται για την πληροφόρηση ούτε ο διαχειριστής του TAXII Server να μπορέσει να πράξει προς το συμφέρον κάποιου συγκεκριμένου μέρους. Το γεγονός ότι οι συναλλαγές καταγράφονται από τους κόμβους όλων των οργανισμών παρέχει εν γένει αυτή την ιδιότητα.

Είναι λοιπόν φανερό ότι η ανάπτυξη μίας πολυμερούς εφαρμογής διαμοιρασμού CTI στο Hyperledger Fabric μπορεί να επιλύσει πολλά από τα προβλήματα που εμφανίζονται στο κλασσικό client server μοντέλο.

4.2 Η εμβέλεια της εφαρμογής

Στόχος στην παρούσα εργασία είναι να αναπτυχθεί ένας βασικός TAXII Server που να καλύπτει τις βασικές διεπαφές μέσω REST API και το επίπεδο πρόσβασης στα δεδομένα να υλοποιείται από Chaincode στο Hyperledger Fabric. Για να πετύχουμε το στόχο αυτό πρέπει να ορίσουμε ένα βασικό σύνολο διεπαφών και χαρακτηριστικών του TAXII προτύπου που θέλουμε να καλύψουμε καθώς το TAXII ορίζει κάποιες βασικές λειτουργίες [12] αλλά η ανάπτυξη του μπορεί να προχωρήσει σε μεγάλο βάθος καλύπτοντας σύνθετα εξατομικευμένα σενάρια. Το διάγραμμα που απεικονίζεται παρακάτω περιγράφει τις βασικές λειτουργίες που εκτίθενται με REST API



Σχήμα 4.2.1

Οι λειτουργίες που μπορεί να εκτελέσει ο διαχειριστής του οργανισμού είναι οι Enroll Admin και Register User [11] και αφορούν καθαρά το κομμάτι του Hyperledger Fabric. Το endpoint Enroll Admin λαμβάνει τα στοιχεία του αρχικού διαχειριστή του δικτύου και προχωρά στην έκδοση ενός πιστοποιητικού x509 το οποίο μπορεί να διανεμηθεί σε άλλους διαχειριστές η να χρησιμοποιηθεί από τον ίδιο. Το endpoint Register User λαμβάνει το προαναφερθέν πιστοποιητικό διαχειριστή x509 και εκδίδει ένα πιστοποιητικό x509 μαζί με επιπρόσθετα μεταδεδομένα το οποίο ονομάζεται πορτοφόλι (Wallet), ενώ ο χρήστης λαμβάνει ένα όνομα χρήστη (Enrollment ID) και έναν κωδικό (Enrollment Secret).

Οι λειτουργίες που μπορεί να εκτελέσει ο χρήστης του οργανισμού είναι όλες οι διεπαφές που ορίζει το πρότυπο TAXII [12] στον αντίστοιχο βαθμό που επιτρέπει ένα σύστημα blockchain ως επίπεδο πρόσβασης στα δεδομένα. Εν συντομία απουσιάζει η λειτουργία του Delete Object καθώς μία τέτοια λειτουργία δεν έχει νόημα σε μία πλατφόρμα όπως το Hyperledger Fabric διότι τα ζεύγη κλειδιών-τιμών που εγγράφονται στο αμετάβλητο καθολικό μέσω συναλλαγών δεν μπορούν να διαγραφούν παρά μόνο να αλλάξουν τιμή. Θα μπορούσε να υλοποιηθεί μία λειτουργία διαγραφής STIX αντικειμένου από μία συλλογή που να αφαιρεί το αντικείμενο από την State Database όμως η προηγούμενη τιμή του θα ήταν ορατή σε όλους τους χρήστες που έχουν πρόσβαση μέσω απλής ανάγνωσης του Blockchain.

Κάθε λειτουργία προς υλοποίηση δέχεται παραμέτρους κυρίως με HTTP Header και URL Parameters οι οποίες υλοποιούν τα χαρακτηριστικά της Αυθεντικοποίησης (Authentication) , της διαπραγμάτευσης περιεχομένου (Content Negotiation), του φιλτραρίσματος (Filtering) και της σελιδοποίησης (Pagination). Δεδομένου ότι καλύπτεται ένα βασικό πρότυπο TAXII για να αναδείξει τα οφέλη του ιδιωτικού Blockchain στο διαμοιρασμό CTI οι λειτουργίες αυτές έχουν υλοποιηθεί σε πολύ συγκεκριμένο βάθος:

Authentication Καλύπτεται το σενάριο της βασικής αυθεντικοποίησης (Authentication Basic)

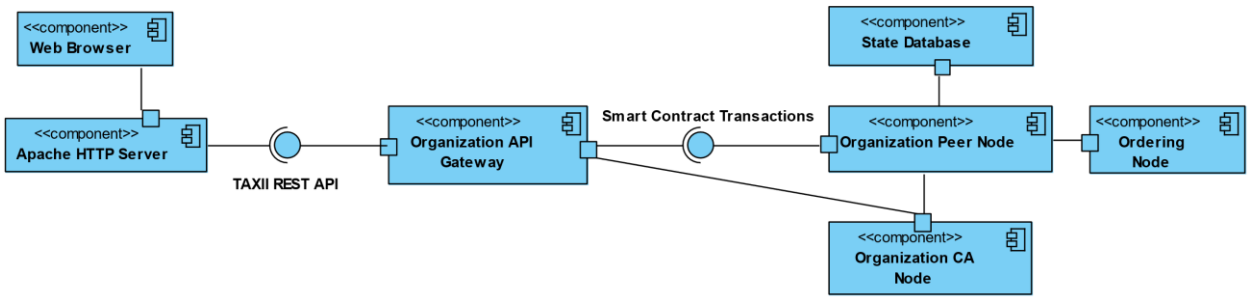
Content Negotiation Ο TAXII Server επιβάλλει προς το παρόν το διαμοιρασμό μόνο περιεχομένου JSON και έκδοσης application/taxii+json;version=2.1

Filtering Ο TAXII Server υλοποιεί filtering για ορισμένα πεδία τα οποία θα αναφερθούν αργότερα

Pagination Ο TAXII Server υλοποιεί σελιδοποίηση μόνο για τα collections τα οποία είναι διαθέσιμα σε όλους τους οργανισμούς δηλαδή όχι για τα private data collections.

Πέρα από τις λειτουργίες που εκτίθενται με REST API υλοποιήθηκε ένα Web Client σε JavaScript το οποίο απεικονίζει με γραφικό τρόπο όλες τις λειτουργίες που αναφέρθηκαν προηγουμένως καθώς αυτό είναι πολύ προτιμότερο σε κάποιες από τις περιπτώσεις ενώ περιλαμβάνει και έναν ενσωματωμένο οπτικοποιητή STIX δεδομένων για την καλύτερη κατανόηση των εμπλεκόμενων εννοιών.

Οι συνιστώσες λογισμικού του συστήματος απεικονίζονται στο παρακάτω UML Component Diagram



Σχήμα 4.2.2

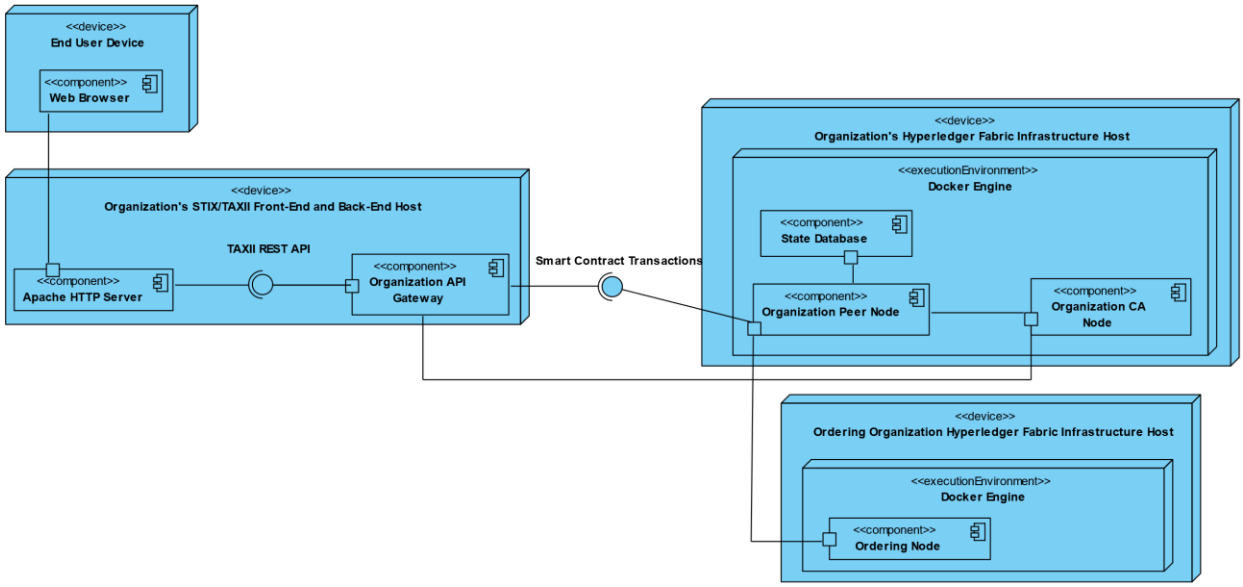
Αυτό που απεικονίζει είναι η αλληλεπίδραση μίας εφαρμογής με το API Gateway του οργανισμού, το οποίο αποτελεί καθαρά διαμεσολαβητή για το δίκτυο του Hyperledger Fabric και συγκεκριμένα τον Peer Node ο οποίος θα αναλάβει να

εκτελέσει την επερώτηση (Query) η την υποβολή συναλλαγής (Transaction Submission) από πλευράς του πελάτη. Ο Peer κόμβος αποστέλει τις συναλλαγές στην υπηρεσία διάταξης και τελικά αφού περάσει τους αντίστοιχους ελέγχους καταλήγει στο κατανεμημένο καθολικό (Distributed Ledger) το οποίο αποτελείται από την State Database και το Blockchain.

Όσον αφορά την αρχιτεκτονική της εφαρμογής χρησιμοποιήθηκε και επεξεργάστηκε κατάλληλα το First Network του Hyperledger Fabric σε ένα τοπικό δίκτυο από Docker Containers. Συγκεκριμένα έγιναν οι παρακάτω αλλαγές

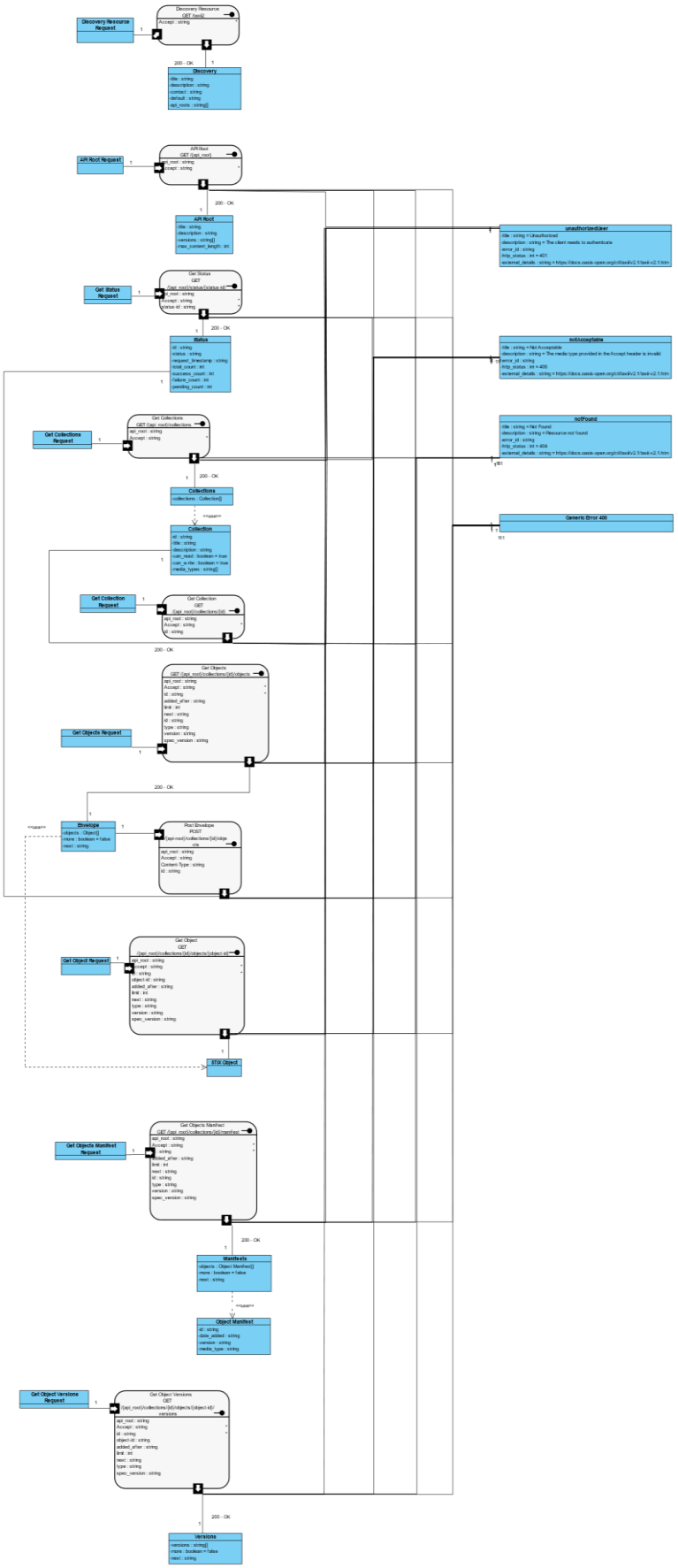
- Προσθήκη τρίτου οργανισμού στο δίκτυο για την καλύτερη ανάδειξη των λειτουργιών της εφαρμογής και τον έλεγχο των αλγορίθμων consensus σε ρεαλιστικότερες συνθήκες
- Αλλαγή της προκαθορισμένης State Database σε CouchDB σύμφωνα με την τεκμηρίωση του Hyperledger Fabric για την ευκολότερη εποπτεία των δεδομένων , την επίδοση των επερωτημάτων και την ενεργοποίηση των πλούσιων επερωτημάτων (rich queries)
- Ενεργοποίηση της δυνατότητας για Private Data Collections στο δίκτυο για προκαθορισμένους οργανισμούς μέσω αρχείου παραμετροποίησης κατά την εκκίνηση του δικτύου.

Ακολουθεί το Deployment Diagram της εφαρμογής και του αντιστοίχου δικτύου Blockchain που λειτουργεί ως επίπεδο πρόσβασης στα δεδομένα. Το διάγραμμα αυτό απεικονίζει το πως διατάσσονται οι παραπάνω συνιστώσες λογισμικού σε φυσικό επίπεδο:



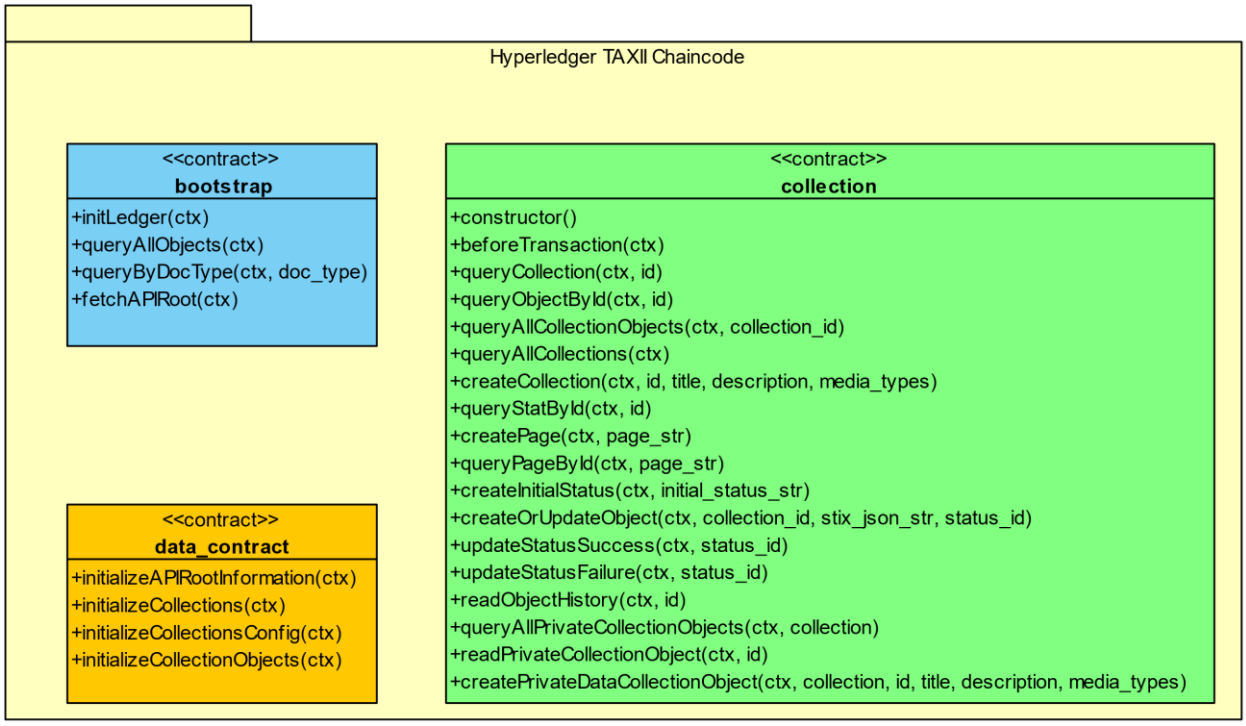
Σχήμα 4.2.3

Το διάγραμμα αυτό δείχνει την εικόνα της υποδομής σε υψηλό επίπεδο από την οπτική του πρώτου οργανισμού. Υπάρχουν ακόμη δύο οργανισμοί οι οποίοι έχουν πανομοιότυπη λογική και φυσική υποδομή με τον παραπάνω. Το Class Diagram που εμβαθύνει περισσότερο στις διεπαφές REST API που εκθέτει ο TAXII Server [12] είναι το εξής:



Σχήμα 4.2.4

Πέρα από το διάγραμμα UML Class που τεκμηριώνει τη διεπαφή REST API του API Gateway έχει σχεδιαστεί το παρακάτω UML Class Diagram που τεκμηριώνει τα smart contracts



Σχήμα 4.2.5

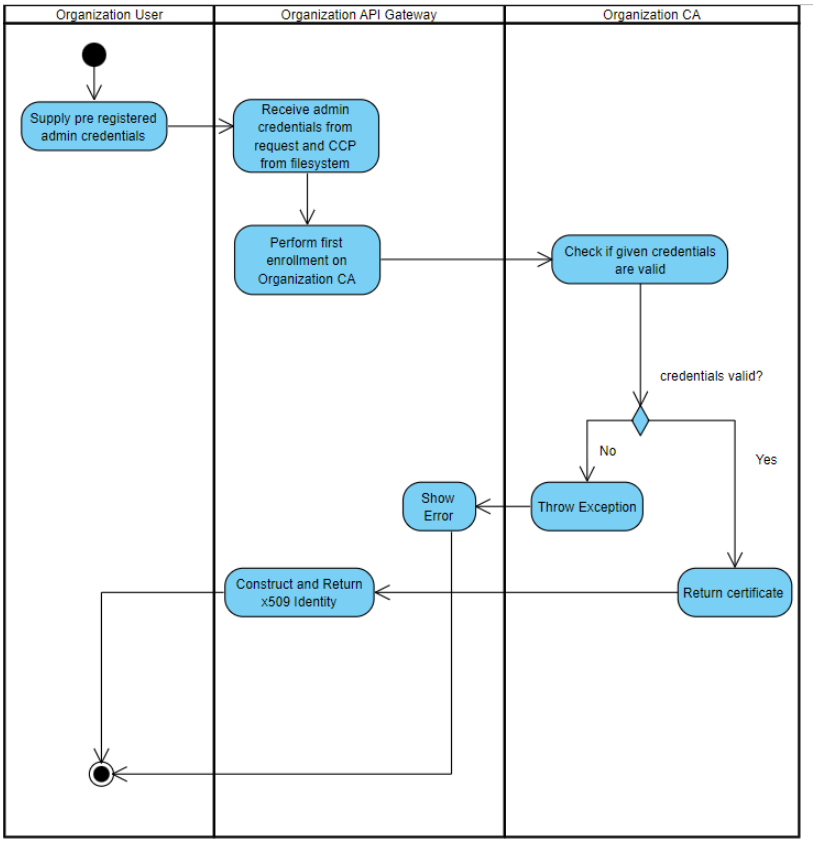
Παρακάτω θα αναλύσουμε πως τα παραπάνω δύο διαγράμματα που ορίζουν τις διεπαφές από πλευράς REST και από πλευράς Chaincode συνδυάζονται μεταξύ τους για να σχεδιαστεί ο TAXII Server.

4.3 Περίπτωση χρήσης Enroll Admin

4.3.1. Σύντομη περιγραφή

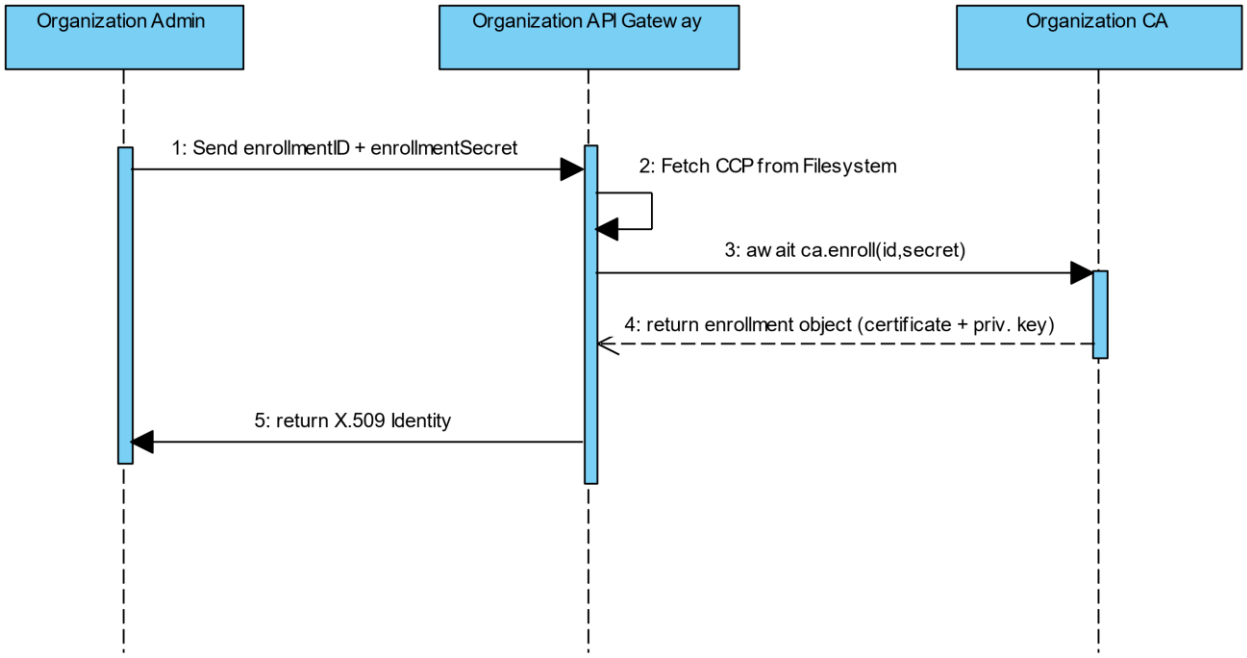
Η λειτουργία αυτή υπάρχει έτσι ώστε χρησιμοποιώντας τα προεγγεγραμμένα στοιχεία των διαχειριστών του Hyperledger Fabric στο σύστημα να εκδοθεί το πιστοποιητικό τους (Enroll). Αυτό απαιτείται για να μπορέσουν να αλληλεπιδράσουν με τη αρχή πιστοποίησης (Certificate Authority) και να εκδόσουν χρήστες (Users). Η κλήση αυτού το endpoint αφορά αμιγώς το Hyperledger Fabric.

4.3.2 Activity Diagram



Σχήμα 4.3.1

4.3.3 Sequence Diagram



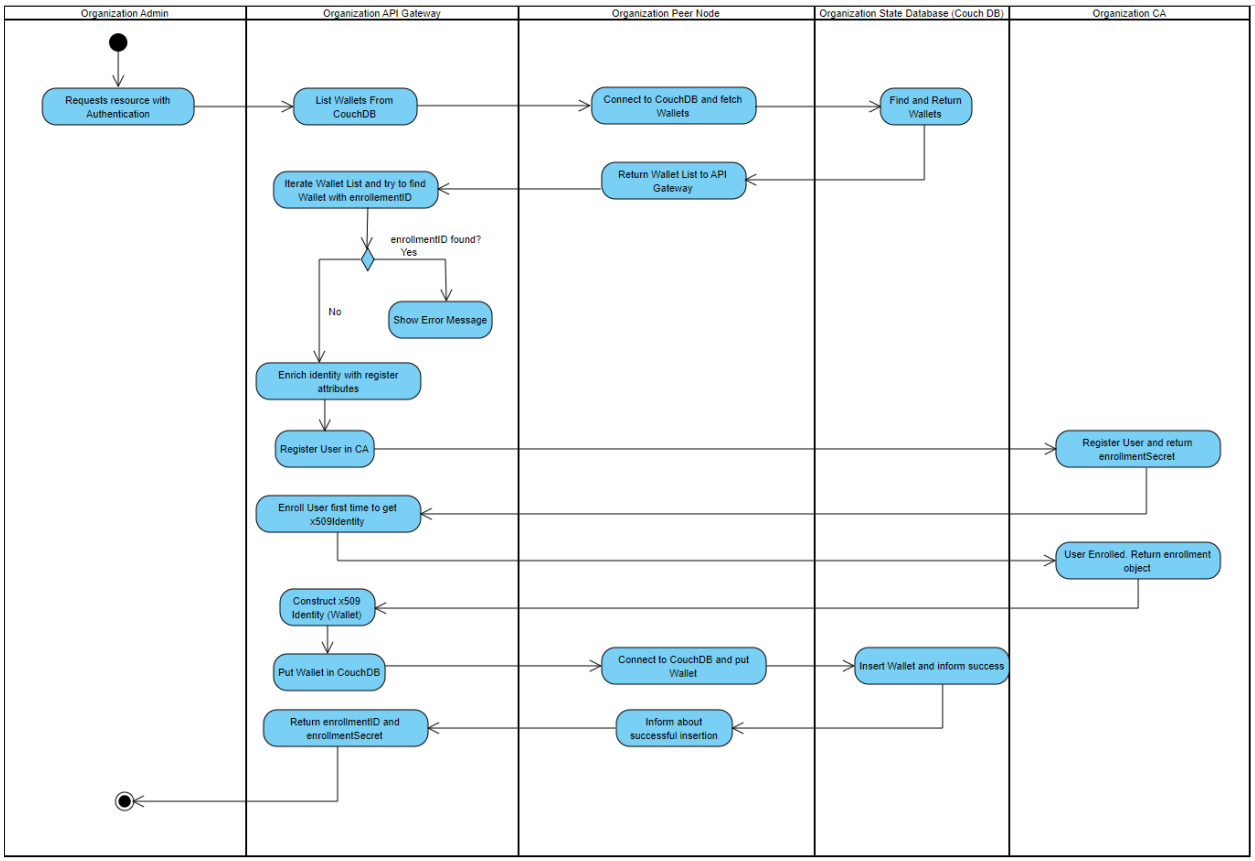
Σχήμα 4.3.2

4.4 Περίπτωση χρήσης Register User

4.4.1. Σύντομη περιγραφή

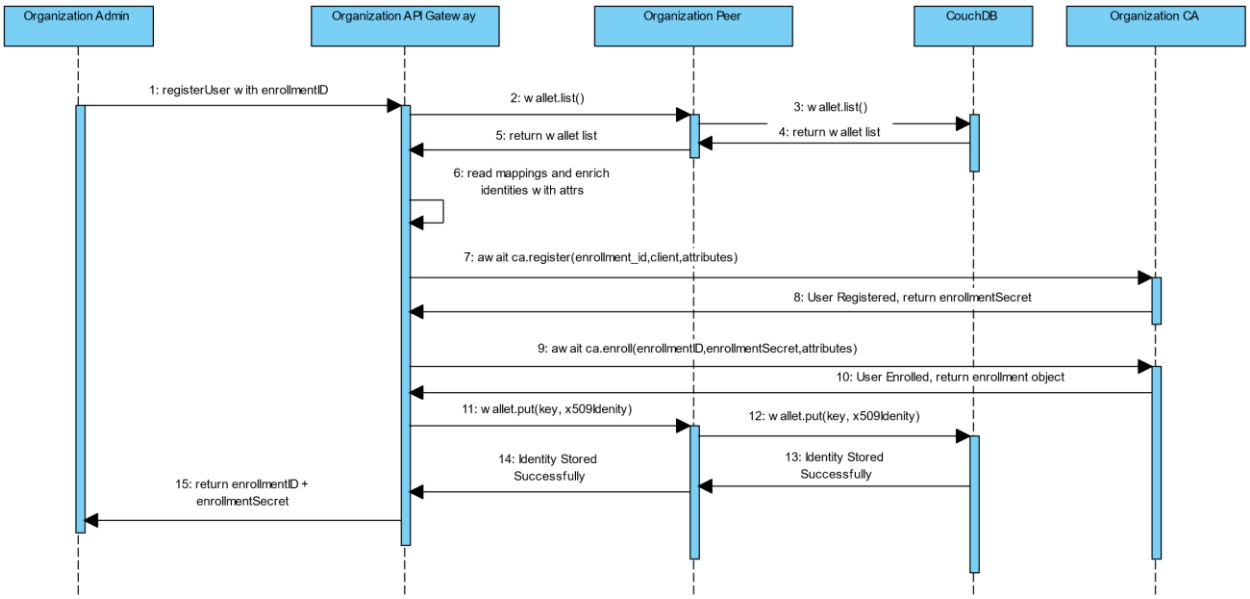
Η λειτουργία αυτή υπάρχει έτσι ώστε χρησιμοποιώντας το πιστοποιητικό διαχειριστή που έχει εκδοθεί από την κλήση της enroll admin να γίνουν η εγγραφή του χρήστη στη βάση δεδομένων της αρχής πιστοποίησης (CA) , η έκδοση του πρωταρχικού πιστοποιητικού (enrollment) , η αποθήκευση της ταυτότητας του χρήστη (wallet ή identity) στην CouchDB και η επιστροφή των credentials (enrollmentID, enrollmentSecret) στο χρήστη ώστε να μπορεί να έχει πρόσβαση στο wallet του για τις επόμενες κλήσεις. [11]

4.4.2 Activity Diagram



Σχήμα 4.4.1

4.4.3 Sequence Diagram



Σχήμα 4.4.2

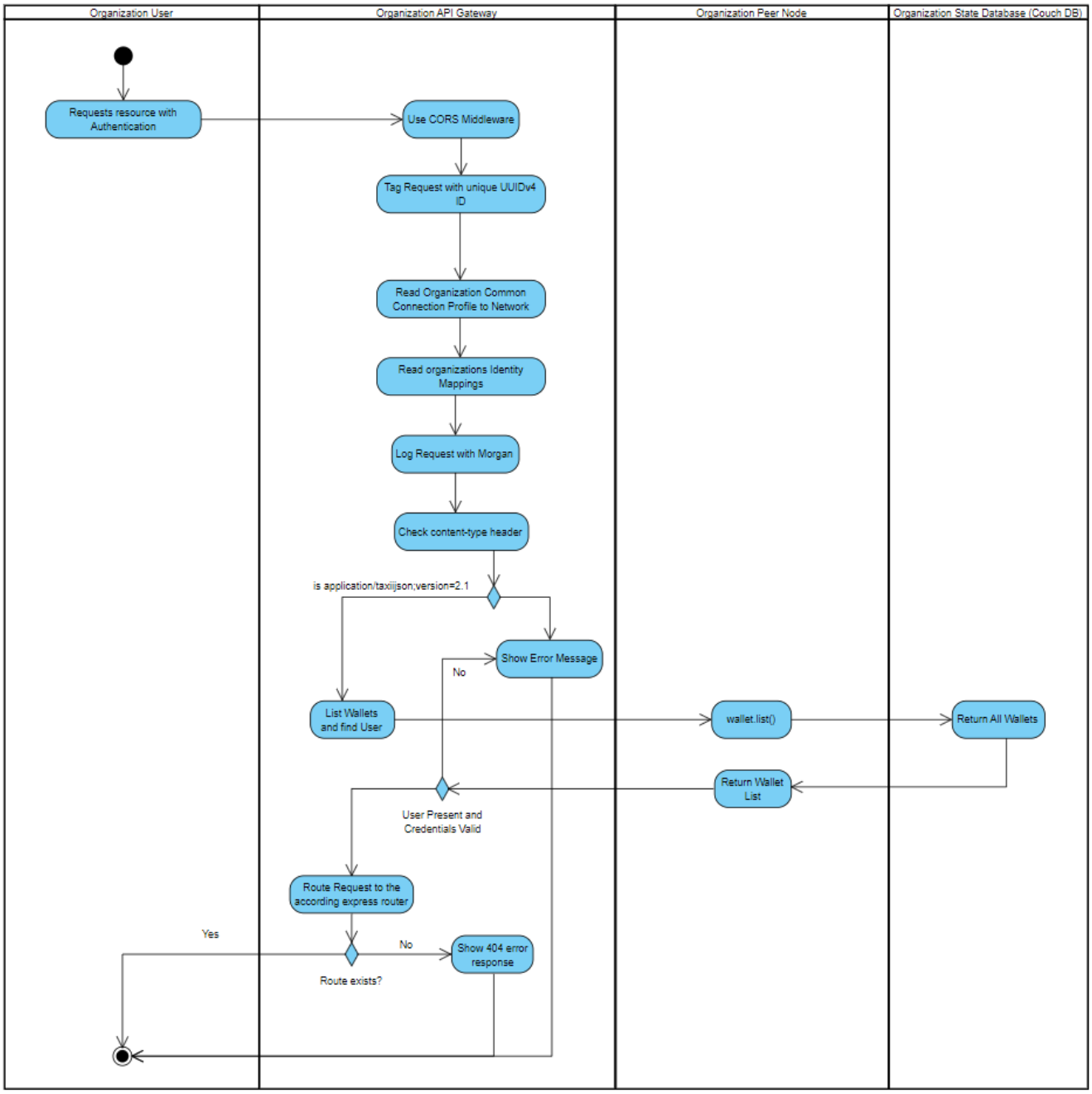
4.5 Περίπτωση χρήσης Middleware και Authentication

4.5.1. Σύντομη περιγραφή

Οι λειτουργίες αυτές υπάρχουν με τη μορφή middleware στον expressJS server και καλύπτουν όλο το φάσμα των υπόλοιπων REST API Endpoints σε επίπεδο middleware και οι δύο βασικοί στόχοι τους είναι η συμμόρφωση με το πρότυπο STIX/TAXII [12] και η ενσωμάτωση με το Hyperledger Fabric. Συγκεκριμένα καλύπτεται το κομμάτι του CORS (Cross Origin Resource Sharing) , το κομμάτι του content negotiation στο οποίο έχει ληφθεί η απόφαση για ανταλλαγή μόνο STIX version 2.1 με JSON format , το κομμάτι του logging ώστε να μπορούν να ανιχνεύονται πιθανά προβλήματα και το κομμάτι του Authentication. Το Authentication που

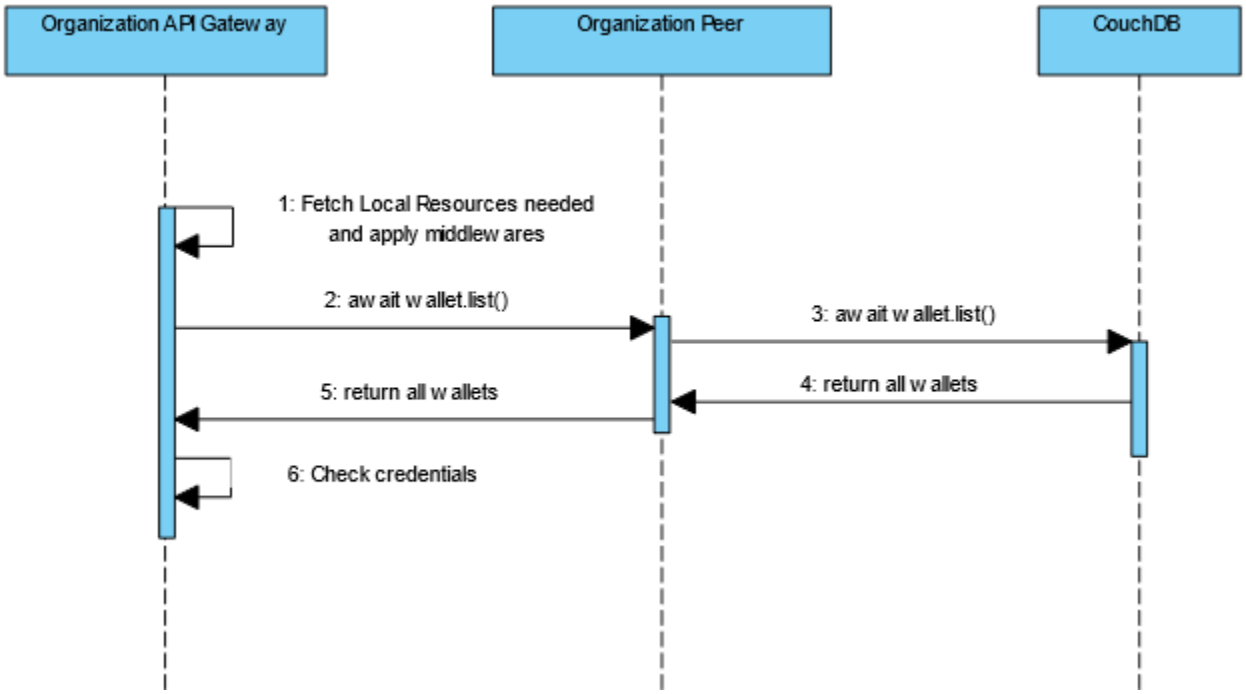
αποτελεί και το συνθετότερο επίπεδο middleware συνίσταται από την αποκωδικοποίηση του Authentication Basic header , την επερώτηση της CouchDB για την ύπαρξη κλειδιού με τιμή ίση με το username του παραπάνω header και την ανάκτηση του πιστοποιητικού από τη βάση. Σε περίπτωση μη ύπαρξης πιστοποιητικού για αυτό το χρήστη η σε περίπτωση λάθος κωδικού ο χρήστης λαμβάνει αντίστοιχο μήνυμα σφάλματος ενώ σε περίπτωση επιτυχημένης ταυτοποίησης οι επόμενες κλήσεις στο blockchain δίκτυο γίνονται με το πιστοποιητικό του χρήστη.

4.5.2 Activity Diagram



Σχήμα 4.5.1

4.5.3 Sequence Diagram



Σχήμα 4.5.2

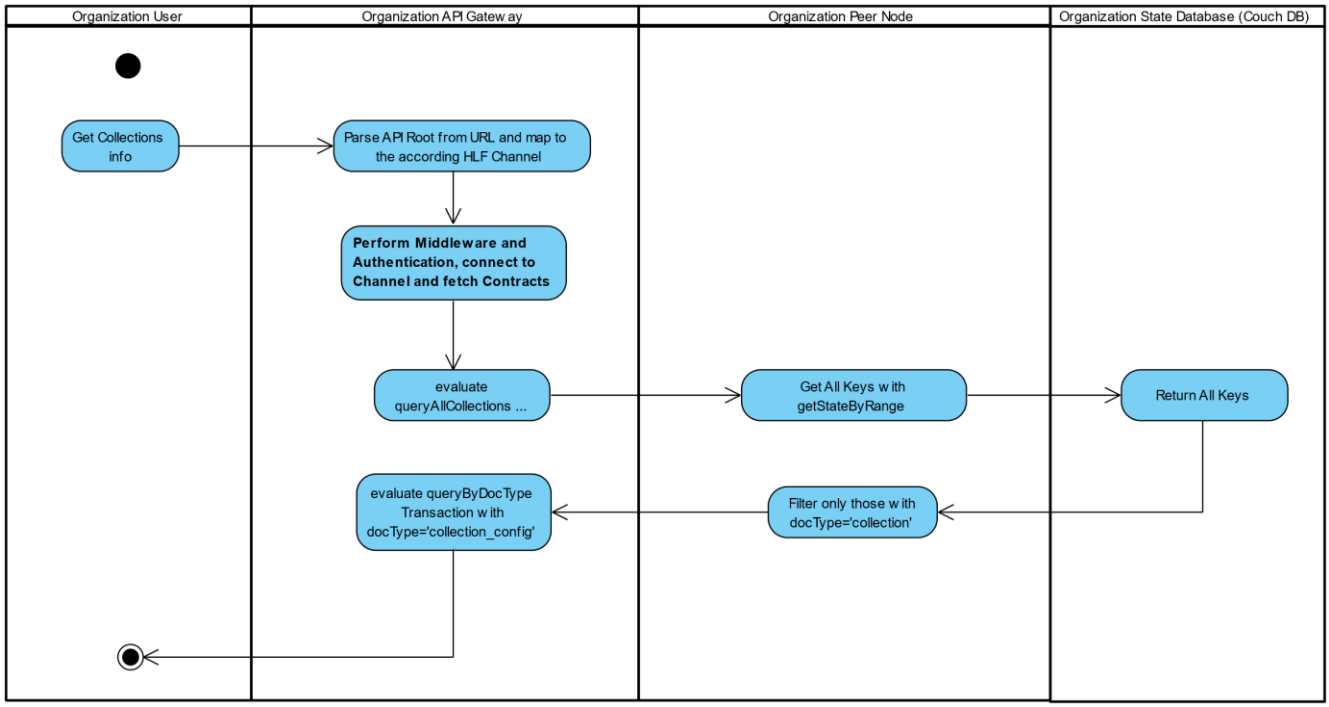
4.6 Περίπτωση χρήσης GET API Root

4.6.1. Σύντομη περιγραφή

Η λειτουργία αυτή εξυπηρετεί τη λήψη επιπλέον πληροφοριών σχετικά με τα API Roots του TAXII Server [12]. Τα API Roots είναι ο υψηλότερου επιπέδου λογικό διαχωρισμός των TAXII Servers και στο πλαίσιο της εργασίας αυτής έχει γίνει η παραδοχή ότι ένα API Root TAXII αντιστοιχεί σε ένα ακριβώς Hyperledger Fabric Channel το οποίο με τη σειρά του είναι το υψηλότερο επίπεδο λογικού διαχωρισμού στο Fabric μετά το network. Η συμμετοχή συνεπώς σε ένα κανάλι Hyperledger fabric συνεπάγεται άμεσα τη συμμετοχή στο αντίστοιχο API Root , οπότε το endpoint αυτό

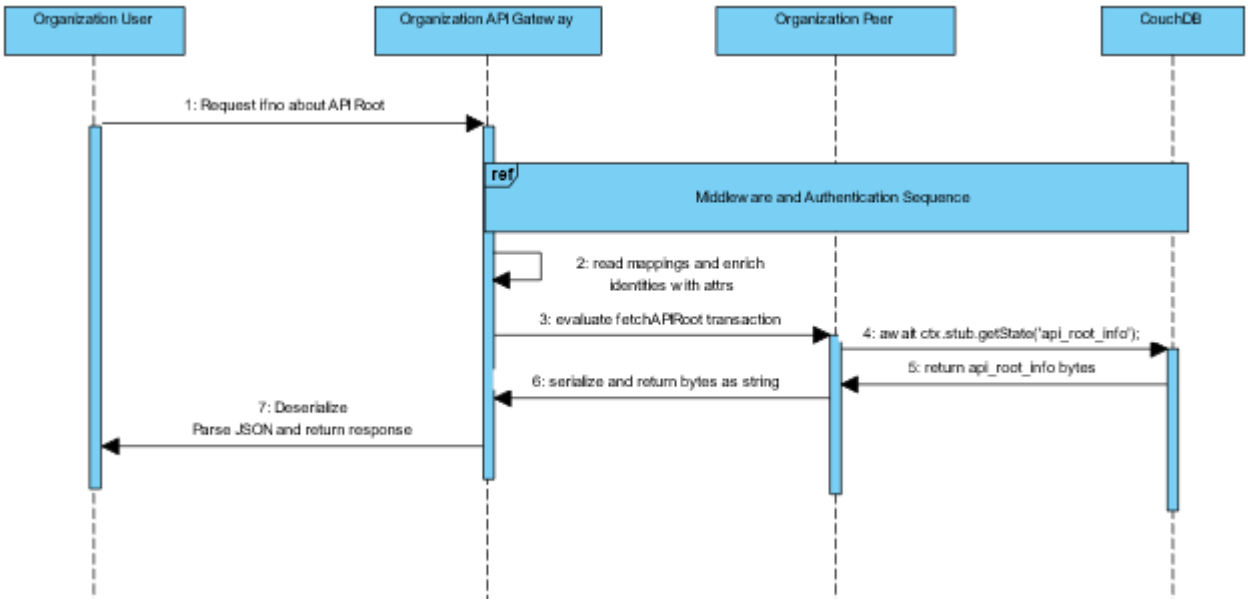
έχει σκοπό τη λήψη περαιτέρω πληροφοριών για το API Root και των συμμετεχόντων αυτού.

4.6.2 Activity Diagram



Σχήμα 4.6.1

4.6.3 Sequence Diagram



Σχήμα 4.6.2

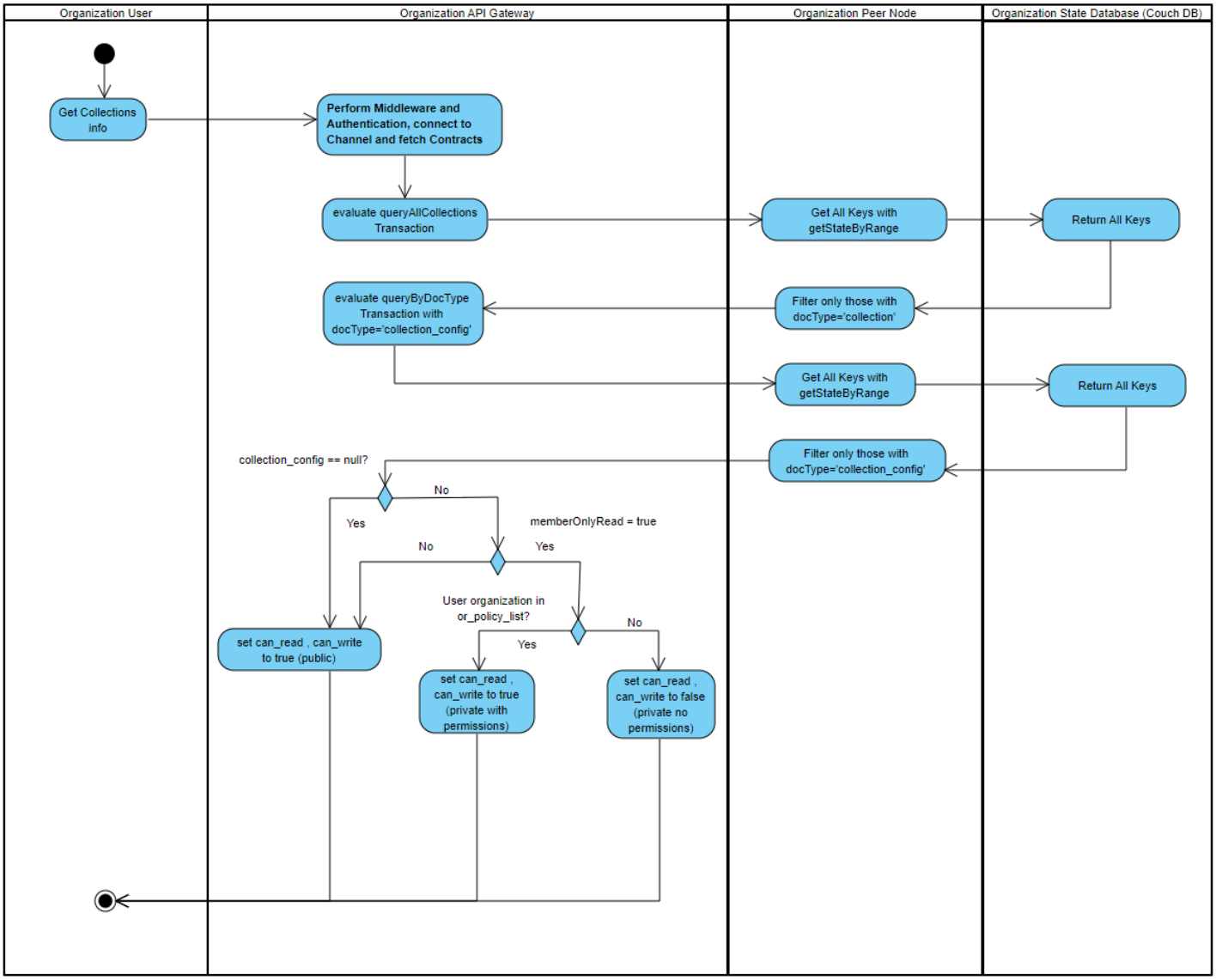
4.7 Περίπτωση χρήσης GET Collections

4.7.1. Σύντομη περιγραφή

Η λειτουργία αυτή εξυπηρετεί την ανάγνωση περαιτέρω στοιχείων και των δικαιωμάτων του χρήστη επί των TAXII Collections που βρίσκονται σε ένα συγκεκριμένο API Root [12]. Τα TAXII Collections είναι το δεύτερο ιεραρχικά επίπεδο λογικής ομαδοποίησης των STIX Objects μετά τα API Roots και η πρόσβαση ενός οργανισμού σε αυτά πρέπει να ρυθμίζεται από δικαιώματα εγγραφής και ανάγνωσης. Για να καλυφθεί το σενάριο όπου ένα η περισσότερα TAXII Collections πρέπει να είναι προσβάσιμα μόνο από συγκεκριμένους οργανισμούς χρησιμοποιήθηκε ο μηχανισμός των private data collections με τα οποία μόνο οι δηλωμένοι σύμφωνα με το αρχείο collections_config οργανισμοί έχουν πρόσβαση στα αναφερθέντα εντός του αρχείου

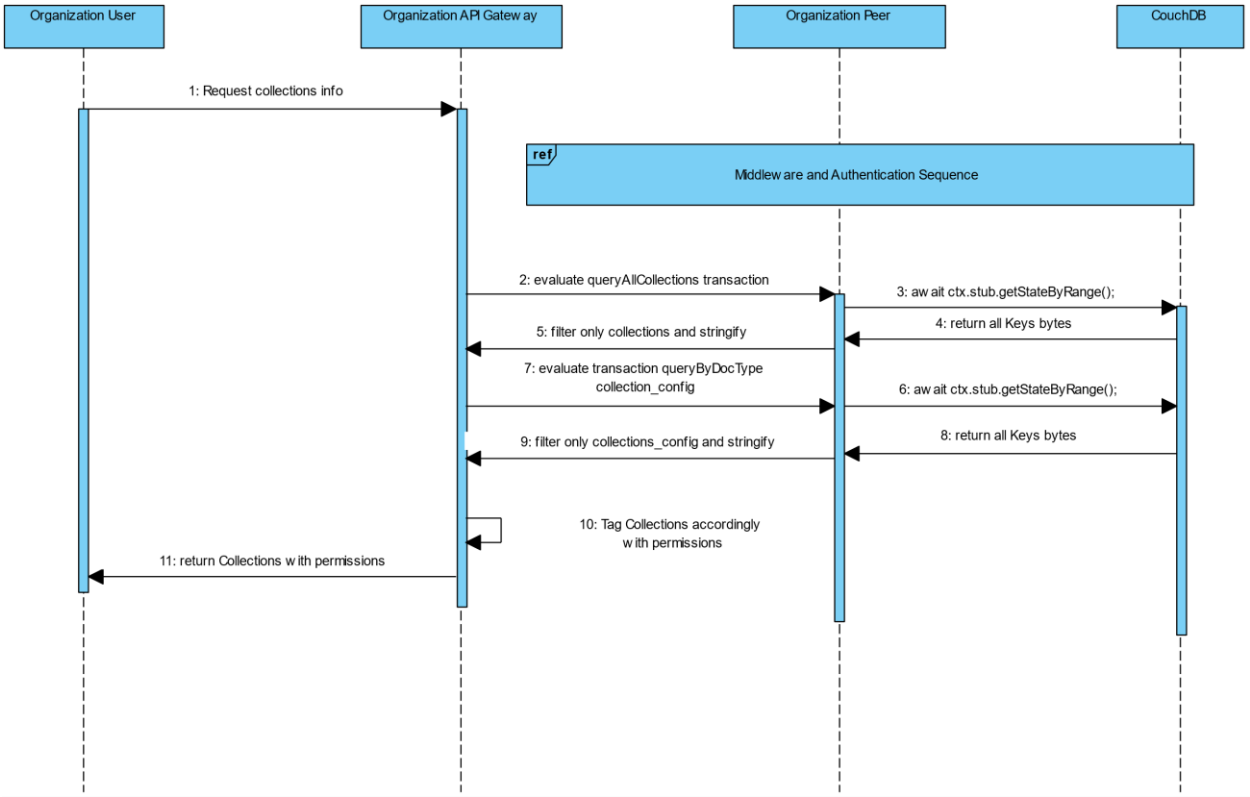
collections και με τα συγκεκριμένα δικαιώματα που αναγράφονται σε αυτό. Το αρχείο είναι σε JSON format και αξιοποιείται μαζί με τα υπόλοιπα αρχεία που χρησιμοποιούνται για να κάνουν deploy το δίκτυο. Για να διευκολυνθεί η διαδικασία υπολογισμού των δικαιωμάτων του χρήστη το collections_config αρχείο αποθηκεύεται στο blockchain και χρησιμοποιείται για να ενημερώσει δυναμικά τους χρήστες των οργανισμών για την πρόσβαση τους στα private data collections. Επίσης αποθηκεύεται το configuration για κάθε Collection ξεχωριστά.

4.7.2 Activity Diagram



Σχήμα 4.7.1

4.7.3 Sequence Diagram



Σχήμα 4.7.2

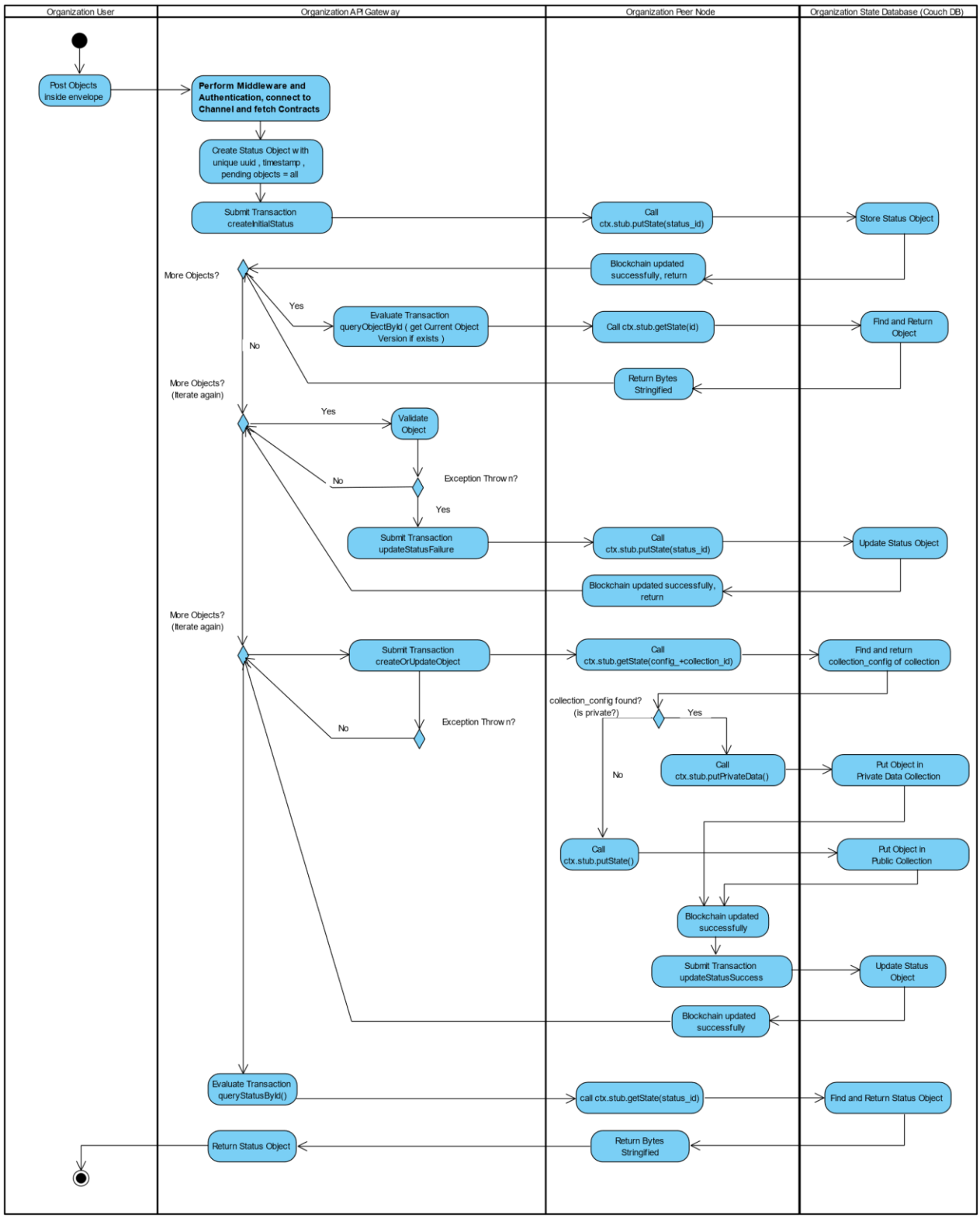
4.8 Περίπτωση χρήσης POST Envelope

4.8.1 Σύντομη περιγραφή

Η λειτουργία αυτή εξυπηρετεί την δημιουργία και την ανανέωση των STIX Objects εντός ενός συγκεκριμένου Collection [12]. Συγκεκριμένα λαμβάνεται ως είσοδος ένα envelope object το οποίο είναι στην πραγματικότητα μία wrapper λίστα πάνω από STIX Objects. Ο χρήστης του οργανισμού δίνει το API Root και το Collection στο URL

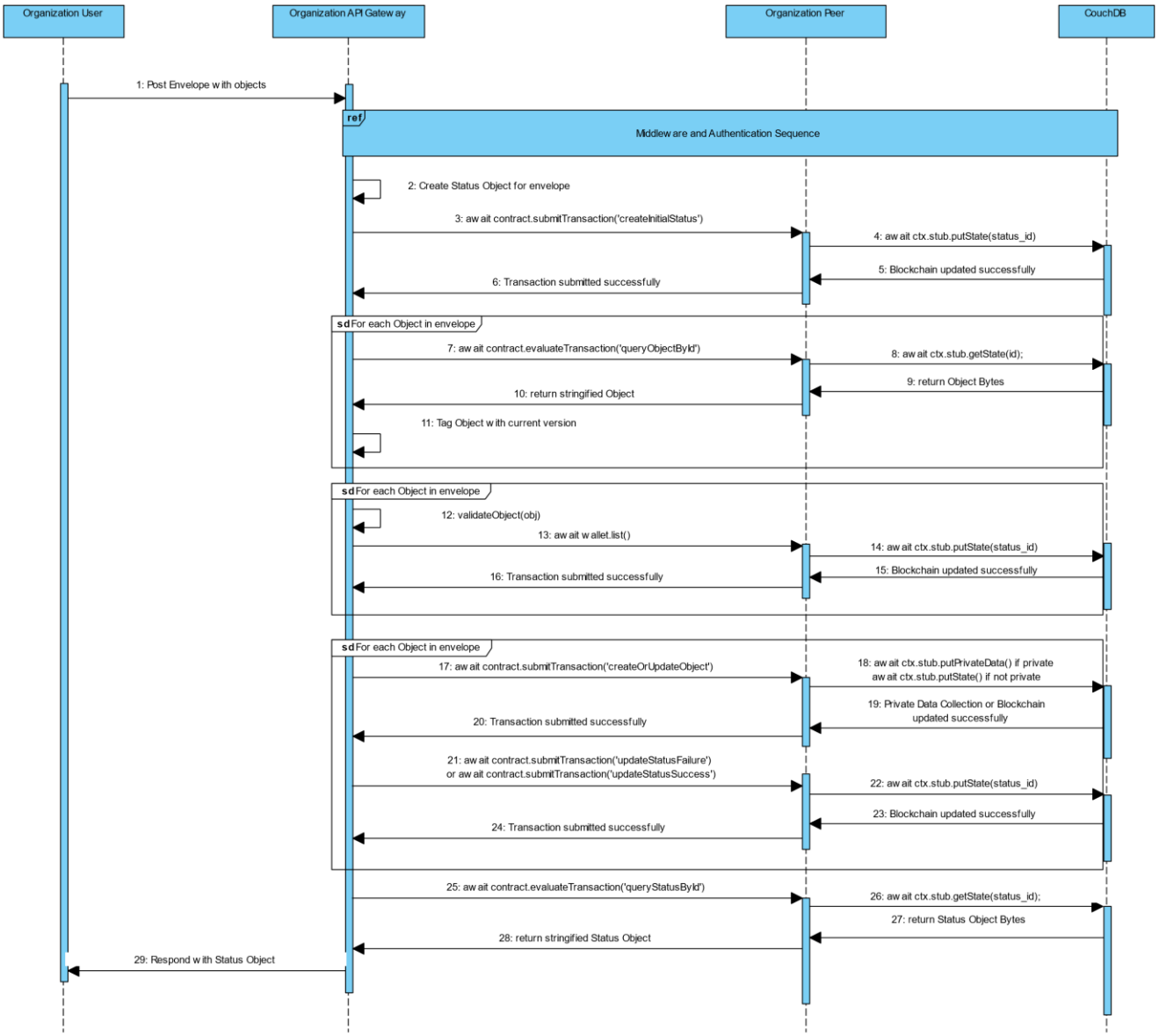
του endpoint και τη λίστα με τα αντικείμενα ως Envelope στο Request Body. Το envelope διαβάζεται και δημιουργείται ένα Status Object το οποίο λαμβάνει ένα μοναδικό αναγωνριστικό και ένα timestamp ενώ διατηρεί τα πεδία total count , success count , failure count για να αναφέρει αργότερα στο χρήστη πόσα από τα αντικείμενα καταχωρήθηκαν επιτυχώς στο Blockchain. Η δομή αυτή επιβάλλεται από το πρότυπο TAXII με στόχο να επιστραφεί στον χρήστη στο τέλος της κλήσης της POST Envelope ή να επιστραφεί ασύγχρονα στο χρήστη με την λειτουργία GET Status η οποία θα τεκμηριωθεί αργότερα. Στο status object δεν αναγράφεται η αιτία αποτυχίας της εισαγωγής ή της αλλαγής του εκάστοτε αντικειμένου παρά μόνο τα γενικά στατιστικά. Περισσότερες πληροφορίες μπορούν να βρεθούν στα Logs του API Gateway και του Organization Peer Node.

4.8.2 Activity Diagram



Σχήμα 4.8.1

4.8.3 Sequence Diagram



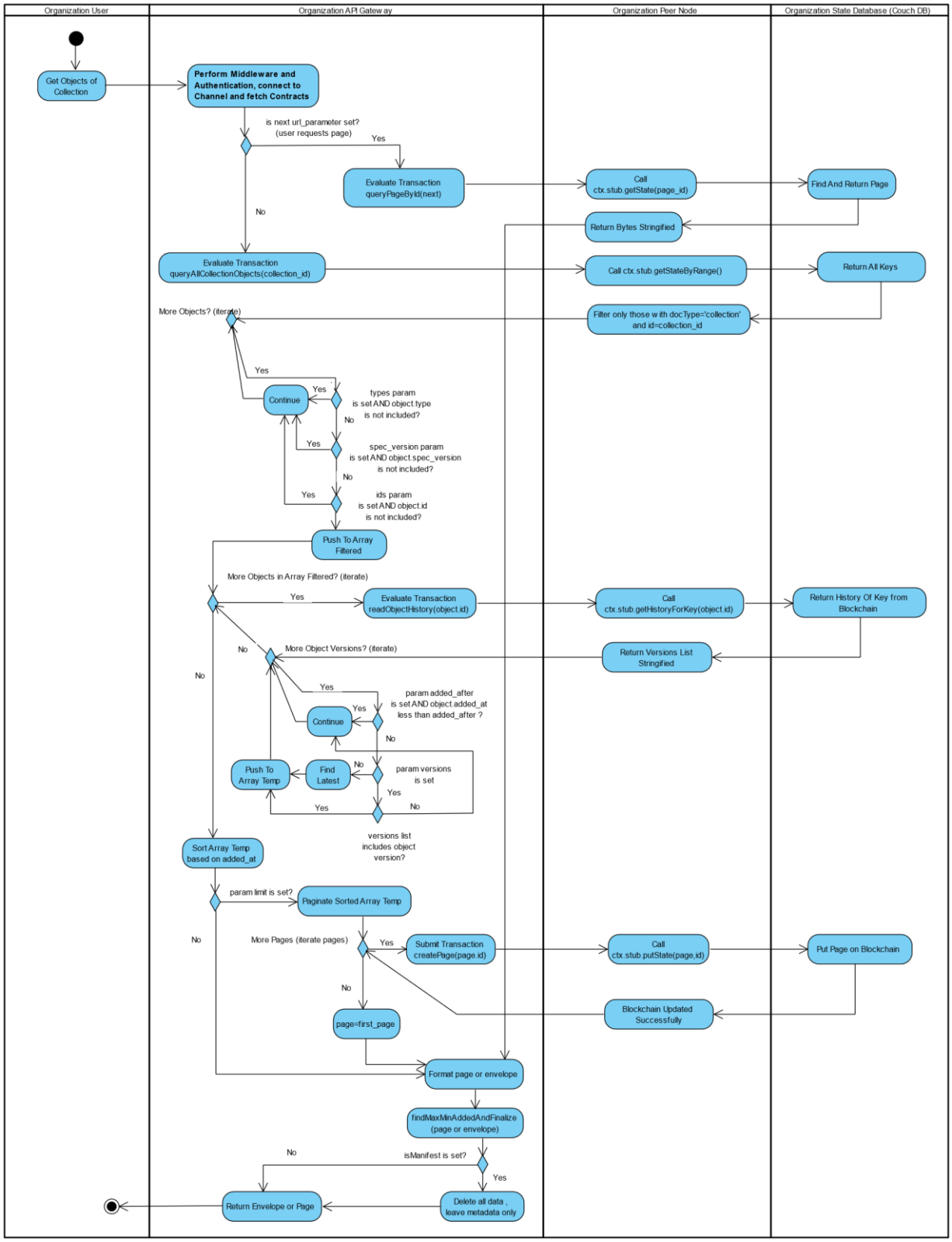
Σχήμα 4.8.2

4.9 Περίπτωση χρήσης GET Objects

4.9.1. Σύντομη περιγραφή

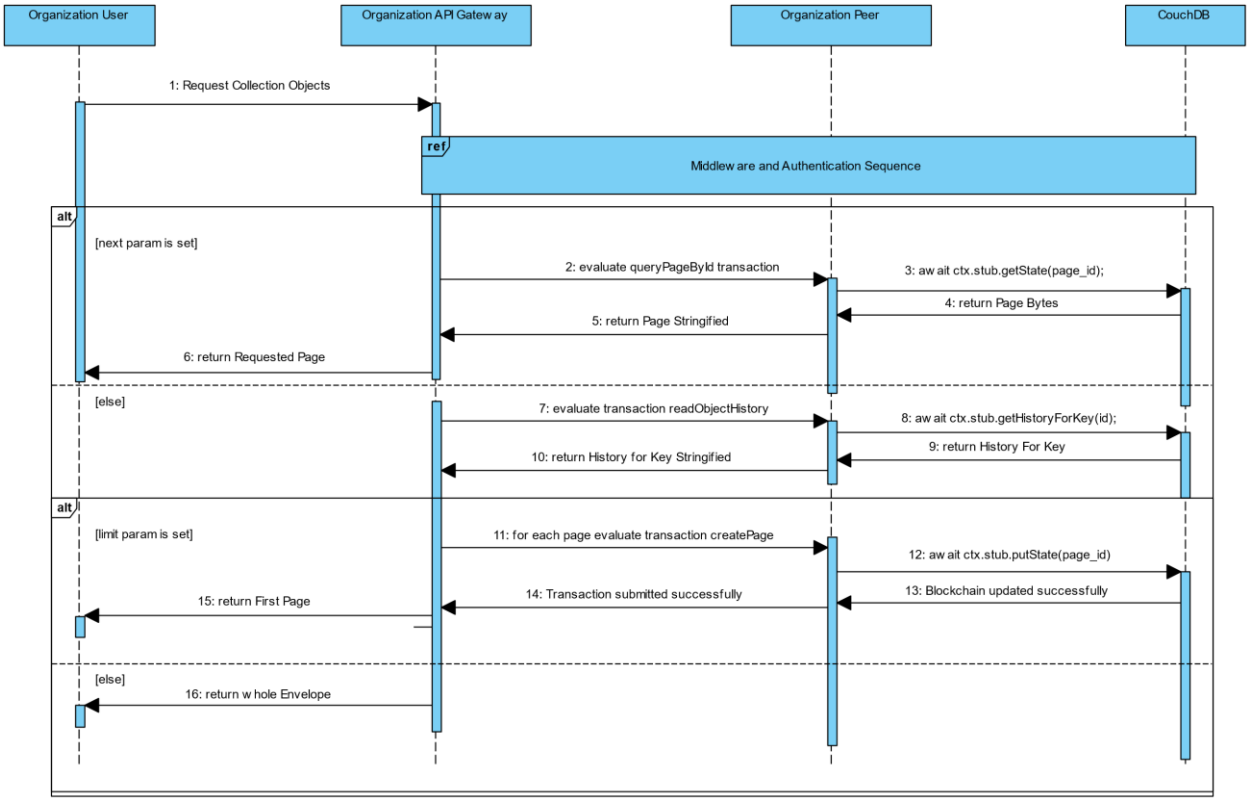
Η λειτουργία αυτή εξυπηρετεί την προβολή των αντικειμένων που βρίσκονται σε ένα TAXII Collection και αποτελεί τον πυρήνα της εργασίας [12]. Τα αντικείμενα ανακτώνται από το Hyperledger Fabric δίκτυο με κλήση των αντίστοιχων Transactions με διαφορετικούς τρόπους ανάλογα με τις παραμέτρους εισόδου που δίνει ο χρήστης. Σε υψηλό επίπεδο ο χρήστης μπορεί να περάσει από φίλτρα διαφόρων τύπων τα αντικείμενα για να λάβει μόνο το σχετικό περιεχόμενο και μπορεί να σελιδοποιήσει τη λίστα με τα αντικείμενα για λόγους παρουσίασης. Στο πλαίσιο της εργασίας δεν αναπύχθηκε πλήρως η ανάκτηση αντικειμένων από Private Data Collections καθώς δεν υποστηρίζονται ακόμα πολλές λειτουργίες από πλευράς Hyperledger Fabric. Ο χρήστης δίνει παραμέτρους φίλτρων οι οποίες καθορίζουν ποιά από τα αντικείμενα θα περάσουν εν τέλει στη λίστα, για παράδειγμα αποκλειστικά αντικείμενα με type: malware ή indicator of compromise η αντικείμενα που προστέθηκαν στο blockchain μετά τις 2022-01-01:00:00:00 στο Blockchain ή αντικείμενα με TAXII spec_version=2.1. Σε περίπτωση που ο χρήστης δώσει την παράμετρο next τότε επιστρέφεται από το Blockchain η συγκεκριμένη σελίδα η οποία αναζητά ο χρήστης σε άλλη περίπτωση εάν έχει τεθεί η παράμετρος limit λαμβάνεται η σελιδοποιημένη κατα limit εκδοχή της λίστας αντικειμένων με ένα δείκτη στην επόμενη σελίδα αφού πρώτα έχουν δημιουργηθεί και αποθηκευτεί όλες οι σελίδες στο Blockchain. Σε περίπτωση που δεν έχει τεθεί η παράμετρος limit επιστρέφονται όλα τα αντικείμενα σε μία λίστα. Σε κάθε περίπτωση τα response headers X-TAXII-Date-Added-First και X-TAXII-Date-Added-Last ρυθμίζονται να δείχνουν την ημερομηνία προσθήκης του παλαιότερου και του νεότερου αντικειμένου που βρίσκεται στη συγκεκριμένη λίστα η σελίδα. Τέλος εάν έχει τεθεί η παράμετρος is_manifest τότε το Endpoint αυτό λειτουργεί σύμφωνα με την περίπτωση χρήσης GET Manifest που θα αναφερθεί αργότερα.

4.9.2. Activity Diagram



Σχήμα 4.9.1

4.9.3 Sequence Diagram



Σχήμα 4.9,2

4.10 Περίπτωση χρήσης GET Object

4.10.1. Σύντομη περιγραφή

Η λειτουργία αυτή είναι στην πραγματικότητα η GET Objects δηλαδή η περίπτωση χρήσης 4.9 για match[id]=object_id [12] . Εφόσον σχεδιάστηκε και επαληθεύτηκε η ορθή λειτουργία του φίλτρου match[id] από την περίπτωση χρήσης 4.9 τότε το μόνο που πρέπει να γίνει από πλευράς κώδικα είναι η παρεμβολή ενός middleware επιπέδου όπου θέτει την παράμερο URL match[id] ίση με το δοθέν object_id σαν να είχε δοθεί από request χρήστη. Τα υπόλοιπα φίλτρα και οι λειτουργίες σελιδοποίησης είναι ακριβώς οι ίδιες.

4.11 Περίπτωση χρήσης GET Manifest

4.11.1. Σύντομη περιγραφή

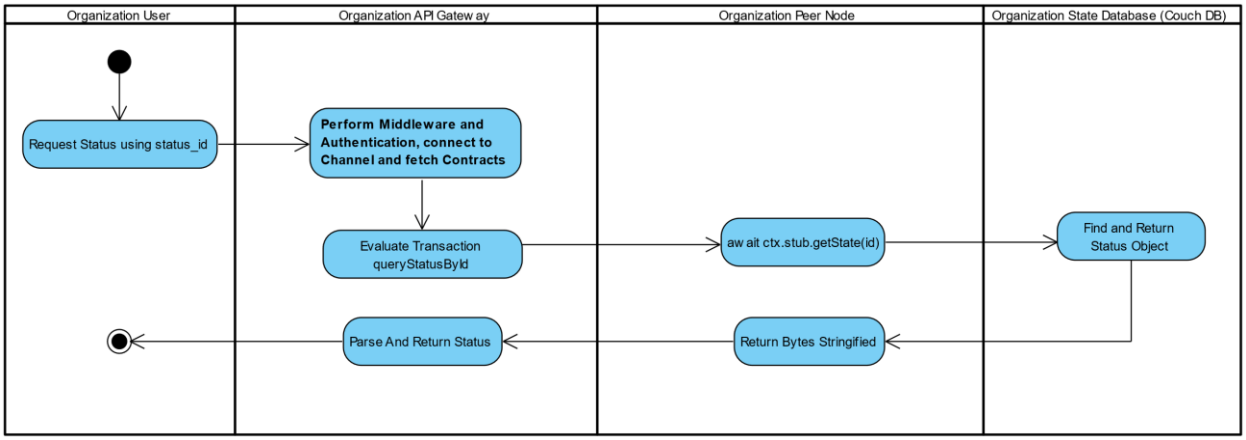
Η λειτουργία αυτή είναι στην πραγματικότητα η GET Objects μόνο που αντί για τα πραγματικά δεδομένα διατηρούνται τα μεταδεδομένα TAXII δηλαδή μόνο τα id, date_added, version και media_type [12] . Η σκοπιμότητα της λειτουργίας είναι η μείωση του όγκου του Request που μεταδίδεται πάνω από το δίκτυο συνήθως όταν αφορά τους χρήστες μόνο κάποια από τα παραπάνω μεταδεδομένα με πίο σύνηθες το date_added το οποίο δεν εμφανίζεται στο κανονικό request στην GET Objects. Ο τρόπος που υλοποιήθηκε η παραπάνω λειτουργία είναι με τη χρήση μίας προδιαγεγραμμένης μεταβλήτής is_manifest η οποία όταν τεθεί αναγνωρίζεται από την GET Objects η οποία διαγράφει τα δεδομένα και κρατάει μόνο τα μεταδεδομένα της λίστας ενώ διατηρεί όλα τα φίλτρα και την σελιδοποίηση που έχει γίνει.

4.12 Περίπτωση χρήσης GET Status

4.12.1. Σύντομη περιγραφή

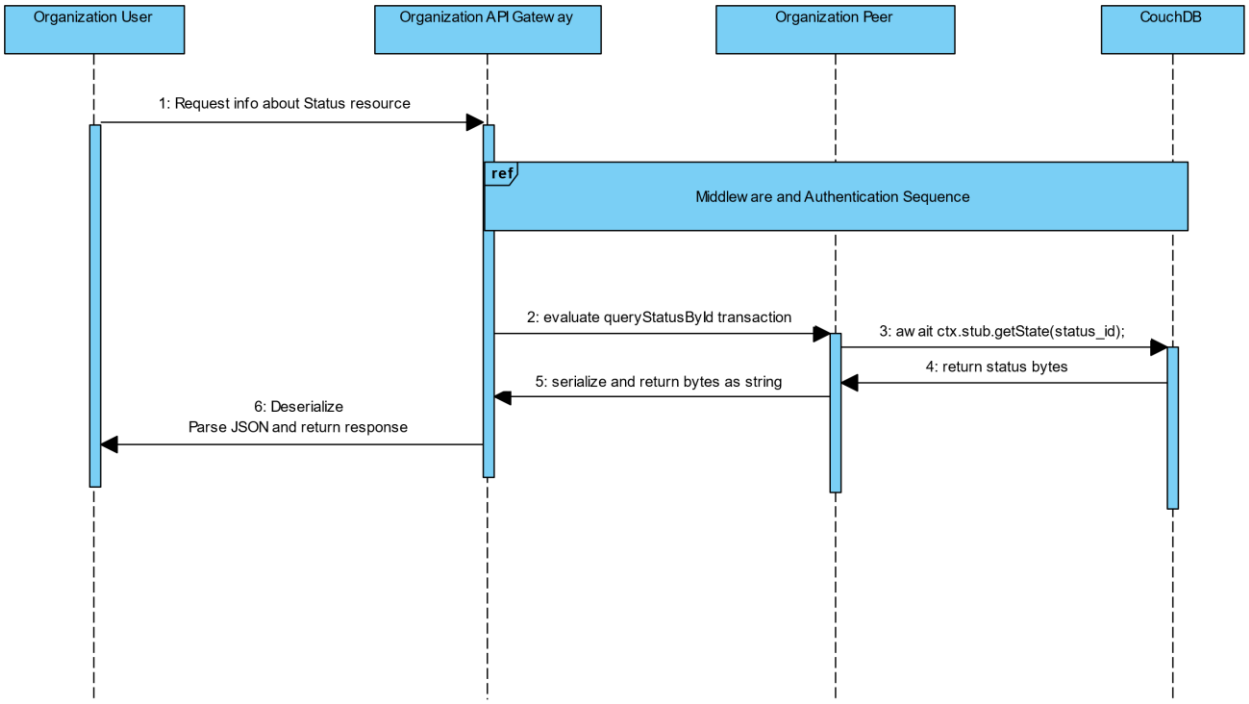
Η λειτουργία αυτή εξυπηρετεί την ασύγχρονη ανάκτηση του status μίας εισαγωγής αντικειμένων (POST Envelope) [12] στο blockchain και επιβάλλεται από το πρότυπο TAXII. Όσον αφορά στο επίπεδο λεπτομέρειας του status resource στο πλαίσιο της εργασίας αναπτύχθηκε η απλή εκδοχή του όπου δείχνει το ποσοστό επιτυχημένων εισαγωγών επί των συνολικών χωρίς περαιτέρω debug logs τα οποία καταγράφονται από τον http server.

4.12.2. Activity Diagram



Σχήμα 4.12.1

4.12.3. Sequence Diagram



Σχήμα 4.12.2

Κεφάλαιο 5 Επίδειξη Εφαρμογής

5.1 Γενικός σχολιασμός

Στο κεφάλαιο αυτό θα παρουσιαστούν περισσότερες λεπτομέρειες για τη διεπαφή χρήστη και την εφαρμογή στην ολότητα της ενώ θα συμπεριληφθούν στιγμιότυπα οθόνης και αλληλουχίες μετάβασης από τη μία διεπαφή στην άλλη. Η διεπαφή χρήστη έχει σχεδιαστεί με ένα σαφή στόχο, να αναδείξει όλες τις περιπτώσεις χρήσης που αναφέρθηκαν στην υποενότητα 4.2 και να καλύψει μερικώς κάποια από τα πιθανά σφάλματα του

5.2 Τεχνολογίες Client Application

Οι τεχνολογίες που αξιοποιήθηκαν για την υλοποίηση του client application έχουν επιλεχθεί με κριτήριο την απλότητα , την πληθώρα τεκμηρίωσης στον παγκόσμιο ιστό και την ασφάλεια.

JavaScript

Η Javascript είναι η γλώσσα προγραμματισμού όλων των web browsers και ο κύριος τρόπος αλληλεπίδρασης μέ τα στοιχεία του Document Object Model η DOM των δικτυακών σελίδων. Είναι ελαφριά, interpreted, μονονηματική, just in time compiled και έχει κυρίως στοιχεία συναρτησιακού προγραμματισμού. Τα τελευταία χρόνια είναι αρκετά δημοφιλή στην κοινότητα του δικτυακού προγραμματισμού τα JavaScript Frameworks παρ όλα στο πλαίσιο της εργασίας λήφθηκε η απόφαση να γραφτεί η εφαρμογή σε απλή JavaScript ενσωματωμένη σε html αρχεία. [14]

Apache HTTP Server

Ο HTTP Server του Apache project είναι μία προσπάθεια να αναπτυχθεί και να διατηρηθεί ένας ανοιχτού τύπου HTTP Server για μοντέρνα λειτουργικά συστήματα UNIX και Windows. Η πρώτη έκδοση του ξεκίνησε το 1995 από το Apache Software Foundation και από τότε είναι ο δημοφιλέστερος εξυπηρετητής HTTP. Στο πλαίσιο της εργασίας δεν έγινε κάποια επιπλέον παραμετροποίηση του Apache σε επίπεδο λειτουργικού συστήματος χρησιμοποιήθηκε για τον βασικότερο σκοπό του την εξυπηρέτηση σελίδων html. [15]

jQuery

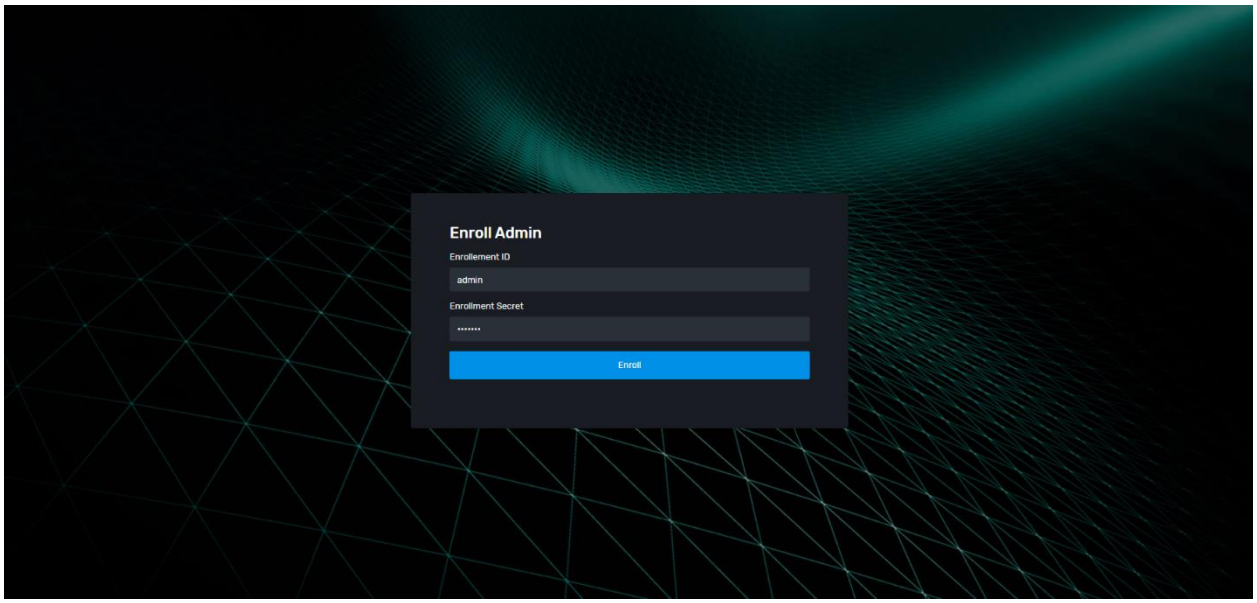
Το jQuery είναι μια γρήγορη και πλούσια σε χαρακτηριστικά βιβλιοθήκη JavaScript. Κάνει πράγματα όπως η διέλευση και ο χειρισμός εγγράφων HTML, ο χειρισμός συμβάντων, animation και το AJAX πολύ πιο απλά με ένα εύχρηστο API που λειτουργεί στους περισσότερους δημοφιλείς περιηγητές. Ο λόγος που χρησιμοποιήθηκε το jQuery είναι η απλότητα του σε σχέση με τα built-ins της JavaScript για τις ίδιες διαδικασίες.[16]

OASIS STIX Visualizer

Το STIX Visualizer προορίζεται να παρέχει στους παραγωγούς και τους καταναλωτές περιεχομένου STIX έναν γρήγορο τρόπο οπτικοποίησης των αντικειμένων σε ένα αρχείο STIX JSON και των σχέσεων μεταξύ αυτών των αντικειμένων. Η οπτικοποίηση υλοποιείται σε HTML, CSS και JavaScript (χρησιμοποιώντας τη βιβλιοθήκη D3.js) και είναι κατάλληλη για αυτόνομη χρήση. Η επεξεργασία του STIX περιεχομένου γίνεται αυστηρά μέσα στο πρόγραμμα περιήγησης στο οποίο εκτελείται ο κώδικας, επομένως είναι κατάλληλο για δεδομένα που ο χρήστης δεν επιθυμεί να κοινοποιήσει.[13]

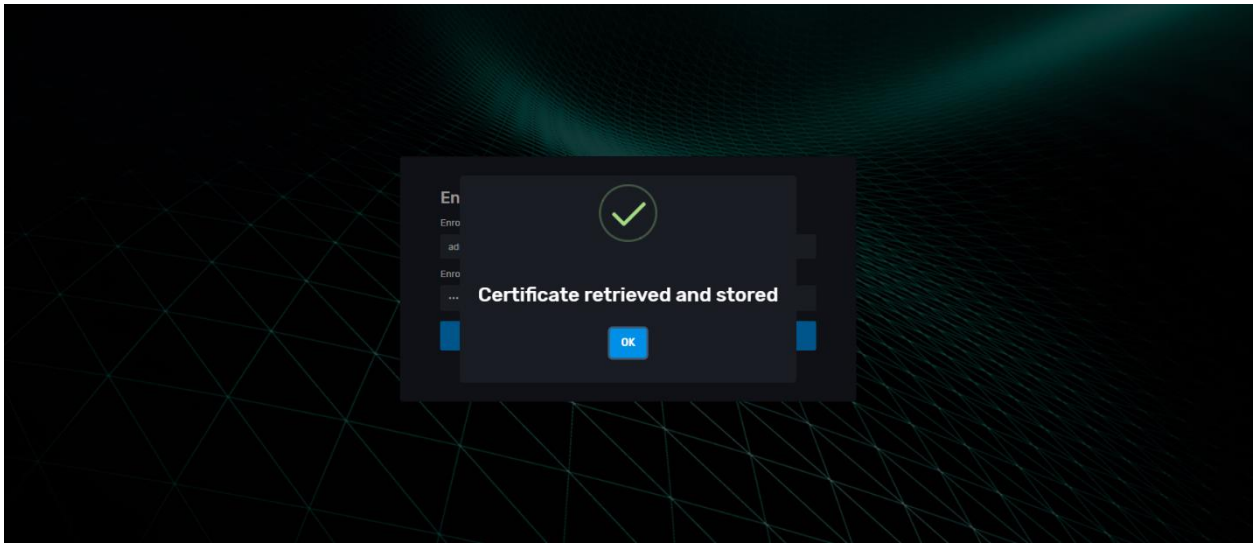
5.3 Enroll Admin

Η διεπαφή αυτή εμφανίζεται όταν ένας διαχειριστής θέλει να εκδόσει το πρωταρχικό πιστοποιητικό για τον εαυτό του ώστε κατόπιν να μπορεί να γράφει χρήστες του οργανισμού στη βάση της αρχής πιστοποίησης και γενικότερα να εκτελεί διαχειριστικές λειτουργίες.



Σχήμα 5.3.1

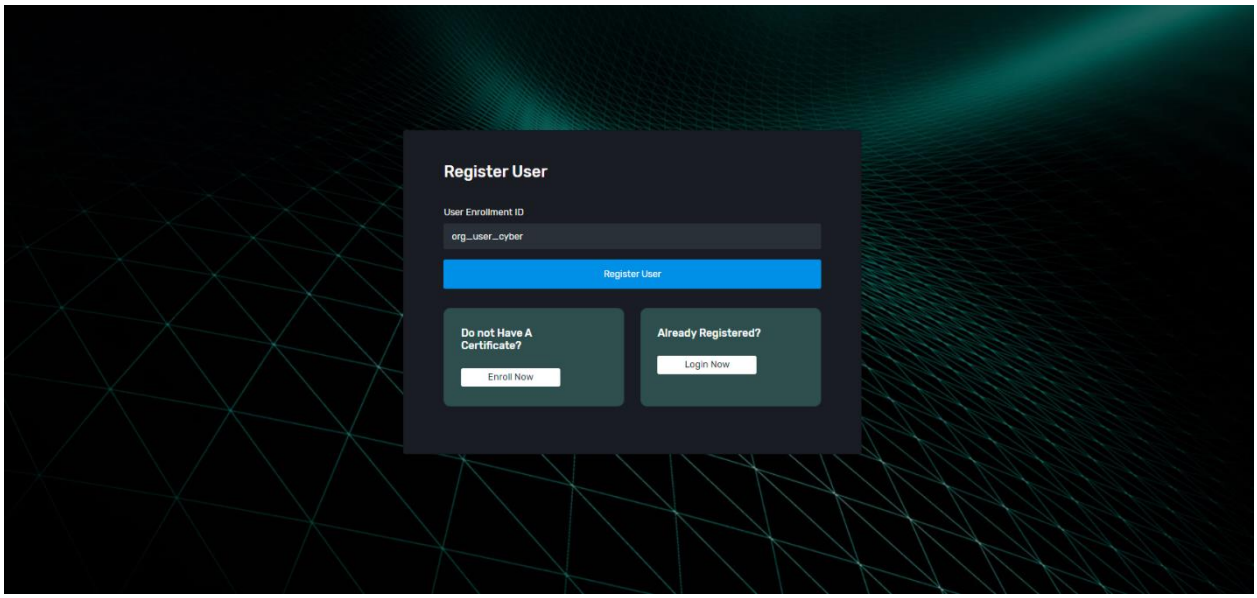
Όταν συμπληρωθούν τα στοιχεία και αποσταλεί το αίτημα εάν είναι επιτυχημένο λαμβάνεται το παρακάτω μήνυμα:



Σχήμα 5.3.2

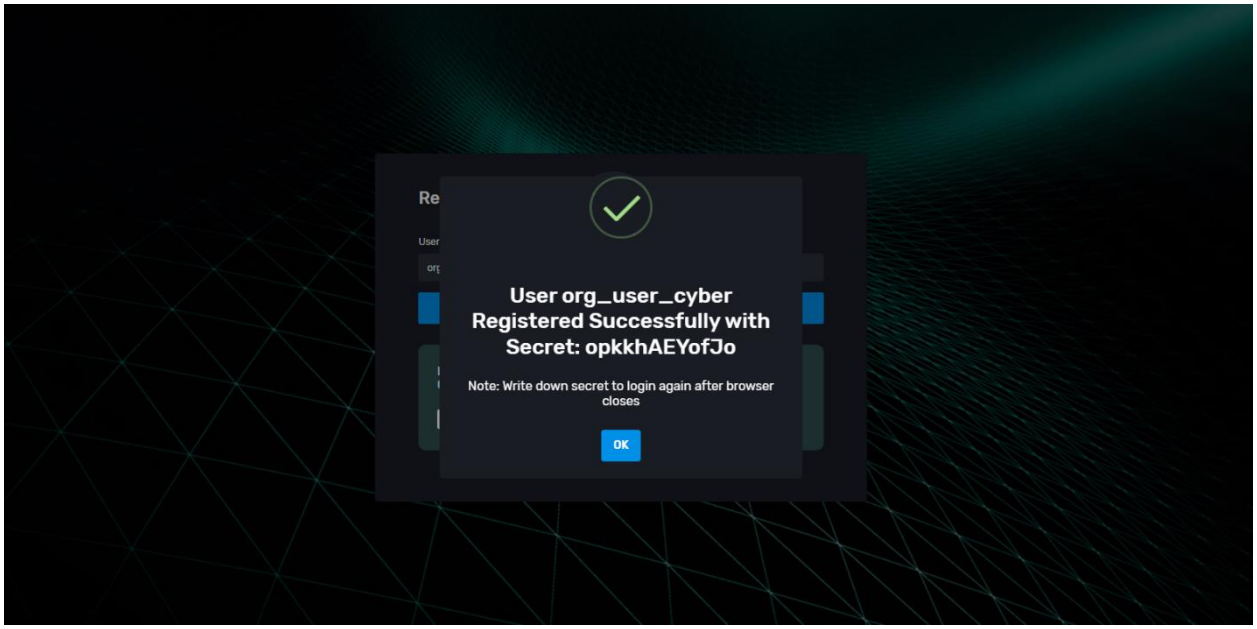
5.4 Register User

Η διεπαφή αυτή εμφανίζεται όταν ο χρήστης προσπαθεί να αποκτήσει πρόσβαση σε οποιαδήποτε σελίδα χωρίς να είναι πρώτα αυθεντικοποιημένος. Η οθόνη αυτή επιτρέπει στο διαχειριστή να κάνει εγγραφή ενός χρήστη. Σε περίπτωση που δεν έχει αποκτήσει ο διαχειριστής το δικό του πιστοποιητικό για να προβεί στην κλήση της register πρέπει να μεταβεί στην διεπαφή Enroll Admin εάν ο χρήστης έχει γίνει ήδη register τότε πρέπει να μεταβεί στην διεπαφή Login User.



Σχήμα 5.4.1

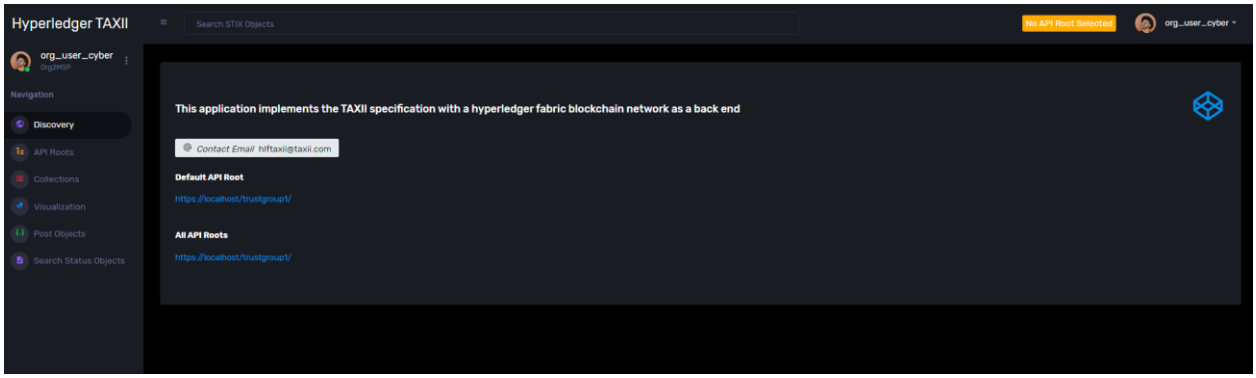
Όταν συμπληρωθεί το όνομα του χρήστη , εάν ο διαχειριστής έχει λάβει πιστοποιητικό και είναι αποθηκευμένο στο browser και το όνομα δεν έχει χρησιμοποιηθεί ήδη λαμβάνεται το παρακάτω μήνυμα



Σχήμα 5.4.2

5.5 Discovery

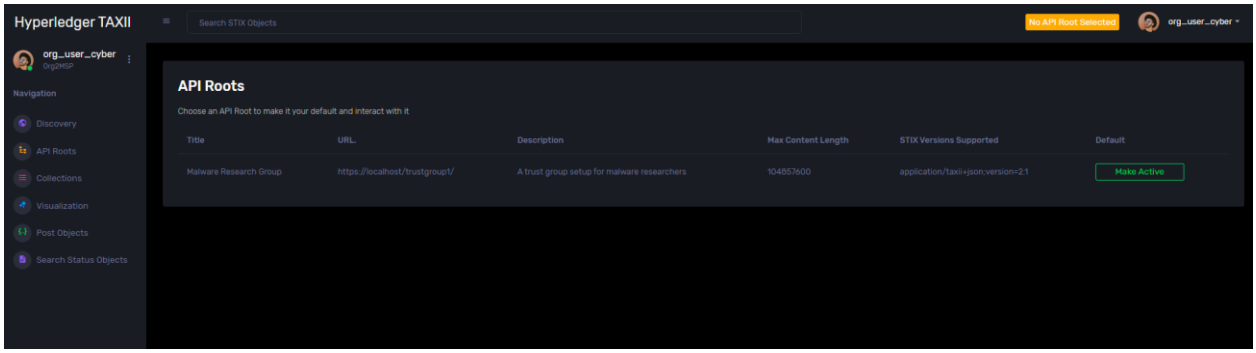
Η επιτυχής εγγραφή του χρήστη τον συνδέει αυτόματα με τον κωδικό που έλαβε στην παραπάνω διεπαφή και τον παραπέμπει στην αρχική οθόνη δηλαδή τη διεπαφή Discovery. Εδώ καλείται το αντίστοιχο TAXII REST API Discovery και τα αποτελέσματα εμφανίζονται στην οθόνη. Σημαντική λεπτομέρεια εδώ είναι ότι επειδή δεν έχει γίνει ενεργή κάποια από τις API Roots στο πάνω δεξιά μέρος της οθόνης φαίνεται με κίτρινα γράμματα υποδεικνύοντας warning το γεγονός αυτό



Σχήμα 5.5.1

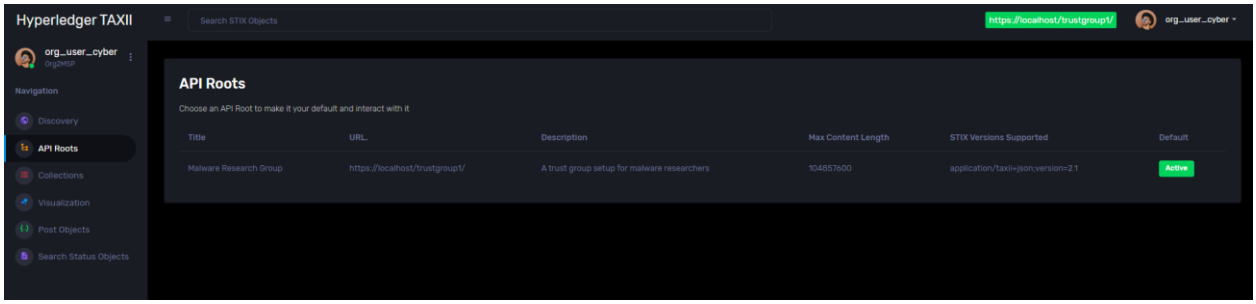
5.6 API Roots

Η διεπαφή αυτή χρησιμεύει για να γίνει ενεργό ένα API Root και να χρησιμοποιείται για να καλούνται τα επόμενα REST API. Στην οθόνη απαριθμούνται τα API Roots με κλήση του αντίστοιχου API για κάθε αναγνωριστικό που υπάρχει στη λίστα API roots του discovery resource. Επίσης ελέγχεται ποιό έχει επιλέξει ο χρήστης να είναι το ενεργό ελέγχοντας το local storage του browser.



Σχήμα 5.6.1

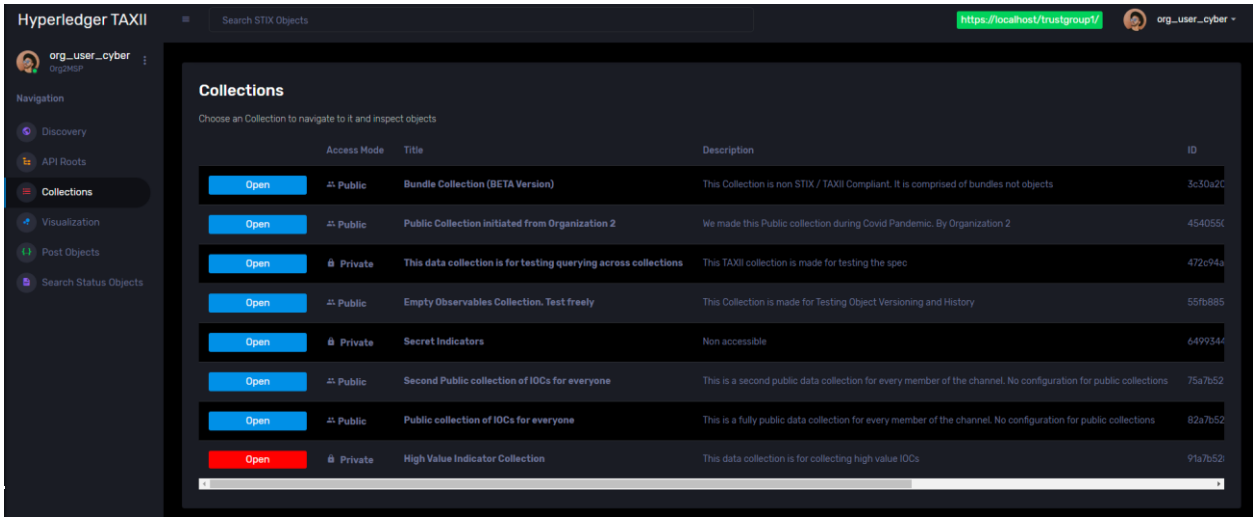
Η επιλογή Make Active για κάποιο api root που απαριθμείται στην διεπαφή αλλάζει το warning μήνυμα στην πανω δεξιά πλευρά σε success και ενεργοποιεί το column default για το api root που επιλέχθηκε.



Σχήμα 5.6.2

5.7 Collections

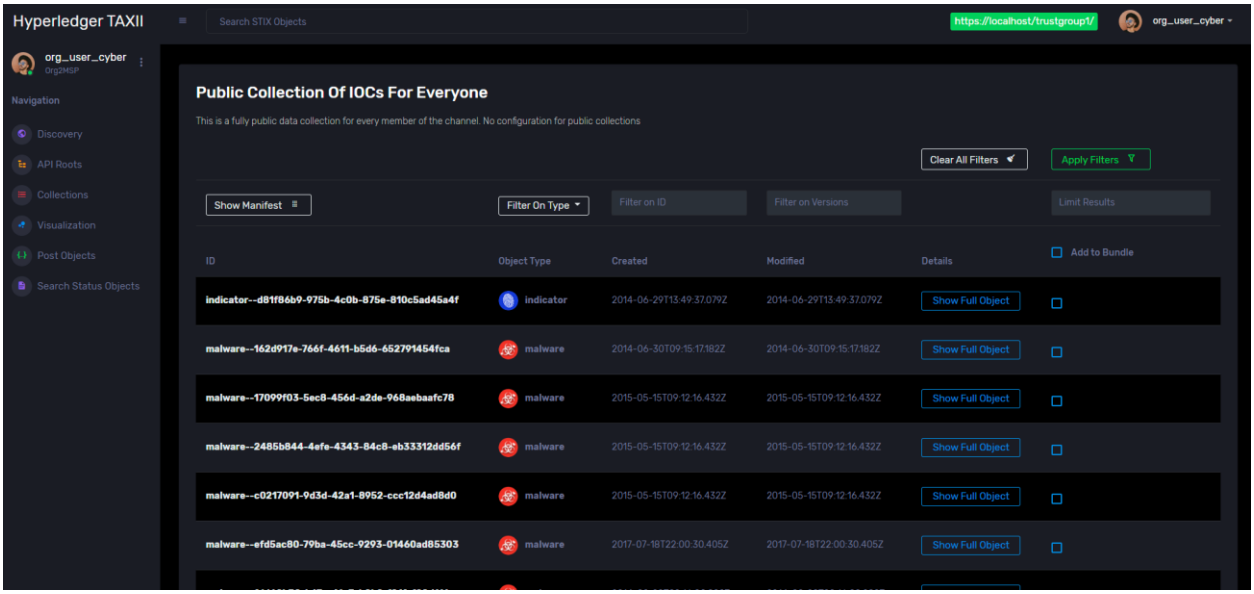
Η ενεργοποίηση ενός api root επιτρέπει την κλήση των επόμενων REST API με url path παράμετρο api root την παραπάνω. Η πρώτη διεπαφή που έχει νόημα να διερευνηθεί είναι η Collections η οποία απαριθμεί τις συλλογές TAXII δείχνοντας το αν είναι public ή private και εάν ο χρήστης έχει δικαιώματα πρόσβασης στη συλλογή



Σχήμα 5.7.1

5.8 Collection

Η επιλογή open για κάποιο από τα παραπάνω collection οδηγεί στη σημαντικότερη διεπαφή της εφαρμογής την Collection, η οποία καλεί την GET Objects εφαρμόζοντας τα κατάλληλα φίλτρα. Η περίπτωση χρήσης GET Manifest έχει επίσης ενσωματωθεί σε αυτή τη σελίδα με τη μορφή έπεκτασης των αντικειμένων με μία column που περιέχει το μεταδεδομένο που αφορά την χρονοσφραγίδα εισαγωγής.

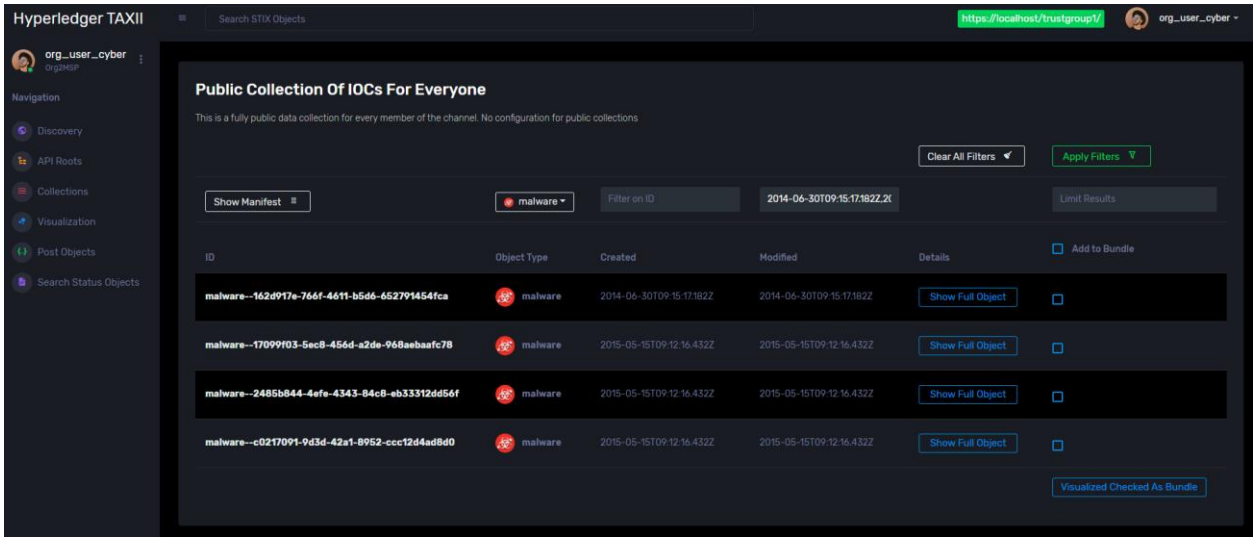


Σχήμα 5.8.1

Οι δυνατές λειτουργίες από τη διεπαφή αυτή είναι οι εξής:

5.8.1 Εισαγωγή φίλτρων και επιλογή Apply Filters

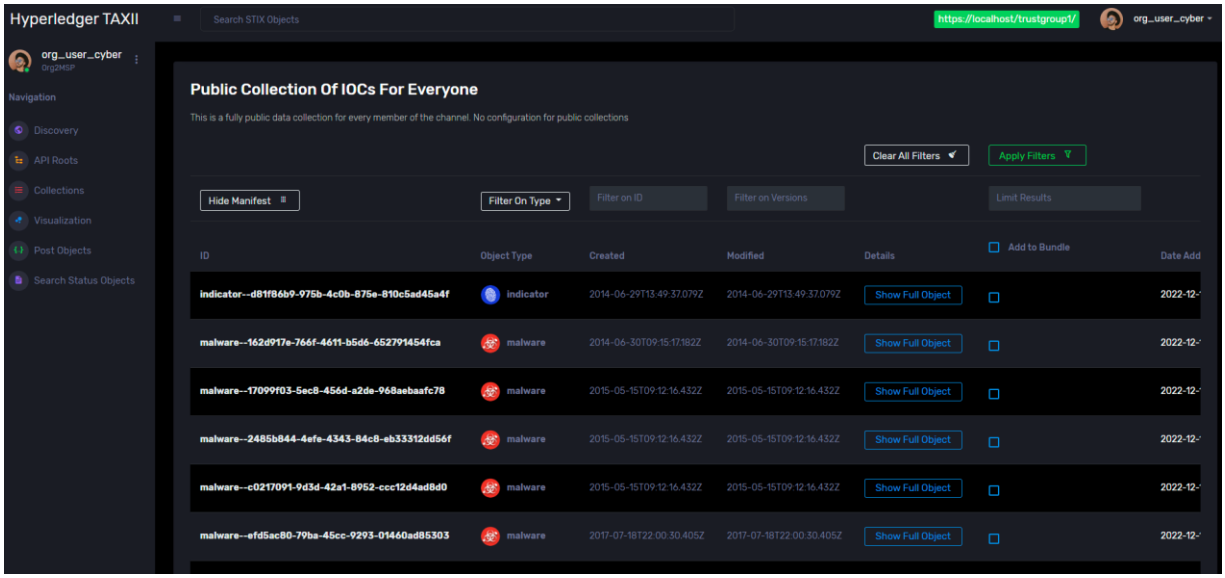
Η λειτουργία αυτή καθαρίζει τον πίνακα, εισάγει φίλτρα στο url , καλεί το αντίστοιχο API και ξαναγεμίζει τον πίνακα με δεδομένα



Σχήμα 5.8.1

5.8.2 Επιλογή Show Manifest

Η λειτουργία αυτή δείχνει το μεταδεδομένο της χρονοσφραγίδας εισαγωγής στην αντίστοιχη column Date Added



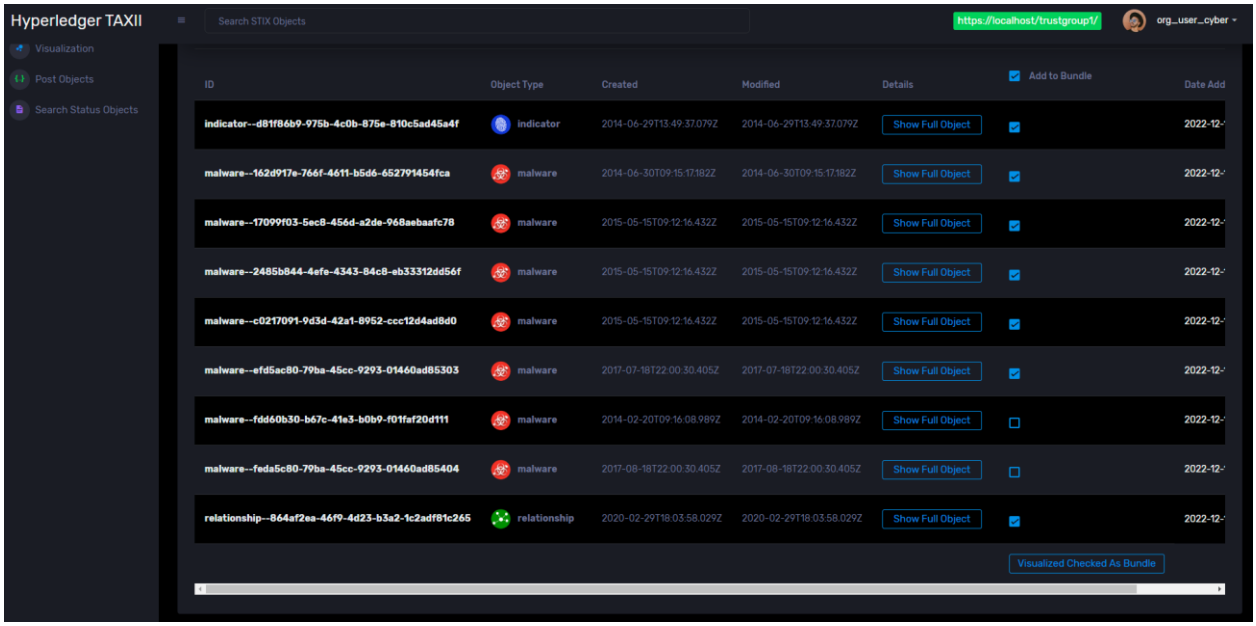
Σχήμα 5.8.2

5.8.3 Επιλογή Show Full Object

Η λειτουργία αυτή αφορά τη διεπαφή 5.9 όπου φαίνεται η πλήρης αποτύπωση του αντικειμένου STIX με τη εμφωλιασμένη δομή του και τις εκδοχές του ανά το χρόνο.

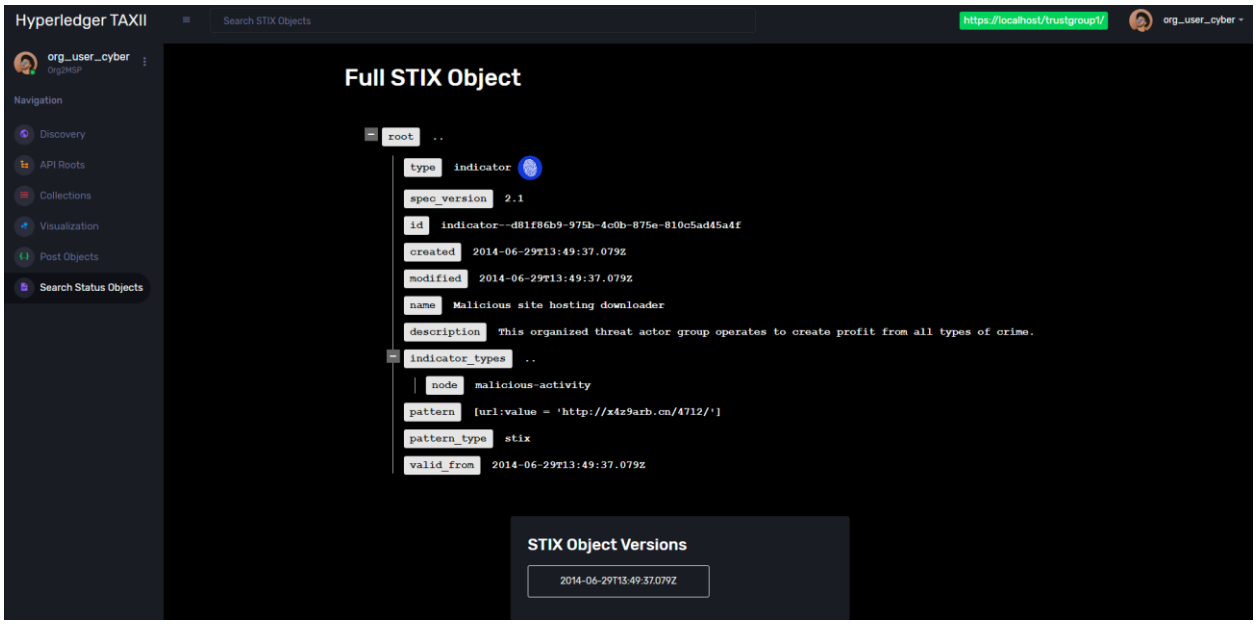
5.8.4 Ομαδοποίηση ορισμένων η όλων των αντικειμένων και επιλογή οπτικοποίησης

Η λειτουργία αυτή ομαδοποιεί τα αντικείμενα σε ένα envelope και τα δίνει σαν είσοδο στον οπτικοποιητή STIX. Στον οπτικοποιητή μπορεί να γίνει μετάβαση και από το sidebar με την επιλογή visualization και τη χειροκίνητη εισαγωγή STIX envelopes σε μορφή JSON για οπτικοποίηση.



Σχήμα 5.8.3

5.9 Object

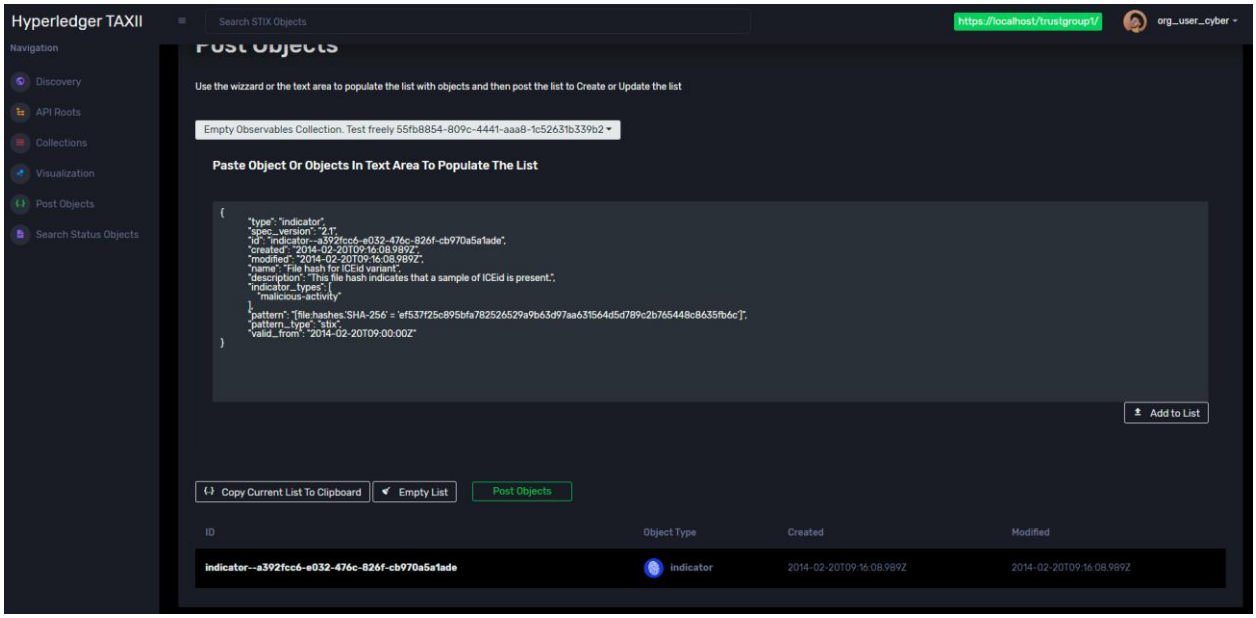


Σχήμα 5.9.1

Η διεπαφή αυτή υπάρχει για περαιτέρω ανάλυση πάνω στο αντικείμενο STIX και καλεί τα REST API GET Object και GET Object Versions. Στη διεπαφή μπορούμε να δούμε τα διάφορα επίπεδα του αντικειμένου σε εμφωλιασμένη μορφή και να επιλέξουμε άλλα versions του ίδιου αντικειμένου για να δούμε το πως άλλαξαν στο χρόνο.

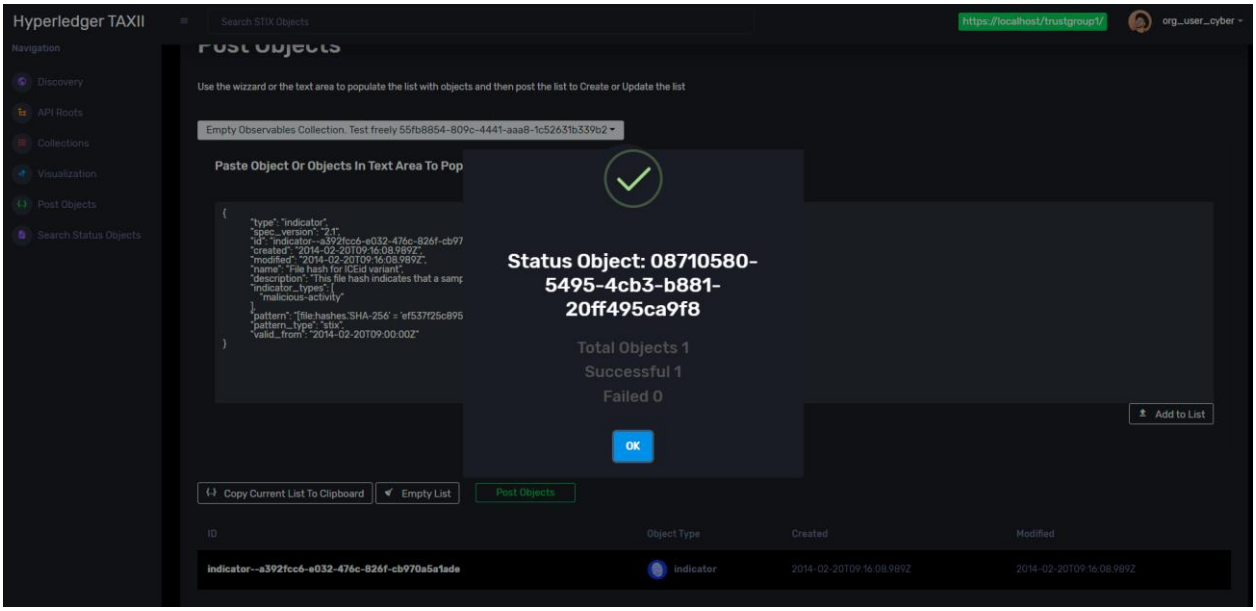
5.10 Post Objects

Η διεπαφή χρησιμοποιείται για την εισαγωγή αντικειμένων σε μία συλλογή TAXII μέσω της κλήσης του API, POST Envelope. Η λογική σε αυτή τη διεπαφή είναι η συσσώρευση των αντικειμένων σε μία προσωρινή λίστα είτε ως envelope είτε ένα ένα και η περαιτέρω αποστολή του αιτήματος με το κουμπί Post Objects



Σχήμα 5.10.1

Στην παραπάνω προσωρινή λίστα έχει προστεθεί ο indicator που φαίνεται μέσω του text area και πρόκειται να αποσταλεί στον TAXII Server. Μετά την επιτυχημένη καταχώρηση του αντικειμένου στο blockchain , στη συγκεκριμένη συλλογή που έχει επιλεχθεί λαμβάνεται η παρακάτω ειδοποίηση:



Σχήμα 5.8.1

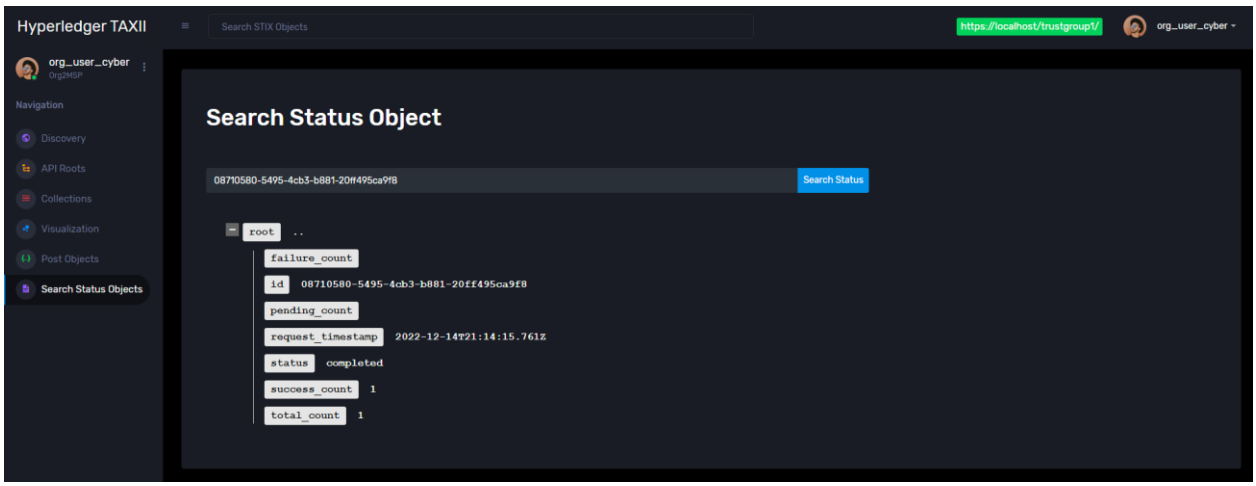
Στην πραγματικότητα επιστρέφεται το status object το οποίο δημιουργείται πρωτού γίνει η πραγματική εισαγωγή στο blockchain. Το αποτέλεσμα εδώ είναι ποσοστό επιτυχίας 100%.

5.11 Search Status Object

Η διεπαφή αυτή είναι αρκετά απλή καθώς χρησιμοποιείται μόνο για να κάνει αναζήτηση σε ένα συγκεκριμένο status_id.

Σχήμα 5.11.1

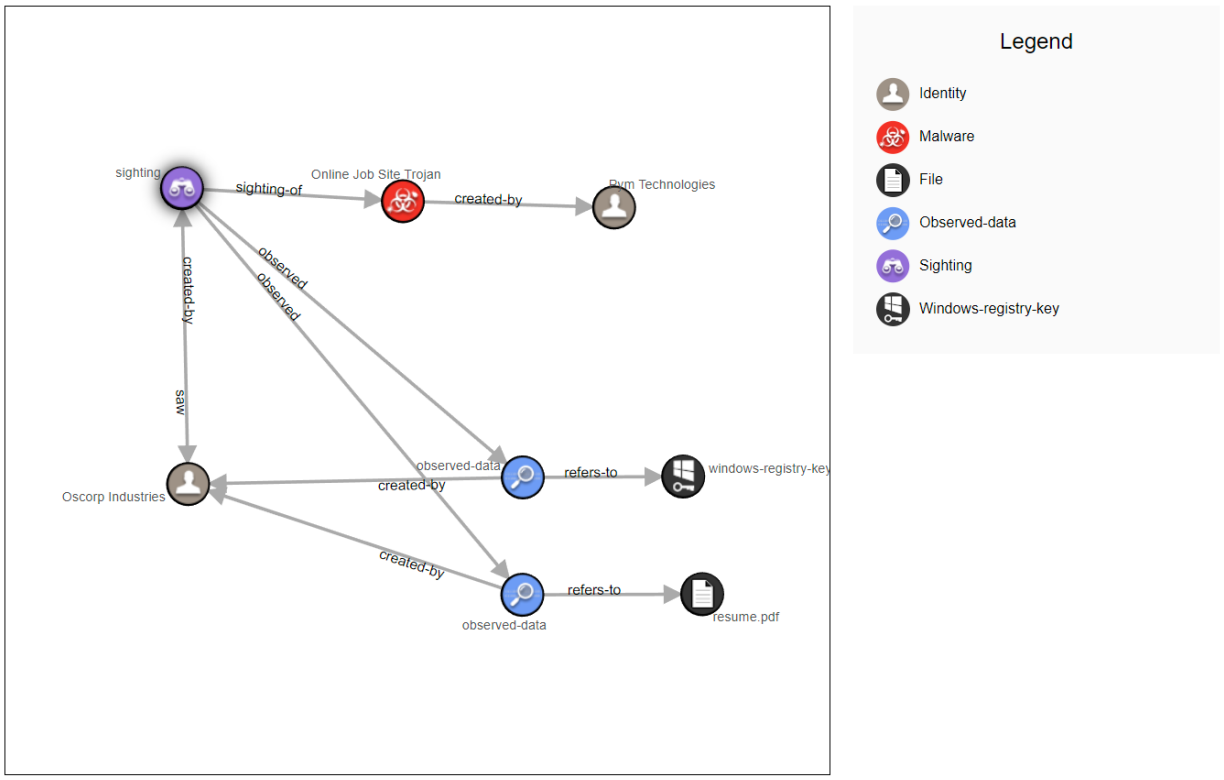
Μετά την επιτυχή αναζήτηση λαμβάνεται το παρακάτω μήνυμα:



Σχήμα 5.11.2

5.12 Visualization

Η διεπαφή αυτή αποτελεί έργο του οργανισμού OASIS. Έχει ενσωματωθεί στην εφαρμογή και έχει επεξεργαστεί αρκετά ώστε να μπορεί να λάβει ένα objects envelope από τις υπόλοιπες σελίδες και να το οπτικοποιήσει. Η μετάβαση μπορεί να γίνει είτε με ομαδοποίηση αντικειμένων εντός του collection (τρόπος 6.8.4) είτε από το sidebar.



Σχήμα 5.12.1

Κεφάλαιο 6 Επίλογος

6.1 Δυσκολίες στο σχεδιασμό

Η μεταφορά ενός client server συστήματος σε μία πλήρως αποκεντρωμένη αρχιτεκτονική παρουσιάσε δυσκολίες οι οποίες έπρεπε να είτε να αντιμετωπιστούν με κάποια ειδική λύση είτε να καταγραφεί η δυσκολία και να τεκμηριωθεί θεωρητικά η επίλυση της. Στο κεφάλαιο αυτό θα δούμε τις δυσκολίες που παρουσιάστηκαν στο σχεδιασμό του συστήματος.

Η στρατηγική τοποθέτηση του κώδικα του TAXII Server και η επιλογή χρήσης API Gateway.

Ένα πρόβλημα το οποίο αντιμετωπίζει ένας συντάκτης εφαρμογής σε blockchain πλατφόρμα είτε ιδιωτική είτε δημόσια είναι ότι η σχεδίαση οποιασδήποτε εφαρμογής συνθετότερης από την κλήση μίας συνάρτησης απαιτεί πολλαπλές αλληλεπιδράσεις με το blockchain σύστημα και κλήση πολλαπλών transactions για μία λογική διαδικασία υψηλού επιπέδου. Οι επιλογές που έχει ένας σχεδιαστής του συστήματος είναι οι εξής:

> **Συγγραφή μεγάλων και ατομικών συναλλαγών αντί για περισσότερες και μικρότερες σε έκταση συναλλαγές.** Η επιλογή αυτή δεν έχει κάτι εν γένει λάθος και είναι ο αυστηρότερος και ορθότερος τρόπος να εγγυηθούμε την απόλυτη ασφάλεια στην αλληλουχία εκτέλεσης των συναλλαγών και την ατομικότητα σε επίπεδο λογικής διαδικασίας. Στην πράξη παρ όλα αυτά υπάρχουν πολλά tradeoffs στη στρατηγική αυτή. Τα σημαντικότερα είναι η επεκτασιμότητα στην ταχύτητα εκτέλεσης , η εμφάνιση δυσεύρετων bugs που αφορούν τη συναίνεση (consensus) σε τυχαίους αριθμούς και η βραδία ανάπτυξη του λογισμικού λόγω της δυσκολίας της διαδικασίας packaging και deployment blockchain κώδικα ακόμα και σε test περιβάλλοντα.

Συγγραφή μικρότερων σε έκταση συνναλαγών με την εξασφάλιση της σωστής ακολουθίας κλήσεων να γίνεται από τον κώδικα του Client. Ο τρόπος αυτός είναι το standard συγγραφής εφαρμογών που τρέχουν σε δημόσιο αλλά και ιδιωτικό blockchain. Ο τρόπος αυτός εξασφαλίζει ανθεκτικό κώδικα σε επίπεδο blockchain και η ορθότητα των συναλλαγών μπορεί να επαληθευτεί ευκολότερα ενώ ο σχεδιαστής μπορεί να μεταφέρει σταδιακά τον κώδικα στο blockchain. Το κυριότερο πρόβλημα που παρουσιάζει αυτή η επιλογή είναι εξασφάλιση της ατομικότητας στη λογική διαδικασία και τα ανεπιθύμητα αποτελέσματα από την εκτέλεση των συναλλαγών με αυθαίρετη σειρά είτε από κακόβουλους χρήστες είτε από σφάλμα. Το γεγονός ότι οι συναλλαγές βρίσκονται στην πλευρά του πελάτη αυτόματα σημαίνει ότι δεν μπορεί να εξασφαλιστεί η επιθυμητή αλληλουχία εκτέλεσης.

Συγγραφή μικρότερων σε έκταση συνναλαγών με την εξασφάλιση της σωστής ακολουθίας κλήσεων να γίνεται από τον κώδικα ενός Server. Ο τρόπος αυτός είναι μία επιλογή η οποία είναι εφικτή μόνο σε υποδομή ιδιωτικού blockchain καθώς απαιτεί κάποια κεντρική αρχή , τον server ο οποίος πρέπει να ανήκει στον αντίστοιχο οργανισμό. Στο δημόσιο blockchain η σχεδιαστική αυτή αρχή παραβιάζει το αποκεντρωμένο του blockchain παρ όλα αυτά στο ιδιωτικό blockchain που έχουμε αποκέντρωση μεταξύ οργανισμών είναι κάτι το οποίο μπορεί να υποστηριχθεί με τον ίδιο τρόπο που κάθε οργανισμός μπορεί να έχει δική του αρχή πιστοποίσης (CA). Το κυριότερο πλεονέκτημα αυτού το τρόπου είναι ότι αποκρύπτει την υποδομή blockchain από τους αντίστοιχους clients και εκθέτει αποκλειστικά ένα REST API Endpoint. Αυτό σημαίνει ότι με τη χρήση κάποιου host firewall μπορούμε να αφήσουμε τη διέλευση κίνησης προς την υποδομή Blockchain μόνο από τον Server αυτό και να προστατέψουμε έτσι την πολυμερή υποδομή από εξωτερικές επιθέσεις. Το μειονέκτημα αυτής της προσέγγισης είναι ότι οι διαχειριστές του Server που φιλοξενεί των κώδικα μπορούν να αποτελέσουν απειλή καθώς μπορούν να αλλάξουν τους κανόνες του host firewall και να επιτρέψουν κίνηση από αυθαίρετους hosts καθώς και να καλέσουν τα transactions με ανεπιθύμητη σειρά επί του Server για να επηρεάσουν την εφαρμογή. Συνεπώς σε κάθε περίπτωση επιθυμητό είναι οι συναλλαγές να

σχεδιάζονται με τέτοιο τρόπο που να μην επιτρέπουν λογικές επιθέσεις ακόμα και από τους διαχειριστές της υποδομής blockchain.

Η συμφωνία των peer nodes σε τυχαίους αριθμούς.

Η κλήση ενός blockchain transaction πρέπει να οδηγεί σε ένα ντετερμινιστικό αποτέλεσμα καθώς σε άλλη περίπτωση πρώτον το σύστημα δεν είναι συνεπές μεταξύ οργανισμών και δεύτερον δεν μπορεί να γίνει διάκριση του κάτα πόσον κάποιος κόμβος αποκλίνει προς συμφέρον του και δεν εκτελεί τον επιθυμητό κώδικα. Η παραγωγή τυχαίων αριθμών στην πλευρά του peer node και η αλλαγή της ροής εκτέλεσης βάσει αυτών ή η καταχώρηση των τυχαίων δεδομένων στο blockchain οδηγεί με βεβαιότητα σε αδυναμία consensus. Οι επιλογές για τη λύση αυτής της ιδιαιτερότητας είναι οι εξής

Χρήση τρίτου έξυπνου συμβολαίου. Η επιλογής αυτή είναι ο ορθότερος τρόπος να εξασφαλίσουμε τυχαιότητα και consensus σε ένα dApp παρ όλα αυτά σε περίπτωση που θέλουμε να δημιουργήσουμε έναν τυχαίο αριθμό για αναγνωριστικό κάποιου αντικειμένου ο τρόπος αυτός απαιτεί σύνθετο σχεδιασμό και είναι περιττός. [17]

Παραγωγή τυχαίου αριθμού στην πλευρά του Client. Στην επιλογή αυτή παράγουμε έναν αρθμό στον client και αργότερα δημιουργούμε ένα transaction για την καταχώρηση του αποτελέσματος στο Blockchain. Ο τρόπος αυτός δεν μπορεί να χρησιμοποιηθεί στην περίπτωση που υλοποιείται κάποιος αλγόριθμος όπου η εμπιστοσύνη για την παραγωγή του αριθμού σε έναν οργανισμό είναι σφάλμα ασφάλειας. Στο πλαίσιο της εφαρμογής η παραγωγή ενός τυχαίου uuid για την καταχώρηση ενός status resource δεν έχει αυτή την απαίτηση ασφάλειας συνεπώς έγινε επιλογή αυτού του τρόπου.

Η συμμόρφωση με το πρότυπο TAXII.

Το πρότυπο TAXII από την OASIS ορίζει με σαφήνεια ότι η λογική της ανταλλαγής των δεδομένων CTI πρέπει να κωδικοποιείται με REST API πάνω από HTTP χρησιμοποιώντας αυστηρά τα αντίστοιχα εργαλεία. Το Hyperledger Fabric λειτουργεί με gRPC calls [18] το οποίο λειτουργεί πάνω από το HTTP πρωτόκολλο.

Τα gRPC calls παρ όλα αυτά χρησιμοποιούνται εσωτερικά στο επίπεδο ελέγχου , αυθεντικοποίησης και μετάδοσης μηνυμάτων του Hyperledger Fabric επομένως έπρεπε να χρησιμοποιηθεί ένας διαφορετικός REST API Server για τη λογική TAXII της εφαρμογής. Εφόσον δε διατίθεται επίσημα μία αρχιτεκτονική για την ανάπτυξη ενός REST API Server με native εργαλεία πάνω στο Hyperledger χρησιμοποιήθηκε ένας ExpressJS Server εξωτερικά της υποδομής Fabric ο οποίος φαίνεται στην εφαρμογή ως client application [19] όχι ως Organization User.

Η συμμόρφωση με το πρότυπο STIX.

Το πρόβλημα του STIX Validation εμφανίζεται τόσο στην αρχιτεκτονική Blockchain όσο και στην αρχιτεκτονική Client Server καθώς είναι ένα πρόβλημα εγκυρότητας δεδομένων. Η λύση στο πρόβλημα της εγκυρότητας των STIX δεδομένων δίνεται από την OASIS στο αντίστοιχο repository [20]. Τα προβλήματα με τον STIX Validator είναι κατα βάση δύο

> **Η ελαστικότητα του προτύπου STIX.** Το πρότυπο STIX είναι ελαστικό με τους ορισμούς των CTI δεδομένων επιτρέποντας την υλοποίηση ενός υποσυνόλου του προτύπου. Το γεγονός αυτό οδηγεί πολλές φορές σε απόρριψη δεδομένων στην πραγματικότητα βάσιμων για την εκδοχή STIX που υλοποιείται [3].
>
> **Η επεκτασιμότητα του προτύπου STIX.** Το πρότυπο STIX επιτρέπει την επέκταση της γλώσσας για το χειρισμό δεδομένων που αφορούν συγκεκριμένες περιπτώσεις χρήσης οργανισμών μέσω των Extension Definitions. Η χρήση των extensions μπορεί να οδηγήσει σε απόρριψη δεδομένων από τον προκαθορισμένο validator STIX. [3]

Συνεπώς ο Validator εξαρτάται από την εκδοχή του STIX προτύπου που υλοποιείται και απαιτεί διαρκή παραμετροποίηση. Σε κάθε περίπτωση το πρόγραμμα είναι γραμμένο σε γλώσσα προγραμματισμού Python συνεπώς δεν ταιριάζει με τα περιβάλλοντα εκτέλεσης JavaScript/Typescript και Java ή την εκτελέσιμη GO που δίνει σαν επιλογές Chaincode το Hyperledger Fabric. Έχει υλοποιηθεί άρα ένας απλοϊκός validator με μορφή συνάρτησης JavaScript επί του API Gateway που

αναζητά κάποια βασικά λάθη σχετικά με το πρότυπο STIX και απέχει αρκετά από τον OASIS Validator.

Η πλήρης υλοποίηση των Private Data Collections.

Τα Private Data Collections είναι ο μηχανισμός που χρησιμοποιήθηκε για την υλοποίηση των δικαιωμάτων πρόσβασης επί των STIX Collections. Το Hyperledger Fabric παρ όλα αυτά δε διαθέτει μία πλήρη διεπαφή με τα Private Data Collections μέσω του Fabric SDK και λείπουν λειτουργίες οι οποίες είναι σημαντικές για την πλήρη υλοποίηση. Η μία λειτουργία η οποία λείπει και είναι σημαντική είναι η αντίστοιχη της getHistoryForKey για τα private data collections. Η συνάρτηση αυτή δίνει το ιστορικό ενός κλειδιού/asset και είναι κρισιμότατη λειτουργία τόσο για το blockchain όσο και το πρότυπο TAXII το οποίο απαιτεί versioning ακόμα και στη βασική του εκδοχή. Η δεύτερη λειτουργία η οποία λείπει είναι η αντίστοιχη της getQueryResultWithPagination για τα private data collections. Η λειτουργία του pagination σε ένα blockchain σύστημα χρησιμοποιείται πέρα από λόγους παρουσιασιμότητας και για αύξηση της επίδοσης των επερωτημάτων. Για τους δύο παραπάνω λόγους λήφθηκε η απόφαση τα private data collections να παραμείνουν σε ένα πειραματικό στάδιο μέχρι να υπάρξει η αντίστοιχη υποστήριξη από πλευράς Hyperledger Fabric.

Η υλοποίηση της μεθόδου DELETE Object

Η μέθοδος DELETE Object χρησιμοποιείται για να διαγραφεί ένα αντικείμενο STIX από μία συλλογή CTI. Στην περίπτωση της κλασσικής client server εφαρμογής η κλήση αυτή διαγράφει εντελώς αντικείμενο από το αντίστοιχο key value store που χρησιμοποιείται ως βάση δεδομένων. Σε ένα σύστημα blockchain παρ όλα αυτά υπάρχει η δυνατότητα για διαγραφή ενός κλειδιού αλλά μόνο επιφανειακά, δηλαδή από το current state. Αυτό σημαίνει ότι μετά την κλήση της deleteState του FabricSDK η επόμενη κλήση της getState δεν θα επιστρέψει ότι δεν βρέθηκε το κλειδί. Η κλήση

όμως της getHistoryForKey θα επιστρέψει κανονικά όλο το ιστορικό του κλειδιού με όλες τις παρελθοντικές τιμές του καθώς η συνάρτηση αυτή ανατρέχει όλο το blockchain αντί για το world state. Συνεπώς η υλοποίηση της μεθόδου DELETE Object θα μπορούσε να υλοποιηθεί σε ένα TAXII πάνω από Hyperledger Fabric σύστημα αλλά δε θα ικανοποιούσε πλήρως τα κριτήρια για διαγραφή και αυτό αφορά την εν γένει σχεδίαση των συστημάτων blockchain. [21]

6.2 Ασφάλεια και επιφάνειες επίθεσης

Στο κεφάλαιο αυτό γίνεται μία πιο λεπτομερής ανάλυση σχετικά με την ασφάλεια και τις επιφάνειες επίθεσης του συστήματος. Το μοντέλο απειλής σε μία εφαρμογή CTI συνοψίζεται στις παρακάτω δύο υψηλού επιπέδου κατηγορίες:

Επεξεργασία των δεδομένων κυβερνοασφάλειας

Η κατηγορία αυτή καλύπτει ένα ευρύ φάσμα κινήτρων και κακόβουλων παραγόντων από τον ίδιο τον οργανισμό , από άλλους οργανισμούς εντός του δικτύου blockchain και από εξωτερικές απειλές. Το κίνητρο του επιτθέμενου μπορεί να είναι η απόκρυψη ενός ίχνους , η μόλυνση του CTI Dataset με ψευδή δεδομένα για την απόκρυψη αυτών που έχουν πραγματική αξία ή η γενική αναστάτωση των διαχειριστών της πλατφόρμας. Η επεξεργασία των δεδομένων CTI μπορεί να γίνει από τρία διαφορετικά επίπεδα.

Κλήση της μεθόδου POST Envelope. Η μέθοδος POST Envelope είναι ο ορθός από άποψη προτύπου TAXII τρόπος να αλλάξουν αντικείμενα στο επίπεδο των δεδομένων. Η κλοπή των Basic Authentication Credentials του χρήστη θα μπορούσε να οδηγήσει σε τέτοιου τύπου επίθεση καθώς ο κακόβουλος παράγοντας μπορεί νόμιμα να καλέσει το REST API όντας αυθεντικοποιημένος ως χρήστης. Το ιστορικό παρ όλα αυτά του αντικειμένου δεν μπορεί να αλλάξει λόγω του αμετάβλητου ενώ η συναλλαγή του κακόβουλου παράγοντα δεν

μπορεί να αποσιωπηθεί επίσης. Επομένως δεν υπάρχει προστασία από αυτή την επίθεση αλλά υπάρχει ελεγξιμότητα.

Κλήση του chaincode transaction createOrUpdateObject. Η συναλλαγή αυτή καλείται από την παραπάνω μέθοδο για να αλλάξει την κατάσταση του blockchain. Παρ όλα αυτά μπορεί να κληθεί και αυτόνομα εκτός της μεθόδου POST Envelope εφόσον κάποιος κακόβουλος παράγοντας έχει υποκλέψει το πιστοποιητικό από την βάση δεδομένων η τα credentials του χρήστη. Στην περίπτωση αυτή ισχύει το ίδιο με την κακόβουλη χρήση της POST Envelope δηλαδή δεν υπάρχει προστασία αλλά ελεγξιμότητα.

Επεξεργασία σε επίπεδο βάσης δεδομένων. Η επίθεση αυτή μπορεί να πραγματοποιηθεί είτε με υποκλοπή των στοιχείων του χρήστη CouchDB είτε με αλλοίωση των δεδομένων κατά την αποστολή του αιτήματος στον Database Server. Η πρώτη περίπτωση καλύπτεται από το γεγονός ότι τα δεδομένα αποστέλλονται σε όλους τους οργανισμούς ενώ υπολογίζονται και τα αντίστοιχα hashes επομένως αυτή η επίθεση όχι μόνο δεν επιτυγχάνει το στόχο της αντιθέτως ειδοποιεί τα μέρη του δικτύου ότι υπήρξε αλλοίωση δεδομένων. Η δεύτερη περίπτωση καλύπτεται από την παρεμβολή TLS πρωτοκόλλου ανάμεσα στον Database Client και Database Server.

Ανάγνωση των δεδομένων κυβερνοασφάλειας

Η μη αδειοδοτημένη ανάγνωση των δεδομένων κυβερνοασφάλειας είναι η δεύτερη απειλή στο σύστημα CTI. Η διαχείριση και ο διαμοιρασμός του CTI θεωρείται κρίσιμη διαδικασία καθώς μπορεί να δώσει στρατηγικό πλεονέκτημα σε κακόβουλους παράγοντες, να βλάψει τη φήμη οργανισμών και να εκθέσει τη δομή του εσωτερικού δικτύου του οργανισμού. Η ανάγνωση των δεδομένων CTI μπορεί να γίνει από συγκεκριμένα επίπεδα

Κλήση της μεθόδου GET Objects. Η μέθοδος GET Objects είναι ο νόμιμος τρόπος να ανακτηθούν τα αντικείμενα σύμφωνα με το πρότυπο TAXII. Η υποκλοπή των Basic Authentication Credentials του χρήστη θα μπορούσε να οδηγήσει σε τέτοιου τύπου επίθεση καθώς ο κακόβουλος παράγοντας μπορεί

νόμιμα να καλέσει το REST API όντας αυθεντικοποιημένος ως χρήστης. Δεν υπάρχει κανένας τρόπος διάκρισης μεταξύ εξουσιοδοτημένων και μη κλήσεων.

Κλήση των Chaincode transactions queryAllCollectionObjects, queryObjectById, readObjectHistory, queryByDocType. Όλες οι παραπάνω συναλλαγές αλληλεπιδρούν με το blockchain και επιστρέφουν τα αντίστοιχα δεδομένα. Ανεπιθύμητη κλήση τους μπορεί να πραγματοποιηθεί εφόσων έχει κλαπέι ένα έγκυρο πιστοποιητικό του χρήστη ή τα credentials του στην οποία περίπτωση μπορούν να εκδοθούν (enroll) ανεμπόδιστα καινούργια πιστοποιητικά από τον κακόβουλο παράγοντα.

Ανάγνωση σε επίπεδο βάσης δεδομένων. Η επίθεση αυτή μπορεί να πραγματοποιηθεί είτε με υποκλοπή των στοιχείων του χρήστη CouchDB είτε με παρακολούθηση του καναλιού μεταξύ Database Client και Database Server. Η πρώτη περίπτωση είναι δυσκολότερη στην αντιμετώπιση καθώς δεν υπάρχει αντίστοιχος μηχανισμός με την προστασία εγγραφής ενώ η δεύτερη αντιμετωπίζεται με χρήση του TLS πρωτοκόλλου.

6.3 Μελλοντική βελτίωση

Στο κεφάλαιο αυτό θα παρουσιαστούν κάποια σημεία για μελλοντικές βελτιώσεις στο κομμάτι της λειτουργικότητας , της ασφάλειας και της επίδοσης.

Ανθεκτικότερο σχήμα αυθεντικοποίησης. Το βασικό πρότυπο TAXII χρησιμοποιεί για αυθεντικοποίηση το σχήμα Basic Authentication. Αυτό όπως έγινε σαφές και παραπάνω είναι το απλούστερο σχήμα αυθεντικοποίησης και παρουσιάζει κινδύνους. Μία ασφαλέστερη εκδοχή αυθεντικοποίησης θα μπορούσε να αξιοποιήσει το Basic Authentication σε συνδυασμό με Multi Factor Authentication για να κάνει generate ένα καινούργιο πιστοποιητικό. Ο συνδυασμός Basic Authentication και Multi Factor Authentication καλύπτει την περίπτωση όπου ένας κακόβουλος παράγοντας έχει υποκλέψει τα στοιχεία enrollmentID και enrollmentSecret καθώς η πιθανότητα να έχει πρόσβαση και στον επόμενο δεύτερο τρόπο αυθεντικοποίησης είναι ελάχιστη. Η

χρήση του πιστοποιητικού αντί για τα enrollmentID και enrollmentSecret έχει δύο βασικά πλεονεκτήματα. Το ένα είναι ότι εκτίθενται έλάχιστες φορές τα credentials του χρήστη πάνω απο κάποιο κανάλι ακόμα και κρυπτογραφημένο με TLS και το δεύτερο είναι ότι τα πιστοποιητικά είναι μικρής διάρκειας και εάν εκτεθούν σε κάποιον κακόβουλο παράγοντα μπορούν να ανακληθούν (revoke) [22]

Ενσωμάτωση STIX Validator στο Chaincode

Ένας τρόπος να υπάρξει συμφωνία δεδομένων και εξασφάλιση κοινού μορφότυπου είναι η επικύρωση των δεδομένων STIX μέσω του validator πριν αποθηκευτούν στον εκάστοτε TAXII Server. Αυτή τη στιγμή η επικύρωση των δεδομένων γίνεται σε επίπεδο API Gateway και μάλιστα σε πολύ απλοικό επίπεδο ενώ κάθε οργανισμός με αυτό τον τρόπο θα μπορούσε να παρεκλίνει από το πρότυπο STIX αφού επεξεργαστεί τον κώδικα του Gateway που είναι κατα βάση off chain. Για το λόγο αυτό προτείνεται σα μελλοντική βελτίωση η επικύρωση των δεδομένων να γίνεται στους peer nodes του Hyperledger Fabric μέσω Chaincode transactions. Αυτό θα έλυνε το πρόβλημα της συμφωνίας των οργανισμών σε μία κοινή λογική επικύρωσης δεδομένων καθώς ο κώδικας θα ήταν κοινός και ορατός από όλους. Επίσης ο κώδικας αυτός μπορεί να αλλάξει κάθε στιγμή μέσω της διαδικασίας του Fabric Chaincode Lifecycle με τρόπο συμφωνημένο και εγκεκριμένο από όλους τους οργανισμούς. [23]

Περαιτέρω συμμόρφωση με το πρότυπο TAXII

Στο πλαίσιο της εργασίας υλοποιήθηκε ένα υποσύνολο του προτύπου TAXII που ήταν εφικτό να μεταφερθεί σε μία αποκεντρωμένη πλατφόρμα όπως το Hyperledger. Η ενίσχυση των μηνυμάτων σφάλματος και των λειτουργιών, η υλοποίηση των προαιρετικών λειτουργιών και γλωσσικών χαρακτηριστικών του STIX και η γενικότερη αυστηρότητα στην ακολούθηση του προτύπου είναι πεδίο για μελλοντική βελτίωση της εργασίας.

Βιβλιογραφία

[1] «What Is Threat Intelligence,» [Ηλεκτρονικό]. Available: https://www.techtarget.com/whatis/definition/threat-intelligence-cyber-threat-intelligence.

[2] «Introduction to STIX,» [Ηλεκτρονικό]. Available: https://oasis-open.github.io/cti-documentation/stix/intro.

[3] «STIX v2.1 OASIS Documentation,» [Ηλεκτρονικό]. Available: "STIX v2.1 OASIS Documentation," [Online]. Available: https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html..

[4] «Introduction to TAXII,» [Ηλεκτρονικό]. Available: https://oasis-open.github.io/cti-documentation/taxii/intro.html.

[5] «What is Blockchain Technology,» [Ηλεκτρονικό]. Available: https://www.ibm.com/topics/what-is-blockchain.

[6] W. i. H. Fabric. [Ηλεκτρονικό]. Available: https://www.ibm.com/topics/hyperledger.

[7] «Hyperledger Fabric Model,» [Ηλεκτρονικό]. Available: https://hyperledger-fabric.readthedocs.io/en/latest/fabric_model.html#.

[8] «Understanding the Fabcar Network,» [Ηλεκτρονικό]. Available: https://hyperledger-fabric.readthedocs.io/en/release-1.2/understand_fabcar_network.html.

[9] «Securing Communication With Transport Layer Security (TLS),» [Ηλεκτρονικό]. Available: https://hyperledger-fabric.readthedocs.io/en/latest/enable_tls.html.

[10] «Private data,» [Ηλεκτρονικό]. Available: https://hyperledger-fabric.readthedocs.io/en/release-2.2/private-data/private-data.html.

[11] E. F.-C. R. a. Enrollment. [Ηλεκτρονικό]. Available: https://kctheservant.medium.com/exploring-fabric-ca-registration-and-enrollment-1b9f4a1b3ace.

[12] «TAXII Specification,» [Ηλεκτρονικό]. Available: https://docs.oasis-open.org/cti/taxii/v2.1/os/taxii-v2.1-os.html.

[13] «STIX Visualizer Repository,» [Ηλεκτρονικό]. Available: https://github.com/oasis-open/cti-stix-visualization.

[14] «Javascript Language,» [Ηλεκτρονικό]. Available: https://developer.mozilla.org/en-US/docs/Web/JavaScript .

[15] «Apache HTTP Server,» [Ηλεκτρονικό]. Available: https://httpd.apache.org/ .

[16] «JQuery Javascript Library,» [Ηλεκτρονικό]. Available: https://jquery.com/ .

[17] «Blockchain Random Numbers,» [Ηλεκτρονικό]. Available: https://blog.chain.link/random-number-generation-solidity/ .

[18] «Fabric Protocols,» [Ηλεκτρονικό]. Available: https://github.com/hyperledger/fabric-protos.

[19] «Fabric Client Application,» [Ηλεκτρονικό]. Available: https://hyperledger.github.io/fabric-sdk-node/release-2.2/Client.html.

[20] «STIX Validator,» [Ηλεκτρονικό]. Available: https://github.com/oasis-open/cti-pattern-validator.

[21] «Blockchain Data Removal,» [Ηλεκτρονικό]. Available: https://www.makeuseof.com/no-you-cannot-remove-data-from-the-blockchain-heres-why/#:~:text=The%20shortest%20answer%20to%20this,cannot%20be%20altered%20or%20deleted.

[22] «What is MFA,» [Ηλεκτρονικό]. Available: https://www.onelogin.com/learn/what-is-mfa .

[23] «Fabric Chaincode Lifecycle,» [Ηλεκτρονικό]. Available: https://hyperledger-fabric.readthedocs.io/en/latest/chaincode_lifecycle.html#:~:text=The%20Fabric%20chaincode%20lifecycle%20is,Upgrade%20a%20chaincode .